CRANFIELD UNIVERSITY

Sundar Sherchan

A study of the cyber security awareness and use of protective cyber security practices in defence settings

Cranfield School of Defence and Security
Information Capability Management

MSc
Academic Years: 2017-2018

Supervisor: Victoria Smy
July 2018

CRANFIELD UNIVERSITY

Cranfield Defence and Security School
Information Capability Management

MSc

Academic Year 2017- 2018

Sundar Sherchan

A study of the cyber security awareness and use of protective cyber security practices in defence settings

Supervisor: Victoria Smy

July 2018

ABSTRACT

The UK Strategic Defence and Security Review (2015), places ‘cyber’ in the highest category tier-one risk. The threats from cyberspace is ever increasing as UK Armed Forces is becoming increasingly dependent on its’ information systems and networks for daily business processes. Hardware and software technological defences are effective tools to protect our systems and networks, nonetheless these defences are useless if humans operators allows attackers to maliciously exploit our systems through use of social engineering techniques. There is currently no measurement framework in the R SIGNALS or the Army to assess basic cyber awareness and behaviour of soldiers and officers and benchmarking user cyber awareness maturity state.

In this study, the author creates an innovative measurement framework that is utilised to measure cyber security awareness and behaviour in the R SIGNALS. The framework is an extension and adaptation of the government NCSC infographics for basic cyber security protective practices which in this study is split into five themes for measuring awareness (device safety, device backup, phishing, password and malware) and one theme for behaviour. The research adopts a quantitative positivist approach with using a questionnaire to measure human cyber awareness and behaviour. Study of human psychology models in the literature indicates that factors such as awareness and subsequent attitudes have direct influences on human behaviour. Results after codification and statistical analysis confirmed that technical trades in the R SIGNALS has better awareness of device safety, malware and phishing while cyber training was directly related to user behaviour and awareness of device safety. Overall user awareness in the R SIGNALS was found to be at Integrated level out of the five levels in the Community Cyber Security Maturity Model.

The measurement framework is not limited to application to R SIGNALS and has the utility for other corps and organisations within the Army. Key future research recommendations included adding an attitude scale to the framework and having the correct sample to represent population variation.

Keywords: cyber security awareness, information security awareness, human and cyber, cyber behaviour, cyber training, cyber hygiene, cyber awareness measurement, information security awareness measurement, cyber maturity model.

ACKNOWLEDGEMENTS

Firstly, I would like to express my heartfelt thanks to my dissertation supervisor Dr Victoria Smy for her undivided support and her patience with me during this study. Without her invaluable support, this study would not have been successful.

I would like to convey my thanks to all the R SIGNALS soldiers and officers who took part in the survey.

Finally, I would also like to thank all those individuals who have directly or indirectly contributed to this study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

LIST OF ABBREVIATIONS

A2020R	Army 2020 Refine
ALARP	As low as reasonably practicable
APC	Army Personnel Centre
CCSCMM	Community Cyber Security Capability Maturity Model
CMM	Capability Maturity Model
CPT	Cyber Protection Team
CURES	Cranfield University Research Ethics System
DE Officer	Direct Entry Officer
DoS	Denail of Service
ENISA	European Union Agency for Network and Information Security
FofS	Foreman of Signals
HAIS	Human Aspect of Information Security
HM Govt	Her Majesty's Government
ICT	Information Communication Technology
ICM	Information Capability Management
ILO	Intended Learning Objectives
IS	Information Systems
ISA	Information Security Awareness
ISO	International Security Standard
IT	Information Technology
JPA	Joint Personal Administration
KAB	Knowledge, Attitude and Behaviour

LE Officer	Late Entry Officer
MOD	Ministry of Defence
NCSC	National Cyber Security Centre
NICE	National Initiative for Cybersecurity Education
NSRA	National Security Risk Assessment
R SIGNALS	Royal Corps of Signals
RAF	Royal Air Force
RD	Regimental Duties
RQ	Research Question
RN	Royal Navy
SDSR	Strategic Defence and Security Review
SPSS	Statistical Package for the Social Sciences
Tfc Offr	Traffic Officer
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned action
TAM	Technology Acceptance Model
Trg	Training
TOT	Technical Officer Telecommunications
UK	United Kingdom
YofS	Yeoman of Signals

1 INTRODUCTION

In the world that we live in today Information Technology (IT) is ubiquitous and there is greater risk to cyberspace than ever before as access to computer and networks have become more prevalent and organisations have become more dependent on the information systems that is used to carry out daily business processes. Because of these risks organisations employ cyber security strategies and policies which defines protective security practices that should be applied to prevent or reduce the likelihood of cyber-attacks.

> "*Cyber Security of any organisation can only be as strong as its weakest link. The biggest vulnerabilities of a system are not necessarily found in hardware or software, but rather with the people who use it*" (Wright, 2016).

The National Security Strategy and Strategic Defence and Security Review (SDSR) (HM Government, 2015) highlights that 'Cyber' is one of the tier one risks (shown in Figure 1) which is the highest priority risk for national security over the next five years and remains a priority for Ministry of Defence (MOD).

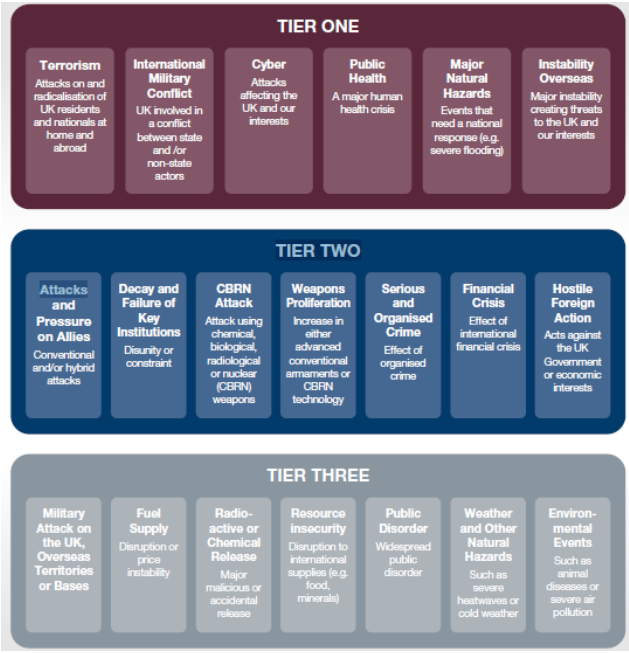


Figure 1 - NSRA 2015 Priority Risks (HM Govt, 2015, p.87)

Due to the likelihood and impact of risks posed from cyberspace and the priority placed on it, the UK government (2015) announced that £1.9 billion would be spent for the following five years on UK's cyber security. A portion of the budget will be allocated to the Armed Forces to improve the cyber defences and cyber security programmes. Effective cyber security programmes in the military will need mechanisms for enhancing basic user security awareness and adoption of safe computing behaviour.

In the UK National Cyber Security Strategy defines 'cyber security' as:

> *"The protection of information (hardware, software and associated infrastructure), the data on them, and the services they provide from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of a system, or accidentally, as a result of failing to follow security procedures"* (HM Government, 2016, p15).

To avoid becoming susceptible to cyber-attack, it is imperative that cyber security strategy and policies within it are understood and cyber security awareness is widespread amongst employees within an organisation that interacts with the cyberspace whether at home or at work. Employees should also be able to adopt protective cyber security practices to prevent becoming victim of organised cyber criminals. The MOD Cyber Primer doctrine mentions the importance of cyber awareness, education, individual and collective training exercises and an understanding of risk management in the cyberspace (HM Govt, MOD, 2016). Although, the doctrine mentions about the MOD cyber good practice guide, there is currently no cyber strategy document for the Army unlike the Royal Air Force (RAF) which was published in 2014. In the Army Information Sub-Strategy paper (General Semple, 2015) written by the Directorate Information, Army Headquarters it is mentioned that 'cyber' has not yet been embraced by the Army and is a priority area of modernisation to achieve success in the information age. Whether back in base or in a deployed

environment, R SIGNALS units and employees are responsible for providing and maintaining communication infrastructure, networks, systems and services to the wider Army, hence makes it prone to cyber-attack if robust cyber security strategy is not implemented and soldiers and officers are not well acquainted with cyber protection measures.

Due to the technical nature of R SIGNALS, the corps becomes a key point of focus when searching pathways to aid the Army 'embrace' cyber. Under Army 2020 Refine (A2020R), R SIGNALS is restructuring with added focus in the field of cyber in addition to providing IS, networks and services (R SIGNALSa, 2017). This means there is greater importance for soldiers and officers to be aware of basic cyber security protective practices. While there are policies and doctrines to aid cyber security at high level, there is a need to assess user awareness of basic cyber protective practices and to examine they exhibit safe and secure cyber behaviour. There is currently no measurement framework in the R SIGNALS or the Army for testing basic user cyber awareness and behaviour. In this research, the author will develop an innovative and novel measurement framework in the form of a questionnaire to assess cyber security awareness and behaviour in the novel context of R SIGNALS. The measurement results can then be extrapolated to benchmark user cyber security awareness level using existing cyber security maturity models found in literature. This framework will not be limited to R SIGNALS and the benefits can be realised by other corps within the Army or other services.

1.1 Research Overview

Cyber security is key to protect our infrastructure, systems, networks and services. Understanding the threats and vulnerabilities to our systems and networks is key to developing a strategy that reduces the risk of an attack. Due to rapid technological advances, cyber security tends to be challenging and difficult to maintain as hackers find more sophisticated form of attacks to infiltrate our networks to gain valuable information or inflict damage. There are numerous online cyber security awareness initiatives and campaigns led by the UK Govt which defines safe practices but these are useless unless the user

communities are aware of it and in compliance. There is also an issue with whether users have the right attitude and behaviour to follow the safe practices despite being aware of it. Hence, it is equally important to understand the motivational aspects of cyber behaviour and what influences users to adopt cyber security protection measures. The Army currently do not have a cyber security strategy and, although Cyber Protection Teams (CPTs) recently have formed which comprises of cyber professionals, there is no empirical evidence on the level of awareness amongst normal users. There are numerous academic research outputs that show that technological defences and cyber professionals alone cannot provide full cyber security. This research will look at cyber security awareness and human behavioural models and explore what influences users' cyber behaviour.

1.2 Research Context

To fulfil the overall aim of the disseration the research will consider the following two research questions:

Research Question 1 (RQ1) – How can cyber security awareness be measured? Can an explicit framework for cyber awareness be constructed to inform measurement of cyber security awareness?

Research Question 2 (RQ2) – Can measurements be used to form an assessment of cyber awareness capability maturity?

1.2.1 Research Rationale

Cyber security awareness and the application of security practices are crucial to deter adversaries from gaining access to our networks and systems. The MOD has a cyber strategy which should be used to develop strategies for the three services (Army, Navy, Air Force). The Army currently do not have a cyber strategy hence it is difficult to interpret what cyber practices should be employed at ground level by the user communities. It is important to understand what cyber situational awareness means and what basic practices ought to be used by normal users. This research will help understand the level of cyber security

awareness amongst soldiers and officers in the R SIGNALS. It will further examine cyber behaviour by use of behavioural models to understand what motivates employees to adopt cyber practices and preventative cyber security measures. The key responsibility of R SIGNALS units and personnel are to provide networks, systems and services in barracks and in a deployed environment in operations. As soldiers and officers have access to the cyberspace through the network and systems, it is important for them to understand the risks and vulnerabilities of cyber intrusions by the adversaries and have awareness of basic cyber security practices.

This thesis study will aim to fulfil the dissertation module aims and Intended Learning Outcomes (ILOs) for Information Capability Management (ICM). The study will be closely aligned to Cyber Security module of Information Capability Management (ICM). The thesis study will conduct an investigative study of cyber security awareness and the application of safe cyber security practices in R SIGNALS organisation in terms of producing recommendations for cyber training in the future. The study includes critical evaluation and integration of published research studies that are applicable to cyber security awareness and cyber behavioural models. Evaluation and analysis of behavioural models and cyber capability maturity models will be carried out to produce cyber awareness training recommendations and benchmarking cyber security awareness for soldiers and officers in the R SIGNALS.

1.2.2 Research Aim and Objectives

The aim of this research is to study the human perspectives of cyber security capability in defence settings. This research will look at cyber security awareness and cyber behaviours amongst soldiers and officers in the R SIGNALS to provide recommendations on future cyber security training. Along with answering the research questions set out above, objectives of the study will entail:

a. Study of cyber security awareness and behaviour amongst soldiers and officers in the R SIGNALS.

b. Understand UK and Defence cyber security strategy and how it applies to the Army.

c. Study of cyber behaviour through use of behavioural models and factors that influences cyber behaviour.

d. By use of government infographics on cyber security for small businesses understand cyber security awareness and protective practices adopted in the R SIGNALS and how best to deliver them.

e. Find a suitable capability maturity model to analyse and benchmark cyber security capability maturity in R SIGNALS.

1.3 Thesis Structure

The report will include six chapters and will comprise of Introduction, Literature Review, Research Methodology, Results, Discussion and Conclusion.

Chapter 1 – Introduction: This chapter will provide an overview of the research area and describe how the research will benefit R SIGNALS. It will also explain the research rationale and highlight the research questions to achieve the aim of the dissertation. Furthermore, the chapter will outline the aim and objectives of the research.

Chapter 2 – Literature Review: This chapter will include critical appraisal of research literature from multiple sources. The research literature will examine background factors and demographics which may have an effect to cyber security awareness. It will also investigate the human aspects of cyber in general which could lead to or influence cyber security behaviour. Furthermore, the research will investigate the most promising cyber security awareness measurement models and aim to overlap with the government infographic on cyber security for small businesses. Finally, a detailed study of cyber security capability maturity models is going to be carried out to benchmark cyber awareness state in the R SIGNALS.

Chapter 3 – Research Methodology

Chapter 3 will look at various research methodologies and adopt the most suitable research philosophy to address the research questions. The research methodology used will be most closely aligned with the ‘positivist’ philosophical approach. This method will be objective and will collect quantitative data from soldiers and officers through an online survey questionnaire designed using Qualtrics.

Chapter 4 – Results

This chapter will look at the results from the data collected from soldiers and officers in the R SIGNALS using the questionnaire. It will also interpret the results returned from the critical literature review and justify the use of cyber security awareness measurement framework in this research.

Chapter 5 – Discussion

This chapter will look at the results returned from the hypothesis tested for the research. It will discuss results obtained from the survey and literature review and analyse the research questions in detail. Evaluation of the methodology used for the research will be conducted with comments on strengths and weaknesses of the methods used. Furthermore, recommendations will be made for future research.

6 – Conclusions

This chapter will highlight the conclusions drawn from this research and present a summary of findings about the research and cyber security awareness and behaviour of soldiers and officers in R SIGNALS. It will also include summary of the hypothesis results and highlight key recommendations for future research.

2 LITERATURE REVIEW

2.1.1 Literature Review Overview

In this chapter a critical review of literature will be conducted and relevant research literature from multiple sources will be rigorously evaluated to inform the dissertation aim and objectives. The literature review will include research on cyber security awareness, and more importantly, measurement frameworks available to measure cyber awareness. This approach will be adopted to explore the linkage between the practitioner (industry/defence) and academic domain with respect to cyber security awareness. In addition to this, aspects of human behaviours in cyber security will be investigated to find the factors which influences cyber security awareness in general. A detailed study of cyber awareness frameworks and cyber security maturity models will be carried out to measure cyber awareness and benchmark cyber awareness maturity state in the R SIGNALS.

2.1.2 Research Search Strategy

“For most research questions and objectives, you will have a good idea of which subject matter is going to be relevant. You will, however, be less clear about the parameters within which you need to search” (Saunders, Lewis and Thornhill, 2009, p75). For this research an effective search strategy was applied to gain access to high quality and relevant information from the electronic databases available. Given the aims and timescales of research at master’s level a bounded literature review was conducted on cyber situational awareness, cyber behaviour, cyber security measurement frameworks and cyber security maturity models. Keywords such as ‘Cyber’ and ‘Cyberspace’ were considered too broad for the research topic and were considered out of scope of the aims and objectives of the present research. Abstract reviews was used to determine the right literature fo the thesis using electronic sources available through Cranfield University login credentials.

A detailed search strategy was devised and run through the electronic databases; Cranfield University Barrington Library, IEEEXplore, Google

Scholar, Scopus, Science Direct, ACM, Emerald, SpringerLink etc available through the Cranfield University website. Keywords such as ‘Cyber Security’, ‘Cyber Awareness’, ‘Cyber Awareness Measurements’, ‘Information Security Awareness’, ‘Cyber Security Capability Maturity Models’’, ‘Cyber Hygiene’ and ‘Cyber Behaviour’ were used in the electronic databases to find the research material. The results presented from the databases when using the keywords were then filtered by checking whether the search terms were included in the title, keywords or abstract. In addition to this, several past Cranfield University dissertations which were available through the Barrington Library portal were reviewed. Academic articles and journals were filtered to provide results between 2000 – 2018 and an inclusion criteria of peer-reviewed was set. Furthermore, MOD Intranet was used to find military doctrines and articles which would inform how the military respond to Cyber Security.

The resulting literature returned from the online databases were then grouped together into several themes for the author to review distinct aspects of cyber security awareness. This also helped the author to coherently separate areas of literature into different themes and link it to the research questions. Outputs from the literature are presented in the sections that follow.

2.1.3 Literature Review Themes

The materials returned from the literature review has been outlined into a number of themes. This was to allow the author to demonstrate a good understanding of the research area and ensure every aspect of cyber awareness is captured to inform the research questions.

Literature search was conducted using keywords on online databases and results filtered after reading the abstract and title of the documents. The core areas of the thesis were then identified and grouped into several themes. The eight themes identified are as follows:

1. Cyber Security
2. Threat from Cyberspace

3. Cyber Security Awareness

4. Factors affecting Cyber Awareness

5. The Human Factor

6. Cyber Awareness Measurement Frameworks

7. Cyber Security Maturity Models

8. MOD Doctrine

Appendix A includes academic, white and grey literature that was used for this research.

2.1.4 What is Cyber Security?

> *"Cyber Security refers generally to the ability to control access to networked systems and information they contain. Where cyber security controls are effective, cyberspace is considered a reliable, resilient, and trustworthy digital infrastructure"* (Bayuk et al., 2012, p1).

The world is interconnected with internet of things which comprises of devices and networks that are capable of exchanging information. Whilst the benefits of a connected world are realised via the human kind, it is also important to understand and be aware of what risks and vulnerabilities exists by a globally connected world. This means that we need to be conversant with the protective measures that needs to be applied to reduce the probability of a cyber-attack from malicious users. Cyber security is protecting our networks, information systems and devices that are connected in the cyberspace. The Defence Cyber Primer (2016) describes the importance of Cyber Security for MOD as follows:

> *"Cyber security is also vital to Defence as our Armed Forces depend on information and communication systems, both in the UK and on operations around the world. Our adversaries' activities present a real and rapidly developing threat to these systems"* (HM Government, MOD, 2016, p.1).

The 2016 National Cyber Strategy aim to invest £1.9 billion to protect the UK's systems and infrastructure and to counter the threats from cyberspace. The budget will be invested into three different areas; defend against attack, deter hostile cyber actions from adversaries and develop cyber innovation. The investment will not only look at protecting public and private sector, big companies and industries but also look at investing in people to ensure development of a whole society capability for the UK. For the MOD, this investment is crucial as all sectors of defence are dependent on its critical networks, systems and information which in one way or another are connected to the wider digital space. Organisations must have a good understanding about the risks and vulnerabilities that is prevalent by connecting to this digital space know as the 'cyberspace'.

2.1.4.1 The Threat from Cyberspace

The MOD SDSR (2015) identifies 'Cyber' as the fifth domain of warfare. Traditionally, warfare was limited to four domains; land, sea, air and space but as the information age evolved and the geopolitical landscape progressed into an internet of things the threat from cyberspace has become more prominent. "The information age is interconnected use of electronics, which moves digitised data through the electromagnetic spectrum, and has brought forth a fifth domain." (Crowell, 2010, p.2)).

President Obama stated that cyber threat would cause serious economic and national security challenge for America and added that the country's prosperity would depend on cyber security (White House, 2009). The ever-increasing dependence on our Information Communication Technology (ICT) in military operations has meant our systems, network, data and people are vulnerable from the threat that cyberspace exposes. It is important that the armed forces counter these threats to allow freedom on manoeuvre in the battlespace and have the technological and operational advantage against the adversaries.

There are numerous examples of cyberattack which can be in the form of a malware planted within a target system to steal information or to disable and encrypt the system holding it to ransom. Alternatively, it may be in the form of a phishing email that is intended to fool the victim in offering in personal information. Recent attacks include Russian aggression against Estonia through a Denial of Service (DoS) in 2007 which disabled a number of key infrastructures (BBC News, 2008a) and crashed servers running websites for state government, political parties and leading newspapers. Another example is the hacking of the Yahoo email system in 2013 where one billion accounts were affected and resulted in stolen passwords and account details (The Guardian, 2016). In 2017, NBC news (Johnson, 2017) reported a phishing attack on Gmail users using a worm posing as an email which affected roughly a billion users worldwide. It is of paramount importance that cyber security measures are in place and ICT infrastructure improved to counter these type of threats that is posed by cyberspace. The next section will look at what 'cyber security awareness' is and the importance it has for defending against social engineering exploitation of computer users.

2.1.4.2 Cyber Security Awareness

While organisations invest in their cyber security professionals, it is equally important that cyber awareness amongst normal users are also addressed as lack of cyber security awareness can be exploited by cyber criminals (as indicated in the Google attack). "Operating systems and programmes are more protected these days and attackers have shifted their attention to human elements to break into the organisation's IS" (Abawajy, 2014, p237). As technological defences are getting stronger, cyber criminals are using social engineering techniques to target human weaknesses. User carelessness and lack of awareness can lead to system security breaches. Therefore, there is a need to address the cyber security awareness to protect the IT systems and networks. Rouse (2006, cited in Bullée et al., 2015, p98) mentions that as

organisations become increasingly dependent on their ICT, social engineering will become the greatest threat in the cyberspace.

Choo (2011) classifies cyber-attacks into ‘syntactic, ‘semantic’ or a combination of both called the ‘blended attack’. Syntactic attack is carried out exploiting the technical vulnerabilities in software and hardware, whereas semantic attack is carried out using social engineering techniques exploiting human weaknesses. Brynielsson and Frank (2014) argues that although nations have adopted their cyber strategies, they are not always in agreement but priorities remain common in the need to protect critical national infrastructure and improve cyber awareness. It is important that these cyber strategic documents are translated into cyber policies and practices that are easy to understand and apply within organisations that employs IT systems that extend to the wider cyberspace. Cyber security situational awareness not only includes understanding the threat posed from a technical viewpoint but also from a human perspective to interpret the signs of malicious activities. Cyber security knowledge and awareness is essential to identify and take preventative measures if exposed to an attack from malicious users. Abawajy (2014) in his research on cyber awareness programme delivery method mentions ISA is the understanding from users about the importance of information security protective practices. Users should adopt these practices with good cyber hygiene.

2.1.4.3 What is Cyber Hygiene?

Protecting our network and IS connected to the cyberspace requires good cyber hygiene of doing the right thing, putting into place safe practices and exhibiting good cyber behaviour. The European Union Agency for Network and Information Security (ENISA, 2016) mentions cyber hygiene should be incorporated into organisation’s daily routine and should be maintained regularly like personal health to keep it in a good condition and to minimise risks from cyber threats. It further states that good cyber hygiene is essential for protecting data, networks and infrastructure for businesses and organisations against nefarious users.

Crannell, Moulton and Sheppard (2013) in their study comes with a concept of ‘Cyber first AID’ with AID standing for adaptable, integrated and deliberate. The approach is aimed at putting a cyber-attack response plan in place which can be adapted to deal with any form of attack. The plan should be fully integrated in the organisation’s routine and is deliberate in the form that everyone is aware of their role and the plan is regularly practiced.

2.1.4.4 Factors affecting Cyber Security Awareness

Barford, Dretterrich and Fredrikson (2010) highlights the seven aspects of cyber situational awareness as being aware of the present situation, awareness of the damage an attack can have, awareness of how situation unfolds, being aware of behaviour of malicious users, awareness how the situation is caused, being aware of the quality of the collected situation awareness information and predicting possible futures. It is important that cyber security awareness is addressed to reduce the risks posed by the adversaries from cyberspace and that countermeasures are put into place against the likelihood of an attack. To improve cyber security awareness in an organisation, technology defences alone are not enough to mitigate against risks posed by the cyber space. There are other factors that need to be considered such as cyber security policies, training, culture etc., but the most critical component is the human factor (Colwill, 2009). Organisations invest in technologies and train cyber practitioners to protect their networks and systems but often fail to address security awareness of normal users making them the weakest link (Aloul, 2012). The next section goes on to expand upon the human elements of cyber that affect cyber security awareness and behaviour.

2.1.5 The Human Factor

As organisations increase their use of advanced secure technologies with modern hardware and software, hackers are attempting to break into organisations by targeting the weakest link; the uneducated computer user (Katz, 2005). Whilst it is important to put in place technological defences and

employ cyber professionals to protect computer systems and networks, it is also important that all employees within an organisation are trained on basic cyber protection measures so that they are fully aware of the risks and vulnerabilities when connected to cyberspace. Furthermore, employee compliance to organisational information security policies, rules and guidelines needs to be put in place to reduce the threat from cyberspace. Bulgurcu, Hasan and Benbasat (2010) adopts the Theory of Planned Behaviour (TPB) model to prove compliance behaviour depends on user intentions and then intentions are dependent on normative beliefs, attitudes and self-efficacy. Normative beliefs are one's perception of how friends or close ones act in a certain way. Self-efficacy refers to individual's confidence on oneself to successfully act in a given situation and attitude is how someone feels about something (Fang and Shih, 2004). Kim, Rhee and Ryu (2009) study the importance of self-efficacy in information security and recommends being used to design cyber awareness programs. The study tested how much influence self-efficacy has on risk management behaviour and the intention to comply with security policies. Results from the study showed survey participants with high self-efficacy exhibited better cyber behaviour by adopting safe protective practices and showed intention to improve their security efforts.

Figure 2 illustrates the six interdependent layers of cyberspace as social, people, persona, information, network and real (HM Govt, 2016, p5). The social, people and persona layer belong to the cognitive domain of cyberspace and this is how humans interconnect with the cyberspace. To address the cognitive domain, it is imperative to ensure people are cyber trained and have awareness of basic protective cyber measures when connecting to the cyberspace. Not only this, it is also important to make sure that people apply safe security behaviours and have the motivation to avoid making themselves vulnerable to cyber-attacks from malicious users.

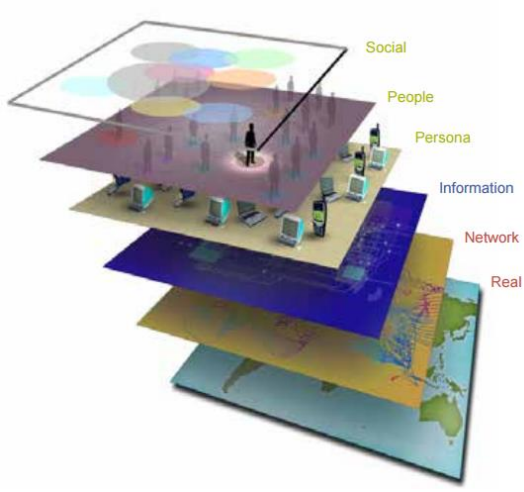


Figure 2 - Six Layers of Cyberspace (MOD Cyber Primer, 2016, p5)

Changing information security behaviour is not just about giving employees information on risks associated with the cyberspace and protective practices that should be undertaken through preventative behaviour. Organisations must ensure employees understand and are willing to take these advice and this requires changes to attitude and intentions (Bada and Sasse, 2014).

"One of the most intriguing findings from IBM's 2014 Cyber Security Intelligence Index is that 95 percent of all security incidents involve human error" (Howarth, 2014). These errors can be from malicious insiders from within the organisation or from someone who has accidentally breached security by mistake or due to poor organisational policies. Impact of human error leading to cyber incidents can hamper on an organisation's ability to operate and loses the culture of trust within the workforce. For example, in 2017 ransomware WannaCry virus decapitated the UK's National Health Services ability to operate for a significant period just because the computers were not kept up to date and latest software patches were not installed (BBC News, 2017b). Williams (2008) states that organisations often overlook the importance of workplace culture in defending the computer networks and just focuses on the perimeter defences such as intrusion detection, firewall etc. Governance of information security should be from strategic level and capture all the actions that are necessary to counter possible reasons that could lead to a security breach.

Ögütçü, Testik and Chouseinoglou (2014) states that “security is not a problem with technology but a problem of human nature and the effective behaviour of IS users and their security awareness which needs to be assessed, evaluated and addressed accordingly”. Ng Kankanhalli and Yunjie (2009) uses a Health Belief Model, adapted from the healthcare literature, to study users’ computer security behaviour. Furthermore, computer security behaviour not only includes using protective technologies but also behaviours such as selecting strong passwords, regular data backup and becoming careful when opening suspicious emails. It is important to understand what influences a computer user behaviour to be more motivated in complying with the organisational cyber security policies and align cyber security awareness programs accordingly. It is vital to understand what influences a user behaviour to adopt and be compliant of cyber security practices. This section explored the ‘human factor’ which has to be addressed for keeping IT systems and network safe from exploitation. The next section will look at a number of psychological models for predicting human behaviour.

2.1.5.1 How is it possible to influence user actions for safe and secure Cyber Behaviour?

> *“Actions and intentions do not always align”* (Gilovich and Kruger, 2004, p328).

It would be fair to say that good intentions do not always follow with the correct actions. No matter how good the cyber strategy is for an organisation and how much there is done to raise cyber security awareness of employees, it is worthless if users do not take the necessary actions to prevent against cyber incidents from occurring and failing to show safe IT behaviour. Lebek et al. (2014) conducted a detailed study on Information Systems (IS) behaviour using four psychological theories (Theory of Planned Behaviour (TPB), General Deterrence Theory, Protection Motivation Theory and Technology Acceptance Model) to investigate factors influencing human behaviour. The study confirmed that all the models researched had their own factors that influenced behavioural intentions and actual behaviour.

It is important to understand the behavioural models available within psychological literature to identify how attitudes are linked to behavioural intentions. A model that is often used in academic studies is the TPB which was previously known as Theory of Reasoned Action (TRA) developed by Ajzen and Fishbein in the 1980s. According to Arnold et al. (2005, p254) TRA model was first developed to highlight the relationship between attitudes and behaviour. TRA works in the belief that behaviour is linked to intentions and intentions linked to attitude. This later became the TPB with the addition of perceived behavioural control portion. The added portion was to do with the belief or self-control that one must and can act in a certain way in different situations. Figure 3 illustrates the concept of TPB. The model highlights that the way a human action takes place is dependent on the humans' intentions and intentions can be shaped and predicted by behavioural beliefs, normative beliefs and subsequent attitudes. Fielding, McDonald and Louis (2008) uses the TPB model as applied to students in a sustainability conference to investigate engagement into environmental activism and found that that students with positive attitudes and normative beliefs had the intention to engage in the desired behaviours.

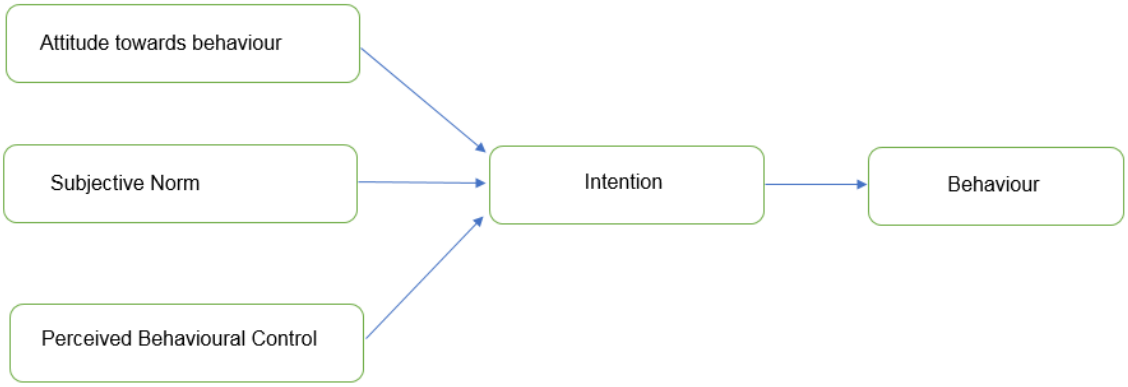
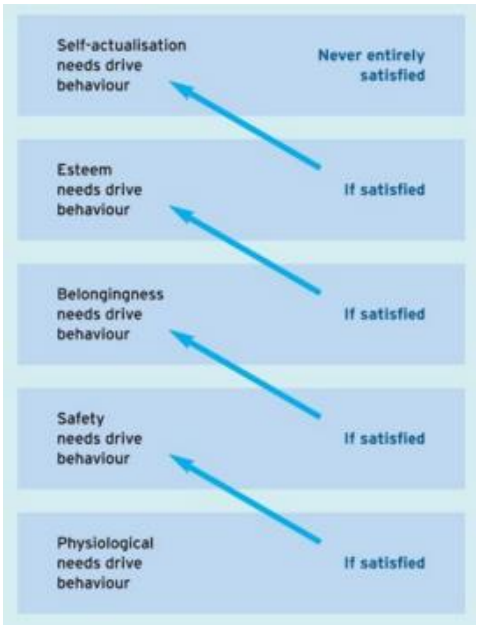


Figure 3 - Theory of Planned Behaviour (Adapted from Hoeksma, Gerritzen, Lokhorst et al. 2017,p.17)

Similarly, Fang and Shih (2018) successfully used the TPB model to predict customer's intention to exhibit suitable online banking behaviour by measuring the factors influencing attitudes and behaviour. Since the model was introduced there have been many success stories in the employment of the model

(including health research) to influence behavioural actions. However, it has also not been short of criticism and researchers have critiqued about the predicted validity of the model as it fails to address unconscious behavioural influences such as affect and emotions (Sniehotta, Presseau and Araújo-Soares, 2014, Ajzen, 2011). Conner (2015) argues that there is no evidence to support the views that critiques have made about the theory and researchers should continue adapting it and extend the theory to benefit their studies. The theory is relevant to cyber security as perceived behavioural control, attitude and normative beliefs can be used to predict behaviour of IT users.

To improve cyber security, it is important to address these factors (attitude, subjective norms, behavioural control) which influences secure behaviours to ensure desired cyber behaviour is adopted by employees in an organisation. Unless these factors are understood clearly and addressed, cyber security awareness campaigns and education will prove to be futile in addressing cyber security risks and vulnerabilities within an organisation. Another factor that is linked with intention is 'motivation' which is crucial in translating intentions into desired behaviour (Bada and Sasse, 2014). It is important for employers to ensure motivation is taken into consideration in the cyber security awareness strategy in order to promote safe cyber security practices and behaviour. Figure 4 illustrates Maslow's hierarchy of needs which is a psychological motivational theory developed by Abraham Maslow (1954).



`

Figure 4 - Maslow's Hierarchy of Needs (Arnold et al., 2005, p313)

Maslow's model is based on human desires which includes, physiological, safety, belongingness, esteem and self-actualisation needs. In an organisation, these needs should be addressed and managed carefully by the employers to get the employees to show desired behaviours in cyber security. Another motivation theory include Festinger's (1957) cognitive dissonance theory which assumes behaviour as a function of cognitive process and interpretation of information and is key for employers to understand workplace behaviours. Harmon-Jones (2015, p.184) explains cognitive dissonance occurs when individuals have thoughts that are related but are inconsistent or when actions do not align their beliefs causing discomfort in the situation. The discomfort encourages the individual to reduce the dissonance by taking actions that align to his thoughts or by changing his thoughts to align with his actions. Ward and Meade (2018) uses cognitive dissonance to tackle careless responding of online surveys by including questions that increased cognitive dissonance in the participants. Through hypothesis testing, it was proven that careless responding reduced when participants'cognitive dissonance was changed.

Technological Acceptance Model (TAM) is another theory which could impact the way how employees behave when they come to use IS or IT equipment.

Durlabhji and Fusilier (2005, p234) mentions “TAM states behavioural intention to use a technology derives from two beliefs”. The two beliefs are listed as perceived usefulness of technology and ease of use. It is imperative that employers address these beliefs so that employees perception of the system in use has a positive effect on behaviour. Whilst it is necessary to ensure attitude and intentions follow safe computing behaviour, it is also important to take into consideration the organisational culture in an organisation. Schlienger and Teufel (2003) mentions two facets of organisational culture as basic assumptions and beliefs which are exhibited by values, norms and knowledge of the organisation. These factors are also equally important to address in order bring desired behavioural changes in the employees. In addition to this, cultivating information security culture within an organisational culture is essential where users identify and adopt the most appropriate security controls successfully (Veiga and Eloff, 2010).

Sharma, Warkentin and Shropshire (2015) in their study argues that intention may not be the best predictor for the actual behaviour and states personality traits works better when predicting variable behaviour. The study further intends to root out personality traits which influences people engaging with the correct cyber behaviour. Goldberg (1990) comes up with the concept of the ‘big five’ personal traits which are extraversion, agreeableness, conscientiousness, neuroticism and openness (as shown in Table 1).

Table 1 - Big Five Personality Traits (Adapted from Heinek and Anger, 2010, p536)

Personality Traits	**Description**
Extraversion	Outgoing, ambitious and sociability
Agreeableness	Cooperative and likeable
Conscientiousness	Degree of self control, need for achievement
Neuroticism	Someone tense, anxious or moody
Openness	Flexible, creative and intellectually orientated

For researchers who do not have full confidence on the validity of TPB model, maybe personality traits is the way forward for predicting human behaviour. Sharma et al. (2015) in their study reported that people with conscientiousness and agreeableness traits had positive link with computer behaviour. An exploratory study conducted by Marks and Rezgui (2007) on ISA in higher education concluded that factors such as conscientiousness, cultural assumptions and beliefs and social conditions affected the behaviour and attitude of university staff.

This section explored different human psychological models to explore factors that have direct influence over behaviour. The next section will look at whether demographics have any influence on cyber security awareness and behaviour.

2.1.5.2 Is Cyber Security affected by Demographics?

Humans are often targets to hackers who use social engineering techniques to exploit our systems and networks to steal information or with other malicious intentions. It is important for employers to understand the demographic background of their workforce to determine their likelihood of becoming victims of cyber-attacks through social engineering. This will help in devising a cyber security strategy which can take into consideration the demographic aspect of employees in an organisation, especially if there is relationship between demographics and susceptibility to attack. Aloul, Darwish and Zarka (2013) carried out a study to understand victim's background and personality traits to phishing attacks; a very popular form of attack used by hackers. The study makes comments that factors such as demographics could have a link to users getting victimised of phishing attacks. Table 2 illustrates the demographics vs phishing susceptibility (Aloul et al., 2013). The personality trait results from this experiment contradicted with the study that Sharma et al. (2015) conducted where it was reported that people with agreeableness personality had better cyber behaviour. The research for using personality traits to predict computer behaviour needs to be further validated due to this.

Table 2 - Demographics Vs Phishing Susceptibility (Aloul et al., 2013, p5)

	Highly Susceptible	**Less Susceptible**
Age	18 -24 years old or less	25 years old or more
Gender	Female	Male
Anti-phishing Training	No Training	Anti-Phishing trained
Education	Humanities	Computer Science
Training Delivery Method	Non-embedded	Embedded (in games for example)
Personality	Agreeableness	Conscientiousness
Internet Usage Behaviour	E-commerce and Online Banking	Emails and simple browsing

The term phishing means how hackers coax their victims to provide them personal information through social engineering attacks. It is a very common form of attack used by hackers to gain sensitive information and use it to their advantage. Many studies have taken place using role-play techniques to establish relations between user demographics and likelihood of falling victim to a phishing attack. A role-play study conducted by Sheng, Holbrook, Kumaraguru et.al. (2010) concluded that 18 – 25-year-old are more susceptible to phishing and females are more likely to fall in trap of phishing than males, therefore converging with the findings of Aloul et al. (2013).

This section covered a number of human behavioural models to understand the relationship between attitude, intention and behaviour. It also covered that personality traits are key to observe variation in human behaviour. Finally, past research indicated that it might be important to consider demographics when attempting to measure cyber security awareness and behaviour. The following section will now explore the utility of cyber security awareness measurement framework.

2.1.6 Cyber Security Awareness Measurement Frameworks

One of the key objective for this research is to investigate whether there are any frameworks available in literature to measure cyber security awareness. To be able to quantify basic user cyber awareness for an organisation will be very beneficial for employers, as the results can be used to drive cyber awareness programs and change policies to address where shortfall exists. By addressing these cyber awareness shortfalls and implementing cyber education and training programs, organisations can influence business continuity and organisational sustainability to protect their networks and people against malicious users and activities. The effectiveness of such training programs can also be tested using an awareness measurement framework.

The brand that R SIGNALS are known by is ‘Leaders of the Digital Age’. This is because the organistion is responsible for providing agile and rich information services, networks and infrastruture to the Army whether deployed abroad on Operations or on training activities within the UK. Although, R SIGNALS soldiers and officers deal with IT equipment and networks as part of daily their business processes, there is currently no measurement framework in place to assess basic user cyber security awareness. The author intends to close this gap by creating one which will measure basic cyber awareness and behaviour of computer users in the R SIGNALS. The author adapts and extends the NCSC cyber security infographic guide (shown in Figure 5) to create and measure five areas of cyber security. The guide makes further claims that time, money and business’ reputation can be saved by following the basic cyber protective practices to protect against common form of cyber attacks (NCSC, 2017). There were five measurement themes chosen for awareness which was Device Backup, Device Safety, Malware, Phishing, Password Safety and one theme for behaviour and these will be tested using Awareness and Frequency Likert scales. The framework will need refining and further validation before it can be fully used to assess cyber security awareness and behaviour.

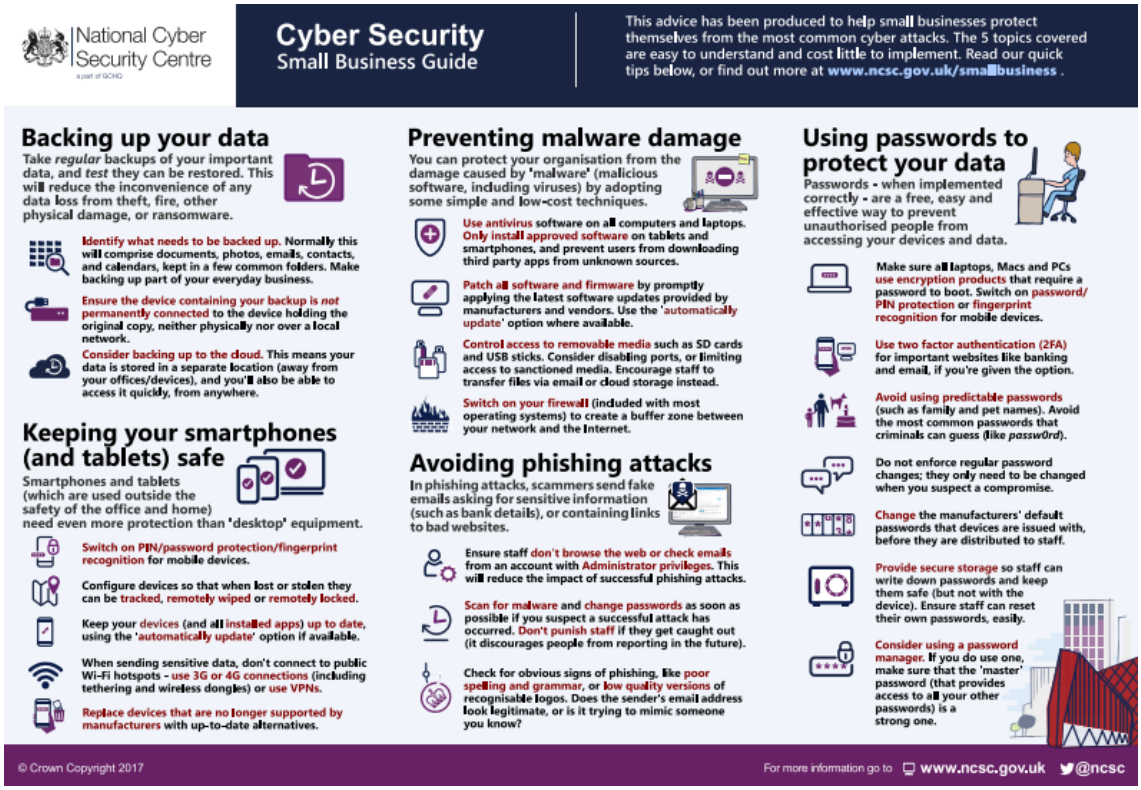


Figure 5 -NCSC Cyber Security for Small Businesses (NCSC, 2017)

Niekerk and Solms (2013) mentions that the term cyber security is often interchangeable with information security. Although the two terms ‘cyber security’ and ‘information security’ are similar in meaning the term cyber security is more to do with securing the cyber space and the entities (devices, system, infrastructure, network, information, people) within them whereas information security is to do with protecting confidentiality, integrity and availability of information and the devices and servers that hold the data. The present study will look at a number of measurement frameworks for ISA and look at the benefits of utilising them to capture or measure cyber security awareness in an organisation.

From the literature review, it was identified that many academics have conducted measurements of security awareness through use of their own unique frameworks. Ng, Kankanhalli and Xu (2009) highlights that there is a shortage of empirical evidence to indicate that security training and awareness programs are enough for people to show safe computing behaviour.

Wahyudiwan, Suchayo and Gandhi (2017) in their case study to improve information security within public services uses seven focus areas as shown in Figure 6 to test ISA. The study made use of an online questionnaire to assess ISA using knowledge, attitude and behaviour as variables. The study results identified that knowledge had influence over attitude and behaviour and attitude had influence over behaviour.

Focus Area	Sub-Areas
Password management	• Locking workstations • Password sharing • Choosing a good password
Email use	• Forwarding emails • Opening attachments • IT department level of responsibility
Internet use	• Installing unauthorized software • Accessing dubious websites • Inappropriate use of internet
Social networking site (SNS) use	• Amount of work time spent on SNS • Consequences of SNS • Posting about work on SNS
Incident reporting	• Reporting suspicious individuals • Reporting bad behavior by colleagues • Reporting all security incidents
Mobile computing	• Physically securing personal electronic devices • Sending sensitive information via mobile networks • Checking work email via free network
Information handling	• Disposing of sensitive documents • Inserting DVDs/USB devices • Leaving sensitive material unsecured

`

Figure 6 - Focus Areas for ISA (Wahyudiwan, Suchayo and Gandhi, 2017, p.655)

Lebek et al. (2014) recommends the use of Intended Behaviour (IB) scale rather than using the Actual Behaviour (AB) scale to assess security-complaint behaviour. He further added that it is important to recognise the factors that influence intended behaviour rather than measuring ISA to protect organisation against information breaches.

To practise safe cyber security practices, organisations should design security awareness programmes and cyber security training events to ensure employees are fully aware of safe practices when using computing technology. However, awareness on its own is just not enough, users should align their

behavioural actions. Therefore, it is useful if cyber security awareness measurement models can be used on employees to test their awareness level and to investigate whether their knowledge and awareness aligns with safe computing behaviour. Ögütçü et al. (2016) created a framework (questionnaire) with the aim to assess the relationship between people's risk perception and behaviour using four independent scales which were Risky Behaviour Scale (RBS), Conservative Behaviour Scale, Exposure to Offence Scale (EoS) and Risk Perception Scale (RPS). One of the significant findings from the study is to do with survey participants' education level and information security training. It is reported that that participants with better education level and those who had information security training were more security aware than others. These findings complement Aloul et al (2013) phishing experiment to measure ISA. Although the model has been found useful in measuring ISA, Parsons, Calic, Pattinson et al. (2017) criticises the model for not having a holistic measurement for all aspects of awareness and behaviour and makes further comments that it is still at early stages of development with minimal assessment on validity and reliability.

Parsons et al. (2017) takes a different approach with a framework called the Human Aspect of Information Security (HAIS) model where he uses a Knowledge Attitude and Behaviour (KAB) model and a follow-up phishing experiment to measure ISA. Through evidence it is reported that the framework can predict security behaviour and justifies why it is better than other measurements which deals with only certain aspects of ISA. There are other models of behaviours such as the Health Belief Model (Ng et al, 2009) that relate to ISA but these models only explain some aspects of ISA. It does not provide an all-inclusive view of security awareness as the one Parsons et al. offers that has been tested rigorously with diverse populations and has proved useful and reliable. One area which can be further exploited by this measure is personality traits (Sharma et al., 2015) which has influence on how humans adopt safe computing behaviour. The model is designed to be modular

therefore it is possible to use portion of the model if there is no requirement to use it fully.

Lastly, Kruger and Kearney (2006) measures the effectiveness of awareness campaigns in a mining company by a prototype model for ISA. Awareness campaigns are not just about bringing in technological defences, setting up security policies but ensuring users are aware of the risks associated with cyber security and also their roles to minimise risks of a breach. The model was brought in to measure the effectiveness of ISA campaigns used to enhance safe computing behaviour. The model looks at a common technique used in social psychology of how people think and behave and examines the knowledge, attitude and behaviour to measure ISA and to evaluate the effectiveness of awareness campaigns. To ensure awareness campaigns are successful in bringing change to cyber security awareness and behaviour in an organisation, it is important to ensure that the campaigns are bringing positive changes and the methods need to be reviewed regularly and measured for effectiveness.

This section looked at the innovative cyber measurement framework that the author has created for this research to address cyber security awareness in the R SIGNALS. A number of other models were also explored which academics have used in the past to measure ISA and address safe computing behaviour.

The following section will now look at the importance of cyber security awareness delivery methods and the reasons why it needs to be effective for increasing cyber security awareness and behaviour.

2.1.7 Common and Proven Cyber Awareness Delivery Methods

For small enterprises and organisations, it is easier to communicate direction, policies about information security from management to employees who work at ground level. However, for big organisations this can be challenging because employees can be in physically dispersed locations or there is minimal

opportunity for management to disseminate strategic information to the employees as there are no direct lines of communications between employees and management level (Solms and Solms, 2004). Lebek et al (2014) suggests information security policies, security training and awareness programs as non-technical measures to improve safe computing behaviour in an organisation. Deloitte (2012) recommends organisations must implement good cyber security frameworks which complies with International Security Standard (ISO) 27001 (Guidelines for Information Security) and the technical controls to protect against social engineering attacks, hacking, malware, spyware and unwanted softwares included in ISO 27032 (Guidelines for Cyber Security). The information from these standards must also be used when designing cyber awareness campaigns.

There are many proven methods of delivering cyber training and awareness. Training types can range from classroom based training to interactive games. Awareness can be promoted with the use of news bulletin, noticeboards, newspapers, emails, posters etc. Cone, Irvine and Thompson (2007) breaks down awareness and training into formal training sessions (instructor-led), passive computer based training or web-based training, strategic placement of awareness messages and interactive computer based training through use of virtual world scenarios including the human and the technical factors. Interactive games were proven to be effective due to the problem-solving approach the training exposs the trainees to. The virtual game-based training allowed participants to be part of role-based scenarios where they are decision makers in performing actions to complete information security objectives. Abawajy and Kim (2010) conducted research to find out the most effective ISA training delivery methods amongst text-based, game-based and video presentation. Their research concluded that combined method was the most effect out of all. Similarly, Abawajy (2014) breaks security awareness training into three areas; web-based training, contextual training and embedded training. In his study, again it was proven that combined training delivery methods was better than individual training methods. Many researchers have utilised Phishing to

increase ISA. Carver, Dodge Jr and Ferguson (2007) uses phishing for evaluating the effectiveness of security awareness program in the US Military Academy and finds it to be a useful training method for increasing awareness on cyber security.

Chen, Medlin and Shaw (2008) states that the effectiveness of information security training delivery methods depends on the cultural background as he found out that training program was more effective with the US students than with the Taiwanese although both groups had the same type of training. This means that when training program are designed it is important to consider the background of the people being trained. Korpela (2015) recommends the use of learning analytics, an area of data analytics to provide added value to the cyber awareness programs and potentially using data from firewall logs, learning management systems, awareness programs etc to design effective cyber security awareness delivery methods.

This section researched on the importance of cyber awareness training delivery methods and provided an overview of methods that have been proven effective in past research. The next section will look at capability maturity models that can be use to assess cyber security maturity states.

2.1.8 Cyber Security Capability Maturity Model

> *"A maturity model allows an organisation or industry to have its practices, processes, and methods evaluated against a clear set of artefacts that establish a benchmark. These artefacts typically represent best practice and may incorporate standards or other codes of practice that are important in a particular domain or discipline"* (Caralli and Butkovic, 2013, p.1).

One of the main objectives of this study is to evaluate cyber security maturity state of R SIGNALS and benchmark it using a Capability Maturity Model

(CMM). CMM were first developed to improve software development and management processes. The model can be applied to cyber security to continuously improve cyber security processes and practices. Hoang and Le (2007) carries out an investigative study into CMM and its application to cyber security and provides benefits of using the model. The first model developed by Humphrey's (1989, cited in Hoang and Le, 2007) was to improve quality of softwares and had five maturity levels as shown in Figure 7.

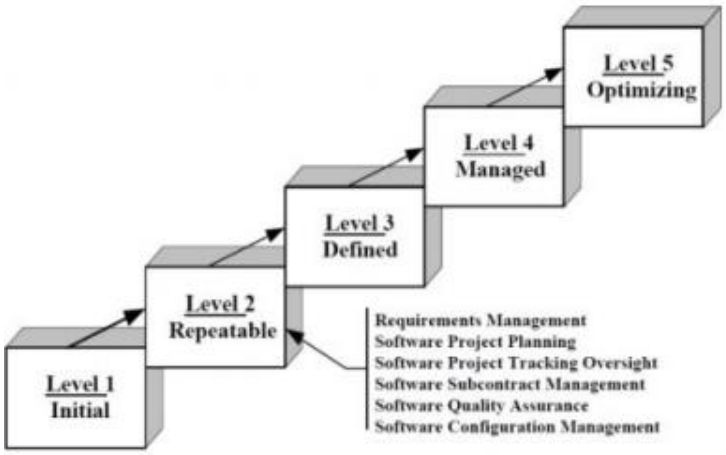


Figure 7 - Humphreys Capability Maturity Levels (1989, cited in Hoang and Le, 2007, p.4))

For each maturity level the software had to be of a certain quality and had to complete a set of designated practices. This was an evolutionary approach to software quality development and allowed benchmarking to the CMM levels. The model can be modified to represent cyber security capability maturity states for organisational performance on cyber security.

From the maturity model which Humphries first developed in 1989, there are numerous capability maturity models that are employed by organisations to improve their processes and practices for software development, knowledge management, data management, businesses or improving their IT risk management posture. There are very few that have been used assess the cyber security maturity of an organisation. In order to gauge an organisations' cyber security capability maturity it is important to consider how best to measure

the human organisational elements of cyber. The next section considers suitable measurements that already exists.

2.1.9 Measures and Metrics of Cyber Security Capability Maturity

Curtis and Mehravari (2015) examines two Cyber CMM used by the US Department of Energy (DoE) sector and highlights the benefits of using the models to improve cyber security capabilities and promoting safe practices. The model used for the electricity sector uses three maturity levels (Initiated, Performed and Managed) to assess maturity state as shown in Figure 8. The model was split into ten domains and to reach a maturity level, a number of cyber security practices had to be completed for each domain.

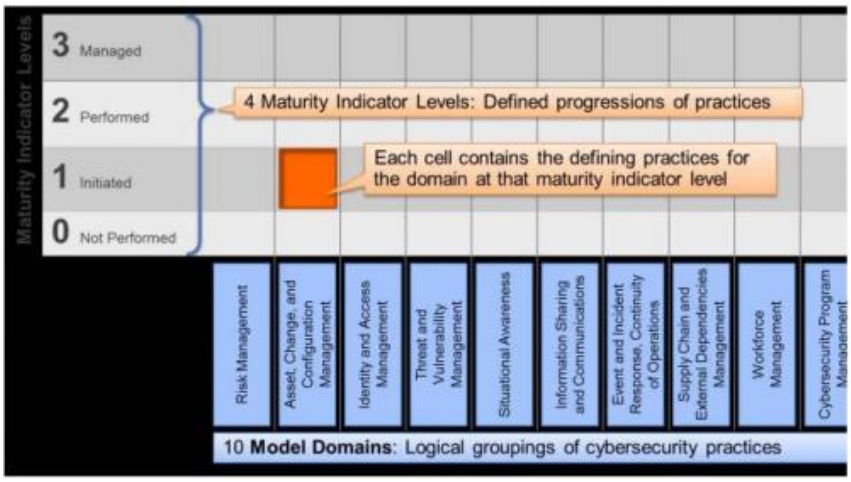


Figure 8 - Cyber CMM Model for US Electricity Sector (Curtisand Mehravari, 2015, p.4)

Another model developed by White (2011) is called the ‘Community Cyber Security Capability Maturity Model (CCSCMM) which is used a ‘yardstick’ for developing cyber security programs for communities. The yardstick is based on three mechanisms; establishing the current maturity state, a strategy to improve the maturity state and then a plan to share experiences and lessons learnt with other communities. His model is shown in Figure 9. Each level of the CCSCMM requires completing a pre-determined cyber security practices before progressing to the next level.

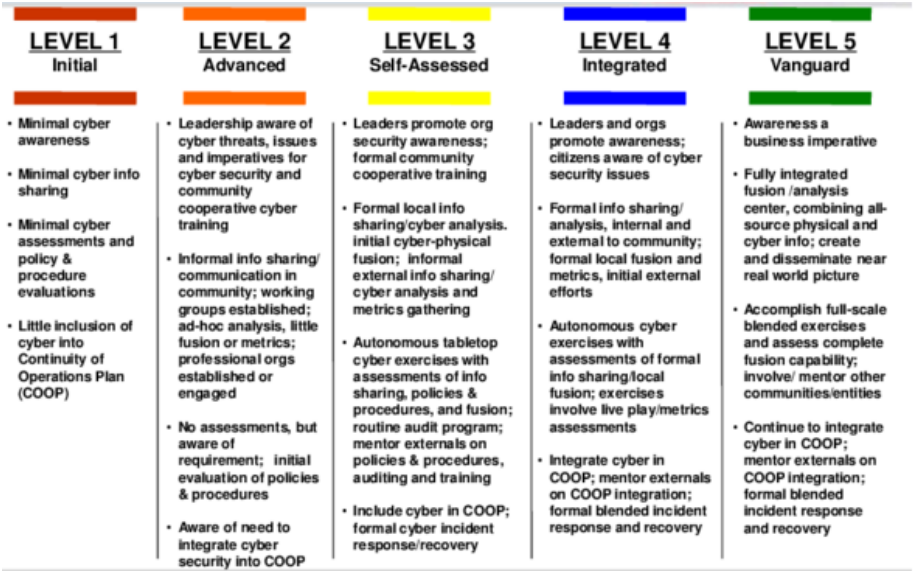


Figure 9 - Community Cyber Security Maturity Model (White, 2011, p175)

For an organisation to be have the defensive measure against cyber threats and vulnerabilities, it is important to ensure the cyber security posture is in place and process for improvements are highlighted. Maturity models helps benchmark current level of maturity in a particular discipline and also help clarify what needs improving to progress onto the next maturity level.

Barclay (2014) in her study introduces another Cybersecurity Capability Maturity Model which includes six levels as shown in Figure 10. The model is designed to illustrate the level of readiness for any cyber security related threats and vulnerabilities. Each of the levels has different indicators which includes a number of practices that has to be achieved before progressing to the next maturity level.

INDICATORS	LEVEL 0 UNDEFINED	LEVEL 1 BASIC	LEVEL 2 INITIAL	LEVEL 3 DEFINED	LEVEL 4 DYNAMIC	LEVEL 5 OPTIMIZING
Attitude to threats & vulnerabilities	Largely ignorant	Basic awareness	Reactive	Reactive	Proactive	Highly proactive
Technological Development	Limited awareness and use	Basic use	Effective use	Effective use and application	Innovation	Pervasive innovation
Societal response	Limited levels of awareness and efficiency and largely inflexible	Low levels of awareness, low efficiency and inflexible	Medium levels of awareness, efficiency and flexibility	Medium to High levels of awareness, efficiency and flexibility	High levels of awareness, efficiency and flexibility	Pervasive levels of awareness, efficiency and flexibility
Technical measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Business measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Legal & Regulatory measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Operational measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures
Education/capability building measures	Undefined/ Limited	Unstructured ad-hoc measures	Unstructured Threat-based measures	Structured threat-based measures	Structured capability-based measures	Highly structured capability-based measures

Figure 10 - Cyber Capability Maturity Model (Barclay, 2014, p.7)

All capability models researched for this study have a similar method of capturing maturity state for improving business processes or cyber security capabilities. Therefore, organisations that want to adopt a model can use any of the models and modify to their own unique requirements. This research will be using White's (2011) model to reflect R SIGNALS' maturity state on user cyber security awareness and beahaviour.

In this section, a number of capability maturity models that have been used in the past have been explored and the benefits of using them explained. The next section will look at UK cyber strategy and how it relates to Defence.

2.1.10 UK and Defence Cyber Security Strategy

The UK Cyber Security Strategy (2011, p.11) refers to 'cyberspace' as "an interactive domain made up of digital networks that are used to store, modify and communicate information".

The National Security Strategy (2016) indicate ICT has evolved and is in every aspect of our lives, technologies and geopolitical landscape has extended way beyond humans can imagine. As technology is developing malicious activities by criminals still continue to happen as cyberspace boundary increases with connection to nation's critical infrastructure such as power grids, air-traffic

control and traffic controls etc. Basic cyber hygiene amongst users in the cyberspace has to be effective so that threats are removed and risks reduced to as low as practicable (ALARP). “The future of the UK’s security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats, and equipped with the knowledge and capabilities required to maximise opportunities and manage risks” (National Cyber Security Strategy, 2016, p.9) .

The SDSR (2015) mentioned about addressing the risks and vulnerabilities posed by the cyberspace with an effective cyber security programme. For the military it is crucial that risks from cyberspace are mitigated and our systems, networks and infrastructure protected together with the confidentiality, integrity and availability of the data/information hosted in the cyberspace. Joint Force Cyber Group (JFCyG) was created in 2013 to deliver defence’s cyber capability (Defence Intranet, 2014) and staffed by Army, Navy and Airforce and civilians with various cyber skillsets in support of the national cyber activity (Air Cdr Brazier, 2014).

Both the Navy and Airforce have a cyber security strategy whereas the Army currently do not have one. The Airforce Cyber strategy was first implemented in 2014 through RAF cyber programme and simplified trifold was created and distributed to every organisation with the view of raising cyber security awareness. The strategy includes five strategic objectives which includes cyber awareness through training, education and career management.

Similarly, the Royal Navy has a cyber security strategy (2011) which outlines the vision into several high-level objectives which includes developing personnel and training to enhance cyber awareness, understanding risks and vulnerabilities of cyberspace and development of a defensive posture, cyber manoeuvrability and effect through doctrine and via ensuring cyber is integrated across naval service. “By 2020 The Royal Navy intends to be a cyber aware force which has the capability to operate in a contested cyberspace and maintain information superiority” (Royal Navy, 2011).

Like the Royal Air Force and the Royal Navy, there is a need for the Army to develop a cyber strategy to provide direction in the field of cyber and implementing cyber security program. This would be very useful to enhance the defensive posture and equally raise cyber security awareness and conduct training to avoid becoming a cause for cyber incidents to our detriment.

2.1.11 Research Context – The Royal Corps of Signals

> *"The R SIGNALS structure has been designed to provide a force that can deliver a robust, resilient and secure network of information services for the 21st century. This requires a range of new skills including expertise in software, data management and exploitation, and Cyber"* (ACIN 15/17, 2017*).*

R SIGNALS is an organisation within the Army which provides combat command support to deployable forces on operations or training exercises and are Army's battlefield communicators and information systems provider. "Everywhere the Army deploys – from special forces and intelligence gathering teams to personnel deployed in armoured vehicles, the R SIGNALS deploy*"* (R SIGNALSb, 2018). The organisation has been involved in every operations that the Army has taken part in providing satellite communications, voice and data networks and application services to deployed forces. R SIGNALS holds and manages state of the art technological equipment, systems and networks at home and in the deployed space which requires all users to be aware of the threats and vulnerabilities presented by the cyberspace.

There are currently 859 officers and 6723 soldiers in the R SIGNALS dispersed within units at different geographical locations in and outside of the UK. There are in total 6 trades for R SIGNALS soldiers which are listed as below:

a. Communication Logistic Specialist
b. Communication Systems Engineer
c. Communication Systems Operator
d. Electronic Warfare Systems Operator
e. Installation Technicians

f. R SIGNALS electricians

Soldiers go through their trade training in Blandford and get qualified to be employed in their role and upon finishing training they are posted to their working units. The trades that are more technical are communications systems engineer and communications systems operator as they need to have a good understanding of technologies and information systems. Hence, they are expected to be more cyber aware than the other trades due to the training and exposure they have with networks and systems compared to the other trade groups.

The officer cohort are made up of Late Entry (LE) Officers and Direct Entry (DE) officers. LE officers are ones who promote from the ranks and have mostly done full service as a soldier. LE officers generally fall into two categories; technical and non-technical. The technical officers are those who are in a technical trade-group by background and pursue their career either as a Telecommunications Officer Technical (TOT) or a Traffic Officer (Tfc Offr). These officers are more experienced in service and the technology that R SIGNALS employ in order to provide networks, infrastructure and services to the customers. The LE officers on non-technical posts are those who are in general administration, welfare, career management, logistic role etc. DE officers join the military directly as an officer and are in average young in service and experience and less exposed to the technologies that R SIGNALS use. DE officers are generally more educated than soldiers due to the education entry criteria to get selected as officers in the Army.

This context can be considered to be a priority for gauging cyber security in an Army context and could prove key to enabling Army to develop its own cyber security policies and practices. For instances, lapses in cyber security capability here could have wide ranging impact on MOD activities and goals worldwide. The combination of technical and non-technical roles, DE and LE officers may make R SIGNALS ideal for gauging Army specific demographics that effect the human elements of cyber security in various settings.

2.2 Summary

In this chapter a bounded literature review was conducted in cyber security awareness, measurement frameworks, behavioural models and cyber security maturity models. The literature review was an exploratory study to address the research aim and objectives and make comparison with the results obtained through a survey questionnaire which was designed by the author to measure cyber security awareness and behaviour. More details was provided on how the author constructed his own framework for measuring awareness and behaviour using NCSC's infographics on cyber security for small businesses.

To improve cyber security awareness in an organisation it is important to understand behavioural aspects of employees and what makes them adopt safe computing behaviour. Ultimately, employers must ensure awareness and intentions are translated into desired security behaviour. So cyber security awareness is not only to do with how much knowledge someone has with regards to the protective practices but about whether that knowledge is put into actions when required.

A number of frameworks were examined to investigate past measurement frameworks that have been used by academics to measure cyber security awareness. The most suitable one is from Parsons et al. (2017) which uses a questionnaire to measure knowledge, attitude and behaviour and has been rigorously tested for validity and reliability.

Cyber security capability maturity models were also examined to determine the most suitable to benchmark cyber maturity state in the R SIGNALS. A number of maturity models were explored and past research indicated that they are perfect medium to assess capability maturity state and has been used by different sectors of government in the US. White (2011) developed a cyber security maturity model which is most suitable to utilise for this study as it is simple to use and is flexible irrespective of the size of an organisation, community or state.

3 METHODOLOGY

Introduction

This section will include the research philosophies, methodology and methods adopted throughout the study and justify the research approach taken. This research is conducted to investigate how cyber awareness can be measured and mapped against a capability maturity model to provide recommendations for future cyber training in the R SIGNALS. The research is an adaptation and extension of the UK government National Cyber Security Centre (NCSC) infographic framework for cyber awareness which was used to develop a questionnaire with the aim of investigating cyber awareness and behaviour of the participants. The questionnaire has 59 items divided into demographics, awareness and behaviour specific questions broken down in six themes (Data Backup, Device Safety, Malware, Phishing, Passwords and Behaviour). This chapter will also define the rationale behind the methodological and philosophical choices for the study and explain how the research questions have been addressed.

3.1 Research Philosophy

> *"A methodology cannot be derived from research but instead has to be grounded in that form of a priori theoretical knowledge usually referred to as 'philosophy"* (Car, 2006).

When taking research studies, it is important to understand the philosophical stance and take the right approach to gather data for the research. The selection of correct philosophy is an important part of research methodology as it addresses the beliefs and assumptions that the author should consider when carrying out the study. This research follows the research onion (Saunders et al., 2009, p108) illustrated in Figure 11 and the philosophical layer is the outer layer which has to be addressed first. From then on, the inner layers will be peeled and examined to devise the best research approach for the thesis. For this study research philosophy will be positivist with a deductive approach.

Research strategy will include an online survey using a set of quantitative questions. Time horizon will be cross-sectional and data collection methods will be through an online questionnaire distributed to the sample population.

“The research philosophy you adopt contains important assumptions and beliefs about the way in which you view the world. These assumptions will underpin your research strategy and the methods you choose as part of that strategy” (Saunders et al, 2009, p108). Choosing the correct philosophical approach allows the author to lead into adopting the right methodology for the research and help into formulating a research strategy that is relevant to the development of the knowledge for the study and answering the research questions.

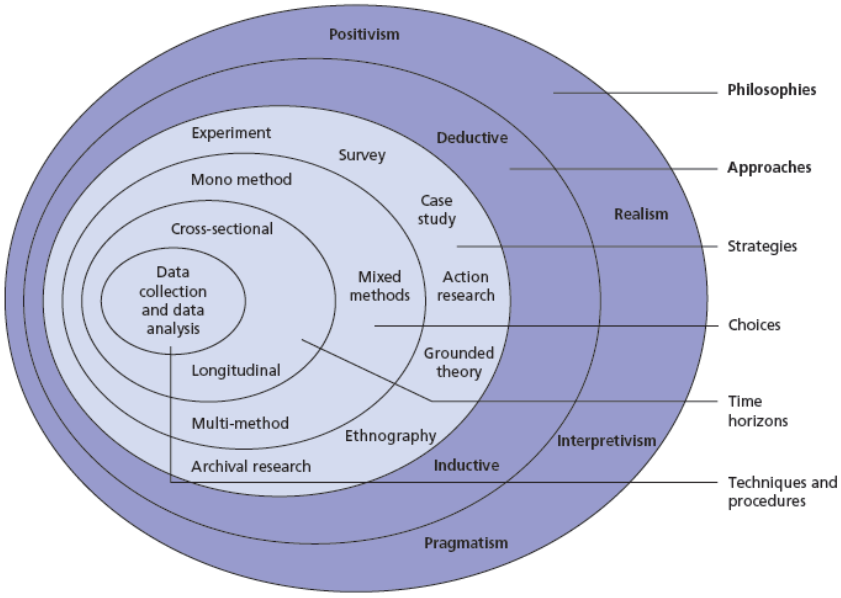


Figure 11 - Research Onion (Saunders, Lewis and Thornhill, 2009)

“In research it is important to identify the philosophical and theoretical assumptions that lead to the choice of appropriate methodology” (Dobson, 2001, p200). Before selecting what methodology to use, it is also important to understand the philosophical stance for the research. Both ontological and epistemological positions for the research has been analysed to enable the author to select the right methodology. “Philosophy is generally concerned with three basic issues; being (ontology), knowing (epistemology) and acting

(axiology)" (Denzin and Lincoln 2000). The ontological position in a research allows the researcher to understand the reality in the world about the knowledge we know and what is true, epistemological position provides a perspective of what we think is true and how we know about it and axiological position explains what is beneficial about the research and how we should act. The justification of choosing a certain methodology can be supported and informed by the philosophical position adopted for the research. Lynham and Ruona (2004, p155) explains the three components of philosophy as illustrated in Figure 12 as a framework for congruent and coherent system of thought and action. The interconnected components as part of the philosophical framework allows us to realise how we think and see the world. Saunders et al. (2009, p108) recommends not to make a judgement that one research philosophy is superior than another as it depends what the research is about and what kind of knowledge is being developed through the research questions.

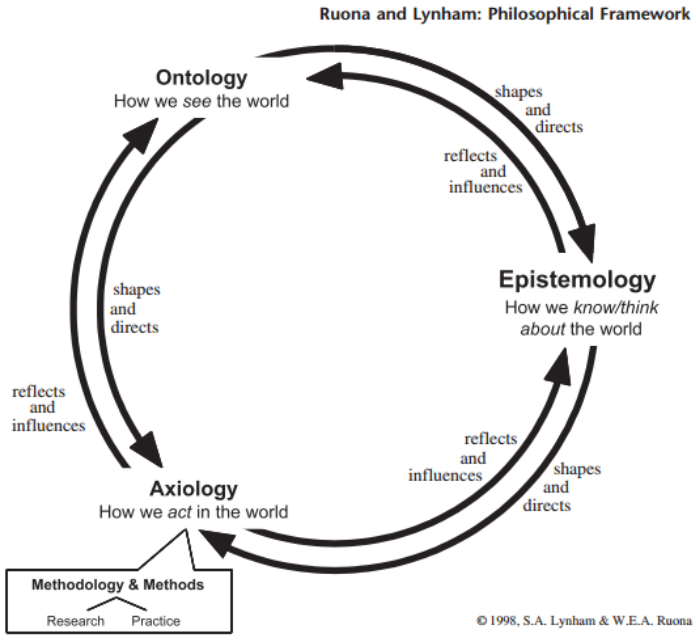


Figure 1 A philosophical framework for thought and practice

Figure 12 - A Philosophical Framework for Thought and Practice (Lynham and Ruona, 2014, p155)

The reason for taking ontological approach is because the research will be conducted based on how the researcher view the reality of cyber security awareness and the knowledge that exists about the research question. In

addition to this, it is about discovering knowledge that is unknown and external to the researcher.

Looking at the Layer 1 of the research onion illustrated in Figure 11, there are a number of philosophical stances that can be examined to find out which best fits the criteria to answer the research questions. This research will follow a positivist approach and use quantitative technique for data collection from soldiers and officers from the R SIGNALS. From the results a deductive approach will be used for generalisation. The role of the researcher will be neutral on this study and research of this nature is high in reliability which means it can produce accurate replicable measurements and represent the population but it is not good for validity. Reliable means replicable measurements and validity alludes to inductive insights. The research is not creating a theory although is supported by an academic narrative backing in the literature review. The approach will be to measure and analyse cyber security awareness and behaviour and its implications within R SIGNALS.

Positivist research approach is ideal for social research and generates statistics as evidence to support the study. It is scientific in nature and looks at the hard facts with an objective view to a problem. In the context of this research, a positivist approach will be ideal for efficient and effective data collection through a utility of an online survey questionnaire using Qualtrics to assess cyber security awareness and behaviour of officers and soldiers in the R SIGNALS. It will also provide data which can be used to provide statistics and as evidence in this research. However, Veiga (2016) states that although survey questionnaires provide precise and accurate measures there might be instances when survey participants may find questions ambiguous and the cyber security awareness background may not be the same for all. Hence, an interpretivist approach i.e. a qualitative method may be useful to prod and obtain more information on the results provided by the questionnaire. This study is an exploratory application of a deductive approach taking into account a positivist philosophical approach as it will enable the results from the statistical analysis to be compared with the outcome from the literature review. The

framework developed from the government cyber awareness infographics and theoretical position from the literature review will be utilized by adopting a deductive approach to test against the data obtained from the survey questionnaire. Saunders et al. (2009) mentions that a survey strategy is usually associated with the deductive approach and provides an easy way to collect data from a sizeable population without much hassle. The survey strategy will also allow to capture opinions, behaviour and attributes of the population in terms of the research questions. A number of hypothesis will be tested on the quantitative data collected from the questionnaire.

3.2 Participants

3.2.1 Sampling Strategy

To capture the right data for the research it is important to select appropriate samples to ensure generalisation can be made from the results obtained from the survey. Generalisation, which is an act of reasoning from which inferences can be made from observations, is widely-acknowledged as a quality standard in quantitative research, but is more controversial in qualitative research (Beck and Polit, 2010). According to Saunders et al. (2009) sampling techniques provide a range of methods which allows considering data from a sub-group than an entire population. This enables reduction of data required to be collected for the research but is good enough to make inferences about the population. For this research, it was not possible to capture all members of R SIGNALS in the survey given the dispersed nature of geographical locations of units and the officers and soldiers. Not only this, the time allocated for the dissertation was not enough to capture every single member of the organisation. Therefore, it was decided that a sample of the population would be chosen to take part in the survey questionnaire. Initially, the intention was to include soldiers and officers from 16 Signal Regiment; the author's home Regiment. However, it was deemed that the number of participants for the survey would not be enough, hence the survey was pushed out to other R SIGNALS units. Figure 13 illustrates what sample and individual elements mean in a population under research.

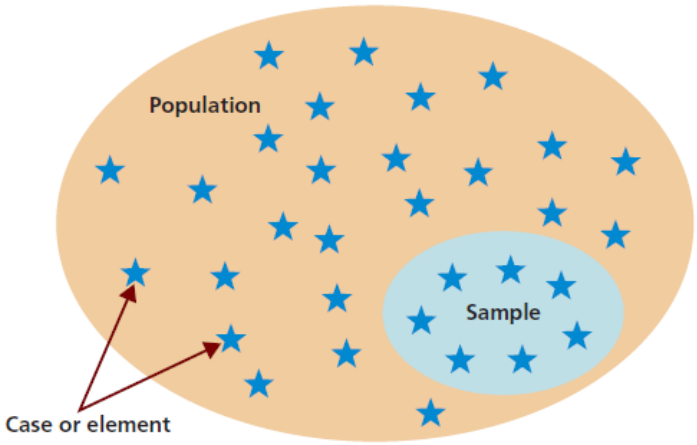


Figure 13 - Population, Sample and Individual cases (Saunders et al., 2009, p211)

Maxwell and Delaney (2004) mentions the importance of sample size and how it affects statistical significance with larger samples producing stable statistics and reduced sampling error. Saunders et al. (2009) divides sampling techniques into two types which are as follows:

a. Probability or representative sampling
b. Non-probability or judgmental sampling

Probability sampling is highly suitable for quantitative research where inferences can be made about the population through statistical measurements. In this type of sampling design everyone in the population has an equal probability for being selected in the sample and is considered to be highly representive of the overall population. It was considered that probability sampling would be possible for this research as it was considered achievable to provide a sample population from the R SIGNALS to be included in the survey. In non-probability sampling each unit in the population do not have a specific probability of getting selected as a sample hence this type of sampling technique can be non-representative of the population albeit some generalisation can be made. The technique used for this research will include probability sampling as there will be a need to answer the research question and address the objectives using statistical analysis from the survey. Although it is impossible to capture every single serving soldiers and officers from the R SIGNALS, the sample selected is relevant to the research questions and

objectives. Newman (2014) states that a properly conducted probability sampling will be economical for gathering data on an entire population. According to Saunders et al. (2009) probability sampling is divided into four stages which includes deciding on the sampling frame, sample size, selection of sampling technique and ensuring sample represents the population under study.

The manning figures (Army Personnel Centre, 2018) reported the total population in the R SIGNALS as 7582 of which 6723 are soldiers and 859 officers. The percentage breakdown is approximately 88% soldiers and 12% officers and are employed in different units within R SIGNALS or attached to other organisations. The targeted population frame used will be 7582 for this research. Once the sampling frame is obtained, it is important to decide on the appropriate sample size as this will be crucial in the generalisation that will be made to address the research questions from the data collected. Saunders et al. (2009, p218) states that “statisticians have shown that a sample size of 30 or more will usually result in a sampling distribution for the mean that is very close to normal distribution”. The size of the sample must be representative of the population under research which will boost confidence on the data collected. Figure 14 (Saunders et al., 2009) provides the formula for calculating the minimum sample size. Once the minimum sample size is calculated then adjusted minimum sample size using the formula in Figure 15 can be calculated as the total population is less than 10,000.

$$n = p\% \times q\% \times \left[\frac{z}{e\%}\right]^2$$

where
n is the minimum sample size required
$p\%$ is the proportion belonging to the specified category
$q\%$ is the proportion not belonging to the specified category
z is the z value corresponding to the level of confidence required
$e\%$is the margin of error required.

Level of confidence	z value
90% certain	1.65
95% certain	1.96
99% certain	2.57

Figure 14 - Calculating Minimum Sample Size (Saunders et al., 2009, p581)

$$n' = \frac{n}{1 + \left(\frac{n}{N}\right)}$$

where
n' is the adjusted minimum sample size
n is the minimum sample size (as calculated above)
N is the total population.

Figure 15 - Adjusted Minimum Sample Size (Saunders et al., 2009, p582)

3.2.1.1 Minimum Sample Size

Using the formula in Figure 14, the minimum sample size is as follows:

p% = 88 (percentage of soldiers)

q% = 12 (percentage of officers)

z = 1.96

e% = 5 (margin of error %)

Minimum Sample Size (n) = 88 x 12 x $\left(\frac{1.96}{5}\right)^2$ = 162.62

3.2.1.2 Adjusted Minimum Sample Size

Now using formula in Figure 15, the adjusted minimum sample size is as follows:

n = minimum sample size = 162.62

N = Total population = 7582

Adjusted minimum Sample Size (n') = 159.28

3.2.2 Sample Selection

Once the minimum sample size was calculated it was important to ensure the representation of soldiers and officers in the sample correlated with the percentage difference between the two in the total population. To get 100% accuracy would be impossible given the scope and timeframe of the MSc thesis, however the split of samples that took part in the survey was approximately 70% soldiers and 30% officers. This was deemed reasonable to start with the data collection. As it was not possible to get the required sample from the author's home regiment, the invitation to take part in the survey questionnaire was extended to other regiments and puddles of R SIGNALS personnel present in other organisations. These were additional efforts to achieve a representative sample using multiple participation routes. There was no requirement to have a split of gender in the sample selected. The invitation to take part in the survey took place using two approaches. First approach was asking the Commanding Officers of each Regiment to grant permission to roll out the survey in his/her unit. The second approach was by using Whatsapp or Mobile Phone messaging to send the survey link to subjects who the author knew personally. These approaches allowed the author to contact enough participants to take part in the survey questionnaire.

The online survey was created with the intent to measure cyber security awareness and understand cyber security behaviour of R SIGNALS personnel. It is important to understand the demographics and characteristics of the respondents taking part in the survey. Hence the survey included a number of

demographic questions that would later on assist with identifying bias in answers presented by the respondents. Demographics information for this survey included age, gender, rank, officer or soldier, length of time served, trade, cyber training and level of education. The demographics information will be used to test the hypothesis presented for the research and investigate differences in responses from respondents from different background. The research was conducted on military personnel and did not include MOD employed civilians.

3.2.3 Design and Materials

The survey questionnaire was created with an online software tool called Qualtrics available through Cranfield University. Qualtrics is a data collection platform which is easy to use and is mobile device friendly which meant that participants could access the survey from anywhere from any device with a connection to internet. The tool not only provided means for creating a questionnaire but had the features to provide basic analysis of data and exporting data to be analysed by rigorous software tools. Zhou, Zhou, Chen et al. (2017, p.710) states that “online surveys can establish asynchronous contacts with respondents on the move, achieve faster, simpler and cheaper surveys, improve the quality of survey responses”. For this research the data collection technique had to be in the form of an online survey questionnaire to capture the information required with the constraints imposed by the time available to complete the dissertation and the number of participants that was required. Traditional paper survey was considered but this would bring the challenge of keeping the survey anonymous and also getting hold of the required number of intended participants resulting in lower survey completion rates.

3.2.4 Questionnaire Design

The survey design incorporated traditional survey principles and adopted the Likert scale questionnaire first developed in the 1930s to capture the quantitative data from the respondents. An example Likert scale used is illustrated in Figure 16.

Response Set	Strongly Disagree (1)	Disagree (2)	Neither agree Nor disagree (3)	Agree (4)	Strongly Agree (5)
You should always backup your work and personal files	[ ]	[ ]	[ ]	[ ]	[ ]

Figure 16 - Example Likert Scale on Agreement

When the questions were originally designed four types of Likert scale was adopted (importance, frequency, awareness, agreement) however, this was reduced down to two 5-point Likert scales (frequency and awareness) due to problems it may create during data analysis phase and having to analyse each type of Likert scales separately. Furthermore, the reduction of Likert scale types was to potentially combine items in a meaningful way that might show systematic variation in either Frequency of behaviour or Awareness of the participants.

The questions in the themes were designed to capture cyber security behaviour and cyber security awareness amongst survey participants. “Likert scales provide an ordinal-level measure of a person’s attitude and are often called summated-rating or additive scales as a participant’s score is calculated by summing the number of responses they give” (Neuman, 2014, p230). The questions design was intended such that they were unambiguous, short and concise to make it more appealing to participate for the respondents. A full copy of the questionnaire is attached in Appendix B. Some example items include:

Response Set (Frequency)	Never (1)	Rarely (2)	Sometimes (3)	Often (4)	Always (5)
How often do you send files via email using cloud storage?	[ ]	[ ]	[ ]	[ ]	[ ]

Response Set (Awareness)	Not at all aware (1)	Slightly Aware (2)	Moderately Aware (3)	Very Aware (4)	Extremely Aware (5)
Are you aware phishing attacks are conducted using fake emails and links to redundant websites and carried out by asking for sensitive information?	[ ]	[ ]	[ ]	[ ]	[ ]

It was important to create a front page in the questionnaire to ensure participants were aware of the type of survey that they were taking part in and

to obtain consent before proceeding with the participation in the survey. This part also explained about the anonymity of the survey and how all data would be stored securely and held in strict confidence. Following on from this was the information on the background or demographics of the participants. This was very important to ensure the sample contained right percentage breakdown of officers and soldiers in the R SIGNALS. Further information on officers and soldiers also had to be extrapolated from the questionnaire to spot any linkage or relation between cyber awareness/behaviour and demographics such as cyber education, time served in the military, age group, rank range, trade and level of education for the participants. This information would later be used to test a number of hypothesis created for the research.

The remainder of the questionnaire was based on 6 themes of cyber security awareness and cyber behaviour. The themes are as follows:

a. **Data Backup**. This is important to ensure data can be restored if it is destroyed through natural calamities or stolen by hackers.

b. **Device Safety**. Protecting personal devices and office computers from malicious users by keeping it safe using security features available and not sending sensitive information using public WiFi hotspots.

c. **Malware**. Protection against malicious software using anti-virus and simple techniques such as keeping the computers and personal devices up to date.

d. **Phishing**. Avoidance from phishing attacks by recognising signs of rogue emails and links.

e. **Passwords**. Protection of personal and official data through use of secure passwords.

f. **Behaviour**. Expected cyber behaviour to protect and prevent malicious attacks to personal and office devices and networks.

The themes were extracted from the government infographics on cyber security practices for small sized businesses. The questions related to either personal,

or work use, and occasional combined use of information technologies by soldiers and officers from the R SIGNALS to ascertain all areas were captured. For each item, the target (personal, work, both) was explicitly stated in the questionnaire. The original question set for the survey had four type of Likert scales (as shown in Table 3) for the 6 themes of cyber security awareness and behaviour. Upon further consideration of data analytics this was reduced to just frequency and awareness (as shown in Table 4) (as it was highlighted that having a lot of Likert scales would introduce issues during data analysis phase).

Table 3 - Initial Questions Design using 4 Likert Scale Types

	Theme 1 – Backup	Theme 2– Device Safety	Theme 3 – Malware	Theme 4 – Phishing	Theme 5 – Passwords	Theme 6 - Behaviours
Importance	1	1	2	1	1	
Frequency	2	3	3	2	3	3
Awareness	1	3	3	2	1	
Agreement				1		3
Total Items	4	7	8	6	5	6

Table 4 -Question Design with 2 Likert Scale Types

	Theme 1 – Backup	Theme 2– Device Safety	Theme 3 – Malware	Theme 4 – Phishing	Theme 5 – Passwords	Theme 6 - Behaviours
Frequency	3	3	5	4	4	7
Awareness	3	5	4	5	4	
Total Items	6	8	9	9	8	7

Once the questions were designed with the two Likert scale response types, it was necessary that some questions required reverse coding to avoid ‘response sets’. Neuman (2014, p232) defines response set as “a tendency to agree with every question in a series rather than carefully thinking through one’s answer to

each". One example of reverse coding was for the question 'Do you leave your personal devices unattended when you are in public places' with the response scale including never, rarely, sometimes, often and always. This question was reverse coded to 'Do you have your personal devices attended when you are in public places'. By switching the polarity of the question, this would avoid response sets from participants.

In addition to this, the question randomisation feature in Qualtrics was utilised to randomise the presentation order of the two Likert scale type questions. This would mitigate against response sets and still output the data in the order the questions were entered into Qualtrics. It also helps spread the risk of any disengagement and fatigue towards the end of the participation being spread across the items presented rather than unduly degrading consideration of items at the end of a scale. The survey was open for 30 days to ensure enough time was available to collect data from the sample selected.

3.2.5 Pilot Survey

Once the online survey questionnaire was ready, it was deemed necessary to pilot the survey. Saunders et al. (2009) highlights the importance of the pilot in order to further improve the questionnaire so that respondents will have no issues answering the questions and there are no problems with recoding the data. The piloting process did not check the validity and reliability of the data collected. Once the survey questionnaire was ready for pilot this was distributed to some work colleagues and to the project supervisor. The link to the Qualtrics Survey questionnaire was sent to the pilot team to check for suitability of questions, length of time to take the survey and provide feedback on the survey. It was also to ensure questions in the survey items were unambiguous and layout was clear and appealing for the participants. All the colleagues who were part of the pilot were military and due to their trade had basic knowledge of cyber security awareness and the practices although the pilot could have included people without cyber security background due to the simple nature of the questions in the survey.

Feedback from the pilot on the length of time to complete the survey was between 12 – 15 mins which was considered to be reasonable for the survey. There were no other comments made on the pilot by the author's work colleagues who generally gave a good review about the questionnaire. The dissertation tutor advised reverse coding on few more questions. This was implemented by making changes to a number of questions in order to avoid bias in responses.

3.2.6 Procedure

The sample required for the survey was chosen from different R SIGNALS units. This included soldiers and officers from a number of Regiments by explicitly asking permission from their commanding officers to go ahead with the survey. A link to the survey was sent to the commanding officers stating the need and importance of the research and explaining the potential benefits of future cyber security training recommendations. Soldiers and officers of R SIGNALS were considered to be the right population to take part in the survey as they operate IT equipment daily and is business as usual. The exposure to the state of the art technology equipment and systems makes them vulnerable to cyber-attack from the adversaries. Hence cyber security awareness is crucial in this organisation. Although, it was not possible to reach all the population in the R SIGNALS, best effort was used to reach out to maximum number of officers and soldiers to take part in the survey. The adjusted sample size calculated was 160, only 118 soldiers and officers took part in the survey before it was closed after 30 days. So, the response rate was approximately 73%.

3.2.7 Ethics

The ethical considerations and approach taken for this research is based on the Cranfield University Research Ethics System (CURES). Throughout this study, the research complied with the code of conduct set up by the CURES Ethics committee. The research was graded 2b and risks associated with it was classed as being low. Email confirmation with regards to CURES approval for the study is attached at Appendix C.

The study was designed with full consideration to ethics and protection and welfare of the research participants. The research was conducted with diligence and avoided causing any harm, discomfort and invasion of privacy of the participants. All those taking part in the data collection process had to provide an informed consent before proceeding with the survey and had the right to withdraw at any time. Personal details such as names, Army number, unit address were excluded from the research to maintain anonymity and confidentiality of participants' details in the research outputs. The purpose and potential benefits of the study were also explained to the participants prior to partaking in the survey. All the data collected from this research will be treated strictly in confidence as per the Data Protection Act 1988.

4 RESULTS

Introduction

This chapter will provide results from the survey conducted using Qualtrics online survey software tool on cyber security awareness and behaviour of soldiers and officers from R SIGNALS. The first part of the questionnaire included a consent form for taking part in the survey followed by questions on demographics. The remaining part was to do with cyber security awareness and behaviour related questions. The results will be presented using graphs and tables and will include explanation of the data collected. The subsequent chapters will include detailed analysis and interpretation in conjunction with comparative view of the results in light of the literature review and research questions.

4.1 Quantitative Data Treatment

In total 118 participants took part in the survey of which 14 participants had significant data missing hence they were ignored for the research analytics. Therefore, the actual sample size for the research was 104. The sample size of 104 included 70 soldiers and 34 officers. The officers were further categorised into 18 DE officers and 16 LE officers. LE officers are those who commission from the ranks having spent a lot of years and experience in service. DE officers are those who join the military directly as an officer through Sandhurst selection and start from the rank of Second Lieutenant and tend to be young in age and inexperienced compared to LE officers.

It was considered important to categorise the sample in terms of their trades. Although all the participants were from R SIGNALS and are professional communicators in the British Army, the difference in trade means that some are likely to be more cyber aware than others. For example, a soldier who is communication system engineer by trade would be more familiar with the technical and cyber security aspects of information systems and technologies than a communication systems operator who most of the time is trained in the operation of the equipment. Similarly, and in most cases LE officers are expected to have more experience and knowledge on cyber security than young DE officers. The next category was about cyber security training. From the results it was identified that 65.4% of respondents had cyber security training whereas the remainder 34.6% responded ‘no’ to the question. The question initially intended to capture the time scales of training but further inspection of the results meant that it was not statistically viable and therefore, responses were classed as a ‘yes’ or ‘no’. People who have had cyber training were expected to be more cyber aware than those who didn’t.

Another category from the demographics was to do with level of education of the participants. One respondent detailed a MSc which was re-categorised to ‘Postgraduate education’. Five ‘other’ responses were deleted as these were considered as not interpretable for the results. Some reverse scoring work had to be carried out for questions that were negatively worded to ensure

appropriate scoring. In total, there were 12 items that were reverse scored of which 11 were to do with frequency behaviours and one was to do with reported satisfaction with training.

4.1.1 Cronbach's Reliability of (Sub)Scales

Cronbach's alpha is a psychometric statistic that was introduced by Cronbach in 1952.

> *"Cronbach's alpha is a statistic that measures the internal consistency among a set of survey items that (a) a researcher believes all measure the same construct, (b) are therefore correlated with each other, and (c) thus could be formed into some type of scale. It belongs to a wide range of reliability measures"* (Trobia, 2017, p2).

The questionnaire uses two Likert type scales (awareness, frequency) and multiple items with the intention to measure cyber security awareness and frequency of behaviour of participants in the survey sample. Cronbach's alpha helps measure the internal consistency i.e. reliability of the survey items. Equation 1 shows the formula for calculating Cronbach's alpha where n represents number of items and $\bar{r}$ represents the intercorrelation between items:

$$\alpha = \frac{n\bar{r}}{1+\bar{r}(n-1)},$$

Equation 1 - Cronbach Alpha Formula (Trobia, 2017)

Table 5 shows the reliability criteria for Cronbach's alpha.

Table 5 - Reliability Criteria using SPSS Software (SPSS, 2018)

Cronbach's Alpha	Internal Consistency
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	Good

0.8 > α ≥ 0.7	Acceptable
0.7 > α ≥ 0.6	Questionable
0.6 > α ≥ 0.5	Poor

The survey participants data from Qualtrics was exported into Microsoft Excel and then imported in Statistical Package for the Social Sciences (SPSS). This was to calculate the Cronbach's alpha based on the themes for the question with the Likert scales used. Each theme included composite item made of several questions. The Cronbach's alpha values calculated from SPSS for the two type of Likert scales and themes are included in Table 6.

Table 6 - Cronbach's Alpha Results

THEME Likert scale	**Back-up behaviour**	**Device Safety**	**Malware**	**Phishing**	**Passwords**	**Behaviours**	**Total**
Frequency	α = .51	α = .40	α = -.13	α = -.53	α = .49	α = .51	α = .78
Awareness	α = .77	α = .87	α = .89	α = .83	α = .79	n/a	n/a

For the Frequency Likert scale, many of the themes did not reach an acceptable level of Cronbach's alpha. According to Trobia (2017, p3), negative Cronbach's alpha is statistically possible but meaningless in respects to interpretation and could be due to the orientation of items being scaled. This would mean poor correlation between items. However, the Cronbach's alpha in totality for the whole frequency was 0.78 which is good according to the reliability criteria Table 5.

For awareness Likert scale, all the composite items in the themes had a Cronbach alpha of 0.7 or more hence was considered reliable for the research. It meant that the results would be acceptable to consider reliable.

4.2 Descriptive Results

4.2.1 Sample Characteristics

The next set of results included details on the sample characteristics. Figure 17 illustrates the age group breakdown of officers and soldiers who took part in the

survey. It was necessary to capture the age group to investigate whether cyber security awareness has any relationship with age. Details on gender was also captured but as there were only 10% females and it was considered any observations made with regards to females would not be valid.

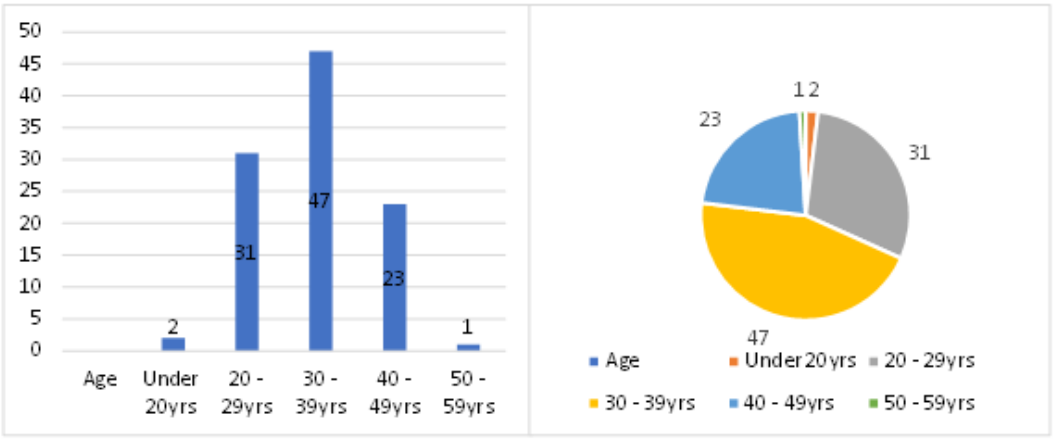


Figure 17 - Sample Age Group

Figure 18 illustrates the breakdown of officer vs soldiers who took part in the survey. The data could later to utilised to highlight any difference in cyber security awareness between officers and soldiers.

Out of 104 participants 70 were soldiers and 34 were officers. For soldiers and LE officers it can be assumed that with rank comes more experience and exposure to IT equipment hence will probably be more aware of cyber security risks and vulnerabilities. This would also apply to DE officers in some cases particularly who are in technical posts within R SIGNALS.

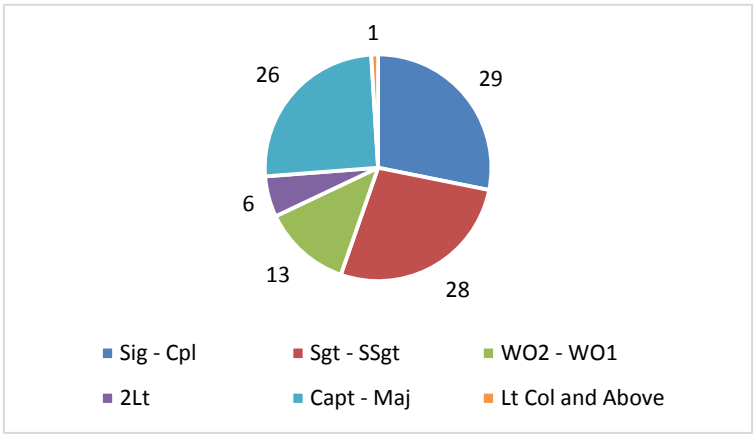


Figure 18 - Sample Breakdown of Ranks

Figure 19 shows the length of time-served in the R SIGNALS for the participants. The organisation's role is to provide communication systems and networks to deployed forces whilst out on operations or for training support activities. The longer the time served, soldiers and officers are expected to be more experienced and knowledgeable with technologies that we hold in the corps, through training and operation of IT equipment. Participants who have served longer and have more experience with IT equipment are expected to have better cyber awareness.

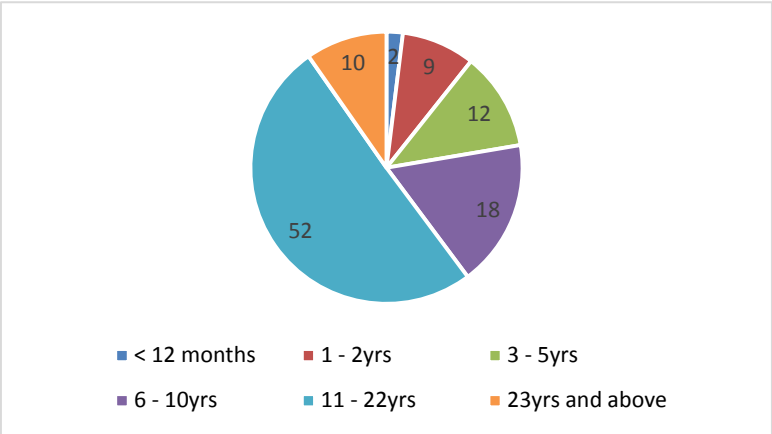


Figure 19 - Length of Time Served of Participants

Figure 20 illustrates the trade breakdown for soldiers and officers. The trade defines what role soldiers and officers have for their daily business within R SIGNALS. After joining the R SIGNALS soldiers will go through their trade training. The length of time for trade training is different for a communication systems engineer and communication systems operator as the former training is much more technical and detailed than the latter. Soldiers and LE officers in trade are expected to have a much better understanding of technologies than DE officers who are on regimental duties in the R SIGNALS. It is expected that technical trades will have influence in the understanding and awareness of cyber security.

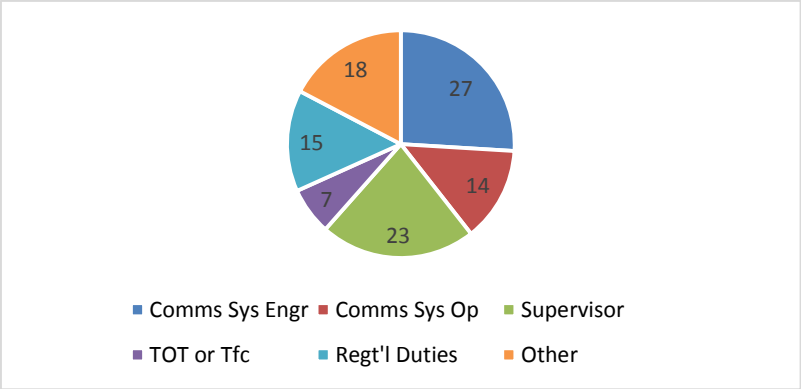


Figure 20 - Trade Breakdown of Participants

Figure 21 shows the breakdown of participants against Cyber Training. Only 36 out of 104 had gone through some form of Cyber Training. The remainder 68 reported they did not have any training. This can have an impact on the results of this survey as it can be expected that more participants will be less cyber aware and perform poorly when responding to the questionnaire.

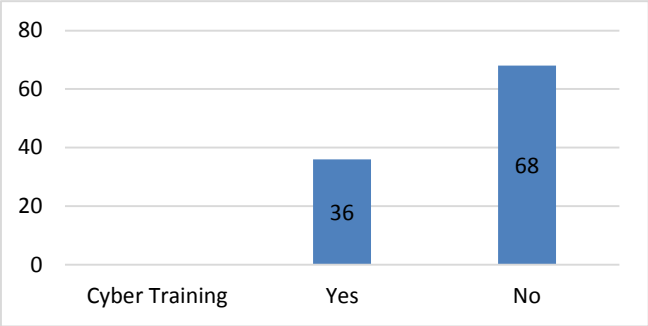


Figure 21 - Cyber Training Breakdown

Figure 22 shows the level of education amongst participants. The figures illustrate that majority of the participants have a foundation degree or above which means that the sample selected are fairly educated. The level of education may have a correlation to the cyber awareness scale and how they behave in terms of becoming ‘cyber safe’ when operating computers and personal devices whether at work or at home.

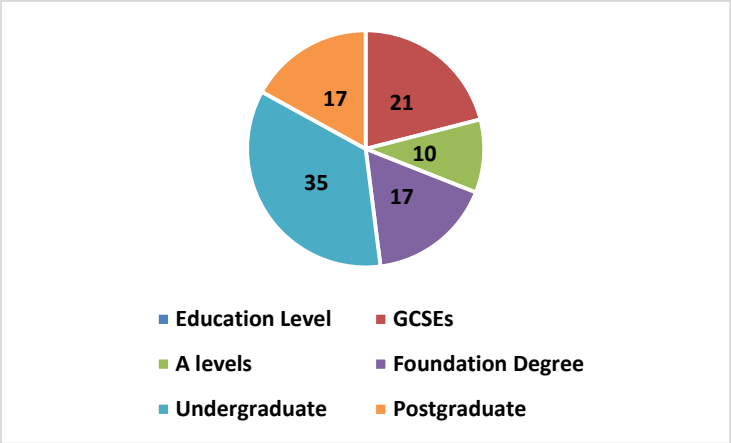


Figure 22 - Participants Education Level

4.2.2 Pearson's Correlation

Table 7 shows the intercorrelation information and linear relationship between variables which was extracted using the SPSS software. The correlation between variables is represented by Pearson's 'r' value which ranges from -1 to +1.

Table 7 - Pearson's Intercorrelation

	Variables	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Age														
2	Gender	.04													
3	Soldier/Officer	**.29****	.19												
4	Rank range	**.50****	.18	**.91****											
5	Time in R SIGS	**.69****	.07	.06	**.33****										
6	Trade	**.24***	.11	**.73****	**.74****	.05									
7	Cyber training	**.22***	.10	.02	.08	**.21***	.06								
8	Education	**.35****	.09	**.42****	**.57****	**.24***	**.44****	**.20***							
9	FREQUENCY	.19	-.02	.02	.60	.04	-.12	**.27****	.04						
10	Back-up behaviour (awareness)	.19	-.12	-.02	.07	.08	-.19	.12	.12	**.59****					
11	Device safety (awareness)	.19	-.05	-.09	-.01	.15	**-.30****	.23*	.12	**.71****	**.78****				
12	Malware (awareness)	**.20***	-.04	-.07	.03	.10	**-.23***	.18	.15	**.70****	**.77****	**.85****			
13	Phishing (awareness)	**.23***	-.09	-.08	.02	.14	**-.28****	.12	.04	**.70****	**.79****	**.86****	**.82****		
14	Passwords (awareness)	.17	-.06	-.01	.04	.05	-.16	.17	.08	**.71****	**.78****	**.85****	**.84****	**.81****	
15	Training satisfaction	.09	-.05	.10	.13	.14	.09	**.24***	-.03	.17	**.27****	**.27****	**.21***	**.21***	**.21***

* = significant at the p < .05 level

** = significant at the p < .01 level

There can be three types of outcome between two variables using Pearson's 'r'. A positive relationship is when a higher score on a variable will associate to a higher score on the second variable. A negative relationship is when a higher score on a variable has an inverse relationship on the second variable. The last type of relationship is when there is no discernable significant relationship between the variables.

The Pearson's intercorrelation table generated a significant number of results from the survey. All the significant results have been bolded in Table 7 to make them easier to be seen where relationships existed between variables. The ones highlighted are with the asterisk where * denotes correlation at $p< 0.05$ level and ** denotes correlation at $p<0.01$ level. Whilst both indicate significant relationship (and rejects a null hypothesis between two variables is appropriate), those correlations at $p<0.01$ indicates significant result. All the variables related to the quantitative survey questions are listed vertically on the left. The variables are repeated horizontally at the top but only with the number associated to the variable. Where the vertical variable meets the horizontal variable that is where the Pearson's 'r' value is displayed. Variables 1 – 8 is related to the demographic information about the participants. Variable 9 (Frequency) represents summed scale of respondents cyber behaviour in relation to cyber security awareness. Variables 10 -14 represents the summed scales of questions in the themes. Variable 15 represents the measurement for cyber security training amongst the participants.

In the intercorrelation table, there is a great deal of 'r' values that are significant between variables. It would not be feasible to describe and analyse them all therefore only key relationship between variables will be discussed and analysed. It was observed that age has a positive relationship with time spent in the R SIGNALS, Cyber Training and Education which was expected. As age increases the time spent in R SIGNALS increases ($r = 0.69$, $p <.01$), cyber training increases ($r = 0.22$, $p<.05$) and education increases ($r = 0.35$, $p<01$). There is also correlation between Age and Malware ($r = 0.20$, $p<.05$) and Phishing awareness ($r = 0.23$, $p<.05$). There was correlation between rank

range and time spent in R SIGNALS and Education as expected. As soldiers and officers spend more time in the R SIGNALS rank increases ($r = 0.33$, $p<.01$) and education is expected to increase ($r = 0.57$, $p<.01$). As officers and soldiers spend more time in the Army, there is likelihood of increase in promotion and education opportunities. Time in R SIGNALS had a positive relationship with cyber training ($r = 0.21$, $p<.05$) and education ($r = 0.24$, $p<.05$).

4.2.3 Research Question Specific Correlations

It was observed that soldier/officer was unrelated to cyber awareness or cyber behaviours. Time in R SIGNALS was unrelated to all attitudes of interest (variable 9 – 15) and training satisfaction. However, trade was related to awareness about best practice for device safety ($r = -.30$, $p<.01$), malware ($r = -.23$, $p<.05$) and Phishing ($r = -.28$, $p<.01$).

Cyber training was related to education ($r = .20$, $p<.05$), reported frequency of cyber behaviour ($r = .27$, $p<.01$), awareness of device safety ($r = .23$, $p<.05$) and training satisfaction ($r = .24$,$p<.05$). Education was unexpectedly observed to be unrelated to all cyber attitudes of interest.

Training satisfaction was related to reported cyber training ($r = .24$, p,.05), backup behaviour ($r = .27$, $p<.01$), device safety ($r = .27$, $p<.01$), malware ($r = .21$, $p<.05$), phishing ($r = .21$, $p<.05$) and passwords ($r = .21$, $p<.05$). The higher the awareness of cyber security best practice, the more satisfied are soldiers and officers with the level of training. It was unrelated to education level and self-reported frequency of cyber behaviours.

4.3 Statistical Analysis

4.3.1 Independent Sample t-test

Independent samples t – tests were carried out on SPSS between Cyber Training and all attitudes with results shown in Table 8. The t -test calculates means of variables for two types of people who are either cyber trained or not trained against all attitudes.

Mean and Standard Deviations:

Table 8 - Independent Test Results (Cyber Training Vs All attitudes)

Attitude	Not Cyber trained (Mean(standard deviation)	Cyber trained (Mean(standard deviation)	t-test
FREQUENCY	3.59 (.44)	3.84 (.36)	t(102) = -2.90, p < .01 **
AWARE Back-up	3.92 (.89)	4.14 (.74)	t(102) = -1.25, p = n.s.
AWARE device safety	3.68 (.97)	4.12 (.80)	t(102) = -2.33, p < .05 *
AWARE malware	4.00 (.91)	4.32 (.69)	t(102) = -1.82, p = n.s.
AWARE phishing	3.73 (.90)	3.94 (.69)	t(102) = -1.22, p = n.s.
AWARE passwords	3.89 (.88)	4.19 (.73)	t(102) = -1.74, p = n.s.
Training satisfaction	2.87 (1.14)	3.47 (1.23)	t(102) = -2.50, p < .05 *

NB: n.s is not significant

From the independent t-tests the following results were found to be significant.

a. **Frequency**. This matches with the Pearson's correlation test with the t-test results as t(102) -2.90, p<.01**. As people are more cyber trained, their cyber behaviour frequency is also expected to improve.

b. **Awareness of Device Safety**. The t-test result is t (102) = -2.33, p<.05*. Cyber Training would help increase awareness about device safety.

c. **Training Satisfaction**. The t-test results is t (102) = -2.50,p<.05*. This is not surprising as training satisfaction can increase if people get cyber trained.

4.3.2 One-Way Anova Test

A One-way Analysis of Variance (ANOVA) was conducted to examine the impact of differing trades on cyber attitudes.

4.3.2.1 Non-Significant Results

There was no significant effect of Trade on the self-reported frequency of cyber behaviours (F(5, 103) = 1.88, MSE .18, p = n.s.). There was no significant effect on Trade on the awareness of best practice in backup behaviours (F(5, 103) =

3.24, MSE .63, p = n.s.). There was no significant effect of Trade on the awareness of best practice in Passwords (F(5, 103) = 2.01, MSE .66, p = n.s.).

4.3.2.2 Significant Results

There was a significant effect of Trade on the awareness of best practice in Device Safety (F(5, 103) = 5.54, MSE .70, p < .01 **). Follow up comparisons revealed that there was a significant difference between those describing their trade as ‘other’ and communications systems engineer (p<.01), supervisors (p<.01) and TOT or Tfc Offr (p<.01). There was also a significant effect of Trade on the awareness of best practice in phishing protection (F(5, 103) = 4.50, MSE .60, p < .01 **). Further comparisons revealed that there was a significant difference between those describing their trade as ‘other’ and communication systems engineer(p<.05), supervisors (p<.05) and TOT or Tfc Offr (p<.05).

Those listing their trade as ‘other’ were as follows:

- Commanding officer (n = 1)
- Officer (n = 7)
- DE Officer (n = 2)
- Troop Commander (n = 3)
- Squadron 2IC (n = 1)
- Royal Signals electrician (n = 2)
- Communication logistics specialist (n = 1)

The trades and roles above are non-technical and in most cases, are job roles or trades where soldiers and officers do not get involved in the technical operation of IT equipment and therefore be unaware of phishing protection and device safety. For example, a Squadron 2IC is generally involved in the administration and disciplinary matters for soldiers. He would not be operating technical equipment on a day to day basis on his job role.

One-way ANOVAs was also carried out on Education and all attitudes but there were no significant effects observed.

4.3.2.3 Further Observations

One-Sample t-test was conducted on each of the awareness subcategories such that each sub-theme was compared to the overall mean awareness which was inclusive of all six sub-themes of awareness. Table 9 illustrates the results.

Table 9 - One Sample t-test Results

Measure	**Mean**	**Standard deviation**	**One sample t-test** **(against overall awareness average)**
1. Back-up	4.00	.84	n.s.
2. Device safety	3.83	.93	n.s.
3. Malware	4.12	.85	Significantly higher, p <.05
4. Phishing	3.80	.83	Approaching significance, p = .72
5. Passwords	3.99	.83	n.s.
ALL AWARENESS MEASURES	3.95	.79	n/a

From the results it can be seen that Malware Mean 4.12 at p<.05 was found to be significantly higher compared to the other sub-themes whereas phishing was found to be approaching significance.

4.4 Cyber Capability Maturity for R SIGNALS

One of the objective for this thesis was to benchmark cyber capability maturity in the R SIGNALS and understand what level of maturity the organisation falls under in terms of cyber security awareness and behaviour. Capability maturity was inferred and calculated using participants' scores from Qualtrics and through use of the maturity levels in Table 10 from the Community Cyber Capability Maturity Model developed by White (2011). Capability maturity categories were designated via quartile splits of the Likert scale scoring (1-5). From Qualtrics results, overall average for each item across the entire sample

was extracted. Given the Likert ratings used, the possible scores were between 1 to 5 per individual, so across the entire sample, scores ranged between 1.00 to 5.00 (2 decimal places). These were then divided into the 5 capability maturity levels (1 – 1.80 for Initial, 1.81 – 2.60 for Advanced, 2.61 – 3.40 for Self-Assessment, 3.41 – 4.20 for Integrated and 4.21 – 5.00 for Advanced). Based on the overall average score across all items, R SIGNALS was identified to fall on the 'Integrated' Level in the model.

The table below indicates different levels of cyber maturity model and where R SIGNALS maturity placement is.

Table 10 - Cyber Maturity Model Levels (White, 2011)

Initial – Average R SIGNALS score between 1-1.8, indicating no active management of this aspect of cyber security
Advanced
Self-Assessment
Integrated – R SIGNALS overall average across all items
Vanguard

All the questionnaire items were split into 5 categories. The percentage breakdown of items falling into each category is illustrated in Figure 23 below:

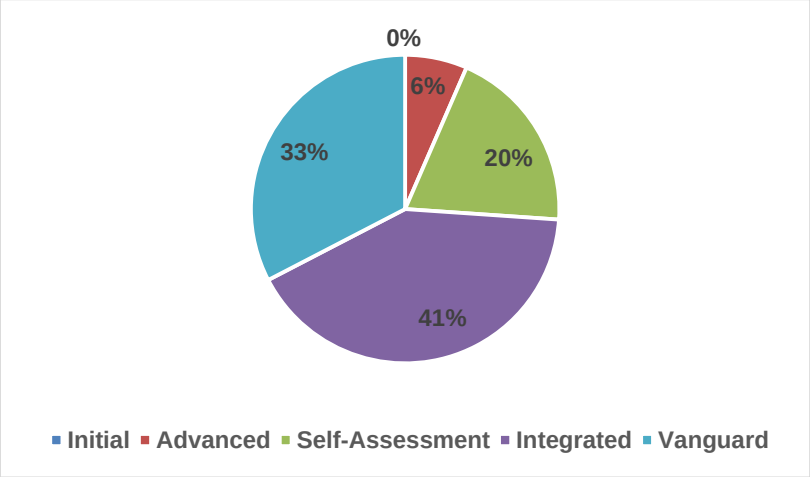


Figure 23 - Breakdown for Different Maturity Levels

Further breakdown of item types against themes is included in the table in Appendix D.

5 DISCUSSION

5.1 Introduction

This research is an exploratory deductive study to understand cyber awareness and behaviour within the context of R SIGNALS. The organisation also known as ‘professional communicators’ hosts and operates a myriad of information systems that is connected to MOD proprietary networks. These networks and systems are protected by technological defences where possible from the public networks however it is crucial that users and operators of these systems understand the risks and vulnerabilities associated with connection to the cyberspace. The research adopts a quantitative method to investigate cyber awareness and behaviour amongst soldiers and officers in the R SIGNALS and benchmark user cyber security capability maturity state. This chapter will conduct a critical study and synthesise the results obtained from the quantitative study and will aim to answer the research aim and objectives. It will also include the findings from the literature review to address the research aim and objectives where appropriate.

5.2 Research Questions and Objectives

It is important to recap the research aim and objectives in this section to set the scene before looking at the in-depth analysis of the results from the data collection and literature review sections. There were two research questions with regards to this research. The first question “*How can cyber awareness be measured? Can an explicit framework of cyber awareness be constructed to inform measurement of cyber awareness?”* is addressed through an innovative online questionnaire that was devised using the government infographic for basic cyber security practices. Along with this, a literature review was conducted in this area to identify whether there are other frameworks to measure cyber security awareness and behaviour and what factors affect the behavioural aspect of cyber security awareness. Models like the HAIS framework (Parsons et al., 2017), risky behaviour scales (Ögütçü et al., 2016) and the KAB model (Kruger and Kearney, 2016) were found to be useful in

measuring security awareness and behaviour. The second question "*Can measurements be used to form an assessment of cyber awareness capability maturity?"* was addressed via reflection upon the capability maturity models in use by industry and academia using literature review and application of a cyber capability maturity model to determine the maturity state of R SIGNALS.

To address the research questions the study focussed on a number of objectives. These included researching for cyber security awareness and behavioural measurement frameworks and devising a refined technique to assess awareness and security behaviour of soldiers and officers in the R SIGNALS, a novel context. The next objective was to carry out a study of UK and Defence cyber security strategy and understand how it applies to the Army. A study was also to be carried on cyber behaviour and factors that are intrinsically linked to the cyber attitudes and intentions of a computer user. Another objective was to do with understanding cyber security awareness about protective practices and how best to deliver a cyber security awareness program. Finally, the last objective was to do with the study of capability maturity models and finding a suitable one to benchmark user cyber security awareness level in the R SIGNALS. Each of the objectives were designed to help address the two research questions in the thesis.

5.2.1 Research Question 1 (RQ1)

This Research Question has two parts; first one is to investigate whether measurements of cyber awareness is possible and if so, the second part is to investigate what methods that are out there used by industry and academia to measure cyber awareness. While effective cyber security policies exist cyber awareness campaigns are key in raising cyber security awareness in organisations as, it is important for organisations to ensure the knowledge of protective practices translates into appropriate cyber behaviour.

5.2.1.1 Research Question 1 Findings

How can cyber awareness be measured?

Cyber awareness is vital for organisations that employ information systems and networks and users must be aware of the risks and vulnerabilities posed by the cyberspace. Good cyber hygiene is extremely important to ensure employers do their part to avoid malicious users gaining illegal access and exploiting our networks, information systems and data within it. Cyber First AID (adaptable, integrated and deliberate) is a concept that Crannell et al. (2013) proposes to ensure good cyber hygiene is adopted. When carrying out the literature review it was identified that there have been extensive work carried out by academia in measuring ISA as opposed specifically to cyber security awareness. Although, the term 'information security' and 'cyber security' is similar in many respects. Neikerk and Solms (2013) argues that the two terms are not totally analogous however, the human awareness and behavioural piece remains similar. The components linked with security awareness for both cyber security and information security remains the same. In past research studies both information security and cyber security awareness measurements studies have included knowledge, attitude and behaviour as metrics to capture awareness. Kruger and Kearney (2006) uses these three components, although he refers to them as affect, behaviour and cognition when measuring ISA in a mining company. Parsons et al. (2017) uses knowledge, attitude and behaviour to measure cyber security awareness of university students and working population in Australia. Cyber security is not just about having the knowledge and being aware of organisational protective practices from cyber security policies, it is also about how much employees are willing to adopt the practices with safe computing behaviour. Therefore, it is important to understand what factors affect safe computing behaviour. Hence, in past research studies knowledge, attitude and behaviour are often used for cyber security awareness. There are different human psychological models that were researched for this study in order to investigate the factors that influences human to adopt safe computing behaviour and how closely attitude and behaviour are linked such as how attitudes influences behaviour.

One model that was researched is the TPB developed by Ajzen and Fishbein (1980, cited in Arnold et al., 2005) and which was originally called the theory of

reasoned action. The model has been successfully used in the past to predict human behaviours (e.g., Arnold et al., 2005) and takes into account attitudes, subjective norms, perceived behavioural control and attitudes. To ensure employees exhibit correct cyber behaviour, it is important for employers to understand the factors which influences cyber attitudes. If these factors are addressed correctly then security awareness will be followed by safe and secure behaviour. The other model that is useful in influencing human behaviours is the 'Technology Acceptance Model' which highlights what factors affect the use of information systems (Arnold et al. 2005). The factors that affect attitudes and behaviours to use protective cyber measures include the perceived ease of use and the perceived usefulness of the protective measures. Employers need to understand and address these two aspects of IT adoption which should assist with employees following protective practices with the correct behaviour.

To further investigate how cyber security awareness can be aptly measured within a Defence context, the author created a measurement framework to quantify cyber security awareness and behaviour. This framework adapted the NCSC (NCSC, 2017) cyber security infographic for cyber security for small businesses and created 6 themes (Device Backup, Device Safety, Malware, Phishing, Passwords, Behaviour), and devised a measurement questionnaire. The themes are considered by NCSC as the most common methods of exploiting cyberspace by cyber criminals. The survey was conducted using soldiers and officers from R SIGNALS to capture awareness of basic cyber protective practices and their behaviour. Two types of Likert scales was used to measure awareness and frequency of behaviour across all themes. When calculating internal consistencies using Cronbach's alpha between items in the questionnaire, the frequency questions resulted with negative or poor alpha values. Further statistical analysis could have been conducted to investigate the low Cronbach's alpha and making constructive changes to the questioning themes, however due to the nature of the research project (MSc research) and time constraints, this was not presently possible.

There were four hypothesis created for the survey in order to capture demographic factors that would influence cyber security awareness and behaviour in the R SIGNALS. The hypothesis are as follows:

Hypothesis 1 (H1) – Due to educational differences, officers will be more cyber aware than soldiers.

Hypothesis 2 (H2) – Soldiers and officers who have served longer in the R SIGNALS will have better cyber awareness and behaviour.

Hypothesis 3 (H3) – Those who have undergone cyber security training will be more cyber aware with better behaviours.

Hypothesis 4 (H4) – Those in technical trades in the R SIGNALS will be more cyber aware than others.

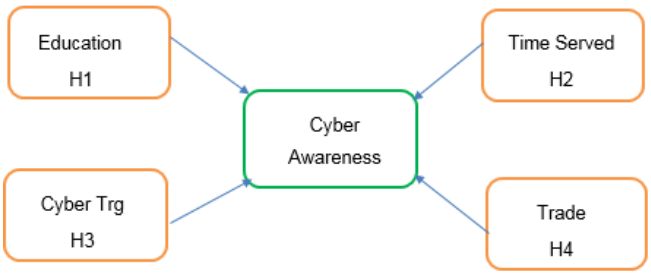


Figure 24 - Hypothesis Testing for Cyber Awareness

Figure 24 illustrates how the author predicted the four factors (education, time served, cyber training and trade) would affect cyber security awareness and behaviours in the R SIGNALS. Initially, gender was also considered as a determinant for the variance in cyber awareness but this was disregarded in the survey results as only 10% participants were female and the results would not have enabled a valid judgement.

Hypothesis 1 (H1) – Due to educational differences, officers will be more cyber aware than soldiers.

Author's Prediction: Most of the DE officers who join Sandhurst have university degrees. "Male and female cadets are trained together in integrated platoons and the majority come from state-funded education, with around 90% holding university degrees" (RMAS website, 2018. All TOT officers in R SIGNALS will have an undergraduate degree as they would have attended the Foreman of Signals (FofS) training as a soldier which would provide them with a Bachelor's Degree in Telecommunications Systems Engineering. Tfc Offrs have to go through 'Yeoman of Signals' training as a soldier and would get a Bachelor's degree in Communications Management (R SIGNALSb, 2018). All other LE officers who are on Regimental Duties role would also have the opportunity to gain academic qualifications through professional development throughout their career.

To join the R SIGNALS as a soldier, GCSE grade A – C in at least English Language, Maths and an IT or science based subject is required. However, soldiers with better grades have more chance of getting selected in technical trades such as communication systems engineer and communications systems operator. Although soldiers are on technical trades, it is assumed that they would not have the required experience and maturity with IT capabilities hence cyber awareness was expected to be lower relative to officers. The literature review indicated similar expectations. Aloul, et al. (2012) in their survey, stated that participants with computer science degrees were less susceptible to phishing attack. Also, Sheng et al. (2010) conducted demographic analysis of phishing in which it was stated that younger participants had lower level of education hence was more susceptible to the attack.

Findings:

Out of the sample selected for the survey, 70 were soldiers and 34 were officers (as shown in Figure 18, p.58). From Pearson's intercorrelation, there was no significant association between officers and soldiers against cyber awareness

or cyber behaviour, as measured presently. The results therefore contradict findings from the literature review which indicated that users with better academic qualifications were less susceptible to cyber-attacks such as phishing. The disparity in results could be because majority of the soldiers (52 in total) who took part in the survey had served between 11 – 22 years and would have the experience of working with IT equipment and also would have an undergraduate or a Foundation degree through their trade training.

Hypothesis 2 (H2) – Soldiers and Officers who have served longer in the R SIGNALS will have better cyber awareness and behaviour.

Author's Prediction: The author expected cyber awareness and behaviour to improve as time served in the R SIGNALS increased for soldiers and officers. The reason why this was predicted was because soldiers and officers become more experienced in operating and managing information systems technology equipment and are expected to be more aware of 'dos' and 'donts' for cyber security as they spend more time in the R SIGNALS. On top of this, during the trade training soldiers on technical trades get taught on the risks and vulnerabilities of using information systems and networks. R SIGNALS is classed as a technical Corps due to the information services, infrastructure and networks that is provided to the customers when deployed on operations abroad or on other supporting activities at home in the UK.

Findings: From Pearson's intercorrelation, it was found that there was no significant association between time served in R SIGNALS and cyber awareness and behaviours, as measured currently. From the results it can be seen that cyber security awareness and behaviours is not dependent on time served in the military. This is a hypothesis that could be further examined in future research. Maybe training included during soldier's trade training is sufficient and there is a skill-fade amongst those who have served for longer. Such users may require cyber security refresher training to polish their knowledge.

Hypothesis 3 (H3) – Those who have undergone cyber security training will be more cyber aware with better behaviours.

Author's Prediction: The author predicted that those who have attended cyber training would be more cyber security aware and more likely to exhibit safe computing behaviour. In the research Aloul et al. (2013) conducted, it was stated that those who had phishing training were less susceptible to a phishing attack compared to the ones who did not undergo the training. Siponen, Mahmood, Pahnila (2014) agrees that information security education and hands-on training enhances confidence in the employee's ability to comply with security policies. However, it is important to select the correct method of training delivery as it needs to be simple, easy and an effective way of increasing user awareness of cyber security.

Findings: Results from the survey indicated that only 36 out of 104 participants had some form of Cyber Training. This was unexpected for the author as there were more than 34 soldiers and officers who took part in the survey who were of technical trades. The Pearson's intercorrelation supported this hypothesis and showed significant correlation between cyber training and reported frequency of cyber behaviour. However, out of the six themes only device safety had significant correlation with cyber training. Further to this, an independent sample t-test was conducted between cyber training and all attitudes. The results from this test showed significant relation between cyber training and frequency of reported behaviour. It also re-confirmed significant relationship between cyber training and awareness of device safety. This showed that soldiers and officers who are trained on cyber security have more likelihood of exhibiting good cyber behaviour and will have better awareness on device safety.

Hypothesis 4 (H4) – Those in technical trades in the R SIGNALS will be more cyber aware than others.

Author's Prediction: There are six trades in the R SIGNALS, but not all trades are technical and related with the daily operation of information systems and technology used within the Corps. The two trades communications systems engineer and communications systems operator are highly technical in nature and comprises of training on information systems, networks and infrastructure. As engineers and operators progress on through their career they have an

option to train as supervisors; operators progress onto becoming ‘Yeoman of Signals’ and engineers progress onto becoming ‘Foreman of Signals’. Both YofS and FofS course includes a bachelor’s degree, and course content includes extensive training on information systems and security. Soldiers in these trades were expected to show increased awareness in cyber security and exhibit good cyber behaviour.

Findings: The results from Pearson’s intercorrelation showed significant correlation between trade and awareness of device safety, malware awareness and phishing awareness. It was unexpected that there was no correlation between trade and frequency of reported cyber behaviours as the author expected that technical trades would have better awareness, and therefore subsequently, their cyber behaviour would be better. A one-way ANOVA test was conducted to examine the association between differing trades and cyber attitudes. The results confirmed that there was no significant effect of trade on self-reported frequency of cyber behaviours. The ANOVA tests also confirmed significant effects of trade on phishing, malware and device safety. Further observations indicated there was difference between those participants who had mentioned their trade as ‘other’ and communication systems engineer, supervisors (FofS and YofS) and TOT or Tfc Offr. This difference may be down to non-technical trades who listed their trade as ‘other’.

The next section will now explore measurement frameworks that have been used in the past by industry and academia to address the second part of RQ1.

Can an explicit framework of cyber awareness be constructed to inform measurement of cyber security awareness?

Cyber security awareness is very important to avoid the weakest link (humans) (Wright, 2016) from getting exploited by adversaries so as to protect our IS and networks. However, research in suitable measurement frameworks are sparse (Ögütçü et al., 2016). and Ng et al. (2009, p815)) agrees that there are few theoretical grounded research publications focusing on factors associated with safe computing behaviour. The literature review researched a number of frameworks that has been used in the past by academics to measure cyber

security awareness or ISA. These models are generally based on measuring three aspects of ISA; knowledge, attitude and behaviour. Parsons et al. (2017) uses knowledge, attitude and behaviour to construct a framework called the HAIS model to investigate ISA and validates the measurements with populations of different demographics in Australia. The model uses 7 focus areas; password management, email use, internet use, social media use, mobile devices, information handling and incident reporting. Each of the focus areas then was divided into 3 sub-areas which was then measured using knowledge, attitude and behaviour scales. Once the survey was conducted this was followed by a phishing experiment to validate the results from the questionnaire. The framework is used to prove that knowledge about safe computing behaviour helps improve user's attitude towards cyber security and this in turn improves actions taken by users in adopting protective practices for information security or cyber security.

The second measurement framework researched was by Ögütçü et al. (2016) where both computer user behaviour and awareness is measured using four scales; Risky Behaviour Scale, Conservative Behaviour Scale, Exposure to Offence Scale and Risk Perception Scale. These scales are then used as metrics in a questionnaire to measure user computer security behaviour and awareness. Risky Behaviour Scale measures the degree of risk of user computing behaviour, Conservative Behaviour Scale measures how much wary users are when taking risks associated when using computers, exposure to offence scale measures how likely users are to cause a security incident and finally risk perception scale is to measure the awareness of safe security behaviour. The novelty of this research is that it does not use the commonly used knowledge, attitude and behaviour to investigate cyber security awareness and produces a framework that is unique but effective in terms of measuring cyber security awareness and behaviour.

Egelman, Harbach and Peer (2016) uses a Security Behaviour Intentions Scale (SeBIS) to measure attitudes of computer users and chooses awareness, passwords, updating and securement as scales to predict user computing

behaviour. The authors claim that the tool is a valid measurement framework to capture user secure computing behaviour. Awareness is measured to predict how effective a computer user is in detecting phishing incidents. The password scale is used to measure how good users are in creating safe and secure passwords. The updating scale is used to measure how likely users are in applying software patches and finally the securement scale is used to detect how users select secret codes to lock their phones.

Parsons et al. (2017) argues that information security measurement framework from other researchers are still at early stages of development to measure every aspects of information security and claims his HAIS questionnaire has been tested rigorously for validity and reliability. The HAIS questionnaire presents a holistic measurement of ISA incorporating all aspects of safe computing behaviour capturing knowledge, attitude and behaviour of computer users.

The next section will discuss and analyse the results from the literature review and data collection for cyber security capability maturity models which forms Research Question 2.

5.2.2 Research Question 2 (RQ2)

Can measurements be used to form an assessment of cyber security awareness capability maturity?

Research Question 2 required exploratory study of cyber security capability maturity models used by academics to assess maturity level in cyber security. The second part included data collected from the survey questionnaire to benchmark cyber security maturity level for R SIGNALS.

The importance of cyber security awareness in R SIGNALS is ever increasing. Army 2020 Refine changes has meant that the organisation will be become more technical with more emphasis on improved skills for software engineering, data analytics, applications and cyber activities. The new changes will include two new cyber regiments entirely focused to produce cyber professionals and protecting the corps' IS and networks. The new structure will also mean R

SIGNALS will be designed to deliver robust, resilient and secure networks of information services for the 21st Century (Gen Pope, 2018). To provide such a capability cyber security awareness will be essential to deter malicious users gaining access for exploiting MOD systems, networks and personnel. A cyber capability maturity model will help establish what maturity state R SIGNALS is currently at and what improvement is required in the field of cyber security to improve cyber security awareness and behaviour amongst computer users.

As part of the literature review, a number of capability maturity models were researched to find a suitable model for benchmarking R SIGNAL's cyber security capability maturity. As mentioned in the literature review, the word 'information security awareness' and 'cyber security awareness' has been used interchangeably in this research as the awareness aspects of both fields are very similar. Capability maturity models were first developed for software development to improve and optimise their processes however with time, the models have evolved and have been modified by other government sectors and industries to improve their respective business processes.

The first model that was researched was Curtis and Mehravari (2015) Cyber CMM used by the electricity sector and using three levels(Initiated, Performed and managed). This model was split into ten domains with key cyber security pratices to be completed to progress onto the next level in that domain. As this model was considered to be of a high level and designed for professional cyber practitioners it was considered unsuitable for assessing maturity for R SIGNALS. Another model explored was the Community Cyber Security Model which was developed by White (2011) and included five levels (Initial, Advanced, Self-Assessed, Integrated and Vanguard) of cyber security maturity. All levels used user awareness, information sharing, processes and procedures and integration as practices to determine the delineation of maturity levels. An organisation at the lowest level of maturity would have minimal cyber awareness amongst users, safe information sharing on cyber security would be minimal, established processes and procedures to follow after a cyber incident would be minimal and the ability to respond to a cyber incident would be close

to non-existent. The beauty of this model is that it can be used by organisation of any size and is simple to follow. The maturity levels from this model was used in conjunction with the results from the survey questionnaire to assess cyber security awareness and behaviour across R SIGNALS.

Whilst this model seeks to overlay maturity across the organisational culture (to reflect overall responsibility and accountability as may be formalised through chain of command and leadership hierarchy) of an entire organisation, the author wanted the model to reflect awareness and behaviour across R SIGNALS at the level of individual users. All of the survey questionnaire items were intended to have respondent rate their own perceptions and capabilities rather than their perception of the capabilities and responsibilities within their workplace (e.g. leadership, cyber professional roles). As such the model was adapted to reflect this individual perspective across R SIGNALS.

Only the security level labels from the community cyber security model was used to define R SIGNALS maturity state. Capability descriptors (the blurb/description below each title) from the Community Cyber Security model whilst useful was not deemed to be entirely appropriate for this research. Based on the overall average score across all items, R SIGNALS was identified to fall at the Integrated Level as shown in Table 11.

Table 11 - Cyber Security Maturity Level for R SIGNALS

Level 1 Initial	**Level 2 Advanced**	**Level 3 Self – Assessment**	**Level 4 Integrated**	**Level 5 Vanguard**
			R SIGNALS overall average across all items	

5.3 Research Generalisation

This research has been successful in highlighting cyber security awareness and security complaint behaviour in R SIGNALS. The study has also been useful in assessing cyber security capability maturity state of R SIGNALS as an organisation. Generalisation is dependent on selecting the representative and correct quantity of sample population. Saunders etal. (2009, p217) states that the error in generalisation to a population gets lower as the sample population increases.

The minimum sample size calculated for this research was 162, however the number of participants for the survey was 104 which was much lower than the designated minimum sample size. This would mean generalisation of the population based on the results from the sample selected would be erroneous. For quantitative research like the one conducted for this study, correct sample size which is representative of the population must be obtained to make any generalisation. If correct sample size would have been achieved then inferences could have been made about the entire population of R SIGNALS.

Although cyber awareness and behaviour measurement framework developed for this study will come in useful for other corps and services, generalisation from the survey results for this study cannot be made for them with any confidence. In any case, this is not advisable as the population for other services and corps would have different cyber aptitude and their trades and roles within the military will be substantially different to R SIGNALS.

5.4 Organisational Recommendations

This research carried out an overall assessment of R SIGNALS soldiers and officers on cyber security awareness and behaviour. The study has been successful to draw out recommendations for improving cyber security awareness and improving computing behaviour. The research identifies a number of areas of cyber where improvement is crucial and have made recommendations split into quick wins and medium-term goals as outlined below.

5.4.1 Recommendations – Quick Wins

5.4.1.1 Cyber Awareness, Attitude and Behaviour Measurement

This research used a novel measurement framework devised by the author to measure cyber awareness and behaviour in the R SIGNALS. Although the framework requires refining and further validation, a similar measurement framework like the one from Parsons et al. (2017) which has been validated rigorously can be used to evaluate cyber awareness, attitude and behaviour in the R SIGNALS. The evaluation is necessary to baseline user awareness and their computing attitude and behaviour to inform future training on basic cyber protective practices. It may further serve to ascertain the convergent validity between the measurement framework generated in the present research and pre-exisiting measures that have already been validated.

5.4.1.2 Cyber Training Delivery Methods

The research highlighted that cyber security policies, awareness campaigns and training are measures organisations adopt to raise cyber security awareness and educate users to adopt safe computing behaviour. However, these measures are found to be inadequate if the training delivery methods are unsuitable for the population in R SIGNALS. Therefore, a detailed study on the population will be required, perhaps through a survey to indicate user preferences on training delivery methods. Training delivery incorporating a mixed approach like Abawajy and Kim (2010) suggests with methods incorporating text-based, game-based and video presentation might prove to be particularly advantageous.

5.4.1.3 Cyber Awareness Training on Basic Protective Practices

While the CPTs within the Army deals with the high level defensive and offensive cyber tactics to protect our systems and networks, basic user awareness is important to avoid social engineering attacks from cyber criminals. Training on basic cyber protective practices must be generic for everyone from the R SIGNALS. Less than 50% participants in the survey indicated that they had some form of cyber training which means there is a requirement to ensure training and refresher training is made mandatory for everyone in the R

SIGNALS. While comprehensive cyber training might be designed based on the results from this research project, for the short term, R SIGNALS employees can be directed to take the cyber awareness training on Defence Learning Environment (DLE) and this can be registered on their Joint Personal Administration (JPA) database as a competency to encourage training uptake.

5.4.1.4 Research Identified Cyber Awareness and Behaviour Shortfall – Areas of Targeted Training

The research looked at the relationship between cyber awareness and behaviour with factors such as academic qualification, time served, cyber training and trades using hypothesis testing. Targeted training can be delivered based on the results obtained from the survey. The survey results indicated that cyber training was related to all frequency reported behaviours but only related to device safety in awareness. This would mean more awareness training would be required to improve knowledge on malware, phishing, back-up and passwords. The testing of relationship between trades and cyber awareness implied that the technical trades were associated with the frequency of reported behaviours, as well as having awareness on device safety, malware and phishing. This indicated that targeted training would be required in other areas such as device backup and passwords.

5.4.2 Recommendations – Medium Term

5.4.2.1 Need for Army Cyber Strategy

As highlighted in this report, the Army currently do not have a Cyber Strategy. The other two services , the Royal Navy and the Royal Air Force have their own cyber strategies and provide detailed direction on cyber security for their individual services. There is a need for the Army to create a cyber strategy so that direction is provided to all the corps and organisations that fall within it. R SIGNALS can then create its own strategy document forging a basis and direction for an Army Cyber Strategy.

5.4.2.2 Capability Maturity Model Usage

Maturity models are useful in assessing organisational cyber maturity state and identifying processes and procedures that require improving to protect our cyberspace and digitally connected networks, people and infrastructure. In this research, adoption of the community cyber security maturity model (White, 2011) was used to benchmark cyber maturity in R SIGNALS. However, the adoption of the model was only limited to the participants rating their own perception and capabilities rather than providing a holistic view of their workplace culture. Future recommendations for use of maturity model should include assessment of maturity across organisational culture to reflect overall responsibility and accountability formalised through the chain of command (and formal professional roles). Capability measurement should then be conducted regularly to enable effective capability monitoring and to regularly identify areas for improvement.

5.5 Methodological Evaluation

The research adopted a cross-sectional study with quantitative data collection technique using an online survey questionnaire. This section will outline the methodological limitations and constraints. Also included will be an assessment of strengths and weaknesses of the methodology used for the research questions undertaken in the present research.

5.5.1 Methodology Limitations and Constraints

The inability to conduct longitudinal study for this research was due to time constraints hence a cross-sectional approach was adopted. Saunders et al. (2009) states that longitudinal studies have the capacity to track change and development whereas cross-sectional studies are only related to a particular time when the research takes place. Although, the research may have been improved using the longitudinal approach, the author did not have enough time or the resources to adopt it for this study. As the author is studying part-time to complete this thesis, it would have been difficult to afford time for this kind of study.

The sample completing the questionnaire was not numerically representative of the diverse population of R SIGNALS as the calculated sample size was not met (See Section 3.2.6). This may have been due to the length of time the survey was opened for which was not long enough to meet the minimum sample required. In addition to this, responses from 18 participants were excluded as part of data treatment as there was significant data missing. Hence generalisation cannot be confidently made about the entire R SIGNALS population with the results achieved with this study. The sample selected for soldiers was also not representative for 'time served' as most of respondents were between 11 – 22 years of service and there was very little representation from soldiers young in service. This meant that the validity of responses from the soldiers may be poor as only experienced soldiers were taking part in the survey. Similarly, the representation of females from the sample was not suitable, hence gender was disregarded from the survey.

Once the survey was opened for the participants it was impossible to make changes to the questions if discrepancies were found as it may have nullified the use of previous respondents data. The pilot study was the only opportunity to find discrepancies with all aspects of the survey questionnaire. The results from Pearson's coefficient test on reliability for frequency scale was negative or very low hence signifying poor reliability. This could have been further explored through statistical analysis and making changes to the grouping of question themes, however this could not be conducted within the present research timeframe.

Another notable limitation is that quantitative surveys might often be prone to biased answers such as response sets. For this questionnaire, the possibility of response set was discouraged using the reverse-coding technique for questions. Nevertheless, it is possible that bias or inaccuracies in answer could still have been found due to several reasons, such as, the participants becoming bored of the questions and answering all the questions quickly without giving much thought. Another example maybe that the participant have

the habit of providing the same answers for questions that are similar. Hence, reverse coding of questions was used in order to avoid bias.

A further critique of quantitative surveys such as this are that only one dimension is captured in terms of data collection. It cannot capture the subjective views of respondents that you would normally able to capture through an interview. Subjective views can be used to elaborate and confirm and/or contest the results obtained from quantitative methods.

The survey was designed using an online software called Qualtrics. The online questionnaire meant that it was easier to distribute to participants irrespective of where they were located geographically. The compatibility of the questionnaire to be used in smart devices meant that users could take part in the survey using their phones while in the office or at their leisure. This was considered to be a strength of the research approach adopted presently. A challenge that the author encountered was the use of SPSS software to carry out data analysis. However, the dissertation supervisor provided the support required to use the SPSS software and with the data analysis.

From the survey results there were some unexpected answers which could have been erroneous. For example when carrying out the Pearson's intercorrelation, the technical trades had no relationship with frequency of reported behaviour. This was unexpected and could have been down to the poor reliability (Cronbach's alpha) results for the frequency questions.

Finally, although literature review is a complex process and full of challenges, it is a very useful method of studying work conducted by other researchers in your problem context. The main challenge included getting the keywords right when searching electronic databases and filtering materials by reviewing abstracts. When conducting a search in the online databases the results returned can sometimes be quite overwhelming and unmanageable. By having a good literature review strategy it was possible to coherently evaluate relevant literature that provided information for the problem that was being researched. This advanced the research agenda in a productive fashion.

5.6 Future Research

This research has been useful in creating and validating an innovative cyber awareness and behaviour measurement framework in order to measure cyber security awareness and behaviour of soldiers and officers from R SIGNALS. However, like any research there is scope to take this research forward and improve the measurement framework, avoiding some of the methodological limitations as noted above whilst attempting to validate useful findings. A number of recommendations have been made below with regards to exploring and advancing the research areas further.

5.6.1.1 Inclusion of Attitude Scale to the Measurement Framework

The author developed an innovative framework for measuring basic cyber awareness and behaviour in this research. The two scales for measurement was awareness and behaviour. After conducting the literature review, it was identified that attitude forms an important part for computer users adopting safe computing behaviour. Many researchers have used knowledge, attitude and behaviour as their scales for measuring security awareness. Parsons et al. (2017) uses knowledge, attitude and behaviour to measure ISA. The TPB explains how attitude, subjective norms and perceived behavioural control are factors which has direct influence on human intentions to behave in a particular way. It is important to understand what influences users to take the correct actions in terms of safe computing behaviour. The addition of the third scale 'attitude' will make the security awareness measurement framework better by providing information about user's perception to cyber security protective practices.

When carrying out the awareness survey it is important to ensure the results are reliable and valid. This can perhaps be tested by a follow-up phishing experiment where the results of actual behaviour can be compared with the results from the survey (self-reported behaviour). If results from the phishing experiment correspond to that from the survey then this implies validity and reliability of the results obtained from the survey.

5.6.1.2 Better Sample Selection and Demographics Distribution

The sampling technique used for this research was ‘probability sampling’. The intention was to make inferences with the results obtained from the representative sample to the R SIGNALS population. However, there were two issues with the samples. Firstly, the author was unsuccessful in meeting the minimal sample size requirement which was compounded by having to reject 18 participants for incomplete data. Secondly, the distribution of samples were not uniform in terms of trades, time served, age, gender and rank. Hence, generalisation cannot be confidently made to the R SIGNALS population using the results from this research. Future research should include a quota sample of the demographic characteristics required for generalisation. The samples must be selected so that distribution of population variation in the samples are uniform which will increase the validity and reliability of the hypothesis test results.

5.6.1.3 Questionnaire Pilot Study

Once the questionnaire was designed and ready to be distributed, it had to be pilot tested before data collection. Saunders et al. (2009) recommends a minimum number of ten participants for small surveys and the sample selected should include major variation in the population that would impact the results. However, this study did not include enough participants for the pilot with the correct distribution of population variation due to time constraints. Further research must include the right sample selection for the pilot survey and results checked for reliability and validity before commencing with data collection.

5.6.1.4 Mixed Approach Research Design

This research exclusively used a quantitative method of data collection and analysis through the use of a survey questionnaire. A mixed method approach allows the use of both quantitative and qualitative techniques to address a research problem. Saunders et al. (2009) explains mixed approaches provides greater confidence in the results from a research. Quantitative methods alone do not include subjective views and observations of a research context and lacks greater understanding to a problem. Therefore, future research should

include a qualitative method which can be used to extend, validate, confirm or refute the results from the quantitative study. This would also allow greater validity of the results by triangulating data obtained from the mixed method approach and the literature review.

5.6.1.5 Capability Maturity Models

In this research the community cyber capability maturity model was adopted to benchmark cyber security maturity in the R SIGNALS. However, the model was adopted in the most simplistic way and and it was used at the level of individual users. Future research on this study could include comprehensive use of the model by comparing the practices (user awareness, information sharing, processes and procedures and integration) at each level (e.g. team, company, chain of command) to further determine R SIGNALS placement within the correct capability maturity level.

5.6.1.6 Longitudinal Study

Further validation of the framework can be assessed using a Longitudinal approach to this research study. This approach will require time and resources to conduct it therefore will require someone who is undergoing an extended full time study. This study may present differing sets of results in terms of awareness and behaviour as cyber security awareness and processes evolves and matures in an organisation with time.

5.7 Summary

The research aimed to measure cyber security awareness and behaviour of officers and soldiers in the R SIGNALS using an innovative method that the author had created. It also included benchmarking cyber capability maturity level for R SIGNALS using cyber capability maturity models.

This chapter answered the research questions and objectives through the use of results from the literature review and data collected using an online questionnaire. The author makes recommendations for future research which

includes addition of the attitude scale to the measurement framework and comprehensive use of capability maturity model to benchmark cyber maturity in R SIGNALS.

6 CONCLUSION

This chapter will highlight the conclusions drawn from this research and present a summary of findings for cyber security awareness and behaviour in R SIGNALS. The research strategy included a positivist approach with quantitative data collection technique.

6.1 Research Outcomes

6.1.1 Research Question 1 (RQ1)

The first part of RQ1 was investigating how cyber awareness could be measured. To address this question, an innovative measurement framework in the form of an online questionnaire was created by the author to measure cyber awareness and behaviour of soldiers and officers from R SIGNALS. The questionnaire adapted basic cyber protective practices from the NCSC infographics on cyber security for small businesses and created six themes to test awareness and behaviour of the sample selected for the survey. A number of hypothesis was created to test them with the results obtained from the respondents.

H1 – Due to educational differences officers will be more cyber aware than soldiers.

The author predicted that the hypothesis would prove to be true but results from the survey concluded that educational differences between soldiers and officers did not have any influence on cyber awareness or behaviour in the R SIGNALS.

H2 – Soldiers and Officers who have served longer in the R SIGNALS will have better cyber awareness and behaviour.

The author predicted that time served would have a positive effect on cyber awareness and behaviour. The findings from the survey concluded that time served in the R SIGNALS did not have any influence on cyber security awareness and behaviour.

H3 – Those who have undergone cyber security training will be more cyber aware with better behaviours.

The author predicted that soldiers and officers who attended cyber security training would have better cyber awareness and behaviour. Results from the survey concluded that cyber training showed significant correlations with reported frequency of behaviour and awareness on device safety. Recommendations made for targeted training on five other themes (malware, device backup, phishing and passwords).

H4 – Those in technical trades in the R SIGNALS will be more cyber aware than others.

The author predicted that technical trades (communication systems engineer, communciations systems operator, FofS, YofS, TOT and Tfc Offr) would have better cyber awareness and behaviours. Results from the survey showed correlation between technical trades and awareness of device safety, malware and phishing. There was no correlation between trades and reported frequency of behaviour. Recommendations were made for targeted training for technical trades on awareness of passwords and device backup.

Further research using literature review identified that awareness is not enough in exhibiting safe computing behaviour. Behavioural models like the ‘Theory of Planned Behaviour’ (Arnold et al., 2005, Bulgurcu et al., 2010, Lebek et al., 2014, Feielding et al., 2008 and Fang and Shih, 2018) was used in this research to identify factors that affect human attitudes that influences intentions

and behaviours. Another useful model researched is called the 'Technology Acceptance Model' (Arnold et al, 2005) where computer users look at perceived usefulness and ease of using the technology and behave accordingly. Application of these models to address human behavioural factors such as attitude can influence how users adopt safe computing behaviour.

The second part of RQ 1 was investigating awareness measurement framework used by academics in past research. From the literature review, a number of measurement frameworks were identified for measuring cyber awareness and behaviour. The first one investigated was of Parsons et al. (2017) which uses knowledge, attitude and behaviour to test security awareness. The framework has been tested multiple times for validity and reliability. Another framework that was researched was the one developed by Ögütçü et al. (2016) which uses four scales for user awareness; Risky Behaviour Scale, Conservative Behaviour Scale, Exposure to Offence Scale and Risk Perception Scale. The author feels that the novelty of this research is that it is unique and effective way to measure user security awareness and behaviour appropriate for the Defence (R SIGNALS) context.

Furthermore, the literature review highlighted that selection of training delivery methods for awareness and safe computing behaviour is absolutely vital to improve organisational cyber security awareness and behaviour. Choosing the right delivery method would ensure that knowledge is translated into awareness and awareness and intentions translated into safe and secure behaviour. A mixed approach was found to be the most effective using text-based, game-based and video presentation based training methods (Abawajy and Kim, 2010, Saunders et al., 2009).

6.1.2 Research Question 2 (RQ 2)

An exploratory study of cyber security capability maturity models was conducted during the literature review to assess maturity levels of organisations in cyber security. A number of maturity models were considered for the research (Curtis and Mehravari, 2015, Barclay, 2014, White, 2011). The first two were disregarded for this research as it was considered too high level for

benchmarking cyber capability maturity for R SIGNALS. The Community Cybersecurity Maturity Model which uses five levels for maturity was adopted in the most simplistic way to benchmark cyber maturity in R SIGNALS. Using the results from the questionnaire, and based on user cyber security awareness R SIGNALS was placed at the Integrated Level of maturity (Level 4).

Key recommendations for future research include addition of an 'attitude scale' to the measurement framework devised by the author to have a holistic understanding of cyber awareness and behaviours for soldiers and officers in the R SIGNALS. The exisiting HAIS framework (Parsons et al, 2017) which has been proved for validity and reliability can be used to measure users' attitude, however future researchers will benefit from conducting a review of development of the attitude scale between this research and the next one. A further recommendation of note included the comprehensive use of the Community Cybersecurity Model for R SIGNALS to include aspects of cyber culture within the Corps.

This section has covered in summary whether the study answered the research questions and highlighted recommendations that have been made in the previous chapter. The following will cover literature considerations and final thoughts for the research.

6.1.3 Literature Consideration

The relation between the results from the literature review was at times both convergent and divergent with the results returned from the survey. The literature review indicated that users with better academic qualifications would be more cyber aware but results returned from the survey diverged, and failed to support this theory. On the other hand, both the measurement frameworks identified from the literature review and the one devised by the author was similar in terms of measurement of cyber security awareness, indicative of convergence. To further confirm convergence, future research could incorporate all of the scales, i.e. knowledge, attitude and behaviours. The three scales may

provide a holistic view of user awareness and behaviour in adopting basic cyber security protective practices.

6.1.4 Final Thoughts

With the structural changes dictated by A2020 Refine (Gen Pope, 2018), R SIGNALS remains to be a technical corps but will require a greater range of technical skills that includes expertise or basic protective skills in the ‘cyber’ arena. Until now, there is no cyber awareness framework that has been used by the Army to assess cyber awareness and behaviour. The novel measurement framework devised by the author in assessing cyber security awareness and behaviour can help identify and recommend aspects of cyber training for organisations. The framework once refined with the addition of an ‘attitude’ scale will quantify a holistic measurement of cyber security awareness and behaviour in an organisation. This could potentially be used as a generic framework for measurement within other corps and organisations in the Army. The results from the measurement framework can then be transposed into a cyber capability model to benchmark cyber maturity state.

REFERENCES

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology*, 33(3), pp.237-248, Available at: https://doi.org/10.1080/0144929X.2012.708787 (Accessed: 26 July 2018).

Abawajy, J., and Kim, T. (2010) 'Performance analysis of cyber security awareness delivery methods'. *In: Kim T., Fang W., Khan M.K., Arnett K.P., Kang H., and Ślęzak D. (Eds.) Security Technology, Disaster Recovery and Business Continuity. Communications in Computer and Information Science*,122, Springer, Berlin, Heidelberg. Available at: https://doi.org/10.1007/978-3-642-17610-4_16 (Accessed: 28 July 2018).

ACIN 15/17. (2017) ' Army 2020 Refine (A2020R): Royal Corps of Signals and Intelligence Corps structural change, *Defence Intranet.* Available at: http://defenceintranet.diif.r.mil.uk/libraries/1/Docs9/20170530.1/20170628-ACIN_A2020R_Update_RSIG_INTCORPS_Final_v2_AS(L)-OS.doc. (Accessed: 11 June 2018).

Ajzen, I. (2011) 'The theory of planned behaviour: Reactions and reflections', *Psychology & Health*, 26(9), pp.1113-1127 Available at: https://doi.org/10.1080/08870446.2011.613995 (Accessed: 27 July 2018).

Aloul, F. (2010) 'The need for effective information security awareness', *International Journal of Intelligent Computing Research,* 1(3), pp.176-183, Available at: https://www.researchgate.net/profile/Fadi_Aloul/publication/257980212_The_Need_for_Effective_Information_Security_Awareness/links/02e7e526829271ef77000000/The-Need-for-Effective-Information-Security-Awareness.pdf (Accessed: 26 July 2018).

Aloul, F., Darwish, A., and Zarka, A.E. (2012) 'Towards understanding Phishing victims' profile', *2012 International Conference on Computer Systems and Industrial Informatics*, Sharjah, 2012, pp.1-5.

Available at: https://doi.org/10.1109/ICCSII.2012.6454454 (Accessed: 17 May 2018).

Arnold, J., Silvester, J., Patterson, F., Robertson, I., Cooper, C. and Burnes, B (2005) *Work psychology: Understanding human behaviour in a workplace,* 4th Edn. Harlow, England: Pearson Education M.U.A. Available at: https://www.dawsonera.com/readonline/9781405870375 (Accessed: 18 Feb 2018).

Bada, M., and Sasse, A. (2014) 'Cyber security awareness campaigns: Why do they fail to change behaviour?' *Global Cyber Security Capacity Centre: Draft Working Paper*, University of Oxford. Available at: http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf (Accessed: 18 January 2018).

Barclay, C. (2014) 'Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM^2) - *Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world - Impossible without standards?*, St. Petersburg, 3-5 June, pp.275-282. Available at: https://doi.org/10.1109/Kaleidoscope.2014.6858466 (Accessed: 28 July 2018).

Barford, P., Dacier, M., Dietterich, T.G., Fredrikson, M., Giffin, J., Jojodia, S., Jha, S., Li, J., Liu, P., Ning. P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C. and Yen, J. (2009) 'Situational awareness for cyber defense'. In Jajodia S., Liu P., Swarup V., and Wang C. (Eds.) *Cyber Situational Awareness. Advances in Information Security*, 46, pp.3-13, Available at: https://doi.org/10.1007/978-1-4419-0140-8_1 (Accessed 26 July 2018).

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. and Weiss, J. (2012) *Cyber security policy guidebook* - (1st Edn.). Jon Wiley and Sons Inc. Available at: https://books.google.co.uk/books (Accessed: 25 July 2018).

BBC News (2008a) 'Estonia fines man for 'cyber war'', *BBC News,* 25 January, Available at: http://news.bbc.co.uk/1/hi/technology/7208511.stm (Accessed: 12

December 2017).

BBC News (2017b) ‘NHS 'could have prevented' WannaCry ransomware attack’, *BBC News, 27 October,* Available at: https://www.bbc.co.uk/news/technology-41753022 (Accessed: 15 January 2018).

Beck, C and Polit, D. (2010) ‘Generalization in quantitative and qualitative research: Myths and strategies’. *International Journal of Nursing Studies*. 47 (11), pp.1451 - 1458. Available at: https://doi.org/10.1016/j.ijnurstu.2010.06.004 (Accessed: 15 June 2018).

Brazier, C. (2014) ‘Defence strategic communication framework – ‘cyber’, *Defence Intranet.* Available at: http://defenceintranet.diif.r.mil.uk/libraries/8/Docs6/20150820.1/20141021-Cyber%20Strat%20Comms%20Framework%20FINALv3-OS%20_2_.pdf. (Accessed 9 June 2018).

Brynielsson, J., and Franke, U. (2014) ‘Cyber situational awareness – A systematic review of the literature’, Computers and Security. 46 (0), pp.18-31. Available at: https://doi.org/10.1016/j.cose.2014.06.008 (Accessed 26 July 2018)

Bullée, J-W.H., Montoya, L., Pieters, W., Junger, M. and Hartel, P.H. (2015) ‘The persuasion and security awareness experiment: reducing the success of social engineering attacks’, *Journal of Experimental Criminology*,11(1), pp.97 – 115. Available at: https://doi.org/10.1007/s11292-014-9222-7 (Accessed: 26 July 2018).

Bulgurcu, B., Hasan, C. and Benbasat, I. (2010). ‘Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness’, *MIS Quarterly* 34(3), pp. 523 – 548, Available at: https://dl.acm.org/citation.cfm?id=2017477 (Accessed: 26 July 2018).

Butkovic, M.J, and Caralli, R.A. (2013) *CMU/SEI-2013-TN-028:* ‘Advancing cybersecurity capability measurement using the CERT®-RMM maturity indicator

level scale', SIE: Carnegie Mellon University. Available: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_69194.pdf. (Accessed 18 July 2018).

Car, W. (2006) 'Philosophy, methodology and action research', *Journal of Philosophy and Education,* 40(4), pp.421-435. Available at: https://doi.org/10.1111/j.1467-9752.2006.00517.x (Accessed: 28 July 2018).

Carver, C., Dodge Jr, R.C. and Ferguson, A.J. (2007) 'Phishing for user security awareness', *Computer and Security,* 26(1), pp.73 – 80. Available at: https://doi.org/10.1016/j.cose.2006.10.009 (Accessed: 16 July 2018).

Chen, C.C., Medlin, B.D., and Shaw, R.S. (2008) 'A cross-cultural investigation of situational information security awareness programs', *Information Management & Computer Security*, 16(4), pp.360-376. Available at: https://doi.org/10.1108/09685220810908787 (Accessed: 16 July 2018).

Choo, K-K.R. (2011). 'The cyber threat landscape: Challenges and future research directions'. *Computers and Security,* 30(8), pp.719-731, Available at: https://doi.org/10.1016/j.cose.2011.08.004 (Accessed: 26 July 2018).

Colwill, C. (2009) 'Human factors in information security: The insider threat – Who can you trust these days?', *Information Security Technical Report*, 14(4), pp186-196, Available at: https://doi.org/10.1016/j.istr.2010.04.004 (Accessed: 26 July 2018).

Conner., M. (2015) 'Extending not retiring the Theory of Planned Behaviour: A commentary on Sniehotta, Presseau and Araújo-Soares', *Health Psychology Review*, 9(2), pp.141-145. Available at: https://doi.org/10.1080/17437199.2014.899060 (Accessed: 27 July 2018).

Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007) 'A video game for cyber security training and awareness', *Computers and Security,* 36, pp.63 – 72. Available at: https://doi.org/10.1016/j.cose.2006.10.005 (Accessed: 20 July 2018).

Crannel, M., Moulton, J. and Sheppard, B. (2013) 'Cyber first aid: proactive risk management and decision-making', *Environmental Systems and Decisions*, 33(4), pp.530-535. Available at: https://doi.org/10.1007/s10669-013-9474-1 (Accessed: 26 July 2018).

Crowell, M.C (2010) War in the information age: 'A primer for cyberspace operations in 21st century warfare'. US Naval War College. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a514490.pdf (Accessed: 9 June 2018).

Curtis, P.D. and Mehravari, N. (2015) 'Evaluating and improving cybersecurity capabilities of the energy critical infrastructure', *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 14 – 16 April, pp.1-6. Available at: https://doi.org/10.1109/THS.2015.7225323 (Accessed: 25 July 2018).

Deloitte. (2012). *ISO 27032 Guidelines for Cyber Security: Deloitte point of view for analysing and implementing the guidelines.* Available at:: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/iso27032_guidelines_cybersecurity_2011_deloitte_uk.pdf . (Accessed 16 July 2018).

DDC News. (2018). 'Advice and guidance on personal online security', *Defence Intranet.* Available at: http://defenceintranet.diif.r.mil.uk/News/Announcements/Pages/Adviceandguidanceonpersonalonlinesecurity.aspx. Accessed: 9 June 2018).

Denzin, N. K. and Lincoln, Y. S. (2000) *Handbook of Qualitative Research*, (2nd Edn.), Thousand Oaks, CA: Sage.

DMC Online News (2014) 'Thinking defence: How the cyber security programme protects MOD', *MOD Intranet*, Available: http://defenceintranet.diif.r.mil.uk/News/BySubject/DefencePolicyandBusiness/Pages/ThinkingDefencehowtheCyberSecurityProgrammeprotectstheMOD.aspx. (Accessed 8 June 2018).

Dobson, P.J. (2001) 'The philosophy of critical realism—An opportunity for

information systems research'. *Information Systems Frontiers,* 3 (2), pp.199 - 210. Available at: https://link.springer.com/content/pdf/10.1023%2FA%3A1011495424958.pdf (Accessed: 18 July 2018).

Durlabhji, S., and Fusilier, M. (2005) 'An exploration of student internet use in India: the technology acceptance model and the theory of planned behaviour', *Campus-Wide Information Systems*, 22(4), pp.233-246. Available at: https://doi.org/10.1108/1065074051061753 (Accessed: 15 May 2018).

Egelman, S., Harbach, M., and Peer, E. (2016) 'Behavior ever follows intention?: A validation of the Security Behavior Intentions Scale (SeBIS)'. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16). San Jose, California, 7 – 12 May, ACM, New York, NY, USA. Available at: https://doi.org/10.1145/2858036.2858265 (Accessed: 20 July 2018).

ENISA (2016) *Review of cyber hygiene practices.* Available at: https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport (Accessed 26 July 2018).

Fang, K., and Shih, Ya.Y. (2004) 'The use of a decomposed theory of planned behavior to study internet banking in Taiwan', *Internet Research*, 14(3), pp.213-223. Available at: https://doi.org/10.1108/10662240410542643 (Accessed: 15 July 2018).

Fielding, K.S., McDonald, R. and Louis, W.R. (2008) 'Theory of planned behaviour, identity and intentions to engage in environmental activism' *Journal of Environmental Psychology,* 28(4), p318 – 326. Available at: https://doi.org/10.1016/j.jenvp.2008.03.003 (Accessed:13 July 2018).

Gilovich, T., and Kruger, J. (2004) 'Actions, intentions, and self-assessment: The road to self-enhancement is paved with good intentions, *Personality and Social Psychology Bulletin* , 30(3), pp.328 – 339. Available at: https://doi.org/10.1177/0146167203259932 (Accessed: 25 June 2018).

Goldberg, L. R. (1990) 'An alternative description of personality: The big-five factor structure'. *Journal of Personality and Social Psychology*, 59(6), pp.1216–1229. Available at: https://projects.ori.org/lrg/PDFs_papers/Goldberg.Big-Five-FactorsStructure.JPSP.1990.pdf (Accessed: 13 July 2018).

HM Government (2015) *National security strategy and strategic defence and security review 2015: A secure and prosperous United Kingdom* – U.K: Williams Lea Group. Available at: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 (Accessed: 25 July 2018).

HM Government (2016) *National cyber security strategy 2016 – 2021.* Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (Accessed: 25 July 2018).

HM Government (2011) T*he UK Cyber Security Strategy – Protecting and promoting the UK in a digital world*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Accessed: 25 July 2018).

MOD (2016) *Cyber Primer (2nd Edn.)* – DCDC MOD. Available at: https://www.gov.uk/government/publications/cyber-primer (Accessed 1 July 2018).

Guardian (2016) 'Yahoo hack: 1bn accounts compromised by biggest data breach in history', The Guardian, 14 December, Available at: https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached (Accessed 15 January 2018).

Harmon-Jones, E., Harmon-Jones, C. and Levy, N. (2015) 'An action-based model of cognitive dissonance processes, *Current Directions in Psychological Science,* 24(3), pp.184-189. Available at: http://www2.psych.ubc.ca/~schaller/308Readings/HarmonJones2015.pdf (Accessed: 27 July 2018).

Hoang D.B. and Le, N.T. (2016) 'Can maturity models support cyber security', *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, Las Vegas, NV, 9 – 11 December, pp.1-7. Available at: https://doi.org/10.1109/PCCC.2016.7820663 (Accessed: 17 July 2018).

Hoeksma, M.A., Gerritzen, Lokhorst, A.M and Poortvliet, P.M. (2017) 'An extended theory of planned behaviour to predict consumers' willingness to buy mobile slaughter unit meat', *Journal of Meat Science,* 128, pp.15-23. Available at: https://doi.org/10.1016/j.meatsci.2017.01.011 (Accessed: 27 July 2018).

Heineck, G. and Anger, S. (2010) 'The return of cognitive abilities and personality traits in Germany', *Labour Economics',* 17, pp.535-546. Available at: https://doi.org/10.1016/j.labeco.2009.06.001 (Accessed: 27 July 2018).

Howarth, F. (2014) *The role of human error in successful security attacks.* Available at: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ (Accessed: 12 December 2017).

Johnson, A. (2017) 'Massive Phishing attacks targets Gmail users', *NBC News,* 4 May, Available at: https://www.nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501 (Accessed: 26 July 2018)

Katz, F.H. (2005) 'The effect of a university information security survey on instruction methods in information security', *InfoSecCD '05 Proceedings of the 2nd annual conference on Information security curriculum development,* Kennesaw Georgia, 23 – 24 September 2005, Armstrong Atlantic State University, pp. 43 – 48. Available at: https://doi.org/10.1145/1107622.1107633 (Accessed: 26 July 2018).

Kim, C., Rhee, H-S, and Ryu, Y.U (2009) Self-efficacy in information security: Its influence on end users' information security practice behaviour, *Computers & Security,* 28(8), pp.816-826, Available at: https://doi.org/10.1016/j.cose.2009.05.008 (Accessed: 20 July 2018).

Korpela, K. (2015*)* 'Improving cyber security awareness and training programs

with data analytics', *Information Security Journal: A Global Perspective,* 24(1-3), pp.72-77, Available at: https://doi.org/10.1080/19393555.2015.1051676 (Accessed: 16 July 2018).

Kruger, H.A. and Kearney, W.D. (2006) 'A prototype for assessing information security awareness', *Computers and Security,* 24(4), pp.289-296. (Available at: https://doi.org/10.1016/j.cose.2006.02.008 (Accessed: 17 June 2018).

Lebek, B., Uffen, J., Neumann, M., Hohler, B and Breitner, M.H. (2014) 'Information security awareness and behavior: a theory-based literature review', *Management Research Review*, 37(12), pp.1049-1092. Available at: https://doi.org/10.1108/MRR-04-2013-0085 (Accessed: 20 June 2018).

Lynham, S., and Ruona, W. (2004) 'A philosophical framework for thought and practice in human resource development'. *Human Resource Development,* 7 (2), pp.151-154. Available at: https://doi.org/10.1080/13678860310001630665 (Accessed: 25 June 2018).

Marks, A. and Rezgui, Y. (2008) 'Information security awareness in higher education: An exploratory study', *Computers and Security,* 27(7-8), pp.241-253). Available at: https://doi.org/10.1016/j.cose.2008.07.008 (Accessed: 27 July 2018).

Maslow, A. (1954) *'Motivation and Personality'*, England: Harper & Row Publishers. Available at: http://s-f-walker.org.uk/pubsebooks/pdfs/Motivation_and_Personality-Maslow.pdf (Accessed: 27 July 2018).

MOD, (2015) '2014/2015 Defence cyber security education and training', *Defence Intranet.* Available at: http://defenceintranet.diif.r.mil.uk/libraries/corporate/DINStraining/2014/2014DIN07-155.pdf. (Accessed 8 June 18).

Neuman, W.L. (2014) *Social research methods: Qualitative and quantitative approaches,* (7th Edn.) UK: Pearson Education M.U.A. Available at: https://www.dawsonera.com/readonline/9781292033617 (Accessed: 25 June.

2018).

NCSC (2017) ‘Cyber security small business guide’, [diagram], *GCHQ*, 11 October. Available at: https://www.ncsc.gov.uk/guidance/cyber-security-small-business-guide-infographic (Accessed: 20 January 2018).

Ng, B-Y., Kankanhalli and Yunjie, X. (2009). ‘Studying users' computer security behavior: A health belief perspective’. *Journal of Decision Support Systems*. 46(4), pp815 – 825. Available at: https://doi.org/10.1016/j.dss.2008.11.010 (Accessed: 28 January 2018).

Ögütçü, G., Testik, O.M. and Chouseinoglou, O. (2016) ‘Analysis of personal information security behavior and awareness’, *Computer and Security,* 56, pp.83-93. Available at: https://doi.org/10.1016/j.cose.2015.10.002 (Accessed: 25 January 2018).

Pope, N.A.W (2018) Intent of the future of the Corps, *Facebook,* 28 July. Available at: https://en-gb.facebook.com/RSIGNALS/ (Accessed: 28 July 2018).

R SIGNALSa (2017) ‘The CADUCEUS programme – A Corps for the 21st Century’, *Royal Signals website*. Available at: https://royalsignals.org/rsi/wp-content/uploads/sites/6/2017/10/20170921-Master-of-Signals-Presentation.pdf (Accessed: 25 July 2018).

R SIGNALSb (2018) ‘Royal Corps of Signals – Leaders in the Digital Age’, *Royal Signals website.* Available at: https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-signals/ (Accessed: 28 July 2018).

RMAS (2018) ‘Royal Military Sandhurst: Preparing for excellence’*, MOD website,* Available at: https://www.army.mod.uk/who-we-are/our-schools-and-colleges/rma-sandhurst/ (Accessed: 18 July 2018).

Royal Navy, (2011) ‘Royal Navy cyber security strategy’, *Defence Intranet,* Available: http://defenceintranet.diif.r.mil.uk/libraries/4/Docs7/20150211.1/15_091_Royal%20Navy%20Cyber%20Strategy.pdf. (Accessed 8 June 2018).

Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research methods for*

business students, (5th Edn). Harlow, Essex: Pearson Education.

Schlienger, T., and Teufel, S. (2003) 'Information security culture – From analysis to change: Research article'*. South African Computer Journal*,31, pp.46 – 52. Available at: http://icsa.cs.up.ac.za/issa/2003/Publications/INFORMATION%20SECURITY%20CULTURE.pdf (Accessed: 27 July 2018).

Semple, R. (2015) *Army information sub-strategy (2015 – 2018).* Available at: https://www.army.mod.uk/documents/general/20151201_Army_Info_Sub_Strategy-EXTERNAL_V1.pdf (Accessed 1 Jan 2018).

Sharma, S., Warkentin, M. and Shropshire, J. (2015) 'Personality, attitudes, and intentions: Predicting initial adoption of information security behaviour', *Computers and Security,* 49, pp.177-191. Available at: https://doi.org/10.1016/j.cose.2015.01.002 (Accessed: 20 May 2018).

Sheng. S., Holbrook. M., Kumaraguru, P., Cranor, L. and Downs, J. (2010) 'Who falls for the phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions'. *Conference on human factors in Computing Systems*. pp.372 – 383, Available at: http://lorrie.cranor.org/pubs/pap1162-sheng.pdf (Accessed: 28 July 2018).

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information and Management*, 51(2), pp.217-224. Available at: https://doi.org/10.1016/j.im.2013.08.006 (Accessed: 18 July 2018).

Sniehotta, F.F., Presseau, J. and Araújo-Soares, V (2014) 'Time to retire the theory of planned behaviour', *Health Psychology Review*, 8(1), pp.1-7. Available at: https://doi.org/10.1080/17437199.2013.869710 (Accessed: 21 June 2018).

Solms, R.V. and Solms, B.V. (2004) 'From policies to culture', *Computers and Security,* 23(4), pp.275-279. Available at:https://doi.org/10.1016/j.cose.2004.01.013 (Accessed: 20 June 2018).

SPSS (2018) *'Cronbach's alpha to measure internal consistency/reliability using SPSS'*. Available at: https://www.de.sarupub.org/cronbachs-alpha-to-measure-internal-consistencyreliability-using-spss/ (Accessed: 31 July 2018).

Trobia, A (2011) *Encyclopedia of survey research methods*. (2nd Edn.). Thousand Oaks: Sage Publications, Inc. pp.169 - 170. Available at: http://dx.doi.org/10.4135/9781412963947 (Accessed: 15 June 2018).

Veiga, A.D. and Eloff, J.H.P. (2010) 'A framework and assessment instrument for information security culture', *Computers & Security,* 29(2), pp.196-207. Available at: https://doi.org/10.1016/j.cose.2009.09.002 (Accessed: 17 May 2018).

Veiga, D (2016) 'A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument', *2016 SAI Computing Conference (SAI)*, pp.1006-1015. Available at: https://doi.org/10.1109/SAI.2016.7556102 (Accessed: 20 June 2018).

Wahyudiwan, D.D.H., Sucahyo, Y.G and Gandhi, A. (2017) 'Information security awareness level measurement for employee', *3rd International Conference on Science in Information Technology: Case Study at Ministry of Research, Technology and Higher Education (ICSITech)*, Bandung, 25 – 26 Oct 2017, IEEE. Available at: https://doi.org/10.1109/ICSITech.2017.8257194 (Accessed: 28 July 2018).

White, G.B. (2011) 'The community cyber security maturity model', *2011 IEEE International Conference n Technologies for Homeland Security (HST)*, Waltham, MA, 15 – 17 November, pp.173-178. Available at: https://doi.org/10.1109/THS.2011.6107866 (Accessed: 25 June 2018).

Whitehouse (2009) *Remarks by the President on security our nation's cyber infrastructure,* White House, Available at: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (Accessed: 12 January 2018).

Williams, P.A.H (2008) ‘In a ‘trusting’ environment, everyone is responsible for information security’, *Information Security Technical Report*, 13(4), pp.207-215. Available at: https://doi.org/10.1016/j.istr.2008.10.009 (Accessed: 13 December 2017).

Wright, A. (2016) ‘Humans in cyber security – the weakest link’, [Blog] *IT governance Blog*, 13 April. Available at https://www.itgovernance.co.uk/blog/humans-in-cyber-security-the-weakest-link/ (Accessed: 1 January 2018).

Y. Zhou, Y. Zhou, S. Chen and S. S. Wu (2017) ‘Achieving strong privacy in online survey’, *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, 5-8 June,pp.710-719. Available at: https://doi.org/10.1109/ICDCS.2017.247 (Accessed: 19 July 2018).

APPENDICES

Appendix A – Literature Use for Research

Literature Themes	Relevant References
Cyber Security	Bayuk et al. (2012) * Defence Cyber Primer (2016) ° National Cyber Security Strategy (2015) °
Threat from Cyberspace	Crowell (2010) ° White House (2009) °
Cyber Security Awareness	Abawajy (2014) * Bullée et al. (2015) Choo (2011) * Brynielsson and Frank (2014) * ENISA (2016) ° Crannel, Moulton and Sheppard (2013) *
Factors affecting Cyber Security Awareness	Barford et al. (2010) * Aloul (2012) * Colwill (2009)
The Human Factor	Katz (2005) * Bulgurcu et al. (2010) * Kim et al. (2009) * MOD Cyber Primer (2016) ° Bada and Sasse (2014) * Howarth (2014) * Ögütçü, Testik and Chouseinoglou (2016)* Ng et al. (2009) * Gilovich and Kruger (2004) * Lebek et al. (2014) * Sharma et al. (2015) *

	Marks and Rezgui (2007) * Fielding, McDonald and Louis (2008) * Fang and Shih (2018) * Sniehotta, Presseau and Araújo-Soares (2014) * Harmon-Jones (2012) * Ward and Meade (2018) * Durlabhji and Fusilier (2005) * Schlienger and Teufel (2003) * Aloul, Darwish and Zarka (2013) * Sheng, Holbrook, Kumaraguru et.al. *
Cyber Awareness Measurement Framework	Neikerk and Solms (2013) * Lebek et al.(2014) * Ng et al (2009) * Ögütçü, Testik and Chouseinoglou (2016)* Parsons et al (2017) * Sharma et al (2015) * Galba et al (2015) * Kruger and Kearney (2006) * Solms and Solms (2004) * Deloitte (2012) * Cone et al (2007) * Abawajy and Kim (2010) * Carver et al. (2007) * Chen et al (2008) * Korpela (2015) *
Cyber Security Maturity Models	Hoang and Le (2007) * Carrali and Butkovic (2013) ° National Initiative for Cybersecurity Education (2014) ° Department of Homeland Security

	(2014) ° White (2011) *
MOD Doctrine and R SIGNALS	Defence Cyber Primer (2016)° UK Cyber Security Strategy (2011) ° Strategic and Defence Security Review (2010) ° Defence Intranet (2014) ⁑ Airforce Cyber Strategy (2014) ° Royal Navy Cyber Strategy (2011) ° ACIN 15/17 (2017) ⁑

NB. *denotes an academic paper, ° a white paper, and ⁑ another source (e.g., blog, newspaper article)

Appendix B – Survey Questionnaire

Title of the Project: A study of the cyber security awareness and use of protective cyber security practices in defence settings.

Research team: Sundar Sherchan, Victoria Smy

Contact Details: sundar.sherchan@cranfield.ac.uk, v.smy@cranfield.ac.uk

Aims and objectives:

This research that you have been invited to participate in examines key themes aligned to cyber security. More specifically, the research will examine your impressions of cyber security practice when working with computers within your typical work duties or at home. Your responses will be helpful in generating an overview of cyber practice and make recommendations to future training requirements. As such (and should you consent to provide your views), you are encouraged to answer questions as honestly as possible.

1. I understand that this research is being undertaken with a view to completion of an MSc.

2. I confirm that I have been informed about the aim and objectives of this research project and have voluntarily agreed to give my inputs.

3. I understand that my responses are recorded anonymously and I will not be identifiable in any of the research outputs.

4. I understand that the data collected will be kept in a secure location and used for the purposes of the project outlined.

5. I understand that my raw data will be accessible only to the Cranfield University research team, as outlined above.

6. I understand that no commercially sensitive or classified data will be collected, and that all written research outputs will be sanitised appropriately

7. I understand that I am free to withdraw at any point by simply closing the web browser.

Should you consent to take part in this research, please continue onto the questions that follow.

QUESTIONNAIRE

The next set of questions will be based on the demographics of the participants taking the survey.

1. Which age group do you fall under?

   Under 20

   20 -29

   30 – 39

   40 -49

   50 -59

2. What is your gender?

   Male

   Female

3. Are you a soldier or an officer?

   Soldier

   Officer direct entry

   Officer late entry

4. Which rank-range do you fall under?

Signaller – Corporal

Sergeant – Staff Sergeant

Warrant Officer Class 2 – Warrant Officer Class 1

Second Lieutenant – Lieutenant

Captain - Major

Lieutenant Colonel and above

5. Length of time served in the ROYAL SIGNALS.

<12 months

1-2 years

3-5 years

6-10 years

11-22 years

23 years and above

6. What is your trade?

Communications System Engineer

Communications Systems Operator

Supervisor

TOT or Traffic

Regimental Duties

Other, please describe [ ]

7. Have you taken part in any cyber security training? If so, how recently did you attend this training?

n/a – no cyber security training

In the past 12 months

In the past 2 years

Longer than 2 years ago

8. What is your highest level of education

GCSEs
A Levels
Foundation Degree
Undergraduate Degree
Postgraduate Degree

Other, please describe [ ]

The questions that follow tap into a number of cyber security practices and behaviours. These relate to both your work role and your personal (home, public) use of information technologies, unless otherwise stipulated. Please pick the response that most closely matches your thoughts and practices.

Likert FREQUENCY (F) scales

NEVER (1)	**RARELY (2)**	**SOMETIMES (3)**	**OFTEN (4)**	**ALWAYS (5)**

Question order	**Question**	**Theme**	**CODE** (for later data analysis)

Q10	1	How often do you carry out data backups for your work and personal files?	**Data Backup (1)**	**DBup-F1**
Q11	2	Do you utilise cloud storage facilities to back up your work/personal files?	**Data Backup (2)**	**DBup_F2**
Q12	3	Do you regularly test restoration of your backup data?	**Data Backup (3)**	**DBup_F3**
Q13	4	Do you switch on pin, password protection or fingerprint recognition on your mobile devices?	**Device Safety (1)**	**Safe_F1**
Q14	5	Do you keep your devices (and all installed apps) up to date, using the 'automatically update' option if available? (Applicable to your personal life outside of work)	**Device Safety (2)**	**Safe_F2_P**
Q15	6	Do you connect to Wi-Fi Hotspots when you need to send sensitive data?	**Device Safety (3)**	**Safe_F3** (negative coding)
Q16	7	Do you impose strict access rules for the use of removable media devices such as USB sticks and SD cards?	**Malware Defences (1)**	**MalD_F1**
Q17	8	How often do you send work/personal files using cloud storage?	**Malware Defences (2)**	**MalD_F2**
Q18	9	Do you use anti-virus software on all the	**Malware**	**MalD_F3**

		computers and laptops that you use?	**Defences (3)**	
Q19	10	Do you download third party apps from unknown sources? (Applicable to your personal life)	**Malware Defences (4)**	**MalD_F4_P** (negative coding)
Q20	11	How often do you check your protective firewalls are up-to-date??	**Malware Defences (5)**	**MalD_F5**
Q21	12	How frequently do you scan your systems for security breaches such as malware attacks? (Applicable to your personal life)	**Phishing Attacks (1)**	**Phish_F1_P**
Q22	13	Have you ever clicked on a potentially fraudulent website or link asking for your personal/financial information?	**Phishing Attacks (2)**	**Phis_F2** (negative coding)
Q23	14	How often do you check your emails for signs of phishing? Signs could be poor spelling and grammar, low quality logos etc.	**Phishing Attacks (3)**	**Phis_F3**
Q24	15	Do you report to your chain of command if you get an email asking for personal or financial information?	**Phishing Attacks (4)**	**Phis_F4**
Q25	16	Do you use two factor authentication methods when logging into a website containing sensitive data such as your bank accounts and work emails?	**Password Usage (1)**	**PUse_F1**
Q26	17	Do you change the manufacturer's default passwords that your devices are	**Password Usage (2)**	**PUse_F2_P**

		issued with? (Applicable to your personal life)		
Q27	18	How often do you use predictable passwords (such as family and pet names)?	**Password Usage (3)**	**PUse_F3** (negative coding)
Q28	19	How frequently do you keep some note of your passwords near to your devices?	**Password Usage (4)**	**PUse_F4** (negative coding)
Q29	20	Do you share your password with others?	**Cyber Behaviour (1)**	**Cyb_F1** (negative coding)
Q30	21	Do you voluntarily change your password regularly?	**Cyber Behaviour (2)**	**Cyb_F2**
Q31	22	Do you open email attachments from unknown sources without checking for viruses?	**Cyber Behaviour (3)**	**Cyb_F3** (negative coding)
Q32	23	Do you send sensitive information without checking that the 'https' prefix is present in the URL (web address)?	**Cyber Behaviour (4)**	**Cyb_F4_W** (negative coding)
Q33	24	Do you report poor security behaviour by your colleagues? (Applicable to work only)	**Cyber Behaviour (5)**	**Cyb_F5**
Q34	25	If you found a USB stick in public place, would you plug into your computer?	**Cyber Behaviour (6)**	**Cyb_F6** (negative coding)
Q35	26	Do you ever leave your personal	**Cyber**	**Cyb_F7_P**

		devices unattended when you are in public places? (Applicable to your personal life)	**Behaviour (7)**	(negative coding)
Q36	27	How often do you send work/personal files using email?	**Malware Defences (6)**	**MalD_F6** (negative coding)

Likert AWARENESS (A) scales

NEVER (1)	**RARELY (2)**	**SOMETIMES (3)**	**OFTEN (4)**	**ALWAYS (5)**

Question order		**Question**	**Theme**	**CODE**
Q37	1	Are you aware of the importance of data backup?	**Data Backup (4)**	**DBup_A4**
Q38	2	Are you aware that devices containing your backup data should not be permanently connected to the device holding the original copy neither physically nor over a local network?	**Data Backup (5)**	**DBup_A5**
Q39	3	Are you aware that cloud storage facilities allow you to access your data quickly from anywhere?	**Data Backup (6)**	**DBup_A6**
Q40	4	Are you aware that mobile devices can be configured to be tracked, remotely wiped or remotely locked when lost or	**Device Safety (4)**	**Safe_A4**

		stolen?		
Q41	5	Were you aware that VPN and 3G or 4G Connections are more secure than WiFi hotspots when sending sensitive data?	**Device Safety (5)**	**Safe_A5**
Q42	6	Are you aware that people with malicious intent may use shoulder surfing techniques to steal information from you?	**Device Safety (6)**	**Safe_A6**
Q43	7	Were you aware that personal devices such as smartphones and tablets used outside of the safety of home or office require more protection than 'desktop' equipment? (Applicable to your personal life)	**Device Safety (7)**	**Safe_A7_P**
Q44	8	Do you know it is important to replace devices that are no longer supported by manufacturers with more up-to-date alternatives? (Applicable to your personal life)	**Device Safety (8)**	**Safe_A8_P**
Q45	9	Are you aware it is important to protect your computer systems against malware (malicious software including viruses)?	**Malware Defences (7)**	**MalD_A7**
Q46	10	Are you aware that use of non-approved software on tablets and smartphones could be harmful for your devices and may increase the risk of attack from malwares?	**Malware Defences (8)**	**MalD_A8**

Q47	11	Are you aware that patches for software and firmware should be promptly applied with latest software updates provided by manufacturers and vendors using the 'automatically update' option where available?	**Malware Defences (9)**	**MalD_A9**
Q48	12	Were you aware that most operating systems come with firewall which can be used as protection between your network and public networks?	**Malware Defences (10)**	**MalD_A10**
Q49	13	Are you aware of how to report suspected security breaches at work? (Applicable to work)	**Phishing Attack (5)**	**Phis_A5_W**
Q50	14	Are you aware you must change your password as soon as you suspect a successful phishing attack has taken place?	**Phishing Attack (6)**	**Phis_A6**
Q51	15	Are you aware that phishing attacks are often conducted using fake emails and through links to redundant websites and carried out by asking for sensitive information?	**Phishing Attack (7)**	**Phis_A7**
Q52	16	Did you know that you can reduce the impact of phishing attacks by reducing personal use of work computers? (Applicable to work)	**Phishing Attack (8)**	**Phis_A8_W**
Q53	17	Are you aware you should report malware attack if you suspect a successful attack has taken place?	**Phishing Attack (9)**	**Phis_A9**

Q54	18	Are you aware that all laptops, MACs and PCs can use encryption products that require a password to load up?	**Password Usage (5)**	**PUse_A5**
Q55	19	Are you aware you should switch on your password, PIN protection or fingerprint recognition for mobile devices? (Applicable to your personal life)	**Password Usage (6)**	**PUse_A6_P**
Q56	20	Are you aware you should report to your IT department if your password is stolen or you suspect someone knows it? (Applicable to work)	**Password Usage (7)**	**PUse_A7_W**
Q57	21	Are you aware you can use a 'password manager' to store passwords for your less important websites and accounts? (Applicable to your personal life)	**Password Usage (8)**	**PUse_A8_P**
Q58	22	Are you aware of any negative consequences of reporting security breaches? (Applicable to work)	**Phishing Attach (10)**	**Phis_A10_W** (negative coding)

Finishing Questions

59. Do you perceive there to be any barriers to implementing cyber security practices within your job role? If so, please describe below.

60. Are you satisfied with the level of cyber security training you have received?

Satisfied
Somewhat satisfied
Neither satisfied or unsatisfied

Somewhat dissatisfied

Dissatisfied

61. What additional training, resources or support would you like to have access to?

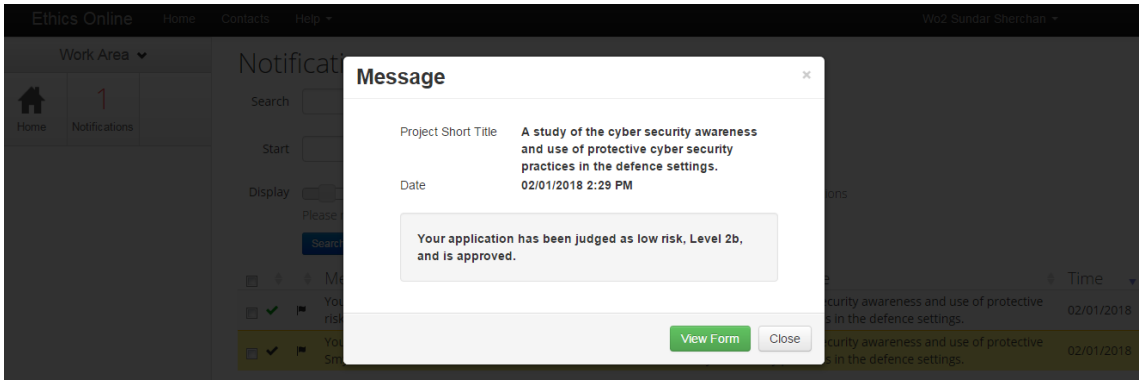
62. Do you have any further comments concerning cyber security? If so, please describe below.

DEBRIEF

Thank you very much for your time participating in this project. As mentioned earlier the data provided by you will be recorded anonymously.

Should you have any concerns or queries, please feel free to contact the research lead Sundar Sherchan (email: sundar.sherchan@cranfield.ac.uk, Mobile: 07917694955

Appendix C – Ethical Approval Email



Dear Sundar

Reference: CURES/3664/2018
Title: A study of the human perspectives on cyber security capabilities in defence settings.

Thank you for your application to the Cranfield University Research Ethics System (CURES).

Your proposed research activity has been confirmed as Level 2b risk in terms of research ethics. You may now proceed with the research activities you have sought approval for.

Please remember that CURES occasionally conducts audits of projects. We may therefore contact you during or following execution of your fieldwork. Guidance on good practice is available on the research ethics intranet pages.

If you have any queries, please contact cures-support@cranfield.ac.uk

We wish you every success with your project.

Regards

CURES Team

Appendix D – R SIGNALS Placement in Community Cyber Capability Maturity Model

Initial (reactive only) - 1-1.80 - n/a	
Advanced (lessons captured) **R SIGNALS average score between 1.81-2.60**	***FREQUENCY ITEMS:*** 3 - Do you regularly test restoration of your backup data? 8 - How often do you send work/personal files using cloud storage? 23 - Do you send sensitive information without checking that the 'https' prefix is present in the URL (web address)? ***AWARENESS ITEMS: n/a***
Self-Assessment (leader directed) **R SIGNALS average score between 2.61- 3.40** **N = 9 items**	***FREQUENCY ITEMS:*** 1 - How often do you carry out data backups for your work/personal files? 2 – Do you utilise cloud storage facilities to back up your work/personal files? 7 - Do you impose strict access rules for the use of removable media devices such as USB sticks and SD cards? 11 - How often do you check your protective firewalls are up-to-date? 12 - How frequently do you scan your systems for security breaches such as malware attacks? (Applicable to your personal life) 15 - Do you report to your chain of command if you get an email asking for personal or financial information? 21 - Do you voluntarily change your password regularly? 27 - How often do you send work/personal files using email? ***AWARENESS ITEMS:*** 22 - Are you aware of any negative consequences of reporting security breaches? (Applicable to work)

Integrated (role accountability) **R SIGNALS average score between 3.41-4.2** **N = 19 items**	***FREQUENCY ITEMS:*** 5 - Do you keep your devices (and all installed apps) up to date, using the 'automatically update' option if available? (Applicable to your personal life outside of work) 14 - How often do you check your emails for signs of phishing? Signs could be poor spelling and grammar, low quality logos etc. 18 - How often do you use predictable passwords (such as family and pet names)? 23 - Do you send sensitive information without checking that the 'https' prefix is present in the URL (web address)? 1 - Are you aware of the importance of data backup? ***AWARENESS ITEMS:*** 2 - Are you aware that devices containing your backup data should not be permanently connected to the device holding the original copy neither physically nor over a local network? 4 - Are you aware that mobile devices can be configured to be tracked, remotely wiped or remotely locked when lost or stolen? 5 - Were you aware that VPN and 3G or 4G Connections are more secure than WiFi hotspots when sending sensitive data? 6 - Are you aware that people with malicious intent may use shoulder surfing techniques to steal information from you? 7 - Were you aware that personal devices such as smartphones and tablets used outside of the safety of home or office require more protection than 'desktop' equipment? (Applicable to your personal life) 8 - Do you know it is important to replace devices that are no longer supported by manufacturers with more up-to-date alternatives? (Applicable to your personal life) 10 - Are you aware that use of non-approved software on tablets and smartphones could be harmful for your devices and may increase the risk of attack from malwares? 11 - Are you aware that patches for software and firmware should be promptly applied with latest software updates provided by manufacturers and vendors using the 'automatically update' option where available? 12 - Were you aware that most operating systems come with firewall which can be used as protection between your network and public networks? 13 - Are you aware of how to report suspected security breaches at work? 15 - Are you aware that phishing attacks are often conducted using fake emails and through links to redundant websites and carried out by asking for sensitive information? 16 - Did you know that you can reduce the impact of phishing attacks by reducing personal use of work computers? (Applicable to work) 17 - Are you aware you should report malware attack if you suspect a successful attack has taken place? 18 - Are you aware that all laptops, MACs and PCs can use encryption products that require a password to load up? 21 - Are you aware you can use a 'password manager' to store passwords for your less important websites and accounts? (Applicable to your personal life 20 - Are you aware you should report to your IT department if your password is stolen or you suspect someone knows it? (Applicable to work)

Vanguard (Co-evolving) **R SIGNALS average score between** **4.21-5** **N = 15 items**	***FREQUENCY ITEMS:*** 4 -Do you switch on pin, password protection or fingerprint recognition on your mobile devices? 6 - Do you connect to Wi-Fi Hotspots when you need to send sensitive data? 9 - Do you use anti-virus software on all the computers and laptops that you use? 10 - Do you download third party apps from unknown sources? (Applicable to your personal life) 13 - Have you ever clicked on a potentially fraudulent website or link asking for your personal/financial information? 16 - Do you use two factor authentication methods when logging into a website containing sensitive data such as your bank accounts and work emails? 17 - Do you change the manufacturer's default passwords that your devices are issued with? (Applicable to your personal life) 19 - How frequently do you keep some note of your passwords near to your devices? 20 - Do you share your password with others? 22 - Do you open email attachments from unknown sources without checking for viruses? 25 - If you found a USB stick in public place, would you plug into your computer? 26 - Do you ever leave your personal devices unattended when you are in public places? (Applicable to your personal life) ***AWARENESS ITEMS:*** 3 - Are you aware that cloud storage facilities allow you to access your data quickly from anywhere? 9 - Are you aware it is important to protect your computer systems against malware (malicious software including viruses)? 14 - Are you aware you must change your password as soon as you suspect a successful phishing attack has taken place? 19 - Are you aware you should switch on your password, PIN protection or fingerprint recognition for mobile devices? (Applicable to your personal life)