CRANFIELD UNIVERSITY

NAJWA HAYAATI MOHD ALWI

E-LEARNING STAKEHOLDERS INFORMATION SECURITY VULNERABILTY MODEL

SCHOOL OF APPLIED SCIENCES

PhD THESIS
Academic Year: 2008 - 2012

Supervisor: Dr Ip-Shing Fan
March 2012

CRANFIELD UNIVERSITY

SCHOOL OF APPLIED SCIENCES

PhD

Academic Year 2008 - 2012

NAJWA HAYAATI MOHD ALWI

E-LEARNING STAKEHOLDERS INFORMATION SECURITY VULNERABILTY MODEL

Supervisor: Dr Ip-Shing Fan
March 2012

This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

ABSTRACT

The motivation to conduct this research has come from awareness that the Internet exposes the e-learning environment to information security threats and vulnerabilities. Information security management as practised as a top down approach in many organisations tend to detach of people's responsibility in ensuring the security of e-learning. Literature has pointed out that people's behaviour required to be addressed to control the information security threats. This research proposes an ISM human behaviour model for e-learning provider in public universities in Malaysia. With socio technical reflection, this model aims to improve the implementation and management of information security in e-learning taking consideration of the user perspective.

This research consists of four phases, the Planning phase, Data Collection and Analysis Phase, Model development Phase and Discussion and Conclusion Phase. A pilot study highlighted data confidentiality difficulties and pointed to data collection by using existing public from multiple sources. Six multi-method studies were conducted to generate the dimensions for the model development. Review from expert confirmed the research findings and validated the practicality of addressing people behaviours in information security management.

This research contributes to better understanding of the people complexity in information security. The research suggests that the culture view of individual is significant in preparing information security management. This model makes clear the influence of people towards security threats and vulnerabilities. This approach can guide on what can be done to improve the stakeholder's participation and responsibilities on securing e-learning. This research is also extending the existing knowledge of information security and e-learning fields by analytically focussing on the intersection of both fields. New knowledge about the security in e-learning environment from the users' perspective is derived.

CANDIDATE BIOGRAPHY & PUBLICATIONS

This author holds Bachelor of IT and Master in IT from National University in Malaysia. The author has developed a strong interest in security since the completion of her post graduate study in 1999. She then increased her interest in e-learning during her first job. The experience of working in the first virtual private university in Malaysia has increased the interest in the information security aspect of e-learning. Currently the author is working as a lecturer in a public university and has since worked closely with e-learning implementation. It is a hope to raise the awareness of how essential information security management is to e-learning among users, with the work of this thesis.

The author has produced a number of publications regarding the research conducted and listed as below:

1. Alwi, N.H.M. and Fan, I. (2010), "E-learning and Information Security Management", *International Journal Digital Society (IJDS)* Vol.1, Issue 2.

2. Alwi, N.H.M. and Fan, I. (2010), "Threats Analysis for E-Learning, International", *Journal of Technology Enhanced Learning (IJTEL).*

3. Alwi, N.H.M. and Fan, I. (2012), "Cultural Views Inclusive in E-learning Risk Analysis", *8th International Conference on Information Science and Digital Content Technology (ICIS and IDCTA), June 26-28, Jeju, Korea (submitted)*

4. Alwi, N.H.M. and Fan, I. (2009), "Information Security Management in E-Learning", *Proceeding of International Conference on Internet Technology and Secured Transactions (ICITST) 2009, IEEE Xplore,* November 9-12, London, UK.

5. Alwi, N.H.M. and Fan, I. (2009), "Users' Perception in Information

Security Threats in E-Learning", *Proceedings International Conference on Education, Research and Innovation (ICERI 2009).* November 16-18, Madrid, Spain.

6. Alwi, N.H.M. and Fan, I. (2010), "Information Security Threats Analysis for E-Learning", *1st International Conference on Reforming Education and Quality of Teaching: Learning Technologies, Quality of Education, Educational Systems, Evaluation, Pedagogies-Tech Education 2010*, May 19-21, Athens, Greece.

7. Alwi, N.H.M. and Fan, I. (2010) "Information Security in E-Learning: A discussion of empirical data on information security and e-learning", *5th International Conference on E-Learning (ICEL) 2010,* July 12-13 July, Penang, Malaysia.

ACKNOWLEDGEMENTS

In the name of Allah, the Most Merciful, the Most Graceful.

This has been a long journey, although it is full with memories. The journey has indeed been unforgettable. Importantly, not everything has gone as planned, and not everyone understands the hardship. Nevertheless, a lot of lessons have been learned; and a lot of effort has been invested.

I would like to thank Dr Ip-Shing Fan, without whom this work would not be possible. His guidance and understanding is not comparable anywhere else and has guided my research through to the end. Moreover, his understanding concerning my family throughout the study has been greatly appreciated.

To my husband , my parent and my children, you are the source of inspirations with the word of wisdoms and straight talking, who has always been with me, supported my ups and down on this journey; thank you for your love and sacrifice, for which I will always be grateful. I dedicate this thesis to all of you.

To my friends who continuously improved my days at Cranfield University from the first day I arrived, Marini, Nani and Salwa and until the last day Hana and Tagrid, Wasim—thank you very much for your comfort and wonderful friendships. To the late night shift study team- Sara, Erin, Peter, Simon, Mohamad and Mustapha, the last six months wouldn’t have been manageable without you.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYM

Abbreviations / Acronym	Description
CIA	Confidentiality, Integrity, Availability
CNII	Critical National Information Infrastructure
Cultural Theory	Grid and Group Cultural Theory
EC	E-Learning Centre Personnel
EGA	Egalitarianism
FMEA	Failure Mode and Effect Analysis
FTL	Fatalism
HIE	Hierarchism
HLI	Higher Learning Institution
ICT	Information and Communication Technology
IND	Individualism
ISM	Information Security Management
ISMS	Information Security Management System
IT	IT Personnel
IWAS	Improving Web Application Security
LEC	Lecturer
MEIPTA	Malaysia E–learning in Public Higher Learning Institution (National Central Body)
MOHE	Ministry of Higher Education in Malaysia
MyCert	Malaysia Computer Emergency Response Team
OB	Organisational Behaviour
OC	Organisational Culture
OWASP	Open Web Application Security Project
RPN	Risk Priority Number

Security	In most context refers to information security
ST	Student
STS	Social Technical System
Study 1	User's Perception on Information Security in E-Learning
Study 2	Threats Analysis
Study 3	Incident Logging
Study 4	E-Learning and Its Information Security Issues in Malaysia
Study 5	Stakeholder Cultural View Modelling
Study 6	Cultural View inclusive Risk Analysis
TM	Top Management

1 INTRODUCTION

This thesis reports on a multi-method research on how to reduce the human risk of e-learning in public universities in Malaysia. The research was based on analytical process in the public domain knowledge from the literature. The overall aim is to study, analyse and develop a model on ISM that takes into consideration the behaviour and cultural views pertinent to social-technical state. This study looks to contribute to the approach of security culture cultivation, by correlating the culture view posed by the people in e-learning, with varying responses to security threats. Malaysian public universities have been chosen for the context of this research because Malaysia is among the early developing countries embarking on e-learning. Furthermore this research is being sponsored by the Malaysia Government.

This first chapter of the thesis presents the background of the research (section 1.1), specifies the research problem (section 1.2), presents the research aim and objectives (section 1.3) the research scope (section 1.4) the overview of the methodology used and the research process (section 1.5). This chapter also presents the research contribution (section 1.6) and outlines the structure of the thesis (section 1.7).

1.1 Background of Research

The growth of Information and Communication Technology (ICT) has a significant effect on people around the world. With this growth, people are able to connect with each other, especially through the Internet. The Internet itself is drastically changing the provision of services and goods, simply because of its features: immediacy, openness, ubiquity, and global reach. Services such as e-learning have been introduced widely and well accepted as the alternative method of pursuing study. However, despite the Internet being a place to obtain information and knowledge, it has also become the venue for a new set of illegal activities, which can cause real life threats, and causing security threats.

A lot of work has been done to provide technological solutions to address security threats. In addition to this, controls via management perspective were implemented with the development of information security management (ISM) procedures and standard. This section will further discuss ISM, e-learning security issues and e-learning in Malaysia in order to explain the background that influenced the execution of this study.

1.1.1 Information Security Management (ISM)

ISM standard has been developed since 1995 (use reference as BS 7799) and has been updated continuously. ISM includes policies, processes, procedures, organisational structures, software and hardware functions which work together to ensure that risk is sensibly managed.

Organisations have been urged to establish Information Security Management System (ISMS), in order to effectively manage threats and risks to the organisation's security information. ISMS can be executed by following a standard known as ISO/IEC 27001, which has been designed to ensure the selection of adequate and proportionate security controls. The standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the ISMS in organisations. Even with the implementation of ISMS, websites and information systems, infrastructures are not immune from attacks and threats, which show that the ISM effectiveness is not total. This situation has created the questions why and what is missing from the current ISM.

The ISM standards and procedures have been implemented by the organisations in such a way that emphasises the responsibility to comply is more with the management rather than the staff (end users). The organisations didn't realise that this method of implementation has not made users aware of their responsibility on security issues even though important parts of ISM that need participation from them. The differing attitudes and behaviour towards security issues have made the people dimension imperative in information security management strategies (Vroom and Von Solms, 2004). There are a lot

of ‘do and don’t’ guidelines to the users, but the importance of adherence has rarely been emphasised to the users. The implementation has not always observed. People have different tasks and roles in organisations. The exposure to security risks and responsibility thus varies.

1.1.2 E-learning Security Issues

E-learning is defined as the use of communication technologies and team learning systems for the purpose of enhancing the teaching and learning process. Gunasekaran et al. (2002) define ’e-learning’ as an education or training which takes place via a computer and is also known as Internet-enabled learning. As a consequence of e-learning having to depend on the Internet or, specifically, mostly via web applications, the e-learning environment has also become affected by security threats.

In late 2002, the Knowledgeville University in Southeastern US experienced an attack, which resulted in the server hosting the e-learning system application shutting down in the middle of a semester (Ramim and Levy, 2006). This situation consequently halted students’ and faculty members’ ability to perform the learning and teaching process. Having a denial of service or an interruption during online examinations and online classes would ultimately prove to be a disaster for students. Furthermore, students would similarly expect continuous availability along with the integrity of information provided by the e-learning provider to be unquestionable. Students will experience concern if information can potentially be tampered with or otherwise fabricated by an unauthorised party. The issue of information security threats also impact on the e-learning provider, consequently causing them to suffer a reduction in student enrolment and difficulties in terms of ensuring business continuity.

The information security threats for e-learning includes the loss of confidentiality, availability, exposure of critical data, and the vandalism of public information services (Graf, 2002). Other security threats are malicious software, hacking and denial of services, masquerade, fraud, data theft (Furnell and Karweni, 2001), passwords and URL management, non-repudiation (Warren

and Hutchinson, 2003), and unauthorised use of digital content (Weippl, 2005b). All these threats are application challenges that may occur and exist during the process of student enrolment, teaching and learning, assessment, and the awarding of the completion certificate via applications in an e-learning environment.

Both the e-learning provider and the user can be affected by security issues. The users include the staff and the students. Importantly, the e-learning provider needs to ensure that the e-learning environment is both safe and secure; thus, they need to recognise the vulnerabilities within the e-learning environment, and accordingly take the necessary action to overcome and reduce such occurrences. The students need assurance that the data and information received are not only reliable but also accurate, whilst staff need the systems to work fully, so as to efficiently deliver within the e-learning environment. Currently, e-learning is considered as part of normal IT and relies on the common ISM standard that is implemented to secure the whole IT system and website of e-learning providers. There is no specific ISM framework or model for e-learning.

1.1.3 E-Learning in Malaysia

E-learning in Malaysia began as early as 2000 and most e-learning implementation is blended learning (Fook et al., 2005). Blended learning has been recommended and used to resolve challenges and limitations of implementing e-learning in Malaysia. The early universities that have used blended learning include University Sains Malaysia (USM) and University Tun Abdul Razak (UNITAR). Among the challenges and limitations facing them are a of lack awareness on the effectiveness of e-learning, low adoption rates, lack of e-content, inadequate infrastructure, digital divide problem, bandwidth issues and connectivity, computer literacy and digital divide (Fook et al., 2005) and support and trust (Goi and Ng, 2009). These have indicated the insecure feeling among the students towards the new online method and system.

Though e-learning is claimed to have started more than ten years ago, Malaysia is still in the earlier stages of e-learning implementation. The Malaysia government have encouraged e-learning implementation among public universities. While the usage of e-learning in public universities in Malaysia increases, the threats would also increase. The situation regarding e-learning and security in Malaysia has yet to be explored.

1.2 Research Problem

This research was initiated to develop knowledge which would improve e-learning security in public universities in Malaysia. The initial stage of the research was to explore the wide range of security issues. As the knowledge develops, the research interest focuses on specific ISM for different user groups in e-learning. This lead to the research problem that this study addresses:

'What kind of ISM model that considers the people's behaviour can be developed to help the university's top management in ensuring the security of e-learning environment?'

In particular the variety of perception and behaviour of people that may make Malaysian e-learning vulnerable needs to be addressed.

1.3 Research Aim and Objectives

The major aim is to propose an approach for e-learning management or provider in public universities in Malaysia, in order to improve the implementation and management of information security in e-learning.

This research contains a number of objectives that incrementally build up to the research aim:

- To identify the information security issues in e-learning
- To identify threats and incidents in e-learning

- To define the current e-learning implementation and security in e-learning in Malaysia
- To design e-learning ISM human behaviour model (approach) appropriate to Malaysian characteristics

1.4 Research Scope

This research has been conducted using the existing knowledge from three main areas: information security, e-learning and Malaysia context. The reviews on the first two areas can be found in Chapter 2 and the latter in Chapter 3. The intersection of these three main areas is the focus of this research - the e-learning security in Malaysia, using the social technical approach of the public universities focusing on people.

1.5 Research Methodology

This research is carried out to propose an effective way to help the e-learning management in the implementation of ISM in e-learning, by developing an ISM model. With such purpose, this research is carried out in the constructive and interpretive paradigm, fitting in the qualitative research perspective. The research methodology is divided into four phases: Planning phase, Data Collection and Analysis Phase, Model development Phase and Discussion and Conclusion Phase. Figure 1-1 illustrated the research process of the four phases.

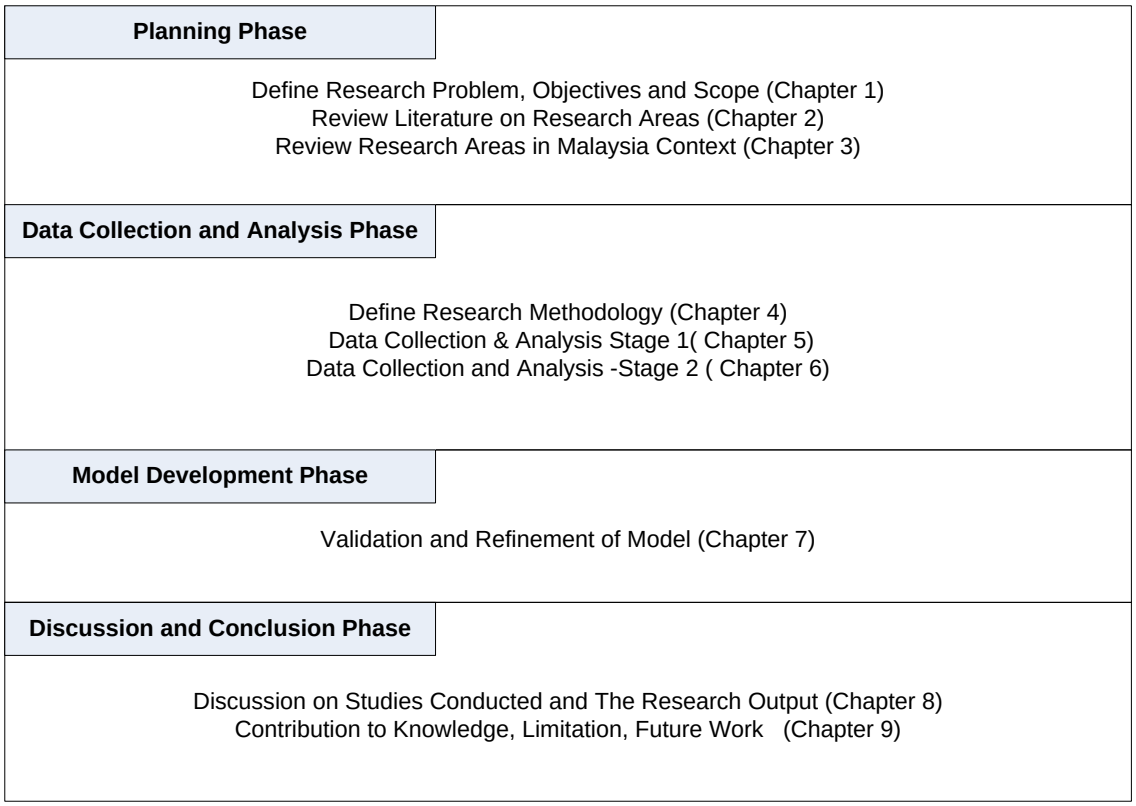


Figure 1-1 Four Phases of Research Methodology

1.5.1 Planning Phase

The Planning Phase studies the research topic and finds the literature gap. In this phase, the research problem, objective and scope were initially defined. In order to further understand the topic, the main research areas - information security, e-learning and Malaysia context have been reviewed. The literature review has revealed that little research has been conducted in securing e-learning. The reviews on information security and e-learning can be found in Chapter 2 and the Malaysia context is detailed in Chapter 3. At the end of the review, gaps and unknown situations are found. The output of this phase has lead to the definition of research requirement.

1.5.2 Data Collection and Analysis Phase

In this second phase, the research method is designed, based on the research problem and literature gaps found from the Planning Phase. A pilot study was also conducted to review security issues in the e-learning environment. This study has indicated that the best way to collect data is by using the existing knowledge that can be found from multiple sources. This research is conducted with a qualitative research strategy using multi methods of data collection and analysis. The multi methods are chosen, as the pilot study has indicated that data are difficult to collect due to the private and confidential issue. The data collection and analysis are conducted in two stages as depicted in Figure 1-2.

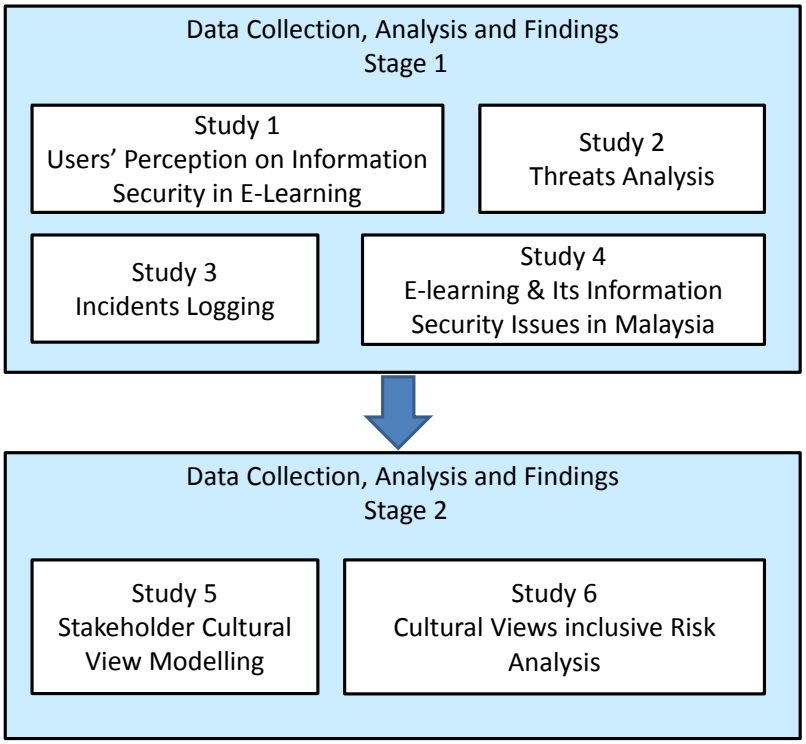


Figure 1-2 Data Collection Analysis and Findings Stages

The first stage attempts to understand and identify the requirement of security in e-learning which resulted in the identification of the dimensions for ISM model. Four studies have been carried out in the first stage. The output of the first stage identified insider as one of the main threats and focus studies in the

second stage, which is to understand cultural views and their impact on e-learning. Two studies have been carried out in the second. The outputs of second stage correlate the cultural view with different types of responses to threats. The methods used in these data collections and analysis phase includes an online questionnaire, interview, and document analysis. This phase has contributed to the building model of ISM for e-learning. Details on research methodology are described in Chapter 4, while details on stage 1 and stage 2 activities have been written separately in Chapter 5 and Chapter 6.

1.5.3 Model Development Phase

In this phase, model validation activity is carried out. Expert reviews on the research findings and model were performed. The open ended questionnaire was used to extract the experts' opinion regarding the model potential and applicability of the research findings. Description on the experts review is in Chapter 7.

1.5.4 Discussion and Conclusion Phase

The final phase reflects on the development as a part of academic research. The discussion addresses the aim and the objectives, while the conclusion summarises the research contribution and future work. This phase can be found in Chapter 8 and Chapter 9.

1.6 Contribution to Knowledge

This research has contributed to the three communities as discuss below.

1.6.1 Information Security Community

This study is a significant endeavour to address the human risk of e-learning. Previously, security emphasis was made to the technological solutions. With this research, it guides on dealing with the complexity of people towards

information security. This study indicates that the cultural views of individuals are significant in the preparation of information security management.

Currently, Internet threats are using the social engineering techniques which are manipulating perceptions and attitudes towards IT. This study shows the way to control these threats, such as spam, phishing and other social engineering threats. In addition to using the technological control this study provides insight into security control by addressing cultural views.

1.6.2 E-learning Community

The outcome of this research is to provide the model of information security management for the e-learning environment. This model will allow the e-learning provider to manage the security of e-learning from a different angle - the user/human risk perspectives. It would be beneficial to the provider to classify the suitable controls and solution to increase the awareness of their employees towards security.

This study extends the existing knowledge of information security and e-learning fields by analytically focussing on the intersection of both fields. New knowledge about the security in e-learning environment is thus derived. Although much research has been carried out on information security, no single study exists which adequately covers cultural views on e-learning environment. This study suggests that the relationship between the cultural views of the people in e-learning with different types of responses to security threats.

1.6.3 Others E-Services Community

The model can be replicated for other e-services. Although this model has initially been developed for e-learning environment, the existing components such as stakeholders, application and process can easily be replicated, mapped, traced and analysed for other e-services.

This research also strengthens the new knowledge on the e-learning and security in the Malaysia context. The government of Malaysia can use the

model as a guideline to design suitable training and education modules to improve and increase the security awareness among its citizens.

1.7 Thesis Structure

This thesis is presented in nine chapters. The summary of each chapter is provided below.

Chapter 1: Introduction

This chapter provides the background of the research, research aim and objectives; and the research scope. In addition this chapter, brief on the methodology used up to the contribution to knowledge.

Chapter 2: Literature review

This chapter provides reviews on two main areas of research: e-learning and information security. This chapter will review the existing conditions of security in e-learning. Included in the review is the organisation culture and Socio Technical System (STS). The research gaps from the two main reviewed topics are listed.

Chapter 3: Malaysia Context

This chapter presents the Malaysia background, particularly on the e-learning and security implementation. This chapter attempts to explain the characteristics of security in e-learning in public universities in Malaysia.

Chapter 4: Research Methodology

The chapter presents the methodology used in this research. The methodology discussed here includes the research perspectives and research design. In addition, the research processes are shown.

Chapter 5: Exploring E-Learning Security

This chapter elaborates on the exploration on e-learning security via four multi-method studies. The purpose, method and findings for each study are detailed in this chapter.

Chapter 6: Development of E-Learning Stakeholders Information Security Vulnerability Model

This chapter explains the experimentation in building the model for e-learning. There are two studies conducted in this stage. Each study in this chapter is detailed with the purpose, methodology, results and finding. This chapter presents the model developed, -namely the E-learning Stakeholders Information Security Vulnerability Model.

Chapter 7: Security Countermeasures Designed with Vulnerability Model

This chapter presents the feedback obtained from the experts, with the ISM background on illustration of countermeasures to represent the cultural viewpoints. The feedback represents the sensibility, potential, impact and applicability of the research findings.

Chapter 8: Discussions

This chapter provides the research findings as achievement of the research aim and objectives. Remarks on advancement of the findings to literature are also discussed.

Chapter 9: Conclusions

The chapter re-visits the aim aims and objectives, providing a summary of the research process and findings. The chapter presents the contribution to theoretical knowledge, research limitations and future work. The thesis ends with the research conclusion.

2 LITERATURE REVIEW

A large body of literature on both Information Security and E-learning research areas provides a basis for the present study. This chapter explains the process in reviewing that literature (section 2.1) and then examines the concepts of two research areas - Information Security (section 2.2) and E-learning (section 2.3). Prior to the section on the e-learning concept discussion, a review on information security in e-service is discussed (section 2.2.7). In addition, this chapter will present the previous studies conducted on information security in e-learning which is the intersection of both main research areas (section 2.4).

In the second year of research, the research focus moved towards addressing the human element of unintended security threats, literature reviews on socio-technical (section 2.5) approach and organisational culture (section 2.6), is added.

2.1 Literature Search Process

The following review was developed through a systematic literature review approach (Hylton and Lewis, 2006). It was conducted systematically by the identification of the research topic and evocation of basic keywords from the research topic. From here, useful and related sources were identified. As this research is carried out, other pertinent keywords for the literature review emerged accordingly.

The topic for this research is the information security management in e-learning which is the intersection of the two main areas, namely information security and e-learning. Therefore, the concepts of both main areas need to be comprehensible too. The literature review was conducted by searching using keywords related to the research topics. Search activities were accomplished using international databases such as Elsevier Science Journal (Science Direct), IEEE (Com Soc & Xplore), ACM Digital library, Ebscohost, AIS Electronic Library (AiSel), ProQuest (ABI/INFORM), Emerald Management First

and Google Scholar. The main keywords used include information security and e-learning, with some alternative words for information security, such as, computer security, threats, data security, safety and some alternative words for e-learning such as, distance learning, computer-based learning, Computer-Supported Collaborative Learning (CSCL), Technology- Enhanced Learning (TEL), Learning Management System (LMS). The literature resources searched include, journal articles, conference papers, white papers, magazines, books, and articles from trusted websites (websites of relevant associations, societies, centres of excellence and government bodies) of both research areas.

The duration for searching published studies or articles for the literature review is set between 1990 and 2011. As the research emerges, the choice of keywords expands and the time period is changed, based on each study's objectives. The literature review step is a continuous process performed throughout the duration of the research.

2.2 Information Security

A large and growing number of literatures have reported on ensuring the safety of data, information and system. The following subsections explain the concepts of information security, including definition, principles, information as an asset, the threats and risks, the controls, including the standards to achieve the objectives and principles of security and finally the overview of information security in e-services.

2.2.1 Definition

In the past, information security has been known by different names, such as IT security, computer security or data security. However these terms, with the exception of data security, disregard the fact that information contained on the computers is worth many times more than the computer itself. Legally, information security means protecting information and information systems from unauthorised access and use, disclosure, disruption, modification, perusal,

inspection, recording or destruction, in order to meet the information security principle (Legal Information Institute, 1992).

Gollman (1999), Pfleeger and Pfleeger (2007) and Stallings (2007) claim that information security involves controlling access to information assets to ensure Confidentiality, Integrity and Availability (CIA) of the assets to legitimate users at all times. The information assets are discussed in section 2.2.3. The latest definition by Whitman and Mattord (2011) has suggested the protection of information is needed, whether in storage, processing, or transmission.

In conclusion, information security includes complete protection of information in storage, processing, or transmission mode to ensure the CIA and to avoid the fabrication, modification, interruption and interception of the respective information.

2.2.2 Principle of Information Security

The three core principles of information security are the CIA as mentioned above in the definition section. Figure 2-1 illustrates the principles of information security. Each principle can be defined as follows:

Confidentiality is the protection of information in the system so that unauthorised persons cannot access it. It is a requirement to keep sensitive information from being disclosed to unauthorised users (Jung et al., 2001). Confidentiality can be compromised in several ways. The following examples are some of the most commonly encountered threats to information confidentiality: hackers, masqueraders, unauthorised user activity, unprotected downloaded files, local area networks (LANs), and Trojan horses.

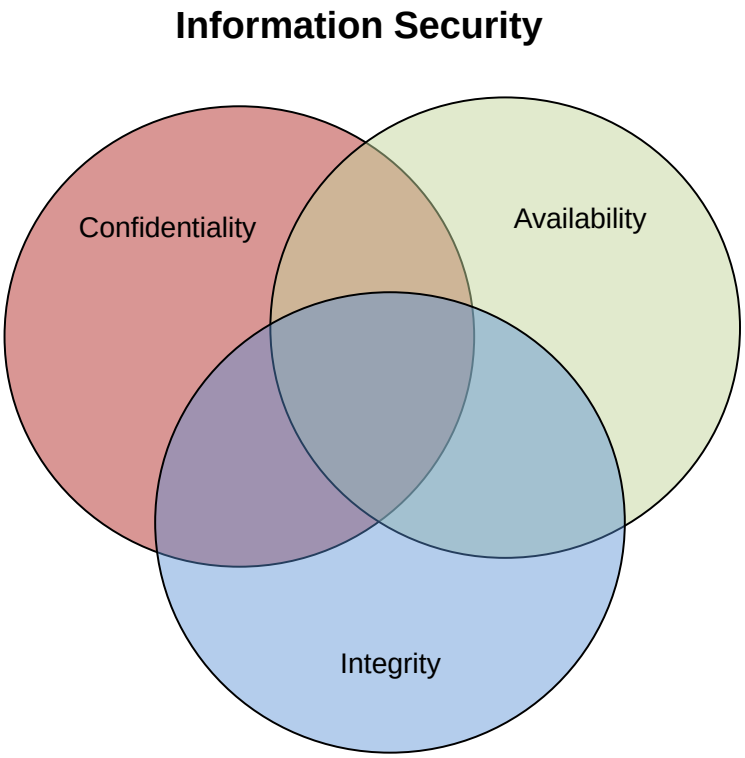


Figure 2-1 Information Security Principles

Integrity is the assurance that the information is authentic and complete. The integrity of data depends not only on whether the data is 'correct', but whether it can be trusted and reliable. Integrity is an indication of the information accuracy and reliability (Jung et al., 2001). Integrity depends on access controls; therefore, it is necessary to positively and uniquely identify all persons who attempt access. Similar to confidentiality, integrity can be compromised by hackers, masqueraders, unauthorised user activity, unprotected downloaded files, LANs, and unauthorised programs (e.g., Trojan horses and viruses) where each of these threats can lead to unauthorised changes to data or programs. For instance, authorised users can accidentally or intentionally corrupt data and programs, if their activities on the system are not properly controlled.

Meanwhile, availability is the assurance that a computer system is accessible by authorised users whenever needed (Tipton and Krause, 2007). Two facets of

availability typically discussed are denial of service and loss of data processing capabilities. This principle is very important to e-services, as the business transactions are highly dependent on information provided electronically, thus it needs to exist (Further discussion in section 2.2.7 Information Security in E-Services).

These three principles have been at the root of information security since the conception of computing and there is a growing need for information security. With the evolution of technology and its usage, authenticity and non-repudiation has been introduced (Tipton and Krause, 2007). It is important to validate the authenticity of the parties involved that they are who they claim to be, to ensure transactions via internet are genuine. On the other hand, non-repudiation implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction. It is common nowadays for e-services to use technology such as digital signatures and encryptions to establish authenticity and non-repudiation.

2.2.3 Information Assets

According to the definition in section 2.2.1, information needs to be protected. Information assets are sometimes referred to as information resources and include hardware, software and people that organisations use to perform computing tasks (Pfleeger and Pfleeger, 2007). Evans (2003) in Information Security Guideline for New South Wales (NSW) Government has defined an asset as below:

"'An asset is something that the agency values and therefore has to protect. Assets include all the information and supporting items that an agency requires to conduct its business. Example of assets includes:

- *Information/data (e.g. files containing payment details, voice records, images files, product information, manuals and continuity plans);*

- *Paper documents (e.g. contracts, completed forms)*

- *Software (e.g. system software, application software, developments tools and utilities)*
- *Physical equipment (e.g. computer and communication equipment, environmental equipment, furniture, accommodation)*
- *Services (e.g. computing and communication services, service providers and utilities)*
- *People and their knowledge(e.g. technical, operational, marketing, legal, financial, contractors and consultants, outsource providers)*
- *Image and reputation of the organisation "*

Assets as described earlier may be called information which can exist in many forms. As suggested by ISO 17799, information is an asset which can be "*printed or written on paper, stored electronically and transmitted by post or by using electronic means. Whatever forms that information takes, or means by which it is shared, it should always be appropriately protected from any possible information security threats*."

2.2.4 Information Security Threats

A threat is any circumstance or event with the potential to harm an information system through unauthorised access, destruction, disclosure, modification of data, and/or denial of service (Committee on National Security Systems (CNSS), 2006). Information security threats can be discussed from many different perspectives such as: source of threats (internal or external), type of threats (deliberate or accidental), type of impact (fabrication, modification, interception, or interruption), severity of impact (operational impact, monetary impact, regulatory impact, or reputation impact) and likelihood of occurring (very likely, likely, unlikely, very unlikely). Nevertheless, all of these perspectives are somehow related to each other. This view is supported by Al-Zubi (2010) who suggested the threats chain: threats source – factor (Vulnerability) – threats (Action) – Implications (Attack).

2.2.4.1 Threats Source

Basically information security threats can be classified into three categories (Parker, 1981): natural disasters, errors or omissions, and intentional acts. The first two are accidental and the last is deliberately conducted. The source of security threats can be laid out as in Figure 2-2. The main source of security threats are people and natural disasters.

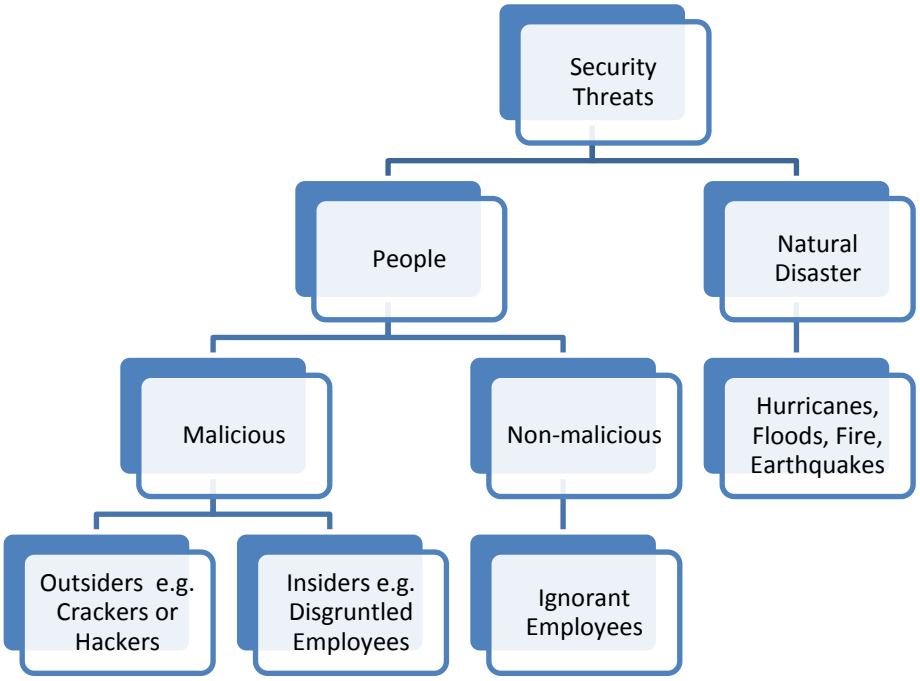


Figure 2-2 Source of Security Threats

Source: Microsoft Technet, 2009

Natural disasters which include hurricanes, floods, fire and earthquakes can cause severe damage to computers and information systems. Although natural disasters cannot be prevented from taking their course, the best approach is to have a business continuity plan and disaster recovery plans in place (Microsoft Technet, 2009).

People can be the source of threats, either by maliciously harming or accidently disrupting the organisation by their non-malicious acts. Malicious people, who are known as attackers, could be outsiders or insiders of organisations. Outsiders are people with no authorisation or who intentionally overstep their bounds on systems for which they do not have legitimate access and are called

hackers or crackers. However, the most dangerous are usually the malicious insiders, such as disgruntled employees or former disgruntled employees as they know many of the codes and security measures in the organisation (Furnell, 2004). An insider threat comprises of (posed by) an individual with privileges who misuses them or whose access results in misuse (Hunker and Probst, 2011). The insider threats have been predicted and listed as one of the top potential security threats in 2011 by security websites (Lingenfelter, 2011; SecurITy Pub, 2010; Underwood, 2010; Help Net Security, 2010).

The non-malicious threats are usually from employees who are “untrained” in computers and are unaware of security threats and vulnerabilities (Microsoft Technet 2009). Users, data entry clerks, system operators, and programmers frequently make unintentional errors that contribute to security problems, directly and indirectly. Sometimes the error is the threat (Whitman, 2003), such as a data entry error or a programming error that crashes a system. In other cases, errors create vulnerabilities and errors can occur in all phases of the system life cycle.

2.2.4.2 Factor (vulnerabilities)

Another way to understand the information security threats is by identifying the vulnerabilities. ISO/IEC 27005:2008 defines vulnerabilities as a weakness of an asset or group of assets that can be exploited by one or more threats. The vulnerability will define the possible threats (action) and implications (attack). The ISO/IEC 27005: 2008 standard also states that vulnerabilities are classified according to the asset class they relate to. Table 2-1 shows the ten categories of vulnerabilities that apply to the web-based application.

Table 2-1 Application Vulnerabilities Categories

Category	Threats / Attacks
Input Validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Authentication	Network eavesdropping; brute force attacks; dictionary attacks; cookie replay; credential theft
Authorisation	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorised access to administration interfaces; unauthorised access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive data	Access sensitive data in storage; network eavesdropping; data tampering
Session management	Session hijacking; session replay; man-in-the-middle
Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

Source: (Meier et al., 2003)

With reference to the standard definition of vulnerabilities above, people, as assets to an organisation that hold information, can be vulnerable, even though they have no intention of bringing any threat. A recent technique used in exposing information to a threat is known as social engineering. Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques (Workman, 2007). With the use of this technique, further actions and attacks seem to be more easily accomplished and are less traceable.

2.2.4.3 Threats (Action) – Implications (Attack).

The information security threats (action) are varied and can be found in many security books and websites. A list of threats (Bagad, 2008) is summarised in Table 2-2. The threats are listed in three main high level categories with examples of threats and their definition. The categories are malicious (intentional), non-malicious (unintentional) and physical threats.

The implication of the above mentioned actions lead to data and information to be disclosed, modified, lost and destructed, and interrupted. This outcome is illustrated in Figure 2-3 translated as interception, modification, fabrication, interruption (Pfleeger and Pfleeger, 2007; Stallings, 2007). Each is defined as below.

- Interruption- an information asset is destroyed or becomes unavailable or unusable. This is an attack on availability.

- Interception- unauthorised entity gains access to an information asset. Interception outcome is basically an attack on confidentiality. The unauthorised entity could be a person, a program or a computer.

- Modification- unauthorised entity not only gains access but also tampers with an asset. This is an attack on integrity.

- Fabrication- unauthorised entity inserts counterfeit objects into the system. This is an attack on authenticity.

Table 2-2 Categories of Threats

Category	Threats	Definition
Malicious (Intentional) Threats		
Software	Virus	Malicious software that attaches itself to the other software.
	Worm	Malicious software which is a standalone application.
	Trojan horse	A worm which pretends to be a useful program or virus which is purposely attached to a useful program prior to distribution.
	Time bomb	A virus or worm designed to activate at a certain date/time.
	Logic bomb	A virus or worm designed to activate under certain conditions.
	Rabbit	A worm designed to replicate to the point of exhausting computer resources.
	Bacterium	A virus designed to attach itself to the OS in particular (rather than any application in general) and exhaust computer resources, especially CPU cycles.
Spoofing	Spoofing	Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network.
	Masquerade	Accessing a computer by pretending to have an authorised user identity.

Scanning	Sequential scanning	Sequentially testing passwords/ authentication codes until one is successful.
	Dictionary scanning	Scanning through a dictionary of commonly used passwords/authentication codes until one is successful.
Snooping (eavesdropping)	Digital snooping	Electronic monitoring of digital networks to uncover passwords or other data.
	Shoulder surfing	Direct visual observation of monitor displays to obtain access.
Scavenging	Dumpster diving	Accessing discarded trash to obtain passwords and other data.
	Browsing	Usually automated scanning of large quantities of unprotected data (discarded media or online “finger” type commands) to obtain clues as to how to achieve access.
Spamming	Spamming	Overloading a system with incoming message or other traffic to cause system crashes.
Tunneling	Tunneling	Any digital attack that attempts to get “under” a security system by accessing very low level system functions (e.g., device drivers, OS kernels).
Unintentional Threats		
Malfunction	Equipment malfunction	Hardware operates in abnormal, unintended mode.
	Software malfunction	Software behaviour is in conflict with intended behaviour.

Human error	Trap door (back door)	System access for developers inadvertently left available after software delivery.
	User/operator error	Inadvertent alteration, manipulation or destruction of programs. Data files or hardware.
Physical Threats		
Physical environment	Power loss	Computers or vital supporting equipment fail due to lack of power.

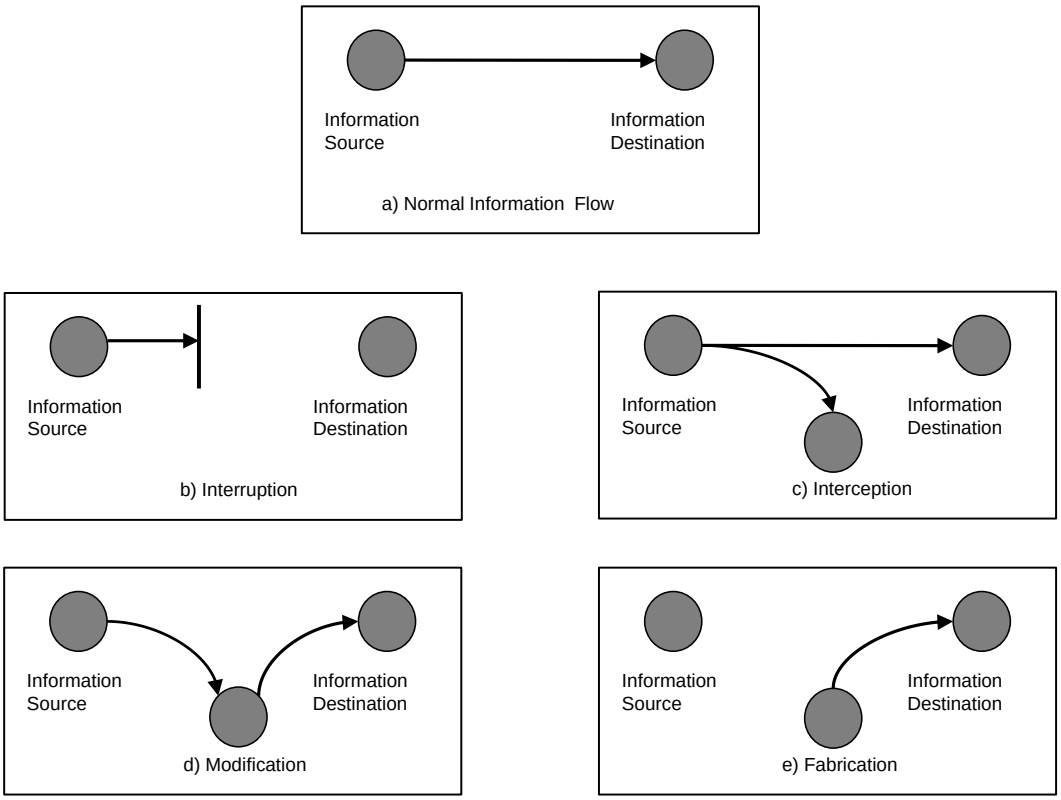


Figure 2-3 Outcome of Security Breach

(Source: Stallings, 2007)

Information security threats can be viewed in many different perspectives such as threats source – factor (vulnerability) – threats (action) – implications (attack). These different perspectives are connected and it is vital that they are understood in order to assess the possible risk and design controls appropriate to an organisation.

2.2.5 Security Risk

The likelihood that an information security threat will exploit a vulnerability to cause harm creates a security risk. When a threat does use a vulnerability to inflict harm, it has an impact on the information security principles and creates risk such as loss of availability, integrity, and confidentiality. Being “at risk" is being exposed to threats. Pfleeger and Pfleeger (2007) defines security risk as referring to relative exposure of an information asset and the probability or likelihood that the asset can be compromised plus the possible loss. Risk can be translated as the formula below:

Risk = Threat x Vulnerability

It is established that the risk, threats and vulnerabilities are closely related and Figure 2-4 exemplifies the relationship between them.

Pfleeger and Pfleeger (2007) highlight that “*computer items* (including information) *must be protected only until they lose their value. They must be protected to a degree consistent with their value”*. Thus ensuring the value, it is important to identify the risk. The process of identifying the risk is called risk management.

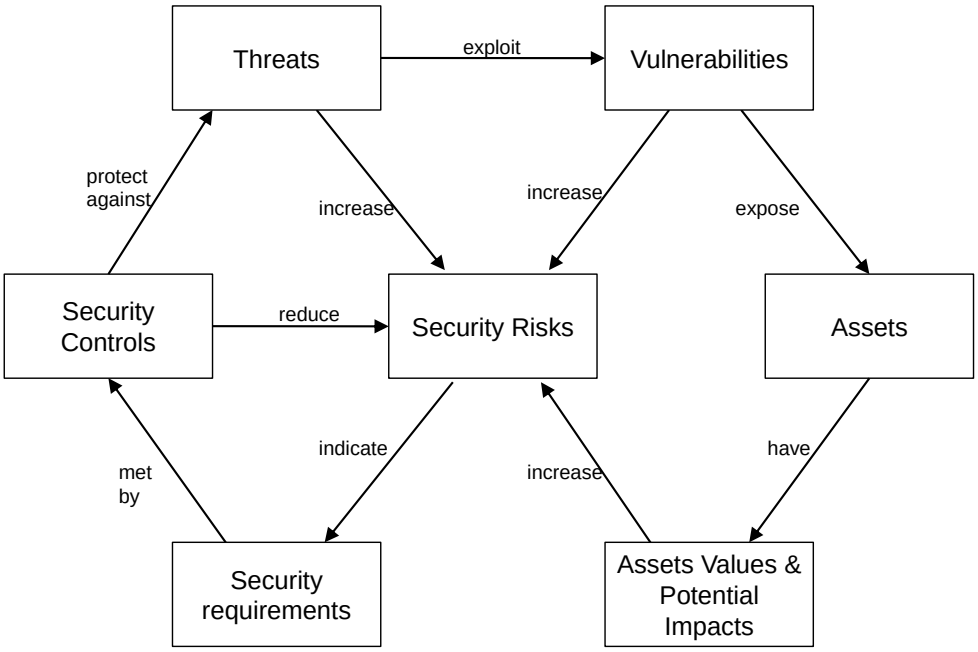


Figure 2-4 Risk Concept Relationship

(Source: Australian Standard Handbook of Information security risk management – HB231:2000)

2.2.5.1 Risk Management

Caelli et al. (1989) writes that risk management aims to *"identify, measure and control uncertain events*" in order to minimise loss and optimise the return on the money invested for security purposes. The CISA Review Manual by ISACA (2006) provides the following definition of risk management: "*Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organisation"*. Risk management is also strategies consisting of policy options that have varying effects on risk, including the reduction, removal, or reallocation of risk. The

ultimate goal is to help organisations to better manage IT-related mission risks. One of the tasks in risk management is conducting risk analysis.

2.2.5.2 Risk Analysis

A range of techniques and tools can be used to analyse risks. The results of the risk analysis process are used to produce a risk profile which gives a significance rating to each risk and provides a tool for prioritising risk treatment efforts. This ranks each identified risk to provide a view of the relative importance. This process allows the risk to be mapped to the business area affected, describes the primary control procedures in place and indicates areas where the level of risk control investment might be increased, decreased or reapportioned.

In the context of information security, threats are analysed with respect to their likelihood of occurrence, their possible impact on individual users and the system, and the global risk they represent. It is common to carry out threats analysis, risk analysis or Failure Mode and Effects Analysis (FMEA). FMEA is a structured, proactive technique which actively identifies the ways by which a product or process can fail, and ways in which to accordingly prevent such failures (McDermott et al., 2009).

According to Weippl (2005b), there are five common steps in most risk analysis approaches: identification of assets; estimation or calculation of threats and risks; setting priorities; implementation of controls and counter measures; and the monitoring of risks and of the effectiveness of counter measures. These steps have similarities with other approaches concerned with the handling of web applications, such as Open Web Application Security Project (OWASP) and the Improving Web Application Security (IWAS) guide (Meier et al., 2003). IWAS proposes a threat modelling approach comprising five steps: identify security objectives; application overview; decompose application; identify threats; and identify vulnerabilities. IWAS also includes application security vulnerabilities' categories (Table 2-1) in the approach. At the end of the analysis process, countermeasures or control will be suggested.

2.2.6 Control

Security controls are safeguards or countermeasures that reduce a threat, a vulnerability, or an attack. Controls to secure information can be categorised as physical, technical, and administrative (Tipton and Krause, 2007). Physical security is the use of any physical measures e.g. identity card, locks, alarms to control the access to building, computer, equipment, and the processing resource itself. The technical security, occasionally referred to as logical controls, involves protection integrated in the computer hardware, operations or applications software, communications hardware and software, and related devices. Administrative security is established to provide protection in managerial context. This includes management constraints, operational procedures, accountability procedures, and supplemental administrative controls. These three categories of controls can be further classified as either preventive or detective as Figure 2-5.

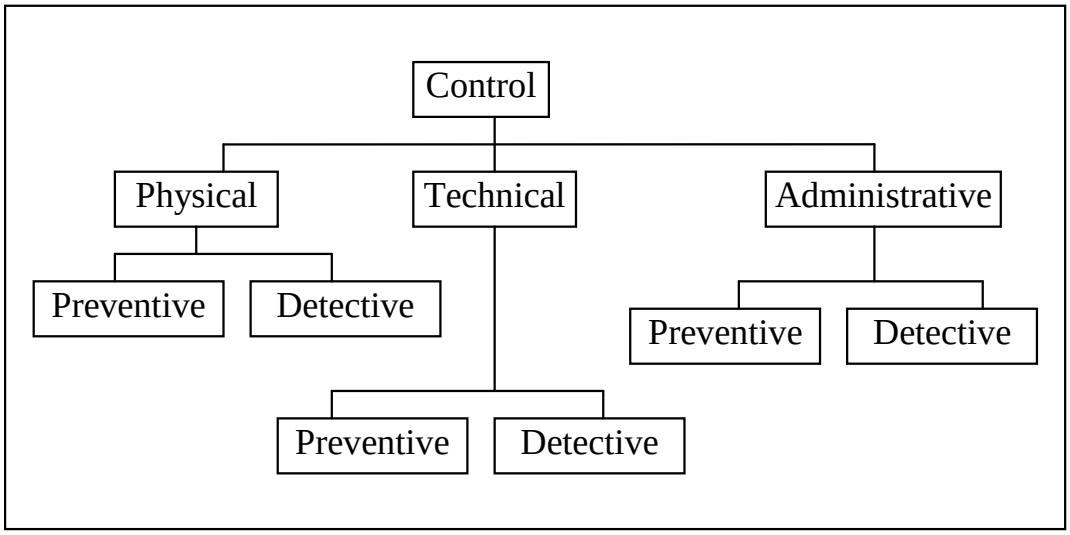


Figure 2-5: Categories of Controls

Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Detective controls comprise audit trails, intrusion detection methods, and checksums (Tipton and Krause, 2007). Preventive controls usually restrain

the use of computing resources. Therefore preventive controls need to engage with the users so that they are willing to accept the controls in their job roles. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems (Tipton and Krause, 2007). Under the definition of administrative controls, information security management is being established.

2.2.6.1 Information Security Management

Information security management (ISM) describes controls that an organisation needs to implement to ensure that it is sensibly managing the risks. An ISM embraces policies, processes, procedures, organisational structures and software and hardware functions. A systematic approach of ISM to manage organisation information is known as Information Security Management System (ISMS). This approach encompasses people, processes and IT systems. ISMS is also interchangeably known as standard or guideline. The best known ISMS is described in ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002. The first standard provides the overview and vocabulary used in ISMS is ISO/IEC 27000: ISMS Overview and Vocabulary. While the two later standards have a bigger contribution which explains in detail the requirements and method of implementation.

ISO/IEC 27001 published in 2005 is known as ISO/IEC 27001: Requirements. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof. ISO/IEC 27002 is known as ISO/IEC 27002: Code of practice for information security management. ISO/IEC 27002 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002

contains best practices of control objectives and controls in the following areas of information security management:

- security policy
- organisation of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management
- compliance

Competing standard is the Standard of Good Practice (SOGP) developed by Information Security Forum (ISF). It is more best practice-based as it comes from ISF's industry experiences. Other frameworks are Control Objectives for Information and related Technology (COBIT) by Information Systems Audit and Control Association (ISACA) and Information Technology Infrastructure Library (ITIL). Both touch on security issues, but are mainly geared toward creating a governance framework for information and IT more generally. COBIT has a companion framework Risk IT dedicated to Information security. One thing in common is that, these standards have not taken human behaviour much into account Similarly Al Aziz in 2008 claimed that there is no characteristic of human behaviour and awareness in the security standard such as BS7799 (earliest version of ISO/IEC 27001), BSI IT COBIT and GASSP. Table 2-3 shows the components of each standard and guideline.

Table 2-3 Information Security Standard and Guideline

ISO/IEC	SoGP	COBIT	ITIL
• ISO/IEC 27000: ISMS Overview and Vocabulary • ISO/IEC 27001: ISMS requirement • ISO/IEC 27002: • Code of Practice for ISM	• Computer Installations Networks • Critical Business Applications • End-User Environment • Systems Development • Security Management	• Framework • Process descriptions • Control objectives • Management guidelines • Maturity models	• ITSM • Service Support • Service Delivery • ICT Infrastructure Management • Security Management • The Business Perspective • Application Management • Software Asset Management

2.2.7 Information Security in E-Services

The evolution of the Internet has brought interconnectivity between consumers and service providers to a new dimension of e-services. Rowley (2006) defines e-services as actions and performance delivered by information technology. The increasing Internet usage has initiated e-services for banking, shopping, learning, healthcare and government (Yee et al., 2006). E-services have led to changes in the strategies of businesses development, where companies have to consider and introduce the use of e-services to be more innovative and competitive (Scupola, 2008).

Service quality models for e-services claimed by Kang and James (2004) include reliability, assurance, tangibility, empathy, and responsive. In the online

environment, reliability reflects the capability of the company to provide accurate information on the respective products. Assurance might reflect the confidence that the customer can get when they trust and purchase products from the seller. Tangibility refers to the design of the user interface that might provide contact between the customer and the online firm. Empathy would be the customization on the interface that the customer might enjoy. Lastly, the responsiveness might be in terms of timely response to e-mail requests or complaints, and confirmation of orders, etc. All of these elements are related to the information security elements and principle. There are vulnerabilities and flaws in e-services such as *"weak cryptography, software implementation, social engineering and human factors, bad failure-recovery procedures*" (Hassler, 2001). Sheth and Sharma (2007) identified some challenges in e-services including fraud on the Internet space which is estimated around 2.8 billion USD and privacy due the emergence of various types of spyware and security holes. Security is the most important challenge that faces the implementation of e-services. People want to be assured that they are safe when they are conducting online services and that their information will remain secure and confidential.

Currently there are many studies and discussions on securing e-banking, e-commerce and e-government as these services involve monetary value. E-learning though seems to have a lower monetary value, however, it has significant functionalities that need to be secured. Table 2-4 lists the common activities which could also be the security triggers and issues in the application of e-banking, e-commerce, e-government and e-learning.

Table 2-4 E-Services Activities Threaten by Security Threats

E-service	Common activities that are exposed to security threats

E-Banking (Anjo, 2009)	• Transactional
	  ○ Electronic bill presentment and payment - EBPP
	  ○ Funds transfer
	  ○ Investment purchase or sale
	  ○ Loan applications and transactions, such as repayments
	• Non-transactional (e.g., online statements, check links, browsing, chat)
	  ○ Bank statements
	• Financial Institution Administration
	• ASP/Hosting Administration

E-Commerce (Merchant Glossary, 2009)	• E-mail and messaging • Content Management Systems • Documents, spread sheets, database • Accounting and finance systems • Orders and shipment information • Enterprise and client information reporting • Domestic and international payment systems • Newsgroup • On-line Shopping • Messaging • Conferencing
E-Government (Palvia and Sharma, 2007)	• Pushing information over the Internet, e.g.: regulatory services, general holidays, public hearing schedules, issue briefs, notifications, etc. • Two-way communications between the agency and the citizen, a

	business, or another government agency. Users can engage in dialogue with agencies and post problems, comments, or requests to the agency. • Conducting transactions, e.g.: lodging tax returns, applying for services and grants. • Governance, e.g.: online polling, voting, and campaigning.
<u>E-learning</u> (Furnell and Karweni, 2001)	• Enrolment: ○ Register user & establishes authentication parameters ○ Payment of registration fees, ○ Verification of previous qualifications • Study: ○ Access control on module content ○ Secure submission of work ○ Confidentiality and non-repudiation of communications ○ Service monitoring ○ Learning resource provider provision of a trusted repository • Completion: ○ Issue of electronic certificate • Termination: ○ Revocation of access • Suspension: ○ Restrict of access ○ Continued protection of registered details.

2.2.8 Summary of Information Security

Information security includes protection of any threats to avoid the fabrication, modification, interruption and interception of information. Information security threats are mainly caused by persons who intentionally or unintentionally interfere with the normal business process. A variety of controls are in the market to ensure the continuity of business and minimise the loss. ISM provides

standards - ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002 as guidance to manage information security. The standards set outline the policy, training and education to improve the security culture among users. However this standard is designed and implemented in such a way that it is an obligation by the users without considering their differences in behaviour and perception. The behaviour and perception towards security could vary according to the job task, the mission and vision of the organisation. For instance, the different business activities between e-services could lead to differences in organisational behaviour and perception towards security.

The next section provides an overview of e-learning followed by the review on security in e-learning.

2.3 E-Learning

E-learning is one of the e-services from the networked technology evolution. In recent years, there has been an increasing amount of literature on e-learning. The following subsections explain the concepts of e-learning including definition, e-learning type, history of e-learning development, benefit, growth, and the stakeholders of e-learning and finally e-learning current challenges.

2.3.1 Definition

The definition of e-learning has been made in different ways: some focus on the content, some on communication and others on the technology (Mason and Rennie, 2006). One of the early definitions for e-learning was by the American Society for Training and Development (ASTD), which claimed that e-learning covers a wide set of applications and processes, such as web-based learning, computer-based learning, virtual classrooms and digital collaboration. ASTD

even includes the delivery of content via audio and videotape; satellite broadcast, interactive TV and CD ROM[1].

E-learning is the implementation of technology to support the learning process (Johnson et al., 2008), and information or knowledge can be accessed by using communication technology (Wong, 2006). The learning process can be continuously provided when the content is available on the net. Eklund (2003) defines e-learning as a component of flexible learning which is a wide set of applications and processes that use all available electronic media to deliver the education and training. This includes computer-based learning, web-based learning, virtual classrooms and digital collaboration.

However for the focus of definitions, e-learning is understood as the use of the ICT to enhance the teaching and learning experience which includes the web and other internet technologies.

2.3.2 E-learning Type

E-learning has previously been used as synonyms to abbreviations like CBT (*Computer-Based Training*), IBT (*Internet-Based Training*) or WBT (*Web-Based Training*). In addition, there are some common terms that are used interchangeably to reflect the usage of technology in education such as distributed education, e-learning, distance education, blended learning and online classes (Mason and Rennie, 2006).

Distributed and distance education represents more on the self-learning; the learning materials are posted through physical mail or can be accessed online. The meeting sessions are conducted several times per semester. Whilst, a combination of face-to-face and online learning sessions is called blended learning (Fook et al., 2005), it is viewed as a method of educating at a distance, that uses technology combined with traditional education or training. Mason and Rennie (2006) positioned e-learning as a type of distance education. Figure 2-6

[1] http://www.learningcircuits.org/glossary.html

illustrates distributed education is a broader term which includes aspects of distance and online education, as well as blending with face-to-face learning.

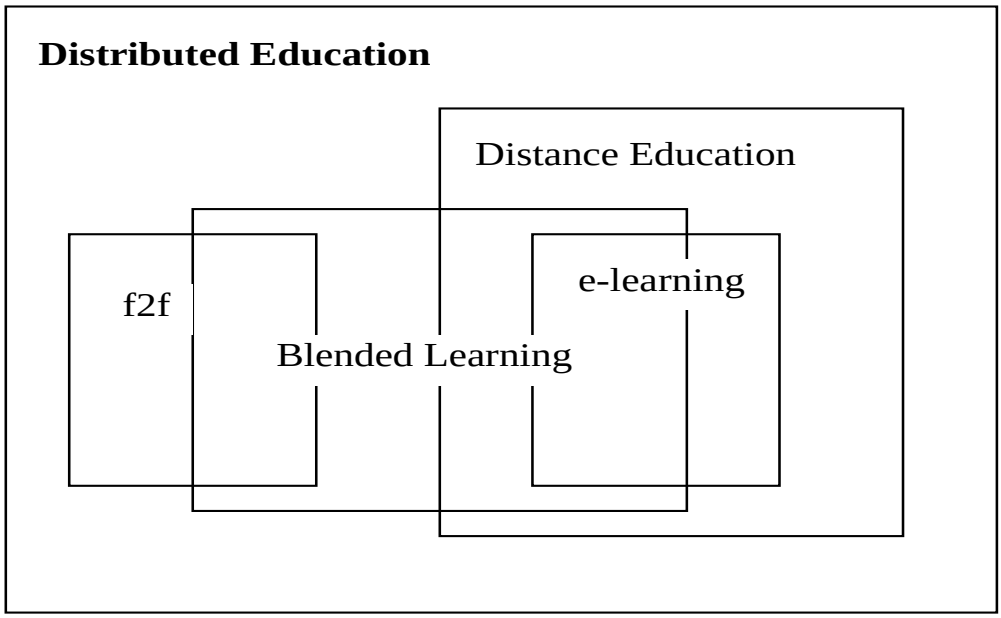


Figure 2-6: The Relationship of E-learning to Distribution Learning

Source: Mason & Rennie, (2006)

Morrison (2003) listed strategic use of learning delivery channels such as physical classroom, virtual classroom, print, email, message board, the telephone, coaching and mentoring systems, software simulations, online collaboration, self-paced e-learning and knowledge management channels and increasingly, mobile and wireless channels. These learning delivery channels covered almost all the methods used in e-learning.

Currently, the implementation of e-learning is executed using any of these three methods:

1. using technology asynchronously only as tools to support or supplement a traditional (face-to-face) learning,

2. using technology asynchronously and synchronously as tools to support or supplement a traditional (face-to-face) learning,

3. using technology asynchronously and synchronously to deliver a learning course (completely online).

2.3.3 History of E-learning

Pre 1983 - Era of Instructor-led Training	This was the dominant teaching tool before computers became widely available and interactions between the instructor and students took place in the classrooms.
1984-1993 – Multimedia	Windows 3.1, Macintosh and CD ROMs were the main technology developments in this period. However, classroom interactions and dynamic presentations were lacking in this medium.
1994-2000 – Web Infancy	As the web evolved, the arrival of e-mail, media players and streamed audio/ video began to change the face of multimedia mediums. Students can access the lecture notes or materials from the web anytime, anyplace.
***2001 and beyond – Next Generation* Web**	Advanced website designs, rich streaming media (real audio/video) and high bandwidth (faster data flow) will revolutionise the way in which education will be delivered. Instructor led, interactive mode can now happen via the web, reaching far more students than before.

Figure 2-7 The Maturity of E-learning

Source: (Dietinger, 2003)

In conjunction with the dissemination of the computer for personal use in 1980s, the use of technology to support the learning process is said to have started at a similar time. Conole et al., (2007) claimed higher learning institutions have changed dramatically in the last thirty years through policy drivers, such as widening participation, long-life learning and ensuring quality assurance.

Dietinger (2003) exhibits the maturity of e-learning through 1983 until today as shown in Figure 2-7. The emphasis on e-learning in the past has been on the ‘e’ which means electronic or the technology, even though there is an urge to shift to the learning (content) in ensuring the success of e-learning (Hamid, 2002).

2.3.4 Benefit of E-learning

E-learning has provided numerous benefits to its user. The obvious benefits are that e-learning offers everyone the chance to be a learner. The concept of anytime, anywhere learning has promoted lifelong learning and makes distance a problem of the past for students.

The flexibility that e-learning offers to the students is the main motivating factor in choosing online courses (Jain and Ngoh, 2003). According to Khan (2004), e-learning provides opportunities to create well-designed, learner-centered, engaging, interactive, affordable, efficient, easily accessible, flexible, distributed and facilitated e-learning environments.

Students can save money and time spent on travelling and obtaining materials for their study (Khan, 2004). Printing costs can be reduced by reading the available learning material online. E-learning also allows students wider access to limited resources such as e-journals and e-books (Concannon et al., 2005), (Khan, 2004). This can provide further support to the students to enhance their learning. The improved communication link and better students’ access encourages them to participate more (Concannon et al., 2005), (Khan, 2004). They can have a public forum among the peers or even a private forum with the lecturer or instructor. Another benefit offered by e-learning is faster delivery of assessment (Chin, 2004). The lecturers can provide feedback faster, compared with the traditional method and the peer students can also contribute to the feedback among themselves.

The benefits of e-learning are obvious to the students. However, other users of e-learning also gain benefits on the efficiency and effectiveness in managing and performing their roles.

2.3.5 E-learning Growth

Recent studies have indicated that e-learning has been growing and is widely used. Developments in Internet and multimedia technologies are the basic enabler of e-learning, with consulting, content, technologies, services and support being identified as the five key sectors of the e-learning industry (Nagy, 2005).

Regardless of the claim that many e-learning initiatives had fallen short of expectation, the market of e-learning is growing (Hamid, 2002). According to the Sloan Foundation reports (Allen and Seaman, 2003; Allen et al., 2005) there has been an increase of around 12–14 percent per year on average in enrolments for fully online learning over the five years 2004–2009 in the US post-secondary system, compared with an average of approximately 2 percent increase per year in enrolments overall. Allen and Seamen (2010) claimed that almost a quarter of all students in post-secondary education in US were taking fully online courses in 2008, and a report by Ambient Insight Research (2009) suggests that in 2009, 44 per cent of post-secondary students in the USA were taking some or all of their courses online, and projected that this figure would rise to 81 percent by 2014. This can be the indicator that implementation of e-learning also has been spread all over the world.

This growth is fuelled by new institutions entering the online arena combined with a continuous student demand for online learning options (Mason and Rennie, 2006). The necessity of knowledgeable workers has also contributed to the growth of e-learning. Every employee needs to equip themselves with as much knowledge and skill as possible and the easiest way to do this is to enrol as an e-learning student.

The functionality of e-learning has also grown in parallel with the need and the development of technology. Figure 2-8 shows the growth in e-learning

functionality.

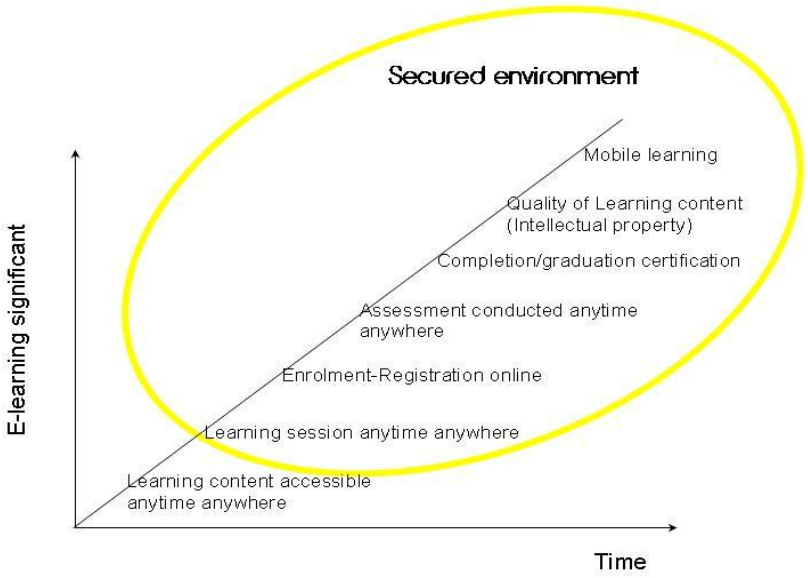


Figure 2-8 Growth in E-Learning Functionality

Initially e-learning deposited the learning content on the Internet to be accessed by the user at anytime and anywhere (asynchronous learning) (Rosenberg, 2001). Then it broadened to allow the learning session to be conducted at anytime and anywhere based (synchronous learning) among the users (instructor/ lecturer and students) (Mason and Rennie, 2006). E-learning now enables the registration, assessment, and posting graduation certification online. With the intention of adding more flexibility, mobile learning (Corbeil and Valdes-Corbeil, 2007) has been introduced even though currently not used to its full potential. As the functionality of e-learning keeps on growing, the e-learning environment needs to be secured. Providing more functionality to the users makes the e-learning environment more open and exposed to the information security threats.

2.3.6 E-learning Stakeholders

E-learning consists of a community of people to make it work and to benefit from it. With everyone playing their role and moving towards the same vision and mission of the organisation, e-learning implementation can be a successful. This successful of implementation benefited the employer and client. In an organisational context, a stakeholder is a constituent of an organisation (Thompson and Strickland, 2001). In the same sense, the stakeholders of e-learning are those that are affected by it. Wagner (2008) has compiled the main stakeholder groups in the context of higher education. They are students, instructors, educational institutions, content providers, technology providers, accreditation bodies and employers.

Students have been the main reason for which e-learning was invented. The student's role is to participate in the learning process (collaborative exercises to enhance learning). Instructors play a critical role in e-learning; they must therefore be equipped with an appropriate set of skills and attributes in addition to subject matter expertise (McPherson and Nunes, 2004). Educational institutions in the context of higher education include colleges and universities while content providers could be instructors or external sources such as commercial educational content creators. Meanwhile technology providers develop the technology that enables e-learning delivery. This category consists of a broad range of services, from the facilitation of individual distance learning courses, to complete Learning Management Systems (LMS) provided by companies such as Blackboard. Similar to content providers, technology providers are motivated to provide learning environments that will result in effective learning for students. Accreditation bodies are organisations that assess the quality of education institutions' offerings. Those institutions meeting the minimum requirements will be accredited, providing them with a level of credibility that non-accredited institutions will not possess. On the other hand employers, in this context, are those organisations that will potentially hire graduates of higher education institutions.

Khan (2004) in his model, suggested people contribute in two main processes in e-learning: content development and content delivery. The process content development consists of a planning team, design team, production team, and evaluation team. While process content delivery includes a delivery team to manage the delivery and maintenance. There are other sub-teams such as an instructional team, learning support services, and administrative services that deal with e-learning end-users such as lecturers and students.

In a way, the e-learning community can be classified as two groups: The Supply group and Demand group. The Supply group is the learning provider that offers the e-learning environment. This group consists of top management, IT department staff, e-learning service centre and other staff that support the e-learning development and delivery process. The demand group consists of end-users that will benefit the most from this environment. They are lecturers and students.

2.3.7 E-learning Challenges

Despite the benefits offered by e-learning, there are challenges that hinder e-learning implementation. These challenges can be viewed from the e-learning providers and users perspectives.

E-Learning providers such as Higher Learning Institutions (HLI) are having difficulties in technological issues including preparing an efficient infrastructure. Bandwidth and connectivity are necessary, since students will be depending on these to access the learning material on the web. The delivery of high bandwidth content, such as digital video is still problematic to the home user (Catherall, 2005). Learning material is also an issue given the lack of quality content prepared. Developing good content for students should take into consideration many things such as pedagogical aspect, human computer interface and expertise. Ensuring all of these are well prepared requires a high investment and results in a high cost of implementation (Folorunso et al., 2006). In a developing country, all these challenges are even more difficult because of limited resources.

From the users' perspective, the challenges could be explained in the context of readiness. A. Aziz et.al (2006) identified, critical factors in preparing people readiness are commitment and skills. Readiness includes readiness of knowledge plus readiness of motivation for self-learning. Students could be unready for e-learning because of low computer literacy and low self-discipline (Wong, 2006) for the self-learning method. According to the Technology Acceptance Model (TAM) (Davis, 1989; Davis et al., 1989), the perceived usefulness and perceived ease of use have an impact on the users' acceptance of the technology. If they don't see how the e-learning can help them, the student may cease to continue or even fail to enrol because they think they would fail because of lack of support and training provided by the learning provider. Instructors would also feel the same and may not use e-learning because they see little reward or recognition, and yet there are a great many things which would ensure the success of e-learning (Rossman and Rossman, 2008).

2.3.8 Summary of E-learning

E-learning is similar with other e-services as it depends on the communication technology and internet technology. However each e-service is different from another, due to different objectives of implementation and the applications used in their environment.

E-learning offers many benefits and has been widely adopted all over the world. Many studies have been carried out with the aim of ensuring the successful implementation of e-learning. Such studies include not only the technical aspect, such as the infrastructure and technological devices, but also the aspect concerned with ensuring a successful learning process. As the functionality of e-learning keeps growing, more challenges need to be addressed. The providers and the users need to be supported and guided. Since more functionality is presented to users, the e-learning environment becomes more open and exposed to the information security threats. At the moment security

has not been defined as one the challenges in e-learning though the interaction between the organisations, technical and socio-cultural areas has positioned the security issues in e-learning as one of the hidden challenges that need to be addressed. The following section will present more about security in e-learning.

2.4 Security in E-Learning

E-learning is an example of e-services where information and the appropriate presentation of information, known as learning material/ content, are provided and require adequate protection. One of the most pressing issues is the effective protection of digital content as the value of many digital goods lies not in the content itself but in the presentation (Weippl, 2005a). Furthermore students need to submit assignments to a course website from where the lecturer retrieve and mark the assignment. Students also access the course websites to get the results. This process suffers from security threats and risks such as the alteration of course material by unauthorised people or submitted assignment can be changed or deleted by unauthorised parties. Denial of service attempts against course websites could prevent authorised students from accessing the website (Kritzinger and von Solms, 2006). Users ID and password can be intercepted and misused. If the e-learning environment is at risk, it could be difficult to verify if the assignment is completed and sent by a valid student.

Previous studies have shown that there is a barrier to the wide-spread adoption of online education (Allen and Seaman, 2007). It is claimed that the reason behind this barrier is not only the high cost or further preparation has still to be done but also the security aspect which is something that is completely intangible in the cyber world (Zhang and Nunamaker, 2003). It has been said that e-learning institutions try to address privacy and security, however the standards are implanted superficially (El-Khatib et al., 2003).

In the e-learning environment, the e-learning provider is required to prepare an efficient and effective e-learning environment by setting a proper goal and

actionable plan. The e-learning provider should also be aware of and entertain the requirements of other groups of users in e-learning. The delivery and maintenance team is responsible for on-going updating and monitoring, including security measures for access control and information confidentiality. No institutions are immune from hackers and any networks can be the target for hackers if security is weak (Khan, 2004). From a students' point of view, they would feel more confident in interacting and collaborating with others when there are mechanisms in place to establish privacy and trust (Raitman et al., 2005). The students will look for the institution that can provide the secure and guaranteed environment before enrolling onto the e-learning course.

2.4.1 Research in Security of E-Learning

Despite the importance of security in e-learning, not much effort has been made. Most emphasis has been placed on enhancing the content and technology as both has been recognised as the challenges to having successful e-learning (Cantoni et al., 2004). Security in e-learning has been ignored (El-Khatib et al., 2003) and neglected (Raitman et al., 2005).

Researches in e-learning security have focussed mainly on three main areas : policy (Yang et al., 2002), (El-Khatib et al., 2003), (Boella and van der Torre, 2006); identity of users which refer to access management (Raitman et al., 2005), (Yong, 2007), (Lim and Jin, 2006), (Jalal and Zeb, 2008), (Saxena, 2004), (Bruns et al., 2003), (El-Khatib et al., 2003), and intellectual property (Graf, 2002), (Kennedy, 2002), (Samuels, 2004). Security issues in e-learning have been addressed generally through security technology, for example, a technical framework on authentication and accountability, access control, protecting communications, non-repudiation issues and learning resource provider server protection (Furnell and Karweni, 2001).

Most researchers state that the way to avoid an attack on e-learning is by controlling the access. One of the ways is the authentication and authorisation process. Jalal and Zeb (2008) recommended an authentication process to identify a legal user. This will overcome the illegal use of an application.

Applying too much security will result in the system being difficult to use by the user. In order to balance access and security, (Saxena, 2004) discussed the merit of providing users with single sign on authentication and authorisation services to all authorised web applications and web resources. Graf (2002) suggested an approach to protect intellectual property by extending the control of the copyright holder to the entire lifetime of digital data. He suggested a method called CIPRESS which controls the access to the material. Yong (2007) had discussed another technical aspect on how to secure e-learning by digital identity design and privacy preservation.

2.4.2 Information Security Management in E-Learning

Literature on ISM in e-learning found are mostly conceptual discussions. Yang et.al (2002) suggested that it is obligatory to have effective mechanisms for security and privacy control and management. At present, information security technology, hardware and software have been used to secure the e-learning environment. Kritzinger & Von Solm (2006) suggested four main elements of information security within e-learning: ensuring e-learning information security governance, creating e-learning information security policy and procedures, implementation of e-learning information security countermeasures, and monitoring the e-learning information security countermeasures. The elements suggested include the management aspect to ensure that the security implementation achieved its objective.

Nosworthy (2000) assembled the following factors that should be considered during ISM implementation: people, culture (organisational culture), people's attitude (perceptions and views towards security), security education and training, ownership, and job description. This has been supported by empirical studies by Kankanhalli et al., (2003). He developed an integrative model of information security effectiveness which has defined these factors: organisational size, top management support and industry type. Abu-Zineh (2006) has claimed that the successful factors of ISM include top management support, IS policy, job responsibilities, motivation to employees, awareness and training programs, compliance with the information security international

standard, and using the services of information security external advisors. Though it is obvious that people and culture have been successful factors, no research has been found which discusses both dimensions in an e-learning security context.

2.4.3 Summary of Security in E-Learning

The success factors for e-learning implementation include technological support, institutional culture, staff development and students' receptivity and learning behaviours (Liu et al., 2010).

Warren (2003) claimed *'it should be noted that the security requirements of e-learning seldom appear in the literature in relation to e-learning. But security is an important aspect of all IT systems.'* Information security management in e-learning can be similar to other e-services. However the emphasis on the services is different. E-learning offers flexibility to the user as a learner and at the same time ensures the availability, integrity and confidentiality of information. The discussion on security in e-learning in literature has placed the responsibility to secure e-learning on the top management and the IT personnel whereas the security should be the responsibilities of everyone in an organisation. It is known that the success of information security management in e-learning relies on technological software and hardware control, however the fact that people are the main key to the realisation of the control can't be denied.

2.5 Socio- Technical System Approach

The review on the socio-technical system has been added after the research obtained an insight into the behaviour of the people. In ISM, people are required to follow policy, procedures and other guidelines. However people themselves are potential vulnerabilities through password sharing, by generating non repudiation issues or even inviting malware infection with their behaviour. Since

people are complex and have varieties of behaviour and perception towards the security system, the socio technical approach is studied.

The term socio-technical system (STS) was coined in the 1960s by Eric Trist, Ken Bamforth and Fred Emery, who were working as consultants at the Tavistock Institute in London. Emery and Trist claimed during that time, STS was directed more at the design of work systems in factories and offices, and initially focused on a traditional non-computing manufacturing system (Scacchi, 2004). It is also known that STS originated from General System Theory by Ludwig von Bertalanffy in 1949; which was later expanded and indicated that technology, people and process as the elements of general information system (Schneier, 2000).

With such origin, the STS approach is built on the assumption that information system development involves the design of a work organisation (Lyytinen, 1987). In 1994, Kowalski developed a model that illustrated these three elements as the technical and social components in a system. See Figure 2-9. The technical subsystem has tasks and technology as components while the social subsystem has culture and structure as the components. Task and technology refers to the hardware, software, procedures, data and data structures. While culture and structures represents physical surroundings, people, laws and regulations.

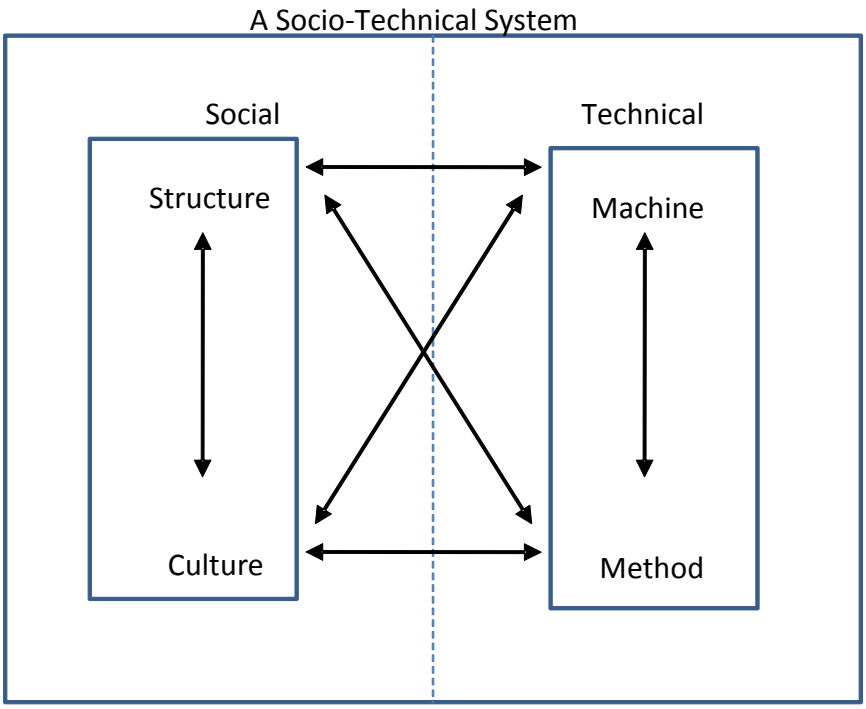


Figure 2-9 Socio Technical System Model

Source: Kowalski, (1994)

Gradually STS is widely used relating to theory regarding the social aspects of people and society, and the technical aspects of organisational structure and processes (Walker et al., 2008) in creating organisational performance. This includes the goal directed behaviour, even in a computing environment. It provides a richer descriptive and conceptual language for describing, analysing and designing organisations by including people, technology and process. STS emphasises joint optimization which means a shared emphasis on achievement of both excellence in technical performance and quality in people's work lives (Walker et al., 2008; Rousseau, 1977).

The literature discussed earlier in this chapter has recognised that it is necessary to include people to ensure the security of information in e-learning. E-learning and information security are considered to be technical areas, in

which both exist because of the evolution and development of ICT generally and information system specifically. The issues of information security in an e-learning environment are closely related to the social needs; which are to satisfy people such as the stakeholders. E-learning security issues are similar to those of the information system that were described as a 'technical system with social implications' (Goldkuhl and Lyytinen, 1982). It is a system that includes technical systems but also operational processes and people who use and interact with the technical systems. Thus, there is a need for more involvement of users and user management in the planning and on-going management of information security (James, 1996).

Despite the technological solutions that have been developed and used for the majority of security issues, there are still many challenges such as human computer interface, password control-passwords sharing, and non-repudiation issues. The organisational feature of information security can be viewed as technical, social and socio-technical (Iivari and Hirschheim, 1996). The technical view emphasises the fact that information security development relies primarily on technical aspects. The social view emphasises the development of organisational systems above technical issues, and the socio-technical view, which is a joint optimisation between both technical and social, as equally important. As the technical solution has not been successful, Dhillon and Backhouse (2001) proposed the socio-organisational aspects of information security, asserting the need to understand the complex interplay between technological structures and behavioural patterns to ensure proper security. However emphasis on the socio-organisational aspect itself is not enough. Eloff and Eloff (2003) argue that Information Security Management System (ISMS) consists of many aspects as policies, standard, guidelines, codes of practices, technology, human issues, legal and ethical issues. He claimed that it is necessary to identify those human elements that affect the effectiveness of the whole system in order to design strategies that can minimise their weaknesses.

Similarly, in an e-learning environment, the people and process context has recently been a debatable topic. Thus, the people factor represents a key issue

that has to be addressed by managers for effective ISM to take place in e-learning environments. Konrad et.al (1999) claimed that building trust in e-commerce is not only a technical system but rather a socio-technical system. This is similar situation to e-learning as it shares the same criteria as e-service, due to the involvement of users (stakeholders), business practices/ objectives and related institutions. It is important also to note that from the socio-technical system approach, e-learning has different context from other e-services.

There were many examples of the introduction of technology being associated with implementation problems, often linked to resistance by the work force and a failure to achieve the expected benefits (Jackson, 2010). Casmir (2005) proved that an information system failed not only because of problems with technology used but also a lack of security awareness of the end users. End users or people have different perceptions and behaviour towards security. This perception and behaviour reflects the culture that each individual holds. Organisational culture contributes in a social context in defining the security risk (Whitman and Mattord, 2011; Karyda et al., 2004; Tsohou et al., 2006; Oltedal et al., 2004).

2.6 Organisational Culture

Organisational culture comprises the attitudes, experiences, beliefs and values of an organisation. Hill and Jones (2007) defined organisational culture as the specific collection of values and norms that are shared by people and groups in an organisation, that control the way they interact among themselves and with people outside the organisation. It is an assumption of the mind that guides interpretation and action in organisations towards something by defining appropriate behaviour for various situations. Relevant literature that may explain security risk through organisational culture is explored.

In organisational culture, many classifications schemes have been made and include those by Kennedy and Deal (1982), Handy (1993), Schein (2010), Hofstede (1983).

Kennedy and Deal (1982) define organisational culture as the way things are done in the organisation. They measured the organisation based on feedback and risk. There are four classifications of organisational culture based on feedback and risk:

- The Tough-Guy Macho Culture. Feedback is quick and the rewards are high.
- The Work Hard/Play Hard Culture is characterized by few risks being taken, all with rapid feedback.
- The Bet your Company Culture, where big stakes decisions are taken, but it may be years before the results are known.
- The Process Culture occurs in organisations where there is little or no feedback.

Handy (1993) popularised the 1972 work of Roger Harrison of looking at culture which some scholars have used to link organisational structure to organisational culture. He describes Harrison's four types as power culture, role culture, task culture and person culture. Below is the description by Handy,

> *'A Power Culture which concentrates power among a few… Power and influence spread out from a central figure or group. Power desired from the top person and personal relationships with that individual matters more than any formal title of position. Power Cultures have few rules and little bureaucracy; swift decisions can thus ensue.'*
>
> *'In a Role Culture, people have clearly delegated authorities within a highly defined structure. Typically, these organisations form hierarchical bureaucracies. Power derives from a person's position and little scope exists for expert power. Controlled by procedures, role descriptions and authority definitions, predictable and consistent systems and procedures are highly valued.'*
>
> *'By contrast, in a Task Culture, teams are formed to solve particular problems. Power derives from expertise as long as a team requires*

expertise. These cultures often feature the multiple reporting lines of a matrix structure. It is a small team approach, who are highly skilled and specialists in their own markets of experience.'

'A Person Culture exists where all individuals believe themselves superior to the organisation. Survival can become difficult for such organisations, since the concept of an organisation suggests that a group of like-minded individuals pursue the organisational goals. Some professional partnerships can operate as person cultures, because each partner brings a particular expertise and clientele to the firm.'

Schein (2010) developed a model depicting a culture which exists on three levels: artefact, values and underlying assumptions. Artefacts deal with organisational attributes that can be observed, felt and heard as an individual enters a new culture. Values are the level that deals with the espoused goals, ideals, norms, standards, and moral principles and is usually the level that is measured through survey questionnaires. While underlying assumptions is the level that deals with phenomena that remain unexplained when insiders are asked about the values of the organisational culture. Information is gathered at this level by observing behaviour carefully to gather underlying assumptions because they are sometimes taken for granted and not recognised. According to Schein, the essence of organisational culture lies at this level.

Hofstede (1983) demonstrated that there are national and regional cultural groupings that affect the behaviour of organisations. Hofstede (2010) identified five dimensions in his national culture model: power distance, uncertainty avoidance, individualism, masculinity and time orientation. The brief description as below:

- Power Distance is the extent to which the less powerful members of organisations and institutions accept and expect that power is distributed unequally.
- Individualism on the one side, versus its opposite collectivism, that is the degree to which individuals are integrated into groups.

- Masculinity versus its opposite femininity, refers to the distribution of roles between the genders which is another fundamental issue for any society to which a range of solutions are found.
- Uncertainty Avoidance deals with a society's tolerance for uncertainty and ambiguity; it ultimately refers to man's search for truth. It indicates to what extent a culture programmes its members to feel either uncomfortable or comfortable in unstructured situations.
- Term Orientation is the degree to which a culture focuses on long-term or short-term orientation planning.

In some studies the security culture was observed as part of national culture (Chaula et al., 2006) whilst in others there was a specific focus on the culture of the organisation (Chang and Ho, 2006), (Chang and Lin, 2007), (Ruighaver et al., 2007).The above mentioned classification schemes focused more on the behaviour at organisational and group levels.

2.6.1 Organisational Behaviour

Tyson and Jackson (1992) define the study of organisational behaviour (OB) as a process to analyse and interpret people's behaviour in work organisations. Some of the basic theories in OB such as: security motivation theories, goal setting theory, reinforcement theory and law of effect theory have offered mechanisms to influence the human behaviour.

OB can be perceived (analysis) in three levels (Robbins and Judge, 2008): Individual level, Group/ Interpersonal level and Organisation level. Vroom and Von Solms (2004) argue that including security practices in the organisational culture proactively and spontaneously for day-to-day operations has a positive impact on the success of the organisation. However, since culture is rooted from the individual, security can be argued to be affected more by the individual cultural view. One known theory is the Grid and Group Cultural Theory or simply as Cultural Theory.

2.6.2 Grid and Group Cultural Theory

Grid and Group cultural theory (Cultural Theory) was developed over the past thirty years through the work of British anthropologists Mary Douglas and Michael Thompson. This theory addresses the level of an individual in an organisation. It attempts to explain the changes both within and between dimensions and deals with dynamism (Thompson et al., 1990). Cultural Theory has been used to study the different views of environmental and technological risks in society (Karyda et al., 2004; Tsohou et al., 2006; Karyda et al., 2005).

The Cultural Theory framework has two dimensions, namely the Grid and the Group. The Grid dimension refers to the degree to which a social context is regulated and restrictive in regard to the individuals' behaviour, while the Group dimension refers to an individual as a member of bonded social units, specifically on '*how absorbing the group's activities are on the individual'* (Oltedal et al., 2004). The two dimensions give four different cultural views with distinct ways of life or world views (Mamadouh, 1999). Figure 2-10 depicts the relationship of Grid and Group with the four ways of life:

Cultural view	Grid	Group
Fatalism	Strong/High	Weak/Low
Hierarchism	Strong/High	Strong/High
Individualism	Weak/Low	Weak/Low
Egalitarianism	Weak/Low	Strong/High

Figure 2-10 Grid and Group Cultural View

Fatalism is a view held by individuals which have a weak bond with other people (Thompson et al., 1990). They are strong in Grid, which may have many and varied interpersonal differences. They are left to their own fates, which may be positive or negative for them. Values related to fatalism are apathy and isolation.

Hierarchism is a view held by people with control and a strong Grid and Group, which reflect the control and power values. They are strongly connected, yet are very different. This leads to the development of institutions, hierarchies and laws that both regulate individual actions and provide for weaker social members (Mamadouh, 1999).

In the Individualism view, people are relatively similar, yet have little obligation to one another. People enjoy their differences more than their similarities and seek to avoid central authority. They are weak in both Grid and Group dimensions. Values related to individualism are independence and self-reliance (Thompson et al., 1990).

Egalitarian is a view held by individuals who show teamwork and cooperation. They have strong Group bonds between other people (Thompson et al., 1990). They have a weak Grid which shows significant similarity between people. Thus the rule is less about law and more about values. External laws may be seen as necessary only when there is weakness of character, which is prized highly (Oltedal et al., 2004).

Table 2-5 summarised from Tsohou et al. (2006) the characteristics of each cultural view towards security.

Security culture represents the prevailing attitude towards approaches to a secure organisational environment. Raman and Wei, in 1992 in Alfawaz et al., (2010) concluded that culture had a significant impact on how technology meeting systems were perceived, used and adapted.

Table 2-5 List of Characteristics for Each Cultural View

Fatalism view/characters	**Authors**
Believe their autonomy is restricted by social distinctions, however they feel excluded from membership in the institutions responsible for setting the rules. Tend to see themselves as "outsiders".	(Douglas and Wildavsky, 1983), (Langford et al., 2000), (Thompson et al., 1990)
Believe that there is minimal individual autonomy and little room for personal negotiations.	(Altman and Baruch, 1998)
Believe that social classification should be based on ancestry.	(Altman and Baruch, 1998)
Take little part in social.	(Tsohou et al., 2006)
Would rather be unaware of dangers, since they assume that they are unavoidable anyway.	(Oltedal et al., 2004)
Prefer occupying posts with routine tasks.	(Mars, 1996)
Feel that decisions are beyond their control and feel obliged to accept whatever is imposed upon them.	(Langford et al., 2000)
Tendency towards fatalism therefore are not expected to breach security controls for their personal gain, since they believe they have little or no power to influence the course of events in their favour.	(Tsohou et al., 2006)
Hierarchism view/characters	**Authors**
Status demarcation unquestionable.	(Douglas and Wildavsky, 1983), (Langford et al., 2000), (Thompson et al., 1990)
Trust rules and regulation and the experts.	(Lima and Castro, 2005)
Realise and act according to the roles.	(Altman and Baruch, 1998)
Act as a group in an orderly, disciplined and co-ordinated way, with respect for their own rules, limits and precedents even when cheating or making mistakes.	(Mars, 1996)

Low adaptability to change. Dependence on routine ways of work.	(Mars, 1996)
Trust the experts.	(Lima and Castro, 2005), (Oltedal et al., 2004)
Fear of disruption to the social order. Emphasises on establishing and preserving the nature and social order.	(Langford et al., 2000), (Marris et al., 1996), (Oltedal et al., 2004)
Individualism view/characters	**Authors**
Bound neither by group integration nor by prescribed roles, and assert that all boundaries are subject to negotiation.	(Karyda et al., 2005),(Langford et al., 2000)
Barely feel responsible towards other members of society.	(Langford et al., 2000)
Believe that each person is responsible for oneself.	(Altman and Baruch, 1998)
Concerned for the maintenance of freedom to continue life and business as usual.	(Lima and Castro, 2005)
Afraid of things that might obstruct their individual freedom.	(Oltedal et al., 2004)
Reluctant to accept rules or to follow defined instructions or procedures.	(Mars, 1996)
Mostly build short-term relationships with their superiors.	(Mars, 1996)
Associated with corner cutting, rule breaking and cheating.	(Tsohou et al., 2006)
High propensity for risk taking.	(Mars, 1996)
Prefer methods that are based on economic factors, and in particular cost-benefit analysis.	(Langford et al., 2000), (Marris et al., 1996)
Egalitarianism view/characters	**Authors**
High degree of the group dimension and not prescribed by role differentiation.	(Tsohou et al., 2006)
Negotiation in relationship and nobody is granted	(Marris et al., 1996),(Langford et al.,

authority by virtue of his or her position.	2000)
Believe that leadership must be charismatic.	(Altman and Baruch, 1998)
Intense sense of equality.	(Tsohou et al., 2006)
Sceptical to expert knowledge, suspects the expert and strong institution, misuse the power/authority.	((Oltedal et al., 2004)
Dislikes others deciding for their life and actions, and prefers to have information provided to them, based upon which they can make their own personal choices.	(Finucane and Holup, 2005)
Support decision-making processes that encourage public participation.	(Marris et al., 1996)
Difficulty in accepting role differentiations.	(Langford et al., 2000) (Marris et al., 1996)
Prone to break rules if they feel that these rules generate inequalities or if they are not convinced of their purpose.	(Tsohou et al., 2006)

2.6.3 Summary of Social Technical Approach and Organisational Culture

Both information security and e-learning are the consequence of the introduction of an information technology (IT) system to the world. A social technical system has the elements of technical system: technology and process (task), and the elements of social system: people and structure. People hold culture which generally is based on a set of shared underlying assumptions about reality (Robbins and Judge, 2008). Culture has effects on attitudes and belief, which in turn play apart in individual behaviours—actions and/or reactions. Thus, there is a prime need to identify attitude and belief of each stakeholder towards security so that a security aware culture can be cultivated in an organisation and further will lead to guide on how desirable attitudes and beliefs can be imprinted into formal operational methods to produce the desired outcomes—secure systems, networks, and operations. The

above sections have discussed the organisational culture, defining people in the social context especially in information security matters. Many classification schemes in organisational culture have focused on the organisational and group level and upwards to national level. Cultural Theory is one that highlights the individual view in the social technical system.

2.7 Chapter Summary

A literature review was conducted in this chapter to understand the gap in the research area. This chapter has explained the process in selecting and reviewing literature. The literature has covered security knowledge such as threats and vulnerabilities and the effective countermeasures. It is noted from the literature on information security that people's behaviour is not typically specifically addressed in the security control mechanisms, though they are one of the components of IT systems and a source of information security threats. ISM standard has been deployed from top to bottom and a security policy is blanketed for all users. A policy that is specifically designed for targeted people may improve its likelihood of compliance.

The review has established that e-learning shares similarities of other e-services.

E-learning is different from other e-services in the applications used, the procedures and the stakeholder behaviour shaped the environment in e-learning. Issues of reliability of the system in course material, data privacy in the grading result, non-repudiation and misuse of e-learning LMS are example of social technical security issue which is specifically related to people.

People need to follow policy, procedures and others activities to ensure the CIA is achieved. People are expected to be the security controllers themselves. However people also can be the vulnerabilities where threat can occur, for instance: password sharing, non-repudiation, and malware infection. The current trend of social engineering manipulates people's level of security

awareness, for example phishing that allures users into giving information. This suggests that individual action can cause security threats. Literature on socio-technical system and organisation culture was studied to understand the response of people towards security. Studying people's minds (psychological), specifically the perception which is reflected by their behaviour may help in understanding people's response towards security.

Group psychology in the work context was reviewed, including organisational culture, national culture and organisational behaviour. Organisational behaviour offers theories to explain behaviour and attitude. Grid and Group cultural theory provides an approach to classify individual behaviour and perception towards security.

The literature has shown gaps that can be concluded as:

- people, as the main source of threats have not been particularly be addressed in the security standards and guidelines
- there is lack of discussion on information security management for e-learning; the process of securing an information system in e-learning requires the knowledge of the possible risks specific to the context of systems and available controls
- behaviour of people needs to be understood and predicted

The scope of this research is on these three main areas: information security, e-learning and Malaysia context. This chapter has reviewed two main areas of this research. Thus, in order to complete the literature review on the last area of this research, the following chapter will discuss research in the context of Malaysia. The next chapter will provide the Malaysia background and define the e-learning status and information security implementation in Malaysia.

3 MALAYSIA CONTEXT

Previously in Chapter 2, the literature review on information security, e-learning and the socio-technical system have been reported. This chapter compliments the literature review by reporting on the Malaysia context. The literature resources used, include, journal articles, conference papers, white papers, magazines, books, and articles from trusted websites (websites of relevant associations, societies, centres of excellence and government bodies). The duration for searching the studies published or articles for the literature review is set between 1990 and 2011. This chapter aims to describe the Malaysian context (section 3.1), a review of the e-learning status (section 3.2), information security implementation in Malaysia (section 3.3) and the Malaysia security e-learning characteristics (section 3.4).

3.1 Malaysia Background

3.1.1 Country

Malaysia is located in the middle of South East Asia and is made up of 13 states and three federal territories. The population of Malaysia, estimated to be 28 million, consists of many ethnic groups, with the majority races being Malays, Chinese, and Indians. Malaysia is a federal constitutional elective monarchy where the supreme ruler or king is the head of state and the prime minister is the head of the government.

After Malaysia gained its independence, the economy has grown. As a middle-income country, Malaysia has transformed itself since the 1970s from a producer of raw materials into an emerging multi-sector economy. In 2010, the gross domestic product (GDP) per capita purchasing power parity (PPP) was $414.400 billion, which resulted in Malaysia becoming the 3rd largest economy in ASEAN and the 30th largest economy in the world (CIA, 2011).

Currently, Malaysia is attempting to achieve high-income status by 2020 and to move further up the value-added production chain by attracting investment including those in high technology industries and services.

3.1.1.1 Malaysia and ICT

Malaysia is one of the developing countries. However the developing terminology doesn't imply that all developing countries are experiencing similar development. Each country is unique and has constraints such as political, economic and social (Alfawaz et al., 2010). Those constraints will impose different issues especially relevant to ICT transfer and implementation. Developing countries encounter social obstacles when attempting to transfer technology created abroad into practice at home (Yavas, 1992).

The introduction of personal computer technology in Malaysia in the early 1980s has offered facilities and opportunities to government departments in improving work efficiency and productivity (Mohamed and Appalanaidu, 1998). The culture among Malaysians themselves towards ICT acceptance and usage varies. A study by Ramayah and Jantan (2004) has concluded that perceived usefulness is the driver to any technology acceptance in Malaysia. Demographic characteristics such as age, gender, prior experience education, living place and status can be the antecedents to the perceived usefulness.

With differences in value, resource, skill, political, economic, and social and cultural situations, Malaysia is different from other developed countries. In the technology context, Ramayah and Jantan (2004) claimed that it is difficult to achieve technology maturity in Malaysia. It is argued that culture is having a significant impact on values, attitudes and behaviours.

3.1.2 Education in Malaysia

Education in Malaysia is governed by two ministries. The Ministry of Education (MOE) handles all matters pertaining to primary and secondary schools. While tertiary education, also known as higher education, is dealt with by the Ministry of Higher Education (MOHE). Tertiary education is a growing industry with most

of the Malaysian citizens furthering their study after completing secondary school. Malaysia is gaining acceptance as a reputable study destination for higher education in the region. The education sector offers a variety of higher educational programmes as well as professional and specialised skill courses that are competitively priced and of excellent quality.

Higher education in Malaysia has been triggered by the effects of globalisation and the growth of communication technologies. The economic and political situations in Malaysia have also shaped the progress of education recently. Education in Malaysia has progressed in line with the shift towards productivity and growth, based upon knowledge and innovation. For instance, the national gross expenditure on research and development (GERD) grew from RM1.1 billion to RM4.3 billion in 2005. Within the same period, the use of ICT grew from 1.2% to 21.8% (Ninth Malaysia Plan 2006-2010). There is increasing demand for knowledge-based input in practically all aspects of life (Chiam et al., 2011).

In order to respond to the demands of highly qualified and technically intelligent graduates, higher education has to take responsibility in catering for the growing population of students. Currently there are 61 private universities and 22 public universities. The citizens prefer to further their study in the public universities.

3.1.3 Public Universities

Public universities in Malaysia are categorised into three groups, research universities, focused universities (technical educational, management and defence) and comprehensive universities. Currently there are 20 public universities consisting of four research universities, four comprehensive universities and the other twelve are focused universities. Research universities have an emphasis towards research, focused universities concentrate on specific areas of focus related to its formation, while a comprehensive university offers a variety of courses and fields of study (Portal MOHE, 2010). Listed in Table 3-1 are the 20 public universities in Malaysia.

Table 3-1 Malaysia Public University

No.	Name
1	University of Malaya (UM)
2	Science University of Malaysia (USM)
3	National University of Malaysia (UKM)
4	Universiti Putra Malaysia (UPM)
5	Universiti Teknologi Malaysia (UTM)
6	International Islamic University Malaysia (IIUM)
7	Universiti Utara Malaysia (UUM)
8	Universiti Malaysia Sarawak (UNIMAS)
9	Universiti Malaysia Sabah (UMS)
10	Universiti Pendidikan Sultan Idris (UPSI)
11	Islamic Science University of Malaysia (USIM)
12	Universiti Teknologi MARA (UiTM)
13	University of Malaysia Terengganu (UMT)
14	Tun Hussein Onn University of Malaysia (UTHM)
15	University of Technical Malaysia Melaka (UTeM)
16	University of Malaysia Pahang (UMP)
17	University of Malaysia Perlis (UniMAP)
18	Universiti Sultan Zainal Abidin (UNISZA)
19	Universiti Malaysia Kelantan (UMK)
20	Universiti Pertahanan Nasional Malaysia (UPNM)

The listed public universities as shown are heavily subsidised by the Malaysian government and are governed as self-managed institutions by MOHE. In each public university, stakeholders are involved in managing conventional education. The stakeholders in Malaysia's public universities include the senior management, administrative groups (e.g. registrar, treasurer, academic, library) to manage and support the university operation, lecturers as the main contributor (key player) for the teaching and learning process and the students

that are the output of the university. Each stakeholder plays different roles and work together to achieve the university's objective and missions.

Student statistic report by MOHE has indicated that student's enrolment in public university has increased every year. Table 3-2 shows the numbers of students' enrolments in the public universities. In eight years (2002 to 2010), there was a significant increase in the students' enrolment of about 64.2%. Data on students' entrance, enrolment and output/graduation from 2002 until 2010 is in Figure 3-1.

Due to the increase in demand, and the expensive cost of building and maintaining new universities, the established universities in Malaysia started to implement e-learning (Raja Maznah, 2004).

Table 3-2 Students Enrolment in Public Universities in Malaysia

Year	2002	2003	2004	2005	2006	2007	2008	2009	2010
Enrolment	281839	294359	293978	307121	331025	382997	419334	437,420	462,780

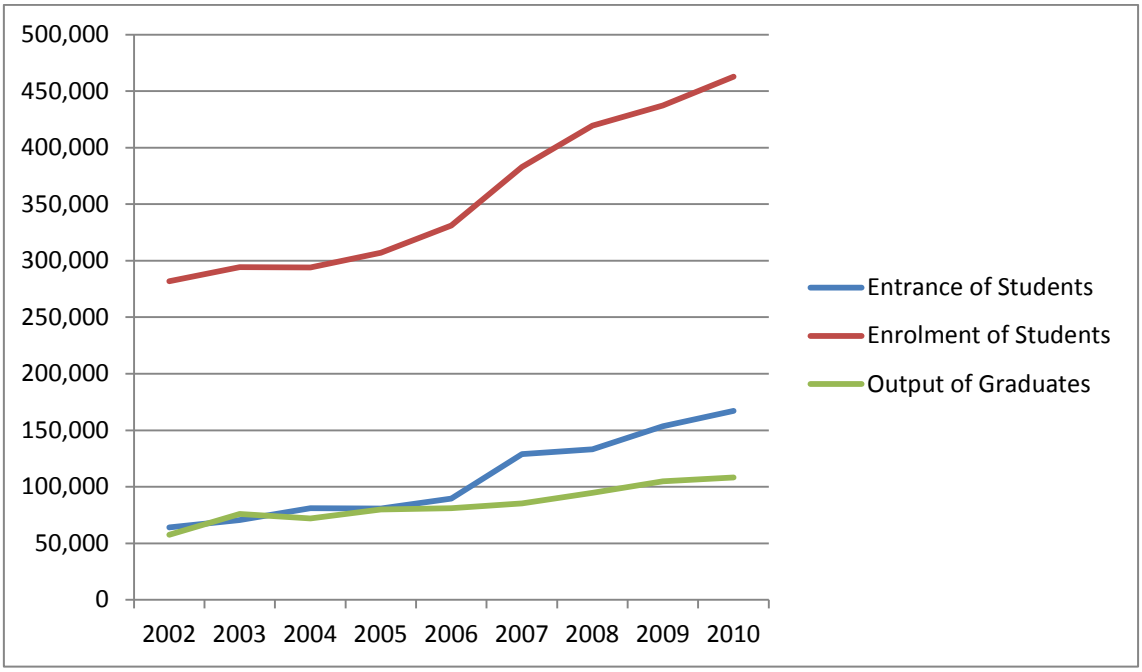


Figure 3-1 Students' Entrance, Enrolment and Output/Graduation from 2002 until 2010

Source: Students' Statistic Report

-Macro Data of Higher Education, (2010)

3.2 E-Learning in Malaysia

E-Learning has been used by several institutions of higher learning in Malaysia since 1990. During that time the implementation of technology in education was limited to the use of computers to increase the understanding of certain topics in the class. In university, the exposure of internet usage and further knowledge of computers is limited to those who are in the school of computer science. Despite this, Asirvatham (2005) claimed that the development of e-learning in Malaysia started during the pre e-learning era when the Educational Technology Division was formed by the Ministry of Education in 1972; possibly using a different technology media.

Even though it was started in 1990, there has not been a comprehensive study on the implementation of e-learning in Malaysian public universities. It is known

that the rapid growth of web-based technologies and the high usage of the internet in Malaysia have made e-learning more viable in recent years. Portals have been set up by many universities to offer e-learning environment either as teaching aids to support a conventional teaching approach or as a teaching medium for long-distance or off-campus programs (Khalid et al., 2006).

In Malaysia, the implementation of e-learning at the higher learning institutions varies (Puteh, 2007). There are three patterns:

a) Using the technology to support or supplement a traditional course

This can be done by placing the course administration information (like syllabuses and study guides) as well as teaching materials (e.g. lecture hand outs and presentations) online, thereby creating a resource base for all the materials. In other words, this information is made easily accessible by the students. Most universities in Malaysia have implemented this way.

b) Integrating online activities in a traditional course to enhance the learning experience

This method is known as blended learning, which most public universities have adopted. There are many ways to integrate Internet-based activities within the traditional course, both individual and group work. For examples:

- online activities to study online learning resources
- online tests to self-assess their own understanding of the subject
- online discussions to maintain a seminar discussion over a longer period of time
- collaborative learning activities for students to work together on research without necessarily being in the same room

c) Delivering a course completely online

Use technology to deliver the course completely online, possibly in parallel with a traditional course or ideally to provide opportunities for both remote and local learners to study in the most appropriate way for their circumstances. In this case all course contents and all course

communications would be available online. The Open University Malaysia (OUM), a private university, implemented this.

Most e-learning in Malaysia is blended learning (Fook et al., 2005). Blended learning has been recommended and used to resolve challenges and limitation of e-learning implementation in Malaysia. The challenges in Malaysia (Ali, 2004) include:

- lacks awareness on the effectiveness of e-learning among parents
- low adoption rate-lack of e-content, inadequate infrastructure, digital divide problem
- bandwidth issues and connectivity
- computer literary and digital divide
- lack of quality e-content
- difficulty in engaging learners online (self-discipline, self-learn and self-motivated attitude)
- language barrier- extensive use of English in e-learning contents

All public universities in Malaysia selected blended learning as their e-learning mode. However the blended learning definition has not been clear and tends to vary at different universities, as guideline of implementation is not available. According to the Asia e-learning Network (AEN) report on Malaysia, few universities were embarking e-learning in 2004 (Asia e-Learning Network, 2004). They are Multimedia University (MMU), Universiti Tun Abdul Razak (UNITAR), Open University Malaysia (UNITEM), Universiti Sains Malaysia (USM), Universiti Teknologi Mara (UiTM), Universiti Putra Malaysia (UPM). The latter three are public universities.

E-learning implementation in public universities started more as individual (lecturer) initiatives and more recently become part of the university's initiative and strategy to enhance the teaching and learning process. E-learning team is developed at the university level and they usually report to the university ICT council to plan and progress e-learning. Although there are government agencies and bodies established to promote national ICT programme such as

the Malaysian Institute of Microelectronic Systems (MIMOS), The Malaysian Communications and Multimedia Commission (MCMC) and National Information Technology Center (NITC), there are no integrated efforts to establish a central body at national level for supporting and monitoring e-learning implementation in higher learning institutions. This situation is due to the concentration of effort on the infrastructure and learning content (Ali, 2004).

As e-learning has been announced as one of the Critical Agenda Projects (CAP) and one of the Key Result Areas (KRA) of MOHE in 2007 (National Higher Education Action Plan 2007-2010, 2007), the Malaysia e–learning in Public Higher Learning Institution known as MEIPTA was established. MEIPTA is a national central body functioning to pilot, drive and guide the e-learning implementation process to ensure the success of e-learning implementation in public universities. Currently the members of MEIPTA are representatives from all the public universities. They are responsible for e-learning initiatives at their respective institutions. Membership does not include any representative from any ministry or government agencies that have a direct link with e-learning in higher education.

The success of e-learning implementation depends very much on the diffusion and adoption rate among the lecturers. If the lecturer uses e-learning, the students' usage will increase. The research conducted among three universities in Malaysia showed the students' need can be categorised as: instructor support, access to structured and focused resources and regulation of motivation and regulation of learning activities (Alias and Jamaludin, 2005). In addition, study by Goi and Ng (2009) has included website security and support as two of the main criteria of success for e-learning implementation in Malaysia. Using a university in Malaysia experience, they have identified maintenance of system and infrastructure safety, intellectual property and copyright among the barriers to e-learning (Karim and Hashim, 2004).

In summary, e-learning in public universities in Malaysia is still at the beginning stage. Based on the e-learning Maturity Model (Marshall and Mitchell, 2007), e-learning in Malaysia public universities is considered at the delivery level (Basir

et al., 2010). A few important management initiatives such as developing a formal e-learning policy, strengthening the top-down strategy and essential initiatives have indicated that e-learning is gradually moving towards the governing stage.

3.3 Information Security Implementation in Malaysia

3.3.1 Threats and Attack

In 2001, Malaysia's Internet infrastructure was attacked by a malicious code-the Code Red worm. This attack, in which the worm spread very fast, brought the national communication network to idle. It was reported that the relevant agencies took three months to eradicate this worm and the estimated minimum loss was RM22 million, which does not include the losses to the business fraternity and other sectors (Yunos, 2008). In 2003, other incidents of cyber-attacks were caused by the Blaster and Naachi worms. The incident started with the propagation of the Blaster worm through the scanning of vulnerable machines via the network, followed by Naachi worms. These worms exploited the vulnerability found in the Windows NT, 2000 and XP software. The estimated cost to eradicate this worm was about RM31 milllion, not including lost productivity and the cost of lost opportunity (Yunos, 2008).

Today, a common attack in Malaysia is the defacement of a website. Web defacement is a malicious activity whereby a website is "vandalised". Malaysia has a vibrant Internet culture that has gained a mass following in a nation where the mainstream media is tightly controlled. In June 2011, Malaysian government's online portal was attacked by the Internet vigilante group Anonymous over government acts of censorship (Koswanage, 2011). Anonymous is a group of global activists lobbying for Internet freedom who frequently try to shut down the websites of businesses and other organisations that they oppose. The hackers attempted to deface the Malaysian government portal and bring it down by overwhelming them with traffic using "denial of service" attacks (Richardson and Koswanage, 2011). The government

managed to react adequately to reduce the incidents of attacks. The affected or attacked websites were recovered in a short time.

Similar to other parts of the world, there are issues and challenges of information security in Malaysia. It was reported in 2009 that the growing dependence on ICT had fuelled problems (News Straight Times, 2009). The most dominant threat is cyberstalking, which is to stalk someone with malicious intent. Reliance on the internet, email, instant messaging, chatrooms, and other communications technologies have made cyberstalking a growing social ill that can affect computer users anywhere in the world. Cyberstalking is a new form of deviant behaviour that uses technology to harass others in various ways including false accusations, slander, sexual exploitation and abuse of victims' email accounts.

The number of reported cybercrimes in Malaysia almost doubled to 5181 in the year 2010, compared with 2642 in 2009 (InfoSecurity.com, 2010). In 2010, it was reported that cyber-attacks were under control (Bernama, 2010), however the situation quickly changed, as in the first four months of 2011, a drastic rise in cybercrimes attacks was reported (The Star, 2011). The number of incidents shown in Figure 3-2, Figure 3-3, Figure 3-4, Table 3-3, Table 3-4, and Table 3-5 produced by CyberSecurity Malaysia represents the increase of incidents from 2008 until 2010. The type of incidents also increased from six classifications in 2008 to nine classifications in 2010. The three most reported incidents are fraud, intrusion and malicious code.

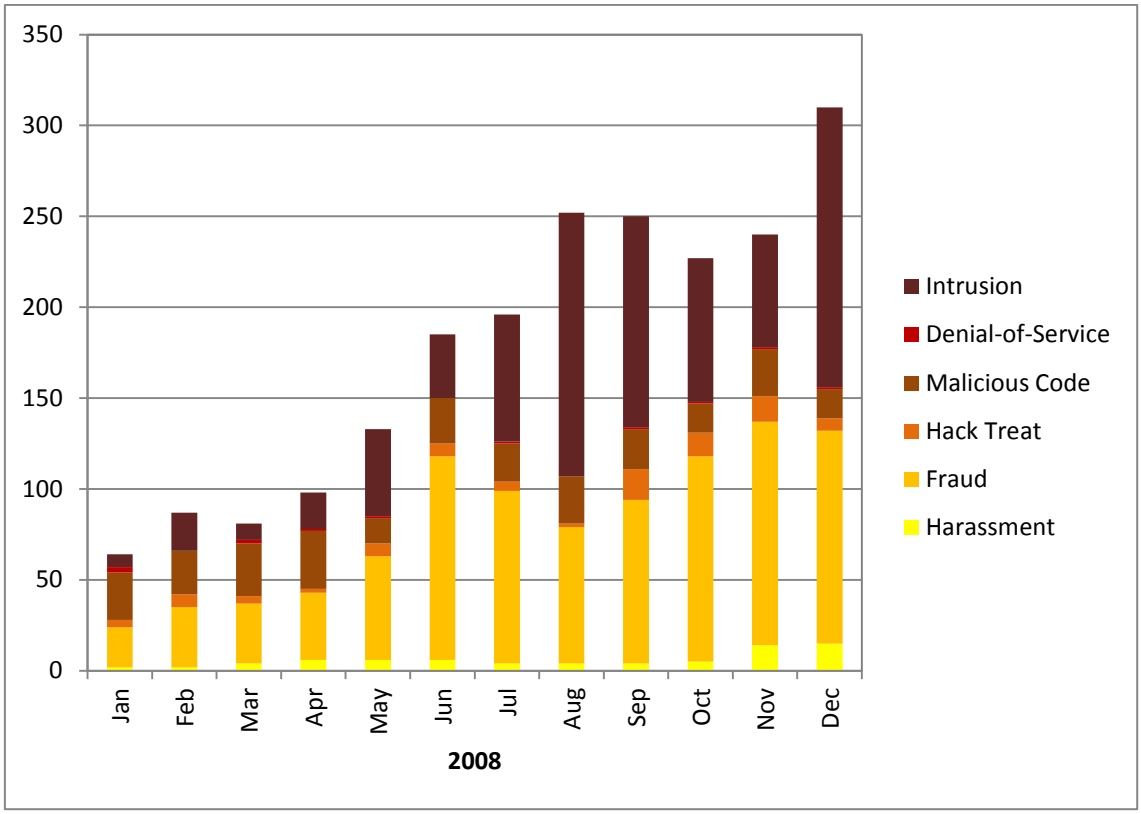


Figure 3-2 Incident Statistics for 2008

Source: (MyCERT CyberSecurity Malaysia, 2010)

Table 3-3 Incident Statistics for 2008

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Harassment	2	2	4	6	6	6	4	4	4	5	14	15	72
Fraud	22	33	33	37	57	112	95	75	90	113	123	117	907
Hack Treat	4	7	4	2	7	7	5	2	17	13	14	7	89
Malicious Code	26	24	29	32	14	25	21	26	22	16	26	16	277
Denial-of-Service	3	0	2	1	1	0	1	0	1	1	1	1	12
Intrusion	7	21	9	20	48	35	70	145	116	79	62	154	766
TOTAL	64	87	81	98	133	185	196	252	250	227	240	310	2123

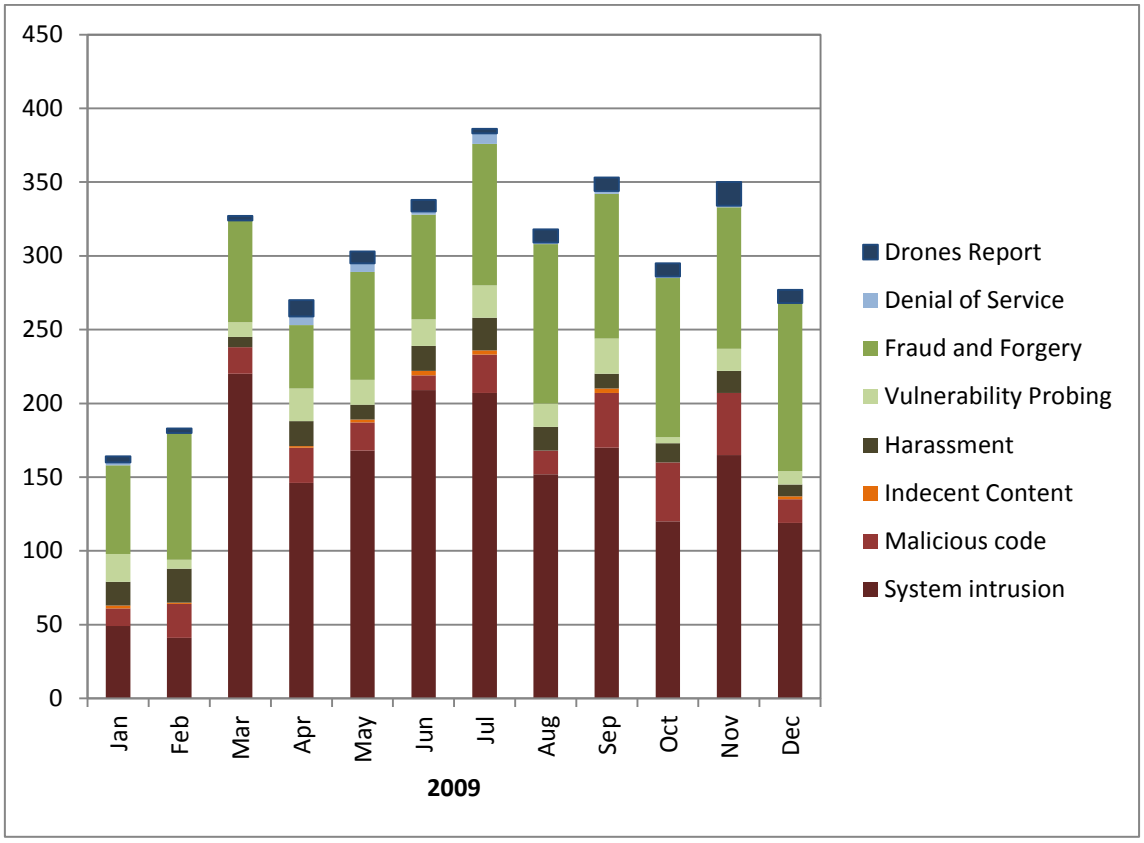


Figure 3-3 Reported Incidents based on General Classification Statistics 2009

Source: (MyCERT CyberSecurity Malaysia, 2010)

Table 3-4 Reported Incidents based on General Classification Statistics 2009

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Drones Report	4	3	3	11	8	8	3	9	9	9	16	9	92
Denial of Service	2	0	0	6	6	2	7	1	2	1	1	0	28
Fraud and Forgery	60	86	69	43	73	71	96	108	98	108	96	114	1022
Vulnerability Probing	19	6	10	22	17	18	22	16	24	4	15	9	182
Harassment	16	23	7	17	10	17	22	16	10	13	15	8	174
Indecent Content	2	1	0	1	2	3	3	0	3	0	0	2	17
Malicious code	12	23	18	24	19	10	26	16	37	40	42	16	283
System intrusion	49	41	220	146	168	209	207	152	170	120	165	119	1766
TOTAL	164	183	327	270	303	338	386	318	353	295	350	277	3564

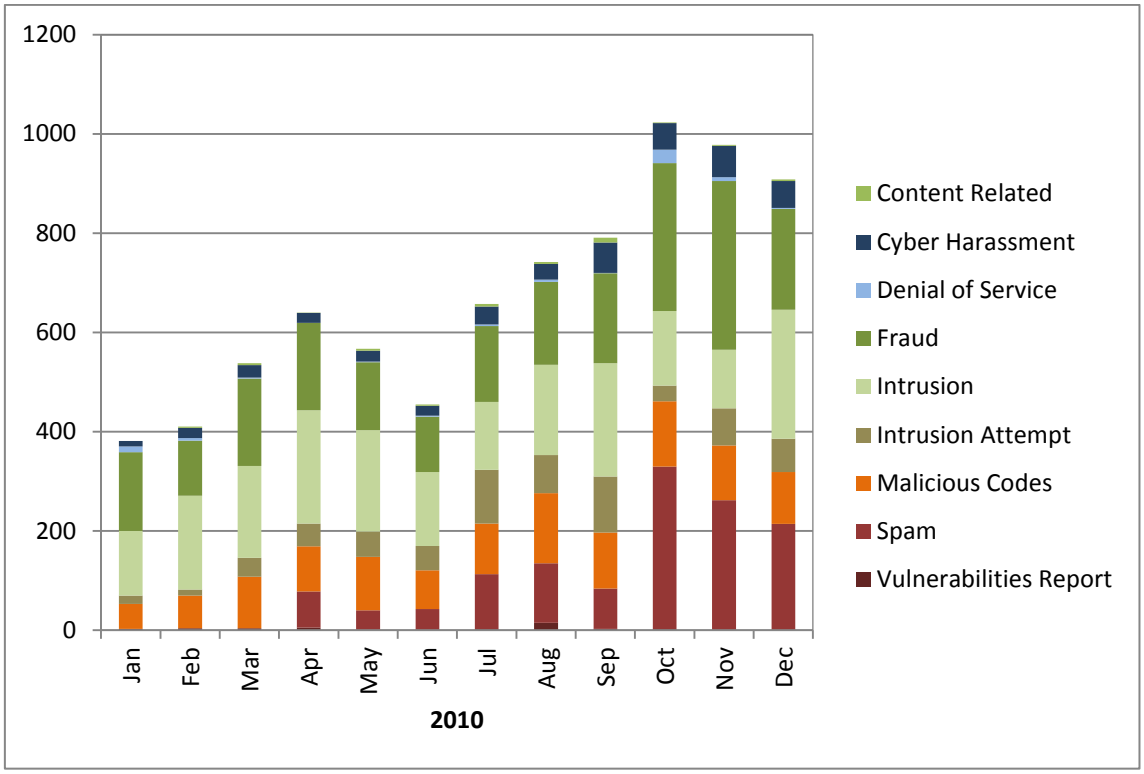


Figure 3-4 Reported Incidents based on General Classification Statistics 2010

Source: (MyCERT CyberSecurity Malaysia, 2010)

Table 3-5 Reported Incidents based on General Classification Statistics 2010

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Content Related	0	2	4	1	4	3	5	4	10	1	2	3	39
Cyber Harass-ment	11	21	25	20	22	20	36	32	61	54	63	54	419
Denial of Service	11	5	2	0	1	2	3	4	1	27	8	2	66
Fraud	159	111	176	176	137	111	153	167	181	298	340	203	2212
Intrusion	130	189	185	228	204	149	137	182	228	150	118	260	2160
Intrusion Attempt	17	12	38	46	51	49	108	77	113	32	75	67	685
Malicious Codes	50	66	104	91	108	78	102	141	113	131	110	105	1199
Spam	0	0	0	73	39	42	111	120	81	328	261	213	1268
Vulnerabili-ties Report	3	4	4	5	1	1	2	15	3	2	1	1	42
TOTAL	381	410	538	640	567	455	657	742	791	1023	978	908	8090

Malaysia has 17 million people surfing the Internet on a regular basis, and this number is expected to increase as the government funds deployment of broadband networks throughout the country (InfoSecurity.com, 2010). The Deputy Minister of Science, Technology and Innovation, Datuk Fadillah Yusof in his speech at Cyber Security Malaysia Awards, Conference and Exhibition 2010 claimed that with the rise of digital cities in Malaysia, it has become even more crucial to put in place the policies and mechanisms to ensure the security of government, businesses and individuals. With security assurance in place, government, businesses and individuals can continue to play an innovative and creative role in sustaining the digital cities. Thus, information security especially the cyber security has become an important and significant component of national security, public safety and privacy in all domains.

3.3.2 Governance

It is claimed that cyber-attack in Malaysia is under control, since the Malaysia government has put efforts in ensuring a safe electronic environment in the country (Bernama, 2010). The focus of security in Malaysia is to:

- reduce the vulnerability of ICT systems and networks
- nurture a culture of cyber security among users and critical sectors
- strengthen Malaysian self-reliance in terms of technology and human resources

Currently security in Malaysia is monitored by CyberSecurity Malaysia which is an agency under the Ministry of Science and Innovation (MOSTI). Earlier in 1997, *Malaysian Computer Emergency Response Team (MyCERT)* was established to address computer security issues among Malaysian Internet users. The team to manage information security had gone under multiple transformations. Since 2007 the team was renamed as Cybersecurity Malaysia. In 2008 the government appointed CyberSecurity Malaysia as the sole certification body for the evaluation and certification scheme based on MS ISO/IEC 15408: 2005 *Information Technology - Security Techniques -*

Evaluation Criteria for IT Security. This certification body is named *Malaysian Common Criteria Certification Body (MyCB*).

3.3.3 Function of CyberSecurity Malaysia

Many Malaysia internet users are not aware that there is an agency that looks after the safety of Malaysian cyberspace. Among services offered by CyberSecurity Malaysia is a help centre called the Cyber999^{TM} service, to provide consultancy to organisations and individuals on cyber security incidents, such as harassment and malware infections on their computers. They provide advice on how to cope with cyber threats and deal with safety issues, provide specialised services to support the growth of digital forensics, security management & best practices and cyber security products evaluation based on international standards. They also provide an evaluation facility for third party validation on quality and reliability of Malaysian-made security products to ensure that Malaysian products get accepted globally. They provide training and create awareness in the area of cyber security with a training and examination centre for many international certifications in helping to increase the number of cyber security professionals. In addition, CyberSecurity also develop educational content on cyber security, suitable for internet users from different age groups ranging from students, office workers to home users. These can be downloaded for free from the website www.cybersecurity.my or through an independent awareness website, www.cybersafe.my .

Malaysia also introduced a National Cyber Security Policy (NCSP) in 2005 which aims to reduce the vulnerability of ICT systems and networks. This policy aims to address and mitigate the risks that are faced by the Critical National Information Infrastructure (CNII) sectors in facing cyber threats (CNII Portal). The CNII sectors are:

- National Defence & Security
- Banking & Finance
- Information & Communications
- Energy

- Transportation
- Water
- Health Services
- Government
- Emergency Services
- Food & Agriculture

Critical National Information Infrastructure (CNII) is defined as assets (real and virtual), systems and functions that are vital to the nations and the incapacity or destruction of these would have a devastating impact on:

- National economic strength; Confidence that the nation's key growth area can successfully compete in global market while maintaining favourable standards of living.
- National image; Projection of national image towards enhancing stature and sphere of influence.
- National defence and security; guarantee sovereignty and independence whilst maintaining internal security.
- Government capability to functions; maintain order to perform and deliver minimum essential public services.
- Public health and safety; delivering and managing optimal health care to the citizen.

The NCSP outlines a set of action plans that should be implemented to achieve the NCSP's objectives, which include identifying appropriate cyber security measures, developing a comprehensive cyber security programme and a series of frameworks for protecting CNIIs. It tries to instil a culture of cyber security among Internet users and strengthen Malaysian self-reliance in terms of technology and human resources. Not many countries have such a policy or enacted laws like the Computer Crime Act 1997 and the Communication and Multimedia Act 1998.

Media release has reported the implementation of ISMS by CNII sectors to enhance information security (CyberSecurity Press Release, 2010). The implementation of ISMS will ensure that CNII organisations have information security management systems that meet international standards. The Malaysia standard developed is identical to ISO/IEC 17799:2000 which was published by the International Organisation Standard and International Electronically Commission (IEC).

Security awareness is one of the issues and on-going activities have been planned to increase the security awareness among the Malaysian user. It is very important for Malaysia to take information security seriously when devoting its efforts to use information technology now and in the future (Al-Salihy et al., 2003).

3.4 Malaysia Security in E-Learning

Similar to the rest of the world, e-learning in Malaysia needs to be secured. ISM is the stream of management activities that aim to protect information assets and secure the framework of organisation where the information system is operated (Von Solms, 1998). It implies that assessment of information assets might differ from organisation to organisation depending on the geography and business scope of the organisation. Malaysia as a developing country would have different point of views towards information assets and managing information security. This is due to different levels of economic development, technological know-how and education that have been discussed in the earlier sections. Even among the developing countries, there would be differences for example, the varying percentage of the IT illiterate population which might prevent organisations in developing countries from noticing their information security needs. Though the threats of attack on information assets would be less in developing countries compared to developed countries with a large IT literate population (Abu-Zineh, 2006), the threats of misuse and loss of information assets in developing countries might be higher than in developed

countries. This is can be seen in Figure 3-2, Figure 3-3, Figure 3-4, Table 3-3, Table 3-4, and Table 3-5 by CyberSecurity which indicates that most threats are fraud, intrusion and malicious code.

Though ISMS has been introduced in Malaysia using the adaptation of international standards, the sectors that have been classified as critical have been the focus. Unfortunately education is not classified as a critical sector in Malaysia. Therefore there is no specific policy or guidance on information security in education or for e-learning environments.

In CyberSecurity Malaysia's website, there are many guidelines and best practices prepared for users. These include safety information on online shopping, online banking, social networking, including safe online gaming. Unfortunately there is no such best practice or guideline for safe e-learning.

Technology in Malaysia may be better than other developing countries. The mixed background of Malaysia with its various levels of education, social status and culture has influenced perceptions towards security. E-learning in Malaysia is at the early implementation stage, where the main concern revolves around the high investment cost, infrastructure setup, contents and acceptance, and the security issues have not been given priority.

The e-learning security characteristics in Malaysia public university are unknown. It is assumed that most universities are using the general guidance provided by the government on how to combat the security issues in e-learning. E-learning is always believed to be one of the secured systems with the assumption that security technology has been embedded together within the system.

3.5 Chapter Summary

This chapter has explored the information security management gap in e-learning in Malaysia. At the moment, information security management in e-learning in Malaysian public universities is a grey area. Based on the country's CNII background, e-learning and education has not been considered as a critical sector. However with the increase usage in e-learning, the information security threats in e-learning would be more important to be addressed.

The following chapter will discuss the research methodology used to address the research gap found from both Chapter 2 and Chapter 3.

4 RESEARCH METHODOLOGY

This chapter explain the methodology used in this research. This research was carried out with a constructive–interpretive philosophical assumption applying qualitative research strategy. This research has gone through four phases as illustrated in figure 1.1 in Chapter 1. Multi-method studies in two stages of data collection and analysis has been conducted. This chapter is divided into three sections, namely research philosophical assumption and paradigm, research design and research process. The research philosophical assumption and paradigm section discuses on how the social research is viewed. The research design section explains the applied strategy and methods. The research process details the phases conducted.

Embracing the socio-technical system thinking, this research aims to develop an ISM model incorporating the people behaviour. This model is developed to help the e-learning management to pre–empt the vulnerabilities and threats that are induced by the stakeholders in the e-learning environment. The research is conducted to discover the dimensions that need to be analysed for e-learning security.

Better understanding of the behaviour of stakeholders, potential threats can be predicted and suitable control can be suggested. There is no established e-learning stakeholder security for the author to build on. Therefore studies listed below were conducted:

- the perception of security issues among users in e-learning
- the information security threats for e-learning
- the security attacks and incidents in e-learning environment
- the current status of e-learning implementation and security issues in Malaysia Public universities

4.1 Research Assumptions and Paradigms

The way of looking at the world when conducting research is known as research philosophical assumption and research paradigm. Basically there are three main research assumptions: ontological, epistemological and methodological.

The ontological assumption relates to the nature of reality and what exists. Ontological assumptions can be divided into two categories, namely objectivism and constructivism. Bryman and Bell (2007) explained objectivism as an ontological position that asserts social phenomena, and their meanings have an existence that is independent of social actors. It connotes that social phenomena and the categories used in everyday discourse have an existence that is independent or separate from actors. While constructivism is an ontological position which claim that social phenomena and their meanings are continually being accomplished by social actors (Bryman and Bell, 2007). It suggests that social phenomena and categories are not only produced through social interaction but they are in a constant state of alteration or revision.

The epistemology assumption of a research is about the researcher interaction with the object of research and can affect that object; findings are created through interaction between researchers and researched. There are three philosophical epistemologies commonly used in research namely positivism, interpretivism and realism. According to positivists, knowledge is valid only within observable and measurable phenomena. Interpretivist is the term given in complete contrast to positivism; it is concerned with the understanding of human behaviour from the participant‘s own frame of reference (Hussey and Hussey, 1997). Realism or critical social science stands between positivism and interpretivism (Bryman, 2008); realism agrees with the positivism view that society is an unchanging order, and adds the social context, which is not considered in positivism. Table 4-1 illustrates the features of positivism and interpretivism (Collis and Hussey, 2009). While the realism sits between both.

Table 4-1 Features of Positivism and Interpretivism

Positivism tends to:	Interpretivism tends to:
• Use large samples • Have an artificial location • Be concerned with hypotheses testing • Produce precise, objective, quantitative data • Produce result with high reliability but low validity • Allow results to be generalised from the sample to population • Use methodologies such as surveys, experimental studies and cross-sectional studies.	• Use small samples • Have a natural location • Be concerned with generating theories • Produce rich, subjective, qualitative data • Produce result with high validity but low reliability • Allow findings to be generalised from one setting to another similar setting • Use methodologies such as case studies, grounded theory and action research.

It is important to define the strategy of research conducted. Research can be conducted using quantitative (fixed design) or qualitative (flexible) research strategy. Blaikie (2000) explained that *'Quantitative methods are generally concerned with counting and measuring aspects of social life, while qualitative methods are more concerned with producing discursive descriptions and exploring social actors' meaning and interpretations'*. Qualitative research is a form of social inquiry that focuses on the way people interpret and make sense of their experience and the world in which they live (Holloway, 1997). Bryman & Bell (2007) indicated that quantitative data leans towards positivism and objectivism. In contrast, qualitative data research deals with interpretivism under epistemological assumptions, and constructivism under ontological assumptions. A comparison is made between two types of data: quantitative and qualitative and summarised in Table 4-2.

Table 4-2 Quantitative and Qualitative (Robson, 2002)

Quantitative	**Qualitative**
• Is used in research that requires facts and figures in order to answer the research question (through verification of hypothesis). • Seeks to measure, test, and quantify elements in order to explain or describe something	• Deals mainly with the exploration of issues and the generation of theories within new and emerging subject areas. • Is used to develop insight and understanding of a subject. • Seeks to create gestalt and holistic interpretations.

Finally, methodological assumption focuses on analysis of the methods used for gaining the data. Creswell (2009) summarised methodologies associated with different epistemology and ontology, as can be seen in Table 4-3.

Table 4-3 Research Assumption, Paradigm and Type

Research assumption	**Paradigm and Type**		
Ontology	Objectivism	Constructivism	
Epistemology	Positivism	Realism	Interpretivism
Methodology (Strategy)	Quantitative • Experimental design • Non-experimental design (survey)	Quantitative + Qualitative • Sequential • Concurrent • Transformative	Qualitative • Narrative research • Phenomenology • Ethnographies • Ground theory studies • Case study

4.2 Research Design

Information security management in e-learning has been neglected and most research related to this topic focus on the technical issues. Management control has typically been top down, where the policy and procedures are drawn to be followed by the users. Yet little is known on the bottom up direction that considers the end users behaviour, based on their roles in organisation. This research gap could yield significant insight to complement the current ISM standards. It is aimed at looking at the procedures and policies for targeted groups of behaviour rather than having the same policy applied to every group of people. A model or an approach that helps to identify the groups, security behaviour and control is to be created. The subject of inquiry deals with people putting this research in the social technical system context.

This research requires understanding of the e-learning stakeholders and their experience, which posits the constructivism assumption. Based on the nature of the research problem, the constructivism- interpretivism paradigm is adopted, as this approach focus on human beings and their way of interpreting and making sense of reality.

Qualitative research is commonly premised on the idea that the theory and method will emerge during the course of the research and will not be specific at the beginning (Denscombe, 2010). Theories can be developed and tested as part of the on-going process (Glaser and Strauss, 1967). Moreover the sample to be investigated will depend on following up leads, thus how many or which people or events will be investigated will not be known or determined until certain preparation is made and necessary requirement recognised (pre-studied). Therefore an analytical approach with multi-method studies has been chosen as the method to answers to the research problem.

The pilot study to understand user security perception indicated that interaction only with stakeholders may not answer the research problem. Primary data related to the security threats and issues in organisations are considered as private and confidential and it is quite impossible to obtain such first-hand

knowledge. The ideal way to collect data is to use the existing knowledge that can be found from multiple sources. The use of such multiple methods has the important benefit of reducing inappropriate certainty, where a single line of investigation produces a clear-cut result that may lead investigators to believe they have found the `right' or complete answer (Robson, 2002). Due to the emergent nature of research, this study has conducted two stages of data collection and analysis.

The first stage of data collection, analysis and findings is to explore and understand the security in e-learning. From the literature reviews, it is realised that some studies have been done on security in e-learning with most of them focusing on the technological aspect. Therefore as a start, a pilot study, using online web survey was conducted to explore the information security threats and issue in e-learning among the e-learning users. The results of the pilot study demonstrated the difficulties in collecting data from people on the topic of information security. Two desk studies were conducted. Threats analysis study was conducted to achieve a list of information security threats for e-learning. The incident logging study was conducted to identify the security attacks and incidents in e-learning environment. To gather more information about security in e-learning in Malaysia, an interview had been carried out. The intended results for these studies are to fill the literature knowledge gaps and clarify the situation in Malaysia e-learning. The findings from this stage provided insight to proceed to the second stage of data collection, analysis and findings.

The second stage of data collection, analysis and findings is to understand the cultural view in people and its impact on e-learning for ISM model building. E-learning community modelling identified the stakeholders and roles, and the possible significant individual culture view. The stake holder cultural view analysis was an attempt to identify the susceptibility of threats according to the cultural view of stakeholders.

4.3 Research Process

This section details the four stages of the research process, which consists of six main steps. Figure 4-1 (page 98 & 95) illustrates the research process together with the input and output for each process. The following explains the details of the steps in each phase. The phases are Planning, Data Collection and Analysis, Model Development, and Discussion and Conclusion. Mapping to the Figure 1.1 in Chapter 1, the Planning phase is broken down as step1 and 2. The Data Collection and Analysis phase is detailed as step 3 and 4. Model developed from step 4 validated in step 5 and Discussion and Conclusion Phase is elaborated in step 6. Table 4-4 presents the mapping.

Table 4-4 Four Phases of Research Methodology vs. Seven Steps Research Process

Phase	Research Process Step
Planning	Step 1: Formulate Research Problem Step 2: Review Literature on Research Areas
Data Collection and Analysis	Step 3: Designing Research Methodology Step 4: Research Realisation – Model Built
Model/Approach Development	Step 5: Model Validation
Discussion and Conclusion	Step 6: Discussion and Conclusion

4.3.1 Step1: Formulate Research Problem

The initial stage of the research was to explore the information security issues. It was then narrowed down to address ISM for the different users groups in e-learning due to the fact that most discussions have neglected the targeted behaviour of users in dealing or suggesting countermeasures. The research aimed at investigating on how to enhance information security management in

the e-learning environment security. It is argued that addressing the stakeholder's behaviour improved information security management. The main objective of this research is to develop an ISM model/approach that can effectively recognise and use the behaviour of e-learning stakeholders. This approach positively influences the stakeholders to cultivate security awareness. Malaysia was selected as the evaluation context due to three reasons, firstly the author is sponsored by Malaysia government; secondly due to Malaysia's interest and continued effort in e-learning implementation where the data collection and findings may contribute to e-learning effort in the country; and thirdly due to the author's work experience and future career remains in the country context.

4.3.2 Step 2: Review Literature on Research Areas

The literature review was conducted by systematically identifying the research topic and basic keywords (Hylton and Lewis, 2006). The literature includes journal articles, conference papers, white papers, magazines, books, and trusted websites articles.

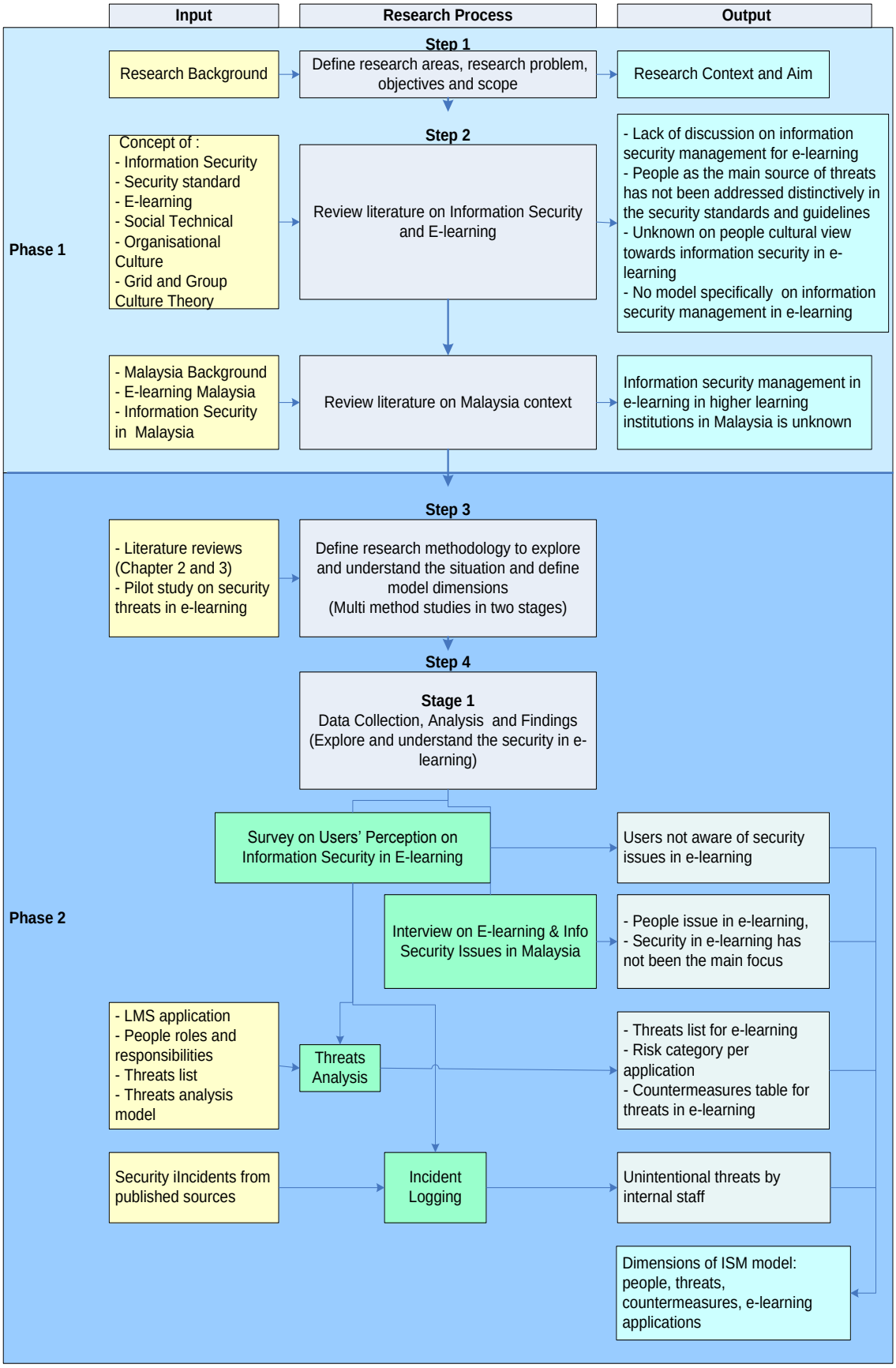
During this stage, the author studied and reviewed the literature regarding the concept of information security and e-learning which provide greater knowledge and understanding regarding both areas. A review on information security and e-learning in Malaysia context was conducted as well. The duration used for searching the articles was between 1990 and 2011. Literature review on the security of e-learning was carried out to look at previous researches and publication that has been conducted. The review on the management and system has led to the use of the social technical approach in conducting this research and the use of Cultural Theory in the study. In Malaysia context review, this step has guided the shaping of the research problem and research methodology. The literature review step is a continuous process and was conducted throughout the research duration.

4.3.3 Step 3: Designing Research Methodology

Based on the input from literature gaps and the situation of Malaysia, the interpretivism approach has been chosen. Qualitative strategy, using multi-method studies in data collection and analysis has been carried out for this research. Table 4-5 displays the two stages of multi-method data collection and analysis type conducted for this research.

Table 4-5 Two Stages of Multi-Method Data Collection and Analysis Type

Stage	Study	Method of Data Collection	Analysis Type
1	1 - User's Perception on Information Security In E-Learning	Questionnaire online web survey (Field study)	Descriptive analysis
	2 - Threats Analysis	Literature/documents survey (Desk study)	Content analysis-categorical
	3 - Incident Logging	Literature/documents survey (Desk study)	Content analysis-categorical
	4 - E-Learning & Its Information Security Issues in Malaysia	Interview survey (Field study)	Theme analysis-summary
2	5 – Stakeholder Cultural View Modelling	Literature/documents survey (Desk study)	Content analysis-categorical
	6 – Cultural Views inclusive Risk Analysis	Literature/documents survey (Desk study)	Content analysis-categorical


Input
Research Process
Output
Phase 1
Step 1
Research Background
Define research areas, research problem, objectives and scope
Research Context and Aim
Step 2
Concept of :
- Information Security
- Security standard
- E-learning
- Social Technical
- Organisational Culture
- Grid and Group Culture Theory
Review literature on Information Security and E-learning
- Lack of discussion on information security management for e-learning
- People as the main source of threats has not been addressed distinctively in the security standards and guidelines
- Unknown on people cultural view towards information security in e-learning
- No model specifically on information security management in e-learning
- Malaysia Background
- E-learning Malaysia
- Information Security in Malaysia
Review literature on Malaysia context
Information security management in e-learning in higher learning institutions in Malaysia is unknown
Phase 2
Step 3
- Literature reviews (Chapter 2 and 3)
- Pilot study on security threats in e-learning
Define research methodology to explore and understand the situation and define model dimensions
(Multi method studies in two stages)
Step 4
Stage 1
Data Collection, Analysis and Findings
(Explore and understand the security in e-learning)
Survey on Users' Perception on Information Security in E-learning
Users not aware of security issues in e-learning
Interview on E-learning & Info Security Issues in Malaysia
- People issue in e-learning,
- Security in e-learning has not been the main focus
- LMS application
- People roles and responsibilities
- Threats list
- Threats analysis model
Threats Analysis
- Threats list for e-learning
- Risk category per application
- Countermeasures table for threats in e-learning
Security iIncidents from published sources
Incident Logging
Unintentional threats by internal staff
Dimensions of ISM model: people, threats, countermeasures, e-learning applications

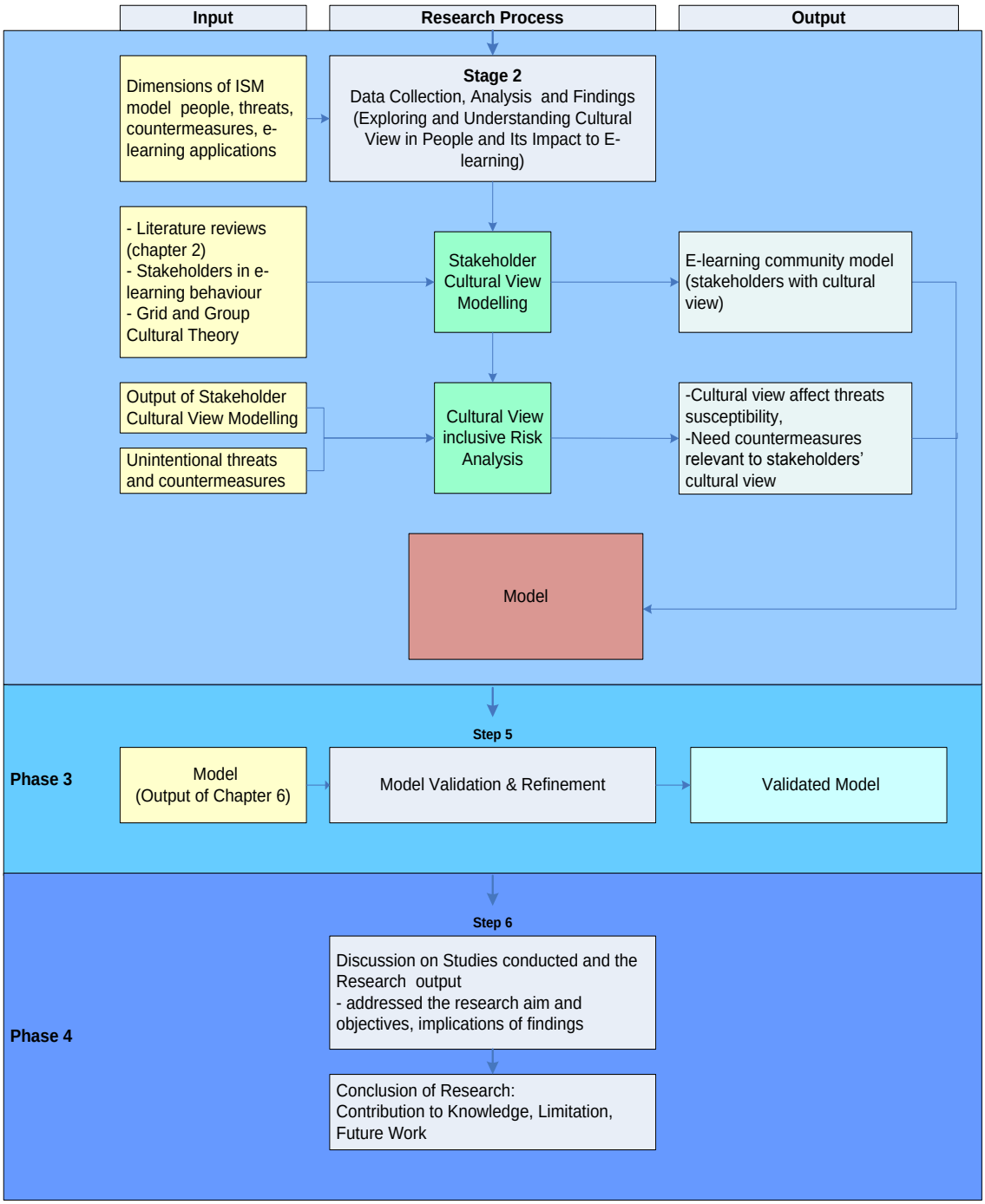


Figure 4-1 Research Process

4.3.4 Step 4: Research Realisation –Stage 1 and 2.

Six studies were done to build up the knowledge necessary for model building:

- Study 1- User's Perception on Information Security in E-Learning
- Study 2: Threats Analysis
- Study 3: Incident Logging
- Study 4: E-Learning and Its Information Security Issues in Malaysia
- Study 5: Stakeholder Cultural View Modelling
- Study 6: Cultural View inclusive Risk Analysis

The purpose, design analysis and results are reported in Chapter 5 and 6. Model building is discussed in Chapter 6.

4.3.5 Step 5: Validation (Expert Review)

An open ended questionnaire was provided to security and e-learning experts to review the model applicability and effectiveness. The process of validation is discussed in Chapter 7.

4.3.6 Step 6: Discussion and Conclusion

The final step is the discussion and the preparation for thesis writing. Chapter 8 and 9 has the discussion and conclusion for this research.

4.4 Chapter Summary

In this chapter, the research design considerations are discussed and the methodologies and methods chosen to tackle the research problem are explained. The choice of research philosophy, strategy and methods are summarised in Table 4-6.

This chapter also explained the research process. Data collection and analysis are conducted in two stages. The details of each study are explained in the following chapters. Chapter 5 explains the first stage of data collection, analysis and findings which consists of four studies, while Chapter 6 explains the building of model with the second stage of studies. Two studies were conducted and a model developed.

Table 4-6 Research Considerations Summary

<table>
<tr><th>Research consideration</th><th colspan="2">Paradigm and Type</th></tr>
<tr><td>Ontology assumption</td><td colspan="2">Constructivism</td></tr>
<tr><td>Epistemology assumption</td><td colspan="2">Interpretivism</td></tr>
<tr><td>Strategy</td><td colspan="2">Qualitative</td></tr>
<tr><td rowspan="2">Methods (Data collection and analysis)</td><td colspan="2">Multi-method studies</td></tr>
<tr><td><u>Desk study</u>
• Literature/Document survey</td><td><u>Field study</u>
• Online questionnaire survey
• Open ended interview</td></tr>
</table>

5 EXPLORING E-LEARNING SECURITY

This chapter explains the studies conducted in the first stage of Step 4 of the research methodology. The aim of this stage is to explore and understand security in e-learning, with the intention to discover feasible dimensions for designing the ISM model. There are four studies in this stage. Two studies were conducted as field studies and the other two as desk studies. In this chapter, each study is reported in detail with the purpose, methodology, results and findings. At the end of the chapter, the integration and significance of the four studies will be highlighted.

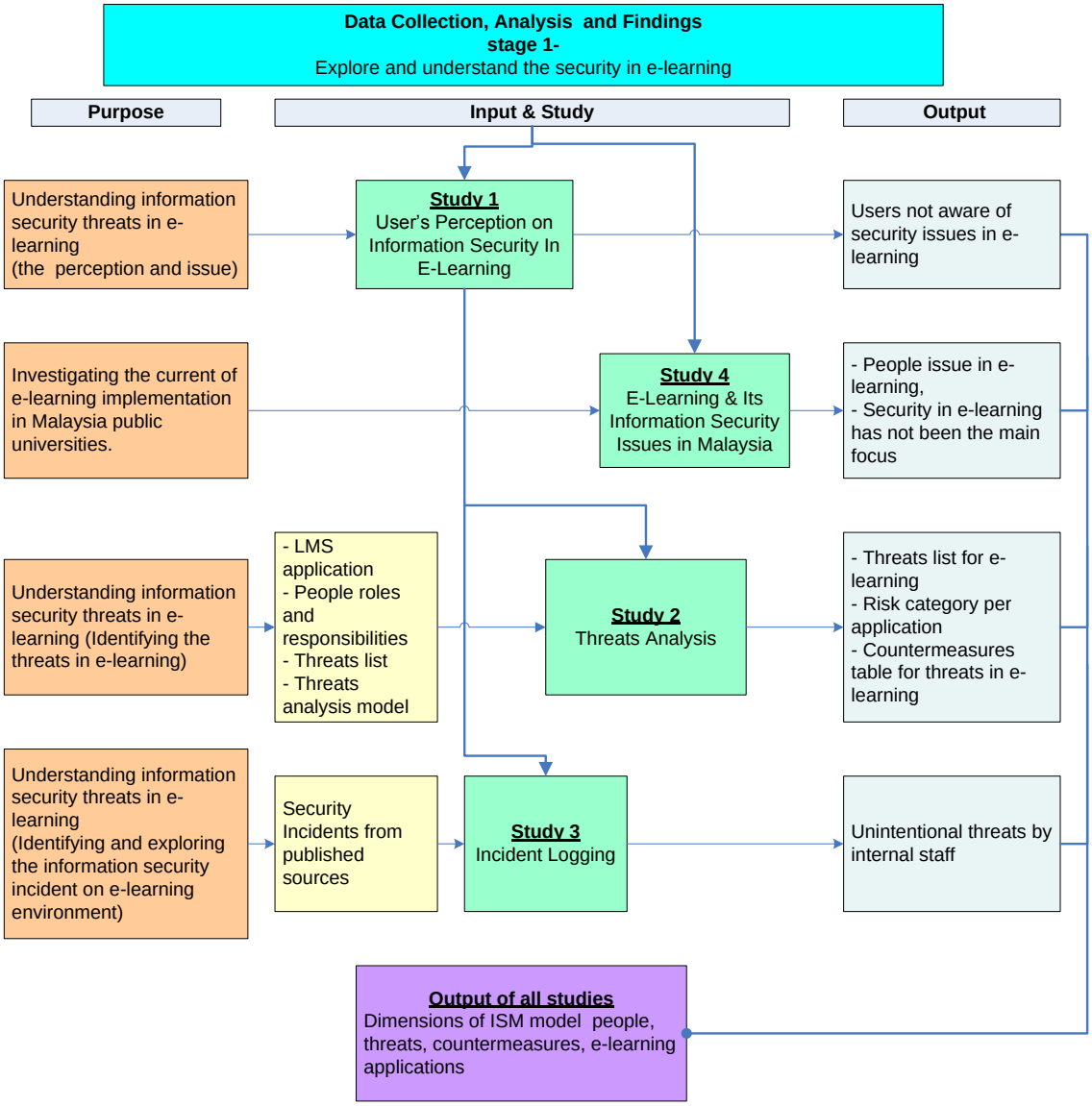


Figure 5-1 Stage 1- Study Purpose, Input and Output

Figure 5-1 illustrates the elements related to data collection, analysis and findings for the first stage of this research. Due to the findings from Study 1 not being satisfactory, Study 2 and Study 3 were carried out.

5.1 Study 1- User's Perception on Information Security in E-Learning

5.1.1 Purpose

In a functional e-learning environment, the content and services to the users must be interoperable, usable, manageable and durable (Norman and Da Costa, 2003). A functional e-learning environment includes the users' security and users' protection. At present, information security technology hardware and software are being used to secure e-learning environments either as the preventive or detective control. Understanding the perception of users towards the security threats and issues in the e-learning environment will help in identifying what needs to be protected and how best to protect it (Adams and Blandford, 2003).

As discussed in section 2.3.6, users in an e-learning environment can be classified as two main groups, which are the supply and the demand group. The supply group refers to the people who ensure that teaching and learning takes place in the e-learning environment. This group may consist of people from management, education (lecturer) and technical backgrounds. The demand group are the clients of the e-learning services who are the students, sometimes lecturers are also considered in this group.

An online survey study which focused on the supply group was carried out to collect information from e-learning users regarding their perception on information security threats in the e-learning environment. The study was conducted to explore the users' perception on:

1. Information security threats in e-learning
2. The impact of the information security threats in e-learning

3. The importance of good security management in e-learning

4. The ranking of different information security threats in e-learning

This study also later analysed whether:

1. the user's role influences the perception of information security threats

2. the user's institution influences the perception of information security threats

3. the level of information security awareness influences the users' perception of security

Influence is analysed as a relationship between the e-learning entity (users, institution categories, level of information security awareness) and information security threats.

5.1.2 Methods

The online survey strategy was used as this study is intended to investigate the users' perception and issues of what is currently happening in their institutions. Surveys are appropriate for self-reported beliefs or behaviour (Neuman, 2005), therefore only people who are particularly involved in that environment can describe the situation. This online survey website is secured by the third level of Secure Socket Layer (SSL) version 3.

The targeted respondents are practitioners of e-learning such as instructors, IT support and administrative staff. They could be from higher learning institutions, further education institutions and training institutions which use e-learning.

Measurement development

The questionnaire developed, based on the literature reviews. The questionnaire labelled as Appendix A in this thesis. The questionnaire consists of 24 questions with multiple sub questions and divided into three sections: user background, institution background and information security threats. Most of the

questions were structured to a five point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree. There is also a ranking question.

The questionnaire piloted for reliability and validity with the Cranfield University learning service team. Some items were revised and deleted to improve the content validity and reliability as well as the questionnaire interface.

The subject and procedure

The online survey website opened for response for two months, starting on 30th November 08 until 31st January 09. Invitations to participate in this survey were sent to the 20 *Joint Information Systems Committee* (JISC) mailing list groups related to e-learning. JISC is a committee, funded by the United Kingdom Higher Education and Further Education funding bodies, to provide world-class leadership in the innovative use of ICT to support education and research.

In order to determine if they are qualified or experienced enough to answer subsequent questions, a filter or contingency question asked.

Data analysis

A tool called *Analyse Survey Responses* given by the online web survey provider and MS Excel spread sheet were used as analysis tools. The results were presented in descriptive statistic which were later descriptively analysed.

5.1.3 Results & Analysis

This section discusses the data collected concerning the users' perception of information security threats in an e-learning environment, the impact of threats to the learning providers and good security management in e-learning and the threats ranks in e-learning. Table 5-1 summarises the users' profile and descriptive statistics of the respondents.

Table 5-1 Summary of the Users' Profile and Descriptive Statistics of the Respondents

Subject (n=48)	*Demographic*	
Measure and items	*Response Frequency (%)*	*Response Count*
Computer Literacy		
Low	*0.0*	*0*
Medium	*18.8*	*9*
High	*81.2*	*39**
Security Awareness		
Low	*0.0*	*0*
Medium	*45.8*	*22*
High	*54.2*	*26**
Working experience in e-learning environment (year)		
Less than 1	*12.5*	*6*
Between 1- 5	*41.7*	*20**
Between 6-10	*29.2*	*14*
More than 10	*16.7*	*8*
Number of years institution been operating an e-learning environment		
Less than 1 year	*2.1*	*1*
Between 1- 5 years	*35.4*	*17*
Between 6-10 years	*50.0*	*24**
More than 10 years	*12.5*	*6*
**mode= the most frequent*		

5.1.3.1 Respondents

The number of respondents who started the survey was 115. However the number of respondents who completed the survey was 50. Many of them decided not to continue answering the questions because they said they didn't know the answers. After considering the filter or contingency questions for the respondents, a total number of 48 completed surveys can be used which gives an effective response rate of 41.7%. Table 5-2 lists the percentage of respondents according to the roles.

Table 5-2 Respondents Roles in E-Learning Institution

No.	*Roles*	*Percentage*
1.	*Management*	*20.2*
2.	*Instructor/ Lecturer*	*36.8*
3.	*IT Personnel*	*6.2*
4.	*Others*	*36.8*

The respondents are 20.2% from management, 36.8% as an instructor or lecturer, 6.2 % are IT personnel and others are 36.8%. Others include librarians and other positions which are not in the above categories. This data showed that most respondents are users of e-learning, working not as IT specialists, therefore the data collected reflected the e-learning users' opinion, based on their experience working in the e-learning environment, with limited access to the technical details of security information in e-learning.

5.1.3.2 Users' Perception on Information Security in E-Learning Institutions

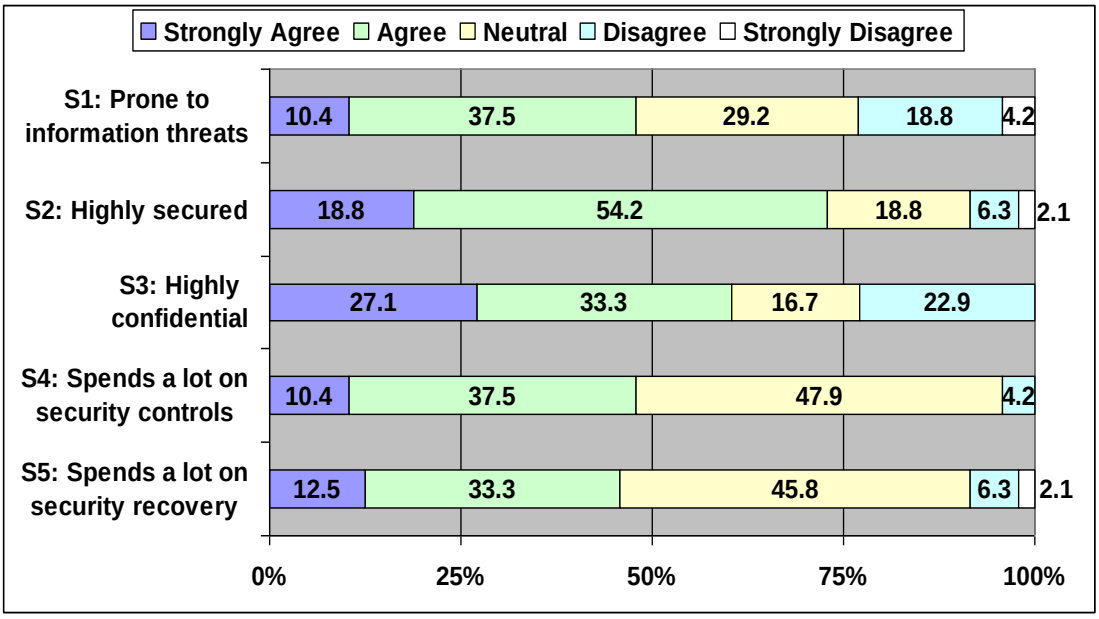


Figure 5-2 Users' Perception on Information Security in E-Learning Institutions

The respondents were asked to define their level of agreement in the statements related to information security in their e-learning institution.

Figure 5-2 illustrates the users' perception in information security in e-learning institutions.

Almost 50% of respondents chose *the agree* and *strongly agree* categories for statements *S1: E-Learning environment is prone to information threats, S4: My e-learning institution spends a lot on security controls,* and *S5: My e-learning institution spends a lot on security solutions and recovery*. More than 50% of respondents agreed on statement *S2: My e-learning institution is highly secure* and *S3: My e-learning institution has information that is highly confidential*. Even though the respondents said that their e-learning institution is highly secure, they did agree that their institution is prone to threat. 60.4% of respondents agree that information in e-learning is highly confidential, therefore needs to be secured. The respondents also suggested that their institution spends a lot on security control implementation and also for security solutions and recovery. The small differences in percentage for statements *S4* and *S5* showed that even though the institution has spent a lot on security control, they still have to spend a lot more for the security solution and recovery after the attack incident. This might be because the security control implemented is insufficient.

5.1.3.3 Users' Perception on the Impact of Threat to E-learning

The respondents were asked for their opinion on the impact of threats to their e-learning institution. I1: My e-learning institution would face significant business disruption; if the information is not available and I2: My e-learning institution would face significant business disruption, if the information is corrupted. 75% of respondents agreed that their e-learning would face significant business disruption if the information is not available to the users. 70.8% of respondents agreed that their e-learning institution would face significant business disruption if the information is corrupted. Figure 5-3 depicted the users' perception on the impact of threats to e-learning.

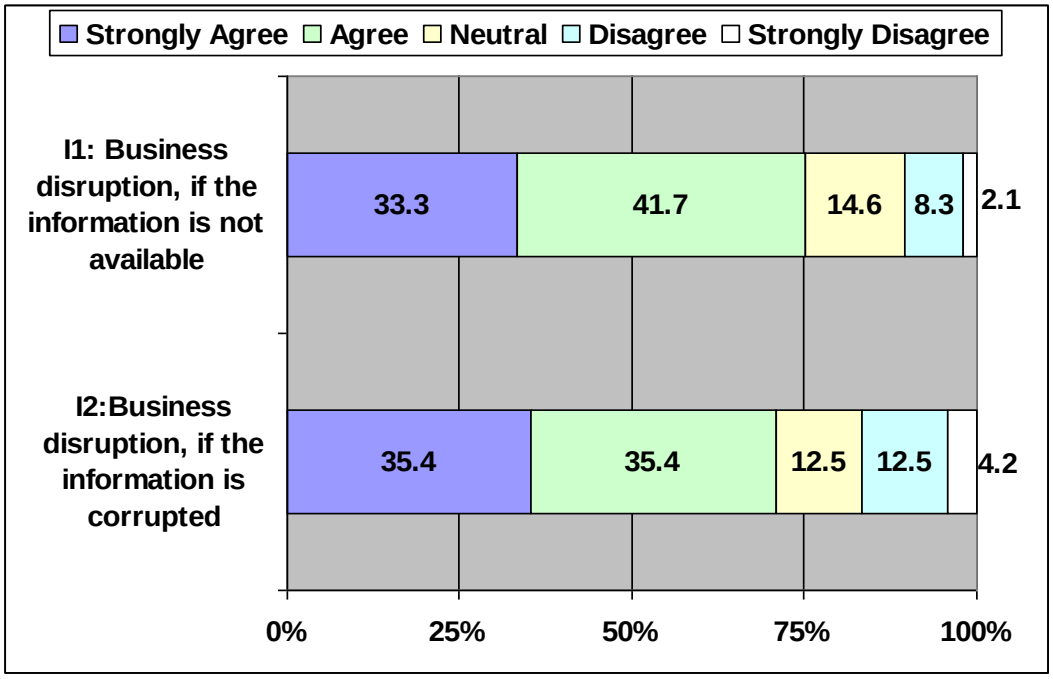


Figure 5-3 Users' Perception on the Impact of Threat to E-learning

5.1.3.4 Users' Perception on the Importance of Good Security Management in E-learning

The data collected reveals that 83% of respondents agreed that G2: Good security management practices are important in ensuring a high level of security awareness amongst staff and students. Meanwhile 90% of respondents agreed that G1: Good security management is important in ensuring the successful implementation of appropriate security controls. Figure 5-4 shows the details.

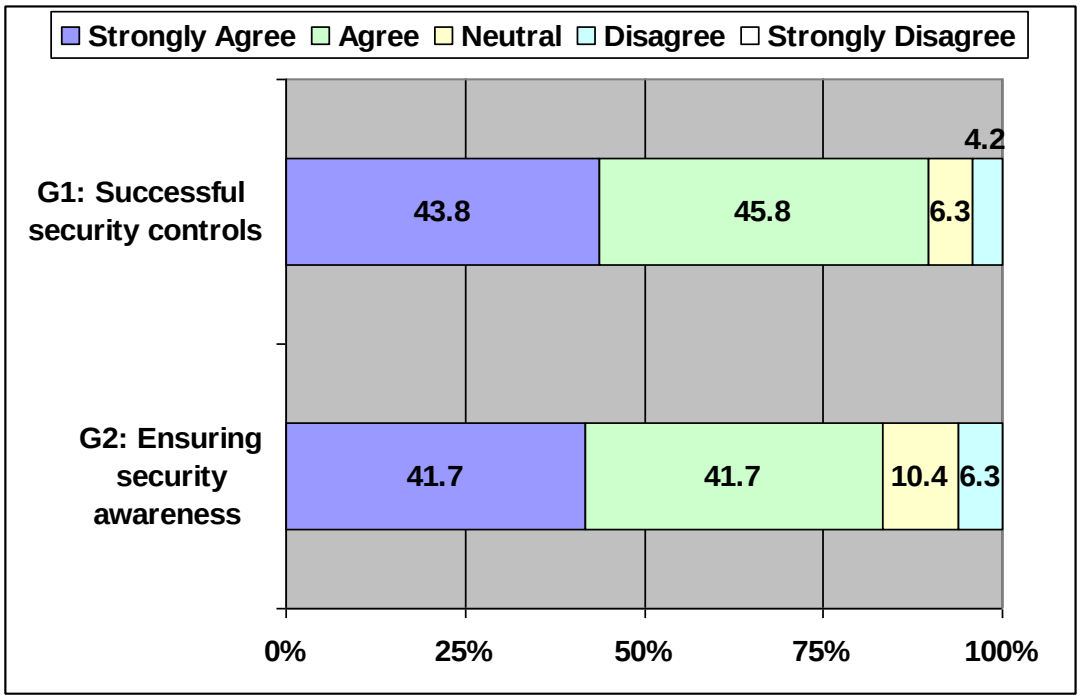


Figure 5-4 Users' Opinion on Important of Good Security Management

5.1.3.5 Threats Rank in E-learning

Respondents had ranked the list of threats given to them according to their perception of which will cause most damage to their e-learning Institution. The result can be seen as Table 5-3.

The threats were categorised into three categories, namely intentional threats, unintentional threats and physical threats. The first eleven threats are from both the intentional and unintentional threat categories. The physical threats were ranked at the bottom, as they are not specific to the e-learning environment.

Table 5-3 Threats Rank In E-learning

Ranking	Threats	Type of Threats
1	Virus and Worm	Intentional Threats
2	User/Operator Error	Unintentional Threats
3	Spamming	Intentional Threats
4	Equipment Malfunction	Unintentional Threats
5	Spoofing and Masquerade	Intentional Threats
6	Software Malfunction	Unintentional Threats
7	Digital Snooping and Shoulder Surfing	Intentional Threats
8	Sequential and Dictionary Scanning	Intentional Threats
9	Trap Door (back door)	Unintentional Threats
10	Tunnelling	Intentional Threats
11	Scavenging (Dumpster Diving / Browsing)	Intentional Threats
11	Power loss	Physical Threats
12	Water damage	Physical Threats
13	Fire damage	Physical Threats
14	Natural disaster	Physical Threats

5.1.3.6 The Relationship between the E-Learning Entity (Users, Institution Categories, Level of Information Security Awareness) and Information Security Threats

The data were analysed using cross-tabulation (crosstab) to find the relationship between the users' roles and their perception of security, the relationship between the type of institution and perceptions of security and the relationship of security awareness level among users and their perception of security. A rating average was calculated to identify the respondent's tendency towards choice of answer; the rating average is the weighted average per

column and row. Table 2 shows the result of the crosstab analysis of questions on security in e-learning and user roles, type of institution and level of awareness. Here, the first rating scale choice was valued at 1 (Strongly Disagree), the second at 2 (Disagree), the third at 3 (Neutral), the fourth at 4 (Agree) and the fifth at 5 (Strongly Agree). A response rating of, for example, 3.60 meant that the response fell to the right of neutral and closer to the agree rating. Respondents were asked to state their agreement with the following statements:

Q1: The e-learning environment is prone to information security threats.

Q2: My e-learning institution is highly secured.

Q3: My e-learning institution has information that is highly confidential.

Q4: My e-learning institution would face significant business disruption if the information were corrupted.

Q5: My e-learning institution would face significant business disruption if the information were not available.

Q6: My e-learning institution spends a lot on security controls.

Q7: My e-learning institution spends a lot on security solutions and recovery.

The data in Table 5-4 showed that all responses ranged from Neutral towards Strongly Agree with regard to security in e-learning. This demonstrated that the respondents agreed that e-learning is prone to threats, even though they perceived that their own e-learning institution was highly secure. Similar opinions were held with regard to the subsequent questions. The data also reflects that there were no significant difference in perceptions of security depending on each user's role, type of institution and level of security awareness.

Table 5-4 Crosstab on Perception of Information Security Threats in E-Learning Based on Users' Roles, Type of Institution and Level of Awareness

	Role				**Type of Institution**			**Level of Awareness**	
	Management	Education	IT	Others	Higher Education	Further Education	Training	Higher	Medium
Q1	3.80	3.00	4.67	3.11	3.17	3.75	3.60	3.27	3.35
Q2	3.90	3.82	4.33	3.67	3.77	4.00	3.80	3.50	4.08
Q3	4.30	3.24	4.67	3.50	3.63	3.38	4.20	3.41	3.85
Q4	4.00	4.00	3.67	3.67	3.86	3.75	4.00	3.73	3.96
Q5	4.20	4.06	3.67	3.78	4.06	3.38	4.20	3.91	4.00
Q6	3.40	3.47	4.00	3.61	3.54	3.38	3.80	3.32	3.73
Q7	3.60	3.29	4.33	3.44	3.49	3.13	4.00	3.32	3.62

In Table 5-5, the results were cross-tabbed to look at respondents from different users' role groups- management, educator, IT personnel and other. Each group was divided to reflect differing levels of security awareness- high, medium and low. None of the respondents claimed that they have low level awareness therefore the table only shows two levels of awareness – high and medium. Data showed that all responses ranged from Neutral towards Strongly Agree, however the level of awareness does not reflect any significant relationship with their perception towards the security questions. People with a high level of awareness should have a higher awareness regarding how e-learning is prone to information security threats but not all groups of the average rating data in the Table 5-5 reflect that.

Table 5-5 Crosstab of User Types with Different Levels of Awareness of Perceptions of Information Security in E-Learning

Awareness / Security questions	Role within the institution							
	Management (10)		Educator (17)		IT Personnel (3)		Other (18)	
	Higher (5)	Medium (5)	Higher (10)	Medium (7)	Higher (2)	Medium (1)	Higher (9)	Medium (9)
Q1: E-learning environment is prone to information security threats								
	4.40	3.20	2.70	3.43	4.50	5.00	3.22	3.00
Q2: My e-learning institution is highly secured								
	4.00	3.80	3.90	3.71	5.00	3.00	4.11	3.22
Q3: My e-learning institution has information that is highly confidential								
	4.40	4.20	3.50	2.86	4.50	5.00	3.78	3.22
Q4: My e-learning institution would face significant business disruption if the information was corrupted								
	4.00	4.00	4.20	3.71	3.50	4.00	3.78	3.56
Q5: My e-learning institution would face significant business disruption if the information was not available								
	4.00	4.40	4.20	3.86	3.50	4.00	3.89	3.67
Q6: My e-learning institution spends a lot on security controls								
	3.40	3.40	3.60	3.29	4.50	3.00	3.89	3.33
Q7: My e-learning institution spends a lot on security solutions and recovery								
	3.40	3.80	3.50	3.00	4.50	4.00	3.67	3.22

Table 5-6 shows the crosstab results of user types with different levels of awareness with regards to their concerns about issues and challenges in e-learning institutions. Here, the first rating scale choice was valued at 1 (Not a Concern), the second at 2 (Minimal Concern), the third at 3 (Some Concern), the fourth at 4 (Concern) and the fifth at 5 (Extremely Concerned). The data showed that the users are concerned about the issues and challenges in e-learning institutions and their level of concern ranges from minimal to extremely concerned. However the higher level of awareness does not necessarily show

that they are more concerned than the medium level of awareness. Therefore the level of awareness does not show significant relationship with the level of concern.

Table 5-6 Crosstab of User Types with Different Awareness Level on Issues and Challenges in E-Learning Institutions

Awareness / Issues & Challenges	Role within the institution							
	Management (10)		Educator (17)		IT Personnel (3)		Other (18)	
	Higher (5)	Medium (5)	Higher (10)	Medium (7)	Higher (2)	Medium (1)	Higher (9)	Medium (9)
Malicious code infection (viruses, Trojan horse, worms)								
	3.60	3.20	3.60	3.43	4.50	4.00	3.22	3.11
Loss of privacy / confidentiality (abuse or misuse of data)								
	3.80	4.20	4.20	3.29	5.00	5.00	3.67	3.89
Electronic exploits/tools (cracking, eavesdropping, spoofing)								
	3.40	3.20	3.30	3.00	4.50	5.00	3.22	3.44
System unavailability (Denial of Service (DOS), natural disasters, power interruptions, bugs)								
	3.40	4.00	4.10	3.71	5.00	3.00	3.22	3.67
Employee misconduct involving information systems								
	2.80	2.00	3.40	2.71	4.50	2.00	2.67	3.11
Spam								
	2.40	2.60	4.00	2.57	4.00	2.00	3.22	3.67
Misconduct involving third parties with access to information systems								
	2.60	2.80	3.30	3.00	4.50	2.00	2.78	3.33
Theft of proprietary information								
	2.60	2.40	3.50	2.43	5.00	3.00	3.11	3.44

Table 5-7 shows the crosstab of users' perceptions of the most disruptive incidents within the e-learning environment. Here the first rating scale choice was valued at 1 (Unknown), the second at 2 (Insignificant), the third at 3 (Very

Minor), the fourth at 4 (Minor) and the fifth at 5 (Major) and the sixth (Very Major). All of the answers were in the range Unknown to Very Minor; this could be because respondents were unaware of such incidents or because the information had been kept confidential.

Table 5-7 Crosstab of Users' Perceptions of the Most Disruptive Incidents within the E-Learning Environment

Awareness / Incidents	Role within the institution							
	Management (10)		Educator (17)		IT Personnel (3)		Other (18)	
	High (5)	Medium (5)	High (10)	Medium (7)	High (2)	Medium (1)	High (9)	Medium (9)
Installation / use of unauthorised software								
	2.20	1.60	2.20	2.43	2.50	2.00	2.22	2.00
Use of institution computing resources for illegal or illicit communications or activities (porn surfing, e-mail harassment)								
	1.80	2.00	2.00	2.86	2.50	2.00	2.56	1.67
Abuse of computer access controls								
	2.00	1.80	1.90	2.14	2.50	2.00	2.22	2.56
Unauthorised access by outsiders								
	1.60	1.20	2.30	1.57	2.50	4.00	1.67	2.11
Physical theft, sabotage or intentional destruction of computing equipment								
	2.00	2.40	2.20	2.29	2.50	4.00	2.11	2.56
Electronic theft, sabotage or intentional destruction / disclosure of proprietary data or information								
	1.60	1.20	2.10	1.86	2.50	2.00	2.22	1.33
Virus infections or disruptive software								
	2.20	2.20	2.40	2.71	2.50	3.00	2.00	1.33
Denial of service								
	3.20	1.40	2.50	1.71	2.50	2.00	2.44	2.56
System failure or data corruption								
	2.40	3.60	3.60	2.71	3.00	2.00	1.89	2.44

User responses on their perceptions of financial losses caused by security incidents in the e-learning environment are shown in Table 5-8. Most respondents chose Unknown, as per the rating scale, whether they were of higher awareness or medium awareness.

Table 5-8 Crosstab of Users' Responses on the Financial Impact Caused by Security Incidents

Awareness / Financial Impact	Role within the institution									
	Management (10)		Educator (17)		IT Personnel (3)		Other (18)		Response	
	High (5)	Medium (5)	High (10)	Medium (7)	High (2)	Medium (1)	High (9)	Medium (9)	High (%)	Medium (%)
Nothing	3	1	2	1	0	0	1	2	23.1	18.2
Less than £1,000	1	0	0	0	0	0	0	1	3.8	4.5
Between £1,000-£10,000	0	0	0	1	0	0	1	0	3.8	4.5
Between £10,001-£50,000	0	0	0	0	0	0	0	0	0.0	0.0
More than £50,000	0	1	0	0	0	0	0	0	0.0	4.5
Insignificant	0	0	1	0	0	1	1	0	7.7	4.5
Unknown	1	3	7	5	2	0	6	6	61.5	63.6

5.1.4 Key Findings of Study 1

1. This study has found that users are aware that e-learning is prone to the information threats on the Internet. In addition users are also aware of the information security threats in e-learning institutions. However, the majority of the users claimed that their e-learning institutions are highly secure and agreed that the information in e-learning institutions is highly

confidential. This answer is in contrast with the earlier claim which agreed that e-learning is prone to the threats. This perception is due to respondents being unable to access the security information and incidents in an e-learning environment.

2. This study has found that the users are aware of the impact if the institutions were attacked by the information security threats. The institution would face significant business disruption if the information is corrupted or not available. The main long term impact because of this disruption would be the reduced number of students' enrolment, high number of complaints received and also adverse media coverage.

3. Despite spending a lot to control the threats, the institutions also spend a lot in the recovery process. This is likely due to the imbalance countermeasure implementation between the technological solution and the management of an information security solution.

4. Based on this study, users agreed that the implementation of good security management is important to ensure the successful implementation of appropriate security controls. Good security management should make the users at every level aware of what needs to be done to avoid vulnerability and attack.

5. In designing the model or guideline for information security management, the e-learning threats should be defined. The list of threats for e-learning can help in guiding the development of a suitable model for e-learning. This study has found that the users perceive that the two highest threats are viruses and the errors made by the users. These threats can be reduced by the implementation of security management, for example by providing the users' awareness policy and procedures.

6. The study showed there is no significant relationship between the e-learning entity (users, institution categories, and level of information security awareness) and information security threats; the data has

reflected that all users have similar perceptions of security within e-learning. Whatever roles that they are playing, most of the users agreed that e-learning is exposed to information security threats.

7. Information security management requires participation by all users in the organisation. Based on the survey conducted, it can be concluded that users are not participating fully and not aware of the security situation. Therefore as part of information security management, effective security awareness programs need to be implemented. These programs can help to increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems.

8. Empirical data has indicated that different users have similar perceptions of e-learning security; hence users could share a similar model. This combination of information security management and current information security technology could provide better results in terms of successful security implementation.

5.2 Study 2-Threats Analysis

5.2.1 Purpose

This study has developed into a lengthy task and taken a great deal of time. The purpose of this study was to investigate and define the information security threats within an e-learning environment. This study focused on vulnerabilities in relation to the application system and did not cover the vulnerabilities in terms of the host and networks in e-learning. This study identifies the information security threats specific to applications in e-learning environment.

The main aim of this threats analysis was to identify threats and understand how threats occur. Literature shows that research in security is focussed mainly on three areas: policy, identity (referring to access management), and

intellectual property. See Table 5-9 for details of some authors and the year of paper published.

Table 5-9 E-Learning Security Research Area

No.	Research Area	Author and Year
1.	Policy	(Yang et al., 2002); (El-Khatib et al., 2003); (Boella and van der Torre, 2006).
2.	Identity	(El-Khatib et al., 2003); (Bruns et al., 2003); (Saxena, 2004); (Raitman et al., 2005); (Lim and Jin, 2006); (Yong, 2007); (Jalal and Zeb, 2008).
3.	Intellectual property	Graf, 2002; (Kennedy, 2002); (Samuels, 2004).

All of the above studies propose solutions and countermeasures to effectively overcome the threats and attacks in the e-learning environment. Siponen (2009) proposes to have a standard which is specific to certain organisations: a standard can comprise a model or framework consisting of the process and procedures for managing information security. However, in order to produce such a standard, the organisation should initially identify the vulnerabilities and threats to their organisation. Hence this study conducted a threats analysis for e-learning using a threat analysis model.

5.2.2 Methods

This study conducted a threats analysis to identify the sources, types, likelihood and risk of threats involved. It can be defined as a process concerned with the detection, identification and evaluation of vulnerabilities of an operation or system.

A threats analysis model was used by simplifying Improving Web Application Security (IWAS). IWAS is an approach for web application, thus its threat analysis modelling approach is appropriate for this study because e-learning

also uses web applications (Triacca et al., 2004). As the threats analysis is a similar process to risk analysis but with more specific identification of threats, the commonly implemented steps of risk analysis (Weippl, (2005b) have been used in this threats analysis model.

5.2.3 Results

The model consists of five steps as shown in Figure 5-5.

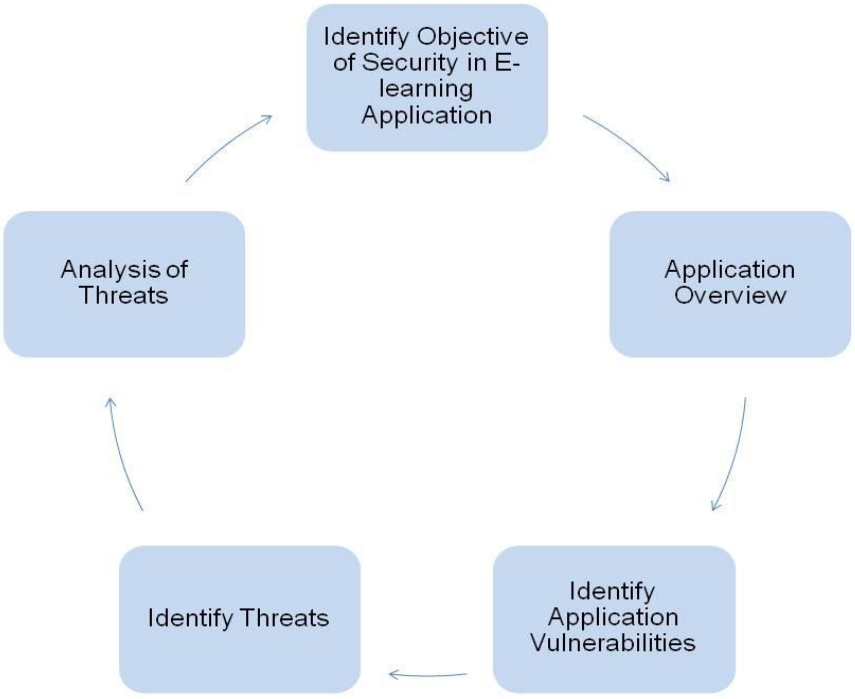


Figure 5-5 Threat Analysis Model

5.2.3.1 Step 1 — Identify security objectives

The threats analysis begins by identifying the objectives of security in e-learning applications. The main elements of security are confidentiality, integrity and availability.

5.2.3.2 Step 2 — Application overview:

In this step, the commonly used applications in the e-learning environment were identified. The applications are listed in Table 5-10. The actors and roles involved in each application are also elaborated in this step. The actors (Khan, 2004) are further divided into two groups, which are registered and unregistered users as in Table 5-11 Actors & Roles. Then, the vulnerabilities for each application were assessed by identifying the application and the users' roles.

Table 5-10 Applications in E-learning

Application	Sub Application
❖ Virtual Learning Environment (VLE):	
• Online Course Administration	✓ Course Listing, ✓ Grading Centre, ✓ Performance Monitoring
• Course Management	✓ Delivering Learning Content, ✓ Delivering Assignment ✓ Collecting Assignment
• Communication tools	✓ Online Session, ✓ Discussion Board, Email, ✓ Personal Portfolio, ✓ File Storage, ✓ File Exchange, ✓ Project Collaboration & Sharing, ✓ Assessment Tool, ✓ Survey Tool ✓ Other.
❖ Registration	
❖ Finance	
❖ Student Administration	
❖ Certification	
❖ Mobile Learning	
❖ Virtual Library	

Table 5-11 Actors & Roles

Actors	Code	Roles
Register user		
Delivery coordinator	DC	Coordinates the implementation of e-learning courses and resources
(System)Administrator	AD	Administrator VLE server, user accounts and network security
Online Course Coordinator	CC	Coordinates the instructional and support staff for online courses
Course manager, Educators or instructors or facilitators	ED	Manage the content and event for students, Teaches online courses
Discussion Facilitator or moderator	DF	Moderates and facilitates online discussions.
Students	ST	'study' the content uploaded and participate and interact in the event
Stake holder or top management	TM	Monitor and assess the course managers (educators) and students' progress. Plan for the future of the organisation
Unregistered user		
Guest or visitor	GU	Browse the website to get information about the organisations. Potential students (unregistered students – first time to register)
Sponsor	SP	Browse the website and View Students Registration.

5.2.3.3 Step 3 — Identify Application Vulnerabilities

In this step the security vulnerabilities for each application within the e-learning environment were identified. The key use and important features have been outlined according to the roles of each actor. Essentially, each actor was

allowed to create, view, update and delete based on the roles and the level of privilege given. The technology used for each application in e-learning was identified and the application vulnerabilities as seen Table 2-1 in Chapter 2, (page 21) were assigned to the applications. The results listed as a table entitled Application Overview and is in Appendix B.

5.2.3.4 Step 4 — Identify Threats

The details of threats were characterised in this step. The possible attacks were defined with regard to whether or not they could be considered intentional threats or unintentional threats. These attacks are also classified in terms of whether or not they will provide the effect of fabrication, modification, interruption or interception to the information. The output of this step was summarised as seen in Figure 5-6 Threats per Application in E-Learning. This figure displayed the potential information security threats for each application of e-learning.

5.2.3.5 Step 5 — Analysis of Threats

Threats were analysed by evaluating the threat's risk. The risk of each threat was quantified by assigning the likelihood of occurrence and impact upon the individual or system. The risk evaluation used a risk evaluation grid proposed by Barbeau (2005), as displayed in Table 5-12.

Table 5-12 Risk Evaluation Grid

		Rationale		
Risk Criteria	Cases	Difficulty (to attack)	Motivation (to attack)	Rank
Likelihood of Occurrence	Unlikely	Strong	Low	1
	Possible	Solvable	Reasonable	2
	Likely	None	High	3
Impact Level		User	System	
	Low	Annoyance	Very Limited Outages	1
	Medium	Loss Of Service	Limited Outages	2
	High	Long Time Loss Of Service	Long Time Outages	3
Risk Classification	Minor	No Need For Countermeasures		1,2
	Major	Threats Need To Be Handled		3,4
	Critical	High Priority		6,9

Source: Barbeau, (2005)

			Applications in e-learning																					
			VLE																					
			Online Course admin			Course Management		Communication Tools																
No	Vulnerabilities Category	Threats	Course Listing	Grading Centre	Performance Monitoring	Deliver Learning Content	Deliver Assignment & Collect Assignment	Online Session	Discussion Board	Email	Personal Portfolio	File Storage	File Exchange	Project Collaboration & Sharing	Assessment Tool	Survey Tool	Other	Registration	Finance	Students Administration	Certification	Mobile Learning	Virtual Library
1	Input & Data Validation	Buffer Overflow	√	√		√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√
2	Authentication	Network Eavesdropping	√	√	√	√	√	√	√	√	√	√			√	√	√	√	√	√	√	√	√
		Password Guessing	√	√	√	√	√	√	√	√	√	√			√	√	√	√	√	√	√	√	√
		Cookie Replay	√	√	√	√	√	√	√			√						√					
		Credential Theft	√	√	√	√	√	√	√			√						√					
3	Authorisation	Elevation of Privilege	√	√	√	√	√																
		Unauthorised Access						√	√	√	√	√			√	√	√	√	√	√	√	√	√
4	Configuration Management	Unauthorised access to administration interfaces and configuration stores	√	√		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
5	Exception Management	Trap Door	√	√	√	√	√				√	√	√	√				√					
		Spamming	√		√	√	√		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
6	Sensitive Data	Tunnelling	√	√	√		√																
		Software Malfunction	√	√	√		√																
		Network Eavesdropping									√	√	√	√						√	√	√	√
7	Session Management	Session Replay						√	√	√			√	√	√	√	√		√				√
		Man in the Middle						√	√				√	√	√								
8	Cryptography	User Error						√	√	√			√	√	√	√	√		√				√
9	Parameter Manipulation	Http Manipulation						√	√	√	√				√	√	√		√	√	√	√	√
		Cookie Manipulation					√	√	√	√	√				√	√	√		√	√	√	√	√
10	Auditing & Logging	User Masquerade						√	√	√	√	√			√	√	√	√	√	√	√	√	√
		Malicious Code	√	√	√	√	√																

Figure 5-6 Threats per Application in E-Learning

Based on the results gathered, concerning information security threats in e-learning, the risk of threats was calculated considering the likelihood of occurrence and the subsequent impact level of each threat. The formula used to calculate the risk is as follows:

Likelihood x Impact Level= Risk

Risks deriving from threat analysis are classified into three main groups, namely minor, major and critical. The summary of the results of the threats analysis has been converted into the e-learning threats' risk matrix, as depicted in Figure 5-7. The matrix highlighting the vulnerabilities or threat versus the application exhibited three meaningful risk groups, which are minor, major and critical. Appendix C exhibits the category of risk.

The result of the threats analysis reveals the potential threats according to the applications in e-learning. 21 applications, including the sub-applications have been identified; in addition, 18 types of threats were listed. The methods of attack were classified according to intentional or unintentional. As an example, a threat, such as buffer overflow, can occur as being both an intentional or unintentional attack: it could be intentional due to extra data containing malicious code, or could be unintentional due to programming errors. This study elaborated the potential impact of an attack upon e-learning. The impacts have been subsequently categorised as interruption, interception, modification and fabrication. The detail result of threats analysis by sub application (step 4 and 5) can be found in Appendix D.

Legend	
CR	Critical
MA	Major
MI	Minor
	Not Relevant

No.	Vulnerabilities Category	Threats	Applications in e-learning																					
			VLE																					
			Online Course admin			*Course Management*		*Communication Tools*																
			Course Listing	Grading Centre	Performance Monitoring	Deliver Learning Content	Deliver Assignment & Collect Assignment	Online Session	Discussion Board	Email	Personal Portfolio	File Storage	File Exchange	Project Collaboration & Sharing	Assessment Tool	Survey Tool	Other	Registration	Finance	Students Administration	Certification	Mobile Learning	Virtual Library
1	Input & Data Validation	Buffer Overflow	MI	MA		MA	MA	MI	MI	MA	MI	MA		MA	CR	MA	MA	CR	MA	MA	MA	MA	MI
2	Authentication	Network Eavesdropping	MI	CR	MI	MI	MA	MI	MI	MA	MA	MA			CR	MI	MA	CR	MA	MI	CR	MA	MI
		Password Guessing	MI	MA	MI	MA	MA	MI	MA	MA	MA	MA			CR	MI	MA	MA	MA	MI	CR	MA	MI
		Cookie Replay	MI	MA	MI	MI	MA	MI	MI			MI						MA					
		Credential Theft	MI	MI	MI	MA	MA	MI	MI			MA						CR					
3	Authorisation	Elevation of Privilege	MA	CR	MA	MA	CR																
		Unauthorised Access						MA	MA	MA	MA	CR			CR	MI	MA	CR	CR	MA	CR	MA	MI
4	Configuration Management	Unauthorised access to administration interfaces and configuration stores	MI	CR		MA	MA	MA	MA	MA	MA	MA	MA	MA	CR	MI	MA	CR	CR	MA	CR	MA	MI
5	Exception Management	Trap Door	MI	MA	MI	MI	MA				CR	MA	MI	MI				MA					
		Spamming	MI		MI	MI	CR		MI	MA	MI	MA	MI	MI	CR	MI	MI	CR	MA	MI	MA	MA	MA
6	Sensitive Data	Tunnelling	MA	CR	MA		MA																
		Software Malfunction	MA	CR	MA		MI																
		Network Eavesdropping									MA	MA	MA	MI						MA	CR	MA	MA
7	Session Management	Session Replay						MI	MI	MI			MI	MI	CR	MI	MI		CR				CR
		Man in the Middle						MI	MI				MI	MI	CR								
8	Cryptography	User Error						MI	MI	MI			MI	MA	CR	MI	MI		CR				MA
9	Parameter Manipulation	Http Manipulation						MI	MI	MI	MI				CR	MI	MI		CR	MI	MA	MA	MI
		Cookie Manipulation					CR	MI	MI	MI	MI				CR	MI	MI		CR	MI	MA	MA	MI
10	Auditing & Logging	User Masquerade						MA	MI	MI	MA	MI			CR	MI	MA	CR	CR	MI	CR	MI	MI
		Malicious Code	MI	MI	MA	MA	MA																

Figure 5-7 E-learning Threats' Risk Matrix

5.2.4 Validation

The study had been validated to confirm the accuracy and reliability of the results. The validation focused on two key areas: i) the e-learning application, and ii) the information security threats associated with the relevant e-learning application. The e-learning application validation was conducted following the completion of Step 2, with the latter conducted upon the completion of Step 5 of the threats analysis.

The validation of e-learning applications was conducted using a website survey on the Blackboard website (http://www.blackboard.com.). Blackboard is known as one of the leading Learning Management Systems (LMS). A comparison was carried out according to the applications in the Blackboard LMS. As a result, some changes were made to the terms used to describe the applications within the e-learning environment. Information security threats associated with the e-learning applications were validated by a subject matter expert, an Information Security specialist from the IT Department of Cranfield University. According to the validation result, the listed threats are correct. Furthermore, based on the comments and suggestions provided by the subject matter expert, a few changes were to be made to the risk assigned to each application.

5.2.5 Key Findings of Study 2

The common threats for most applications are spamming, unauthorised access to administration interfaces and configuration stores, buffer overflow, network eavesdropping, and password guessing. The most critical application is the assessment tool, as it is exposed to 12 listed threats.

The vulnerabilities and threats categorised as critical risk need to be immediately addressed, owing to the impact upon the user and system being severe and having the potential to lead to business discontinuity. The major risk group also needs to be addressed, despite it not being considered as quite as high profile as the critical risk group. Moreover, some additional threats fall into the minor risk group, which reflects the fact that the likelihood of such a threat to occur is low with a corresponding low impact. However, this area nevertheless

requires addressing since there is still the potential of the minor threat consequently leading to a critical threat.

At the end of this study, the results of threats analysis, specifically the list of threats has contributed in proposing the appropriate countermeasures. The general countermeasures from the journal, security books and websites were reviewed and selected to be assigned to the threats according to the vulnerabilities categories. The result is tabled in the Appendix E as the E-Learning Countermeasure Table. The table is the proposed countermeasure which is meant specifically for the e-learning environment.

Research Implications

1. This study has revealed the potential threats according to the applications used in e-learning.

2. The different type of risk associated with each of these threat categories derived from this study will ultimately help the supply group in prioritising which threats need more attention. On the other hand, the demand groups can use the matrix as guidance to protect themselves from threats.

3. The threats analysis conducted can ultimately act as a guide in preparing the security strategies and countermeasures. This finding had led to the proposal of countermeasures to the potential threats in e-learning.

4. This study has provided knowledge of the situation and possible threats to e-learning. It has provided insight into the fact that threats should be one of the components that need to be considered in the ISM model.

5. This study also has detailed the roles and responsibilities of actors in the security issue for each application in e-learning. However the question is, how to address their roles and behaviour in the model. This question has steered to Study 5 and 6 - a social technical approach on the cultural view of users.

5.3 Study 3- Incident Logging

5.3.1 Purpose

This study is conducted as a result of the preceding Study 1, in order to explore the incidence of security attacks in an e-learning environment. In Study 1, information about the attacks could not be gathered from the survey due to the limited information concerning security matters. The main aim of this study is to find examples of information security incidents in e-learning.

5.3.2 Methods

This study adopted a qualitative research method and presents the qualitative data results in the form of numbers.

Information about security incidents has been gathered by searching journal articles, conferences paper, security report/website, FACTIVA database (Dow Jones service covering over 10,000 global press sources), DataLoss DB (data loss database by Open Security Foundation) and theses. In addition to this, white papers newsletters, technology and security related bulletins were subscribed to and reviewed. Both sent the latest news via emails. Listed below are the bulletin and white papers reviewed:

Bulletin

- ICT In Further & Higher Education
- IT Security In Edu
- IT Event

White paper

- Computer Weekly.Com
- Find White Papers
- Techtarget
- Webroot

In this study, data gathered were then reviewed and filtered out to report security incidents in e-learning. Data has been filtered by keyword choice using sector = education, and subsector = university has been chosen.

A systematic search using keywords was performed of published worldwide literatures spanning from 2000-2009. This is the most significant time-span as e-learning and security starts to be acknowledged in the research area from 2000 and this study was conducted in 2009.

Analysis was carried out on these collected incidents in order to determine the most common threats in e-learning and the frequency of occurrence from 2004 until 2009. Keywords like web, server, and electronic were then used to define whether the incidents that occurred in the education sector are under e-learning environments. Graphs were created to represent the results of data collected and its analysis in this study.

Among the published source, DataLoss DB have shown many useful data regarding the security incidents in e-services (Cobos, 2009). Cobos (2009) has used the DataLoss DB as primary data for her data collection and analysis in her research on security incidents in e-services. It is important to highlight that DataLoss DB might have some current changes or update in the database. This study is reporting on the data that have been compiled in 2009, any current changes and update from the DataLoss DB was not included. Her research finding on e-learning has validated the results of this study.

5.3.3 Results and Discussion

Cobos (2009) claimed that e-learning is exposed to threats similar to other e-services. However the search result revealed that there were not many reported incidents for e-learning from sources other than DataLoss DB. All the data used in this analysis process were mostly extracted from the DataLoss DB. In addition, only two incidents were published, one in a journal and the other is reported in a thesis. Both incidents are listed in Table 5-13.

Table 5-13: Security Incident in E-Learning

Threat	Date	Impact	Organisation	Source
Denial of services	late 2002	Shut down the server hosting the e-learning system application	Knowledgeville University in Southeastern US	Journal of Cases on Information Technology, 8(4) 2006
Security system policy violation (internal/external)	Sep 2007	Personal information and social security numbers exposed	Tennessee Tech University (US)	MSc Thesis *Information Security Incidents In E-Services, 2009*

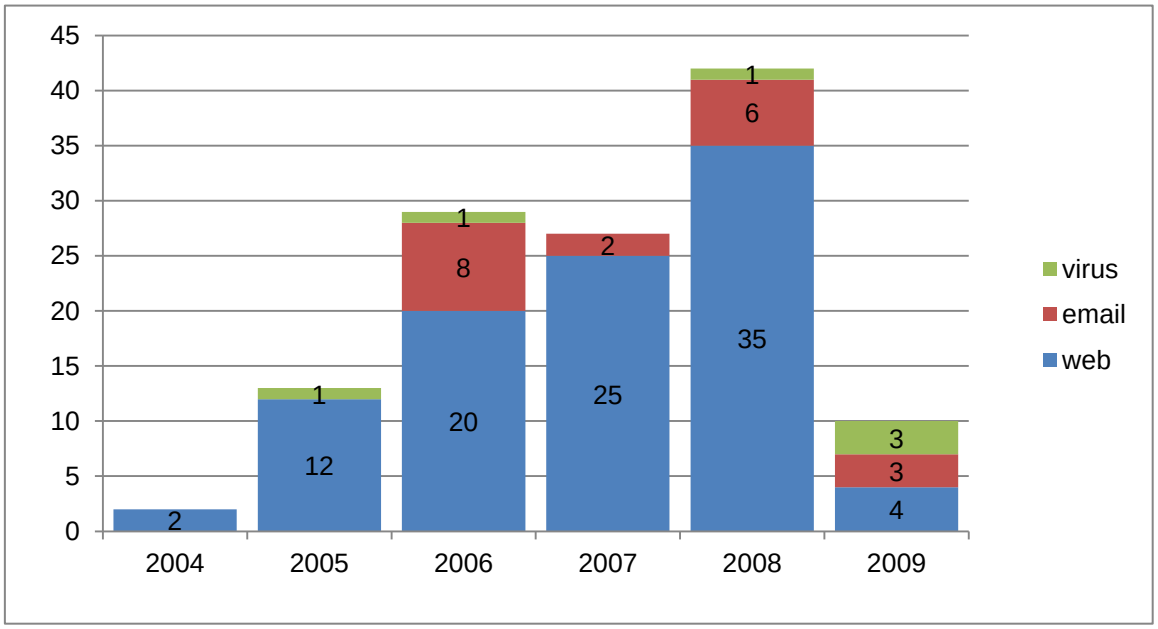


Figure 5-8 Breach Type of Incident by Year

The result of data gathering and analysis from DataLoss DB showed there were incidents which occurred every year starting in 2004 until 2009. The extracted data from DataLoss DB are listed in Appendix F. According to the data, the attacks were from three types of breach namely via web, email and virus. Figure 5-8 displayed the total of information security incidents for each year. The graph includes details with a stacked bar showing the breach type of incident by year.

The graph indicates breaches via the web that have been the common way of attack within those six years.

Analysis of this data also revealed that the incidents of attack were from four sources of threats: inside accidental, inside, outside and unknown. Referring to Figure 2-2 Source of Security Threats in Chapter 2, inside accidental falls under the non-malicious category, while inside and outside are under malicious categories. The non-malicious category is related by ignorant employees who are untrained in computers and are unaware of security threats and vulnerabilities.

Figure 5-9 displayed the source of threats that made the attack by year. The graph indicates that the inside accidental threats have been the most common source of threats/attack for this time except 2007 and in 2009 this threat share the same number with the outside threats. The inside accidental source incidents could be errors or unintentional actions of the organisation's employees revealing personal data of the users. Sometimes it occurs when the employees pick up malware while browsing, and this is later used by an external attacker to gain unauthorised access (Cobos, 2009).

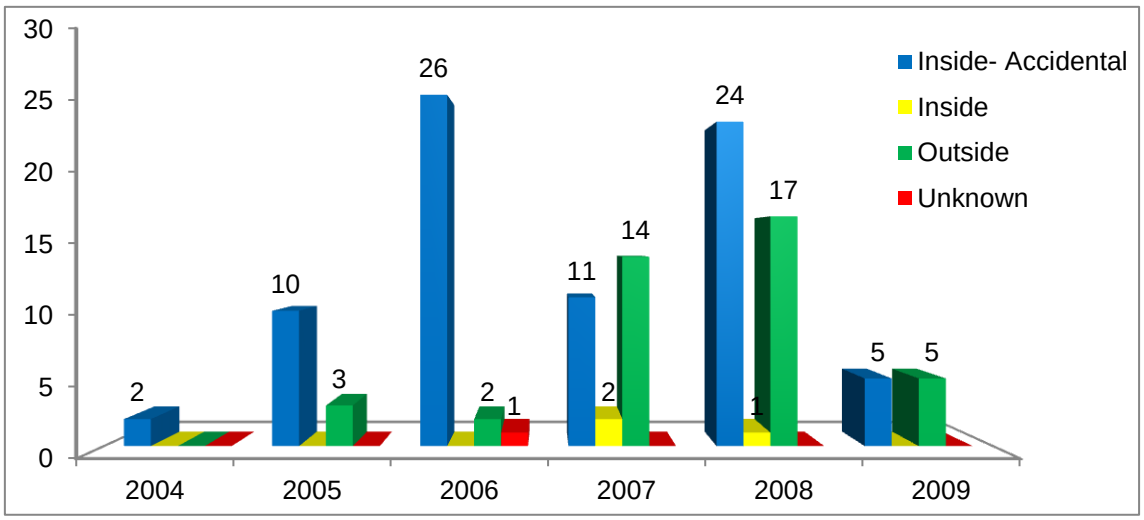


Figure 5-9 Source of Threat of Incidents by Years

The Figure 5-10 cross-analysed the result depicted in Figure 5-8 and Figure 5-9. This figure shows that the inside accidental is the most common source of threat from 2004 until 2009. The web was found to be the most type of breach for inside accidental incident.

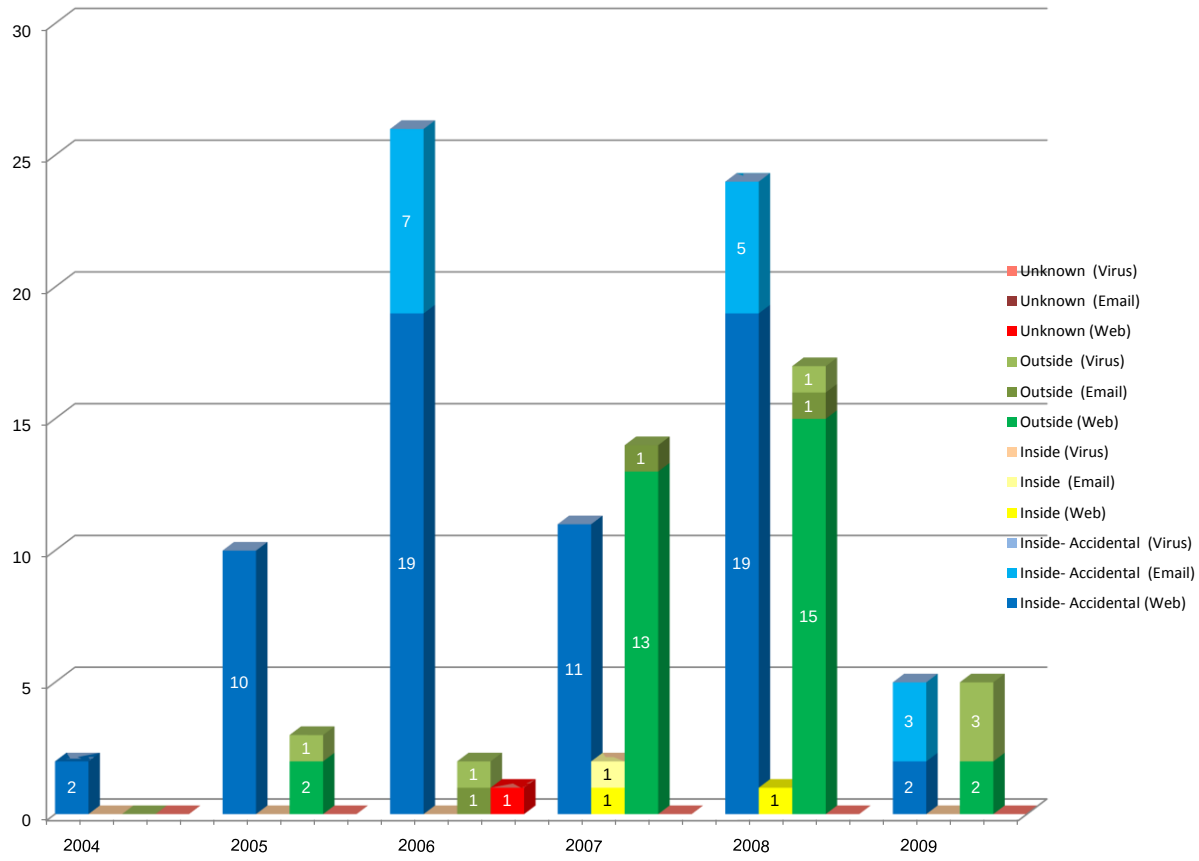


Figure 5-10 Details of Incidents -Source Threats (Breach Type) 2004-2009

Based on the result presented above, the majority of data breaches originated from non-malicious people, who are within organisations who inadvertently cause the threats (internal attacks), for instance downloading a file that deems unsafe which have malware attached.

5.3.4 Key Findings of Study 3

1. Data collected has confirmed that there are incidents of attack to e-learning.
2. The majority of incidents which occurred in the e-learning environment are due to internal security breaches and the majority are due to the non-malicious or unintentional activity by users of e-learning.
3. This has provided an insight into the internal users in an e-learning environment who could be the source of threats and it is important to address the users in the environment to prevent security incidents.

5.4 Study 4- E-Learning and Its Information Security Issues in Malaysia

5.4.1 Purpose

This study will explore the e-learning status in Malaysian public universities. This study also intends to investigate the information security threats and incidents which occurred in universities that have implemented e-learning. With this study, the researcher aims to deepen the understanding of user's culture in e-learning and security.

5.4.2 Methods

A qualitative approach to allow 'meaning to emerge from the subject under investigation' was used for this study (Altman and Baruch, 1998). An interpretive context study approach was adopted. Since the social world is something which is invented and reinvented in an on-going basis by the actors and it requires direct engagement (e.g. interviews, observation etc.) with the parties concerned, this study carried out interviews for data collection. This method was chosen in order to get the real answer and situation in e-learning in Malaysia. All interviews were semi-structured in nature and involved people whose job functions related to e-learning and IT. A semi-structured interview, according to Jankowicz (2005), is a conversation steered by the questioner to

cover certain previously identified issues within a predetermined topic. The questionnaire for the interview was designed to address the purpose of this study. The Interview questions can be found in Appendix G

There are twenty public universities in Malaysia. This study chose potential universities from those twenty public universities which are known to be practicing some kind of e-learning. Twelve public universities were contacted via email with an invitation to participate in this study. At the end of the data collection stage, nine universities had responded and twelve interview sessions were conducted with each interview ranging from one to one and half hours in length. Background of the nine universities can be found in Appendix H. With prior consent from the respondents, all interviews were recorded to ensure all information was obtained and stored for future use and verification. Interviews were conducted within the month of July 2009. Table 5-14 listed the university name and the details of participants.

All interviews were recorded, summarised and analysed later. The interviews were conducted in a mix of Malay and English. Analysis began with the author listening to the recorded interview several times in order to immerse herself in the data and improve her understanding and become more familiar with the data. A general sense of the information was obtained to reflect its overall meaning. The information was organised in a summary interview report for each university. The summaries of the interviews can be read in Appendix I. Subsequently thematic analysis is used and an inferring technique was also applied to obtain the findings. A spread sheet using MS Excel was used to help in managing and analysing the data.

5.4.3 Analysis and Discussion

Table 5-14 presents the background of the interview with the university names, number of interview sessions conducted, and interviewees' job roles and departments.

Table 5-14 Details of Interview Sessions

No.	University Name	Interviews	Interviewees
1.	USIM	2	1 IT department 1 E-learning
2.	USM	2	1 IT department 1 E-learning
3.	UPSI	1	2 IT department (e-learning)
4	UITM	1	1 E-learning
5	UTM	2	1 IT department 1 E-learning
6.	UKM	1	1 E-learning
7.	UNIMAS	1	1 E-learning
8.	UM	1	1 E-learning
9.	UPM	1	1 IT department 1 E-learning

Areas that have been investigated in this study are:

- E-learning implementation (this includes when e-learning was first used in the university and how it was implemented)
- Reasons why e-learning was implemented in the university
- Challenges and issues in e-learning environment
- Acceptance of e-learning among lecturers and students
- Support from the top management regarding the e-learning implementation

- Future plans on addressing the issues and challenges
- Security threats and incidents (this includes the control and countermeasures that had been implemented to safeguard the e-learning environment and the obstacles and challenges in safeguarding e-learning)

The details of the investigated area were written as summaries for each university and can be read from Appendix I.

5.4.3.1 E-learning implementation

Some of the universities claimed that they had started implementing e-learning as early as the late 1990s. After the emphasis made by the Ministry of Higher Education on e-learning usage in public universities in Malaysia, serious steps have been taken. E-learning has been implemented as a top-down approach by eight universities, and one, based on individual initiatives is more a bottom-up approach. Those top-down approach universities have proper governance in e-learning; for example a unit or department specifically set up to administer e-learning related matters. In addition to that, the IT department plays a huge role in supporting the governance of e-learning.

'The IT department known as Information and Communication Development Centre (iDEC) has been helping CADe in supporting the infrastructure and networking for e-learning. The e-learning governance in this university is systematic with enough numbers of staff and each staff member has a very specific and distinctive job role.' (Quote from Interview)

All the universities have recommended a blended learning concept where asynchronous and synchronous learning are used. Some of them have defined the use of e-learning as a supplementary tool in the teaching and learning process.

'… using a blended learning and to be precise, e-learning is used as supplementary tools for teaching and learning. The execution range varies

among each faculty. The usage is between 20-60% with an average of 40%..' (Quote from Interview)

Each university uses different LMS to achieve their objective for e-learning implementation and the university's needs. The universities have also used different approaches in nurturing e-learning use among lecturers. Some provide the policy for e-learning which clearly states the minimum use requirement among lecturers, while others allow flexibility as to whether the lecturer wants to use it or not. So far the universities have been using a lenient approach in nurturing the e-learning usage among lecturers.

'All lecturers are obligated to utilise e-learning in their teaching. There will be monitoring and reports made to the superior party. The deans will keep reminding on the e-learning usage among lecturers. However there is no penalty given to those who do not comply…' (Quote from Interview)

It is not compulsory for lecturers to use e-learning platform as their teaching and learning method. .. The LMS is ready for any activities and depends on the lecturers to make use of it. …' (Quote from Interview)

By encouraging and nurturing e-learning among staff in the public universities, some of the universities have systematic and continuous training on e-learning and the LMS

'.. has conducted a continuous series of training for lecturers and students every semester on the use of the LMS and development of e-learning content. '(Quote from Interview)

5.4.3.2 Reasons E-Learning is implemented in the university.

The universities agreed that the reason for e-learning implementation is to enrich the teaching and learning experience for lecturers and students. They perceived the need and the importance of e-learning as well as noticing the advantages of technology in learning.

'..recognise the important of e-learning…can enrich the learning experience' ((Quote from Interview)

..improving the delivery of knowledge, students nowadays are digital natives..' (Quote from Interview)

5.4.3.3 Issues and challenges

Some of the issues and challenges mentioned by the interviewees were regarding: support from top management, lecturers' acceptance on e-learning, lack of awareness of e-learning benefits, need to keep up-to-date with the technology and high cost.

'..cultivating e-learning use among the lecturers..' (Quote from Interview)

'Less support was received from the administration and management (dean) of each school which has made the lecturers disregard the eLearn@USM LMS. Dean of schools didn't place serious emphasis on the e-learning usage among the faculty members.' (Quote from Interview)

'There is lack of awareness on the importance and benefits of e-learning and how e-learning can help in the teaching and learning process Due to this, resistance from the lecturers was received. (Quote from Interview)

'The implementation cost requires a lot of money.' (Quote from Interview)

5.4.3.4 Acceptance of e-learning among lecturer, student

The interview results have shown that students welcome the use of e-learning as a method of learning. However the frequency of use will be dependent on the use and encouragement of lecturers. The e-learning usage faces some resistance from a small number of lecturers that prefer to use the traditional method of teaching. One of the reasons of low acceptance or resistance is because of time constraints in preparing the content.

‘..are not willing to prepare the e-learning content this will take huge amount of time..’*(Quote from Interview)*

5.4.3.5 Support from the top management regarding the e-learning implementation

Top management are mostly very supportive in e-learning implementation except one university with the bottom-up approach of e-learning implementation.

5.4.3.6 Future plan- Addressing the issues and challenges

In order to address the issues and challenges mentioned in 5.4.3.3, the universities responded that an e-learning policy needs to be put in place and ensure the compliance by proper monitoring and encouragement. The encouragement includes incentive and awards for the staff who are making a positive contribution and championing the e-learning usage in the teaching and learning process. More training will be arranged to increase the awareness and literacy on e-learning.

‘*The university will set up a policy regarding e-learning and make some specifications that meet the university culture.’ (Quote from Interview)*

‘..awareness programme, such as seminars, workshops and training will be organised and attended by all lecturers..’ (Quote from Interview)

‘..design policies, awareness programmes, incentives and awards, special unit dedicated for e-learning..’ (Quote from Interview)

5.4.3.7 Security threats and incidents

The interviewees emphasised various definitions of security threats in e-learning. Some have explained some concerns and the importance of security by suggesting the need for security in e-learning.

'..contents uploaded by lecturers should be available and can be accessed by students.. should be no non-repudiation issue, for example: student submits assignment, however lecturers do not receive..' (Quote from Interview)

'...always available for use, not lose the content, the system should respond to what I want (non-repudiation), feel confident to access at any time and place, have private space, for example only the instructor can see the students work..' (Quote from Interview)

'..protection from alteration of data by intruders, prevent misuse of SPIN(LMS name)..' (Quote from Interview)

Meanwhile, others had mentioned specifically that the threats are from intentional threats.

'..intentional threats/attacks by intruders/hackers/people who deliberately want to prevent users from accessing the content..' (Quote from Interview)

'.. shouldn't be hacked and the data is in safe condition..' (Quote from Interview)

Some of interviewees reported common security threats in e-learning include viruses worms, data leakage, data missing due to human error, and software/bugs problems. Others have positively said the security threats are controllable.

'..before the security infrastructure and equipment has been upgraded, threats like viruses and worms had regularly attacked the network, thus resulting in constant denial of services. However after the major upgrade of the university's network infrastructure with intelligent security system, many threats are controllable, attacks are detectable and the network services remain buoyant..' (Quote from Interview)

It was claimed that there were none or few, security incidents on the e-learning system. However those who claimed that not many incidents had occurred said the incidents included data tampering, system break downs and inaccessibility to servers for 12 hours.

'..no security threats and issue..' (Quote from Interview)

'..not aware of any..' (Quote from Interview)

Controls and countermeasures had been implemented to safeguard the e-learning environment by using the technological approach and the responsibility to guard the security of e-learning were put on IT departments.

'..security is administered by IT department, they might know more.. (Quote from Interview)

'..set up of firewall and other common security control and countermeasures.. storage and database for e-learning is located in a specific place..' (Quote from Interview)

Obstacles and challenges in safeguarding the e-learning include a lack of awareness among staff. They claimed threats are unpredictable and difficult to avoid.

'..not all lecturers and students aware on security issues. They just use the services that are provided by the IT department… Some security issues can be predicted and avoided, but some threats are unpredictable, when and how it is going to occur.' (Quote from Interview)

One of the interviewees suggested proper management of security of e-learning.

> *'.. continuous monitoring and proper infrastructure governance and management of security also should be there..' (Quote from Interview)*

The interview results conducted have demonstrated that public universities in Malaysia are nurturing the use of e-learning in teaching and learning processes. Despite the introduction of e-learning more than ten years ago in Malaysia, the acceptance of e-learning usage among lecturers is low, due to many reasons. Due to this situation, security in e-learning has not been a main issue, instead the focus has been more on the implementation of e-learning. The interview evidence that has shown aligned remarks on security issues is from the IT departments, while the others are from a non-IT background. Some of the interviewees with a non-IT background have confidently claimed that there is no security problem. This could be true; or other possibilities are that they are not aware of the situation as their job role does not cover security issues.

The culture of users in e-learning and security was not mentioned a great deal in the interview. However with inferring techniques, some evidence on the behaviour of stakeholders in Malaysian e-learning managed to be gathered. This will be discussed and used in the analysis of the stakeholder culture view in Study 5 - Stakeholder Cultural View Modelling.

5.4.4 Key Findings of Study 4

1. Malaysia is focussing on the implementation and nurturing the usage of e-learning among e-learning users in the public universities.

2. There is little interest and concern on security in e-learning as they assume security has been fully emphasised and embedded in the infrastructure, though they know it is important to ensure the security of the e-learning environment.

3. There are threats and incidents on information security in e-learning implemented in public universities in Malaysia.

4. Technological countermeasures have been used to secure the universities and now they need a proper governance to manage the security in order to predict and deter the threats and incidents of attack.

5. The current focus of security countermeasures and controls are to protect against malicious attack and those outside the universities.

5.5 Integration of Stage 1 Multi-method Studies Findings

Based on the information gathered, the relevance of the research problem and research purpose was reviewed. The research problem and objectives have taken on people interest. When Study 1 was conducted to explore the security in an e-learning situation, the finding has significantly pointed to the people issues. Users are not aware of the threats and security situation in e-learning. Study 2 has looked into the relationship between people, threats and countermeasures. It has provided knowledge on the roles and responsibilities of actors in the security issue for each application in e-learning, the situation and possible threats of e-learning. Identifying the threats specific to e-learning can help the providers to plan suitable countermeasures. Study 3 used known incidents to understand the types of attack, and people are an important source of attack for e-learning. These studies have led the researcher see that people need to be addressed more visibly in the ISM standard and guidelines. Individual factors and how people perceive risk is a part of the explanation for users' view on information security (Albrechtsen, 2007). The findings from Study 4 have reflected the e-learning situation of the public universities in Malaysia and gained face to face dialogues to corroborate with the other studies.

5.6 Chapter Summary

This chapter has explained the studies conducted in the first stage of this research. The aim of this stage is to explore and understand the security in e-learning. As a result of this stage, concepts for the ISM model for e-learning were developed. This stage has also indicated the needs of the second stage studies to be conducted, to explore and understand people and their impact towards security.

6 DEVELOPMENT OF E-LEARNING STAKEHOLDERS INFORMATION SECURITY VULNERABILITY MODEL

The work reported in this chapter covers the experimentation to discover the relationship between e-learning stakeholders, security threats and their prevention. Some of the work has been reported in the Literature Review chapter with regard to e-learning stakeholders and the 'soft' people studies. The work reported here is the building of the model for e-learning.

Stage one research reported in the last chapter affirmed that e-learning suffers from information security incidents and some of these incidents were the results of lapses in the practice of information security management. This part of the research tried to discover if there are security threats that are particular to different types of stakeholders, or if different stakeholder types are susceptible to particular types of security threats.

There are two studies conducted in this stage. Both are carried out as desk studies. Each study in this chapter is detailed with the purpose, methodology, results and finding. In this chapter the integration and significance of different results of the research (stage 1 and 2 multi-method studies) are explained as to model built. The model developed is presented at the end of this chapter. Figure 6-1 illustrates the elements related to data collection, analysis and findings for the first stage of this research.

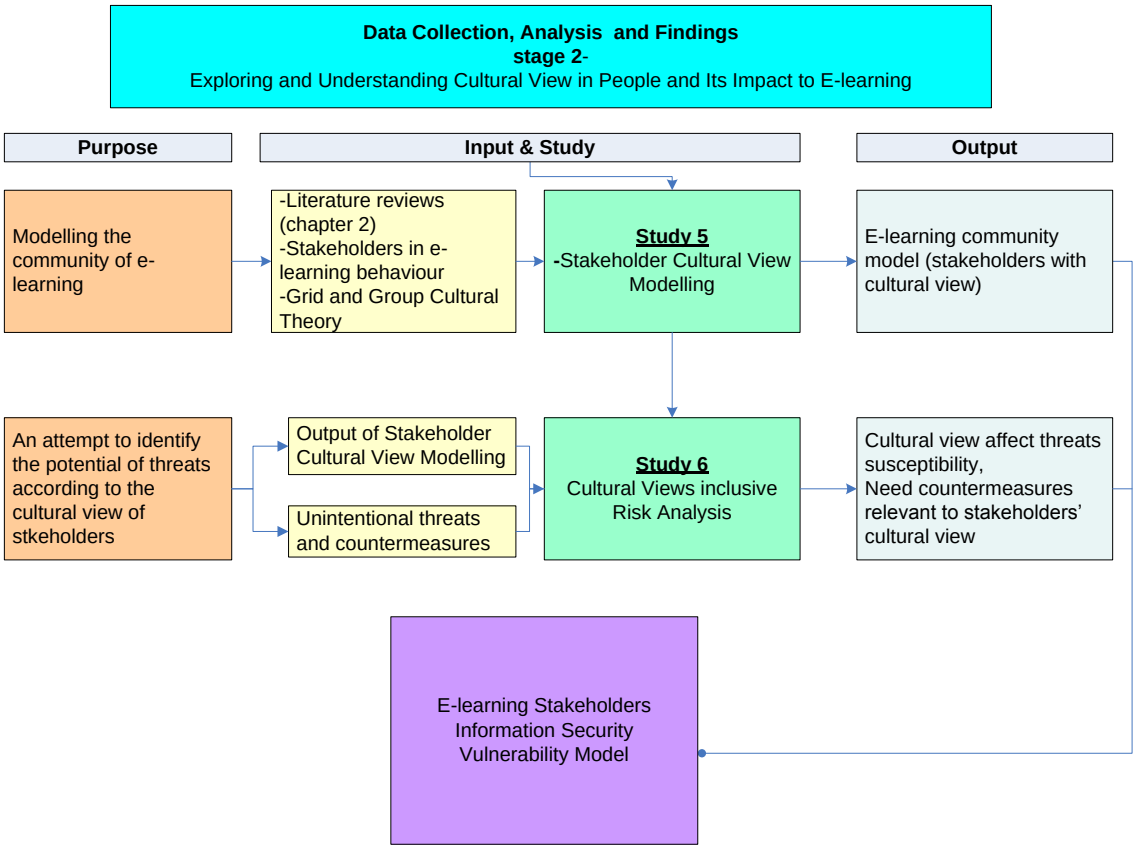


Figure 6-1 Stage 2- Study Purpose, Input and Output

6.1 Study 5- Stakeholder Cultural View Modelling

6.1.1 Purpose

The cultural view types defined in section 2.6.2 refer to groups of individuals from a general population. Anecdotal evidence and common sense suggest that different people are vulnerable to different information threats. This study attempt to apply the Cultural Theory cultural views to the different stakeholders in e-learning, based on their roles and tasks. The result could be a first step towards designing e-learning system interaction, based on the characteristics of the end users.

The research rationale originates from the socio-technical thinking of involving end users in the design of work. However, the research environment prevented 'real' involvement of sufficient e-learning practitioners in the different roles. This

is a ‘thought’ experiment and the results are taken to the next stage with the caveat that reality could be different.

6.1.2 Method

The e-learning community classification reported in section 2.3.6 was used as a starting point.

The stakeholders were grouped into the Supply Group and the Demand Group. The Supply Group is the universities or institutions that provide the e-learning environment and have three roles: Top Management (TM), e-learning Centre personnel (EC), and IT personnel (IT). The Demand Group consists of end-users that use the e-learning environment and have two roles: Lecturers (LEC), Students (ST). The function and task of each stakeholder group was elaborated, based on the work of Study 2, reported in Table 5:10 Applications in E-learning and Table 5.11 Actors and Roles. Table 6.1 presents the outcomes. Data collected from Study 4 (E-Learning and Its Information Security Issues in Malaysia) were used to complement the information gathered from literature for identifying the stakeholders’ behaviour.

Considering the functions and tasks of each stakeholder group, the characteristics for the Cultural Theory cultural views were examined to evaluate what may be exhibited. The four cultural views of the Culture Theory: hierarchism (HIE), egalitarianism (EGA), individualism (IND) and fatalism (FTL), are defined in Table 2.5 in Chapter 2.

The result is the ‘possible’ cultural views, and is not meant to be prescriptive. At first, classification was done based on the analysis of literature just described. A second classification was then done using the Malaysia interview results to adjust the e-learning functions and roles, as well as evidence to allocate the cultural views.

6.1.3 Results and Discussion

Table 6-1 presents the functions and behaviour of stakeholders’ in e-learning. The function explains the job scope of the stakeholders, while the

task/behaviour column illustrates the specific responsibility and activities of the function.

The possible cultural views held by each e-learning stakeholder group were assigned. After comparing the literature based and Malaysian studies, it was concluded that there is no difference between Malaysian e-learning stakeholders with the other e-learning stakeholders in the rest of the world. E-learning's Stakeholders Cultural View as depicted in Figure 6-2. suggests the possible cultural views held by different stakeholders of e-learning.

The Lecturer group is expected to have persons that exhibit one or a combination of the four cultural views. The Top Management group is expected to display primarily the HIE view, in their e-learning TM role. This does not mean that the person on the TM group does not have other cultural views in their normal life. The assigning of cultural view to the stakeholders is in the context of their function and tasks in the e-learning environment only.

The EC and IT groups have responsibility to set up and enforce systems, thus not compatible with the Fatalism view. The students are not expected to set up and enforce systems, thus not compatible with the Hierarchism view.

Table 6-1 E-learning's Stakeholder Functions and Behaviour

Stakeholders	Functions	Task/behaviour
Top management	1.Develop a strategic plan for e-learning implementation	I. Enhance the e-learning infrastructures and facilities II. Collaboration with other parties
	2. Manage the business	I. Using business intelligent tools and data mining process to get high level overview to help in strategic planning.
IT personnel	1.Responsible on the technical part in the e-learning environment and system	I. Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre) II. Working with external parties (LMS vendor)
	2. Create a competent and efficient customer centre support service on e-learning matters	I. Support the customers or users on IT services
	3. Provide operational support on the campus network and telecommunication infrastructure	I. Support the customers or users on network and telecommunication infrastructure
E-learning centre	1. Championing a strategy to develop a successful e-learning environment	I. Manage the LMS II. Provide training on e-learning applications and tools
Lecturers	1. to provide effectively design courses incorporating e-learning for student	I. prepare the teaching and learning materials, upload them on the LMS II. monitor and respond to students usage and discussion
	2. to provide technical and motivational support encouraging the use of e-learning to students and colleagues	I. share experiences and encourage use among lectures II. explore and use technology and tools for education on the internet
Students	1. to participate in learning process	I. view, read and write in the LMS (online session, file storage etc.)
		II. Communicate online with lecturers and peers students
		III. Eager to explore the Internet, and use the application and software downloaded from the Internet

Stakeholders	Possible Cultural view
Supply Group	
Top Management (TM)	Hierarchism (HIE)
E-Learning Centre personnel (EC)	Hierarchism (HIE), Individualism (IND), Egalitarianism (EGA)
IT personnel (IT)	Hierarchism (HIE), Individualism (IND), Egalitarianism (EGA)
Demand Group	
Lecturer (LEC)	Hierarchism (HIE), Individualism (IND), Egalitarianism (EGA), Fatalism (FTL)
Students (ST)	Individualism (IND), Egalitarianism (EGA), Fatalism (FTL)

Figure 6-2 E-Learning's Stakeholders Cultural View

6.2 Study 6 – Cultural Views Inclusive Risk Analysis

6.2.1 Purpose

This study pulled together the work in the previous five studies to consider if the different stakeholder cultural views affect information risks to e-learning systems.

Finding of Study 3 mentioned that most incidents in e-learning were unintentional. From the implementation of ISM, this analysis is focused on unintentional human errors from within the e-learning system. The threat of external malicious attacks had not been look at.

6.2.2 Method

The risk analysis approach of Failure Mode and Effect Analysis (FMEA)(McDermott et al., 2009) was adapted for this study. FMEA calculates risk, based on a Risk Priority Number (RPN) as

$$RPN = P \times S \times D$$

P=Probabilities (chance) of Occurrence

S=Seriousness of Failure

D=Detectability of Failure

In this study, the Probabilities of Occurrence were adapted to the Likelihood of security threat, and was moderated by the cultural view that may make this threat more or less likely. The Seriousness of Failure was adapted to represent the impact to business, drawn from Study 2 reported in section 5.2. The business impact is independent of cultural views. The Detectability of Failure was adapted to represent the effectiveness of threat control, which is moderated with cultural views.

This study calculates the RPN for likely threats of each stakeholders group and then compares the results to understand the possible implications of cultural views on e-learning information security. The flow of steps conducted in this study is displayed in Figure 6-3.

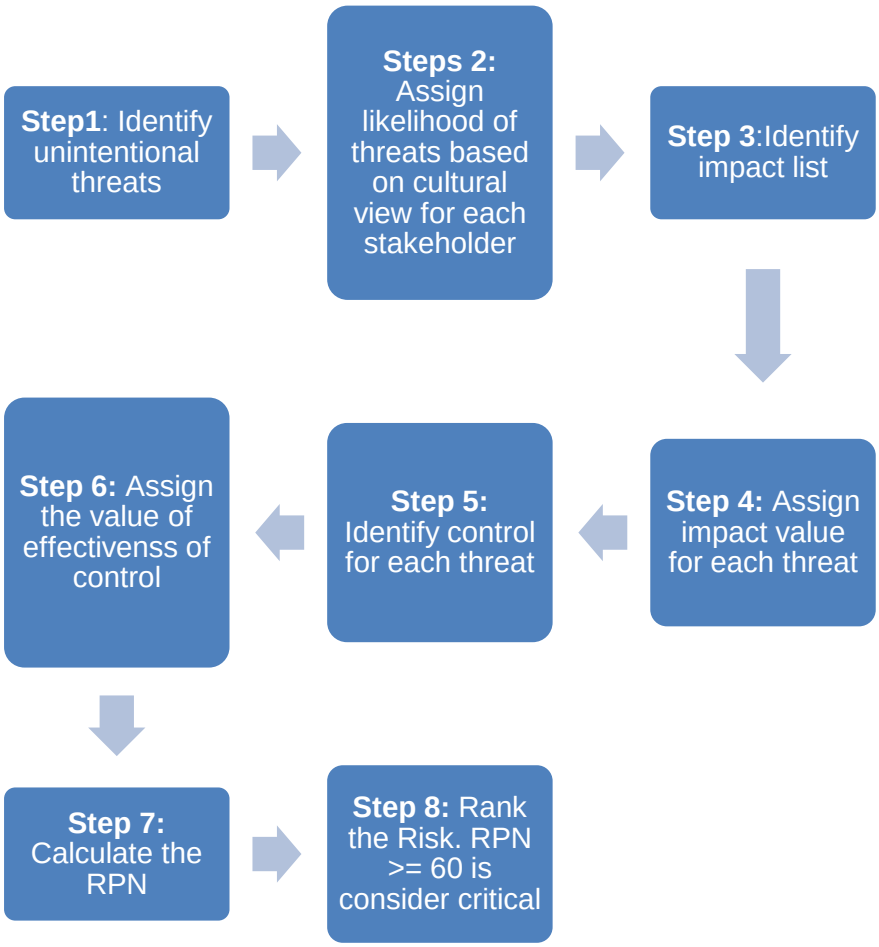


Figure 6-3 Eight Steps of E-learning Stakeholder Threats and Risk Analysis

Step 1: Identify Unintentional Threats

In this step, the unintentional threats that arise from human error that could occur in e-learning were identified. The list of threats was derived from Study 2. The possibility of threats found in this step was correlated to the stakeholder based on the roles and function in the e-learning system and the expected behaviour. Table 6-2 displays the result of this step.

Table 6-2 Possibility of the Stakeholders to Contribute the Threats

Unintentional Threats	Stakeholders				
	TM	EC	IT	LEC	ST
Data Entry Error	√	√	√	√	√
Installation and Maintenance Errors		√	√		
Error of Authorisation or in The Instructions	√	√	√	√	
Transmission Errors	√	√	√	√	√
Operational Support Error		√	√	√	
Use of Software in Unauthorised Way	√	√	√	√	√
Illegal Use of Software	√	√	√	√	√
Accidental Deletion of Data	√	√	√	√	√
Accidental Destruction of Software Programs	√	√	√	√	√
Accidental Destruction of Configurations or Hardware		√	√		
Leaving Weaknesses (Vulnerabilities) in Software		√	√		
Carelessness	√	√	√	√	√
Insufficient Authentications, Weak Password Recovery Validation		√	√		
Insufficient Authorisation, Insufficient Session Expiration		√	√		
Information Disclosure	√	√	√	√	√

Step 2: Assign likelihood of threats based on cultural view for each stakeholder role

The E-learning stakeholder's cultural model as Figure 6-2 developed in Study 5 was used here. Based on the e-learning stakeholder cultural model, a template of the threats that occur in that cultural view was drawn up. Analysis for Students is used for reporting here. The analysis of the other stakeholder groups are in Appendix J. Table 6-3 shows the template used to complete step 2. The likelihood of the threats occurring to the stakeholders was assigned. The threat likelihood had a range of 1-5, with the 1 representing 'not at all likely', 2 is 'a little likely', 3 is 'moderately likely', 4 is 'very likely' and the highest value, 5 representing 'extremely likely'.

Table 6-3 Template of Threats Likelihood for Student

			Likelihood based on culture view topology		
Functions	Task	Threats	FTL	IND	EGA

Step 3: Identify impact list

The security impact included loss of availability (interruption), loss of integrity (modification and fabrication) and loss of confidentiality (interception) of information. The impact affects the organisation and individuals. Table 6-5 shows the generated impact list. This list was based on information gathered from threats analysis in Study 2. Table 6-4 provides the definition of ranking that was used in this step.

Table 6-4 Definition of Impact Rank

Ranking	Impact	Definitions
1	Insignificant	The impact could be **insignificant** on organisational operations, organisational assets, or individuals.
2	Low	The impact could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.
3	Moderate	The impact could be expected to have a **moderate** adverse effect on organisational operations, organisational assets, or individuals.
4	Major	The impact could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.
5	Critical	The impact could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.

Table 6-5 Human Error vs. Impact

Human Errors	Impact
Data entry error	• Confidentiality (Interception), • Integrity (Modification, Fabrication), Availability (Interruption)
Installation and maintenance errors	• Availability (Interruption)
Error of authorisation or in the instructions	• Confidentiality (Interception), Integrity (Modification, Fabrication), Availability (Interruption)
Transmission errors	• Integrity (Modification, Fabrication)
Operational support error	• Availability (Interruption)
Use of software in unauthorised way	• Integrity (Modification, Fabrication)
Illegal use of software	• Confidentiality (Interception), • Integrity (Modification, Fabrication), Availability (Interruption)
Accidental deletion of data	• Integrity (Modification, Fabrication), Availability (Interruption)
Accidental destruction of software programs	• Integrity (Modification, Fabrication), Availability (Interruption)
Accidental destruction of configurations or hardware.	• Integrity (Modification, Fabrication), Availability (Interruption)
Leaving weaknesses (vulnerabilities) in software	• Integrity (Modification, Fabrication), Availability (Interruption)
Carelessness	• Confidentiality (Interception), Integrity (Modification, Fabrication), Availability (Interruption)
Insufficient authentication, weak password recovery validation	• Integrity (Modification, Fabrication), Availability (Interruption)
Insufficient Authorisation, Insufficient Session Expiration	• Confidentiality (Interception), Integrity (Modification, Fabrication), Availability (Interruption)
Information disclosure	• Confidentiality (Interception), Integrity (Modification, Fabrication), Availability (Interruption)

Step 4: Assign impact value for each threat

In this step, the impact value of each threat is assigned with the value ranging from 1 to 5. Each value was given a level of effect namely insignificant, low, moderate, major and severe. These values represent the worst case scenario. This guides the identification of controls that can adequately protect.

To simplify the analysis, the value of impact to the respective threats is assumed to be the same for all the stakeholder roles. Table 6-6 shows the value set for this step based on the understanding of literature review on security risk and Table 6-5.

Table 6-6 Value of Impact Designed

No.	Human Errors	Impact Value
1	Data entry error	4
2	Installation and maintenance errors	4
3	Error of authorisation or in the instructions	5
4	Transmission errors	4
5	Operational support error	5
6	Use of software in unauthorised way	4
7	Illegal use of software	4
8	Accidental deletion of data	4
9	Accidental destruction of software programs	3
10	Accidental destruction of configurations or hardware.	3
11	Leaving weaknesses (vulnerabilities) in software	5
12	Carelessness	5
13	Insufficient authentication, weak password recovery validation	5
14	Insufficient Authorisation, Insufficient Session Expiration	5
15	Information disclosure	5

Step 5: Identify control for each threat

Here, suitable controls were identified for each threat. The threats considered are induced by human error. Table 6-8 lists controls for human error which were drawn from Study 2, published standards and models for security management.

Step 6: Assign the value of control effectiveness

In this step, the effectiveness of each security control is valued according to the cultural view of each stakeholder role. The effectiveness of control had a range of 1-5, with the 1 representing ‘very effective’, 2 is ‘moderately effective’, 3 is ‘a little effective’, 4 is ‘not effective at all’ and 5 representing ‘insignificant’. Table 6-7 represents the template used.

Table 6-7 Template of Effectiveness Value for Student

		Effectiveness value based on culture view topology		
Threats	Control	FTL	IND	EGA

Step 7: Calculate the RPN

Once the likelihood of threats, the impact and the effectiveness of control are valued, the Risk Priority Number (RPN) is calculated. The formula used is:

RPN = likelihood x impact x effectiveness of control

Table 6-8 Security Controls

Human Errors	Counter measure
Data Entry Error	• Users shall be given security education and technical training
Installation and Maintenance Errors	• Strict control shall be exercised over the implementation of software on operational systems • Documented procedures shall be provided for the operation of all computer systems and for systems development, maintenance and testing
Error of Authorisation or in the Instructions	• Information access restriction • Users shall have access only to the services that they are authorised to use
Transmission Errors	• Security of electronic office system • Data and software exchange agreement • Users shall be given security education and technical training
Operational Support Error	• Documented procedures shall be provided for the operation of all computer systems and for systems development, maintenance and testing • Users shall be given security education and technical training
Use of Software in Unauthorised Way	• Users shall have access only to services that they are authorised to use • There shall be formal user registration and de-registration procedures for access to all multiuser information services • Job description shall define security roles and responsibilities
Illegal Use of Software	• Measures shall be taken to comply with contractual restrictions on the use of copyright materials • Use of system utilities

	• Job description shall define security roles and responsibilities
Accidental Deletion of Data	• Users shall be given security education and technical training
Accidental Destruction of Software Programs	• Users shall be given security education and technical training
Accidental Destruction of Configurations or Hardware	• Users shall be given security education and technical training
Leaving Weaknesses (Vulnerabilities) in Software	• Users shall be given security education and technical training
Carelessness	• A range of security controls shall be established to protect data in computer networks • Users shall be given security education and technical training • Inactive terminals in high risk location or serving high risk systems shall be set to time out, to minimise the risk of access by unauthorised person
Insufficient Authentication, Weak Password Recovery Validation	• A range of security controls shall be established to protect data in computer networks
Insufficient Authorisation, Insufficient Session Expiration	• A range of security controls shall be established to protect data in computer networks • Inactive terminals in high risk location or serving high risk systems shall be set to time out, to minimise the risk of access by unauthorised person
Information Disclosure	• Users shall be given security education and technical training • Users shall be required to follow good security practices (i.e. in the selection and use of password)

Step 8: Rank the Risk

The maximum RPN value found from this analysis is 124. This study has chosen 48% as the threshold for critical risks. Therefore, 48% of 125 is 60. All risks with RPN equal and above 60 are identified as Critical and will be marked in red. Hence any RPN equal and above 60 requires review and control improvements.

The same eight step analysis was done for the Malaysian context using the rich interview data that adds the subtleties of country culture and adoption fears. This was to see if there are differences between the general context and the Malaysian context.

The analysis results is an extensive list and a long Spreadsheet with 896 rows. Table 6-9 is a snapshot of the analysis for student only. Steps 1 - 8 of e-learning stakeholders' threats and risk analysis discussed earlier has been implemented here.

The process to calculate the RPN for the first row in Table 6-9 is described below:

Reading from the left, the threats likelihood of 'data entry error' for a person with fatalism cultural view is assessed to be 2. The impact of this threat to the business, no matter what cultural view, is assessed to be 4. The control effectiveness of 'users are given security education and technical training' for a person with fatalism cultural view is assessed to be 4. The RPN for the fatalism view is thus 2 x 2 x 4 = 32.

The same calculation is repeated for the individualism view is 2 x 4 x 3 = 24.

The same calculation is repeated for the egalitarianism view is 2 x 4 x 3 = 24.

As the RPNs for all the cultural views are below 60, this threat (data entry error) is not considered as a critical threat.

Table 6-9 Stakeholders Culture View towards Security Analysis

	STUDENT			Likelihood value based on culture view topology					Effectiveness value based on culture view topology			RPN		
No.	**Stakeholder Function**	**Task/ Behaviour**	**Threats**	**FTL**	**IND**	**EGA**	**Impact Value**	**Controls**	**FTL**	**IND**	**EGA**	**FTL**	**IND**	**EGA**
1	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Data entry error	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
2	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Installation and maintenance errors	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	4	4	4
32	To participate in learning process	Communicate online with lecturers and peers students	Error of authorisation or in the instructions	1	1	1	5	Information access restriction	1	1	1	5	5	5
67	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Users have access only to services that they are authorised to use	1	1	1	20	20	16
68	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
84	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	4	3	100	100	75

6.2.3 Results & Findings

This section presents the results of the risk analysis for each stakeholder cultural view. Extensive Spreadsheets were used to conduct the analysis and only the Students analysis is presented as example. Table 6-10 shows the excerpt of result showing the RPN of threats according to stakeholder (Student) functions and roles. The critical threats and the main contributing cultural views are listed for Students group.

Table 6-10 Excerpt of Result on RPN of Threats According to Stakeholder (Student)

				RPN		
No	stakeholder function	Task/ behaviour	Threats	FTL	IND	EGA
1	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	64	48	48
2	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	64	36	36
3	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Use of software in unauthorised way	64	36	36
4	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Use of software in unauthorised way	64	36	36
8	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Information disclosure	100	75	75
9	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	80	60	60
10	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	80	60	60
11	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	64	36	36
12	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	64	36	36

In the example presented, Student has one function and three different tasks. For each task different cultural view shows different RPN towards the same threat.

Student

In the Student function of “to participate in learning process”, the risk tables for the three tasks follow:

Task: View, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)

No.	Threats	FTL	IND	EGA
1	Transmission errors	64	48	48
2	Use of software in unauthorised way	64	36	36
3	Accidental destruction of software programs	60	45	45
4	Carelessness	100	75	75
5	Information disclosure	100	75	75

Task: Communicate online with lecturers and peers students

No.	Threats	FTL	IND	EGA
1	Transmission errors	80	60	60
2	Use of software in unauthorised way	64	36	36
3	Illegal use of software	80	60	48
4	Carelessness	100	75	75
5	Information disclosure	100	75	75

Task: Eager to explore the Internet, and use the application and software downloaded from the Internet

No.	Threats	FTL	IND	EGA
1	Transmission errors	64	48	36
2	Use of software in unauthorised way	80	60	48
3	Illegal use of software	80	60	48
4	Accidental destruction of software programs	60	45	36
5	Carelessness	100	75	75
6	Information disclosure	100	100	75

Generalising the result as displayed earlier, the author observed that the most common cultural view that is susceptible to threat is FTL. Stakeholder cultural views may increase or reduce information security risks.

The following shows the generalised result of each stakeholder. The result focused on finding the critical threats for e-learning stakeholders.

6.2.3.1 Top Management

Table 6-11 shows the list of critical threats for top management, who have the Hierarchism culture view. Comparison results suggested that the top management in Malaysia have no significant difference from other top management in the world. They share the same list of critical threats.

Table 6-11 Critical Threats for Top Management

No	Threats	Cultural views
1	Carelessness	HIE
2	Information Disclosure	HIE
3	Data Entry Error	HIE
4	Accidental Deletion of Data	HIE

6.2.3.2 IT Personnel

The list of critical threats for IT Personnel showed that Individualism and Egalitarianism are the most exposed cultural views (Table 6-12).

Table 6-12 Critical Threats for IT Personnel

No.	Threats	Cultural views
1	Data Entry Error	IND,EGA
2	Operational Support Error	IND,EGA
3	Accidental Deletion of Data	IND,EGA
4	Leaving Weaknesses (Vulnerabilities) in Software	IND,EGA
5	Carelessness	IND,EGA
6	Information Disclosure	HIE,IND,EGA

Table 6-13 lists the critical threats for Malaysian IT Personnel. The result suggested that Individualism is the most exposed cultural view.

Table 6-13 Critical Threats for IT Personnel (Malaysia)

No.	Threats	Cultural views
1	Data Entry Error	IND,EGA
2	Installation and Maintenance Errors	IND,EGA
3	Operational Support Error	IND,EGA
4	Accidental Deletion of Data	IND,EGA
5	Carelessness	IND,EGA
6	Insufficient Authentications, Weak Password Recovery Validation	IND
7	Insufficient Authorisation, Insufficient Session Expiration	IND
8	Information Disclosure	IND,EGA

The Malaysian results have three additional critical threats compared with the general IT Personnel list. Individualism is the most risky cultural view. The other threats and contributing views are similar to Table 6-12 except for the Information Disclosure. Besides Individualism and Egalitarianism, Hierarchism increases the risks of Information Disclosure.

6.2.3.3 E-learning Centre Personnel

The table of critical threats for an E-learning Centre shows that Egalitarianism is the most exposed cultural view amongst E-learning Centre Personnel, followed closely by Individualism. See Table 6-14.

Table 6-14 Critical Threats for E-learning Centre Personnel

No.	Threats	Cultural views
1	Data Entry Error	IND,EGA
2	Error of Authorisation or in The Instructions	EGA
3	Operational Support Error	IND,EGA
4	Accidental Deletion of Data	IND,EGA
5	Leaving Weaknesses (Vulnerabilities) in Software	IND,EGA
6	Carelessness	IND,EGA
7	Information Disclosure	IND,EGA

For the Malaysian E-learning Centre Personnel (Table 6-15), Individualism is the most exposed to threats, followed closely by Egalitarianism.

The results suggested that Malaysian E-learning Centre Personnel have four extra critical threats; namely Installation and Maintenance Errors, Transmission Errors, Insufficient Authentications, Weak Password Recovery Validation, and Insufficient Authorisation, Insufficient Session Expiration. The most exposed cultural view in Malaysian E-learning Centre Personnel is Individualism, while in the general E-learning Centre Personnel the most exposed view is Egalitarianism.

Table 6-15 Critical Threats for E-learning Centre Personnel (Malaysia)

No.	Threats	Cultural views
1	Data Entry Error	IND,EGA
2	Installation and Maintenance Errors	IND,EGA
3	Error of Authorisation or in The Instructions	IND,EGA
4	Transmission Errors	EGA
5	Operational Support Error	IND,EGA
6	Accidental Deletion of Data	IND,EGA
7	Leaving Weaknesses (Vulnerabilities) in Software	IND,EGA
8	Insufficient Authentications, Weak Password Recovery Validation	IND
9	Insufficient Authorisation, Insufficient Session Expiration	IND
10	Carelessness	IND,EGA
11	Information Disclosure	IND,EGA

6.2.3.4 Lecturer

Table 6-16 is the list of critical threats for lecturers. Individualism and Egalitarianism are the most exposed cultural views, followed closely by Fatalism and Hierarchism. While in Table 6-17, all cultural views are exposed, with Individualism and Egalitarianism being more exposed than the others.

There are 11 threats for the Malaysian lecturer group, with one additional threat in Accidental Destruction of Software Programs. For both the general and Malaysian context, the result suggested that the Individualism and Egalitarianism cultural views are more exposed to threats.

Table 6-16 Critical Threats for Lecturer

No.	Threats	Cultural views
1	Data Entry Error	FTL, HIE, IND, EGA
2	Error of Authorisation or in The Instructions	HIE, EGA, IND
3	Transmission Errors	FTL, HIE, IND, EGA
4	Operational Support Error	FTL, HIE, IND, EGA E
5	Use of Software in Unauthorised Way	FTL, IND, EGA
6	Illegal Use of Software	FTL, IND, EGA
7	Accidental Deletion of Data	FTL, HIE, IND, EGA
8	Carelessness	FTL, HIE, IND, EGA
9	Information Disclosure	FTL, HIE, IND, EGA
10	Installation and Maintenance Errors	FTL, HIE, IND, EGA

Table 6-17 Critical Threats for Lecturer (Malaysia)

No.	Threats	Cultural views
1	Data Entry Error	FTL, HIE, IND, EGA
2	Error of Authorisation or in The Instructions	HIE, IND, EGA
3	Transmission Errors	FTL, HIE, IND, EGA
4	Operational Support Error	FTL, HIE, IND, EGA
5	Use of Software in Unauthorised Way	FTL, IND, EGA
6	Illegal Use of Software	FTL, IND, EGA
7	Accidental Deletion of Data	FTL, HIE, IND, EGA
8	Carelessness	FTL, HIE, IND, EGA
9	Information Disclosure	FTL, HIE, IND, EGA
10	Installation and Maintenance Errors	FTL, IND, EGA
11	Accidental Destruction of Software Programs	IND,EGA

6.2.3.5 Students

Table 6-18 shows the list of critical threats for students and the Fatalism view is the most exposed to threats, followed closely by Individualism.

Table 6-18 Critical Threats for Student

No.	Threats	Cultural views
1	Transmission Errors	FTL, IND, EGA
2	Use of Software in Unauthorised Way	FTL, IND
3	Illegal Use of Software	FTL, IND
4	Accidental Destruction of Software Programs	FTL
5	Carelessness	FTL, IND, EGA
6	Information Disclosure	FTL, IND, EGA

The list of critical threats for Malaysian students is similar to that of general students. This may be due to young people being used to rapid access to global knowledge (IT knowledge or the security knowledge) through the Internet.

The study has shown that stakeholders' cultural view does influence e-learning information security risks. The analysis produced for each stakeholder role a different list of critical threats. For each stakeholder role, certain cultural views are more vulnerable to threats. This is depicted in Table 6-19.

Table 6-19 Critical Threat by Cultural View among Stakeholders

Stakeholders	**General**
Top Management	HIE
IT Personnel	IND, EGA
E-learning Centre Personnel	IND, EGA
Lecturers	IND, EGA, FTL, HIE
Students	FTL, IND

This argues for the cultural view of people needs to be considered in the design of information security management systems, and included as part of the technical and management approach. For Supply Group stakeholders, Individualism and Egalitarianism cultural views are more exposed to threats. For the Demand Group stakeholders, the Fatalism and Individualism cultural view are more exposed. These cultural view differences should be appropriately incorporated in ISM.

6.3 Construct E-Learning Stakeholders Information Security Vulnerability Model

Analytical evidence collected in Study 6 showed that cultural view affects threat susceptibility, thus e-learning ISM could benefit from controls that are relevant to the cultural view of the stakeholders. The E-Learning Stakeholders Information Security Vulnerability Model is constructed based from literature reviews and six multi-method studies. Figure 7-2 represents the four dimensions of E-Learning Stakeholders Information Security Vulnerability Model together with the relationships. The correlation between each dimension in the model was derived from the findings of Study 6 conducted.

The model aims to provide fundamental dimensions in the management of information security for stakeholders in e-learning. The model serves as an integrative structure to understand and define the stakeholder's cultural view in securing the e-learning environment.

The model incorporates the dimensions which bring out the relationship between people's behaviour and information security. The dimensions are Threats, Stakeholders, Cultural View and ISM Elements. Each dimension is positioned in a column that contains the components. The Threats dimension indicates the type of threats that are possible in e-learning. Each type can further define the possible acts that contribute to threats. The Stakeholders dimension reflects the people that form the e-learning community. The Culture View dimension depicts the type of views that are possibly held by the

stakeholders. Finally, the ISM elements dimension presents the three elements of ISM, policy, process and procedures, and organisation structure. The hardware and software element of ISM are not included as they fall specifically in IT personnel job scope.

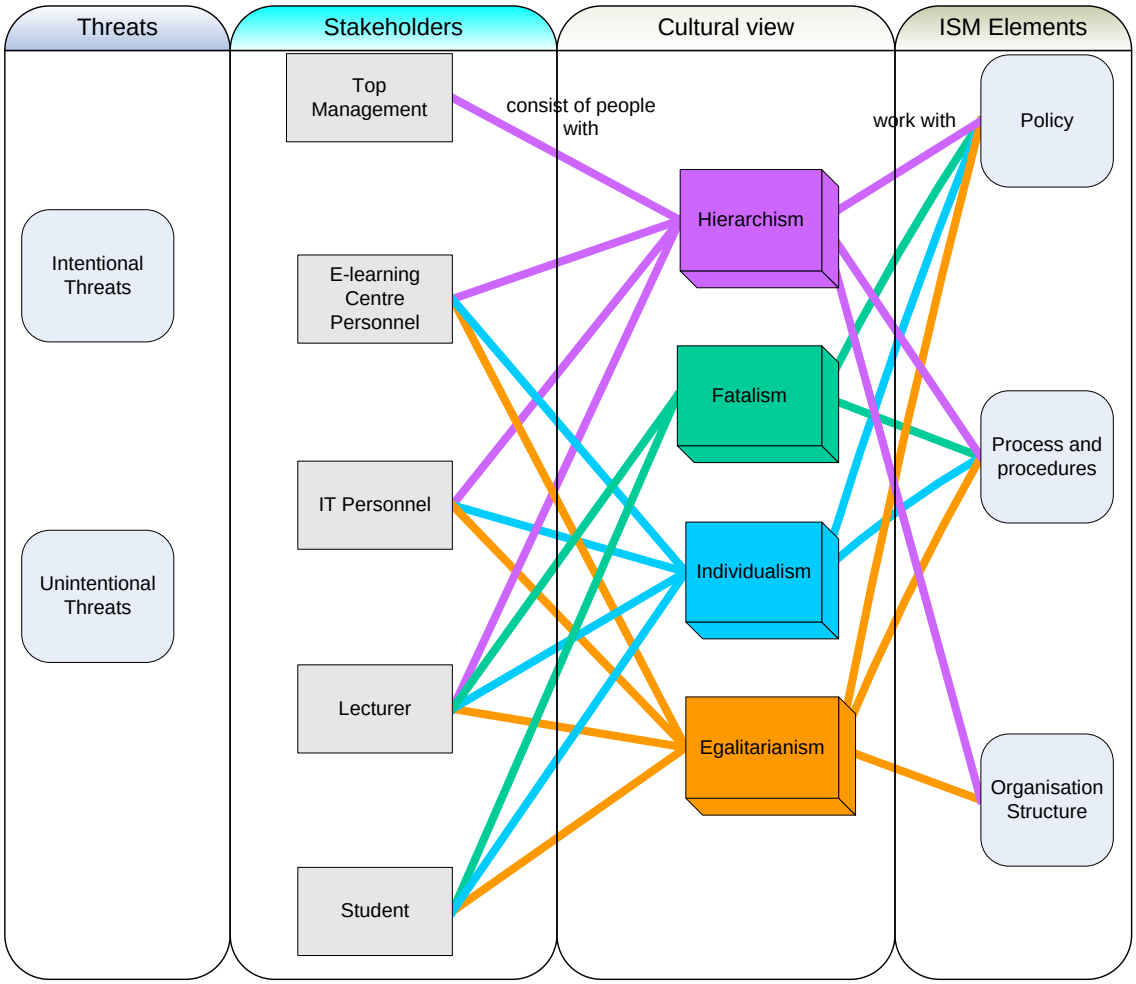


Figure 6-4 E-Learning Stakeholders Information Security Vulnerability Model

6.4 Chapter Summary

This chapter has explained the studies conducted in the second stage of this research to build the E-learning Stakeholders Information Security Vulnerability model. The dimensions and components in the model could guide the identification of possible threats based on the cultural view of stakeholders. Suitable countermeasures could be correlated and assigned. The e-learning provider could be better prepared for information security management.

.

7 SECURITY COUNTERMEASURES DESIGNED WITH VULNERABILITY MODEL

This chapter reports on the feedback obtained from the experts on the correctness, potential and applicability of the research findings. This exercise was conducted after the theoretical model was built and experts were invited to comment on the impact and practicality of this research.

The following section explains the process before, during and output of expert review. This includes how the questions is developed and piloted, who are the expert and why they were chosen, how the process is conducted and the feedback received.

7.1 The Process

The purpose of the expert review is to obtain some expert opinion not on the research process but more to verify whether the research findings and output make sense. This exercise also attempts to understand the potential to apply the research findings in a wider context. This research proposed that the cultural view affects threats vulnerability, and e-learning ISM controls can be more effective if made relevant to the cultural view of the stakeholders. The controls focus on the ISM elements: policy, process and procedures and organisational structure. This research suggests that the controls which address and consider the cultural characteristic and behaviour will lower the criticality of threats. More personalised controls are more likely to be observed by the stakeholder.

This research developed a model as a result of six multi-method studies. The nature of research and output model presented, validating the model dimensions and its correlation will result in full scale real world experiments is impossible. Consequently an illustration of controls (ISM element) designed according to the cultural view has been prepared in Table 7-1. This illustration assists the experts to review the applicability and impact of the model.

The questionnaire script has been prepared to briefly explain the research conducted and the findings. The preparation has gone through a thorough process, including the designing of questions and choosing the relevant material to be included to help the reviewer have a clear picture of the research as well as to provide them with an idea of what is expected from them.

The questionnaire script was piloted by an IT Network Engineer who has an interest in information security from a multinational company in Malaysia. The piloting process was used to improve the questionnaire script design. The final questionnaire script can be found in Appendix K.

The experts were invited to review the illustration of controls designed and to answer the questions. The questionnaire was distributed using email to the four experts with ISM background in UK. Three experts returned their results, with one requesting for face-to-face discussion. The face-to-face discussion clarified the ISM perspective of this research.

Table 7-1 Illustration of controls according to cultural view focussing on ISM elements

Cultural view	**Hierarchism**	**Individualism**	**Egalitarianism**	**Fatalism**
ISM Policy Example of different ways to write the policy on data entry for lecturers.	*'The lecturer shall enter the correct data'.*	*'The lecturer has to ensure data entered is correct due to the massive impact to the student (or other stakeholders').*	*'The lecturer has to ensure data entered are correct in sustaining self-accountability and integrity'.*	*'The lecturer has to be responsible on every data entry'.*
ISM Process and procedures Example of process and procedures in 1) document and record control and 2) conducting training awareness	1) Document and Record Control Messages can be worded to emphasise on aspects that bring out control and power. 2) Training Messages can be framed to emphasise the impact on the image and reputation of the organisation. Also, the impact that may affect their continuing status must be highlighted. Information given in training should be based on the worst possible outcomes	1) Document and Record Control Messages can be in language to stress the reliance on others and threats induced by individualistic behaviour. 2) Training Messages can be framed to emphasise impact of security incident personally on themselves. This will increase the understanding of the influence in their upcoming decision. Their character on risk taking can be neutralised with information regarding their potential rewards or	1) Document and Record Control Messages can be worded to emphasise the importance to keep some information confidential despite the positive teamwork and cooperative value behaviour. 2) Training Messages can be framed that stresses the social costs associated with security breaches since egalitarianists dislike the unnecessary impact implied to them and others.	1) Document and Record Control Messages can be in a simple language, not overcomplicated or negative to help them understand as well as enthuse them so that they can positively support information security. 2) Training Messages can be framed by providing case studies, describing incidents when individuals caused breaches, rather than just providing

	as well as reassured by positive information.	opportunities associated with their behaviour. It is good to channel the attitude of individualists to the positive, such as appoint them to be the security facilitator.		security rules. Encourage them with positive and easy steps on information security. Less overcomplicated or negative vocabulary used (violation, failure etc.).
Organisational structure	Usually hierarchists have high positions in an organisation, therefore their roles, job scope and the level of security privilege should be made clear. They should be well informed about access privileges, security restrictions in sensitive areas, and how to handle sensitive information.	Not related *	The egalitarians are always prepared to help, therefore they should be reminded about the access privileges, security restrictions in sensitive areas, and how to handle sensitive information.	Not related*

*The fatalist and individualist reflect the low bond of social unit and low participation in group activities (Oltedal et al., 2004), thus organisational structure has less effect on people with these cultural views. They are better addressed with policy, process and procedures. On the other hand hierarchists and egalitarians have high bond of social unit and strong participation with group activities, thus organisational structure has a stronger influence on them to take part in information security management.

7.2 The Expert Background

Three experts in IT/ISM responded to the invitation to complete the questionnaire. Expert 1 has an academic and research background and is currently working in the higher education industry (Open University). She is a Reader in Computing in a university in UK which uses e-learning and is involved in Human-Centred Computing research within the same university. Expert 1 has always been aware and interested about information security aspects experience. Expert 2 has 20 years of experience in information security services. He is currently working as senior consultant in a computer organisation (Hewlett-Packard). He is a Certified Information Security Manager (CISM). He is in charge in governance, risk and compliance enterprise security services. Expert 3 is a Head of Security Governance, Risk and Compliance, DIAGEO and also a CISM.

Expert 1 represents the end-user, lecturers and IT experts in e-learning environment. Her academic and research background gives the academic expertise to review the illustration of research findings. Expert 2 and 3 represents the view from the practitioner side of information security. His background of work and experience provides the real-world view.

7.3 Findings of Expert Review Session

This section presents expert's comments on the findings. The section is organised into sub-sections according to the outlined objectives.

7.3.1 Practicality of Using Stakeholder's Cultural View in ISM

Both experts agreed that in addition to the use of technological control, security management could be enhanced by addressing the stakeholder's cultural view. They agreed that the model and related examples in the table indicate that considering cultural views in the training and policy developments may be able

to enhance the adoption of the guidance and policy and raise the awareness of the stakeholders' responsibilities towards information security.

The current reality is that people do not prefer to be classified and differentiated. There are potential equal opportunity and ethical issues to classify people into cultural views; especially in Western countries.

7.3.2 Degree to which Findings Reflect Reality

The proposed model is different from the typical ISM currently implemented. The current practice of ISM, specifically the guidelines and policy documents are different at two levels: technical support team and the end-users. Amongst the end-users the ethos of the guidelines is the same, except for different levels of responsibilities (for example, amongst the lecturers and students). It is unsure whether cultural views have been taken into account. Current approach is to encourage the people to think about how security can impact the organisation information or network. Whereas this research suggests that the culture view of an individual should be addressed, so that users feel more cared for and understand how their behaviour impacts on others.

The expert views that the research findings and the output model seem to be a useful approach. From the experts own experience and understanding, they provide some examples that reflect the illustration proposed.

'For individualists, raising awareness of the consequences is paramount. This is quite true for computing professionals who may think that they know the 'best' in terms of security and privacy. However, if they were made aware of the undesirable consequences and risks of even simple (unintended) actions, then it would help them to become sensitised to these really important issues of information security'.

Experts agreed that people have to be responsible for themselves. Good characters and views from each stakeholder's cultural view should remain and they have to be encouraged to eliminate the bad behaviour or activities by receiving awareness information corresponding to their cultural view group.

7.3.3 The Applicability of Research Findings

A review with experts revealed that the findings adequately reflect the behaviours needed to be emphasised; in controlling the targeted behaviour and perception of stakeholders (rather than having one solution for every cultural view), and the model developed might have practical relevance for the effectiveness of ISM standards. This indicates the applicability of the research findings.

7.3.4 Use of Research Findings in the Wider Context of Information Security Management

The experts commented that the use of cultural views in addressing people's behaviour towards information security seems useful and applicable in a variety of contexts. For example, it could be pertinent in developing guidelines for the use of mobile communications and mobile devices for workplace-related communications and (confidential) document storage. Other example given is providing different types of scenarios and case studies to the users during security awareness training session. This increases their understanding that different behaviours and perceptions can lead to threats however unintentional; and are likely to impact and be relevant to their job roles.

The experts also mentioned that the finding on the cultural view of stakeholders seems a cost-effective way of raising awareness of information security management amongst stakeholders covering methods for all different cultural views. The cost and effort seems practical in implementing the proposed model (e-learning ISM stakeholder's behaviour model).

7.4 Chapter Summary

This chapter presented feedback on the research findings obtained from the ISM experts. The feedback on the findings was positive. The illustration on control-ISM elements reflects the controls that can be applied to the stakeholder based on the cultural view. This finding/illustration has implications for the wider ISM context and potential in guiding the design of ISM elements. The experts' comments added to demonstrate the impact and practicality of the research.

8 DISCUSSION

This research has investigated how the ISM model, considering the people's behaviour, can be developed to help the e-learning provider to improve security in e-learning environment. The research has examined relevant existing literature on information security, e-learning and both in the context of Malaysia. Six multi-method studies have been conducted in two stages. The model dimensions and components are defined; and correlated and constructed as an E-Learning Stakeholders Information Security Vulnerability Model.

The research findings are discussed in the context of achieving the aim and objectives of this research, as well as how the advancement this research contributes to the literature.

8.1 Achievement of Research Aim and Objectives

The major aim of this research is to propose an approach to top management or providers of e-learning in public universities in Malaysia to improve the implementation and management of information security.

This research produced an E-Learning Stakeholders Information Security Vulnerability Model. The model consists of correlated dimensions that could help e-learning providers to target areas that need to be addressed which can enhance the implementation of ISM in e-learning in Malaysia. The objectives of research stated in Chapter 1 are as below:

1. To identify the information security issues in e-learning,
2. To identify threats and incidents in e-learning,
3. To define the current e-learning implementation and security in e-learning in Malaysia
4. To design an e-learning ISM human behaviour model (approach) appropriate to Malaysian characteristics

The first three objectives were intended to understand information security in e-learning, including in the context of Malaysia. As these three objectives were accomplished, it was found that people's culture and its impact needed to be understood before a suitable model could be developed. The first three objectives were achieved through the studies conducted in the first stage of data collection and analysis. The second stage of study addressed the cultural view of e-learning stakeholders and the correlated security threats and impact leading to the e-learning ISM model. The fourth objective was accomplished with the designed model.

8.1.1 Objective 1: To identify the information security issues in e-learning

The research conducted an online survey to identify the information security issues in e-learning and has found that users are not fully participating and are unaware of the security situation in e-learning. Users in the e-learning environment mostly come from a non-IT background. They perceive that e-learning security is embedded in the technology system and that the IT personnel solely are responsible for IT security. The findings have shown that though controls have been designed for security, people have not been made aware of their own responsibilities towards the security of e-learning. This is in accord with the literature review that highlighted security has been implemented in a top-down approach.

Generally the information security issues in any system are similar with the aim of ensuring the confidentiality, integrity and availability of data and information. However, the socio-technical environment differences have made e-learning different from other e-services. The obvious issue from studies and the literature review has indicated that e-learning stakeholders are fundamental to enhance the implementation of ISM in e-learning. Information security management requires participation by all users in the organisation. Effective security awareness programs need to be implemented which can help to increase users'

tolerance for preventive controls; by helping them understand what the threats and vulnerabilities in e-learning and how they originate.

8.1.2 Objective 2: To identify threats and incidents in e-learning

This research has identified a list of significant potential threats according to the applications used in e-learning and incidents which occurred in e-learning through the threat analysis and incident logging studies conducted in first stage of data collection and analysis. Both studies especially threats analysis study, have encompassed a lengthy task and has taken a great deal of time.

The result of the threats analysis reveals the potential threats according to the applications in e-learning. 21 applications, including the sub-applications, have been identified; in addition 18 types of threats were accordingly listed against the application. In the threats analysis, the likelihood of a threat occurring and its associated impact upon both the system and individual has been evaluated. This has resulted in the threats matrix, where different types of risk associated with each potential threats risk category for e-learning have been mapped. The matrix highlighting the vulnerabilities or threats versus the application can be seen in three meaningful risk groups: minor, major and critical. This threats matrix can be used to guide the stakeholders of e-learning on information security management to identify the possible threats and its level of risk at each application. Users of e-learning can use the threats matrix to comprehend the possible threat and risk when accessing e-learning applications and materials.

Through the incident logging study, this research found that information security incidents had occurred in the e-learning environment. Information security incident in education sector is not well discussed in literature. This may be due to the desire to preserve the reputation of the education institutions. Despite the low number of incidents reported, e-learning is not safe from threats. The incident logging study conducted in this research has identified that many types of breach were caused unintentionally by internal people. As an example, employees inside the respective organisations may be causing damage through

ignorance by policy violation or errors (Cobos 2009). It is found that most of the attacks are through the website.

The realisation of this objective has provided understanding that the internal users in an e-learning environment could be the main source of threats and it is important to address these stakeholders to deter security incidents. Hence it is a must to have a robust security policy which must be in place to educate and control the employees. Unintentional threats by internal people or employees often have a serious impact on the organisation, its customers and end users. In most cases reported, the employee, without realizing the harm or the impact, unknowingly causes information to leak or fall into the wrong hands.

8.1.3 Objective 3: To define the current e-learning implementation and security in e-learning in Malaysia

A study to investigate the current e-learning implementation in Malaysia's public universities has been carried out. The study using open-ended interviews also explored any security threats and incidents which occurred in the universities. The finding has revealed that Malaysia is still in the stage of focussing on the implementation and nurturing the use of e-learning among e-learning users in the public universities. In 2008, a dedicated e-learning committee was established to govern the e-learning implementation among the Malaysia public universities (Basir et al., 2010).

There is little interest or concern about information security in e-learning in Malaysian public universities. This is because e-learning users expect that security has been fully addressed and embedded in the IT system and infrastructure technology. This assumption made the issue of security less important to them, despite being aware that security is essential in e-learning. As e-learning security is a part of the security of the whole university system, protected by technological countermeasures, it inherits the threats and incidents of the latter.

A Malaysian newspaper (Ismail, 2011) has reported that cyber security incidents related to online fraud, including phishing and identity theft; has increased by 147 percent, compared to same period in 2010. The increase in cyber security incidents are associated with an increased rate of use of internet, higher number of internet users due rapid development and deployment of broadband infrastructure and the lack of security awareness among internet users. There are currently 17 million internet users in Malaysia (Computerworld, 2011). E-learning, as one of the cyber- or internet-based technologies is soon to be threatened if its security aspect is being left out. The level of security awareness among Malaysian internet users on cyberspace safety issues needs to be improved to keep up with the rapidly growing number of citizens. The current method to bring security awareness is by persuading from the top-down. Since this method has not been fully successful, this research argues that behavioural-based security control, which is more personal in nature, could be one of the many types of security awareness given.

The multi-method studies conducted in the first stage has provided insight on the security situations in e-learning. From the studies conducted, a list of threats for e-learning has been revealed. It is known that people can be susceptible to threats, therefore the understanding of the behaviour and perception of people towards security need to be understood. There is always a connection between technologies, people and process, as these are the three main components that complete the information security equation. It is interesting to look at the socio-technical approach which considered the people and their culture. This insight has led a focus on the culture held by individuals or stakeholders. The second stage of study is executed as an attempt to clarify whether the behaviour of individuals towards security can be predicted by understanding the cultural view that they might possess. Subsequently, their behaviour and perception can be influenced according to the expected behaviour.

This study conducted a threats and risk analysis of unintentional threats in e-learning by considering the cultural view of the stakeholders. The criticality of 15 unintentional threats was evaluated taking into account the business impact, the

influence of stakeholder cultural views on likelihood of threats and effectiveness of possible control.

In the analysis the author uses the understanding of e-learning functions and features to map out the likely system interactions of each stakeholder role. This helps to narrow down the possible unintentional threats each stakeholder role is likely to be exposed to. For each possible cultural view in each of the stakeholder roles, the likelihood of threat is valued using FMEA type logic. The cultural views used are from the Cultural Theory: Fatalism, Hierarchism, Individualism, and Egalitarianism. The effectiveness of control for each threat in the analysis is also evaluated taking into account of the cultural view. The combination of vulnerable cultural views and unsuitable controls increases the criticality of a particular threat.

This work supports the notion that information security should focus on people as much as technology and management. It reinforces the need to design information security management relevant to the end users. This study provides analytical evidence that the cultural view affects threat susceptibility, thus e-learning ISM should have controls that are relevant to the cultural view of the stakeholders.

This second stage of studies has brought out the dimensions needed to be constructed in the ISM model for e-learning.

8.1.4 Objective 4: To design e-learning ISM human behaviour model appropriate to Malaysian Characteristics

Upon completing the six multi-method studies, the dimensions and components for model development were correlated. An E-Learning Stakeholders Information Security Vulnerability Model that has a cultural view relevant to threat and control has been developed. The model has the four dimensions of threats, stakeholders, culture view and the control (ISM elements).

The threats for e-learning include the intentional and unintentional threats which have been achieved in this research. The stakeholders in e-learning include Top Management, E-Learning Centre Personnel, IT Personnel, Lecturers and Students which represent people with different cultural views. Each cultural view from the Cultural Theory has distinctive characteristics and behaviour. This research has found that the classification of stakeholders' perception and behaviour towards security can help in predicting the possible threats and vulnerabilities, thus can help in designing suitable ISM elements to use in preventing the vulnerabilities becoming threats and allowing attacks. Suitable controls that address and consider the culture characteristic and behaviour will lower the criticality of threats. These kinds of controls are more personalised and more likely to be observed by the stakeholder. A validated example is given here to illustrate how the cultural view among lecturers may lead to different ways to write the policy on data entry.

The objectives of this research were met and a model is proposed through this research. Review from the experts confirmed that the model developed is useful and can be applicable at all e-learning public universities in Malaysia and can be implemented as a guide in preparing an ISM for e-learning. The research has been unable to demonstrate specific guidelines for each stakeholder as it would have required more work with psychologists and communication expert. However, this research has brought out the beneficial and practical approach in addressing people in ISM.

This research has been conducted emphasising the validity, reliability and impact. The research reliability has been supported by the validation conducted using multi-method studies. The impact of this research can be seen from the contribution of knowledge on the e-learning and information security community. Positive feedback from the validation of this model has also reinforced the quality of this research.

8.2 Findings Implications to the Literature

The E-Learning Stakeholders Information Security Vulnerability Model is developed for e-learning provider. It serves as an integrative ISM model that aims to help the e-learning provider in understanding security culture view of stakeholder. This will help them manage the stakeholders and ensure the information security management take place.

In addition, the proposed model provides generic dimensions to ISM in e-learning, expected to assist in increasing the awareness and responsibilities of stakeholders towards securing the e-learning environment. This model also contributes in providing control to avoid the threats, usually known as preventive control. Preventive control is taking measures that would prevent the information from being damaged, altered, or stolen by identifying the possible threats and implementing the suitable control based on culture view of stake holders. This model can complement in the critical successful model by Kankanhalli (2003) and achieve successful security standards such as ISO/IEC27002.

This section discussed the implications based on the finding of this research in information security in e-learning and the Malaysian context.

8.2.1 For the Field of Information Security

Literature showed that the ISM standard is designed and implemented in such a way so that it is applied without considering the differences in people's behaviour and perception. However, behaviour and perception towards security varies according to the job tasks and organisational mission and vision. Rather than using the top-down approach, this research proposed a bottom-up approach. The research addressed the targeted behaviour and perception in security control design and implementation. This research suggests that the cultural view of stakeholders can be addressed when designing a security control. With this targeted control, awareness on their responsibility towards security will increase. This research has provided an alternative way of

addressing people's security responsibilities, by specifically addressing the targeted stakeholder behaviour and perception. This research improved the way security could be implemented. This research developed a model to guide on human risk management in e-learning which has been missing from the literature.

8.2.2 For the Field of E-Learning

At the moment, security has not been defined as one of the challenges in e-learning, though the interaction between the organisations, technical and socio-cultural areas has positioned the security issues in e-learning as one of the hidden challenges that need to be addressed. This research has enhanced the literature by emphasising that security is a challenge in e-learning. Since more functionality is presented to users, the e-learning environment becomes more complex, open and exposed to the information security threats.

This research has raised issues that the providers and the users need to be supported and guided in facing the challenges. This research has produced a list of threats in e-learning and the category of risks in e-learning, which can be used as guidance on the possibilities of threats and attacks that could happen in e-learning. The matrix of risk based on application has been designed and can be used as a reference by the e-learning provider. The threat analysis can be used by the e-learning provider to plan any necessary countermeasures. It helps in prioritising threats based on the category of threats risk and is able to guide efforts on control or countermeasures. The threats analysis made for the e-learning provider will contribute as a business intelligence and decision making tool and to make e-learning more secure, which will subsequently benefit the users.

This research has also classified the e-learning stakeholders according to the Cultural Theory in order to find the relationships between them and the threats. The threats and culture view relationship can provide guidance for staff selection, training requirements and countermeasures development. Different criteria could be set up for each stakeholder role.

8.2.3 For the Field of Social Technical System

This research reveals that the cultural view of stakeholders should be added as a factor in the information security effectiveness model. This research provides new insights into the influence of the culture view of stakeholders in the implementation of ISM in e-learning. The four types of stakeholder culture views were adopted in the ISM domain, providing a view that may also be used in other e-services studies to develop greater and deeper understanding on the behaviour of stakeholders regarding security. The proposed model provides descriptive measures that are applicable for other e-services.

8.2.4 For Malaysia Context

This research has provided the latest situation of e-learning implementation in Malaysia. This research has raised the need for the education industry, specifically e-learning, to be well addressed in security matters. Furthermore Malaysia has aimed to be an educational hub for international scholars (Morni et al., 2009). This research has specifically developed a model as a guideline on designing ISM for e-learning. This model has emphasised the awareness of security in e-learning. The model can be generalised and implemented not only for the purpose of e-learning but for the wider education industry in Malaysia.

8.3 Chapter Summary

This chapter compares the achievement of this research from the research aim and its objectives. The research has been conducted with multi-method studies that have provided many insights and had implications that are useful for the three different research fields.

This research has enriched the literature by:

- highlighting the need to address the cultural view of the stakeholder by considering the possible threats and designing countermeasures;

- discussions on information security management for e-learning which has provided additional knowledge to the information security and e-learning society; the process of securing an information system in e-learning requires the knowledge of the possible risks pertaining to the systems and available controls; and
- identifying that the behaviour of people can be understood and predicted and this research chose to classify people using the Cultural Theory.

This research has investigated how the ISM model, considering the people's behaviour, can be developed to help the e-learning provider to ensure the security of the e-learning environment. Through the studies conducted, the dimensions and components are correlated and constructed as an E-Learning Stakeholders Information Security Vulnerability Model.

9 CONCLUSION

This chapter presents the conclusion of the research reported in this thesis. The chapter summaries the research process and research findings, stating the contribution of this research to theoretical knowledge and its implication to practitioners as well as the limitations and future work which arise from this research.

9.1 Summary of Research Process

This research is in a relatively new subject area of security in e-learning in an intersection of existing knowledge in the main research areas. The research is complex, due to the study of people. This research consists of four phases.

Planning Phase:

This phase was a gap finding process which defined the research problem, objective and scope. The literature review on information security, e-learning and Malaysia context has revealed that not much research has been conducted on securing e-learning and the people aspect has not been well addressed in information security control. The output of this phase has led to people being the focus of research.

Data collection and analysis phase:

This phase reviewed the security issues in e-learning; a pilot study was conducted at the early stage of this research. The outcome of the pilot study showed existing knowledge from multiple sources should be used as source for data collection. The data collection and analysis were conducted in two stages.

The first stage, which consist Study 1, Study 2, Study 3 and Study 4, was carried out to better understand the e-learning security. The outcome from the first stage, such as insider and web as sources of threats, have given the second stage a focus of studies, which is to understand the cultural view in people and its impact to e-learning. The second stage, which consists of Study

5 and Study 6, produced a correlation between the cultural view and different types of responses to threats.

In this phase, six multi-method studies with online questionnaire, interview, and document analysis were conducted. The outcome from this phase contributed to the design of ISM model for e-learning.

Model Development Phase:

The multi-method studies and literature review produced findings that supported the selections of appropriate dimensions and components for the ISM model for e-learning that considers human risk and peoples' perspective. This was then validated by experts with ISM background. Experts review clarified the impact and practicality of the research findings.

Discussion and Conclusion Phase:

This phase reflected on the development of this research where research contribution, limitation and future work is stated.

9.2 Summary of Research Findings

The findings of this research are summarised as below:

- It is found that security in e-learning is not well addressed and user awareness of security in e-learning is still low. The study has considered the Malaysia context and found that similar issues occur in the country as to the rest of the world.

- This study highlights the importance of addressing the cultural view in preparing the information security management for e-learning. This study has shown that the possible cultural views posed by stakeholders might increase the chances of unintentional threats. This study also indicates cultural view as one dimension to consider in preparing appropriate and workable controls. Thus, insights from the research may provide a fresh

direction into information security through increased understanding and practice, in order to prevent the incident.

- The six multi-method studies have revealed useful findings to the community of e-learning. Among the key findings include the current situation of security in e-learning, list of threats for e-learning, Malaysia status of security in e-learning, and prediction on the possible cultural view of stakeholder, using Cultural Theory.

- The six multi-method studies and literature review have revealed the model dimensions: threat, stakeholders, cultural view and ISM elements as controls. These are dimensions that need to be considered by the top management of e-learning when establishing the security in e-learning.

- A model has been developed due to the 'something is missing' in security control implementation. Though there are controls and procedures to counter threats, attacks and incident continually take place. This research provides an overview and possibility to improve the approach of security culture cultivation by correlating the cultural view posed by the people in e-learning with different types of responses to security threats.

- A model has been developed to address the gap in literature regarding security in e-learning which would also fit in the Malaysia context. The model concentrates on people behaviour. The experts review agreed that this model is useful and applicable in a wider context.

9.3 Contribution to Theoretical Knowledge

The findings highlighted in the previous section have made an innovative contribution to the theoretical knowledge in the field of information security, e-learning and Malaysia. The outcome of the six studies and the model built

makes a constructive contribution to both academic research and practitioner. These contributions are discussed in the following sections.

9.3.1 Information Security Community

The outcome of this study provides new insight into the current state of information security management. It adds to the existing literature regarding people in information security management. This study is a significant endeavour in addressing the human risk of e-learning in inducing security threats to the e-learning environment. Previously more emphasis is made on the technological solutions. With this research, it explores the complexity of people towards information security. This study indicates the significance of individual cultural views in preparing information security management.

By addressing people's behaviour and their cultural view, a more prudent and robust security policy can be designed particularly to counter threats that employ social engineering techniques that manipulate people's behaviour and perceptions. Instead of using the technological control, this research provided insight into security control by addressing the peoples' cultural view. Awareness training that employs this finding will customize the training content according to the user's requirement, thus improving users' awareness in security, and will be able to avoid unnecessary incidents due to a lack of awareness such as unknowingly passing sensitive information to the wrong hand.

9.3.2 E-learning Community

This research has analytically focussed in the intersection of information security and e-learning where it enhanced the existing knowledge of both fields with the new findings about the security in e-learning environment from the users' perspective. The author had not found research in information security that adequately explored in detail people's cultural views on an e-learning environment. The correlation between cultural views of stakeholders in e-learning and type of responses of security threats helped the design of ISM for e-learning. The E-Learning Stakeholders Information Security Vulnerability

Model developed in this research can be used by the e-learning provider to improve the security of e-learning against the user/human risk perspectives. The e-learning provider would be able to design the necessary controls and solutions.

9.3.3 Other E-Services Community

The model can be replicated for other e-services such as e-commerce, e-government and e-banking. Although this model has initially been developed for the e-learning environment, the existing components such as stakeholders, application and process can easily be replicated, mapped, traced and analysed for other e-services.

9.3.4 Malaysia Context

This research also adds to the new knowledge on the e-learning and security in the Malaysia context. The security in e-learning in Malaysia has not been previously examined; therefore the findings represent a novel contribution to Malaysia in designing ISM for e-learning in Public universities.

In addition to that, emphasis on information security management in the education sector in this thesis reaffirms the importance of security and its impact on the education sector in Malaysia. Furthermore the government of Malaysia can use the model as a guideline in designing suitable training and education material to improve and increase security awareness among its net citizen.

9.4 Research Limitations

Although the research has achieved its aim and objectives, there are limitations in the research methodology process and findings.

In the research methodology, due to the difficulties to obtain data from people in the field, this research has been mainly a desk study. This research conducted

six multi-method studies which were too many to be executed within the time frame given. The data collection and data analysis process in this research were time consuming and demanding in terms of personal effort and cost.

In addition to that, analysing and interpreting the qualitative data is susceptible to researcher bias. This was moderated through peer to peer conversation and regular discussion and consultations. Each study were validated by information security and e-learning experts.

The research findings also have limitations. The findings have not been able to be tested in the real situation and real people due to the time constraints and the difficulties to find suitable contexts or case studies. Further adoption of research findings would require a pilot study, necessary planning, willing organisation as a test-bed and funds.

9.5 Future Work

Suggestions for future work include the following areas:

- Design an approach or tools to enable integration or to address the cultural view in controls in current ISM practice.

- Conduct a case study to prepare model development guidelines. This exercise might help to indicate the timeframe required to apply this model.

- To evaluate the comprehensibility and usefulness of the different set of guidelines from the perspective of different stakeholders, up to what extent do the stakeholders' experiences and comments match with the anticipated cultural views. These evaluations will help raise the confidence of the adoption of this proposed approach, its cost-effectiveness, usefulness and also its usability.

9.6 Research Conclusion

This research is a study that looks at security in e-services specifically on e-learning. It has uniquely highlighted the cultural view of people towards information security. As a result, an E-learning Stakeholders Information Security Vulnerability Model has been developed to help e-learning providers to manage the ISM. This research has spanned the information security management, e-learning and Malaysia towards something uniquely new and useful. The research finding provides a useful approach towards solving the missing human pieces (factor) in managing information security issue. The novelty of this research provides a contribution to substantive knowledge by identifying the cultural view of stakeholders at the core in identifying the possible threat or vulnerabilities and designing ISM elements of controls. This research has emphasised that information security is the responsibility of everyone and the way of enforcing this is by addressing cultural views. This contribution may help the research community to develop further guidelines to a complex and currently technically oriented area.

REFERENCES

Ninth Malaysia Plan 2006-2010, (2006), Government Printers, Kuala Lumpur.

A. Aziz, S. H., M.Yunus, A. S., A. Bakar, K. and B.Meseran, H. (2006), "Design and Development of Learning Management System at Universiti Putra Malaysia: A Case Study of e-SPRINT", *WWW 06: Proceedings of the 15th International Conference on World Wide Web,* May 23 - 26, 2006, Edinburgh, Scotland, ACM, New York, pp. 979--980.

Abu-Zineh, S. (2006), *Success Factors of Information Security Management: A Comparative Analysis between Jordanian and Finnish Companies* (MSc thesis), The Swedish School of Economics and Business Administration, Hanken, Sweden.

Adams, A. and Blandford, A. (2003), "Security and Online Learning: to Protect or Prohibit", in Ghaoui, C. (ed.) *Usability Evaluation of Online Learning Programs,* Information Science Publishing, London, pp. 331-359.

Albrechtsen, E. (2007), "A Qualitative Study of Users' View on Information Security", *Computers & Security,* vol. 26, no. 4, pp. 276-289.

Alfawaz, S., Nelson, K. and Mohannak, K. (2010), "Information Security Culture: A Behaviour Compliance Conceptual Framework", *Proceedings of the Eighth Australasian Conference on Information Security,* Vol. 105, Australian Computer Society, Inc., pp. 47-55.

Ali, A. (2004), "Issues & Challenges in Implementing E-learning in Malaysia", *Asia Pacific Knowledge Base on Open and Distance Learning,* [Online], available at:http://eprints.oum.edu.my

Alias, N. A. and Jamaludin, H. (2005), "The Aches of Online Distance Learning: A Synthesis of Three Malaysian Studies", *Asian Journal of Distance Education,* vol. 3, no. 2, pp. 48-54.

Allen, E. and Seaman, J. (2007), *Online Nation Five Years of Growth in Online Learning,* 1, Sloan Consortium, United States.

Allen, I. E. and Seaman, J. (2003), *Sizing the Opportunity: The Quality and*

Extent of Online Education in the United States, 2002 and 2003, Needham, Mass: Sloan-C, USA.

Allen, I. E. and Seaman, J. (2010), *Learning on Demand, Online Education in the United States, 2009,* Babson Survey Research Group & The Sloan Consortium, United States of America.

Allen, I. E., Seaman, J. and Alfred, P. (2005), *Growing by Degrees: Online Education in the United States, 2005,* Sloan Consortium, USA.

Al-Salihy, W., Ann, J. and Sures, R. (2003), "Effectiveness of Information Systems Security in IT Organizations in Malaysia", *Proceedings of 9th Asia-Pacific Conference on Communications,* Vol. 2, Sept 21-24, 2003, IEEE, pp. 716-720.

Altman, Y. and Baruch, Y. (1998), "Cultural Theory and Organisations: Analytical Method and Cases", *Organization Studies,* vol. 19, no. 5, pp. 769-785.

Al-Zubi, A. A. (2010), "Threats Sources Identification", *Canadian Journal on Network and Information Security,* vol. 1, no. 1, pp. 38-43.

Ambient Insight Research (2009), *US Self-Paced E-Learning Market,* Ambient Insight, Monroe, WA.

Anjo, R. (2009), *Design and Development of an Online Database System for Banks using MySQL and PHP* (Post-Graduate Diploma in Computer Science thesis), University of Jos, Nigeria.

Asia e-Learning Network (2004)*, Survey Research on E-learning in Asian Countries- Fiscal Year 2002, Country Specific Report- Malaysia*, available at: http://203.183.1.152/aen/content/relatedInfo/report.html (accessed June 18, 2009).

Asirvatham, D. (2005), "Effective E-learning Content Management and Delivery: Multimedia University's Experience", [Online], February 15, 2009 available at:http://asiapacific-odl2.oum.edu.my

Australian Standard (2000), *Handbook of Information security risk management*

– *HB23.*

Bagad, I. A. D. V. S. (2008), *Cryptography and Network Security,* Technical Publications.

Barbeau, M. (2005), "WiMax/802.16 Threat Analysis", *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks,* ACM Press, New York, USA, pp. 8-15.

Basir, H. M., Ahmad, A. and Noor, N. L. M. (2010), "Strategic Management of E-learning Implementation Programme in Malaysian Public Universities Issues on Policy and Key Initiatives", *International Conference on Science and Social Research (CSSR),* Dec 5-7 , 2010, Kuala Lumpur, Malaysia, IEEE, pp. 1143-1148.

Bernama (2010), *Cyber Attack in Malaysia Still under Control,* available at: http://biz.thestar.com.my/news/story.asp?file=/2010/2/9/business/20100209123001&sec=business (accessed June 20, 2011).

Blaikie, N. W. H. (2000), *Designing Social Research: The Logic of Anticipation,* Polity Press, Cambridge.

Boella, G. and van der Torre, L. (2006), "Security Policies for Sharing Knowledge in Virtual Communities", *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans,* vol. 36, no. 3, pp. 439-450.

Bruns, R., Dunkel, J. and von Helden, J. (2003), "Secure Smart Card-based Access to an E-learning Portal", *Proceedings of the 5th International Conference on Enterprise Information Systems,* Angers, France, ICEIS Press, pp. 167-172.

Bryman, A. (2008), *Social Research Methods,* 3rd Ed, Oxford University Press, New York.

Bryman, A. and Bell, E. (2007), *Business Research Methods,* Oxford University Press, USA.

Caelli, W. J., Longley, D. and Shain, M. (1989), *Information Security for Managers,* Groves Dictionaries, Inc., Stockton.

Cantoni, V., Cellario, M. and Porta, M. (2004), "Perspectives and Challenges in E-learning: Towards Natural Interaction Paradigms", *Journal of Visual Languages & Computing,* vol. 15, no. 5, pp. 333-345.

Casmir, R. (2005), *A Dynamic and Adaptive Information Security Awareness (DAISA) Approach* (PhD thesis), Stockholm University, Sweden.

Catherall, P. (2005), *Delivering E-learning for Information Services in Higher Education,* Chandos Publishing, Oxford.

Chang, S. E. and Ho, C. B. (2006), "Organisational Factors to the Effectiveness of Implementing Information Security Management", *Industrial Management & Data Systems,* vol. 106, no. 3, pp. 345-361.

Chang, S. E. and Lin, C. S. (2007), "Exploring Organizational Culture for Information Security Management", *Industrial Management & Data Systems,* vol. 107, no. 3, pp. 438-458.

Chaula, J. A., Yngstrom, L. and Kowalski, S. (2006), "Technology as a Tool for Fighting Poverty: How Culture in the Developing World Affect the Security of Information Systems", *Proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries (TEDC'06),* IEEE Computer Society.

Chiam, C. C., Lim, T. M., Norbaini, A. H. and Nur Azlin, O. (2011), "Towards Excellence in Higher Education–The Experience of Open University Malaysia (OUM)", *OUM i-Repository,* [Online], available at: http://eprints.oum.edu.my/568/.

Chin, P. (2004), *Using C&IT to Support Teaching,* RoutledgeFalmer, London.

CIA, (2011), *The World Factbook, Country Comparison: GDP (Purchasing Power Parity)*, available at: https://www.cia.gov/library/publications/the-world-factbook/rankorder/2001rank.html (accessed July 1, 2011).

CNII Portal, available at:http://cnii.cybersecurity.my/main/index.html

Cobos, E. (2009), *Information Security Incidents in E-services* (MSc thesis), Cranfield University, Cranfield.

Collis, J. and Hussey, R. (2009), *Business Research: A Practical Guide for Undergraduate and Postgraduate Students,* 3rd Ed, Palgrave Macmillan, Basingstoke.

Committee on National Security Systems (CNSS), (2006), *National Information Assurance (IA) Glossary.*

Computerworld (2011), *Malaysians need to increase security awareness*, available at: http://www.cybersecurity.my/en/knowledge_bank/news/2011/main/detail/2035/index.html (accessed June 22, 2011).

Concannon, F., Flynn, A. and Campbell, M. (2005), "What Campus-based Students Think about the Quality and Benefits of E-learning", *British Journal of Educational Technology,* vol. 36, no. 3, pp. 501-512.

Conole, G., Smith, J. and White, S. (2007), "A Critique of the Impact of Policy and Funding", in Conole, G. and Oliver, M. (eds.) *Contemporary Perspectives in E-learning Research Themes, Methods and Impact on Practice,* Routledge, London; pp. 38-54.

Corbeil, J. R. and Valdes-Corbeil, M. E. (2007), "Are You Ready for Mobile Learning?", *Educause Quarterly,* vol. 30, no. 2, pp. 51-58.

Creswell, J. W. (2009), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches,* Sage Publications, Inc.

CyberSecurity Malaysia, available at: http://www.cybersecurity.my.

CyberSecurity Press Release (2010), *ISMS Implementation by Critical National Information Infrastructure (CNII) to Enhance Information Security*, available at:http://www.cybersecurity.my/data/content_files/44/731.pdf?.diff=1281320820.

Davis, F. D. (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", *MIS quarterly,* vol. 13, no. 3, pp. 319-340.

Davis, F. D., Bagozzi, R. P. and Warshaw, P. R. (1989), "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models",

Management Science, vol. 35, no. 8, pp. 982-1003.

Denscombe, M. (2010), *The Good Research Guide: For Small-Scale Social Research Projects,* 4th Ed, McGraw-Hill, England.

Dhillon, G. and Backhouse, J. (2001), "Current Directions in IS Security Research: Towards Socio-Organisational Perspectives", *Information Systems Journal,* vol. 11, no. 2, pp. 127-153.

Dietinger, T. (2003), *Aspects of E-Learning Environments* (Doctor of Technical Sciences thesis), Institute for Information Processing and Computer Supported New Media (IICM), Graz University of Technology, Austria.

Douglas, M. and Wildavsky, A. (1983), *Risk and Culture,* University of California Press, Berkeley.

Eklund, J., Kay, M. and Lynch, H. M. (2003), *E-learning: Emerging Issues and Key Trends: A Discussion Paper,* Australian National Training Authority, Australia.

El-Khatib, K., Korba, L., Xu, Y. and Yee, G. (2003), "Privacy and Security in E-learning.", *International Journal of Distance Education Technologies,* vol. 1, no. 4, pp. 1-19.

Eloff, J. H. P. and Eloff, M. (2003), "Information Security Management: A New Paradigm", *Proceedings of SAICSIT: An Enablement through Technology,* South African Institute for Computer Scientists and Information Technologists, Republic of South Africa, pp. 130-136.

Evans, N. (2003), "Information Security Guideline for NSW Government–Part 1 Information Security Risk Management", *Office of Information and Communication Technology Sydney,* [Online], pp. Sept 18, 2008 available at:http://www.oict.nsw.gov.au/pdf/4.4

Finucane, M. L. and Holup, J. L. (2005), "Psychosocial and Cultural Factors Affecting the Perceived Risk of Genetically Modified Food: An Overview of the Literature", *Social Science & Medicine,* vol. 60, no. 7, pp. 1603-1612.

Folorunso, O., Ogunseye, O. S. and Sharma, S. K. (2006), "An Exploratory

Study of the Critical Factors Affecting the Acceptability of E-Learning in Nigerian Universities", *Information Management & Computer Security,* vol. 14, no. 5, pp. 496-505.

Fook, F. S., Kong, N. W., Lan, O. S., Atan, H. and Idrus, R. (2005), "Research in E-Learning in a Hybrid Environment-A Case for Blended Instruction", *Malaysian Online Journal of Instructional Technology,* vol. 2, no. 2, pp. 124-136.

Furnell, S. (2004), "Enemies Within: The Problem of Insider Attacks", *Computer Fraud & Security,* vol. 2004, no. 7, pp. 6-11.

Furnell, S. M. and Karweni, T. (2001), "Security Issues in Online Distance Learning", *VINE: The Journal of Information and Knowledge Management Systems,* vol. 31, no. 2, pp. 28-35.

Glaser, B. G. and Strauss, A. L. (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research,* Aldine de Gruyter, New York.

Goi, C. and Ng, P. Y. (2009), "E-Learning in Malaysia: Success Factors in Implementing E-Learning Program", *International Journal of Teaching and Learning in Higher Education,* vol. 20, no. 2, pp. 237-246.

Goldkuhl, G. and Lyytinen, K. (1982), "A Language Action View of Information Systems", M.Ginzberg , C. R. (ed.), in: *Proceedings of the 3rd International Conference on Information Systems,* Dec 13-15, AnnArbor, Mich., The Institute of Management Sciences, pp. 13-30.

Gollman, D. (1999), *Computer Security,* John Wiley & Sons Ltd, Chichester.

Google Scholar, available at: http://scholar.google.co.uk/.

Graf, F. (2002), "Providing Security for E-Learning", *Computers & Graphics,* vol. 26, no. 2, pp. 355-365.

Gunasekaran, A., McNeil, R. D. and Shaul, D. (2002), "E-learning: Research and Applications", *Industrial and Commercial Training,* vol. 34, no. 2, pp. 44-53.

Hamid, A. A. (2002), "E-Learning Is It The “E” or The Learning That Matters?", *The Internet and Higher Education,* vol. 4, no. 3-4, pp. 311-316.

Handy, C. B. (1993), *Understanding Organizations,* 4th Ed, Penguin Books Ltd., London.

Hassler, V. (2001), *Security Fundamentals for E-Commerce,* Artech House Inc, Norwood MA.

Help Net Security (2010)*, Top 10 Security Threats for 2011*, available at: http://www.net-security.org/secworld.php?id=10154 (accessed July 12, 2011).

Hill, C. W. L. and Jones, G. R. (2007), *Strategic Management: An Integrated Approach,* 8th Ed, Houghton Mifflin Company, Boston, USA.

Hofstede, G. (1983), "National Cultures in Four Dimensions: A Research-based Theory of Cultural Differences among Nations", *International Studies of Management & Organization,* vol. 13, no. 1/2, pp. 46-74.

Hofstede, G. H., Hofstede, G. J. and Minkov, M. (2010), *Cultures and Organisations: Software for the Mind: Intercultural Cooperation and Its Important for Survival,* 3rd Ed, McGraw-Hill Professional, USA.

Holloway, I. (1997), *Basic Concepts for Qualitative Research,* Wiley-Blackwell, Oxford.

Hunker, J. and Probst, C. W. (2011), "Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques", *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* vol. 2, no. 1, pp. 4-27.

Hussey, J. and Hussey, R. (1997), *Business Research: A Practical Guide for Undergraduate and Postgraduate Students,* Macmillan, Basingstoke.

Hylton, B. and Lewis, S. (2006)*, Literature Searching Guidelines Checklist*, available at: http://www.oxfordradcliffe.nhs.uk/research/researchers/news/documents/LiteratureSearchingGuidelinesChecklist.pdf (accessed May 28, 2008).

Iivari, J. and Hirschheim, R. (1996), "Analysing Information Systems Development: A Comparison and Analysis of Eight IS Development Approaches", *Information Systems,* vol. 21, no. 7, pp. 551-575.

InfoSecurity.com (2010), *Malaysia Sees Cybersecurity Industry as Economic Engine*, available at: http://www.infosecuritymagazine.com/view/13664/malaysia-sees-cybersecurity-industry-as-economic-engine/ (accessed Jan 29, 2011).

ISACA (2006), *CISA Review Manual 2006. Information Systems Audit and Control Association* .

M. K. Ismail. (2011) "Insiden keselamatan siber meningkat 147% - 7,404 kes termasuk cubaan dapatkan maklumat sensitive sepanjang", *Utusan Malaysia*.

ISO 17799, *ISO/IEC 17799:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management*, available at: http://www.iso.org/iso/catalogue_detail?csnumber=39612.

Jackson, S. (2010), "A Cultural Theory Analysis of Information Systems Adoption", *AMCIS 2010 Proceedings,* August 12-15, Lima, Peru, Association for Information Systems AIS Electronic Library (AISeL), pp. Paper 275.

Jain, K. K. and Ngoh, L. B. (2003), "Motivating Factors in E-learning - A Case Study of UNITAR", *e-journal,* [Online], vol. 4, no. 1, pp. June 21, 2008 available at:http://www.studentaffairs.com/ejournal/Winter_2003/e-learning.html

Jalal, A. and Zeb, M. A. (2008), "Security Enhancement for E-learning Portal", *International Journal of Computer Science and Network Security,* vol. 8, no. 3, pp. 41-45.

James, H. L. (1996), "Managing Information Systems Security: A Soft Approach", *Information Systems Conference of New Zealand (Proceedings),* Oct 30-31, Palmerston North , New Zealand, Published by the IEEE Computer Society, pp. 10-20.

Jankowicz, A. D. (2005), *Business Research Projects,* 4th Ed, Thomas

Learning, Singapore.

Johnson, R. D., Hornik, S. and Salas, E. (2008), "An Empirical Examination of Factors Contributing to the Creation of Successful E-Learning Environments", *International Journal of Human-Computer Studies,* vol. 66, no. 5, pp. 356-369.

Jung, B., Han, I. and Lee, S. (2001), "Security Threats to Internet: A Korean Multi-Industry Investigation", *Information & Management,* vol. 38, no. 8, pp. 487-498.

Kang, G. D. and James, J. (2004), "Service Quality Dimensions: An Examination of Grönroos's Service Quality Model", *Managing Service Quality,* vol. 14, no. 4, pp. 266-277.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y. and Wei, K. K. (2003), "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management,* vol. 23, no. 2, pp. 139-154.

Karim, M. R. A. and Hashim, Y. (2004), "The Experience of the E-Learning Implementation at the Universiti Pendidikan Sultan Idris, Malaysia", *Malaysian Online Journal of Instructional Technology,* vol. 1, no. 1, pp. 50-59.

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005), "Information Systems Security Policies: A Contextual Perspective", *Computers & Security,* vol. 24, no. 3, pp. 246-260.

Karyda, M., Kokolakis, S. and Kiountouzis, E. (2004), "Information Systems Security and the Structuring of Organisations", *Proceedings of the 7th International Conference on the Social and Ethical Impacts of Information and Communication Technologies (ETHICOMP 2004),* Syros, Greece, pp. 451-61.

Kennedy, A. A. and Deal, T. E. (1982), *Corporate Cultures: The Rites and Rituals of Corporate Life,* Addison-Wesley Publishing Company, Reading, Massachusetts.

Kennedy, G. (2002), "E-Learning Intellectual Property Issues In E-Learning",

Computer Law & Security Report, vol. 18, no. 2, pp. 91-98.

Khalid, M., Yusof, R., Tian, H. C., Yunus, M. R. M. and Ono, O. (2006), "Effective Teaching of Control Systems Using an Expert System Based Virtual Laboratory Systems", *Innovative ASEAN: Creating ASEAN Competitiveness through Innovation, Sciences, and Technology* , LIPI Press, Jakarta, Indonesia, pp. 43-58.

Khan, B. H. (2004), "People, Process and Product Continuum in E-learning: The E-learning P3 Model", *Educational Technology,* vol. 44, no. 5, pp. 33-40.

Konrad, K., Fuchs, G. and Barthel, J. (1999), "Trust and Electronic Commerce-More than A Technical Problem", *Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems,* IEEE, pp. 360-365.

Koswanage, N. (2011), *Malaysia Tries to Stop Threatened Cyber Attack*, available at: http://www.reuters.com/article/2011/06/15/us-cyber-malaysia-idUSTRE75E05N20110615 (accessed June 16, 2011).

Kowalski, S. (1994), *IT Insecurity: A Multi-Disciplinary Inquiry* (PhD thesis), Department of Computer and Systems Sciences, University of Stockholm and Royal Institute of Technology, Stockholm.

Kritzinger, E. and von Solms, S. H. (2006), "E-learning: Incorporating Information Security Governance", *Informing Science: International Journal of an Emerging Transdicipline,* vol. 3, pp. 319-325.

Langford, I. H., Georgiou, S., Bateman, I. J., Day, R. J. and Turner, R. K. (2000), "Public Perceptions of Health Risks from Polluted Coastal Bathing Waters: A Mixed Methodological Analysis using Cultural Theory", *Risk Analysis: An International Journal,* vol. 20, no. 5, pp. 691-704.

Legal Information Institute (1992), *Definitions, Cornell University Law School*, available at: http://www.law.cornell.edu/uscode/44/3542.html (accessed July 2011).

Lim, C. C. and Jin, J. S. (2006), "A Study on Applying Software Security to Information Systems: E-Learning Portals", *Int. Journal of Computer Science and Network Security,* vol. 6, no. 3B, pp. 162-166.

Lima, M. L. and Castro, P. (2005), "Cultural Theory Meets the Community: Worldviews and Local Issues", *Journal of Environmental Psychology,* vol. 25, no. 1, pp. 23-35.

Lingenfelter, D. (2011), *2011 Security Threats*, available at: http://blog.maas360.com/archives/security-information/2011-security-threats/ (accessed July 12, 2011).

Liu, A., Hodgson, G. and Lord, W. (2010), "Innovation in Construction Education: The Role of Culture in E-learning", *Architectural Engineering and Design Management,* vol. 6, no. 2, pp. 91-102.

Lyytinen, K. (1987), "Different Perspectives on Information Systems: Problems and Solutions", *ACM Computing Surveys (CSUR),* vol. 19, no. 1, pp. 5-46.

Mamadouh, V. (1999), "Grid-Group Cultural Theory: An Introduction", *GeoJournal,* vol. 47, no. 3, pp. 395-409.

Marris, C., Langford, I. and O'Riordan, T. (1996), *Integrating Sociological and Psychological Approaches to Public Perceptions of Environmental Risks: Detailed Results from A Questionnaire Survey,* Centre for Social and Economic Research on the Global Environment, University of East Anglia, Norwich, England.

Mars, G. (1996), "Human Factor Failure and the Comparative Structure of Jobs: The Implications for Risk Management", *Journal of Managerial Psychology,* vol. 11, no. 3, pp. 4-11.

Marshall, S. and Mitchell, G. (2007), "Benchmarking International E-learning Capability with the E-learning Maturity Model", *Proceedings of EDUCAUSE in Australasia,* 29 April- 2 May, Melbourne, Australia.

Mason, R. and Rennie, F. (2006), *E-learning : The Key Concepts,* Routledge, Abingdon, Great Britain.

McDermott, R. E., Mikulak, R. J. and Beauregard, M. R. (2009), *The Basics of FMEA,* 2nd Ed, Productivity Press Taylor & Francis Group, New York, USA.

McPherson, M. and Nunes, J. (2004), "The Role of Tutors as An Integral Part of

Online Learning Support", *European Journal of Open and Distance Learning,* [Online], available at: http://www.eurodl.org/index.php?tag=120&article=244&article=105.

Meier, J. D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R. and Murukan, A. (2003), *Improving Web Application Security: Threats and Countermeasures,* Microsoft Press.

Merchant Glossary (2009), *E-Commerce*, available at: http://www.merchantglossary.com/?page_id=82 (accessed June 18, 2009).

Microsoft Technet (2009), *Security Threats*, available at: http://technet.microsoft.com/en-us/library/cc723507.aspx (accessed May 21, 2009).

Mohamed, M. and Appalanaidu, U. (1998), "Information Systems for Decentralisation of Development Planning: Managing the Change Process", *International Journal of Information Management,* vol. 18, no. 1, pp. 49-60.

MOHE (2010), *Students Statistic Report Macro Data of Higher Education*, available at: http://www.mohe.gov.my/web_statistik/statistik2010/BAB1_DATA_MAKRO_PENGAJIAN_TINGGI.pdf (accessed June 2, 2010).

Morni, F., Talip, M. S. A., Bujang, F. and Jusoff, K. (2009), "APEX University: Is it the Malaysian Way Forward?", *International Conference on Computer Technology and Development,* Vol. 2, 526, IEEE, pp. 523.

Morrison, D. (2003), *E-learning Strategies: How to Get Implementation and Delivery Right First Time,* John Wiley & Sons, Inc., New York, USA.

MyCERT CyberSecurity Malaysia (2010), *Incident Statistic*, available at: www.cybersecurity.my (accessed June 18, 2011).

Nagy, A. (2005), "The Impact of E-Learning", in Bruck, P. A., Buchholz, A., Karssen, Z., et al (eds.) *E-Content: Technologies and Perspectives for the European Market,* Springer Verlag, Berlin, pp. 79-96.

National Higher Education Action Plan 2007-2010 (2007), *Triggering Higher*

Education Transformation, available at: http://www.mohe.gov.my/transformasi/images/1_bi.pdf.

Neuman, W. L. (2005), *Social Research Methods: Quantitative and Qualitative Approaches,* 6th Ed, Pearson Education, California.

News Straight Times (2009), *Growing Dependence on ICT Fuels Problem*, available at: www.cybersecurity.org.my/en/knowledge_bank/news/2009/main/detail/1809/index.html+Growing+dependence+on+ICT+fuels+problem+16+November+2009+(The+Star) (accessed June 11, 2010).

Norman, S. and Da Costa, M. (2003), "Overview of e-learning Specifications and Standards", *Open Learning Agency, and Eduspecs Technical Liaison Office*.

Nosworthy, J. D. (2000), "Implementing Information Security in the 21st century – Do you have the balancing factors?", *Computers and Security,* vol. 19, no. 4, pp. 337-347.

Oltedal, S., Moen, B. E., Klempe, H. and Rundmo, T. (2004), "Explaining Risk Perception: An Evaluation of Cultural Theory", *Trondheim: Norwegian University of Science and Technology,* vol. 85, pp. 1-33.

Open Web Application Security Project (2009), *Open Web Application Security Project*, available at: http://owasp.blogspot.com (accessed July 21, 2009).

Palvia, S. C. J. and Sharma, S. S. (2007), "E-Government and E-Governance: Definitions/Domain Framework and Status around the World", A. Agarwal, V. V. R. (ed.), in: *5th International Conference on E-governance (ICEG),* India, pp. 1-12.

Parker, D. B. (1981), *Computer Security Management,* Reston Pub. Co., United States.

Pfleeger, C. P. and Pfleeger, S. L. (2007), *Security in Computing,* 4th Ed, Prentice Hall, New Jersey.

Portal MOHE (2010), *Public Higher Learning Institutions*, available at:

http://www.mohe.gov.my/portal/institusi/ipta.html (accessed June 18, 2010).

Putted, M. (2007), "E-Learning in Malaysian Public Universities: Case Studies of Universiti Kebangsaan Malaysia and Universiti Teknologi Malaysia", *1st International Malaysian Educational Technology Convention,* 2-5 November 2007, Johor Bahru, Malaysia.

Raitman, R., Ngo, L. and Augar, N. (2005), "Security in the Online E-Learning Environment", 706 (ed.), in: *Fifth IEEE International Conference on Advanced Learning Technologies,* IEEE Computer Society, Washington DC, USA, pp. 702.

Raja Maznah, R. (2004), "E-learning in Higher Education Institutions in Malaysia", *E-mentor,* vol. 5, no. 7, pp. 72-75.

Ramayah, T. and Jantan, M. (2004), "Technology Acceptance: An Individual Perspective Current and Future Research in Malaysia", *Review of Business Research,* vol. 2, no. 1, pp. 103-111.

Ramim, M. and Levy, Y. (2006), "Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University", *Journal of Cases on Information Technology,* vol. 8, no. 4, pp. 24-34.

Richardson, A. and Koswanage, N. (2011)*, Hackers Strike Malaysian Websites for A 2nd Day*, available at: http://in.reuters.com/article/2011/06/17/idINIndia-57755820110617 (accessed June 17, 2011).

Robbins, S. and Judge, T. (2008), *Essentials of Organisational Behavior,* 9th Ed, Prentice Hall, US.

Robson, C. (2002), *Real World Research: A Resource for Social Scientists and Practitioner-Researchers,* 2nd Ed, Blackwell Publications, Oxford.

Rosenberg, M. J. (2001), *E-learning Strategies for Delivering Knowledge in the Digital Age,* McGraw-Hill, New York.

Rossman, M. H. and Rossman, M. E. (2008), "Community Building in Distance Education: An International Perspective", *International Journal of Excellence in E-learning,* vol. 1, no. 1, pp. 31-41.

Rousseau, D. M. (1977), "Technological Differences in Job Characteristics, Employee Satisfaction, and Motivation: A Synthesis of Job Design Research and Sociotechnical Systems Theory", *Organizational Behavior and Human Performance,* vol. 19, no. 1, pp. 18-42.

Rowley, J. (2006), "An Analysis of the E-service Literature: Towards A Research Agenda", *Internet Research,* vol. 16, no. 3, pp. 339-359.

Ruighaver, A., Maynard, S. and Chang, S. (2007), "Organisational Security Culture: Extending the End-User Perspective", *Computers & Security,* vol. 26, no. 1, pp. 56-62.

Samuels, R. (2004), "The Future Threat to Computers and Composition: Nontenured Instructors, Intellectual Property, and Distance Education", *Computers and Composition,* vol. 21, no. 1, pp. 63-71.

Saxena, R. (2004), "Security and Online Content Management: Balancing Access and Security", *12th biennial Victorian Association for Library Automation (VALA) Conference and Exhibition,* Melbourne, Australia.

Scacchi, W. (2004), "Socio-Technical Design", *The Encyclopaedia of Human-Computer Interaction,* , pp. 656-659.

Schein, E. H. (2010), *Organizational Culture and Leadership,* 4th Ed, Jossey-Bass, San Francisco.

Schneier, B. (2000), *Secrets and Lies: Digital Security in A Networked World,* 1st Ed, John Wiley & Son, New York.

Scupola, A. (2008), "Conceptualizing Competences in E-Services Adoption and Assimilation in SMEs", *Journal of Electronic Commerce in Organisations,* vol. 6, no. 2, pp. 78-91.

SecurITy Pub (2010), *Top 10 Security Threats for 2011*, available at: http://www.thesecuritypub.com/top-10-security-threats-for-2011 (accessed July 12, 2011).

Sheth, J. N. and Sharma, A. (2007), "E-Services – A Framework for Growth", *Journal of Value Chain Management,* vol. 1, no. 1-2, pp. 7-12.

Siponen, M. and Willison, R. (2009), "Information Security Management Standards: Problems and Solutions", *Information & Management,* vol. 46, no. 5, pp. 267-270.

Stallings, W. (2007), *Network Security Essentials: Applications and Standards,* 3rd Ed, Prentice Hall, New Jersey.

The ISO 27000 Directory (2009), *An Introduction to ISO 27001, ISO 27002....ISO 27008*, available at: http://www.27000.org/ (accessed July 6, 2009).

The Star (2011), *Drastic Rise in Cyber Crimes*, available at: http://www.cybersecurity.my/en/knowledge_bank/news/2011/main/detail/2007/index.html (accessed June 11, 2011).

Thompson, A. A., and Strickland, A. J. (2001), *Crafting and Executing Strategy: Text and Readings,* McGraw-Hill, New York.

Thompson, M., Ellis, R. J., Ellis, R. and Wildavsky, A. B. (1990), *Cultural Theory,* Westview Press.

Tipton, H. F. and Krause, M. (2007), *Handbook of Information Security Management,* 6th Ed, CRC Press, Inc.

Triacca, L., Bolchini, D., Botturi, L. and Inversini, A. (2004), "MiLE: Systematic Usability Evaluation for E-learning Web Applications", *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications,* Cite seer, pp. 4398-4405.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2006), "Formulating Information Systems Risk Management Strategies through Cultural Theory", *Information Management & Computer Security,* vol. 14, no. 3, pp. 198-217.

Tyson, S. and Jackson, T. (1992), *The Essence of Organisational Behaviour,* Prentice Hall.

Underwood, M. (2010), *Seven Overlooked Network Security Threats for 2011*, available at: http://www.techrepublic.com/blog/networking/seven-overlooked-

network-security-threats-for-2011/3637 (accessed July 12, 2011).

Von Solms, R. (1998), "Information Security Management (1): Why Information Security Is So Important", *Information Management & Computer Security,* vol. 6, no. 4, pp. 174-177.

Vroom, C. and Von Solms, R. (2004), "Towards Information Security Behavioural Compliance", *Computers & Security,* vol. 23, no. 3, pp. 191-198.

Wagner, N., Hassanein, K. and Head, M. (2008), "Who is Responsible for E-Learning Success in Higher Education? A Stakeholders' Analysis", *Educational Technology & Society,* vol. 11, no. 3, pp. 26-36.

Walker, G. H., Stanton, N. A., Salmon, P. M. and Jenkins, D. P. (2008), "A Review of Sociotechnical Systems Theory: A Classic Concept for New Command and Control Paradigms", *Theoretical Issues in Ergonomics Science,* vol. 9, no. 6, pp. 479-499.

Warren, M. and Hutchinson, W. (2003), "Information Security-An E-learning Problem", W.Zhou et al. (ed.), in: *Proceeding of the Second International Conference on Advances in Web-Based Learning--(ICWL 2003),* August 18-20, 2003, Melbourne, Australia, Springer, Verlag Berlin Heidelberg, pp. 21-26.

Weippl, E. R. (2005a), *Security in E-learning,* Springer Science + Business Media Inc., USA.

Weippl, E.R., (2005b), *Security in E-learning*, ACM, New York, USA.

Whitman, M. E. (2003), "Enemy At The Gate: Threats to Information Security", *Communications of the ACM,* vol. 46, no. 8, pp. 91-95.

Whitman, M. E. and Mattord, H. J. (2011), *Principles of Information Security,* 4th Ed, Cengage Learning, USA.

Wong, D. (2006), "Fulltime Students' and Working Adults' Perceptions of E-learning in Malaysia", *Asian Journal of Distance Education,* vol. 4, no. 1, pp. 67-84.

Workman, M. (2007), "Gaining Access With Social Engineering: An Empirical Study of The Threat", *Information Systems Security,* vol. 16, no. 6, pp. 315-331.

Yang, C., Lin, F. O. and Lin, H. (2002), "Policy-based Privacy and Security Management for Collaborative E-education Systems", *Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002),* pp. 501–505.

Yavas, U. (1992), "Constraints on The Application of Management Know-How in The Third World", *International Journal of Management,* vol. 9, no. 1, pp. 17-25.

Yee, G., Xu, Y., Korba, L. and El-Khatib, K. (2006), "Privacy and Security in E-Learning", in Shih, T. and Hung, J. (eds.) *Future Directions in Distance Learning and Communication Technologies,* Idea Group Inc., London, pp. 52-75.

Yong, J. (2007), "Digital Identity Design and Privacy Preservation for E-Learning", *Proceeding of the 11th International Conference on Computer Supported Cooperative Work in Design,* IEEE, pp. 858-863.

Yunos, Z. (2008), *The Reality of Cyber-Threats Today*, available at: http://www.cybersecurity.my/data/content_files/13/420.pdf (accessed Jan 22, 2011).

Zhang, D. and Nunamaker, J. F. (2003), "Powering E-learning in The New Millennium: An Overview of E-learning and Enabling Technology", *Information Systems Frontiers,* vol. 5, no. 2, pp. 207-218.

Appendix A Survey Questionnaire

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

USER BACKGROUND

There are six questions in this sections.

1. Please select the age group that you belong to?

- ○ 18-24
- ○ 25-34
- ○ 35-44
- ○ 45-54
- ○ 55-65
- ○ Over 65

2. Please select your computer literacy level.

- ○ Low
- ○ Medium
- ○ High

3. Please select your information security awareness level.

- ○ Low
- ○ Medium
- ○ High

4. What is your role within the institution?

- ○ Management
- ○ Instructor/Facilitator/Lecturer
- ○ IT Personnel
- ○ Other (please specify)

5. Does the institution that you're currently working at offer an e-learning environment?

- ○ Yes
- ○ No

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

6. How long have you been working in this e-learning environment / institution?

- ○ Less than 1 year
- ○ Between 1- 5 years
- ○ Between 6-10 years
- ○ More than 10 years

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INSTITUTION BACKGROUND

There are five questions in this section.

7. Please select your institution category:

- ○ Higher Education Institution
- ○ Further Education Institution
- ○ Training Institution

8. Which type of e-learning does your institution adopt? (you can choose more than one answer)

- ☐ Using technology asynchronously only as tools to support or supplement a traditional (face to face) learning
- ☐ Using technology asynchronously and synchronously as tools to support or supplement a traditional (face to face) learning
- ☐ Using technology asynchronously and synchronously to deliver a learning course (completely online)

9. How many employees does this institution have?

- ○ Less than 100
- ○ Between 100-500
- ○ Between 500-1000
- ○ More than 1000

10. How many students /clients does this institution have?

- ○ Less then 1000
- ○ Between 1000-4999
- ○ Between 5000-9999
- ○ More 10 000

11. How long has the institution been operating an e-learning environment?

- ○ Less than 1 year
- ○ Between 1- 5 years
- ○ Between 6-10 years
- ○ More than 10 years

Your contribution is highly appreciated. Please continue answering the following questions.

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INFORMATION SECURITY THREATS

12. Please indicate your level of agreement with the following statements on information security threats in e-learning institutions.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
E-learning environment is prone to information security threats	○	○	○	○	○
My e-learning institution is highly secured	○	○	○	○	○
My e-learning institution has information that is highly confidential	○	○	○	○	○
My e-learning institution would face significant business disruption, if the information is corrupted	○	○	○	○	○
My e-learning institution would face significant business disruption, if the information is not available	○	○	○	○	○
My e-learning institution spends a lot on security controls	○	○	○	○	○
My e-learning institution spends a lot on security solutions and recovery	○	○	○	○	○
Good security management practices are important in ensuring a high level of security awareness amongst staff and students	○	○	○	○	○
Good security management is important in ensuring the successful implementation of appropriate security controls	○	○	○	○	○

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

13. Please indicate your percentage level of concern about the following information security related issues and challenges in e-learning institution.

	Extremely Concern (100%)	Concern (75%)	Some Concern (50%)	Minimal Concern (25%)	Not A Concern (0 %)
Malicious code infection (viruses, Trojan horse, worms)	○	○	○	○	○
Loss of privacy / confidentiality (abuse or misuse of data)	○	○	○	○	○
Electronic exploits/tools (cracking, eavesdropping, spoofing,)	○	○	○	○	○
System unavailability (Denial of Service (DOS), natural disasters, power interruptions, bugs)	○	○	○	○	○
Employee misconduct involving information systems	○	○	○	○	○
Spam	○	○	○	○	○
Misconduct involving third parties with access to information system	○	○	○	○	○
Theft of proprietary information	○	○	○	○	○

Other (please specify)

Your contribution is highly appreciated. Please continue answering the following questions.

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INFORMATION SECURITY THREATS

Your contribution is highly appreciated. Please continue answering the following questions.

14. Please indicate the frequency your institution has been attacked by the following Intentional (Malicious) Threats within the last 12 months.

	Hundreds a day	Several a day	Once a day	Once a week	Roughly once a month	A few	Only Once	Never	Unknown
Virus- Malicious software that attaches itself to other software	○	○	○	○	○	○	○	○	○
Worm- Malicious software which is a stand alone application that can replicate itself without intervention	○	○	○	○	○	○	○	○	○
Spoofing- Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges, so as to obtain access to other computers on the network	○	○	○	○	○	○	○	○	○
Masquerade -Accessing a computer by pretending to have an authorized user identity	○	○	○	○	○	○	○	○	○
Sequential Scanning- Sequentially testing passwords/authentication codes until one is successful	○	○	○	○	○	○	○	○	○
Dictionary Scanning - Scanning through a dictionary of commonly used passwords/authentication codes until one is successful	○	○	○	○	○	○	○	○	○
Digital Snooping- Electronic monitoring of digital networks to uncover passwords or other data	○	○	○	○	○	○	○	○	○
Shoulder Surfing-Direct visual observation of monitor displays or keyboards to obtain access passwords	○	○	○	○	○	○	○	○	○
Scavenging -Dumpster Diving- Accessing discarded trash to obtain passwords and other data	○	○	○	○	○	○	○	○	○
Scavenging -Browsing- Usually automated scanning of large quantities of unprotected data (discarded media or online "finger" type commands) to obtain clues as to how to achieve access	○	○	○	○	○	○	○	○	○
Spamming -Overloading a system with incoming message or other traffic to cause system crashes/ buffer overflows	○	○	○	○	○	○	○	○	○
Tunnelling -Any digital attack that attempts to	○	○	○	○	○	○	○	○	○

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

very low level system functions (e.g., device drivers, OS kernels)

15. Please indicate the frequency your institution has been attacked by the following Unintentional (Accidental)Threats within the last 12 months.

	Hundreds a day	Several a day	Once a day	Once a week	Roughly once a month	A few	Only Once	Never	Unknown
Equipment Malfunction -Hardware operates in abnormal, unintended mode	○	○	○	○	○	○	○	○	○
Software Malfunction- Software behaviour is in conflict with intended behaviour	○	○	○	○	○	○	○	○	○
Human Error -Trap Door (back door) - System access for developers inadvertently left available after software delivery	○	○	○	○	○	○	○	○	○
Human Error -User/Operator Error- Inadvertent alteration, manipulation or destruction of programs, data files or hardware	○	○	○	○	○	○	○	○	○

16. Please indicate the frequency your institution has been attacked by the following Physical Threats within the last 12 months.

	Hundreds a day	Several a day	Once a day	Once a week	Roughly once a month	A few	Only Once	Never	Unknown
Fire damage - Physical destruction of equipment due to fire or smoke damage	○	○	○	○	○	○	○	○	○
Water damage - Physical destruction of equipment due to water (including sprinkler) damage	○	○	○	○	○	○	○	○	○
Power loss -Computers or vital supporting equipment fail due to lack of power	○	○	○	○	○	○	○	○	○
Natural Disaster - Physical destruction of equipment due to floods, tornados, earthquake or lightning	○	○	○	○	○	○	○	○	○

Your contribution is highly appreciated. Please continue answering the following questions.

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INFORMATION SECURITY THREATS

Your contribution is highly appreciated. Please continue answering the following questions.

17. Which incidents were most disruptive to the e-learning environment in the last 12 months?

	Very Major	Major	Minor	Very Minor	Insignificant	Unknown
Installation / use of unauthorised software	○	○	○	○	○	○
Use of institution computing resources for illegal or illicit communications or activities (porn surfing, e-mail harassment)	○	○	○	○	○	○
Abuse of computer access controls	○	○	○	○	○	○
Unauthorised access by outsiders	○	○	○	○	○	○
Physical theft, sabotage or intentional destruction of computing equipment	○	○	○	○	○	○
Electronic theft, sabotage or intentional destruction / disclosure of proprietary data or information	○	○	○	○	○	○
Viruses infection or disruptive software	○	○	○	○	○	○
Denial of service	○	○	○	○	○	○
System failure or data corruption	○	○	○	○	○	○

Other (please specify)

18. How much disruption to the e-learning environment did the worst security incident cause?

- ○ More than a month and very major disruption
- ○ Between a week and a month and major or very major disruption
- ○ Between a week and a month, but only minor disruption
- ○ Between a day and a week and very major disruption
- ○ Between a day and a week and major disruption
- ○ Between a day and a week but only minor disruption
- ○ Less than a day, but major or very major disruption
- ○ Less than a day and minor disruption
- ○ No interruption
- ○ Insignificant
- ○ Unknown

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

19. What was the direct financial losses caused by security incidents in the e-learning environment in the last 12 months?

- ○ Nothing
- ○ Less than £1,000
- ○ Between £1,000-£10,000
- ○ Between £10,001-£50,000
- ○ More than £50,000
- ○ Insignificant
- ○ Unknown

You have only 5 questions left to be answered!

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INFORMATION SECURITY THREATS

20. To what extent did the security incident damage the reputation of the e-learning environment?

	Very Major damage	Major damage	Minor damage	Very Minor damage	No damage	Unknown
Brand devaluation	○	○	○	○	○	○
Customer complaints	○	○	○	○	○	○
Number of students	○	○	○	○	○	○
Adverse media coverage	○	○	○	○	○	○
Shareholder commitment	○	○	○	○	○	○

21. To what extend did the security incident give impact to the data and information in the e-learning environment?

	Very Major impact	Major impact	Minor impact	Very Minor impact	No impact	Unknown
Lost of privacy and confidentiality	○	○	○	○	○	○
Loss of availability	○	○	○	○	○	○
Lost of integrity	○	○	○	○	○	○

Your contribution is highly appreciated. Please continue answering the following questions.

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INFORMATION SECURITY THREATS

20. To what extent do you think the security incident could damage the reputation of the e-learning environment?

	Very Major damage	Major damage	Minor damage	Very Minor damage	No damage
Brand devaluation	○	○	○	○	○
Customer complaints	○	○	○	○	○
Number of students	○	○	○	○	○
Adverse media coverage	○	○	○	○	○
Shareholder commitment	○	○	○	○	○

21. To what extend do you think the security incident could give impact to the data and information in the e-learning environment?

	Very Major impact	Major impact	Minor impact	Very Minor impact	No impact
Lost of privacy and confidentiality	○	○	○	○	○
Loss of availability	○	○	○	○	○
Lost of integrity	○	○	○	○	○

Your contribution is highly appreciated. Please continue answering the following questions.

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INFORMATION SECURITY THREATS

22. Please indicate the level of importance of the following projects or programs at your e-learning environment / institution.

	Highly Important	Moderately Important	Neutral	Slightly Important	Not At All Important
Strengthening the network parameter to prevent external intrusions	○	○	○	○	○
Security and availability of website and systems for teaching and learning	○	○	○	○	○
Messaging / email security	○	○	○	○	○
Securing remote access for students and remote offices	○	○	○	○	○
Centralised management and controls on data and information	○	○	○	○	○
Preventing employees/insiders from abusing access rights	○	○	○	○	○

Other (please specify)

23. Please indicate the level of relevancy of each obstacle to security management in e-learning Institution.

	Highly Relevant	Moderately Relevant	Neutral	Slightly Not Relevant	Not RelevantAt All
Budget constraints	○	○	○	○	○
Lack of employee and end user awareness on information security	○	○	○	○	○
Lack of management support	○	○	○	○	○
Lack of competent information security personnel	○	○	○	○	○
Lack of internal security policies	○	○	○	○	○
Unclear user responsibilities	○	○	○	○	○
Technical challenges and complexity of products	○	○	○	○	○

Other (please specify)

Your contribution is highly appreciated. Please continue answering the following questions.

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

INFORMATION SECURITY THREATS

24. Please prioritise (rank) what you believe will be the most significant threat to the e-learning environment in your institution during the next 12 months.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Virus and Worm	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Spoofing and Masquerade	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Sequential and Dictionary Scanning	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Digital Snooping and Shoulder Surfing	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Scavenging (Dumpster Diving / Browsing)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Spamming- Overloading a system with incoming message or other traffic to cause system crashes/buffer overflows	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tunneling-Any digital attack that attempts to get "under" a security system by accessing very low level system functions (e.g., device drivers, OS kernels)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Equipment Malfunction -Hardware operates in abnormal, unintended mode	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Software Malfunction- Software behaviour is in conflict with intended behaviour	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Trap Door (back door) - System access for developers inadvertently left available after software delivery	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
User/Operator Error- Inadvertent alteration, manipulation or destruction of programs, data files or hardware	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Fire damage- Physical destruction of equipment due to fire or smoke damage	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Water damage- Physical destruction of equipment due to water (including sprinkler) damage	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Power loss-Computers or vital supporting equipment fail due to lack of power	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Natural disaster- Physical destruction of equipment due to floods, tornados, earthquakes or lightning	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

You have just finished answering the last questions!

INFORMATION SECURITY THREATS IN E-LEARNING ENVIRONMENT -

CONTACT DETAILS

If you are interested with this research and would like to discuss further or willing to be approached for an interview, please leave your details here.

Name:

Email:

Phone Number:

Note: An interview wil give researcher the opportunity to ask you a few in depth questions. It will not take up too much of your time and your name will be kept anonymous. Some of your comments may be included in a study report.

Appendix B Application Overview

Legend Actors and roles

DC: Delivery coordinator AD: (System) Administrator
CC: Online Course Coordinator ED: Educators
TM: Top Management ST: Students
DF: Discussion Facilitator GU: Guest or Visitor
SP: Sponsor

N.	Application	Subset Application	Actors	Key Usage / Important Features	Technology	Application Vulnerability
1.	**VLE** - (1) Online Course Administration (Course Delivery)	Course Listing,	▪ DC ▪ AD ▪ CC ▪ ED	▪ AD Can Create, View, Update, Delete User For Online Course Administration ▪ DC Can View, Update, Course List , ▪ CC Can Create, View, Update, Delete Course List , ▪ CC Can Create, View, Update, Delete Educator List ▪ ED Can View Course List	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Sensitive Data ▪ Exception Management, ▪ Auditing And Logging
		Grading Centre	▪ DC ▪ AD ▪ CC ▪ ED ▪ TM	▪ AD Can Create, View, Update, Delete User For Grading Centre ▪ DC Can View Grading List , ▪ CC Can Create, View, Update, Delete Grade. ▪ ED Can View Students Grade ▪ TM Can View Students Grade	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Sensitive Data ▪ Exception Management, ▪ Auditing And Logging
		Performance Monitoring	▪ DC ▪ AD ▪ CC ▪ ED ▪ TM	▪ AD Can Create, View, Update, Delete Users For Performance Monitoring ▪ DC Can View Performance ▪ CC Can View Performance ▪ ED Can View Performance	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers,	▪ Authentication, ▪ Authorisation, ▪ Sensitive Data ▪ Exception Management, ▪ Auditing And Logging

			▪ TM Can View Performance	▪ Development Languages	
(2)Course Management	Deliver Learning Content ,	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST	▪ AD Create, View, Edit, Delete User For Deliver Content ▪ DC View Folder, Directories And Learning Content ▪ CC View Folder, Directories And Learning Content ▪ ED Create, View, Edit, Delete Folder, ▪ ED Create, View, Edit, Delete Directories, ▪ ED Create, View, Edit, Delete Learning Content ▪ ST View And Download Learning Content	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Exception Management, ▪ Auditing And Logging
	Deliver Assignment And Collect Assignment	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST	▪ AD Create, View, Edit, Delete User For Assignment Section ▪ DC View Folder, Directories And Assignment ▪ CC View Folder, Directories And Assignment ▪ ED Create, View, Edit, Delete Folder, ▪ ED Create, View, Edit, Delete Directories, ▪ ED Create View, Edit, Delete Assignment ▪ ST View And Download Assignment ▪ ST Create And Submit Assignment Answer ▪ ED Download Assignment Answer	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Sensitive Data, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging

(3)Communication Tools	Online Session (Whiteboard, Chat)	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST	▪ CC Create, View, Edit And Delete Online Session, ▪ AD Create, View, Edit, Delete User For Online Session ▪ DC View Online Session ▪ ED Login Online Session, ▪ ST Login Online Session, ▪ ED Use (Read and Write) Whiteboard. ▪ ED Can Deliver Content During The Session ▪ ST Can Receive The Learning Content During The Session ▪ ED Chat with Students. ▪ ST Can Response To Lecturer During The Online Session.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Session Management, ▪ Cryptography, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
	Discussion Board	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST ▪ DF	▪ AD Create, View, Edit And Delete User For Discussion Board, ▪ DC Can View The Discussion Board ▪ CC Create, View, Edit And Delete Discussion Board, ▪ ED Create, View, Edit And Delete Messages, ▪ DF Moderate, View, Edit And Delete Messages, ▪ ST View And Reply Messages	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Session Management, ▪ Cryptography, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
	Email	▪ AD ▪ USER	▪ AD Create And Delete Email Account For Registered User, ▪ Registered User Create, View, Edit Delete Email Messages	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Session Management, ▪ Cryptography, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging

Personal Portfolio	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST ▪ DF	▪ AD Create And Delete Personal Portfolio For Registered User, ▪ Registered User Create, View, Edit And Delete Content In His/hers Personal Portfolio.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Sensitive Data ▪ Exception Management, ▪ Auditing And Logging
File Storage	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST ▪ DF	▪ AD Create And Delete File Storage For User, ▪ User Create, View, Edit And Delete File	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Exception Management, ▪ Auditing And Logging ▪ Sensitive Data
File Exchange	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST ▪ DF	▪ AD view File Exchange among User. ▪ User Create, View, Edit And Delete File	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Configuration Management, ▪ Cryptography, ▪ Exception Management, ▪ Session Management ▪ Sensitive Data
Project Collaboration And Sharing	▪ DC ▪ AD ▪ CC ▪ ED ▪ ST	▪ Administrator View (Admin) File Exchange Among User. ▪ User Create, View, Edit And Delete File.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Configuration Management, ▪ Cryptography, ▪ Exception Management, ▪ Session Management ▪ Sensitive Data
Assessment Tool	▪ AD ▪ ED ▪ ST	▪ AD Create , View ,Edit, Delete User For Survey Tools ▪ ED Create, View, Edit And Delete Questionnaire. ▪ ED Create, View, Edit And Delete Set Of Answer Schema. ▪ ST Login to Take the Test. ▪ ST View and Submit Answers. ▪ ST Allow Taking The Test Once And In Certain Time.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Session Management, ▪ Cryptography, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging

		Survey Tools	▪ AD ▪ ED ▪ ST	▪ AD Create , View ,Edit, Delete User For Survey Tools ▪ ED Create, View, Edit And Delete Questionnaire. ▪ ST Login to Take the Test. ▪ ST View and Submit Answers.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Session Management, ▪ Cryptography, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
		Others (Announcement , Calendar)	▪ ED ▪ ST	▪ ED Can Create View, Edit And Delete Announcement To Students. ▪ ST Can Create, View, Edit And Delete Announcement To Students. ▪ ED And ST Can View Calendar	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Session Management, ▪ Cryptography, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
2.	**Registration**	Profile Database, Qualification Result, Sponsor	▪ AD ▪ ST ▪ GU ▪ SP	▪ AD Create, View, Edit And Delete Profile Database. ▪ ST Can View Profile ▪ GU Can Submit Registration Form, And Attached Related Documents. ▪ Sponsor Can View The Students Registration.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Exception Management, ▪ Auditing And Logging
3.	**Finance**	Admin, Students Database, Bank	▪ AD ▪ Bank	▪ Admin Can View Payment Made By Students. ▪ ST Can Made Payment Online. ▪ Bank Can Transfer Money Paid By Students To University Account	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Session Management, ▪ Cryptography, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
4.	**Students Administration**	Profile Database, Qualification Result,	▪ AD ▪ DC ▪ CC ▪ ED	▪ DC Can View Students Profile, ▪ DC Can View Qualification Result, Course Taken And Course Should Be Taken.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management,

		Sponsor, Courses Taken And Should Be Taken, Results For Every Semester	▪ SP	▪ CC Can Edit, View Students Profile, ▪ CC Can Edit, View Qualification Result, Course Taken And Course Should Be Taken. ▪ ED Can View Edit and Delete Results. ▪ SP Can View Student Results	Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Sensitive Data, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
5.	**Certification**	Link With Registration, Finance, And Students Administration	▪ AD ▪ DC ▪ CC ▪ ST	▪ AD Create, View, Edit, Delete User For Certification Section ▪ CC Can Create, View, Edit And Delete Certification Award To Students ▪ DC Can View And Edit Certification Awards To Students ▪ ST Can (Check) View Certification Award.	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Sensitive Data, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
6.	**Mobile Learning**		▪ AD ▪ ED ▪ ST	▪ AD Create, View Edit And Delete User Roles ▪ ED Can Create, View, Edit And Delete Learning Content (Teach) For Mobile Learning Purpose ▪ ST Can Learn Using The Mobile Learning	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Sensitive Data, ▪ Parameter Manipulation, ▪ Exception Management, ▪ Auditing And Logging
7.	**Virtual Library**		▪ AD ▪ ST ▪ USER	▪ ST Can View, And Update Data Similarly As Physical Library ▪ USERS Can View, And Update Data Similarly As Physical Library	▪ Operating Systems, ▪ Web Server Software, Database Server Software, ▪ Technologies Used In The Presentation, ▪ Business And Data Access Layers, ▪ Development Languages	▪ Input And Data Validation, ▪ Authentication, ▪ Authorisation, ▪ Configuration Management, ▪ Sensitive Data ▪ Parameter Manipulation, ▪ Exception Management ▪ Auditing And Logging ▪ Cryptography ▪ Session Management

* Key Usage Were Confirmed By Referring To Blackboard Manual From Cranfield IT Department And Blackboard Website. >> www.Blackboard.Com

Appendix C Category of Risk

No.	Vulnerabilities Category	Threats	Critical	Major	Minor
1	Input & Data Validation	Buffer Overflow	• VLE-Communication Tool • Registration	• VLE-Online Course Admin • VLE- Course Management • VLE-Communication Tools • Finance • Students Administration • Certification • Mobile Learning	• VLE-Online Course Admin • VLE-Communication Tools • Virtual Library
2	Authentication	Network Eavesdropping	• VLE- Online Course Admin • Communication Tools • Registration Certification	• VLE- Course Management • VLE-Communication Tools • Finance • Mobile Learning	• VLE-Online Course Admin • VLE- Course Management • VLE-Communication Tools • Students Administration • Virtual Library
		Password Guessing	• VLE-Communication Tool • Certification	• VLE-Online Course Admin • VLE- Course Management • VLE-Communication Tools • Registration • Finance • Mobile Learning	• VLE-Online Course Admin • VLE-Communication Tools • Students Administration • Virtual Library
		Cookie Replay		• VLE-Online Course Admin • VLE-Course Management • Registration	• VLE-Online Course Admin • VLE= Course Management • VLE-Communication Tool
		Credential Theft	• Registration	• VLE-Course Management • VLE Communication Tool	• VLE-Online Course Admin • VLE-Communication Tool
3	Authorisation	Elevation Of Privilege	• VLE-Online Course Admin • VLE-Course Management	• VLE-Online Course Admin • VLE-Course Management	
		Unauthorised Access	• VLE- Communication Tools • Registration • Finance	• VLE Communication Tool • Students Administration • Mobile Learning	• VLE Communication Tool • Virtual Library

			• Certification		
4	Configuration Management	Unauthorised Access To Administration Interfaces And Configuration Stores	• VLE-Online Course Admin • VLE- Communication Tools • Registration • Finance • Certification	• VLE- Course Management • VLE Communication Tool • Student Administration • Mobile Learning	• VLE-Online Course Admin • VLE Communication Tool • Virtual Library
5	Exception Management	Trap Door	• VLE- Communication Tool	• VLE-Online Course Admin • VLE- Course Management • VLE Communication Tool • Registration	• VLE-Online Course Admin • VLE- Course Management • VLE Communication Tool •
		Spamming	• VLE- Course Management • VLE Communication Tool • Registration	• VLE- Communication Tool • Finance • Certification • Mobile Learning • Virtual Library	• VLE-Online Course Admin • VLE- Course Management • VLE Communication Tool • Students Administration
6	Sensitive Data	Tunnelling	• VLE-Online Course Admin	• VLE- Communication Tool • VLE- Course Management	
		Software Malfunction	• VLE-Online Course Admin	• VLE-Online Course Admin	• Deliver Assignment & Collect Assignment
		Network Eavesdropping	• Certification	• VLE- Communication Tool • Students Administration • Mobile Learning • Virtual Library	• VLE- Communication Tool
7	Session Management	Session Replay	• VLE- Communication Tool • Finance • Virtual Library	• VLE- Communication Tool	• VLE- Communication Tool
		Man In The Middle	• VLE- Communication Tool	• VLE- Communication Tool	• VLE- Communication Tool
8	Cryptography	User Error	• VLE- Communication Tool • Finance	• VLE- Communication Tool • Virtual Library	• VLE- Communication Tool
9	Parameter Manipulation	Http Manipulation	• VLE- Communication Tool • Finance	• Certification • Mobile Learning	• VLE- Communication Tool • Students Administration • Virtual Library
		Cookie Manipulation	• VLE- Course Management • VLE- Communication Tool	• Certification, • Mobile Learning	• VLE- Communication Tool • Students Administration

			• Finance		• Virtual Library
10	Auditing & Logging	User Masquerade	• VLE- Communication Tool • Registration • Finance, • Certification	• VLE- Online Course Admin • VLE- Communication Tool •	• VLE- Communication Tool • Students Administration • Mobile Learning • Virtual Library
		Malicious Code		• VLE- Online Course Admin • VLE- Course Management	• VLE Online Course Admin

Appendix D Threats Analysis by Sub-Application

IP: Interruption **IC: Interception**

F: Fabrication **M: Modification**

No.	Application	Subset Application/Task	Application Security Mechanism (Vulnerabilities Category)	Threats (Noun) Vulnerabilities	Threats (Verb-Attack) (Intentional & Unintentional)	Threats (Impact) - M F IP IC	Likelihood Of Occurrence	Impact To Individual Or System	Risk
1.	**VLE** (1) Online Course Administration (Course Delivery)	Course Detail Listing	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Low (1)	Minor (1)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Unlikely (1)	Low (1)	Minor (1)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Low (1)	Minor (2)
				Cookie Replay	Intentional Cookie Replay	Information Revealed IC	Possible (2)	Low (1)	Minor (2)
				Credential Theft	Intentional Credential Theft	IC	Unlikely (1)	Low (1)	Minor (1)
			Authorisation	Elevation Of Privilege	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)

			Configuration Management	Unauthorised Access To Administration Interfaces And Configuration Stores	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Unlikely (1)	Medium (2)	Minor (2)
			Sensitive Data	Tunnelling Software Malfunction	Intentional Exploits An Application Without Trace Unintentional Software Conflict	Data Tampering M	Possible (2)	Medium (2)	Major (4)
			Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Unlikely (1)	Low (1)	Minor(1)
				Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)
			Auditing And Logging	Malicious Code	Intentional Exploits An Application Without Trace	Data Tampering M	Unlikely (1)	Low (1)	Minor (1)
		Grading Centre	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Medium (2)	Minor (2)
			Authentication	Network Eavesdropping	Intentional-Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	High (3)	Critical (6)

				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC Tampering Data M Fabricating Data F	Possible (2)	Medium (2)	Major (4)
				Cookie Replay	Intentional Cookie Replay	Information Revealed IC	Possible (2)	Medium (2)	Major (4)
				Credential Theft	Intentional Credential Theft	IC Tampering Data M Fabricating Data F Asset Becoming Lost IP	Unlikely (1)	Low (1	Minor (1)
			Authorisation	Elevation Of Privilege	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Likely (3)	High (3)	Critical (9)
			Configuration Management	Unauthorised Access To Administration Interfaces And Configuration Stores	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Likely (3)	High (3)	Critical (9)
			Sensitive Data	Tunnelling Software Malfunction	Intentional Exploits An Application Without Trace Unintentional Software Conflict	Data Tampering M	Likely (3)	High (3)	Critical (9)
			Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Unlikely (1)	High (3)	Major (3)
			Auditing And Logging	Malicious Code	Intentional Exploits An Application	Denial Of Service IP Data Tampering	Unlikely (1)	Low (1)	Minor (1)

				Without Trace				
	Performance Monitoring	Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Low (1)	Minor (2)
			Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Low (1)	Minor (2)
			Cookie Replay,	Intentional Cookie Replay	Information Revealed IC	Possible (2)	Low (1)	Minor (2)
			Credential Theft	Intentional Credential Theft	IC	Unlikely (1)	Low (1)	Minor (1)
		Authorisation	Elevation Of Privilege	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
		Sensitive Data	Tunnelling Software Malfunction	Intentional Exploits An Application Without Trace Unintentional Software Conflict	Data Tampering M	Possible (2)	Medium (2)	Major (4)
		Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Unlikely (1)	Low (1)	Minor(1)
			Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)
		Auditing And Logging	Malicious Code	Intentional Exploits An Application Without Trace	Denial Of Service IP Data Tampering M	Unlikely (1)	High (3)	Major (3)

(2)Course Management	Deliver Learning Content	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
				Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	High (3)	Major (3)
		Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Unlikely (1)	Low (1)	Minor (1)
			Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
			Cookie Replay	Intentional Cookie Replay	Information Revealed IC	Possible (2)	Low (1)	Minor (2)
			Credential Theft	Intentional Credential Theft	IC	Possible (2)	Medium (2)	Major (4)
		Authorisation	Elevation Of Privilege	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
		Configuration Management,	Unauthorised Access To Administration Interfaces And Configuration Stores	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
		Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Unlikely (1)	Low (1)	Minor(1)
			Spamming	Intentional Overloading	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)

					System With Incoming Message				
			Auditing And Logging	Malicious Code	Intentional Exploits An Application Without Trace	Denial Of Service IP Data Tampering	Unlikely (1)	High (3)	Major (3)
		Deliver Assignment And Collect Assignment	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
				Cookie Replay	Intentional Cookie Replay	Information Revealed IC	Possible (2)	Medium (2)	Major (4)
				Credential Theft	Intentional Credential Theft	IC	Possible (2)	Medium (2)	Major (4)
			Authorisation	Elevation Of Privilege	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	High (3)	Critical (6)
			Configuration Management	Unauthorised Access To Administration Interfaces And Configuration Stores	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Unlikely (1)	High (3)	Major (3)

				Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	High (3)	Critical (6)
			Auditing And Logging	Malicious Code	Exploits An Application Without Trace	Denial Of Service (IP) Data Tampering M	Unlikely (1)	High (3)	Major (3)
			Parameter Manipulation	Cookie Manipulation	Intentional Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Likely (3)	Medium (2)	Critical (6)
			Sensitive Data	Tunnelling	Intentional Exploits An Application Without Trace	Data Tampering In Assignment Questions And Answer. M	Unlikely (1)	High (3)	Major (3)
				Software Malfunction	Unintentional Software Conflict	Data Tampering In Assignment Questions And Answer. M	Unlikely (1)	Medium (2)	Minor (2)
	(3)Communication Tools	Online Session (Whiteboard, Chat)	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Low (1)	Minor (1)
			Authentication	Network Eavesdropping	Intentional-Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Unlikely (1)	Low (1)	Minor (1)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Unlikely (1)	Medium (2)	Minor (2)

				Cookie Replay	Intentional Cookie Replay	Information Revealed IC	Possible (2)	Low (1)	Minor (2)
				Credential Theft	Intentional Credential Theft	IC	Unlikely (1)	Low (1)	Minor (1)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
			Configuration Management	Unauthorised Access To Administration Interfaces And Configuration Stores	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Session Management	Session Replay	Unauthorised Access	Interruption IP	Unlikely (1)	Low (1)	Minor (1)
				Man In The Middle	Unauthorised Access	Data Tampering - M	Possible (2)	Low (1)	Minor (2)
			Auditing And Logging	Users Masquerade	Intentional Masquerade	Tampering Data (M)	Possible (2)	Medium (2)	Major (4)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Intentional Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Unlikely (1)	Low (1)	Minor (1)
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Unlikely (1)	Low (1)	Minor (1)
			Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Low (1)	Minor (1)

		Discussion Board	Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Unlikely (1)	Low (1)	Minor (1)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
				Cookie Replay	Cookie Replay	Information Revealed IC	Possible (2)	Low (1)	Minor (2)
				Credential Theft	Credential Theft	IC	Unlikely (1)	Low (1)	Minor (1)
			Authorisation	Unauthorised Access	Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Session Management	Session Replay	Unauthorised Access	Interruption IP	Unlikely (1)	Low (1)	Minor(1)
				Man In The Middle	Unauthorised Access	Data Tampering - M	Unlikely (1)	Low (1)	Minor(1)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Unlikely (1)	Low (1)	Minor(1)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Unlikely (1)	Low (1)	Minor(1)
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Unlikely (1)	Low (1)	Minor(1)

			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Unlikely (1)	Low (1)	Minor(1)
		Email	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
			Authentication	Network Eavesdropping	Intentional-Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data-IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Medium (2)	Major (4)

			Auditing And Logging	Users Masquerade	Intentional Exploits An Application Without Trace	Modify And Fabricate Data M F	Unlikely (1)	Low (1)	Minor(1)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Intentional Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Unlikely (1)	Low (1)	Minor(1)
			Session Management	Session Replay	Intentional Unauthorised Access	Interruption IP	Unlikely (1)	Low (1)	Minor(1)
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Unlikely (1)	Low (1)	Minor(1)
		Personal Portfolio	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering -	Possible (2)	Medium (2)	Major (4)

						M			
			Configuration Management	Unauthorised Access To Administration Interfaces And Configuration Stores	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Sensitive Data	Network Eavesdropping	Intentional Access Sensitive Data In Storage	Unauthorised Party Gain Access To An Asset IC	Possible (2)	Medium (2)	Major (4)
			Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Possible (2)	High (3)	Critical (6)
				Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)
			Auditing And Logging	Users Masquerade	Intentional Exploits An Application Without Trace	Modify And Fabricate Data M F	Unlikely (1)	Medium (2)	Major (4)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Intentional Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Unlikely (1)	Low (1)	Minor(1)
		File Storage	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
			Authentication	Network Eavesdropping	Intentional-Information Surveillance By Unauthorised	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)

					Party (Digital Snooping)				
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
				Cookie Replay	Intentional Cookie Replay	Information Revealed IC	Possible (2)	Low (1)	Minor (2)
				Credential Theft	Intentional Credential Theft	IC	Possible (2)	Medium (2)	Major (4)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	High (3)	Critical (6)
			Configuration Management	Unauthorised Access To Administration Interfaces And Configuration Stores	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
				Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Medium (2)	Major (4)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Unlikely (1)	Medium (2)	Minor (2)
			Sensitive Data	Network Eavesdropping	Access Sensitive Data In Storage	Unauthorised Party Gain Access To An Asset IC	Possible (2)	Medium (2)	Major (4)
		File Exchange	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error Intentional -	Damage User's File -IP Change Data- M Disclosure	Unlikely (1)	Low(1)	Minor (1)

				Extra Data Contain Malicious Code	Confidentiality -IC			
		Configuration Management	Unauthorised Access To Administration Interfaces, Unauthorised Access To Configuration Store	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
		Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Unlikely (1)	Medium (2)	Minor (2)
		Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Possible (2)	Low (1)	Minor (2)
			Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)
		Session Management	Session Replay	Unauthorised Access	Interruption IP	Unlikely (1)	Low(1)	Minor (1)
			Man In The Middle	Unauthorised Access	Data Tampering - M	Unlikely (1)	Low(1)	Minor (1)
		Sensitive Data	Network Eavesdropping	Intentional Access Sensitive Data In Storage	Unauthorised Party Gain Access To An Asset IC	Possible (2)	Medium (2)	Major (4)
	Project Collaboration And Sharing	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
				Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
		Configuration Management	Unauthorised Access To	Intentional Spoofing Or	Lack Of Individual Accountability,	Possible (2)	Medium (2)	Major (4)

				Administration Interfaces, Unauthorised Access To Configuration Store	Masquerade	Over Privileged Process And Service Accounts M F IP			
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Possible (2)	Medium (2)	Major (4)
			Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Possible (2)	Low (1)	Minor (2)
				Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)
			Session Management	Session Replay	Intentional Unauthorised Access	Interruption IP	Possible (2)	Low (1)	Minor (2)
				Man In The Middle	Intentional Unauthorised Access	Data Tampering - M	Possible (2)	Low (1)	Minor (2)
			Sensitive Data	Network Eavesdropping	Intentional Access Sensitive Data In Storage	Unauthorised Party Gain Access To An Asset IC	Possible (2)	Low (1)	Minor (2)
		Assessment Tool The Session May Be Denied To Be Access; Data May Be Delayed And Unauthorised Access Which Lead To Fabrication, Modification And Deletion Of Data	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	High (3)	Critical (6)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	High (3)	Critical (6)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	High (3)	Critical (6)

					Scanning				
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	High (3)	Critical (6)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	High (3)	Critical (6)
			Session Management	Session Replay	Intentional Unauthorised Access	Information Disclosure Interruption IP	Possible (2)	High (3)	Critical (6)
				Man In The Middle	Intentional Unauthorised Access	Data Tampering - M	Possible (2)	High (3)	Critical (6)
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Possible (2)	High (3)	Critical (6)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Possible (2)	High (3)	Critical (6)
			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	High (3)	Critical (6)
			Auditing And Logging	Users Masquerade	Intentional Exploits An Application Without Trace	Modify And Fabricate Data M F	Likely (3)	High (3)	Critical (9)
		Survey Tools	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)

					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Unlikely (1)	Low (1)	Minor (1)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Low (1)	Minor (2)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Low (1)	Minor (2)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Low (1)	Minor (2)
			Session Management	Session Replay	Intentional Unauthorised Access	Information Disclosure IC Interruption IP	Unlikely (1)	Low (1)	Minor (1)
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Possible (2)	Low (1)	Minor (2)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Possible (2)	Low (1)	Minor (2)
			Exception Management	Spamming	Intentional Overloading System With	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)

					Incoming Message				
			Auditing And Logging	Users Masquerade	Intentional Exploits An Application Without Trace	Modify And Fabricate Data M F	Unlikely (1)	Low (1)	Minor (1)
		Others (Announcement , Calendar)	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File –IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
					Intentional - Extra Data Contain Malicious Code	Damage User's File –IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Low (1)	Minor (2)
			Authentication	Network Eavesdropping	Intentional-Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Session Management	Session Replay	Intentional Unauthorised Access	Information Disclosure IC Interruption IP	Unlikely (1)	Low (1)	Minor (1)

			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Unlikely (1)	Low (1)	Minor (1)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Unlikely (1)	Low (1)	Minor (1)
			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Unlikely (1)	Medium (2)	Minor (2)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Possible (2)	Medium (2)	Major (4)
2.	**Registration**	Profile Database, Qualification Result, Sponsor	Input And Data Validation	Buffer Over Flow	Unintentional-Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	High (3)	Critical (6)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Low (1)	High (3)	Major (3)
			Authentication	Network Eavesdropping	Intentional-Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	High (3)	Critical (6)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Unlikely (1)	High (3)	Major (3)
				Cookie Replay	Cookie Replay	Information Revealed IC	Unlikely (1)	High (3)	Major (3)
				Credential Theft	Credential Theft	IC	Likely (3)	High (3)	Critical (9)

			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	High (3)	Critical (6)
			Configuration Management	Unauthorised Access To Administration Interfaces, Unauthorised Access To Configuration Store	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	High (3)	Critical (6)
			Exception Management	Trap Door	Unintentional Unauthorised System Access	Information Disclosure IC	Unlikely (1)	High (3)	Major (3)
				Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	High (3)	Critical (6)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Likely (3)	High (3)	Critical (9)
3.	**Finance**	Admin, Students Database, Bank (The Session May Be Denied To Be Access; Data May Be Delayed And Unauthorised Access.)	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning,	Password Revealed, Unauthorised User Gain Access	Possible (2)	Medium (2)	Major (4)

					Sequential Scanning	To Information IC			
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	High (3)	Critical (3)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	High (3)	Critical (3)
			Session Management	Session Replay	Intentional Unauthorised Access	Information Disclosure IC Interruption IP	Possible (2)	High (3)	Critical (3)
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Possible (2)	High (3)	Critical (3)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Possible (2)	High (3)	Critical (3)
			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Medium (2)	Major (4)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Possible (2)	High (3)	Critical (3)
4.	**Students Administration**	Profile Database, Qualification Result, Sponsor, Courses Taken And Should Be Taken, Results For Every Semester (Data May Be Copied, Tamper Fabricate And	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Low (1)	Minor (2)

		Deleted. Denial Of Access)	Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Low (1)	Minor (2)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Low (1)	Minor (2)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Sensitive Data	Network Eavesdropping.	Access Sensitive Data In Storage	Information Disclosure IC	Possible (2)	High (3)	Critical (6)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Possible (2)	Low (1)	Minor (2)
			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Low (1)	Minor (2)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Possible (2)	Low (1)	Minor (2)
5.	**Certification**	Link With Registration, Finance, And Students Administration	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)

					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Medium (2)	Minor (2)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Likely (3)	High (3)	Critical (9)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	High (3)	Critical (6)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Likely (3)	High (3)	Critical (9)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Likely (3)	High (3)	Critical (9)
			Sensitive Data	Network Eavesdropping.	Access Sensitive Data In Storage	Information Disclosure IC	Likely (3)	High (3)	Critical (9)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Medium (2)	Major (4)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Likely (3)	High (3)	Critical (9)
6.	**Mobile Learning**	(Data May Be Copied, Tamper Fabricate And	Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP	Possible (2)	Medium (2)	Major (4)

		Deleted. Denial Of Access)				Change Data- M Disclosure Confidentiality -IC			
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Low (1)	Minor (1)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Possible (2)	Medium (2)	Major (4)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Possible (2)	Medium (2)	Major (4)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Possible (2)	Medium (2)	Major (4)
			Sensitive Data	Network Eavesdropping	Access Sensitive Data In Storage	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Possible (2)	Medium (2)	Major (4)
			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Possible (2)	Medium (2)	Major (4)

			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Unlikely (1)	Medium (2)	Minor (2)
7.	**Virtual Library**		Input And Data Validation	Buffer Over Flow	Unintentional- Programming Error	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Possible (2)	Medium (2)	Major (4)
					Intentional - Extra Data Contain Malicious Code	Damage User's File -IP Change Data- M Disclosure Confidentiality -IC	Unlikely (1)	Low (1)	Minor (1)
			Authentication	Network Eavesdropping	Intentional- Information Surveillance By Unauthorised Party (Digital Snooping)	Information Disclosure IC	Unlikely (1)	High (3)	Major (3)
				Password Guessing	Intentional Brute Force Attacks, Dictionary Attack/ Scanning, Sequential Scanning	Password Revealed, Unauthorised User Gain Access To Information IC	Unlikely (1)	Medium (2)	Minor (2)
			Authorisation	Unauthorised Access	Intentional Luring Attacks	Disclosure Of Confidential Data- IC Data Tampering - M	Unlikely (1)	High (3)	Major (3)
			Configuration Management	Unauthorised Access To Administration Interfaces	Intentional Spoofing Or Masquerade	Lack Of Individual Accountability, Over Privileged Process And Service Accounts M F IP	Unlikely (1)	High (3)	Major (3)
			Sensitive Data	Network Eavesdropping	Access Sensitive Data In Storage	Information Disclosure IC	Unlikely (1)	High (3)	Major (3)
			Parameter Manipulation	Cookie Manipulation, Http Manipulation	Injecting A Custom HTTP Header Or By Injecting A META Tag	Information Disclosure IC	Unlikely (1)	Medium (2)	Minor (2)

			Exception Management	Spamming	Intentional Overloading System With Incoming Message	Denial Of Service IP	Unlikely (1)	Medium (2)	Minor (2)
			Auditing And Logging	Users Masquerade	Exploits An Application Without Trace	Modify And Fabricate Data M F	Unlikely (1)	Medium(2)	Minor (2)
			Session Management	Session Replay		Information Disclosure IC	Unlikely (1)	High (3)	Major (3)
			Cryptography	User Error	Unintentional Poor Key Generation Or Key Management, Weak Encryption	Asset Becoming Lost IP Unauthorised Access IC	Unlikely (1)	High (3)	Major (3)

Appendix E Countermeasure Table

No.	Vulnerabilities Category	Threats	Countermeasure	Critical	Major	Minor
1	Input & Data Validation	Buffer Overflow	• (first line of defend)Perform through input validation .constrain input by validating it for type, length, format and range. • When possible, limit the application's use of unmanaged code, and thoroughly inspect the unmanaged Application Programming Interface (APIs) to ensure that input is properly validated.	• VLE-Communication Tool • Registration	• VLE-Online Course Admin • VLE- Course Management • VLE-Communication Tools • Finance • Students Administration • Certification • Mobile Learning	• VLE-Online Course Admin • VLE-Communication Tools • Virtual Library
2	Authentication	Network Eavesdropping	• Use authentication mechanisms that do not transmit the password over the network such as Kerberos protocols or windows authentication. • Make sure passwords are encrypted or use an encrypted communication channel e.g. Secure Socket Layer (SSL)	• VLE- Online Course Admin • Communication Tools • Registration Certification	• VLE- Course Management • VLE-Communication Tools • Finance • Mobile Learning	• VLE-Online Course Admin • VLE- Course Management • VLE-Communication Tools • Students Administration • Virtual Library
		Password Guessing	• Use strong password for all of accounts type • Apply lockout policies to end –user accounts to limit the number of retry attempts that can be used to guess the password	• VLE-Communication Tool • Certification	• VLE-Online Course Admin • VLE- Course Management • VLE-Communication Tools • Registration • Finance • Mobile Learning	• VLE-Online Course Admin • VLE-Communication Tools • Students Administration • Virtual Library
		Cookie Replay	• Use an encrypted communication channel provided by SSL whenever an authentication cookie is transmitted. • Use cookie timeout to a value that forces authentication after a relatively short interval. Although this doesn't prevent replay attacks, it reduces the time interval in which the attacker can replay a request without being forced to re authenticate because the session has timed out		• VLE-Online Course Admin • VLE-Course Management • Registration	• VLE-Online Course Admin • VLE- Course Management • VLE-Communication Tool
		Credential Theft	• Use and enforce strong passwords. • Store password verifiers in the form of one way hashes with added salt • Enforce account lockout for end user	• Registration	• VLE-Course Management • VLE Communication Tool	• VLE-Online Course Admin • VLE-Communication Tool

			accounts after a set number of retry attempts. • To counter the possibility of the browser cache allowing login access, create functionality that either allows the user to choose to no save credentials, or force this functionality as a default policy			
		Elevation Of Privilege	• Consider the threat of an attacker trying to elevate privilege to a powerful account when designing an authorisation model. Use least privilege processes, service and user accounts.	• VLE-Online Course Admin • VLE-Course Management	• VLE-Online Course Admin • VLE-Course Management	
3	Authorisation	Unauthorised Access	<u>Luring attacks</u> Restrict access to trusted code with appropriate authorisation <u>Prevent data disclosure</u> • Perform role checks before allowing access to the operations that could potentially reveal sensitive data • Use strong Access Control List (ACLs) to secure Window resources. • Use standard encryption to store sensitive data in configuration files and databases. <u>Prevent data tampering</u> • Use strong access controls to protect data in persistent stores to ensure that only authorised users can access and modify the data. • Use role-based security to differentiate between users who can view data and users who can modify data.	• VLE- Communication Tools • Registration • Finance • Certification	• VLE Communication Tool • Students Administration • Mobile Learning	• VLE Communication Tool • Virtual Library
4	Configuration Management	Unauthorised Access To Administration	Unauthorised Access To Administration Interfaces • Minimize the number of administration interfaces	• VLE-Online Course Admin • VLE- Communication Tools • Registration • Finance • Certification	• VLE- Course Management • VLE Communication Tool • Student Administration • Mobile Learning	• VLE-Online Course Admin • VLE Communication Tool • Virtual Library

		Interfaces And Configuration Stores	• Use string authentication using certificates • Use strong authorisation with multiple gatekeepers • Consider supporting only local administration. If remote administration is absolutely essential, use encrypted channels e.g. VPN technology or SSL, because of the sensitive nature of the data passed over administrative interfaces. To further reduce risk, also consider using Internet Protocol Security (IPSec) policies to limit remote administration to computers on the internal network. • Unauthorised Access To Configuration Stores • Configure restricted ACLs on text-based configuration files such as Machine.config and Web. config. • Keep custom configuration stores outside of the web space. This removes the potential to download Web server configurations to exploit their vulnerabilities.			
5	Exception Management	Trap Door	• Prevent details from being revealed to the client • Use exception handling throughout the application's code base. • Handle and log exceptions that are allowed to propagate to the application boundary • Return generic, harmless error messages to the client.	• VLE- Communication Tool	• VLE-Online Course Admin • VLE- Course Management • VLE Communication Tool • Registration	• VLE-Online Course Admin • VLE- Course Management • VLE Communication Tool •
		Spamming	• To prevent the denial of service as the result of spamming • Thoroughly validate all input data at server • Use exception handling throughout the application 's code base	• VLE- Course Management • VLE Communication Tool • Registration	• VLE- Communication Tool • Finance • Certification • Mobile Learning • Virtual Library	• VLE-Online Course Admin • VLE- Course Management • VLE Communication Tool • Students Administration
6	Sensitive Data	Tunnelling	Avoid access to sensitive data in storage by:	• VLE-Online Course Admin	• VLE- Communication Tool • VLE- Course Management	

			• Use restricted ACLs on the persistent data stores that contain sensitive data • Store encrypted data • Use identity and role based authorisation to ensure that only the user or users with appropriate level of authority are allowed access to sensitive data. Use role based security to differentiate between users who can view data and users who can modify data.			
		Software Malfunction	• Refer to software manufacturer	• VLE-Online Course Admin	• VLE-Online Course Admin	• Deliver Assignment & Collect Assignment
		Network Eavesdropping	• Encrypt the data • Use an encrypted communication channel e.g. SSL.	• Certification	• VLE- Communication Tool • Students Administration • Mobile Learning • Virtual Library	• VLE- Communication Tool
7	Session Management	Session Replay	• Re- authenticate when performing critical functions. (e.g. Prior to performing a monetary transfer in a banking application, make the user supply the account password again) • Expire sessions appropriately, including all cookies and session tokens • Create a' do not remember me' option to allow no session data to be stored on the client.	• VLE- Communication Tool • Finance • Virtual Library	• VLE- Communication Tool	• VLE- Communication Tool
		Man In The Middle	• Use cryptography. • Use Hashed Message Authentication Codes (HMACs). If an attacker alters the message, the recalculation of the HMAC at the recipient fails and the data can be rejected as invalid.	• VLE- Communication Tool	• VLE- Communication Tool	• VLE- Communication Tool
8	Cryptography	User Error	• Use built in encryption routines that include secure key management. • Use strong random key generation functions and store the key in a restricted location. • Encrypt the encryption key • Expire keys regularly • Do not develop your own custom	• VLE- Communication Tool • Finance	• VLE- Communication Tool • Virtual Library	• VLE- Communication Tool

			algorithms • Use the proven cryptographic services provided by the platform • Stay informed about cracked algorithms and the techniques used to cracks them.			
9	Parameter Manipulation	Http Manipulation	• Do not base any security decisions on HTTP headers. e.g. do not trust the HTTP referrer to determine where a client came from because this is easily falsified.	• VLE- Communication Tool • Finance	• Certification • Mobile Learning	• VLE- Communication Tool • Students Administration • Virtual Library
		Cookie Manipulation	• Encrypt or use an Hashed Message Authentication Codes (HMAC) with the cookie	• VLE- Course Management • VLE- Communication Tool • Finance	• Certification, • Mobile Learning	• VLE- Communication Tool • Students Administration • Virtual Library
10	Auditing & Logging	User Masquerade	• Audit and log activity on the web server and database server and on the application server • Log key events such as transaction and login and logout events • Secure log files by using restricted ACls • Relocate system log files away from their default locations.	• VLE- Communication Tool • Registration • Finance, • Certification	• VLE- Online Course Admin • VLE- Communication Tool •	• VLE- Communication Tool • Students Administration • Mobile Learning • Virtual Library
		Malicious Code	Attacker exploit an application without leaving a trace • Log critical application level operations • Use platform-level auditing to audit login and logout events, access to the file system and failed object access attempts.		• VLE- Online Course Admin • VLE- Course Management	• VLE Online Course Admin

Appendix F Incident Logging

No.	Date	Name	Breach Type	Inside/Outside Threats	reference (URL)
1	03/27/06	Long Island University Brooklyn	Email	Inside-Accidental	http://datalossdb.org/incidents/1333
2	03/30/06	Connecticut Tech High School Sys.	Email	Inside-Accidental	http://datalossdb.org/incidents/253
3	04/14/06	University of South Carolina	Email	Inside-Accidental	http://datalossdb.org/incidents/263
4	11/03/06	University of Virginia	Email	Inside-Accidental	http://datalossdb.org/incidents/486
5	11/17/06	Jefferson College of Health Sciences	Email	Inside-Accidental	http://datalossdb.org/incidents/499
6	12/09/06	Virginia Commonwealth University	Email	Inside-Accidental	http://datalossdb.org/incidents/515
7	12/21/06	City University of New York	Email	Outside	http://datalossdb.org/incidents/1282
8	12/21/06	Hunter College of the City University of New York	Email	Inside-Accidental	http://datalossdb.org/incidents/2233
9	02/08/07	East Carolina University	Email	Inside	http://datalossdb.org/incidents/2258
10	09/14/07	Tennessee Tech University	Email	Outside	http://datalossdb.org/incidents/788
11	02/13/08	University of Toledo	Email	Inside-Accidental	http://datalossdb.org/incidents/1465
12	02/28/08	Fordham University	Email	Inside-Accidental	http://datalossdb.org/incidents/1997
13	03/13/08	The Art Institute of Washington	Email	Inside-Accidental	http://datalossdb.org/incidents/2023
14	03/17/08	Binghamton University	Email	Inside-Accidental	http://datalossdb.org/incidents/933
15	05/06/08	Ohio State University Agricultural Technical Institute	Email	Outside	http://datalossdb.org/incidents/981
16	05/09/08	Princeton University Tower Club	Email	Inside-Accidental	http://datalossdb.org/incidents/987
17	01/21/09	Missouri State University	Email	Inside-Accidental	http://datalossdb.org/incidents/1520
18	01/31/09	Ball State University	Email	Inside-Accidental	http://datalossdb.org/incidents/1636

19	06/07/09	Ohio State University	Email	Inside-Accidental	http://datalossdb.org/incidents/2092
20	08/30/05	California State University	Virus	Outside	http://datalossdb.org/incidents/145
21	02/01/06	University of Colorado CO Springs of Colorado	Virus	Outside	http://datalossdb.org/incidents/214
22	12/15/08	University of North Carolina at Greensboro	Virus	Outside	http://datalossdb.org/incidents/1277
23	03/17/09	Penn State University	Virus	Outside	http://datalossdb.org/incidents/1837
24	04/10/09	Penn State Erie, The Behrend College	Virus	Outside	http://datalossdb.org/incidents/1881
25	05/04/09	Kapiolani Community College	Virus	Outside	http://datalossdb.org/incidents/1951
26	02/15/07	The Professional Education Institute	Web	Inside-Accidental	http://datalossdb.org/incidents/1670
27	11/20/08	Capstone Companies	Web	Inside-Accidental	http://datalossdb.org/incidents/1427
28	01/10/04	New York University	Web	Inside-Accidental	http://datalossdb.org/incidents/35
29	02/03/04	New York University	Web	Inside-Accidental	http://datalossdb.org/incidents/38
30	04/12/05	Tufts University	Web	Outside	http://datalossdb.org/incidents/78
31	07/09/05	University of Southern Cailfornia	Web	Outside	http://datalossdb.org/incidents/124
32	07/30/05	Austin Peay State University	Web	Inside-Accidental	http://datalossdb.org/incidents/131
33	08/19/05	University of Colorado	Web	Inside-Accidental	http://datalossdb.org/incidents/142
34	08/30/05	Stark State College of Technology	Web	Inside-Accidental	http://datalossdb.org/incidents/147
35	09/16/05	Miami Ohio University	Web	Inside-Accidental	http://datalossdb.org/incidents/151
36	09/28/05	City University of New York	Web	Inside-Accidental	http://datalossdb.org/incidents/155
37	10/15/05	Montclair State University	Web	Inside-Accidental	http://datalossdb.org/incidents/160
38	10/20/05	Monmouth University	Web	Inside-Accidental	http://datalossdb.org/incidents/161
39	10/20/05	Vermont Technical College	Web	Inside-Accidental	http://datalossdb.org/incidents/163

40	10/29/05	University of Tennessee	Web	Inside-Accidental	http://datalossdb.org/incidents/166
41	12/08/05	J-Sargeant Reynolds Community College	Web	Inside-Accidental	http://datalossdb.org/incidents/182
42	01/13/06	Suffolk County Community College	Web	Inside-Accidental	http://datalossdb.org/incidents/1346
43	01/20/06	University of Kansas	Web	Inside-Accidental	http://datalossdb.org/incidents/201
44	02/15/06	Old Dominion University	Web	Inside-Accidental	http://datalossdb.org/incidents/221
45	02/16/06	State University of New York Institute of Technology	Web	Inside-Accidental	http://datalossdb.org/incidents/1807
46	03/29/06	University of Nebraska Lincoln	Web	Inside-Accidental	http://datalossdb.org/incidents/250
47	05/26/06	California State University Stanislaus	Web	Inside-Accidental	http://datalossdb.org/incidents/295
48	06/01/06	University of Kentucky	Web	Inside-Accidental	http://datalossdb.org/incidents/302
49	06/24/06	Catawba County Schools	Web	Inside-Accidental	http://datalossdb.org/incidents/334
50	06/27/06	University of Rochester	Web	Inside-Accidental	http://datalossdb.org/incidents/1692
51	07/05/06	Columbia University	Web	Unknown	http://datalossdb.org/incidents/1865
52	08/09/06	Hunter College of the City University of New York	Web	Inside-Accidental	http://datalossdb.org/incidents/2271
53	08/15/06	University of Kentucky	Web	Inside-Accidental	http://datalossdb.org/incidents/394
54	08/15/06	University of Kentucky Department of Geography	Web	Inside-Accidental	http://datalossdb.org/incidents/395
55	09/01/06	Virginia Commonwealth University	Web	Inside-Accidental	http://datalossdb.org/incidents/417
56	11/07/06	Lehman College	Web	Inside-Accidental	http://datalossdb.org/incidents/1365
57	12/19/06	Mississippi State University	Web	Inside-Accidental	http://datalossdb.org/incidents/527
58	12/20/06	Big Foot High School (WI)	Web	Inside-Accidental	http://datalossdb.org/incidents/529
59	12/21/06	City University of New York	Web	Inside-Accidental	http://datalossdb.org/incidents/1619
60	12/21/06	Hunter College of the City University of New York	Web	Inside-Accidental	http://datalossdb.org/incidents/2210

61	12/22/06	Utah Valley State College	Web	Inside-Accidental	http://datalossdb.org/incidents/534
62	02/07/07	University of Nebraska Lincoln	Web	Inside-Accidental	http://datalossdb.org/incidents/577
63	02/09/07	East Carolina University	Web	Inside-Accidental	http://datalossdb.org/incidents/581
64	02/15/07	City College of San Francisco	Web	Inside-Accidental	http://datalossdb.org/incidents/588
65	02/19/07	Clarksville-Montgomery County Schools	Web	Inside-Accidental	http://datalossdb.org/incidents/590
66	03/07/07	Los Rios Community College	Web	Inside-Accidental	http://datalossdb.org/incidents/606
67	03/10/07	University of Idaho	Web	Inside-Accidental	http://datalossdb.org/incidents/609
68	03/12/2007	New York Institute of Technology (NYIT)	Web	Inside-Accidental	http://datalossdb.org/incidents/1596
69	03/27/07	St. Mary Parish Schools (Louisiana)	Web	Outside	http://datalossdb.org/incidents/619
70	04/12/07	Black Hills State University	Web	Outside	http://datalossdb.org/incidents/634
71	04/19/07	New Mexico State University	Web	Outside	http://datalossdb.org/incidents/642
72	04/24/07	Purdue University	Web	Outside	http://datalossdb.org/incidents/649
73	05/03/07	Montgomery College	Web	Outside	http://datalossdb.org/incidents/659
74	05/19/07	Stony Brook University	Web	Inside-Accidental	http://datalossdb.org/incidents/675
75	06/01/07	Northwestern University	Web	Outside	http://datalossdb.org/incidents/695
76	07/17/07	Louisiana Board of Regents	Web	Outside	http://datalossdb.org/incidents/732
77	07/19/07	Jackson Local Schools	Web	Outside	http://datalossdb.org/incidents/735
78	08/17/07	University of New Hampshire	Web	Inside	http://datalossdb.org/incidents/1862
79	09/06/07	University of South Carolina	Web	Outside	http://datalossdb.org/incidents/780
80	09/10/07	Purdue University	Web	Outside	http://datalossdb.org/incidents/783
81	10/09/07	Pembroke School District	Web	Outside	http://datalossdb.org/incidents/804

82	10/23/07	Bates College	Web	Inside-Accidental	http://datalossdb.org/incidents/817
83	10/29/07	New England School of Law	Web	Inside-Accidental	http://datalossdb.org/incidents/1750
84	11/16/07	Kansas State University	Web	Outside	http://datalossdb.org/incidents/837
85	11/21/07	University of Florida	Web	Outside	http://datalossdb.org/incidents/842
86	01/05/08	University of Texas at Austin	Web	Inside-Accidental	http://datalossdb.org/incidents/1719
87	01/07/08	Franklin University	Web	Inside-Accidental	http://datalossdb.org/incidents/1395
88	01/11/08	University of Iowa	Web	Outside	http://datalossdb.org/incidents/882
89	01/12/08	California State University Stanislaus	Web	Outside	http://datalossdb.org/incidents/885
90	01/16/08	University of Wisconsin-Madison	Web	Outside	http://datalossdb.org/incidents/889
91	01/18/08	Colorado State University	Web	Inside-Accidental	http://datalossdb.org/incidents/1720
92	01/25/08	Murray State University	Web	Inside-Accidental	http://datalossdb.org/incidents/1411
93	01/30/08	University of Massachusetts at Dartmouth	Web	Inside-Accidental	http://datalossdb.org/incidents/1722
94	02/04/08	Iowa State University	Web	Inside-Accidental	http://datalossdb.org/incidents/1435
95	02/04/08	University of Iowa	Web	Inside-Accidental	http://datalossdb.org/incidents/1723
96	02/05/08	Rowan University	Web	Inside-Accidental	http://datalossdb.org/incidents/1724
97	02/08/08	East Carolina University	Web	Inside-Accidental	http://datalossdb.org/incidents/1725
98	02/16/08	Texas A&M University	Web	Outside	http://datalossdb.org/incidents/916
99	04/11/08	Bowdoin College	Web	Inside-Accidental	http://datalossdb.org/incidents/955
100	04/13/08	University of Toledo	Web	Inside-Accidental	http://datalossdb.org/incidents/957
101	04/17/08	Hunter College of the City University of New York	Web	Inside-Accidental	http://datalossdb.org/incidents/2175
102	05/08/08	Las Cruces Public Schools	Web	Inside-Accidental	http://datalossdb.org/incidents/986

103	05/20/08	New York University	Web	Outside	http://datalossdb.org/incidents/997
104	05/21/08	University of Nebraska Lincoln	Web	Inside-Accidental	http://datalossdb.org/incidents/1390
105	05/31/08	Pocono Mountain School District	Web	Outside	http://datalossdb.org/incidents/1003
106	06/10/08	University of Florida	Web	Outside	http://datalossdb.org/incidents/1016
107	06/12/08	Columbia University	Web	Outside	http://datalossdb.org/incidents/1018
108	07/15/08	University of Texas at Austin	Web	Inside	http://datalossdb.org/incidents/1050
109	07/24/08	University of Houston	Web	Outside	http://datalossdb.org/incidents/1064
110	07/25/08	Ohio University	Web	Outside	http://datalossdb.org/incidents/1063
111	07/31/08	Ivy Tech Community College	Web	Inside-Accidental	http://datalossdb.org/incidents/1151
112	09/05/08	East Burke (Morganton, NC) High School	Web	Outside	http://datalossdb.org/incidents/1145
113	09/18/08	Sonoma State University	Web	Inside-Accidental	http://datalossdb.org/incidents/1165
114	10/13/08	Southwest Mississippi Community College	Web	Outside	http://datalossdb.org/incidents/1176
115	11/07/08	Texas A&M University-Corpus Christi	Web	Outside	http://datalossdb.org/incidents/1196
116	11/10/08	Sinclair Community College	Web	Outside	http://datalossdb.org/incidents/1197
117	12/04/08	Cal Poly Pomona	Web	Outside	http://datalossdb.org/incidents/1236
118	12/20/08	University of North Carolina School of Arts	Web	Inside-Accidental	http://datalossdb.org/incidents/1293
119	12/31/08	Ohio State University	Web	Inside-Accidental	http://datalossdb.org/incidents/1312
120	01/20/09	University of Florida	Web	Inside-Accidental	http://datalossdb.org/incidents/1800
121	01/30/09	Kansas State University	Web	Outside	http://datalossdb.org/incidents/1568
122	08/13/09	Louisiana State University	Web	Inside-Accidental	http://datalossdb.org/incidents/2282
123	08/20/09	Boston University Army Reserve Officers Training Corps	Web	Outside	http://datalossdb.org/incidents/2293

Appendix G Interview Questions

Background Respondents

What are your job roles/ scope?

How long in this position and handling e-learning?

Interview questions

1. How is e-learning implemented in your place?
2. What is the reason e-learning is implemented in your institutions. Example?
3. How much has e- learning been executed in this university? Give an example.
4. Are there any issues and challenges faced on e-learning implementation? Give an example.
5. How is the acceptance of e-learning among lecturer, students? Give example
6. How is the support from the top management regarding the e-learning implementation? Give an example.
7. How is the support from the staff regarding the e-learning implementation? Give an example.
8. How does the institution address the issues and challenges? Give an example.

Security Threats and incidents

1. What the common security threats in e-learning? Give an example.
2. Have any security incidents happened to the e-learning system in your institution? Give an example.
3. What are the control and countermeasures that had been implemented to safeguard the e-learning environment? Give examples.
4. What are the obstacles and challenges in safeguarding the e-learning? Give an example.

Appendix H Background of Nine Malaysian Public Universities

No.	University Name/ website	Location/ Branches	Profile /history	Date Of Establishment
1.	*Universiti Sains Islam Malaysia* (USIM) www.usim.edu.my	• Main Campus-*Nilai, Negeri Sembilan* • Branch Campus - *Pandan Indah*, *Kuala Lumpur* (Faculty of Medicine & Health Science, and Faculty of Dentistry).	Islamic Science University of Malaysia (USIM) or formerly known as Islamic University College of Malaysia (KUIM) is the 12th Public Higher Education Institution (IPTA) in Malaysia. Among the objectives of the establishment of USIM are to uphold and enhance Islamic studies, bring Islamic Studies into the national main education stream, emphasise the use of information technology in education and research systems. Focus is also put in mastering Arabic and English language as well as the national language.	1998
2.	*Universiti Sains Malaysia* (USM) www.usm.edu.my Has been designated as a research university.	• Main Campus- *Penang* • Branch Campus - 1. *Seri Ampangan* **(**Engineering Campus), 2. *Kubang Kerian Kelantan* ***(***Health Campus***)***	Established as the second university in the country in 1969, University Sains Malaysia (USM) was first known as the University of Penang, before the University's Act came into effect on 4th October 1971. Now, USM offers courses at undergraduate and postgraduate levels to approximately 20,000 students. USM has also become a well-known university locally and internationally. Since its beginning, USM has implemented a school system, as opposed to the traditional faculty system. What is unique about this	1969

			system is that each school could fulfil the needs of a more focused degree in the chosen area of study and at the same time, students could have the opportunity to explore other areas of study offered by another school. The interdisciplinary approach ensures that USM, the first in the country to adopt this system, would produce trained, multi-skilled graduates.	
3.	Universiti Pendidikan Sultan Idris (UPSI) www.upsi.edu.my	Main Campus- *Tanjung Malim, Perak*	An education university-teaching on pedagogy of other fields. The UPSI, one of Malaysia's leading public universities, is a supportive learning community for students and faculty alike. Widely recognised for leadership in teacher's education, UPSI provide innovative programs and real-life learning experiences. UPSI ranks consistently among the top universities in Malaysia.	1997
4	Universiti Teknologi MARA (UiTM) www.uitm.edu.my	The enormous responsibility of managing and educating a large and diverse student population has resulted in the expansion of the university set-up into : • one main campus- Shah Alam, Selangor • several satellite campuses	UiTM is Malaysia's premier institution of higher learning that has experienced phenomenal growth since its inception in 1956. The institution has been upgrade to a university on 1999. The university has expanded nationwide with 15 branch campuses, three satellite campuses, nine city campuses, 21 affiliated colleges and a smart campus for the future. With this vast network and a workforce of 15 000, the university offers more than 300 academic programmes in a conducive and vibrant environment. It is also home to almost 120,000 students. These campuses provide excellent opportunities for *Bumiputeras* all	1999

		• state campuses, • city/town campuses The university also has several affiliated colleges.	over the country to pursue higher education and attain higher economic and social development. **Shah Alam Main Campus** It acts as the focal point of development and expansion to a network of other campuses. **Satellite Campuses** These campuses house specialist programmes and are different from branch campuses, which usually offer a bigger range of academic programmes. **State Campuses** UiTM is the only university in Malaysia that has a state campus in every state of the country. It started its first campus in Sabah in 1973. In a span of 30 years, although most of these campuses started on temporary premises, their establishment has been strategised and well planned. **City/Town Campuses** These campuses are non-residential campuses which ensure that UiTM's academic and professional training programmes reach out to the residents of local communities.	
5	Universiti Teknologi Malaysia (UTM)*	• Main Campus- *Skudai Johore* • Branch Campus - *Jalan Semarak. Kuala Lumpur* **(**International Campus)	Has been designated as a research university.* An innovation-led Research University and a leading research-intensive university in engineering, science and technology. It is located both in Kuala Lumpur, the capital city of Malaysia and Johor Bahru, the southern city in Iskandar Malaysia, which is a vibrant	1972

	www.utm.edu.my		economic corridor in the south of Peninsular Malaysia. There are more than 16,036 full-time undergraduate students at UTM and more than 5,839 enrolled on distance learning programmes as part-time students. In addition, there are more than 6,350 postgraduate students in various fields of specialisation.	
6.	Universiti Kebangsaan Malaysia (UKM)* www.ukm.edu.my	• Main Campus- *Bangi, Selangor* • Branch Campus – Cheras, *Kuala Lumpur* **(**Medical Campus)	Has been designated as a research university.* Universiti Kebangsaan Malaysia (UKM), was established on 18 May 1970, as the only national university in the country that uses Bahasa Melayu (Malay language) as the medium of instruction. With an excellent academic environment, modern campus facilities and campus in park concept, UKM has evolved into one of the leading universities in the region. UKM offers various academic programmes in both arts and science fields. At present, UKM has 13 faculties; eight of them are located in the main Bangi campus. The Faculty of Health Sciences, Faculty of Pharmacy and Faculty of Dentistry are located in the Kuala Lumpur campus. The Faculty of Medicine on the other hand is located in Cheras campus.	1970
7.	Universiti Malaysia Sarawak (UNIMAS) www.unimas.edu.my	• Main Campus- *Kota Samarahan, Sarawak*	The university was officially incorporated on 24th December 1992. UNIMAS is the eighth public university in Malaysia and the first in Sarawak. UNIMAS offers a unique environment for teaching, learning and research.	1992

8.	Universiti Malaya (UM)* www.um.edu.my	• Main Campus- *Kuala Lumpur*	Has been designated as a research university.* **Universiti Malaya**, Malaysia's oldest university is situated on a 750 acre (309 hectare) campus in the southwest of Kuala Lumpur, the capital of Malaysia.	1905
9.	Universiti Putra Malaysia(UPM)* www.upm.edu.my	• Main Campus- *Serdang, Selangor* • Branch Campus - *Bintulu Sarawak* (East Malaysia)	Has been designated as a research university.* The establishment of this university was the result of the merge between the College of Agriculture Malaya with the Faculty of Agriculture, University of Malaya in 1971. Universiti Pertanian Malaysia started its first academic session in July 1973 with three central faculties: the Faculty of Agriculture, Faculty of Forestry, and Faculty of Veterinary Medicine and Animal Science. Besides the three faculties there was a Basic Sciences Division. In the early eighties, however, UPM has expanded its area of studies to the field of Science and Technology (S&T). In 1994, UPM embarked on its ambitious plan to develop as a futuristic university, which would provide better and up-to-date skills and systems for science and technology education by taking full advantage of the rapid development in information technology (IT).	1971

Appendix I Summary of Interviews

Summary of Interview in University 1

Background Respondents

*A Director of i-Learn Center (*i-LeC*)* since 14 December 2009. Previously he is the head of Distance Education Centre. His task is to manage the implementation of e-learning by planning strategies of implementation and infrastructure for e-learning. He also ensures i-LEC provide training on e-learning and training on develop learning content.

E-learning implementation

i-Learn Center (i-LeC*)* was established on the 1st of December 2005 and operate under the Academic Affair Division (HEA). Deputy Vice Chancellor (Academic and Internationalization) is the advisor of the **i-LeC**. The centre is responsible for handling adaptation of e-learning in the university. The centre formally launched its Learning Management System (LMS) portal on the 30th December 2005.

There are two groups of students, the full time (main stream) students and the distance education students. E-learning has been used since 1999 when Distance Education programme was offered by the university. In 2005, e-learning implementation was expanded for full time students. The full time students are using i-Learn as their LMS and the latter are using LMS called i-Class. All e-learning matters are managed by i-LeC except the Distance Education programme. A Distance Education programme is managed by the Distance Education Centre. However the LMS for the distance education programme is developed by i-LeC.

For full time students, blended learning is used. Blended learning here is defined by the use face-to-face classes and online classes alternately. Some of lecturers are using e-learning as supporting tools for learning such as assessment and quiz. The distance education programme is using i-Class almost 90% fully online. Only 10% of meetings are face-to-face in every semester. Meanwhile, usage of e-learning among the full time students is less. In the 2010/2011 academic session all the generic courses were conducted with blended learning where 50% face to face and another 50% online.

The LMS was bought from other university. It has been customised and enhanced according to the university needs, objectives and culture. The LMS can be used for any programme. The university has many programmes from a diploma certification until PhD degree. However the use is on voluntary basis and all lecturers can use the e-learning ((LMS) for any courses. Lecturers can use online classes to replace the tutorial classes.

Currently there is no policy for e-learning in this university. The university is cultivating the use of e-learning among lecturers. Gradually they will make the use of e-learning compulsory. At the moment, 50% of lectures have taken part and almost 80% students are involved in using e-learning.

Reasons why E-Learning is Implemented

E-learning is implemented to fulfil the students' needs. As the educational provider, the university has to follow the current trend based on the needs and not just because it wants to jump on the bandwagon. In addition, it is to assist the lecturer in providing better teaching facilities and to make the teaching more efficient. E-learning can diversify the teaching and delivery of material to students, as example: conversational online, using e- books, computers and internet.

E-learning is the best medium in accomplishing the university target, which is to have 200 thousand students enrol in this university. The university can't afford to employ many lecturers to entertain that number of students therefore; the e-learning is the best methods. This will also reduce the expenses for the classroom, infrastructure and amenities in entertaining 200 thousand students.

Challenges and Issues

Cultivating e-learning use among the lecturers is a challenging issue here. It is difficult to change the mind set of lecturers that have been accustomed to the traditional ways of teaching. This issue mainly comes from senior lecturers, as they feel this is an additional burden. Many of the lecturers are not ready to use e-learning.

Distance Education students also having difficulties due to the network infrastructure problem. They are depending more on the LMS compared to the full time students, where 90% of classes are conducted online.

Acceptance of e-learning among lecturers, students

Lecturers are a bit reluctant to use e-learning. However young lecturers and students support e-learning and looked forward to using it.

Support from the top management regarding e-learning implementation

Top management has been very supportive towards e-learning implementation. They have set up proper governance by establishing I-LEC and have always given full support on infrastructure improvement.

Future Plan- Addressing the Issues and Challenges

- Improve the LMS- i-Learn to be efficient, up-to-date, modern and fast. This will help the lecturers feel more confident and comfortable with the system.
- Improve on the network infrastructure by having new storage and servers. This will aid in ensuring the system can operate as required by the client.
- Carry out an awareness campaign to create awareness among students and among academic staff:
    - i-Learn open day
    - desk-to-desk discussion with the deans, to alert and inform them on e-learning matters
    - conduct training for lecturers and students
    - distribute to the user information on e-learning in flyers or pamphlets
- Increase the usage of e-learning in a fulltime programme. Encourage the students give feedback online.

Security Threats and incidents

Definition of security in e-learning

Intentional threats/attacks by intruders/hackers/people who deliberately want to prevent users accessing the content. It doesn't make sense to claim the weakness of a network as a security threat in e-learning or any system.

Security is more for the intentional disturbance that prevent the users to use e-learning. If the network is suddenly down, we don't call it a security issues (in e-learning). Even though in banking that issue would be considered as a security issue.

If students cannot download the content due to the network problem, it is considered as an unpreventable/inevitable factor and not as a security issue. To be considered as a security issue, there should be a person that can be held accountable of any attack. If there is none, therefore it is not considered as security issue in e-learning.

Common security threats in e-learning

No security threats and issues in e-learning

The control and countermeasures that have been implemented to safeguard the e-learning environment

- Use the common technological countermeasure and control. Conduct patching to the source code whenever necessary.

- i-LeC staff attend training on security provided by Training centre

Summary of Interviews in University 2

Background Respondents

A Deputy Director of the Academic Development Centre (ADeC) and manager of the e-learning unit at ADEC. His main role is to manage the application of technology to the teaching and learning processes especially in the designing and developing of comprehensive delivery systems. He has been two years in this position but has been using e-learning for a number of years.

E-learning implementation

The Academic Development Centre (ADeC) is a one-stop centre for improving and developing learning and teaching among staff during their academic career. The unit is set-up mainly to support and provide trainings for implementation of e-learning. ADeC became the central resource for the LMS and also provides educational support and training. The team has increased contact with faculties in order to support e-learning implementation. In addition to that, call centres and clinics were also provided to the users. Training on managing collaborative tools was also scheduled.

This university wants to implement the students' centred learning. It is important to let the students have the flexibility to learn at anytime and anywhere, as well as sharing the knowledge and information that they have. At the moment the university is running e-learning without an e-learning policy, but with commitment from Vice Chancellor (VC). The VC has suggested having one LMS for all. In view of the fact that many of the academicians have been using Moodle for their own teaching, therefore Moodle has been chosen. ADeC had proposed a plan for the implementation of e-learning. The e-learning implementation schedule was planned to start on 1 June 2009 and expected to end by 2011/2012 academic session. It is hope that by end of the 2011/2012 academic session, e-learning has successfully been fully implemented.

The first LMS known as LearningCare is a locally developed LMS by the IT Centre. During that time some lecturers were using Moodle individually. In 2007 a standalone model named as Moodle Code has been widely used among lecturers. In 2009 with ADeC supervision, a fully integrated LMS-Moodle was introduced to the residents. This integrated LMS has been used in semester1 2009/2010 academic session. The LMS has been managed by ADeC with the help of consultation from outside on the LMS technical issues.

Lecturers are encouraged but not forced to use the LMS. The university has been using a very gentle approach by introducing tools that can be used by lecturers for their teaching as one of the encouragement methods.

E-learning in this university is a blended learning method. The LMS is ready and complemented with all the tools that are suitable for e-learning purposes. It will depend on the lecturer as to how much they would make use of it. At the moment 20% of courses are fully active using the LMS as a tool in teaching and learning.

During the implementation stage, training for trainers (ToT) is planned. At least two academic staff from each faculty will be selected to become resource persons for their respective faculty. (At the moment this is yet not successful).

Reasons why E-Learning is implemented

Besides improving the delivery of knowledge, students nowadays are digital native. They have been using Facebook, web 2.0 and other technologies for communication. That's how the younger generation nowadays do things. In order to catch up with them, academicians need to follow the trend to optimize the acceptance and response to learning.

Challenges and Issues

Although there are currently more than 1,000 courses being used, efforts need to be made to increase the number of users, besides encouraging the current ones to fully utilise the system.

Lecturer resistance

Lecturers are not willing to learn about e-learning even though the manuals are ready for them and can easily be understood. Lecturers believed that e-learning will make them work more without realizing that it is actually helping them and that these are tools to help their life easier.

Ambiguous policy of e-learning

It is unconfirmed as to whether the number of face-to-face classes can be reduced if e-learning is put into practice. At the moment there is no standard on how to calculate and implement this matter. This is an unsolved issue at most universities in Malaysia. With a formula to balance the number of face-to-face and online classes, this will erase the thought that e-learning is an extra work and burden among lecturers.

Accessibility

Sometimes, there are complaints from students on the difficulties of accessing the LMS due to a volatile internet connection.

Acceptance of e-learning among lecturers, students

Lecturer

The usage of e-learning among lectures is only 10%. They are not willing to use it due to the thought that e-learning is extra work. The university is working to increase the usage to a new target of 60—70%.

Students

Students enjoy using e-learning. This can be measured from the number of times access is made by each student to LMS.

Support from the top management regarding the e-learning implementation

The top management has been very supportive regarding the e-learning implementation. The vice chancellor had recently announced that all courses should be placed online using the LMS.

Future Plan- Addressing the Issues and Challenges

Policy

In ensuring a clear direction and smooth implementation of e-learning, there is an urgent need for this university to have its own e-learning policy. The university is waiting until a policy is endorsed by the MEIPTA. MEPITA is an e-learning committee for public universities in Malaysia. This university is planning to employ the policy endorsed by MEIPTA.

Training

Seminars and conferences are suggested to support and consolidate the effort to fully implement e-learning.

Literacy awareness

The resistance among lecturers towards e-learning is not because of IT literacy problems but because they are not aware that e-learning can help them to a better delivery. There are some lecturers with no IT background but able to spend the time to do it. Hence, they disseminate awareness by publishing bulletins/pamphlets and doing road shows on e-learning philosophy, benefits, technologies and tools. Workshops on how to use the LMS are also conducted. Lecturers also are offered with immediate help via email and phone as well as walk-in to the ADeC office.

Incentive, recognition and award

Incentives are offered to the staff involved in the implementation of e-learning. Incentives to people who work hard to make sure the e-learning is a success .

It is also suggested that incentives be given for active involvement in e-learning. Awards such as the most active lecturer, the most active course and the most active faculty should be considered.

ADeC is looking at promoting Moodle as a collaborative learning environment, developing new training and focusing on developing effective online instructions. It also needed to improve the branding of LMS and also to include future extension and tools.

Other than the above, plans are being laid out to ensure that the LMS will be more than just a repository of teaching materials uploaded by the lecturers for students to download.

Security threats and incidents

Definition of security e-learning: The system shouldn't be hacked and the data is in a safe condition. Example of data: quiz and assessment marks.

Common security threats in e-learning

Common security threats re server breakdown, system malfunctions due to infrastructure problems (power blackout) or software corruption. The technical staffs have to reinstall and then perform a recovery. Due to this situation many back-ups are to be done.

Security incidents on e-learning system

So far no incident had happened.

The control and countermeasures that have been implemented to safeguard the e-learning environment

The IT Centre is responsible for handling the technical issues in the university Technical issues include the safeguarding of e-learning. Therefore ADeC assume that all of the control and countermeasures are managed by the IT centre. Among the control and countermeasures implanted are:

- provides a framework for ICT security and quality control to improve quality in all aspects of ICT infrastructure, applications and services
- monitor antivirus and supervise for virus infection
- coordinate the ICT sustainability plan

- monitor network traffic and access control at the server farm and DMZ
- conduct a safety of ICT audit to network hardware, servers and applications
- managing ICT security incidents

Summary of Interviews in University 3

Background Respondents

A Lecturer of Educational Multimedia Department at Faculty of Education. His has been appointed as the IT coordinator at faculty since 2009. He has been involved in e-learning since 2003/2004. His job scope includes being a course creator where he manages courses at faculty level, as a trainer for e-learning training and assist technical job for faculty.

An IT Officer at Centre of ICT (CICT). One of his job task s is to manage e-learning LMS.

E-learning implementation

E-learning is organised by the Centre for Teaching and Learning (CTL). CTL provides support services for teaching staff to promote and enhance the quality of teaching). There is a strong technical team and good management of e-learning implementation. E-learning in this university has been running smoothly using an open source software.

This university uses blended learning, where the LMS is used as a support for the face-to-face classes. The LMS provided the combination of asynchronous forum, email etc. and synchronous mode- chatting etc. However the liveliness of each course will depend on how active the lecturers are in the LMS. The lively course will contribute to the course being actively accessed by students. The course is considered to be active based on the number of students who log in to the LMS.

All lecturers are obliged to utilise e-learning in their teaching. It will be monitored and reports made to the superior party. The deans will have to keep reminding the lecturers about usage. However there is no penalty given to those who didn't comply.

Earlier this university used Web CT license in 2000 as the LMS. After realizing that an open source can offer platform better and be less cost, the university moved to a new open source LMS called Moodle and introduced new LMS. All courses have to use e-learning. The enforcement stage includes three levels. These are the target underlined by the university and at the moment all lecturer should achieve L2. The targets:

L1: upload course syllabus

L2: upload weekly content and quizzes (depends on the skill and creativity of lecturers. The most common are word or .pdf files. Some use video).

L3: assignment, forum and etc. upload to the LMS

Now the university is moving towards web2.0 and is testing Mahara. Mahara is an open source e-portfolio system with a flexible display framework. Mahara is a user-centred environment with a permissions framework that enables different views of an e-portfolio to be easily managed. Mahara also features a weblog, resume-builder and a social networking system, connecting users and creating online learner communities.

Reasons E-Learning is Implemented

The university understand and recognise that e-learning is essential. Previously, the university have been using many technologies to ease the teaching and learning process, for example building personal websites and exchanging notes using pen drives. The problem is when the lecturers are assigned with different courses every semester; they have to build up new content from the

beginning. So everyone has to repeat the task from the start and it is time-consuming, redundant and inefficient. With the use of an e-learning concept, particularly the LMS, systematic application can be used in the processes of teaching and learning. The content is ready as it was developed by the previous lecturer. So the new lecture can update and enrich the content, for example using YouTube.

Moodle offers a lot of tools to enrich the teaching and learning and it is a current technology trend.

Challenges and Issues

Once, senior lecturers were a bit reticent or resentful. Now it is getting better because the number of senior lecturers is reducing some of them have gained an awareness of e-learning via the series of training conducted.

Students prefer the concept of Web 2.0 and social networking. The university is conducting research on identifying suitable applications to be included in e-learning.

Acceptance of e-learning among lecturer, students

Lecturer's acceptance is satisfactory because of the continuous training offered to them. It is quite normal for them to complain a little bit. However the lecturers are considered to becoming more active in using e-learning.

Lecturers are obliged to utilise e-learning in their teaching method. However there is no penalty if they don't.

Students' level of acceptance is tolerable, however there are complaints about some lecturers who don't update the notes or where they give late responses and feedback for forum discussions.

Support from the top management regarding the e-learning implementation

E-learning has always been given priority and received full support from top management. Top management has showed their support by initiating particular governance on e-learning by including e-learning in CTL, and also providing some budget for an e-learning seminar and training for students.

Future Plan- Addressing the Issues and Challenges

Lecturers:

In the beginning of every semester, training will be conducted to refresh their memory on how to use e-learning and how to encourage the students to use e-learning. Training on technical support also will be provided especially for lecturers on content enrichment- video and audio content embedded.

Security Threats and incidents

Definition of security in e-learning:

Any content uploaded by lecturers is available and can be accessed by students. There should be no non-repudiation issues, for example where student submits an assignment, however lectures do not receive it.

Common security threats in e-learning

Virus threats issue. The university is using Linux as the OS platform and Linux is well known as a virus carrier.

Security incidents of the e-learning system

- System black-out or network down due to systems malfunction
- 2006- Hard disk corruption, backup fail for 2 weeks
- Hardware malfunctions/ failures

The control and countermeasures that had been implemented to safeguard the e-learning environment

- An IT personnel dedicated to managing e–learning applications - LMS. His tasks include technical support and security.
- CICT conduct many campaigns on security and training on security. An example is a campaign on antivirus use.
- Conduct Daily backup of data and database.

Summary of Interview in University 4

Background Respondents

An Associate Professor from the Faculty of Cognitive Sciences and Human Development,). Since more than two and a half years ago, she has been appointed as a Deputy Dean (Learning Technology) Centre for Applied Learning and Multimedia (CALM). The job scope includes managing online learning, being in charge of the servers and applications under CALM, and of the training, awareness and awards related to online learning.

Reasons E-Learning is implemented

E-learning was initiated from a research on virtual campus conducted by the Faculty of IT. Since then this university has been inspired to use e-learning.

The e-Learning Unit in the **Centre for Applied Learning and Multimedia**, was formed in February 2002, with the task of spearheading the university initiative in the area of e-Learning. The university sees e-Learning as a support system to enhance the quality of teaching and learning in the university.

In 2002, Lotus Quick Place was used as a platform for the LMS. However it is not meant purposely for e-learning as it incompatible with the newer version of OS that it sits on. In 2004, they developed a customised application for the LMS known as Learnfinity and it was used only for one semester due to a lot of complaint received about problems with bugs. The usage was stopped for patch up and recovery activities. Meanwhile, lectures have been trying open source software called Moodle as the platform for LMS. Further to this the university has embarked the use Moodle and make it known as **MORPHEUS**. **MORPHEUS** is a LMS configured in-house by the university team. **MORPHEUS** is the official online learning system for this university. It has a number of features and activities designed to engage learners and promote collaborative, student-centred learning. **MORPHEUS** provides full authority to lecturers of the university to manage and conduct online activities that would enhance students' learning experience.

The university also holds on to the blended learning policy. In blended learning, a learning solution is created through a mixture of face-to-face and online learning so that the online component becomes a natural extension of the face-to-face learning. This university practices a form of e-Learning which combines the use of audio-visual technology in the physical lecture rooms and the use of the online learning system that is accessible by authorised users via the campus network.

The Unit hosts the online courses and conducts training workshops for academics who wish to get onto the online learning bandwagon. Once the e-Learning Unit creates an online learning environment, it is then totally managed by the lecturer of that course. The number of courses is constantly growing as each faculty strives to move more course content onto the online learning system.

The focus is in making the use of technology as a culture for the user. These technologies should fit seamlessly into the current teaching practices and be friendly to any layman. The Unit is currently looking into the possibility of incorporating webcasts and podcasts of lectures into **MORPHEUS** in the effort to enrich students' online learning experience with more multimedia elements.

Currently the e-learning unit has drafted a policy for e-learning and in the process to get some feedbacks from the e-learning committee. Previously, lecturers were not bounded but were

encouraged to use the online learning. However with the new policy introduced, it is hope that the lecturers will reach a certain level of standards.

This university is using blended learning. So the decision to be made is whether to make it compulsory for lecturers to use it or not. They understand that not all courses can be delivered online so the committee would like to give some flexibility. This is based on the perception from lecturers. Some of the lecturers are just not ready to use e-learning.

In the policy, the university wanted to allow the tutorial sessions to be conducted online. The tutorials activities can be any activities that are enabled by the LMS, for example: mind map and quiz.

Lecturers are not compulsory to use the e-learning platform as their teaching and learning method. There are groups of lecturers using different styles in using the e-learning according to their preferences. Some are very innovative and try to include as much as they could of the material. The LMS is ready for any activities and just depends on the lecturers to make use of it. Some of them use other than the official LMS MORPHEUS, so if any problem arises the university is not able to help because there is no back up done other than **MORPHEUS**. For example if the lecturers are using Facebook, no data will be saved or backed up and thus cannot be used as indication of e-learning use.

Challenges and Issues

E-learning practice

About 50% of the courses are on the LMS and this is unsatisfactory. The usage of e-learning among lecturers is considered low and insufficient.

Keep up to date with the technology

Keep on exploring the new possibilities to enhance and ensure that the performance of online learning is improving. Think of better architecture to ensure that the performance system-wide is enhanced.

Training

Conduct effective training.

Currently conduct face-to-face training; however the attendance is very poor. The university is thinking of doing training online.

Acceptance of e-learning among lecturers, students

Some lecturers see the use and importance of e-learning and they are ready to learn and use the LMS. Therefore they are willing to spend more time on the platform. Some others said that since it is not compulsory they are not going to do it.

They are waiting for the push factor to make them use the LMS. A push factor is needed to encourage the lecturers use e-learning. The endorsement of an e-learning policy by the university can be a push factor.

Therefore, at the university level, they have to acknowledge the lecturers' work on e-learning. So encouragement and recognition from management are very important.

Support from the top management regarding the e-learning implementation

The top-level management have no objection at all and have been very supportive regarding the e-learning implementation. They have always been supportive and helpful in approving the budget requested for infrastructure improvements. They realise it is important and they have given some support but it is not much highlighted.

However, once the Ministry of Higher Education (MOHE) give their full support and direction, for example, by setting up the formal KPI to be used for e-learning, then the university and the lecturers will take it more seriously and will be working towards that direction. Now the MOHE has positioned e-learning as one of the critical agenda projects in Malaysian education.

Future Plan- Addressing the Issues and Challenges

1) Training

Technical part – Will be handled by the IT department

Besides how to use the LMS, the training also includes how to create learning activities

2) Performance of system

The server was upgraded and replaced several times due to many issues and problems. A new high performance server is currently in place to replace the older server. Currently, data migration is in progress from the old to the new server.

It is in the plan to purchase another couple of servers so that applications can be split into different servers. Once ready, the existing server will be used for back up, in case any application system went down. They also have a developmental server for development purposes.

3) Endorsement of e-learning policy

In order to increase the use of e-learning among lecturers, a push factor is needed. The endorsement of the e-learning policy by the university can be a push factor.

At the university level, they have to acknowledge the lecturers' work on e-learning. Encouragement and recognition from management are important. Every year, outstanding online course awards were given out to the lecturers to encourage and recognise their work on e-learning. There is a panel of judges to evaluate various criteria. This effort does work and as a result more people are interested in accomplishing a better online course in order to achieve this award.

Security Threats and incidents

Common security threats in e-learning

The respondent defines security in e-learning as "it is always available to be use, not lose the content, the system should respond to what I want (non repudiation), feel confident to access at any time and where, have private space for example only the instructor can see the students works".

The biggest worry is a system downtime, either due to the unintentional or intentional threats. Another threat is sharing information or content with invalid users. For example:

Video on demand technology

- Which the recorded content could contain some remarks that could be out of context and may become a controversial issue once it is shared with others. It is feared that this unfortunate situation will ruin the reputation of the university

Security incidents on e-learning system

The previous server went down because of a lot of possibilities like network problems, application problems. However IT officers managed to solve it. Now with the new servers everything is improving.

The control and countermeasures that had been implemented to safeguard the e-learning environment

Not aware of this since the unit is not handling the technical issues. (Therefore this is saying that, security is addressed under the technical issues). Network site controlled by the IT people, therefore there is not much information about this. CALM has not conducted training on awareness.

Obstacles and challenges in safeguarding the e-learning.

It is very important to emphasise the security issues. However the unit was not in charge of the safeguarding of e-learning but requests the IT centre to secure the e-learning systems. The unit is aware a disaster could happen if the e-learning system is not well protected and secured.

The unit depends on the ICT centre to help in safeguarding e-learning but the problem is that most of the time e-learning is not considered as the main application system in the university that needs high priority attention. The other applications system for administrative work has a higher priority, despite the fact that the e-learning system has the largest number of users. It is one of the core businesses in the university.

Summary of Interview in University 5

Background Respondents

A Head of Division / Technical (IT Officer) at the Centre of Academic Development CADe. She is the leader and monitors the process of e-learning implementation.

A Coordinator of eLearning & CADe Publication (IT Officer) at CADe. Her task includes identifying any suitable tools to support e-learning.

E-learning implementation

E-learning has been used since late 1990s with the use of the LMS. That time was a cultivation or civilizing period for lecturers and students. Now, e-learning is administered by the Centre of Academic Development (CADe). CADE manages e-learning implementation and content. Users can deal with CADE for any e-learning matters. The LMS has been used for quite a long time, while CADe was only established in 2004. The IT department, known as Information and Communication Development Centre (iDEC), has been helping CADe by supporting the infrastructure and networking for e-learning. The e-learning Governance in this university is systematic with enough numbers of staff with very specific and distinctive job roles.

Seven different versions of the LMS have been used since 1990s. E-learning started with the use of virtual online classes by Lotus Note. This usage was championed by Faculty of Economy and the Faculty of Computer Science. Then in 1999, by using a short term research fund, the university developed and implemented its own e-learning platform called the e-SPRINT. In 2000, the university cultivate the e-learning use by recommending e SPRINT - to be used by all lecturers. In 2003, another research was conducted to enhance the LMS functionalities. This time the lecturers' requirements were gathered. In 2008, a LMS is developed with collaboration from a vendor. The new system was developed using an open source and it is SCORM compliant. Subsequently in July 2009, the university implemented one official LMS named as Putra LMS and since February (semester 1) 2010 all lecturers are obliged to used PutraLMS only.

This university uses a blended learning with the platform ready for asynchronous and synchronous learning. PutraLMS is yet not integrated with any other systems. The university is working towards integrating PutraLMS with its other systems in the university.

Every lecturer has been encouraged to use e-learning in the teaching. Some lecturers have fully utilised the e-learning tools by having online classes, forum and organizing assignment submission. Some of them only use the basic functionalities such as uploading notes. The usage depends on the interest and not the age factor. Now the lecturers are obliged to use e-learning. The approach used now is top-down enforcement. Top management will monitor the usage among lecturers and the deans have to remind the lecturers to use the LMS.

CADe used a friendly approach by offering a simple LMS as a start. Gradually the LMS was upgraded and improved based on lecturers needs. CADe has requested that the lecturers to follow some steps in using the LMS. In the first semester every course should at least upload the course synopsis. In this case, CADe has uploaded the course synopsis which was taken from the course system. The lecturers need to at least upload the lecture notes in the LMS. It is targeted that 100% of the lecturers must use e-learning.

A road show on PutraLMS has been conducted to ensure that all lecturers are aware of the e-learning. Apart from that, training is also organised. CADe has conducted the training for trainers. Training for trainers on the PutraLMS was attended by the selected representative from each faculty, who had shown passion and interest in e-learning. These lecturers will become the trainers of e-learning at their faculty. This approach has been effective because of the friendly environment among colleagues. CADE itself offers Putra LMS training which is handled and organised by CADE staff every three months. This training is meant for those who are not able to attend the training conducted at their faculty.

Reasons why E-Learning is Implemented

It is the need and current trend.

Challenges and Issues

- It is difficult to get a 100% usage from lecturers. Not all lecturers are willing to spend the time and use the LMS. At the moment they only use the basic functionalities in LMS.

- It was also a challenging time during the transformation from the old LMS platform to new LMS platform. Many lecturers complained about the difficulties in using the new LMS. However, after the old LMS was shut down, everyone had to move to use the new LMS.

Acceptance of e-learning among lecturers, students

Lecturer usage is acceptable. This university is cultivating the e-learning use among lecturers.

Students' acceptance is excellent. They are excited about using e-learning.

Support from the top management regarding the e-learning implementation

E-learning here is a top-down approach. Therefore top management has been very supportive on e-learning implementation in this university. The Vice Chancellor had been involved in activities related to e-learning, for example, he had presented a keynote at an e-learning seminar.

Future Plan- Addressing the Issues and Challenges

- Conduct more training - every months
- Conduct training to guide on content development. Lecturers can choose any preferable software and CADe will assist them to learn the software.

Security Threats and incidents

Common security threats in e-learning

There are no serious threats in e-learning. However there is a stage where a manual data transfer needs to be done weekly due integration problem of the LMS with other systems. During this manual data transfer process some common security threats are:

- Data leaked
- Data missing due to human error while entering the data especially during the time out.

Security incidents on the e-learning system

The system broke down. However it is not serious since everyone is informed about this testing situation.

The control and countermeasures that have been implemented to safeguard the e-learning environment

The e-learning server is located at a data centre (iDEC) and the data centre is equipped with suitable controls and is manage by the IT department

According to CADe, there are no security issues for e-learning. However as iDEC is in charge of security for the whole system in the university, they might know more.

Summary of Interview in University 6

Background Respondents

A Deputy Director of ICT Centre

An Information Technology Officer

Both people manage the e-learning system portal called Myguru2 for the university. The Information & Communication Technology (ICT) Centre has been assisting and supporting the Centre for Educational Technology & Multimedia (CETM) in technical and technology services for Myguru2.

The ICT centre was established on 11 June 2001. It provides the latest information and technology services to assist all staff and students. Besides managing the databases for university, this centre aims to have more university students to be well versed with the information system employed.

E-learning implementation

E-learning is managed by the Centre for Educational Technology & Multimedia (CETM). In order to cultivate e-learning systems to complement the teaching and learning of an institute of higher learning, CETM also provides facilities for maintenance and repair of instructional technology equipment and offer advice on the selection and purchase of teleconference technology equipment. CETM is responsible for developing the policy and training regarding e-learning learning management system (LMS).

This university uses blended learning where the traditional classroom remains and e-learning is used as supporting tools in teaching and learning. The use of e-learning started in 1999 when WebCT was used and managed by the Faculty of Information Technology for teaching and learning. In 2003, e-learning was offered to all faculties using a LMS named Myguru (myteacher). The centralised Myguru was developed in 2003 and was integrated with an integrated information system.

In 2007 the university bought a new LMS from other university in Malaysia. The LMS was called Myguru2. Through the memorandum of agreement made by both universities, this university have the freedom to configure and enhance the system. Together with vendor's collaboration this university continuously improved and expanded the system based on the university's needs and culture.

E-learning was implemented using a top down approach and a centralised system. The e-learning method was offered to the undergraduate and postgraduate students.

In the early stage of Myguru2, lecturers were encouraged to use it as teaching and learning tools and it was an optional choice. They were allowed to browse through the system and became more familiar with it.

In 2008, the university developed an e learning and LMS policy to intensify the embracement of the e-learning culture. At the same time, the encouragement of LMS use is conducted in two phases.

- Phase 1- Teaching plan for every course should be uploaded. 95% of courses have been uploaded.
- Phase 2- Upload at least one teaching material.

Content was developed by the lecturer themselves with the help from the e-learning expert team (ELET). The team consists of lecturers that are expert in information communication technology and they will assist the other lecturers that need help in preparing the teaching and learning content.

The LMS is now ready to be used for more activities online, however the lecturers are not ready to use them widely.

Reasons E-Learning is implemented

E-learning is implemented to provide more amenities to students and it offers a lot of benefits. Students can access the learning materials at anytime and anywhere, and can easily be sent important information regarding their courses through the announcement menu from the LMS. Students also have the opportunities to receive assignment questions and submit assignment answer via online. There are also facilities for student to check their understanding on the course by taking the quizzes online.

Challenges and Issues

In the earlier stage of e-learning implementation, this university was having an issue with the e-learning system. It is difficult to customize the system so that it meets the university needs and culture. The university uses blended learning so the system should reflect this learning style.

Another issue is the low acceptance by lecturers with only 30% using the e-learning system. However, after the enforcement of the e-learning policy the usage has been increased to almost 100%.

Acceptance of e-learning among lecturer, students

Students' acceptance is very good. In fact they are the most demanding group and insist on the use of e-learning in teaching and learning.

The lecturers' acceptance has improved with the enforcement of e-learning policy.

Support from the top management regarding the e-learning implementation

Top management is very supportive of the e-learning implementation. The Deputy Vice Chancellor (Academic & International) specifically has really emphasised the usage of e-learning among lecturers. Reports on e-learning usage need to be sent regularly to the deputy vice chancellor for his review. Top management also have showed their support by approving the upgrade of the ICT infrastructure.

Future Plan- Addressing the Issues and Challenges

This university is gradually increasing the culture of e-learning among the staff. They are taking steps to encourage the lecturers to use e-learning. For example developing a policy for e-learning and setting up committee for e-learning at the faculty or school. The committee will guide and help on the use of e-learning. They will act as an e-learning catalyst at their respective faculty.

Security Threats and incidents

Common security threats in e-learning

So far there are no threats in e-learning.

Security incidents on e-learning system

There has not been a specific security incident on LMS but the university website created using Joomla had been hacked once.

The control and countermeasures that had been implemented to safeguard the e-learning environment

For intrusion prevention, the university is using a firewall. Three servers are used to manage the LMS. If any of the servers went down, the other two servers will take over. All activities are backed up using tape in the university and another back up is also conducted by a disaster recovery centre at one of the internet service providers in the country. Besides using technical control, awareness on security has been disseminated. The ICT Centre regularly organises ICT training and has sent reminders in the form of digital posters through email and pasting physical posters on the wall.

Obstacles and challenges in safeguarding e-learning

At the moment there are no obstacles and challenges in safeguarding the e-learning.

Summary -Interview in University 7

Background Respondents

A Deputy Director (e-Learning) of Centre for Academic Development (CADE). His task is to manage e-learning in the university).

Previously e-learning was managed by the IT department. After considering that e-learning is part of the teaching and learning processes, the E-learning unit was established under CADE in 2006. This unit's responsibilities are to:

- Plan, synchronize and monitor e-Learning implementation.
- Increase literacy and training related to e-learning.
- Control, monitor and enhance the quality of teaching and e-learning contents.

The first task after being appointed in 2006 was to design an e-learning policy for e-learning. After several meetings the policy was endorsed and has been used in the university

E-learning implementation

The E-learning system management project was started in 2003 to assist in the dissemination of knowledge quickly, efficiently and effectively. LearningCare Portal was the first learning management system to be used as a medium of communication between students and lecturers in cyberspace. The university's computer centre has been responsible for providing support services in terms of preparation and maintenance of this portal.

E-learning is now managed by CADE. Besides having a team at CADE to enforce e-learning, CADE is also assisted by appointed coordinators at each faculty. Coordinator roles at the faculty institute or centre include:

- designing and implementing an e-learning programme that facilitates the e-learning policy compliance among academicians and students in the faculties, institutes and centres
- monitor and report on the implementation of e-learning at the faculties, institutes, centres level
- assist the faculties, institutes and centres in improving the literacy and training associated with e-learning
- control, monitor and improve the quality of teaching content and e-learning

This university used LearningCare as the first portal learning management system (LMS) in 2003. In 2008, the university developed and introduced a new LMS known as SPIN (Interactive learning and management system). This LMS is integrated with students' system database and student management system. Thus every student can access the LMS.

There are four SPIN engines used in the university campus, including Bangi SPIN for campus residents in Bangi, Medic SPIN for campus residents in Kuala Lumpur, Training SPIN and SPIN for Center of Education Advancement. Training SPIN was developed to support CADE on the implementation of training using a blended method to every university resident. SPIN for Center of Education Advancement is specially developed for the students enrolled in distance education and executive programs.

This university has endorsed e-learning its policy in 2008. This policy acts as guidance on the implementation of e-learning. In order to cultivate the e-learning usage among lectures, the policy includes three levels of usage:

1) Compulsory- course synopsis should be uploaded in the LMS by lecturers.
2) Encourage lecturer- enrich the teaching and learning material (include notes, quiz and forum online)
3) Interactive content- ultimately the content is interactive with Learning Object and SCORM compliance.

As of now, this university is entering the 3rd stage, encouraging lecturers to develop interactive content. Training using simple software to develop the content are provided by CADE.

This university is using blended learning and to be precise, e-learning is used as a supplementary tools for teaching and learning. The execution range varies among faculty. The usage is between 20-60% with an average of 40%. There are evaluation and rewards for e-learning usage. All lecturers are aware of the e-learning policy but there are no penalties if they don't want to use e-learning. Policy is disseminated using a booklet and published in a website.

Reasons why E-Learning is Implemented

This university perceive the need and importance of e-learning. Students nowadays are a net generation and the philosophy of the university is to provide a platform (for teaching and learning). This university perceive the technology as tools to enhance learning.

Challenges and Issues

1) This university is a research university, and has over emphasised of research rather than teaching and learning. Therefore it influenced the lecturers to apply less effort and emphasis learning.
2) The lecturer thinks that they are being force to do that.
3) Senior lecturer resistance. They foresee e-learning as a new work culture and burden for them.
4) Issue of copyright of content. Lectures don't want to share their learning materials with other people.

Acceptance of e-learning among lecturers, students

Lecturer resistance of e-learning is considered acceptable due to allowing the freedom of lecturer. In general students are happy with the e-learning method and enjoy using it. Students are ready and accept e-learning usage.

Support from the top management regarding the e-learning implementation

E-learning here has received full support from the VC. She has agreed upon the establishment of an e-learning committee and e-learning status should be tabled and reported to her.

Future Plan- Addressing the Issues and Challenges

- Include e-learning as a part of evaluation in a yearly appraisal form. This will make more people serious about using e-learning.
- Various areas of e-learning training provided to staff.
- Intensify the monitoring and encouragement of e-learning usage among lecturers.

- In the near future, residents will be able to access Internet via Wi-Fi access points where the university have security elements and requires registration.

Security Threats and incidents

Definition of security in e-learning

- Security protection from hackers/intruders, which may alter quizzes and content. It is to ensure the integrity of the content (safe and sound).
- To prevent misuse of the SPIN system, by using SPIN as a stepping stone to compromise other systems, i.e. using SPIN as a tool to collect data from other systems. SPIN is well integrated with other systems.

Common security threats in e-learning

Not aware of any.

Security incidents in e-learning

Not aware of any reported incident

The control and countermeasures that had been implemented to safeguard the e-learning environment

Not aware of any. This area is covered by IT department.

This university has policies and regulations on ICT. A chapter discusses about the usage of Internet and Intranet and another chapter discusses ICT security.

Summary of Interview in University 8

Background Respondents

A lecturer at the Faculty of Science and Technology. He has just been appointed as a the Coordinator of Learning Network Unit. This unit is under the Centre of Learning and Teaching Innovation. His job roles and scope of work include:

- Coordinating the e-learning system and any related technical problems and to manage the graphics and production related to teaching learning content.
- Managing the implementation of e-learning. Ensure that all lecturers use the learning management system – myLMS.
- Increasing the awareness among lecturers regarding the usefulness of the e-learning system.

He is being assisted by the IT department and the vendor to solve any infrastructure and application system problems.

An IT Officer handling the LMS

E-learning implementation

The initiative of embarking on e-learning has started in 2003 with benchmarking and making comparison of Learning Management System (LMS) platforms. In 2006, a LMS named e-Kulliyah was developed and tested for use. In 2008, a new LMS called myLMS ver. 4.0 (myLMS) was used to replace e-Kulliyah.

This university is using blended learning. Besides the face-to-face classes, which is the main method of teaching and learning, myLMS is utilised as a support tool to supplement the teaching and learning process. MyLMS platform is ready to support any synchronous and asynchronous learning. However, at the moment a more asynchronous mode of learning has been used. For example: publishing learning material as .pdf files and PowerPoint slides on the web, forum discussions, and assignment submissions. Students can access the e-learning system at anytime and anywhere. However the implementation is also subject to the lecturer willingness to commit to using the e-learning system.

The top management wants e-learning to be used as the support tools for learning. All the learning materials are uploaded in the LMS and the students can always use them as references. All lecturers are encouraged to use e-learning in their teaching. Training on how to use the LMS is provided every year to the lecturers who wish to use the e-learning method.

According to the system only 10% of lecturers are using the e-learning system. The university would like to increase the usage to 60—70%. Now the Vice chancellor has announced that every lecturer must use the LMS and the minimum content to be uploaded is the course information and synopsis. The top management can monitor which lecturer had been using the LMS.

The university has always received full support from the vendor if any problem rises. This university and the vendor are planning to collaborate on enhancing the LMS. The vendor will be involved in the system development while the university will conduct user requirement research. This effort is to ensure that the new version of LMS will suit the local needs (the university and its culture needs).

E-learning implementation has been divided into two phases: the usage and content development. The e-leraning is currently in the first stage, which is to encourage users, especially the lecturers, to use the LMS. Once the culture is cultivated, the university will move to the second stage, which is to concentrate on the rich content development.

LMS is also being used as a discussion platform among the staff and students club for example, University Students Association.

Reasons why E-Learning is Implemented

The Ministry of Higher education has emphasised the requirement that each university needs to have an e-learning platform.

- The embracement of e-learning is important so as to be on par with other public universities in Malaysia
- This method will help to ease the teaching and learning process. Example: lecturer prepares the material at the start of the semester and uploads it in the LMS. The lecturer can schedule the date to determine when the content will be available to the students. Lecturers can activate or deactivate each section of the content according to the course syllabus. Another example is assignment announcement and submission; where lecturers can announce the assignment and the students can always refer to the assignment question published on the LMS. The students can also submit the assignment using the LMS.

Challenges and Issues

Poor acceptance among lecturers

- Transition from traditional method to e-learning.
- Literacy problem – Lecturers are reluctant to use e-learning as method of teaching and learning. This is due to ICT literacy problem and some of them think that the courses they are teaching don't need the ICT support.
- Language problem
- LMS is not user-friendly - Lecturers also claim that the interface is so plain and boring (not beautiful)

High Cost

- The implementation is costly in terms of money.

Acceptance of e-learning among lecturers, students

- Lecturers' acceptance is not very encouraging.
- Student's acceptance is good. However the usage of e-learning will be depending on the lecturers. The students will utilise the LMS if their lecturer does.

Support from the top management regarding the e-learning implementation

Top management has been very supportive regarding e-learning implementation, This can be seen by their effort in setting up a division especially to entertain and focus on e-learning matters. The top management has also suggested that an e-learning policy should be designed.

Future Plan- Addressing The Issues and Challenges

- Lecturers

Organise more training on how to use LMS. The training conducted will be faculty-based. Training on the benefit of using LMS for teaching and learning will be conducted to increase the awareness among lecturers. Besides providing training, lecturers' use of e-learning will be a criterion in lecturer's appraisal form. In addition to that lecturers also will be evaluated by students.

- Budget

Organise a workshop to gain user requirements. By having this requirement a budget can be requested.

- Design e-learning policy.

This university is designing an e-learning policy and hope to enforce it by end of this year.

Security Threats and incidents

Common security threats in e-learning

Previously, bugs in the LMS and server breakdown were the main security threats for e-learning. However, currently no threats have been recognised as the LMS is not fully used. The university is focusing to encourage users to engage in e-learning.

Security incidents in the e-learning system

The server cannot be accessed for 12 hours due to integration issues with other application systems.

The control and countermeasures that have been implemented to safeguard the e-learning environment

Set up of a firewall and other common security controls and countermeasures. Data storage and database for e-learning is located at a specific place.

Summary of Interview in University 9

Background Respondents

A Professor of School of Industrial Technology. He was appointed in 2010 as a coordinator of e-learning. His task is to guide the implementation e-learning in the university. He has been one of the key players in the implementation of e-learning.

A Chief Technology Officer/ Head of Department for Centre for Knowledge, Communication and Technology (CKCT). His tasks include ensuring the infrastructure and technical details for e-learning implementation in the university are in place.

E-learning implementation

This university started using internet-based e-learning in 2002, which was used purposely to entertain distance learning program students. The distance learning centre had developed a Learning Management System (LMS) named 'Interactive Distance Education Application' (IDeA) for that purpose.

After conducting benchmarking and comparison on different types of LMS in the market, the IDeA system was changed to a new LMS in 2004. The new LMS was developed using an open source called 'Moodle', where the usage has been extended to all other schools for the bachelor degree program. Each school was encouraged to use the LMS 'Moodle' as an e-learning platform. At this stage, decentralised e-learning is used, in which every school has their own LMS 'Moodle and using their own server. No proper governance or specific organisation structure has been organised for e-learning. The e-learning platform has been used according to individual preferences and has been receiving full support and help from IT department (CKCT) regarding the technical aspects.

In 2009, implementation of e-learning gradually became more focused and structured. A coordinator was appointed to guide and manage the e-learning implementation systematically. The coordinator is assisted by the unofficial unit called elearn@USM and positioned under the deputy vice chancellor office. A centralised 'Moodle' LMS is used for all schools and is named as e-Learn@USM. E-learn@USM is integrated with the centralised database. Thus allows the lecturers to automatically view their courses and students via the LMS at the beginning of every semester.

e-Learn@USM has two main roles in teaching and learning process. The first role is to provide an online learning activities and the second is as a resource for learning software and tools. The centralised e-learn@USM has been in production for two years and the students' acceptance is highly encouraging. On average, 24% of students and lecturers have logged into the e-learn@USM every day for teaching and learning purposes. E-learning is used as a supporting tool for learning. It is a blended learning with using more asynchronous mode.

This university has conducted a continuous series of training sessions for lecturers every semester on using the LMS and developing e-learning content. The e-learning content is lecturers' responsibility. At the moment there is no particular department developing the learning content. However, the IT department (CKCT) and Training Unit are able to facilitate lecturers in preparing the learning content.

Reasons why E-Learning is Implemented

- recognise the importance of e-learning. It can enrich the learning experience
- see the advantages of technology and use the technologies and tools developed for teaching and learning purposes
- E-learning is used to create awareness among staff (lecturers) of various tools that can be used to enhance learning.

Challenges and Issues

Support-

In the early stage, the e-learning agenda was started by individuals' enthusiasm and effort. The management groups, either from top or middle levels were not determined enough for the implementation of e-learning. The top level management particularly from the academic department did gave some support for the implementation, nevertheless there are no proactive actions taken to encourage all residents to use e-learning in their teaching. Lack of support received from the administration and management (dean) of each school allowed the lecturers to disregard the eLearn@USM LMS. The Dean of schools didn't seriously emphasise or encourage e-learning usage among the faculty members.

After the ministry of higher education in Malaysia highlighted on the usage of e-learning in the higher education institution in 2008, accentuation towards e-learning implementation has positively increased. It is expected in one or two years' time that support for e-learning implementation and usage will be received from every level.

There is no proper planning on e-learning implementation. Due to the absence of a physical unit or office to address and administer e-learning matters and the absent of a champion from top management, it is difficult to enforce e-learning on every lecturer. E-learning in this university is more to the individual passion. These individuals have set up a small group to start e-learning in this university and set up a virtual committee to handle the e-learn@USM portal.

Awareness

There is lack of awareness on the importance and benefit of e-learning and how e-learning can help in the teaching and learning process. Due to this, there was much resistance from the lecturer. Many of them preferred the conventional method of teaching in learning. Mostly this occurs in the senior cohorts of lecturers who are not willing to learn new things and to implant new things in teaching. This is the group of users that are difficult to convince on using e-learning in their teaching. It is a mindset challenge. They have a mind set on 'no need' for e-learning. They argue 'many of their students succeed and excelled in their studies even with the use of chalk and board, therefore why should we use a new method called e-learning'.

The lecturers also think that 'it is too time consuming to prepare the e-learning content, yet no credits is given to their effort. Lecturer spend many hours of preparing the e-learning content but when it comes to promotion, yearly appraisal, and evaluation the e-learning effort has not been considered and given credits.

Acceptance of e-learning among lecturers, students

E-learning has received a low acceptance among lecturers. Most of them are not willing to prepare the e-learning content because they think this will take huge amount of time. On the other hand, students are happy and appreciate the new learning experience. According to a survey conducted by a lecturer for his course, students have given positive feedback on learning using e-learning method.

They also put some comments on the computer and internet facilities provided by the university. Due to the access speed being too low for off-campus, the students have to be on campus and use the facilities provided. Unfortunately there are not enough facilities and they have to go to the nearest cybercafé which means that have to fork out some money to use the computer. This is contrary the objective of e-learning which is to be accessible at anywhere and reduce the cost. Instead it increases the students' cost.

Support from the top management regarding the e-learning implementation

Now the support from the top management has increased. With approval from the top management e-learn@USM is now under supervision and management of Deputy Vice Chancellor, Academic & International Affairs office. Top management has appointed a coordinator and two personnel to administer e-learn@USM. The budget cost for e-learning implementation also can be requested via provision from the Academic & International Affairs office.

Future Plan- Addressing the Issues and Challenges

1) Design an e-learning policy

The university will set up a policy regarding e-learning and addresses the specification that meets the university culture. The ministry of higher education is also in the process of designing a policy for all universities. Therefore the university's policy should be in line with the policy set out by the ministry of higher education. Currently this university is planning to organise a workshop on e-learning policy which will involve the deans and representatives of lecturers.

Example of specification that can be set up by the universities:

For the entire full time course, x % of the course should be done by e-learning. Once the policy is addressed, and cascaded down to the school level, the dean will have to make actions to meet the target. This will act as a pushing factor.

2) Awareness Programme

Awareness of e-learning benefit

Disseminate and promote the benefit and usage of e-learning to the lecturers by organising seminars and workshops on e-learning. This also could be done by spreading the information via email, pamphlets and also official letters released by the deputy vice chancellor and deans of schools.

Awareness on e-learning application and tools

Conduct training on how to use the LMS and the supporting tools to prepare the teaching and learning materials.

This university would like to encourage the embracement of ICT in teaching and learning among all lecturers. Therefore an awareness program including seminars, workshops and training will be organised and attended by all lecturers. Previously the attendance was on a voluntary basis and only the enthusiastic lecturers have shown up in any programme for e-learning. Therefore, a top down approach will be put into effect. An effort is being worked out to enable the attendee of the training to be nominated and suggested by the deans of schools and no longer to be on voluntary basis. Support from the deputy vice chancellor is needed to enforce the programmes. The deputy vice chancellor's office will send a memo to the deans of schools to nominate the candidates for the awareness program.

Both awareness programmes are conducted with collaboration of the Training unit. The training includes 3 levels:

Level I : Basic Moodle

Level II : Intermediate

- Multimedia Essential
- Authoring Tools (Articulate, Lecture Maker)

Level III: Students-Centred Learning using Learning Activity Management System (LAMS)

Level I and II training was offered to the lecturers in the 2009/2010 academic year, while Level III training was conducted in the 2010/2011 academic year. It includes hands-on training and using a module developed by e-learning facilitators. Ten facilitators were involved to train lectures in three different campuses. In the 2009/2010 academic year, 278 lecturers in semester 1 and 218 lecturers in semester II have undergone the training.

3) Incentive, Award and Acknowledgement

This university should reward and acknowledge the lecturers that actively use e-Learn@USM, and also to those that contribute excellently to e-learning by conducting research and development in the e-learning area. Every year lecturers will be evaluated based on the annual work target (AWT) for the annual salary movement. Therefore it is hoped that this university will take into account the involvement of lecturers in the e-Learn@USM undertaking their evaluation.

4) Special unit or department dedicated for managing e-learning implementation

A proposal for having an e-learn@USM unit / department with its own staff and funding has been drafted. This unit is dedicated to manage and oversee the implementation of e-learning. The infrastructure and infostructure needs to be enhanced to be able to support the implementation of e-learn @USM effectively. It is important that the top management provide undivided support to the university e-learning agenda. This support includes the allocation of funding and suitable employment.

Security Threats and incidents

Common security threats in e-learning

Before the security infrastructure and equipment were upgraded, threats like viruses and worms had regularly attacked the network, resulting in a constant denial of services. However after the major upgrade to the university's network infrastructure with an intelligent security system, many threats are now controllable, attacks are detectable and the network services remain buoyant.

Security incidents on e-learning system

Few years ago, there were incidents that affected the LMS, which were caused by lecturers setting up a system on their own server. These Moodle –LMS is decentralised and not controlled or monitored by the Centre for Knowledge, Communication and Technology (CKCT). As an open source, Moodle source codes are in public domain and a patch is required from time to time to overcome any vulnerability issues. However, due to lack of awareness regarding this security situation, the lecturers didn't apply the patch which caused the system to be able to be tampered with and fabricated by others.

Lessons were learned from these incidents. The university had centralised the LMS and requested that all lecturers must use it. With these, it is easier to manage and maintain the LMS usage and security as well.

With the use of centralisation of the LMS, there has been no major incident reported.

The control and countermeasures that have been implemented to safeguard the e-learning environment

Security in this university is administered by IT department also known as the Centre for Knowledge, Communication and Technology (CKCT). There is a team that manage the security issues and incidents.

CKCT has been supporting the e-learning implementation from the technical aspect. It has implemented security to the central infrastructure that is USM.net and security on Moodle -LMS itself. Moodle-LMS server is placed in the server farm and handled by the CKCT.

CKCT ensure the security of the whole system by using a firewall and implementing appropriate monitoring of the network activities. At the moment the university is using the system security with 40G. It is a powerful system that many sites have been block for use.

In this university there is an information communication technology Security Officer who has been appointed to monitor the CKCT and the security issues. If there is any incident it should be reported to ICTSO and ICTSO will report that to the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU).

CKCT also provides security awareness services to inform and educate the residents on security issues. It provides training with different modules related to security and is also responsible for information promulgation on security by using the website and pamphlets. Examples of training available are:

1. Basic ICT security and cyber threats
2. Security and Ethical use of email
3. Safety use of Internet resources and use of password
4. Back up and information recovery
5. Antimalware use

Obstacles and challenges in safeguarding e-learning

Not all lecturers and students aware of security issues. They just use the services that are provided by the CKCT.

Threats do exist and with the advance of technology and knowledge, security is always an issue. When dealing with security threats, it is always important to plan how to respond or take action. Some security issues can be predicted and so avoided from happening, but some threats are unpredictable as to when and how they are going to occur. Therefore continuous monitoring and proper infrastructure governance and management of security also should in place.

Appendix J Risk Analysis on Stakeholders Cultural View

Risk Analysis - Top Management

No.	Stakeholder Function	Task	Threats	Likelihood value based on culture view topology HIE	Impact value	Controls	Effectiveness value based on culture view topology HIE	RPN HIE
1	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Data entry error	4	4	Users are given security education and technical training	1	16
2	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Installation and maintenance errors	1	4	Strict control are exercised over the implementation of software on operational systems	1	4
3	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Installation and maintenance errors	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	4
4	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Error of authorisation or in the instructions	3	5	Information access restriction	1	15
5	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Error of authorisation or in the instructions	3	5	Users have access only to the services that they are authorised to use	1	15
6	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Transmission errors	1	4	Security of electronic office system	2	8
7	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Transmission errors	1	4	Data and software exchange agreement	4	16
8	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Transmission errors	1	4	Users are given security education and technical training	1	4
9	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Operational support error	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	5

10	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Operational support error	1	5	Users are given security education and technical training	1	5
11	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Use of software in unauthorised way	2	4	Users have access only to services that they are authorised to use	1	8
12	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Use of software in unauthorised way	2	4	Job description shall define security roles and responsibilities	2	16
13	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Use of software in unauthorised way	2	4	Event logging	1	8
14	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Illegal use of software	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	1	8
15	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Illegal use of software	2	4	Use of system utilities	1	8
16	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Illegal use of software	2	4	Job description shall define security roles and responsibilities	1	8
17	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Accidental deletion of data	4	4	Users are given security education and technical training	2	32
18	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Accidental destruction of software programs	4	3	Users are given security education and technical training	2	24
19	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Accidental destruction of configurations or hardware.	1	3	Users are given security education and technical training	1	3
20	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Leaving weaknesses (vulnerabilities) in software	1	5	Users are given security education and technical training	1	5
21	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Carelessness	5	5	A range of security controls are established to protect data in computer networks	3	75
22	Develop a strategic plan	Enhance the e-learning infrastructures and	Carelessness	5	5	Users are given security education and	3	75

	for e-learning implementation	facilities				technical training		
23	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Carelessness	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	75
24	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Insufficient authentications, weak password recovery validation	1	5	A range of security controls are established to protect data in computer networks	1	5
25	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Insufficient Authorisation, Insufficient Session Expiration	1	5	A range of security controls are established to protect data in computer networks	1	5
26	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Insufficient Authorisation, Insufficient Session Expiration	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	5
27	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Information disclosure	5	5	Users are given security education and technical training	2	50
28	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Information disclosure	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	50
29	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Data entry error	4	4	Users are given security education and technical training	1	16
30	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Installation and maintenance errors	1	4	Strict control are exercised over the implementation of software on operational systems	1	4
31	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Installation and maintenance errors	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	4
32	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Error of authorisation or in the instructions	3	5	Information access restriction	1	15

33	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Error of authorisation or in the instructions	3	5	Users have access only to the services that they are authorised to use	1	15
34	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Transmission errors	3	4	Security of electronic office system	1	12
35	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Transmission errors	3	4	Data and software exchange agreement	1	12
36	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Transmission errors	3	4	Users are given security education and technical training	2	24
37	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Operational support error	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	5
38	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Operational support error	1	5	Users are given security education and technical training	1	5
39	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Use of software in unauthorised way	2	4	Users have access only to services that they are authorised to use	1	8
40	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Use of software in unauthorised way	2	4	Job description shall define security roles and responsibilities	1	8
41	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Use of software in unauthorised way	2	4	Event logging	1	8
42	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Illegal use of software	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	1	8
43	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Illegal use of software	2	4	Use of system utilities	1	8
44	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Illegal use of software	2	4	Job description shall define security roles and responsibilities	1	8
45	Develop a strategic plan for e-learning	Collaboration with other parties	Accidental deletion of data	5	4	Users are given security education and technical training	3	60

	implementation							
46	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Accidental destruction of software programs	5	3	Users are given security education and technical training	3	45
47	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Accidental destruction of configurations or hardware	1	3	Users are given security education and technical training	1	3
48	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Leaving weaknesses (vulnerabilities) in software	1	5	Users are given security education and technical training	1	5
49	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Carelessness	5	5	A range of security controls are established to protect data in computer networks	2	50
50	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Carelessness	5	5	Users are given security education and technical training	3	75
51	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Carelessness	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	50
52	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Insufficient authentications, weak password recovery validation	1	5	A range of security controls are established to protect data in computer networks	1	5
53	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Insufficient Authorisation, Insufficient Session Expiration	1	5	A range of security controls are established to protect data in computer networks	1	5
54	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Insufficient Authorisation, Insufficient Session Expiration	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	5
55	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Information disclosure	5	5	Users are given security education and technical training	3	75

56	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Information disclosure	5	5	Users are required to follow good security practices (i.e. in the selection and use of password)	3	75
57	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Data entry error	5	4	Users are given security education and technical training	3	60
58	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Installation and maintenance errors	1	4	Strict control are exercised over the implementation of software on operational systems	1	4
59	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Installation and maintenance errors	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	4
60	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Error of authorisation or in the instructions	3	5	Information access restriction	1	15
61	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Error of authorisation or in the instructions	3	5	Users have access only to the services that they are authorised to use	1	15
62	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Transmission errors	3	4	Security of electronic office system	1	12
63	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Transmission errors	3	4	Data and software exchange agreement	3	36
64	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly	Transmission errors	3	4	Users are given security education and technical training	2	24

		confidential and high impact information.						
65	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Operational support error	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	5
66	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Operational support error	1	5	Users are given security education and technical training	1	5
67	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Use of software in unauthorised way	3	4	Users have access only to services that they are authorised to use	1	12
68	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Use of software in unauthorised way	3	4	Job description shall define security roles and responsibilities	2	24
69	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Use of software in unauthorised way	3	4	Event logging	1	12
70	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Illegal use of software	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	2	16
71	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Illegal use of software	2	4	Use of system utilities	1	8
72	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly	Illegal use of software	2	4	Job description shall define security roles and responsibilities	2	16

		confidential and high impact information.						
73	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Accidental deletion of data	5	4	Users are given security education and technical training	3	60
74	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Accidental destruction of software programs	5	3	Users are given security education and technical training	3	45
75	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Accidental destruction of configurations or hardware.	1	3	Users are given security education and technical training	1	3
76	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Leaving weaknesses (vulnerabilities) in software	1	5	Users are given security education and technical training	1	5
77	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Carelessness	5	5	A range of security controls are established to protect data in computer networks	2	50
78	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Carelessness	5	5	Users are given security education and technical training	3	75
79	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Carelessness	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	50
80	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly	Insufficient authentications, weak password recovery	1	5	A range of security controls are established to protect data in computer networks	1	5

		confidential and high impact information.	validation					
81	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Insufficient Authorisation, Insufficient Session Expiration	1	5	A range of security controls are established to protect data in computer networks	1	5
82	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Insufficient Authorisation, Insufficient Session Expiration	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	5
83	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Information disclosure	5	5	Users are given security education and technical training	3	75
84	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Information disclosure	5	5	Users are required to follow good security practices (i.e. in the selection and use of password)	3	75

Risk Analysis - Top Management

No.	Stakeholder Function	Task	Threats	Likelihood value based on culture view topology HIE	Impact value	Controls	Effectiveness value based on culture view topology HIE	RPN HIE
1	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Data entry error	4	4	Users are given security education and technical training	1	16
2	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Installation and maintenance errors	1	4	Strict control are exercised over the implementation of software on operational systems	1	4
3	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Installation and maintenance errors	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	4
4	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Error of authorisation or in the instructions	3	5	Information access restriction	1	15
5	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Error of authorisation or in the instructions	3	5	Users have access only to the services that they are authorised to use	1	15
6	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Transmission errors	1	4	Security of electronic office system	2	8
7	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Transmission errors	1	4	Data and software exchange agreement	4	16
8	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Transmission errors	1	4	Users are given security education and technical training	1	4
9	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Operational support error	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	5

10	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Operational support error	1	5	Users are given security education and technical training	1	5
11	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Use of software in unauthorised way	2	4	Users have access only to services that they are authorised to use	1	8
12	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Use of software in unauthorised way	2	4	Job description shall define security roles and responsibilities	2	16
13	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Use of software in unauthorised way	2	4	Event logging	1	8
14	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Illegal use of software	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	1	8
15	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Illegal use of software	2	4	Use of system utilities	1	8
16	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Illegal use of software	2	4	Job description shall define security roles and responsibilities	1	8
17	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Accidental deletion of data	4	4	Users are given security education and technical training	2	32
18	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Accidental destruction of software programs	4	3	Users are given security education and technical training	2	24
19	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Accidental destruction of configurations or hardware.	1	3	Users are given security education and technical training	1	3
20	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Leaving weaknesses (vulnerabilities) in software	1	5	Users are given security education and technical training	1	5

21	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Carelessness	5	5	A range of security controls are established to protect data in computer networks	3	75
22	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Carelessness	5	5	Users are given security education and technical training	3	75
23	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Carelessness	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	75
24	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Insufficient authentications, weak password recovery validation	1	5	A range of security controls are established to protect data in computer networks	1	5
25	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Insufficient Authorisation, Insufficient Session Expiration	1	5	A range of security controls are established to protect data in computer networks	1	5
26	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Insufficient Authorisation, Insufficient Session Expiration	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	5
27	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Information disclosure	5	5	Users are given security education and technical training	2	50
28	Develop a strategic plan for e-learning implementation	Enhance the e-learning infrastructures and facilities	Information disclosure	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	50
29	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Data entry error	4	4	Users are given security education and technical training	1	16
30	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Installation and maintenance errors	1	4	Strict control are exercised over the implementation of software on operational systems	1	4

31	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Installation and maintenance errors	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	4
32	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Error of authorisation or in the instructions	3	5	Information access restriction	1	15
33	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Error of authorisation or in the instructions	3	5	Users have access only to the services that they are authorised to use	1	15
34	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Transmission errors	3	4	Security of electronic office system	1	12
35	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Transmission errors	3	4	Data and software exchange agreement	1	12
36	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Transmission errors	3	4	Users are given security education and technical training	2	24
37	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Operational support error	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	5
38	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Operational support error	1	5	Users are given security education and technical training	1	5
39	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Use of software in unauthorised way	2	4	Users have access only to services that they are authorised to use	1	8
40	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Use of software in unauthorised way	2	4	Job description shall define security roles and responsibilities	1	8
41	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Use of software in unauthorised way	2	4	Event logging	1	8

42	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Illegal use of software	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	1	8
43	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Illegal use of software	2	4	Use of system utilities	1	8
44	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Illegal use of software	2	4	Job description shall define security roles and responsibilities	1	8
45	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Accidental deletion of data	5	4	Users are given security education and technical training	3	60
46	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Accidental destruction of software programs	5	3	Users are given security education and technical training	3	45
47	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Accidental destruction of configurations or hardware	1	3	Users are given security education and technical training	1	3
48	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Leaving weaknesses (vulnerabilities) in software	1	5	Users are given security education and technical training	1	5
49	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Carelessness	5	5	A range of security controls are established to protect data in computer networks	2	50
50	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Carelessness	5	5	Users are given security education and technical training	3	75
51	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Carelessness	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	50
52	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Insufficient authentications, weak password recovery validation	1	5	A range of security controls are established to protect data in computer networks	1	5

53	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Insufficient Authorisation, Insufficient Session Expiration	1	5	A range of security controls are established to protect data in computer networks	1	5
54	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Insufficient Authorisation, Insufficient Session Expiration	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	5
55	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Information disclosure	5	5	Users are given security education and technical training	3	75
56	Develop a strategic plan for e-learning implementation	Collaboration with other parties	Information disclosure	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	3	75
57	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Data entry error	5	4	Users are given security education and technical training	3	60
58	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Installation and maintenance errors	1	4	Strict control are exercised over the implementation of software on operational systems	1	4
59	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Installation and maintenance errors	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	4
60	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Error of authorisation or in the instructions	3	5	Information access restriction	1	15

61	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Error of authorisation or in the instructions	3	5	Users have access only to the services that they are authorised to use	1	15
62	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Transmission errors	3	4	Security of electronic office system	1	12
63	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Transmission errors	3	4	Data and software exchange agreement	3	36
64	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Transmission errors	3	4	Users are given security education and technical training	2	24
65	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Operational support error	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	5
66	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Operational support error	1	5	Users are given security education and technical training	1	5

67	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Use of software in unauthorised way	3	4	Users have access only to services that they are authorised to use	1	12
68	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Use of software in unauthorised way	3	4	Job description shall define security roles and responsibilities	2	24
69	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Use of software in unauthorised way	3	4	Event logging	1	12
70	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Illegal use of software	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	2	16
71	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Illegal use of software	2	4	Use of system utilities	1	8
72	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Illegal use of software	2	4	Job description shall define security roles and responsibilities	2	16

73	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Accidental deletion of data	5	4	Users are given security education and technical training	3	60
74	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Accidental destruction of software programs	5	3	Users are given security education and technical training	3	45
75	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Accidental destruction of configurations or hardware.	1	3	Users are given security education and technical training	1	3
76	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Leaving weaknesses (vulnerabilities) in software	1	5	Users are given security education and technical training	1	5
77	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Carelessness	5	5	A range of security controls are established to protect data in computer networks	2	50
78	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Carelessness	5	5	Users are given security education and technical training	3	75

79	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Carelessness	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	50
80	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Insufficient authentications, weak password recovery validation	1	5	A range of security controls are established to protect data in computer networks	1	5
81	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Insufficient Authorisation, Insufficient Session Expiration	1	5	A range of security controls are established to protect data in computer networks	1	5
82	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Insufficient Authorisation, Insufficient Session Expiration	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	5
83	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Information disclosure	5	5	Users are given security education and technical training	3	75
84	Manage the business	Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.	Information disclosure	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	3	75

Risk Analysis -E-learning Centre Personnel

				Likelihood value based on culture view topology					Effectiveness value based on culture view topology			RPN		
No.	**Stakeholder Function**	**Task/ behaviour**	**Threats**	**HIE**	**IND**	**EGA**	**Impact value**	**Controls**	**HIE**	**IND**	**EGA**	**HIE**	**IND**	**EGA**
1	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Data entry error	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
2	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	12	16	16
3	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Installation and maintenance errors	3	4	4	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	2	2	12	32	32
4	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Error of authorisation or in the instructions	3	4	4	5	Information access restriction	1	2	2	15	40	40
5	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Error of authorisation or in the instructions	3	4	4	5	Users have access only to the services that they are authorised to use	1	2	2	15	40	40
6	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
7	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Transmission errors	3	4	4	4	Data and software exchange agreement	2	2	2	24	32	32
8	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
9	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Operational support error	4	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	40	75	75
10	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Operational support error	4	5	5	5	Users are given security education and technical training	2	3	3	40	75	75
11	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Use of software in unauthorised way	1	3	3	4	Users have access only to services that they are authorised to use	1	2	2	4	24	24
12	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Use of software in unauthorised way	1	3	3	4	Job description shall define security roles and responsibilities	2	3	3	8	36	36
13	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Use of software in unauthorised way	1	3	3	4	Event logging	3	3	3	12	36	36

14	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Illegal use of software	1	3	3	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	36	36
15	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Illegal use of software	1	3	3	4	Use of system utilities	2	2	2	8	24	24
16	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Illegal use of software	1	3	3	4	Job description shall define security roles and responsibilities	1	2	2	4	24	24
17	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
18	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Accidental destruction of software programs	5	5	5	3	Users are given security education and technical training	2	3	3	30	45	45
19	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Accidental destruction of configurations or hardware.	5	5	5	3	Users are given security education and technical training	2	3	3	30	45	45
20	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Leaving weaknesses (vulnerabilities) in software	3	3	3	5	Users are given security education and technical training	2	3	3	30	45	45
21	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
22	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
23	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
24	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Insufficient authentications, weak password recovery validation	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
25	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45

26	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	3	3	45	45	45
27	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
28	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	2	2	50	50	50
29	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Data entry error	2	2	2	4	Users are given security education and technical training	2	3	3	16	24	24
30	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Installation and maintenance errors	2	2	2	4	Strict control are exercised over the implementation of software on operational systems	2	3	3	16	24	24
31	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Installation and maintenance errors	2	2	2	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	16	24	24
32	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Error of authorisation or in the instructions	3	3	4	5	Information access restriction	2	3	3	30	45	60
33	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Error of authorisation or in the instructions	3	3	4	5	Users have access only to the services that they are authorised to use	2	3	3	30	45	60
34	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Transmission errors	3	3	4	4	Security of electronic office system	1	1	1	12	12	16
35	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Transmission errors	3	3	4	4	Data and software exchange agreement	2	3	3	24	36	48

36	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Transmission errors	3	3	4	4	Users are given security education and technical training	2	3	3	24	36	48
37	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Operational support error	4	4	4	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	3	3	20	60	60
38	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Operational support error	4	4	4	5	Users are given security education and technical training	2	3	3	40	60	60
39	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Use of software in unauthorised way	2	2	2	4	Users have access only to services that they are authorised to use	1	2	2	8	16	16
40	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Use of software in unauthorised way	2	2	2	4	Job description shall define security roles and responsibilities	1	2	2	8	16	16
41	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Use of software in unauthorised way	2	2	2	4	Event logging	2	3	3	16	24	24
42	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Illegal use of software	2	2	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	1	1	1	8	8	8
43	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Illegal use of software	2	2	2	4	Use of system utilities	1	1	1	8	8	8
44	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Illegal use of software	2	2	2	4	Job description shall define security roles and responsibilities	1	2	2	8	16	16
45	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Accidental deletion of data	4	5	5	4	Users are given security education and technical training	2	3	3	32	60	60
46	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Accidental destruction of software programs	4	5	5	3	Users are given security education and technical training	2	3	3	24	45	45

47	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Accidental destruction of configurations or hardware.	4	5	5	3	Users are given security education and technical training	2	3	3	24	45	45
48	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Leaving weaknesses (vulnerabilities) in software	3	4	4	5	Users are given security education and technical training	2	3	3	30	60	60
49	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
50	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
51	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
52	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Insufficient authentications, weak password recovery validation	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
53	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
54	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	30	45	45
55	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
56	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	3	3	50	75	75

Risk Analysis - E-learning Centre Personnel Malaysia

No.	Stakeholder Function	Task/ behaviour	Threats	Likelihood value based on culture view topology			Impact Value	Controls	Effectiveness value based on culture view topology			RPN		
				HIE	IND	EGA			HIE	IND	EGA	HIE	IND	EGA
1	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Data entry error	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
2	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Installation and maintenance errors	4	5	5	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	16	20	20
3	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Installation and maintenance errors	4	5	5	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	3	3	16	60	60
4	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50
5	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Error of authorisation or in the instructions	4	5	5	5	Users have access only to the services that they are authorised to use	1	1	1	20	25	25
6	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
7	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Transmission errors	3	4	4	4	Data and software exchange agreement	3	3	3	36	48	48
8	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
9	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Operational support error	4	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	40	75	75
10	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Operational support error	4	5	5	5	Users are given security education and technical training	2	3	3	40	75	75
11	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Use of software in unauthorised way	1	3	3	4	Users have access only to services that they are authorised to use	1	2	2	4	24	24
12	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Use of software in unauthorised way	1	3	3	4	Job description shall define security roles and responsibilities	2	3	3	8	36	36
13	Championing a strategy to develop a successful e-learning	Manage the LMS	Use of software in unauthorised way	1	4	4	4	Event logging	3	3	3	12	48	48

	environment													
14	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Illegal use of software	1	4	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	48	48
15	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Illegal use of software	1	4	4	4	Use of system utilities	2	2	2	8	32	32
16	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Illegal use of software	1	4	4	4	Job description shall define security roles and responsibilities	1	2	2	4	32	32
17	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
18	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
19	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Accidental destruction of configurations or hardware.	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
20	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Leaving weaknesses (vulnerabilities) in software	3	3	3	5	Users are given security education and technical training	2	3	3	30	45	45
21	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
22	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
23	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
24	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Insufficient authentications, weak password recovery validation	3	4	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	60	45
25	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	60	45
26	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	3	3	45	60	45
27	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75

28	Championing a strategy to develop a successful e-learning environment	Manage the LMS	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	2	2	50	50	50
29	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Data entry error	3	3	3	4	Users are given security education and technical training	2	3	3	24	36	36
30	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Installation and maintenance errors	3	3	3	4	Strict control are exercised over the implementation of software on operational systems	2	3	3	24	36	36
31	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Installation and maintenance errors	3	3	3	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	24	36	36
32	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Error of authorisation or in the instructions	4	4	5	5	Information access restriction	2	3	3	40	60	75
33	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Error of authorisation or in the instructions	4	4	5	5	Users have access only to the services that they are authorised to use	2	3	3	40	60	75
34	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Transmission errors	4	4	5	4	Security of electronic office system	1	1	1	16	16	20
35	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Transmission errors	4	4	5	4	Data and software exchange agreement	2	3	3	32	48	60
36	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Transmission errors	4	4	5	4	Users are given security education and technical training	2	3	3	32	48	60
37	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Operational support error	5	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	3	3	25	75	75
38	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Operational support error	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
39	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Use of software in unauthorised way	2	2	2	4	Users have access only to services that they are authorised to use	1	2	2	8	16	16
40	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Use of software in unauthorised way	2	2	2	4	Job description shall define security roles and responsibilities	1	2	2	8	16	16
41	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Use of software in unauthorised way	2	2	2	4	Event logging	2	3	3	16	24	24
42	Championing a strategy to	Provide training on e-	Illegal use of software	2	2	2	4	Measures are taken to comply with	1	1	1	8	8	8

	develop a successful e-learning environment	learning applications and tools						contractual restrictions on the use of copyright materials							
43	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Illegal use of software	2	2	2	4	Use of system utilities	1	1	1	8	8	8
44	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Illegal use of software	2	2	2	4	Job description shall define security roles and responsibilities	1	2	2	8	16	16
45	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
46	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Accidental destruction of software programs	5	5	5	3	Users are given security education and technical training	2	3	3	30	45	45
47	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Accidental destruction of configurations or hardware.	5	5	5	3	Users are given security education and technical training	2	3	3	30	45	45
48	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Leaving weaknesses (vulnerabilities) in software	3	4	4	5	Users are given security education and technical training	2	3	3	30	60	60
49	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
50	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
51	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
52	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Insufficient authentications, weak password recovery validation	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
53	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
54	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	30	45	45
55	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
56	Championing a strategy to develop a successful e-learning environment	Provide training on e-learning applications and tools	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e. in the selection and use of password)	2	3	3	50	75	75

Risk Analysis - IT Personnel

				Likelihood value based on culture view topology					Effectiveness value based on culture view topology			RPN		
No.	**stakeholder function**	**Task/ behaviour**	**Threats**	**HIE**	**IND**	**EGA**	**Impact value**	**Controls**	**HIE**	**IND**	**EGA**	**HIE**	**IND**	**EGA**
1	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Data entry error	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
2	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	12	16	16
3	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Installation and maintenance errors	3	4	4	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	2	2	12	32	32
4	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Error of authorisation or in the instructions	4	4	4	5	Information access restriction	1	2	2	20	40	40
5	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Error of authorisation or in the instructions	4	4	4	5	Users have access only to the services that they are authorised to use	1	2	2	20	40	40
6	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
7	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Transmission errors	3	4	4	4	Data and software exchange agreement	2	2	2	24	32	32
8	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
9	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Operational support error	4	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	40	75	75
10	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-	Operational support error	4	5	5	5	Users are given security education and technical training	2	3	3	40	75	75

		learning centre)													
11	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Use of software in unauthorised way	1	3	3	4	Users have access only to services that they are authorised to use	1	2	2	4	24	24
12	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Use of software in unauthorised way	1	3	3	4	Job description shall define security roles and responsibilities	2	3	3	8	36	36
13	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Use of software in unauthorised way	1	3	3	4	Event logging	3	3	3	12	36	36
14	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Illegal use of software	1	3	3	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	36	36
15	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Illegal use of software	1	3	3	4	Use of system utilities	2	2	2	8	24	24
16	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Illegal use of software	1	3	3	4	Job description shall define security roles and responsibilities	1	2	2	4	24	24
17	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
18	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
19	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Accidental destruction of configurations or hardware.	5	5	5	3	Users are given security education and technical training	2	3	3	30	45	45
20	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Leaving weaknesses (vulnerabilities) in software	3	3	3	5	Users are given security education and technical training	2	3	3	30	45	45
21	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75

22	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
23	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
24	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Insufficient authentications, weak password recovery validation	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
25	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
26	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	3	3	45	45	45
27	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
28	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	2	2	50	50	50
29	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Data entry error	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
30	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	12	16	16
31	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Installation and maintenance errors	3	4	4	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	2	2	12	32	32
32	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50
33	Responsible on the technical part in	Working with external parties	Error of authorisation	4	5	5	5	Users have access only to the	1	2	2	20	50	50

	the e-learning environment and system	(LMS vendor) and/or develop system in house	or in the instructions					services that they are authorised to use						
34	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
35	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Transmission errors	3	4	4	4	Data and software exchange agreement	1	1	1	12	16	16
36	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
37	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Operational support error	3	4	4	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	30	60	60
38	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Operational support error	3	4	4	5	Users are given security education and technical training	2	3	3	30	60	60
39	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Use of software in unauthorised way	1	2	2	4	Users have access only to services that they are authorised to use	1	1	1	4	8	8
40	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Use of software in unauthorised way	1	2	2	4	Job description shall define security roles and responsibilities	2	3	3	8	24	24
41	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Use of software in unauthorised way	1	2	2	4	Event logging	3	3	3	12	24	24
42	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Illegal use of software	1	2	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	24	24
43	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Illegal use of software	1	2	2	4	Use of system utilities	2	2	2	8	16	16
44	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Illegal use of software	1	2	2	4	Job description shall define security roles and responsibilities	1	2	2	4	16	16
45	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Accidental deletion of data	1	2	2	4	Users are given security education and technical training	2	3	3	8	24	24
46	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Accidental destruction of software programs	5	5	5	3	Users are given security education and technical training	2	3	3	30	45	45
47	Responsible on the technical part in the e-learning environment and	Working with external parties (LMS vendor) and/or develop	Accidental destruction of configurations or	5	5	5	3	Users are given security education and technical training	2	3	3	30	45	45

	system	system in house	hardware.												
48	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Leaving weaknesses (vulnerabilities) in software	2	2	2	5	Users are given security education and technical training	2	3	3	20	30	30
49	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
50	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
51	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
52	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Insufficient authentications, weak password recovery validation	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
53	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
54	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	3	3	45	45	45
55	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
56	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	3	3	3	75	75	75
57	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Data entry error	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
58	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	2	2	2	24	32	32
59	Create a competent and efficient customer centre support service on e-learning , campus network and	Support the customers or users on IT services	Installation and maintenance errors	3	4	4	4	Documented procedures are provided for the operation of all computer systems and for systems	1	2	2	12	32	32

	telecommunication infrastructure							development, maintenance and testing						
60	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50
61	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Error of authorisation or in the instructions	4	5	5	5	Users have access only to the services that they are authorised to use	1	2	2	20	50	50
62	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
63	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Transmission errors	3	4	4	4	Data and software exchange agreement	1	2	2	12	32	32
64	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
65	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Operational support error	3	4	4	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	3	3	15	60	60
66	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Operational support error	3	4	4	5	Users are given security education and technical training	2	3	3	30	60	60
67	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Use of software in unauthorised way	3	4	4	4	Users have access only to services that they are authorised to use	1	2	2	12	32	32
68	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Use of software in unauthorised way	3	4	4	4	Job description shall define security roles and responsibilities	1	2	2	12	32	32
69	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Use of software in unauthorised way	3	4	4	4	Event logging	2	3	3	24	48	48
70	Create a competent and efficient customer centre support service on e-	Support the customers or users on IT services	Illegal use of software	1	2	2	4	Measures are taken to comply with contractual restrictions on the use	1	1	1	4	8	8

	learning , campus network and telecommunication infrastructure							of copyright materials							
71	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Illegal use of software	1	2	2	4	Use of system utilities	1	1	1	4	8	8
72	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Illegal use of software	1	2	2	4	Job description shall define security roles and responsibilities	1	2	2	4	16	16
73	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
74	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
75	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Accidental destruction of configurations or hardware.	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
76	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Leaving weaknesses (vulnerabilities) in software	3	4	4	5	Users are given security education and technical training	2	3	3	30	60	60
77	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
78	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
79	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
80	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Insufficient authentications, weak password recovery validation	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
81	Create a competent and efficient customer centre support service on e-	Support the customers or users on IT services	Insufficient Authorisation,	3	3	3	5	A range of security controls are established to protect data in	2	3	3	30	45	45

	learning , campus network and telecommunication infrastructure		Insufficient Session Expiration					computer networks						
82	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	30	45	45
83	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
84	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	3	3	3	75	75	75
85	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Data entry error	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
86	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	2	2	2	24	32	32
87	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Installation and maintenance errors	3	4	4	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	2	2	12	32	32
88	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50
89	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Error of authorisation or in the instructions	4	5	5	5	Users have access only to the services that they are authorised to use	1	2	2	20	50	50
90	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
91	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Transmission errors	3	4	4	4	Data and software exchange agreement	1	2	2	12	32	32
92	Provide operational support on the	Support the customers or users	Transmission errors	3	4	4	4	Users are given security education	2	3	3	24	48	48

	campus network and telecommunication infrastructure	on network and telecommunication infrastructure						and technical training						
93	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Operational support error	3	4	4	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	3	3	15	60	60
94	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Operational support error	3	4	4	5	Users are given security education and technical training	2	3	3	30	60	60
95	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Use of software in unauthorised way	3	4	4	4	Users have access only to services that they are authorised to use	1	2	2	12	32	32
96	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Use of software in unauthorised way	3	4	4	4	Job description shall define security roles and responsibilities	1	2	2	12	32	32
97	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Use of software in unauthorised way	3	4	4	4	Event logging	2	3	3	24	48	48
98	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Illegal use of software	1	2	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	1	1	1	4	8	8
99	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Illegal use of software	1	2	2	4	Use of system utilities	1	1	1	4	8	8
100	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Illegal use of software	1	2	2	4	Job description shall define security roles and responsibilities	1	2	2	4	16	16
101	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
102	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
103	Provide operational support on the	Support the customers or users	Accidental destruction	3	4	4	3	Users are given security education	2	3	3	18	36	36

	campus network and telecommunication infrastructure	on network and telecommunication infrastructure	of configurations or hardware.					and technical training						
104	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Leaving weaknesses (vulnerabilities) in software	3	4	4	5	Users are given security education and technical training	2	3	3	30	60	60
105	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
106	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
107	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
108	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Insufficient authentications, weak password recovery validation	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
109	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	45	45
110	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Insufficient Authorisation, Insufficient Session Expiration	3	3	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	30	45	45
111	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
112	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	3	3	50	75	75

Risk Analysis -IT Personnel Malaysia

				Likelihood value based on culture view topology					Effectiveness value based on culture view topology			RPN		
No.	**Stakeholder Function**	**Task/ behaviour**	**Threats**	**HIE**	**IND**	**EGA**	**Impact Value**	**Controls**	**HIE**	**IND**	**EGA**	**HIE**	**IND**	**EGA**
1	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Data entry error	3	5	5	4	Users are given security education and technical training	2	3	3	24	60	60
2	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Installation and maintenance errors	3	5	5	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	12	20	20
3	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Installation and maintenance errors	3	5	5	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	3	3	12	60	60
4	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50
5	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Error of authorisation or in the instructions	4	5	5	5	Users have access only to the services that they are authorised to use	1	2	2	20	50	50
6	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
7	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Transmission errors	3	4	4	4	Data and software exchange agreement	3	3	3	36	48	48
8	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
9	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Operational support error	4	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	40	75	75
10	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the	Operational support error	4	5	5	5	Users are given security education and technical training	2	3	3	40	75	75

		LMS, (collaborate with e-learning centre)												
11	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Use of software in unauthorised way	1	3	3	4	Users have access only to services that they are authorised to use	1	2	2	4	24	24
12	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Use of software in unauthorised way	1	3	3	4	Job description shall define security roles and responsibilities	2	3	3	8	36	36
13	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Use of software in unauthorised way	1	3	3	4	Event logging	3	3	3	12	36	36
14	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Illegal use of software	1	4	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	48	48
15	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Illegal use of software	1	4	4	4	Use of system utilities	2	2	2	8	32	32
16	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Illegal use of software	1	4	4	4	Job description shall define security roles and responsibilities	1	2	2	4	32	32
17	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
18	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
19	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Accidental destruction of configurations or hardware.	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
20	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Leaving weaknesses (vulnerabilities) in software	3	3	3	5	Users are given security education and technical training	2	3	3	30	45	45
21	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75

		learning centre)												
22	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
23	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	2	2	25	50	50
24	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Insufficient authentications, weak password recovery validation	3	4	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	60	45
25	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	60	45
26	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	3	3	45	60	45
27	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Information disclosure	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
28	Responsible on the technical part in the e-learning environment and system	Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	2	2	50	50	50
29	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Data entry error	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
30	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	12	16	16
31	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Installation and maintenance errors	3	4	4	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	3	3	12	48	48
32	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50

33	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Error of authorisation or in the instructions	4	5	5	5	Users have access only to the services that they are authorised to use	1	2	2	20	50	50
34	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
35	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Transmission errors	3	4	4	4	Data and software exchange agreement	3	3	3	36	48	48
36	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
37	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Operational support error	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	30	75	75
38	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Operational support error	3	5	5	5	Users are given security education and technical training	2	3	3	30	75	75
39	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Use of software in unauthorised way	1	3	3	4	Users have access only to services that they are authorised to use	1	1	1	4	12	12
40	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Use of software in unauthorised way	1	3	3	4	Job description shall define security roles and responsibilities	2	3	3	8	36	36
41	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Use of software in unauthorised way	1	3	3	4	Event logging	3	3	3	12	36	36
42	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Illegal use of software	1	4	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	48	48
43	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Illegal use of software	1	4	4	4	Use of system utilities	2	2	2	8	32	32
44	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Illegal use of software	1	4	4	4	Job description shall define security roles and responsibilities	1	2	2	4	32	32
45	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
46	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
47	Responsible on the technical part in the	Working with external parties	Accidental destruction	3	4	4	3	Users are given security	2	3	3	18	36	36

	e-learning environment and system	(LMS vendor) and/or develop system in house	of configurations or hardware.					education and technical training						
48	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Leaving weaknesses (vulnerabilities) in software	3	3	3	5	Users are given security education and technical training	2	3	3	30	45	45
49	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
50	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
51	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	50	75	75
52	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Insufficient authentications, weak password recovery validation	3	4	3	5	A range of security controls are established to protect data in computer networks	1	2	2	15	40	30
53	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	60	45
54	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	30	60	45
55	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Information disclosure	5	5	5	5	Users are given security education and technical training	3	3	3	75	75	75
56	Responsible on the technical part in the e-learning environment and system	Working with external parties (LMS vendor) and/or develop system in house	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	2	2	50	50	50
57	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Data entry error	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
58	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	12	16	16
59	Create a competent and efficient	Support the customers or users	Installation and	3	4	4	4	Documented procedures are	2	3	3	24	48	48

	customer centre support service on e-learning , campus network and telecommunication infrastructure	on IT services	maintenance errors					provided for the operation of all computer systems and for systems development, maintenance and testing						
60	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50
61	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Error of authorisation or in the instructions	4	5	5	5	Users have access only to the services that they are authorised to use	1	2	2	20	50	50
62	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
63	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Transmission errors	3	4	4	4	Data and software exchange agreement	3	3	3	36	48	48
64	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
65	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Operational support error	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	30	75	75
66	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Operational support error	3	5	5	5	Users are given security education and technical training	2	3	3	30	75	75
67	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Use of software in unauthorised way	1	3	3	4	Users have access only to services that they are authorised to use	1	1	1	4	12	12
68	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Use of software in unauthorised way	1	3	3	4	Job description shall define security roles and responsibilities	2	3	3	8	36	36
69	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Use of software in unauthorised way	1	3	3	4	Event logging	3	3	3	12	36	36

70	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Illegal use of software	1	4	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	48	48
71	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Illegal use of software	1	4	4	4	Use of system utilities	2	2	2	8	32	32
72	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Illegal use of software	1	4	4	4	Job description shall define security roles and responsibilities	1	2	2	4	32	32
73	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
74	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
75	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Accidental destruction of configurations or hardware.	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
76	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Leaving weaknesses (vulnerabilities) in software	3	3	3	5	Users are given security education and technical training	2	3	3	30	45	45
77	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
78	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
79	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	50	75	75
80	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Insufficient authentications, weak password recovery validation	3	4	3	5	A range of security controls are established to protect data in computer networks	1	2	2	15	40	30

81	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	60	45
82	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	30	60	45
83	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Information disclosure	5	5	5	5	Users are given security education and technical training	2	2	2	50	50	50
84	Create a competent and efficient customer centre support service on e-learning , campus network and telecommunication infrastructure	Support the customers or users on IT services	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	3	3	50	75	75
85	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Data entry error	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
86	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Installation and maintenance errors	3	4	4	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	12	16	16
87	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Installation and maintenance errors	3	4	4	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	24	48	48
88	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Error of authorisation or in the instructions	4	5	5	5	Information access restriction	1	2	2	20	50	50
89	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Error of authorisation or in the instructions	4	5	5	5	Users have access only to the services that they are authorised to use	1	2	2	20	50	50
90	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Transmission errors	3	4	4	4	Security of electronic office system	1	1	1	12	16	16
91	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication	Transmission errors	3	4	4	4	Data and software exchange agreement	3	3	3	36	48	48

		infrastructure												
92	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Transmission errors	3	4	4	4	Users are given security education and technical training	2	3	3	24	48	48
93	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Operational support error	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	2	3	3	30	75	75
94	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Operational support error	3	5	5	5	Users are given security education and technical training	2	3	3	30	75	75
95	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Use of software in unauthorised way	1	3	3	4	Users have access only to services that they are authorised to use	1	1	1	4	12	12
96	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Use of software in unauthorised way	1	3	3	4	Job description shall define security roles and responsibilities	2	3	3	8	36	36
97	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Use of software in unauthorised way	1	4	4	4	Event logging	3	3	3	12	48	48
98	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Illegal use of software	1	4	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	12	48	48
99	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Illegal use of software	1	4	4	4	Use of system utilities	2	2	2	8	32	32
100	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Illegal use of software	1	4	4	4	Job description shall define security roles and responsibilities	1	2	2	4	32	32
101	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Accidental deletion of data	5	5	5	4	Users are given security education and technical training	2	3	3	40	60	60
102	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication	Accidental destruction of software programs	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36

		infrastructure												
103	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Accidental destruction of configurations or hardware.	3	4	4	3	Users are given security education and technical training	2	3	3	18	36	36
104	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Leaving weaknesses (vulnerabilities) in software	3	3	3	5	Users are given security education and technical training	2	3	3	30	45	45
105	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	3	3	50	75	75
106	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Carelessness	5	5	5	5	Users are given security education and technical training	2	3	3	50	75	75
107	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	50	75	75
108	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Insufficient authentications, weak password recovery validation	3	4	3	5	A range of security controls are established to protect data in computer networks	1	2	2	15	40	30
109	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	A range of security controls are established to protect data in computer networks	2	3	3	30	60	45
110	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Insufficient Authorisation, Insufficient Session Expiration	3	4	3	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	3	3	30	60	45
111	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Information disclosure	5	5	5	5	Users are given security education and technical training	2	2	2	50	50	50
112	Provide operational support on the campus network and telecommunication infrastructure	Support the customers or users on network and telecommunication infrastructure	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	2	3	3	50	75	75

Risk Analysis - Lecturer

No.	Stakeholder Function	Task	Threats	Likelihood value based on culture view topology				Impact value	Controls	Effectiveness value based on culture view topology				RPN			
				FTL	HIE	IND	EGA			FTL	HIE	IND	EGA	FTL	HIE	IND	EGA
1	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Data entry error	5	4	4	4	4	Users are given security education and technical training	4	4	4	4	80	64	64	64
2	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Installation and maintenance errors	1	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	1	4	4	4	4
3	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Installation and maintenance errors	1	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	1	4	4	4	4
4	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Error of authorisation or in the instructions	1	5	2	4	5	Information access restriction	2	4	4	4	10	100	40	80
5	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Error of authorisation or in the instructions	1	5	2	4	5	Users have access only to the services that they are authorised to use	2	4	3	3	10	100	30	60
6	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Transmission errors	5	4	5	5	4	Security of electronic office system	3	3	3	3	60	48	60	60
7	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Transmission errors	5	4	5	5	4	Data and software exchange agreement	3	3	3	3	60	48	60	60
8	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Transmission errors	5	4	5	5	4	Users are given security education and technical training	4	4	4	4	80	64	80	80
9	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Operational support error	5	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	4	3	3	3	100	45	75	75
10	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Operational support error	5	3	5	5	5	Users are given security education and technical training	4	4	4	4	100	60	100	100
11	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Use of software in unauthorised way	5	2	5	5	4	Users have access only to services that they are authorised to use	3	2	4	4	60	16	80	80

12	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Use of software in unauthorised way	5	2	5	5	4	Job description shall define security roles and responsibilities	3	3	3	3	60	24	60	60
13	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Use of software in unauthorised way	5	2	5	5	4	Event logging	3	3	3	3	60	24	60	60
14	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Illegal use of software	5	2	5	5	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	3	60	24	60	60
15	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Illegal use of software	5	2	5	5	4	Use of system utilities	3	3	3	3	60	24	60	60
16	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Illegal use of software	5	2	5	5	4	Job description shall define security roles and responsibilities	3	3	3	3	60	24	60	60
17	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Accidental deletion of data	5	5	5	5	4	Users are given security education and technical training	4	4	4	4	80	80	80	80
18	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Accidental destruction of software programs	4	4	4	4	3	Users are given security education and technical training	4	4	4	4	48	48	48	48
19	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are given security education and technical training	1	1	1	1	3	3	3	3
20	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Leaving weaknesses (vulnerabilities) in software	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5
21	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Carelessness	5	5	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	75	75	75
22	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Carelessness	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
23	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Carelessness	5	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	50	100	100
24	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Insufficient authentications, weak password	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5

			recovery validation															
25	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
26	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
27	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Information disclosure	4	4	4	4	5	Users are given security education and technical training	4	4	4	4	80	80	80	80
28	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Information disclosure	4	4	4	4	5	Users are required to follow good security practices (i.e in the selection and use of password)	3	2	2	2	60	40	40	40
29	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Data entry error	5	4	4	4	4	Users are given security education and technical training	4	4	4	4	80	64	64	64
30	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Installation and maintenance errors	1	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	1	4	4	4	4
31	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Installation and maintenance errors	1	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	1	4	4	4	4
32	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Error of authorisation or in the instructions	3	5	2	4	5	Information access restriction	2	4	4	4	30	100	40	80
33	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Error of authorisation or in the instructions	3	5	2	4	5	Users have access only to the services that they are authorised to use	2	4	3	3	30	100	30	60
34	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Transmission errors	5	4	5	5	4	Security of electronic office system	3	3	3	3	60	48	60	60
35	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Transmission errors	5	4	5	5	4	Data and software exchange agreement	3	3	3	3	60	48	60	60

36	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Transmission errors	5	4	5	5	4	Users are given security education and technical training	4	4	4	4	80	64	80	80
37	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Operational support error	5	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	4	2	3	3	100	30	75	75
38	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Operational support error	5	3	5	5	5	Users are given security education and technical training	4	4	4	4	100	60	100	100
39	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Use of software in unauthorised way	5	2	5	5	4	Users have access only to services that they are authorised to use	2	1	1	1	40	8	20	20
40	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Use of software in unauthorised way	5	2	5	5	4	Job description shall define security roles and responsibilities	2	1	1	1	40	8	20	20
41	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Use of software in unauthorised way	5	2	5	5	4	Event logging	3	3	3	3	60	24	60	60
42	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Illegal use of software	2	2	2	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	4	3	4	4	32	24	32	32
43	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Illegal use of software	2	2	2	2	4	Use of system utilities	3	3	3	3	24	24	24	24
44	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Illegal use of software	2	2	2	2	4	Job description shall define security roles and responsibilities	2	1	1	1	16	8	8	8
45	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Accidental deletion of data	5	5	5	5	4	Users are given security education and technical training	4	4	4	4	80	80	80	80
46	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Accidental destruction of software programs	2	2	2	2	3	Users are given security education and technical training	4	4	4	4	24	24	24	24
47	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are given security education and technical training	1	1	1	1	3	3	3	3
48	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Leaving weaknesses (vulnerabilities) in software	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5

49	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Carelessness	5	5	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	75	75	75
50	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Carelessness	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
51	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Carelessness	5	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	50	100	100
52	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Insufficient authentications, weak password recovery validation	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
53	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
54	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
55	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Information disclosure	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
56	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Information disclosure	5	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	3	2	2	2	75	50	50	50
57	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Data entry error	3	2	2	2	4	Users are given security education and technical training	4	4	4	4	48	32	32	32
58	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Installation and maintenance errors	1	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	1	4	4	4	4

59	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Installation and maintenance errors	1	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	1	4	4	4	4
60	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Error of authorisation or in the instructions	3	5	2	4	5	Information access restriction	2	4	4	4	30	100	40	80
61	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Error of authorisation or in the instructions	3	5	2	4	5	Uusers have access only to the services that they are authorised to use	2	4	3	3	30	100	30	60
62	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Transmission errors	2	3	3	4	4	Security of electronic office system	3	3	3	3	24	36	36	48
63	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Transmission errors	2	3	3	4	4	Data and software exchange agreement	3	3	3	3	24	36	36	48
64	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Transmission errors	2	3	3	4	4	Users are given security education and technical training	4	4	4	4	32	48	48	64
65	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Operational support error	2	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	3	1	1	1	30	15	25	25
66	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Operational support error	2	3	5	5	5	Users are given security education and technical training	4	4	4	4	40	60	100	100
67	to provide technical and motivational support encouraging the use of e-learning to students and	share experiences and encourage use among lectures	Use of software in unauthorised way	5	2	5	5	4	Users have access only to services that they are authorised to use	2	1	1	1	40	8	20	20

	colleagues																	
68	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Use of software in unauthorised way	5	2	5	5	4	Job description shall define security roles and responsibilities	4	2	3	3	80	16	60	60
69	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Use of software in unauthorised way	5	2	5	5	4	Event logging	3	3	3	3	60	24	60	60
70	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Illegal use of software	5	2	5	5	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	2	2	2	2	40	16	40	40
71	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Illegal use of software	5	2	5	5	4	Use of system utilities	3	3	3	3	60	24	60	60
72	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Illegal use of software	5	2	5	5	4	Job description shall define security roles and responsibilities	4	2	3	3	80	16	60	60
73	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Accidental deletion of data	2	2	2	2	4	Users are given security education and technical training	4	4	4	4	32	32	32	32
74	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Accidental destruction of software programs	2	2	2	2	3	Users are given security education and technical training	4	4	4	4	24	24	24	24
75	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are given security education and technical training	1	1	1	1	3	3	3	3
76	to provide technical and motivational support encouraging the use of e-	share experiences and encourage use among lectures	Leaving weaknesses (vulnerabilities) in	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5

	learning to students and colleagues		software															
77	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Carelessness	5	5	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	75	75	75
78	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Carelessness	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
79	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Carelessness	5	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	50	100	100
80	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Insufficient authentications, weak password recovery validation	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
81	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
82	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
83	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Information disclosure	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
84	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Information disclosure	5	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	3	2	2	2	75	50	50	50

85	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Data entry error	3	2	2	2	4	Users are given security education and technical training	4	4	4	4	48	32	32	32
86	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Installation and maintenance errors	2	2	5	5	4	Strict control are exercised over the implementation of software on operational systems	2	2	2	2	16	16	40	40
87	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Installation and maintenance errors	2	2	5	5	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	4	2	3	3	32	16	60	60
88	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Error of authorisation or in the instructions	3	3	5	5	5	Information access restriction	2	4	4	4	30	60	100	100
89	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Error of authorisation or in the instructions	3	3	5	5	5	Users have access only to the services that they are authorised to use	2	4	3	3	30	60	75	75
90	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Transmission errors	3	3	4	4	4	Security of electronic office system	3	3	3	3	36	36	48	48
91	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Transmission errors	3	3	4	4	4	Data and software exchange agreement	3	3	3	3	36	36	48	48
92	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Transmission errors	3	3	4	4	4	Users are given security education and technical training	4	4	4	4	48	48	64	64
93	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Operational support error	2	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance	4	2	3	3	40	30	75	75

									and testing									
94	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Operational support error	2	3	5	5	5	Users are given security education and technical training	4	4	4	4	40	60	100	100
95	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Use of software in unauthorised way	5	2	5	5	4	Users have access only to services that they are authorised to use	2	1	4	4	40	8	80	80
96	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Use of software in unauthorised way	5	2	5	5	4	Job description shall define security roles and responsibilities	2	1	1	1	40	8	20	20
97	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Use of software in unauthorised way	5	2	5	5	4	Event logging	3	3	3	3	60	24	60	60
98	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Illegal use of software	5	2	5	5	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	4	4	4	4	80	32	80	80
99	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Illegal use of software	5	2	5	5	4	Use of system utilities	3	3	3	3	60	24	60	60
100	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Illegal use of software	5	2	5	5	4	Job description shall define security roles and responsibilities	2	1	1	1	40	8	20	20
101	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Accidental deletion of data	2	2	2	2	4	Users are given security education and technical training	4	2	3	3	32	16	24	24
102	to provide technical and motivational support encouraging the use of e-	explore and use technology and tools for education on the internet	Accidental destruction of software programs	2	2	2	2	3	Users are given security education and technical training	4	4	4	4	24	24	24	24

	learning to students and colleagues																	
103	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are givensecurity education and technical training	1	1	1	1	3	3	3	3
104	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Leaving weaknesses (vulnerabilities) in software	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5
105	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Carelessness	5	5	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	75	75	75
106	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Carelessness	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
107	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Carelessness	5	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	50	100	100
108	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Insufficient authentications, weak password recovery validation	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
109	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
110	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
111	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Information disclosure	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100

Risk Analysis - Lecturer Malaysia

No	Stakeholder Function	Task	Threats	Likelihood value based on culture view topology				Impact value	Controls	Effectiveness value based on culture view topology				RPN			
				FTL	HIE	IND	EGA			FTL	HIE	IND	EGA	FTL	HIE	IND	EGA
1	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Data entry error	5	4	4	4	4	Users are given security education and technical training	5	5	5	5	100	80	80	80
2	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Installation and maintenance errors	1	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	1	4	4	4	4
3	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Installation and maintenance errors	1	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	1	4	4	4	4
4	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Error of authorisation or in the instructions	1	5	3	3	5	Information access restriction	2	2	2	2	10	50	30	30
5	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Error of authorisation or in the instructions	1	5	3	3	5	Users have access only to the services that they are authorised to use	2	2	2	2	10	50	30	30
6	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Transmission errors	5	4	5	5	4	Security of electronic office system	3	3	3	3	60	48	60	60
7	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Transmission errors	5	4	5	5	4	Data and software exchange agreement	3	3	3	3	60	48	60	60
8	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Transmission errors	5	4	5	5	4	Users are given security education and technical training	4	4	4	4	80	64	80	80
9	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Operational support error	3	2	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	4	4	4	4	60	40	100	100
10	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them	Operational support error	3	2	5	5	5	Users are given security education and technical training	4	4	4	4	60	40	100	100

		on the LMS															
11	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Use of software in unauthorised way	5	1	5	5	4	Users have access only to services that they are authorised to use	3	2	4	4	60	8	80	80
12	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Use of software in unauthorised way	5	1	5	5	4	Job description shall define security roles and responsibilities	4	4	4	4	80	16	80	80
13	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Use of software in unauthorised way	5	1	5	5	4	Event logging	3	3	3	3	60	12	60	60
14	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Illegal use of software	1	1	5	5	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	3	3	3	12	12	60	60
15	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Illegal use of software	1	1	5	5	4	Use of system utilities	2	2	2	2	8	8	40	40
16	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Illegal use of software	1	1	5	5	4	Job description shall define security roles and responsibilities	3	3	3	3	12	12	60	60
17	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Accidental deletion of data	5	5	5	5	4	Users are given security education and technical training	4	4	4	4	80	80	80	80
18	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Accidental destruction of software programs	2	4	4	4	3	Users are given security education and technical training	4	4	4	4	24	48	48	48
19	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are given security education and technical training	1	1	1	1	3	3	3	3
20	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Leaving weaknesses (vulnerabilities) in software	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5
21	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them	Carelessness	5	4	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	60	75	75

		on the LMS																
22	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Carelessness	5	4	5	5	5	Users are given security education and technical training	4	4	4	4	100	80	100	100
23	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Carelessness	5	4	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	40	100	100
24	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Insufficient authentications, weak password recovery validation	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
25	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
26	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
27	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Information disclosure	5	4	5	5	5	Users are given security education and technical training	4	4	4	4	100	80	100	100
28	to provide effectively design courses incorporating e-learning for student	prepare the teaching and learning materials and then upload them on the LMS	Information disclosure	5	4	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	2	3	3	100	40	75	75
29	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Data entry error	2	4	5	5	4	Users are given security education and technical training	4	4	4	4	32	64	80	80
30	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Installation and maintenance errors	1	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	1	4	4	4	4
31	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Installation and maintenance errors	1	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development,	1	1	1	1	4	4	4	4

									maintenance and testing									
32	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Error of authorisation or in the instructions	2	5	3	5	5	Information access restriction	2	4	4	4	20	100	60	100
33	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Error of authorisation or in the instructions	2	5	3	5	5	Users have access only to the services that they are authorised to use	2	4	3	3	20	100	45	75
34	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Transmission errors	5	4	5	5	4	Security of electronic office system	3	3	3	3	60	48	60	60
35	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Transmission errors	5	4	5	5	4	Data and software exchange agreement	3	3	3	3	60	48	60	60
36	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Transmission errors	5	4	5	5	4	Users are given security education and technical training	4	4	4	4	80	64	80	80
37	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Operational support error	5	2	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	4	2	3	3	100	20	75	75
38	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Operational support error	5	2	5	5	5	Users are given security education and technical training	4	4	4	4	100	40	100	100
39	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Use of software in unauthorised way	3	1	5	5	4	Users have access only to services that they are authorised to use	2	1	1	1	24	4	20	20
40	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Use of software in unauthorised way	3	1	5	5	4	Job description shall define security roles and responsibilities	4	3	3	3	48	12	60	60
41	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Use of software in unauthorised way	3	1	5	5	4	Event logging	3	3	3	3	36	12	60	60
42	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Illegal use of software	2	1	5	5	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	4	3	4	4	32	12	80	80
43	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Illegal use of software	2	1	5	5	4	Use of system utilities	3	3	3	3	24	12	60	60
44	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Illegal use of software	2	1	5	5	4	Job description shall define security roles and responsibilities	4	3	3	3	32	12	60	60

45	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Accidental deletion of data	5	5	5	5	4	Users are given security education and technical training	4	4	4	4	80	80	80	80
46	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Accidental destruction of software programs	2	2	5	5	3	Users are given security education and technical training	4	4	4	4	24	24	60	60
47	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are given security education and technical training	1	1	1	1	3	3	3	3
48	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Leaving weaknesses (vulnerabilities) in software	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5
49	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Carelessness	5	5	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	75	75	75
50	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Carelessness	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
51	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Carelessness	5	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	50	100	100
52	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Insufficient authentications, weak password recovery validation	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
53	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
54	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
55	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Information disclosure	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
56	to provide effectively design courses incorporating e-learning for student	monitor and respond to students usage and discussion	Information disclosure	5	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of	4	2	3	3	100	50	75	75

									password)								
57	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Data entry error	3	2	4	4	4	Users are given security education and technical training	4	4	4	4	48	32	64	64
58	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Installation and maintenance errors	1	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	1	4	4	4	4
59	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Installation and maintenance errors	1	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	1	4	4	4	4
60	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Error of authorisation or in the instructions	2	5	3	5	5	Information access restriction	2	4	4	4	20	100	60	100
61	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Error of authorisation or in the instructions	2	5	3	5	5	Users have access only to the services that they are authorised to use	2	4	3	3	20	100	45	75
62	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Transmission errors	2	3	4	5	4	Security of electronic office system	3	3	3	3	24	36	48	60
63	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Transmission errors	2	3	4	5	4	Data and software exchange agreement	3	3	3	3	24	36	48	60
64	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Transmission errors	2	3	4	5	4	Users are given security education and technical training	4	4	4	4	32	48	64	80
65	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Operational support error	4	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	3	1	1	1	60	15	25	25
66	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Operational support error	4	3	5	5	5	Users are given security education and technical training	4	4	4	4	80	60	100	100

67	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Use of software in unauthorised way	5	1	5	5	4	Users have access only to services that they are authorised to use	2	1	5	5	40	4	100	100
68	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Use of software in unauthorised way	5	1	5	5	4	Job description shall define security roles and responsibilities	4	2	3	3	80	8	60	60
69	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Use of software in unauthorised way	5	1	5	5	4	Event logging	3	3	3	3	60	12	60	60
70	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Illegal use of software	3	1	5	5	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	5	4	5	5	60	16	100	100
71	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Illegal use of software	3	1	5	5	4	Use of system utilities	3	3	3	3	36	12	60	60
72	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Illegal use of software	3	1	5	5	4	Job description shall define security roles and responsibilities	4	2	3	3	48	8	60	60
73	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Accidental deletion of data	2	2	3	3	4	Users are given security education and technical training	4	4	4	4	32	32	48	48
74	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Accidental destruction of software programs	2	2	3	3	3	Users are given security education and technical training	4	4	4	4	24	24	36	36
75	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are given security education and technical training	1	1	1	1	3	3	3	3
76	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Leaving weaknesses (vulnerabilities) in software	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5
77	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Carelessness	5	5	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	75	75	75

78	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Carelessness	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
79	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Carelessness	5	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	50	100	100
80	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Insufficient authentications, weak password recovery validation	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
81	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
82	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
83	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Information disclosure	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
84	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	share experiences and encourage use among lectures	Information disclosure	5	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	2	3	3	100	50	75	75
85	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Data entry error	2	2	2	2	4	Users are given security education and technical training	4	4	4	4	32	32	32	32
86	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Installation and maintenance errors	4	2	5	5	4	Strict control are exercised over the implementation of software on operational systems	2	2	2	2	32	16	40	40
87	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Installation and maintenance errors	4	2	5	5	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	4	2	3	3	64	16	60	60

88	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Error of authorisation or in the instructions	3	3	5	5	5	Information access restriction	2	4	4	4	30	60	100	100
89	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Error of authorisation or in the instructions	3	3	5	5	5	Users have access only to the services that they are authorised to use	2	4	3	3	30	60	75	75
90	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Transmission errors	3	3	5	5	4	Security of electronic office system	3	3	3	3	36	36	60	60
91	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Transmission errors	3	3	5	5	4	Data and software exchange agreement	3	3	3	3	36	36	60	60
92	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Transmission errors	3	3	5	5	4	Users are given security education and technical training	4	4	4	4	48	48	80	80
93	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Operational support error	2	3	5	5	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	4	2	3	3	40	30	75	75
94	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Operational support error	2	3	5	5	5	Users are given security education and technical training	4	4	4	4	40	60	100	100
95	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Use of software in unauthorised way	5	1	5	5	4	Users have access only to services that they are authorised to use	2	1	4	4	40	4	80	80
96	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Use of software in unauthorised way	5	1	5	5	4	Job description shall define security roles and responsibilities	2	1	1	1	40	4	20	20
97	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Use of software in unauthorised way	5	1	5	5	4	Event logging	3	3	3	3	60	12	60	60
98	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Illegal use of software	5	1	5	5	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	4	4	4	4	80	16	80	80

99	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Illegal use of software	5	1	5	5	4	Use of system utilities	3	3	3	3	60	12	60	60
100	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Illegal use of software	5	1	5	5	4	Job description shall define security roles and responsibilities	4	3	3	3	80	12	60	60
101	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Accidental deletion of data	2	2	2	2	4	Users are given security education and technical training	4	2	4	4	32	16	32	32
102	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Accidental destruction of software programs	2	2	2	2	3	Users are given security education and technical training	4	4	4	4	24	24	24	24
103	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Accidental destruction of configurations or hardware.	1	1	1	1	3	Users are given security education and technical training	1	1	1	1	3	3	3	3
104	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Leaving weaknesses (vulnerabilities) in software	1	1	1	1	5	Users are given security education and technical training	1	1	1	1	5	5	5	5
105	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Carelessness	5	5	5	5	5	A range of security controls are established to protect data in computer networks	3	3	3	3	75	75	75	75
106	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Carelessness	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
107	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Carelessness	5	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	3	2	4	4	75	50	100	100
108	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Insufficient authentications, weak password recovery validation	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5
109	to provide technical and motivational support encouraging the use of e-learning to students	explore and use technology and tools for education on the	Insufficient Authorisation, Insufficient Session	1	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	1	5	5	5	5

	and colleagues	internet	Expiration															
110	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	1	5	5	5	5
111	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Information disclosure	5	5	5	5	5	Users are given security education and technical training	4	4	4	4	100	100	100	100
112	to provide technical and motivational support encouraging the use of e-learning to students and colleagues	explore and use technology and tools for education on the internet	Information disclosure	5	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	2	3	3	100	50	75	75

Risk Analysis - Student

No.	Stakeholder Function	Task/ behaviour	Threats	Likelihood value based on culture view topology			Impact value	Controls	Effectiveness value based on culture view topology			RPN		
				FTL	IND	EGA			FTL	IND	EGA	FTL	IND	EGA
1	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Data entry error	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
2	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Installation and maintenance errors	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	4	4	4
3	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Installation and maintenance errors	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	4	4	4
4	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Error of authorisation or in the instructions	1	1	1	5	Information access restriction	1	1	1	5	5	5
5	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Error of authorisation or in the instructions	1	1	1	5	Users have access only to the services that they are authorised to use	1	1	1	5	5	5
6	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	4	3	3	4	Security of electronic office system	1	1	1	16	12	12
7	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	4	3	3	4	Data and software exchange agreement	4	4	4	64	48	48
8	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	4	3	3	4	Users are given security education and technical training	4	3	3	64	36	36
9	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Operational support error	1	1	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	5	5	5
10	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Operational support error	1	1	1	5	Users are given security education and technical training	4	3	3	20	15	15

11	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Use of software in unauthorised way	4	3	3	4	Users have access only to services that they are authorised to use	1	1	1	16	12	12
12	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Use of software in unauthorised way	4	3	3	4	Job description shall define security roles and responsibilities	4	3	3	64	36	36
13	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Use of software in unauthorised way	4	3	3	4	Event logging	4	3	3	64	36	36
14	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Illegal use of software	2	2	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	2	2	24	16	16
15	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Illegal use of software	2	2	2	4	Use of system utilities	1	1	1	8	8	8
16	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Illegal use of software	2	2	2	4	Job description shall define security roles and responsibilities	4	3	3	32	24	24
17	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Accidental deletion of data	3	3	3	4	Users are given security education and technical training	4	3	3	48	36	36
18	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Accidental destruction of software programs	5	5	5	3	Users are given security education and technical training	4	3	3	60	45	45
19	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Accidental destruction of configurations or hardware.	1	1	1	3	Users are given security education and technical training	1	1	1	3	3	3
20	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Leaving weaknesses (vulnerabilities) in software	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
21	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	2	2	50	50	50

22	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Carelessness	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
23	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	2	2	50	50	50
24	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Insufficient authentications, weak password recovery validation	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
25	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
26	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	5	5	5
27	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Information disclosure	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
28	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	3	3	100	75	75
29	To participate in learning process	Communicate online with lecturers and peers students	Data entry error	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
30	To participate in learning process	Communicate online with lecturers and peers students	Installation and maintenance errors	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	4	4	4
31	To participate in learning process	Communicate online with lecturers and peers students	Installation and maintenance errors	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	4	4	4
32	To participate in learning process	Communicate online with lecturers and peers students	Error of authorisation or in the instructions	1	1	1	5	Information access restriction	1	1	1	5	5	5
33	To participate in learning process	Communicate online with lecturers and peers students	Error of authorisation or in the instructions	1	1	1	5	Users have access only to the services that they are authorised to use	1	1	1	5	5	5
34	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	5	5	5	4	Security of electronic office system	1	1	1	20	20	20
35	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	5	5	5	4	Data and software exchange agreement	4	3	3	80	60	60

36	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	5	5	5	4	Users are given security education and technical training	4	3	3	80	60	60
37	To participate in learning process	Communicate online with lecturers and peers students	Operational support error	1	1	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	5	5	5
38	To participate in learning process	Communicate online with lecturers and peers students	Operational support error	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
39	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	4	3	3	4	Users have access only to services that they are authorised to use	1	1	1	16	12	12
40	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	4	3	3	4	Job description shall define security roles and responsibilities	4	3	3	64	36	36
41	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	4	3	3	4	Event logging	4	3	3	64	36	36
42	To participate in learning process	Communicate online with lecturers and peers students	Illegal use of software	5	5	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	2	2	2	40	40	32
43	To participate in learning process	Communicate online with lecturers and peers students	Illegal use of software	5	5	4	4	Use of system utilities	1	1	1	20	20	16
44	To participate in learning process	Communicate online with lecturers and peers students	Illegal use of software	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
45	To participate in learning process	Communicate online with lecturers and peers students	Accidental deletion of data	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
46	To participate in learning process	Communicate online with lecturers and peers students	Accidental destruction of software programs	3	3	3	3	Users are given security education and technical training	4	3	3	36	27	27
47	To participate in learning process	Communicate online with lecturers and peers students	Accidental destruction of configurations or hardware.	1	1	1	3	Users are given security education and technical training	1	1	1	3	3	3
48	To participate in learning process	Communicate online with lecturers and peers students	Leaving weaknesses (vulnerabilities) in software	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
49	To participate in learning process	Communicate online with lecturers and peers students	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	2	2	50	50	50
50	To participate in learning process	Communicate online with lecturers and peers students	Carelessness	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
51	To participate in learning process	Communicate online with lecturers and peers students	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	2	2	50	50	50
52	To participate in learning process	Communicate online with lecturers and peers students	Insufficient authentications, weak password recovery validation	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5

53	To participate in learning process	Communicate online with lecturers and peers students	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
54	To participate in learning process	Communicate online with lecturers and peers students	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	5	5	5
55	To participate in learning process	Communicate online with lecturers and peers students	Information disclosure	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
56	To participate in learning process	Communicate online with lecturers and peers students	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	3	3	100	75	75
57	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Data entry error	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
58	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Installation and maintenance errors	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	4	4	4
59	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Installation and maintenance errors	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	4	4	4
60	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Error of authorisation or in the instructions	1	1	1	5	Information access restriction	1	1	1	5	5	5
61	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Error of authorisation or in the instructions	1	1	1	5	Users have access only to the services that they are authorised to use	1	1	1	5	5	5
62	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Transmission errors	4	4	3	4	Security of electronic office system	1	1	1	16	16	12
63	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Transmission errors	4	4	3	4	Data and software exchange agreement	4	3	3	64	48	36
64	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Transmission errors	4	4	3	4	Users are given security education and technical training	4	3	3	64	48	36
65	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Operational support error	1	1	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	5	5	5
66	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Operational support error	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5

67	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Users have access only to services that they are authorised to use	1	1	1	20	20	16
68	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
69	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Event logging	4	3	3	80	60	48
70	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Illegal use of software	5	5	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	2	2	60	40	32
71	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Illegal use of software	5	5	4	4	Use of system utilities	1	1	1	20	20	16
72	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Illegal use of software	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
73	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Accidental deletion of data	3	3	3	4	Users are given security education and technical training	4	3	3	48	36	36
74	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Accidental destruction of software programs	5	5	4	3	Users are given security education and technical training	4	3	3	60	45	36
75	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Accidental destruction of configurations or hardware.	1	1	1	3	Users are given security education and technical training	1	1	1	3	3	3
76	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Leaving weaknesses (vulnerabilities) in software	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
77	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	2	2	50	50	50
78	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Carelessness	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
79	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	2	2	50	50	50
80	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Insufficient authentications, weak password recovery validation	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5

81	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
82	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	5	5	5
83	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Information disclosure	5	5	5	5	Users are given security education and technical training	4	4	3	100	100	75
84	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	4	3	100	100	75

Risk Analysis - Student Malaysia

No.	Stakeholder Function	Task/ behaviour	Threats	Likelihood value based on culture view topology			Impact value	Controls	Effectiveness value based on culture view topology			RPN		
				FTL	IND	EGA			FTL	IND	EGA	FTL	IND	EGA
1	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Data entry error	3	3	3	4	Users are given security education and technical training	4	3	3	48	36	36
2	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Installation and maintenance errors	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	4	4	4
3	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Installation and maintenance errors	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	4	4	4
4	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Error of authorisation or in the instructions	1	1	1	5	Information access restriction	1	1	1	5	5	5
5	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Error of authorisation or in the instructions	1	1	1	5	Users have access only to the services that they are authorised to use	1	1	1	5	5	5
6	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	5	4	4	4	Security of electronic office system	1	1	1	20	16	16
7	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	5	4	4	4	Data and software exchange agreement	4	4	4	80	64	64
8	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Transmission errors	5	4	4	4	Users are given security education and technical training	4	3	3	80	48	48
9	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Operational support error	1	1	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	5	5	5
10	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Operational support error	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
11	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Use of software in unauthorised way	4	3	3	4	Users have access only to services that they are authorised to use	1	1	1	16	12	12
12	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Use of software in unauthorised way	4	3	3	4	Job description shall define security roles and responsibilities	4	3	3	64	36	36
13	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session,	Use of software in unauthorised way	4	3	3	4	Event logging	4	3	3	64	36	36

		personal portfolio, file storage)													
14	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Illegal use of software	2	2	2	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	3	2	2	24	16	16
15	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Illegal use of software	2	2	2	4	Use of system utilities	1	1	1	8	8	8
16	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Illegal use of software	2	2	2	4	Job description shall define security roles and responsibilities	4	3	3	32	24	24
17	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Accidental deletion of data	3	3	3	4	Users are given security education and technical training	4	3	3	48	36	36
18	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Accidental destruction of software programs	5	5	5	3	Users are given security education and technical training	4	3	3	60	45	45
19	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Accidental destruction of configurations or hardware.	1	1	1	3	Users are given security education and technical training	1	1	1	3	3	3
20	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Leaving weaknesses (vulnerabilities) in software	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
21	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	2	2	50	50	50
22	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Carelessness	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
23	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	2	2	50	50	50
24	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Insufficient authentications, weak password recovery validation	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
25	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5

26	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	5	5	5
27	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Information disclosure	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
28	To participate in learning process	view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	3	3	100	75	75
29	To participate in learning process	Communicate online with lecturers and peers students	Data entry error	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
30	To participate in learning process	Communicate online with lecturers and peers students	Installation and maintenance errors	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	4	4	4
31	To participate in learning process	Communicate online with lecturers and peers students	Installation and maintenance errors	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	4	4	4
32	To participate in learning process	Communicate online with lecturers and peers students	Error of authorisation or in the instructions	1	1	1	5	Information access restriction	1	1	1	5	5	5
33	To participate in learning process	Communicate online with lecturers and peers students	Error of authorisation or in the instructions	1	1	1	5	Users have access only to the services that they are authorised to use	1	1	1	5	5	5
34	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	5	5	5	4	Security of electronic office system	1	1	1	20	20	20
35	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	5	5	5	4	Data and software exchange agreement	4	3	3	80	60	60
36	To participate in learning process	Communicate online with lecturers and peers students	Transmission errors	5	5	5	4	Users are given security education and technical training	4	3	3	80	60	60
37	To participate in learning process	Communicate online with lecturers and peers students	Operational support error	1	1	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	5	5	5
38	To participate in learning process	Communicate online with lecturers and peers students	Operational support error	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
39	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	5	5	4	4	Users have access only to services that they are authorised to use	1	1	1	20	20	16
40	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
41	To participate in learning process	Communicate online with lecturers and peers students	Use of software in unauthorised way	5	5	4	4	Event logging	4	3	3	80	60	48

42	To participate in learning process	Communicate online with lecturers and peers students	Illegal use of software	5	5	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	2	2	2	40	40	32
43	To participate in learning process	Communicate online with lecturers and peers students	Illegal use of software	5	5	4	4	Use of system utilities	1	1	1	20	20	16
44	To participate in learning process	Communicate online with lecturers and peers students	Illegal use of software	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
45	To participate in learning process	Communicate online with lecturers and peers students	Accidental deletion of data	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
46	To participate in learning process	Communicate online with lecturers and peers students	Accidental destruction of software programs	3	3	3	3	Users are given security education and technical training	4	3	3	36	27	27
47	To participate in learning process	Communicate online with lecturers and peers students	Accidental destruction of configurations or hardware.	1	1	1	3	Users are given security education and technical training	1	1	1	3	3	3
48	To participate in learning process	Communicate online with lecturers and peers students	Leaving weaknesses (vulnerabilities) in software	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
49	To participate in learning process	Communicate online with lecturers and peers students	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	2	2	50	50	50
50	To participate in learning process	Communicate online with lecturers and peers students	Carelessness	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
51	To participate in learning process	Communicate online with lecturers and peers students	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	2	2	50	50	50
52	To participate in learning process	Communicate online with lecturers and peers students	Insufficient authentications, weak password recovery validation	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
53	To participate in learning process	Communicate online with lecturers and peers students	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
54	To participate in learning process	Communicate online with lecturers and peers students	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	5	5	5
55	To participate in learning process	Communicate online with lecturers and peers students	Information disclosure	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
56	To participate in learning process	Communicate online with lecturers and peers students	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	3	3	100	75	75

57	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Data entry error	2	2	2	4	Users are given security education and technical training	4	3	3	32	24	24
58	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Installation and maintenance errors	1	1	1	4	Strict control are exercised over the implementation of software on operational systems	1	1	1	4	4	4
59	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Installation and maintenance errors	1	1	1	4	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	4	4	4
60	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Error of authorisation or in the instructions	1	1	1	5	Information access restriction	1	1	1	5	5	5
61	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Error of authorisation or in the instructions	1	1	1	5	Users have access only to the services that they are authorised to use	1	1	1	5	5	5
62	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Transmission errors	4	4	3	4	Security of electronic office system	1	1	1	16	16	12
63	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Transmission errors	4	4	3	4	Data and software exchange agreement	4	3	3	64	48	36
64	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Transmission errors	4	4	3	4	Users are given security education and technical training	4	3	3	64	48	36
65	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Operational support error	1	1	1	5	Documented procedures are provided for the operation of all computer systems and for systems development, maintenance and testing	1	1	1	5	5	5
66	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Operational support error	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
67	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Users have access only to services that they are authorised to use	4	3	3	80	60	48
68	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
69	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Use of software in unauthorised way	5	5	4	4	Event logging	3	2	2	60	40	32
70	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Illegal use of software	5	5	4	4	Measures are taken to comply with contractual restrictions on the use of copyright materials	1	1	1	20	20	16

71	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Illegal use of software	5	5	4	4	Use of system utilities	4	3	3	80	60	48
72	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Illegal use of software	5	5	4	4	Job description shall define security roles and responsibilities	4	3	3	80	60	48
73	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Accidental deletion of data	3	3	3	4	Users are given security education and technical training	4	3	3	48	36	36
74	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Accidental destruction of software programs	5	5	4	3	Users are given security education and technical training	4	3	3	60	45	36
75	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Accidental destruction of configurations or hardware.	1	1	1	3	Users are given security education and technical training	1	1	1	3	3	3
76	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Leaving weaknesses (vulnerabilities) in software	1	1	1	5	Users are given security education and technical training	1	1	1	5	5	5
77	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Carelessness	5	5	5	5	A range of security controls are established to protect data in computer networks	2	2	2	50	50	50
78	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Carelessness	5	5	5	5	Users are given security education and technical training	4	3	3	100	75	75
79	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Carelessness	5	5	5	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	2	2	2	50	50	50
80	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Insufficient authentications, weak password recovery validation	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
81	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	A range of security controls are established to protect data in computer networks	1	1	1	5	5	5
82	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Insufficient Authorisation, Insufficient Session Expiration	1	1	1	5	Inactive terminals in high risk location or serving high risk systems are set to time out, to minimise the risk of access by unauthorised person	1	1	1	5	5	5
83	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Information disclosure	5	5	5	5	Users are given security education and technical training	4	4	3	100	100	75
84	To participate in learning process	Eager to explore the Internet, and use the application and software downloaded from the Internet	Information disclosure	5	5	5	5	Users are required to follow good security practices (i.e in the selection and use of password)	4	4	3	100	100	75

Top Management

Functions: Develop a strategic plan for e-learning implementation.

Task: Enhance the e-learning infrastructures and facilities.

No.	Threats	Hierarchism
1	Carelessness	75

Task: Collaboration with other parties.

No.	Threats	Hierarchism
1	Accidental deletion of data	60
2	Carelessness	75
3	Information disclosure	75

Functions: Manage the business.
Task: Use business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.

No.	Threats	Hierarchism
1	Data entry error	60
2	Accidental deletion of data	60
3	Carelessness	75
4	Information disclosure	75

Summary

List of threats contribute by top management- hierarchism group (listed according to rank)

No.	Threats
1	Carelessness
2	Information disclosure
3	Data entry error
4	Accidental deletion of data

Top Management Malaysia

Functions: Develop a strategic plan for e-learning implementation

Task: Enhance the e-learning infrastructures and facilities

No.	Threats	Hierarchism
1	Accidental deletion of data	60
2	Carelessness	75
3	Information disclosure	75

Task: Collaboration with other parties

No.	Threats	Hierarchism
1	Accidental deletion of data	60
2	Carelessness	75
3	Information disclosure	75

Functions: Manage the business

Task: Using business intelligent tools and data mining process to get high level overview to help in strategic planning. Therefore may have access to business tools, data mining interfaces, highly confidential and high impact information.

No.	Threats	Hierarchism
1	Data entry error	60
2	Accidental deletion of data	60
3	Carelessness	75
4	Information disclosure	75

Summary

List of threats contribute by top management- hierarchism group (listed according to rank)

No.	Threats
1	Carelessness
2	Information disclosure
3	Data entry error
4	Accidental deletion of data

Comparison: The top management in Malaysia has no significant different from the general top management in the world. They share the same list of threats.

E-learning Centre
Functions: Championing a strategy to develop a successful e-learning environment

Task: Manage the LMS

No.	Threats	HIE	IND	EGA
1	Data entry error	40	60	60
2	Operational support error	40	75	75
3	Accidental deletion of data	40	60	60
4	Carelessness	50	75	75
5	Information disclosure	50	75	75

Task: Provide training on e-learning applications and tools

No.	Threats	HIE	IND	EGA
1	Error of authorisation or in the instructions	30	45	60
2	Operational support error	40	60	60
3	Accidental deletion of data	32	60	60
4	Leaving weaknesses (vulnerabilities) in software	30	60	60
5	Carelessness	50	75	75
6	Information disclosure	50	75	75

Summary

List of threats contribute by E-learning Centre. Egalitarianism (7) is the most contributors to threats. While following closely is Individualism (6).

No.	Threats	Main contributor
1	Data entry error	IND,EGA
2	Error of authorisation or in the instructions	EGA
3	Operational support error	IND,EGA
4	Accidental deletion of data	IND,EGA
5	Leaving weaknesses (vulnerabilities) in software	IND,EGA
6	Carelessness	IND,EGA
7	Information disclosure	IND,EGA

E-learning Centre Malaysia Critical Threats

Functions: Championing a strategy to develop a successful e-learning environment

Task: Manage the LMS

No.	Threats	HIE	IND	EGA
1	Data entry error	40	60	60
2	Installation and maintenance errors	16	60	60
3	Operational support error	40	75	75
4	Accidental deletion of data	40	60	60
5	Carelessness	50	75	75
6	Insufficient authentications, weak password recovery validation	30	60	45
7	Insufficient Authorisation, Insufficient Session Expiration	45	60	45
8	Information disclosure	50	75	75

Task: Provide training on e-learning applications and tools

No.	Threats	HIE	IND	EGA
1	Error of authorisation or in the instructions	40	60	75
2	Transmission errors	32	48	60
3	Operational support error	50	75	75
4	Accidental deletion of data	40	60	60
5	Leaving weaknesses (vulnerabilities) in software	30	60	60
6	Carelessness	50	75	75
7	Information disclosure	50	75	75

Summary

List of threats contribute by E-learning Centre Malaysia. Individualism (10) is the most contributors to threats. While following closely is Egalitarianism (9)

No.	Threats	Main contributor
1	Data entry error	IND,EGA
2	Installation and maintenance errors	IND,EGA
3	Error of authorisation or in the instructions	IND,EGA
4	Transmission errors	EGA
5	Operational support error	IND,EGA
6	Accidental deletion of data	IND,EGA
7	Leaving weaknesses (vulnerabilities) in software	IND,EGA
8	Insufficient authentications, weak password recovery validation	IND
9	Insufficient Authorisation, Insufficient Session Expiration	IND
10	Carelessness	IND,EGA
11	Information disclosure	IND,EGA

Comparison:

E-learning Malaysia has 4 threats more than E-learning general; namely as Installation and maintenance errors, Transmission errors, Insufficient authentications, weak password recovery validation, and Insufficient Authorisation, Insufficient Session Expiration. The main contributors of threats in Malaysia are individualism, while in general the mains contributors are egalitarianisms.

IT Critical Threats

Functions: Responsible on the technical part in the e-learning environment and system

Task: Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)

No.	Threats	HIE	IND	EGA
1	Operational support error	40	75	75
2	Accidental deletion of data	40	60	60
3	Carelessness	50	75	75
4	Information disclosure	50	75	75

Functions: Responsible on the technical part in the e-learning environment and system
Task: Working with external parties (LMS vendor) and/or develop system in house

No.	Threats	HIE	IND	EGA
1	Operational support error	30	60	60
2	Carelessness	50	75	75
3	Information disclosure	75	75	75

Functions: Create a competent and efficient customer centre support service on e-learning, campus network and telecommunication infrastructure

Task: Support the customers or users on IT services

No.	Threats	HIE	IND	EGA
1	Data entry error	40	60	60
2	Operational support error	30	60	60
3	Accidental deletion of data	40	60	60
4	Leaving weaknesses (vulnerabilities) in software	30	60	60
5	Carelessness	50	75	75
6	Information disclosure	75	75	75

Functions: Provide operational support on the campus network and telecommunication infrastructure

Task: Support the customers or users on network and telecommunication infrastructure

No.	Threats	HIE	IND	EGA
1	Data entry error	40	60	60
2	Operational support error	30	60	60
3	Accidental deletion of data	40	60	60
4	Leaving weaknesses (vulnerabilities) in software	30	60	60
5	Carelessness	50	75	75
6	Information disclosure	50	75	75

Summary

List of threats contribute by IT. Individualism and Egalitarianism are the most contributors to threats.

No.	Threats	Main contributor
1	Data entry error	IND,EGA
2	Operational support error	IND,EGA
3	Accidental deletion of data	IND,EGA
4	Leaving weaknesses (vulnerabilities) in software	IND,EGA
5	Carelessness	IND,EGA
6	Information disclosure	HIE, IND,EGA

IT Malaysia

Functions: Responsible on the technical part in the e-learning environment and system

Task: Managed e-learning infrastructures and supports the LMS, (collaborate with e-learning centre)

No.	Threats	HIE	IND	EGA
1	Data entry error	24	60	60
2	Installation and maintenance errors	12	60	60
3	Operational support error	40	75	75
4	Accidental deletion of data	40	60	60
5	Carelessness	50	75	75
6	Insufficient authentications, weak password recovery validation	30	60	45
7	Insufficient Authorisation, Insufficient Session Expiration	45	60	45
8	Information disclosure	50	75	75

Functions: Responsible on the technical part in the e-learning environment and system

Task: Working with external parties (LMS vendor) and/or develop system in house

No.	Threats	HIE	IND	EGA
1	Operational support error	30	75	75
2	Accidental deletion of data	40	60	60
3	Carelessness	50	75	75
4	Insufficient Authorisation, Insufficient Session Expiration	30	60	45
5	Information disclosure	75	75	75

Functions: Create a competent and efficient customer centre support service on e-learning, campus network and telecommunication infrastructure

Task: Support the customers or users on IT services

No.	Threats	HIE	IND	EGA
1	Operational support error	30	75	75
2	Accidental deletion of data	40	60	60
3	Carelessness	50	75	75
4	Insufficient Authorisation, Insufficient Session Expiration	30	60	45
5	Information disclosure	50	75	75

Functions: Provide operational support on the campus network and telecommunication infrastructure

Task: Support the customers or users on network and telecommunication infrastructure

No.	Threats	HIE	IND	EGA
1	Operational support error	30	75	75
2	Accidental deletion of data	40	60	60
3	Carelessness	50	75	75
4	Insufficient Authorisation, Insufficient Session Expiration	30	60	45
5	Information disclosure	50	75	75

Summary

List of threats contribute by IT. Individualism is the most contributors to threats.

No.	Threats	Main contributor
1	Data entry error	IND,EGA
2	Installation and maintenance errors	IND,EGA
3	Operational support error	IND,EGA
4	Accidental deletion of data	IND,EGA
5	Carelessness	IND,EGA
6	Insufficient authentications, weak password recovery validation	IND
7	Insufficient Authorisation, Insufficient Session Expiration	IND
8	Information disclosure	IND,EGA

Comparison: Malaysia has 2 threats more compare to the general IT : Insufficient authentications, weak password recovery validation, Insufficient Authorisation, Insufficient Session Expiration; which are contributed by the individualism. The others threats and contributor are similar with the general IT except the information disclosure. Beside the individualism and egalitarianism, the information disclosure threat was also contributed by the hierarchism.
This is happening due to the different level of knowledge on information and computer security between the IT in Malaysia.

Lecturer critical threats
Functions: to provide effectively design courses incorporating e-learning for student

Task: prepare the teaching and learning materials and then upload them on the LMS

		RPN			
No.	Threats	FTL	HIE	IND	EGA
1	Data entry error	80	64	64	64
2	Error of authorisation or in the instructions	10	100	40	80
3	Transmission errors	80	64	80	80
4	Operational support error	100	60	100	100
5	Use of software in unauthorised way	60	16	80	80
6	Illegal use of software	60	24	60	60
7	Accidental deletion of data	80	80	80	80
8	Carelessness	100	100	100	100
9	Information disclosure	80	80	80	80

Functions: to provide effectively design courses incorporating e-learning for student

Task: monitor and respond to students' usage and discussion

No.	Threats	FTL	HIE	IND	EGA
1	Data entry error	80	64	64	64
2	Error of authorisation or in the instructions	30	100	40	80
3	Transmission errors	80	64	80	80
4	Operational support error	100	60	100	100
5	Use of software in unauthorised way	60	24	60	60
6	Accidental deletion of data	80	80	80	80
7	Carelessness	100	100	100	100
8	Information disclosure	100	100	100	100

Functions: to provide technical and motivational support encouraging the use of e-learning to students and colleagues

Task: share experiences and encourage use among lectures

No.	Threats	FTL	HIE	IND	EGA
1	Error of authorisation or in the instructions	30	100	40	80
2	Transmission errors	32	48	48	64
3	Operational support error	40	60	100	100
4	Use of software in unauthorised way	80	16	60	60
5	Illegal use of software	80	16	60	60
6	Carelessness	100	100	100	100
7	Information disclosure	100	100	100	100

Functions: to provide technical and motivational support encouraging the use of e-learning to students and colleagues

Task: explore and use technology and tools for education on the internet

No.	Threats	FTL	HIE	IND	EGA
1	Installation and maintenance errors	32	16	60	60
2	Error of authorisation or in the instructions	30	60	100	100
3	Transmission errors	48	48	64	64
4	Operational support error	40	60	100	100
5	Use of software in unauthorised way	60	24	60	60
6	Illegal use of software	80	32	80	80
7	Carelessness	100	100	100	100
8	Information disclosure	100	100	100	100

Summary

Below is list of threats for lecturer. Individualism (10), Egalitarianism (10) are the most contributor to threats. F (9) H (8) I (10) E (10)

No.	Threats	Main contributor
1	Data entry error	FTL, HIE, IND, EGA
2	Error of authorisation or in the instructions	HIE, EGA, IND
3	Transmission errors	FTL, HIE, IND, EGA
4	Operational support error	FTL, HIE, IND, EGA
5	Use of software in unauthorised way	FTL,IND,EGA
6	Illegal use of software	FTL,IND,EGA
7	Accidental deletion of data	FTL, HIE, IND, EGA
8	Carelessness	FTL, HIE, IND, EGA
9	Information disclosure	FTL, HIE, IND, EGA
10	Installation and maintenance errors	FTL, HIE, IND, EGA

Lecturer :Malaysia

Functions: to provide effectively design courses incorporating e-learning for student

Task: prepare the teaching and learning materials and then upload them on the LMS

No.	Threats	FTL	HIE	IND	EGA
1	Data entry error	100	80	80	80
2	Transmission errors	80	64	80	80
3	Operational support error	60	40	100	100
4	Use of software in unauthorised way	80	16	80	80
5	Illegal use of software	12	12	60	60
6	Accidental deletion of data	80	80	80	80
7	Carelessness	100	80	100	100
8	Information disclosure	100	80	100	100

Functions: to provide effectively design courses incorporating e-learning for student

Task: monitor and respond to students' usage and discussion

No.	Threats	FTL	HIE	IND	EGA
1	Data entry error	32	64	80	80
2	Error of authorisation or in the instructions	20	100	60	100
3	Transmission errors	80	64	80	80
4	Operational support error	100	40	100	100
5	Use of software in unauthorised way	48	12	60	60
6	Illegal use of software	32	12	60	60
7	Accidental deletion of data	80	80	80	80
8	Accidental destruction of software programs	24	24	60	60
9	Carelessness	100	100	100	100
10	Information disclosure	100	100	100	100

Functions: to provide technical and motivational support encouraging the use of e-learning to students and colleagues

Task: share experiences and encourage use among lectures

No.	Threats	FTL	HIE	IND	EGA
1	Data entry error	48	32	64	64
2	Error of authorisation or in the instructions	20	100	60	100
3	Transmission errors	32	48	64	80
4	Operational support error	80	60	100	100
5	Use of software in unauthorised way	80	8	60	60
6	Illegal use of software	60	16	100	100
7	Carelessness	100	100	100	100
8	Information disclosure	100	100	100	100

Functions: to provide technical and motivational support encouraging the use of e-learning to students and colleagues

Task: explore and use technology and tools for education on the internet

No.	Threats	FTL	HIE	IND	EGA
1	Installation and maintenance errors	64	16	60	60
2	Error of authorisation or in the instructions	30	60	100	100
3	Transmission errors	48	48	80	80
4	Operational support error	40	60	100	100
5	Use of software in unauthorised way	60	12	60	60
6	Illegal use of software	80	16	80	80
7	Carelessness	100	100	100	100
8	Information disclosure	100	100	100	100

Summary

List of threats for lecturer is listed below. The threats were contributed by Individualism (11), Egalitarianism (11), Fatalism (9), and Hierarchism (7). Individualism (11), Egalitarianism (11) are the most contributor to the threats.

No.	Threats	High contributor
1	Data entry error	F,H,I,E
2	Error of authorisation or in the instructions	H, I, E
3	Transmission errors	F,H,I,E
4	Operational support error	F,H,I,E
5	Use of software in unauthorised way	F,I,E
6	Illegal use of software	F,I,E
7	Accidental deletion of data	F,H,I,E
8	Carelessness	F,H,I,E
9	Information disclosure	F,H,I,E
10	Installation and maintenance errors	F,I,E
11	Accidental destruction of software programs	I,E

Comparison:

There are 11 threats from the group of lecturer in Malaysia which 1 more extra compare to the general group. The threats are Accidental destruction of software programs. For both general and Malaysia context, Individualism and Egalitarianisms are the group of culture view that can contribute the threats the most.

Student

Functions: To participate in learning process

Task: view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)

No.	Threats	FTL	IND	EGA
1	Transmission errors	64	48	48
2	Use of software in unauthorised way	64	36	36
3	Accidental destruction of software programs	60	45	45
4	Carelessness	100	75	75
5	Information disclosure	100	75	75

Functions: to participate in learning process

Task: Communicate online with lecturers and peers students

No.	Threats	FTL	IND	EGA
1	Transmission errors	80	60	60
2	Use of software in unauthorised way	64	36	36
3	Illegal use of software	80	60	48
4	Carelessness	100	75	75
5	Information disclosure	100	75	75

Functions: to participate in learning process

Task: Eager to explore the Internet, and use the application and software downloaded from the Internet

No.	Threats	FTL	IND	EGA
1	Transmission errors	64	48	36
2	Use of software in unauthorised way	80	60	48
3	Illegal use of software	80	60	48
4	Accidental destruction of software programs	60	45	36
5	Carelessness	100	75	75
6	Information disclosure	100	100	75

Summary

List of threats contribute by student. Fatalism (6) is the most contributors to threats. I (5), E(3)

No.	Threats	Main contributor
1	Transmission errors	F,I,E
2	Use of software in unauthorised way	F,I
3	Illegal use of software	F,I
4	Accidental destruction of software programs	F
5	Carelessness	F,I,E
6	Information disclosure	F,I,E

Student Malaysia

Functions: To participate in learning process

Task: view, read and write in the LMS at anywhere and anytime (online session, personal portfolio, file storage)

No.	Threats	FTL	IND	EGA
1	Transmission errors	80	64	64
2	Use of software in unauthorised way	64	36	36
3	Accidental destruction of software programs	60	45	45
4	Carelessness	100	75	75
5	Information disclosure	100	75	75

Functions: to participate in learning process

Task: Communicate online with lecturers and peers students

No.	Threats	FTL	IND	EGA
1	Transmission errors	80	60	60
2	Use of software in unauthorised way	80	60	48
3	Illegal use of software	80	60	48
4	Carelessness	100	75	75
5	Information disclosure	100	75	75

Functions: to participate in learning process

Task: Eager to explore the Internet, and use the application and software downloaded from the Internet

No.	Threats	FTL	IND	EGA
1	Transmission errors	64	48	36
2	Use of software in unauthorised way	80	60	48
3	Illegal use of software	80	60	48
4	Accidental destruction of software programs	60	45	36
5	Carelessness	100	75	75
6	Information disclosure	100	100	75

Summary

List of threats contribute by student. Fatalism is the most contributors to threats.

No.	Threats	contributor
1	Transmission errors	FTL,IND,EGA
2	Use of software in unauthorised way	FTL,IND
3	Illegal use of software	FTL,IND
4	Accidental destruction of software programs	FTL
5	Carelessness	FTL,IND,EGA
6	Information disclosure	FTL,IND,EGA

Comparisons:

Malaysia students are similar to general students. This is may be due to the level of knowledge that they have are usually similar at this level. Either the IT knowledge or the security knowledge.

Appendix K Expert review Questionnaire

Research validation expert questionnaire

Research Synopsis

The motivation to conduct this research has come from awareness that the Internet exposes the e-learning environment to information security threats and vulnerabilities. Information Security Management (ISM) as practised as a top down approach in many organisations tends to detach system user's sense of responsibility in ensuring the security of e-learning. Literature has pointed out that people's behaviour should be addressed to manage information security threats. This research proposes an E-Learning Stakeholders Information Security Vulnerability Model to assist e-learning providers in the public universities in Malaysia. Adopting a socio-technical approach, this model aims to improve the implementation and management of e-learning information security by targeting different stakeholders with controls relevant to their behaviour cultural view.

The research started with a pilot study that highlighted data confidentiality difficulties. Six multi-method research actions were conducted using existing public knowledge from multiple sources to generate the dimensions for the model (Figure 1 in Attachment A).

Instructions to the Expert

This research has developed an E-learning Stakeholders Information Security Vulnerability Model (Figure 1 in Attachment A). This research proposes that cultural view affect threats susceptibility, and e-learning ISM controls can be more effective if made relevant to the cultural view of the stakeholders. The controls focus on the ISM elements: policy, process and procedures and organisational structure and are illustrated in Table 1(Attachment B). The cultural view used is derived from the Cultural Theory that defines the distinctive characteristic and behaviour of Hierarchism, Individualism, Egalitarianism and Fatalism (Attachment C).

This research suggests that the controls which address and consider the culture characteristic and behaviour will lower the criticality of threats. More personalised controls are more likely to be observed by the stakeholder.

The experts are invited to review the illustration of controls designed and to answer the questions.

Questions

1. In addition to using the technological control, would security management be enhanced by addressing the stakeholder's cultural view?
2. Is the proposed model different to typical ISM currently implemented?
3. From your own experience and understanding, can you provide one example that reflects what is proposed in Table 1(Attachment B)?
4. Would the illustrations in Table 1(Attachment B) help in designing better training and education to improve security awareness?
5. Please comment on the proposed model in the wider context of information security management.
6. Is the implementation of the proposed model practical in terms of cost and effort?

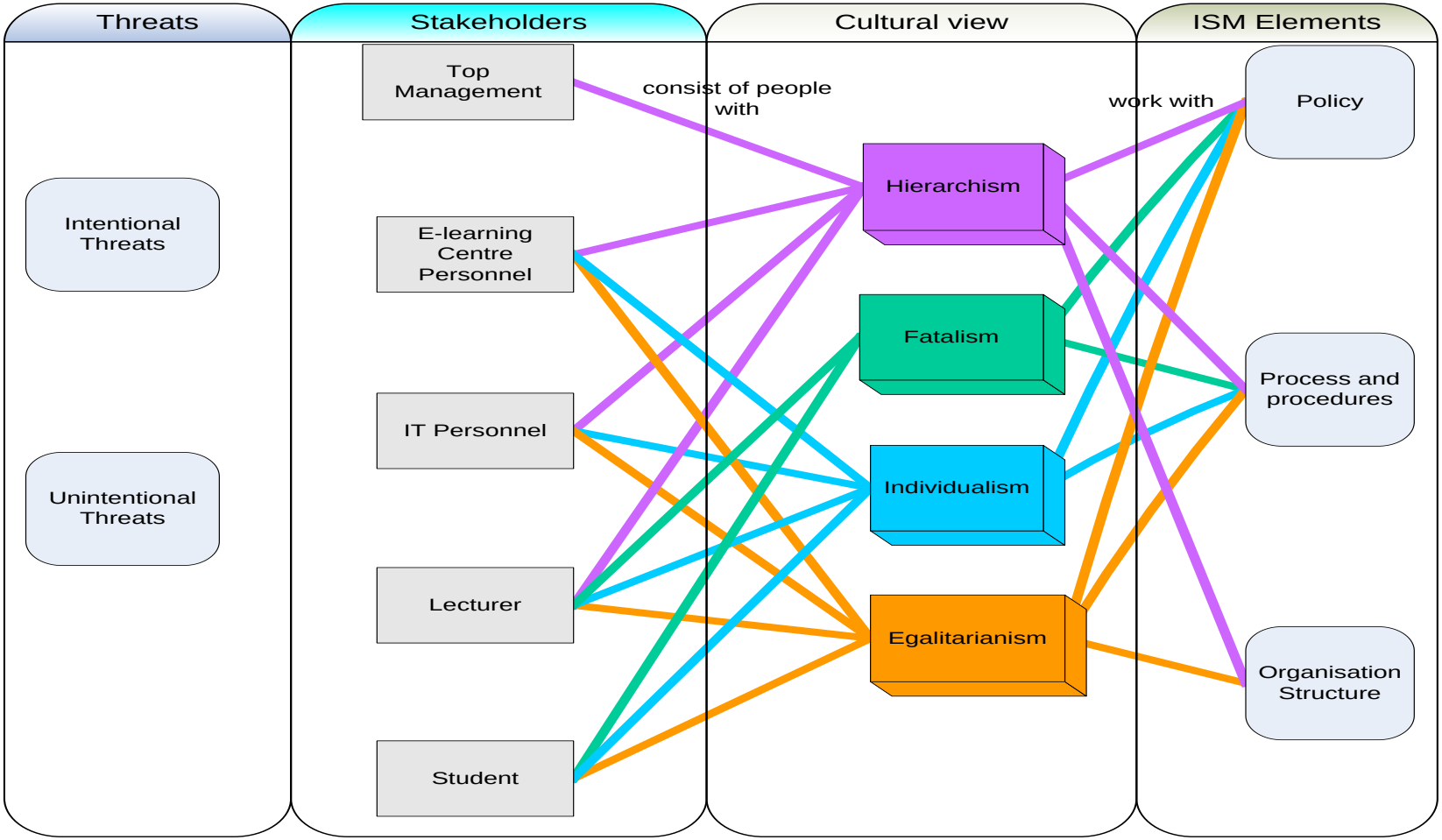


Figure 1- E-Learning Stakeholders Information Security Vulnerability Model

Table 1: Illustration of controls according to cultural view focussing on ISM elements

Cultural view	Hierarchism	Individualism	Egalitarianism	Fatalism
Definitions	Hierarchism represents persons who have always trust and depends on the experts (Marris et al., 1996) and if they are to break rules or act contrarily to a policy, they are expected to do so as a group in an orderly, disciplined and co-ordinated way (Mars, 1996). People with this culture need to be encouraged to be more independent and not solely dependent on experts. They typically act according to the roles, but the given privileges could prove fatal and vulnerable, thus they need to be reminded about this.	Individualists are characterized by a reluctance to accept rules (Mars, 1996), especially if these rules are perceived as obstructing their freedom. Individualists need to be reminded that they are responsible towards other stakeholders.	With intense sense of equality (Tsohou et al 2006), egalitarians have more difficulties in accepting role differentiations (Langford et al., 2000; Marris et al., 1996). However they support decision-making processes that encourage public participation (Marris et al., 1996) Egalitarians are prone to break rules if they feel that these rules generate inequalities or if they are not convinced of their purposes.	Fatalists would rather be unaware of dangers, since they assume that they are unavoidable anyway (Torbjorn, 2004). Fatalists are persons who feel that decisions are beyond their control (Langford et al., 2000). To counteract, they have to feel that they are important and they have the power to influence the course of events in their favour.
Cultural view	**Hierarchism**	**Individualism**	**Egalitarianism**	**Fatalism**
ISM Policy Example on different ways to write the policy on data entry for lecturers.	*'The lecturer shall enter the correct data'.*	*'The lecturer has to ensure data entered is correct due to the massive impact to the student (or other stakeholders').*	*'The lecturer has to ensure data entered are correct in sustaining self-accountability and integrity'.*	*'The lecturer has to be responsible on every data entry'.*
ISM Process and procedures Example of process and procedures in 1) document and record control and 2) conducting training awareness	2) Document and Record Control Messages can be worded to emphasis on aspects that bring out control and power.	2) Document and Record Control Messages can be in language to stress the reliance on others and threats induced by individualistic behaviour.	2) Document and Record Control Messages can be worded to emphasise the importance to keep some information confidential despite the positive teamwork and cooperative value behaviour.	2) Document and Record Control Messages can be in a simple language, not overcomplicated or negative to help them understand as well as enthuse them that they can positively support information security.

	2) Training Messages can be framed to emphasis the impact on the image and reputation of the organisation. Also, the impact that may affect their continuing status must be highlighted. Information given in training should be based on the worst possible outcomes as well as reassured by positive information.	2) Training Messages can be framed to emphasis impact of security incident personally to themselves. This will increase the understanding of the influence in their upcoming decision. Their character on risk taking can be neutralised with information regarding their potential rewards or opportunities associated with their behaviour. It is good to channel the attitude of individualists to the positive such as appoint them to be the security facilitator.	2) Training Messages can be framed that stresses the social costs associated with security breaches since egalitarianists dislike the unnecessary impact implied to them and others.	2) Training Messages can be framed by providing case studies, describing incidents when individuals caused breaches, rather than just providing security rules. Encourage them with positive and easy steps on information security. Less overcomplicated or negative vocabulary used (violation, failure etc.).
Organisational structure	Usually hierarchists have high positions in an organisation, therefore their roles, job scope and the level of security privilege should be made clear. They should be well informed about access privileges, security restrictions in sensitive areas, and how to handle sensitive information.	Not related *	The egalitarians are always prepared to help, therefore they should be reminded about the access privileges, security restrictions in sensitive areas, and how to handle sensitive information.	Not related*

*The fatalist and individualist reflect the low bond of social unit and low participation in group activities (Oltedal et al., 2004), thus organisational structure has less effect on people with these cultural views. They are better addressed with policy, process and procedures. On the other hand hierarchists and egalitarians has high bond of social unit and strong participation with group activities, thus organisational structure has stronger influence on them to take part in information security management.

Overview of Cultural Theory

One known organisation culture theory is the Grid and Group Cultural Theory or simply the Cultural Theory (CT). Cultural Theory was developed over the past thirty years through the work of British anthropologists Mary Douglas and Michael Thompson. This theory addresses the level of an individual in an organisation. It is able to account for changes both within and between dimensions and deals with dynamism. Cultural Theory has been used to study the different views of environmental and technological risks in society.

The Cultural Theory framework has two dimensions, namely the Grid and the Group. The Grid dimension refers to the degree to which a social context is regulated and restrictive in regard to the individual's' behaviour. The Group dimension refers to an individual as a member of bonded social units, how absorbing the group's activities are on the individual (Oltedal et al., 2004). The two dimensions give four different cultural views with distinct ways of life or world views (Mamadouh, 1999). Table 2 list characteristics for each culture view gathered from literature review. A brief explanation on Hierarchism, Fatalism, Individualism and Egalitarianism is as below.

Hierarchism

Hierarchism is a view held by people who are strong in both Grid and Group dimensions, indicating strong control and power. Hierarchists have a disposition to follow the rules and trust experts in general (Marris et al., 1996); and they also are expected to break rules or act contrarily to a policy as a group in an orderly, disciplined and co-ordinated way (Mars, 1996).

Fatalism

Fatalism is a view held by people with a strong Grid and low Group, indicating apathy and isolation. Fatalist would rather be unaware of dangers, since they assume that they are unavoidable anyway (Torbjorn, 2004). They believe that decisions are beyond their control and feel obliged to accept whatever is imposed upon them (Langford et al., 2000). They are not likely to breach security controls for their personal gain, since they believe they have little or no power to influence the course of events in their favour (Tsohou et al 2006). However fatalism views lead to the development of ignorance character, which increases the risks of unintentional threats.

Individualism

Individualism is a view held by people with both low Grid and low Group, indicating independence and self-reliance. Individualists are characterized by a reluctance to accept rules (Mars, 1996), especially if these rules are perceived as obstructing their freedom.

Egalitarianism

Egalitarianism is a view held by people with a low Grid and Strong Group, indicating teamwork and cooperation. With intense sense of equality (Tsohou et al 2006), egalitarians have more difficulties in accepting role differentiations (Langford et al., 2000; Marris et al., 1996). However they support decision-making processes that encourage public participation (Marris et al., 1996).

Table 2 -List of Characteristics for each culture view

Hierarchism view/characters	**Authors**
Status demarcation unquestionable.	(Douglas and Wildavsky, 1983), (Langford et al., 2000), (Thompson et al., 1990)
Trust rules and regulation and the experts.	(Lima and Castro, 2005)
Realise and act according to the roles.	(Altman and Baruch, 1998)
Act as a group in an orderly, disciplined and co-ordinated way, with respect for their own rules, limits and precedents even when cheating or making mistakes.	(Mars, 1996)
Low adaptability to change. Dependence on routine ways of work.	(Mars, 1996)
Trust the experts.	(Lima and Castro, 2005), (Oltedal et al., 2004)
Fear of disruption to the social order. Emphasise on the establishing and preserving the nature and social order.	(Langford et al., 2000), (Marris et al., 1996), (Oltedal et al., 2004)
Individualism view/characters	**Authors**
Bound neither by group integration nor by prescribed roles, and assert that all boundaries are subject to negotiation.	(Karyda et al., 2005),(Langford et al., 2000)
Barely feel responsible towards other members of society.	(Langford et al., 2000)
Believe that each person responsible for oneself.	(Altman and Baruch, 1998)
Concerned for the maintenance of freedom to continue life and business as usual.	(Lima and Castro, 2005)
Afraid of things that might obstruct their individual freedom.	(Oltedal et al., 2004)
Reluctant to accept rules or to follow defined instructions or procedures.	(Mars, 1996)
Mostly built short-term relationships with their superiors.	(Mars, 1996)
Associated with corner cutting, rule breaking and cheating.	(Tsohou et al., 2006)
High propensity for risk taking.	(Mars, 1996)
Prefer methods that are based on economic factors, and in particular cost-benefit analysis.	(Langford et al., 2000), (Marris et al., 1996)
Egalitarianism view/characters	**Authors**
High degree of the group dimension and not prescribed by role differentiation.	(Tsohou et al., 2006)

Negotiation in relationship and nobody is granted authority by virtue of his or her position.	(Marris et al., 1996),(Langford et al., 2000)
Believe that leadership must be charismatic.	(Altman and Baruch, 1998)
Intense sense of equality.	(Tsohou et al., 2006)
Sceptical to expert knowledge, suspect the expert and strong institution misuse the power/authority.	((Oltedal et al., 2004)
Dislike others deciding for their life and actions, and prefer to have information provided to them, based upon which they can make their own personal choices.	(Finucane and Holup, 2005)
Support decision-making processes that encourage public participation.	(Marris et al., 1996)
Difficulty in accepting role differentiations.	(Langford et al., 2000) (Marris et al., 1996)
Prone to break rules if they feel that these rules generate inequalities or if they are not convinced of their purpose.	(Tsohou et al., 2006)
Fatalism view/characters	**Authors**
Believe their autonomy is restricted by social distinctions, however they feel excluded from membership in the institutions responsible for setting the rules. Tend to see themselves as “outsiders”.	(Douglas and Wildavsky, 1983), (Langford et al., 2000), (Thompson et al., 1990)
Believe that there is minimal in individual autonomy and little room for personal negotiations.	(Altman and Baruch, 1998)
Believe that social classification should be based on ancestry.	(Altman and Baruch, 1998)
Take small part in social.	(Tsohou et al., 2006)
Would rather be unaware of dangers, since they assume that they are unavoidable anyway.	(Oltedal et al., 2004)
Prefer occupying posts with routine tasks.	(Mars, 1996)
Feel that decisions are beyond their control and feel obliged to accept whatever is imposed upon them.	(Langford et al., 2000)
Tends to fatalism therefore are not expected to breach security controls for their personal gain, since they believe they have little or no power to influence the course of events in their favour.	(Tsohou et al., 2006)