Journal of Systems and Information Technology, Volume 21, Issue 1, March 2019, pp. 2-35
DOI:10.1108/JSIT-02-2018-0028

Human Factor Security:

Evaluating the Cybersecurity Capacity of the Industrial Workforce

Uchenna Daniel Ani[1], and Hongmei He[2], and Ashutosh Tiwari[3]

[1,2]*Manufacturing Informatics Centre, Cranfield University, UK*

[3]*Department of Automatic Control and Systems Engineering, University of Sheffield, UK.*

Purpose - As cyber-attacks continue to grow, organisations adopting the internet-of-things (IoT) have continued to react to security concerns that threaten their businesses within the current highly competitive environment. Many recorded industrial cyber-attacks have successfully beaten technical security solutions by exploiting human-factor vulnerabilities related to security knowledge and skills, and manipulating human elements into inadvertently conveying access to critical industrial assets. Knowledge and skill capabilities contribute to human analytical proficiencies for enhanced cybersecurity readiness. Thus, a human-factored security endeavour is required to investigate the capabilities of the human constituents (workforce) to appropriately recognise and respond to cyber intrusion events within the industrial control system (ICS) environment.

Methodology - A quantitative approach (statistical analysis) is adopted to provide an approach to quantify the potential cybersecurity capability aptitudes of industrial human actors, identify the least security-capable workforce in the operational domain with the greatest susceptibility likelihood to cyber-attacks (i.e., weakest link), and guide the enhancement of security assurance. To support these objectives, a Human-factored Cyber Security Capability Evaluation approach is presented using conceptual analysis techniques.

Findings - Using a test scenario, the approach demonstrates the capacity to proffer an efficient evaluation of workforce security knowledge and skills capabilities, and the identification of weakest link in the workforce.

Practical Implications - The approach can enable organisations to gain better workforce security perspectives like security-consciousness, alertness, and response aptitudes, thus guide organisations into adopting strategic means of appropriating security remediation outlines, scopes, and resources without undue wastes or redundancies.

Originality/value – This work demonstrates originality by providing a framework and computational approach for characterising and quantify human-factor security capabilities based on security knowledge and security skills. It also supports the identification of potential security weakest links amongst an evaluated industrial workforce (human agents), some key security susceptibility areas, and relevant control interventions. The model and validation results demonstrate the application of action research. The study demonstrates originality by illustrating how action research can be applied within socio-technical dimensions to solve recurrent and dynamic problems related to industrial environment cyber security improvement. It provides value by demonstrating how theoretical security knowledge (awareness) and practical security skills can help resolve cyber security response and control uncertainties within industrial organisations.

Keyword:
Cybersecurity Evaluation, Workforce Security Capacity, Industry Control Environment, Human-Centred Security,

1 Introduction

Cybersecurity in industry control system (ICS) environments has become a growing issue of both national and global security over the last decade. The evolving information technology – operation technology (IT-OT) convergence now implies that organisations, firms, industries, and factories, embracing the much-acclaimed industry 4.0 and industrial internet-of-things (IIoT) paradigms, are reliant on IT infrastructures, open standards and technologies, and the internet (Knowles et al., 2015). It also means that these organisational platforms are susceptible to cyber threats, vulnerabilities, and attacks. ICS is an all-purpose (common) term used to describe various types of automated industrial systems that control, monitor, and manage industrial processes (Macaulay and Singer, 2012; Stouffer et al., 2015). An Industrial Control System Environment (ICSE) refers to a domain where industrial control operations and processes are performed. The basic functions of an ICS involve: sensor measurements, hardware control for actuators (breakers, switches, monitors), human-machine interfacing, and remote diagnostics and maintenance utilities (Amin and Sastry, 2015) (Nicholson et al., 2012).

The modern ICS and it's development trends enable great business and operational profitability, an inevitable array of security susceptibilities are as well introduced, which threaten the functional reliability of operations in the industrial domain (Abe et al., 2016). Over the last years, records continue to show an alarming increase in cyber threats and attacks against ICSs globally.

The attack landscape against ICSEs have strikingly widened with remarkable dynamic patterns of attack vectors (Luallen, 2014; Brassso, 2016; Harp and Gregory-Brown, 2016; Paganini, 2016). Industrial cyber security, SCADA security, etc, are now buzz words for common topics of conversations amongst everyday industrial technology users (Evans *et al.*, 2016), and have become necessities towards normal operations in the industrial domain. Technically, security in IT is fairly standardised and differs from how it applies to ICS. The differences between the two chiefly border on operational requirements and prioritisation (Macaulay and Singer, 2012). Unlike the IT, most ICS security compromises have associated physical consequences and impacts. These are often more severe and abrupt than in the IT domain. Security issues in the ICS environment often appear in the form of habitual maintenance failures and other process anomalies, which make difficult the diagnosis and resolution of the issues. The main reasons for the difficulty of managing the security of ICSE include: vastly dispersed assets with frequent compulsory remote access requirements, traditional IT security applications such as antiviruses and firewalls may not be suitable for compatibility issues, and when possible, application could affect system availability which is not acceptable for ICS as a high-availability system. Older ICS systems are often not open to patching or upgrades. (Macaulay and Singer, 2012; Drias, Serhrouchni and Vogel, 2015). Cyber security threats to ICS encompass threat vectors like non-typical network protocols and instruction sets that cannot be blocked for operations, performance, and safety reasons (e.g. event and alarm traffics). More contextually, technical security control may well be easily subverted by intelligent adversaries who can easily deceive unaware, unskilled, and unsuspecting ICS operators and users into undertaking actions and activities that can grant the attackers easy access and high privilege capacities to execute their malicious intents. These are often also undetectable by security alert systems until serious damages and anomalies begin to emerge (Johansson, Sommestad and Ekstedt, 2009; Fan *et al.*, 2015).

As cyber-attacks exacerbate, organisations have become concerned about how to react to security trends that threaten their business and operational relevance within the current highly-competitive business environment. Many recorded industrial cyber breaches have effectively beaten technological security solutions through exploiting human-factor limitations in knowledge and skills. These attack patterns have manipulated human elements into unintentionally conveying access to critical industrial assets. Cyber security has indeed become a necessary objective to achieve uninterrupted industrial functions in a changing operational technology environment. One way of defining cyber security is 'the harmonisation of capabilities in people, processes, and(or) technologies; to secure and control both authorised and/or unlawful access, disruption, destruction, or modification of electronic computing systems (hardware, software, and networks), the data and information they hold' (Ani, He and Tiwari, 2016). However, most current security solutions are technology-inclined. People and process security contexts and requirements are often not considered (Ramakrishnan and Testani, 2011), often resulting in lopsided security that are malignantly exploited by malicious intelligent actors.

An ICS is a system of industrial technologies and infrastructures built and(or) operated by people (workforce) for the execution of processes towards attaining target products or services. It implies that securing technology (hardware and/or software) alone resolves only a fraction of the larger security problem. A technology is often as weak and vulnerable as the people (workforce) that develop and(or) operate it, and the process(es) designed and structured to use it. For example, suppose Alice is a process engineer that operates an engineering workstation asset of an ICS, and employs technology 'A' firewall and technology 'B' Intrusion Detection System (IDS) to protect her workstation from security compromise. Assuming Alice is unaware and unable to recognise various forms and signatures of social engineering attack schemes. Bob as an intelligent and predetermined attacker employs a deceptive spear-phishing means unknown to Alice and deceives her into clicking or running links or attachments on her workstation that literally enables a backdoor (entry point) into Alice's system and network via a direct remote access. This happens seamlessly despite the presence and functionalities of techs 'A' and 'B' security features. Alice's security ignorance, her uninformed and unskilled state in relations to evolving ICSE security trends such as confronted her, and her consequent actions or inactions undervalues techs 'A' and 'B'; opening the door to an enemy attacker Bob.

The above theoretical scenario highlights the importance of human-factors in ICSE cyber security assurance, especially emphasising the significance of security knowledge (awareness) and practical skills. Human-factor is as important as technical factors in ICSE security. Real scenarios also consolidate this viewpoint. Probably,

the agents of the 2013 Stuxnet attack had the challenge of penetrating the Iranian Nuclear Power plant network since the network was air-gapped from external networks. Thus, the attackers used infected USB drive parking lot attack technique on a third party maintenance organisation, and relied upon human actors connecting the infected devices to their industrial network and provide means for reaching and delivering Stuxnet to the nuclear plant network (Murphy, 2015). Earlier works on the concept of security competence (capability) by Workman et al (2008), which investigated the "knowing-doing" gap in individuals showed that such individuals can have appropriate security skills and knowledge yet not apply these skills in consistent manner. Also, based on the analysed results of 588 workforce members of a technology service company, Workman et al (2008) concludes with the recommendation that security technology should be user-centred to avoid assessment tensions that can affect responses.

Probable motivations for these attacks may have stemmed from the perception that: (i) most ICSE workforce (personnel) are often unfamiliar with advanced digital (cyber) security concepts, and (ii) Information Technology security workforce are often unfamiliar with ICSE operational concepts, and (iii) intelligent attackers now consider human actors (workforce) within the industrial environment as weak attractive exploit targets into operational system and networks (Howarth, 2014). The bid improve security in the ICSE through plugging the holes enumerated above provides motivation for engaging this research direction. Updated security awareness and training can increase security capabilities, thus, presents a viable solution to this issue. However, engaging proper security capabilities hinges on an adequate understanding of recurrent security capacities of the workforce, and a clear outline of areas of weaknesses and strengths. Effectively improving security capacities of a workforce will typically require building strengths in the identified weak areas.

This work builds up on an earlier work on evaluating an industrial environment's security capability based on the quantification of inherent cybersecurity knowledge and skills of the human workforce. Improvements are introduced I the aspect of computationally evaluating and inferring security incapability (vulnerability/susceptibility level) of human-agents from their evaluated capability. This simplifies the process of characterising weak links amongst the workforce members involved. Thus, this study highlights the importance of evaluating workforce security capacities, identifying the weakest security capability member in the workforce (weakest link), and the culminated significance of this approach towards overall security assurance. Understanding the measure of cybersecurity knowledge and skill capacities of the industrial workforce, and keeping abreast with the newest activities and trends in the cyber threat landscape can support the identification of attacks before they happen. As new threats continue to emerge, learning the capability postures of the workforce, determining specific gaps, and plugging into the gaps with the right intelligence, all add-up a potential to minimize damages if a security breach occurs (Mandiant, 2017). In an ICSE, human elements are critical assets and should form a line of defence against security threats. Effectively consolidating security and defence capacities of these elements can be most effective following an understanding of the current security capability and vulnerability levels. This will support informed control applications.

This work aims to provide a human-centred security capability and vulnerability evaluation method which can be used to evaluate the security aptitude of human agents within ICSE. This evaluation approach complements traditional technical capability and vulnerability analysis, thus enables a wider view of vulnerability assessment of an industrial environment where both technology and human agents are involved. More specifically, it explores how to understand and attribute quantitative ratings to security aptitudes of human agents in ICSE, and use such information to drive a robust industrial cyber security responsiveness and resilience. The approach and measures can be useful to security auditors, analysts, managers and industrial system owners in carrying out human-level threats and vulnerabilities assessments, identify most vulnerable human agents, as well as the areas where security is low. Responding to these, can significant influence improvement of overall organisational security. The contribution of this article includes; providing a novel approach for characterising and quantifying human-factor security capabilities based on security knowledge and security skills. It also supports the identification of potential security weakest links amongst an evaluated industrial workforce (human agents). It involves concept description and capability evaluations was associated with defined security standards, guidelines, and baseline requirements. The methodology then prescribed control interventions that are based on discovered weak links and weak security areas.

The rest of the paper is outlined as follows: Section 2 discusses human-factor security issues and requirements, and statistical justifications for the need of human-factored approach to ICS security. Section 3 presents a review of related works in capability evaluations relating to contexts, methods, and tools. Sections 4 presents an overview of the proposed workforce capability evaluation model. Section 5 discusses the validation scenario

adopted, the corresponding outcome and discussions. Sections 6 presents the conclusion and future work in the research.

2 Human-Related Security Issues and Requirements

As cyber-attacks continue to evolve, businesses and organisations have not ceased to express and react to security concerns that threaten their business and operational relevance within the currently highly-competitive business domain (Ralston, Graham and Hieb, 2007; Mirashe and Kalyankar, 2010). Many organisations keep updating technologies equipped with defensive capacities to protect automation processes from cyber intrusions or breaches. Notwithstanding, cyber-attacks and incidents against industrial control environments have continued to rise for couple of reasons. The most important is the reality of a drastic change in targeted vectors of attacks (Knowles *et al.*, 2015). While organisations continue to invest heavily on technology security, attackers have strategically side-tracked attack concentration from technology to people (human) assets (IRM, 2015), since humans (users) typically need to interact with technologies to initiate, implement, and/or manage industrial processes. Somehow, recorded events clearly demonstrate that the analytical proficiencies of the human constituents through the exploitation of cognitive capacities are still crucial for effective security in ICS environment (Chen *et al.*, 2012; Gonzalez *et al.*, 2014; Ben-Asher and Gonzalez, 2015). This is enabled by the existence and expression of easily exploited human weakness in the system process interaction loop. For instance, the analysis of the 2013 data breach against Target Corporation showed that Target's security technology was capable of detecting the breach, but the people (leaders and general employees) who should have been able to take appropriate responses to control the attack impacts, lacked the necessary skills and knowledge (Hershberger, 2014). The attack caused a disaster that cost Target about $148 million, and other financial institutions about $200 million (Tobias, 2014). If Target had proactively evaluated the cybersecurity capability of its workforce and understood the potential knowledge and skills strengths and weaknesses much earlier, such episteme would have spurred the corporation to improve security capability of their workforce in relations to cyber-security awareness, self-protection, organisational preservation, and a security conscious and cultured attitude, and cyber incident response.

Weak cybersecurity *knowledge* and *skills* in the workforce and leadership have become apparent to top the list of several human vulnerabilities in the minds of corporate decision makers, governments, and academic researchers (Adams and Makramalla, 2015). These have been quite dominant in the list of successful attack drivers in the industry. A study indicates that 20% of frightful security breaches in 2015 were attributed to decisive misuse of infrastructure assets, and 31% due to human errors (IRM, 2015). Stolen credentials through phishing accounts for 80% of data breaches (Debo, 2015). Spear Phishing attacks have also topped security concerns for enterprises, accounting for an average loss of $1.6 million, impacting loss of employee productivity (43%), financial losses (32%), damage to company reputation (29%), damage to brand reputation (27%), and loss of intellectual property (25%) (CLOUDMARK, 2016). Such precarious situations continue to press on industries and organisations due to a lack of inadequate understanding of the security capacities of operational workforce, and failure to provide operational staff (humans) with effective and up-to-date cybersecurity knowledge and skills capability to defend against cyber-attacks (Ashford, 2016).

These records suggest that despite any huge investments in technology security solutions to safeguard ICSs, human-factored security characteristics still play very significant roles towards achieving a holistic cyber security posture and assurance. These records and their implications to overall security within the ICS environment clearly support the motivation to explore potential solutions. Knowledge and skills security characteristics are particularly important. The statistics further suggest that the value of an organisation's chief security asset is more in its people – human constituents (workforce), than in technologies or laws and regulations (Navarro, 2007), and also points to humans as being potentially the weakest links (Kaspersky-Labs, 2015) in the ICS operation chain. The success of any security venture is eventually dependent upon the human element – people are both the most significant resource and potentially the major threats to security (PA Consulting Group, 2015). Eventually, a system or an organisation is as weak as its weakest link asset (Russell, 2002; Navarro, 2007). In the ICS environment, these weak links are characterised by industrial control system personnel, such as operators, technicians, experts, and enterprise/corporate users, whose population often outnumber the population in a security and non-security-oriented classification of the workforce (Robert, 2015). These people are typically unfamiliar with digital security concepts, and less keen about the importance of cybersecurity trends and practices, but more on operational performance trends (PA Consulting Group, 2015). This often puts greater demand/responsibility for assuring security on a relatively fewer numbered cybersecurity professionals, compounding their workload. The volumes, variety, and target multi-directivity of attacks patterns also down-plays the capability of cybersecurity professionals to directly

and completely exert control on all forms of attacks that target the industrial environment. Besides, the non-security-savvy ICS workforce seem to be predominantly targeted than the security experts. The former often lack adequate skill capacity for effective response, and sometimes lack updated knowledge as well. Thus, cybersecurity knowledge and practical security response skills are two key attributes of workforce security capability, considered invaluable for achieving a secure industrial operating environment. However, the effective input of security knowledge and skills should be built on; a clear understanding of existing measures of capability, and the identification of capability shortfalls that reveal user vulnerabilities (weaknesses) to cyber attackers. This can only be achieved through evaluations.

A human-involved approach is required to supplement existing technical-based security approaches towards an overall cyber security assurance. Badie and Lashkari (2012) categorised the factors that affect the security of computing systems into two: (i) human factor and, (ii) organization factor. According to the researchers, earlier works indicated that of these two categories, the human factor seemed the most important. A human-factored security endeavour is required that can improve the capabilities of the operational technology human constituents, so that they can appropriately recognise and respond to cyber intrusion events within the ICS environment. Quantitative analysis could provide an easy approach to evaluating the security capability of a user in relations to cyber-attacks, as it can help both senior managers and general infrastructure users to intuitively understand the status of their cybersecurity capability. Quantitative approach also simplifies result presentation and interpretations. Quantitative approaches allow for consistent results, the production of trend interpolations and forecasts, quicker situational understanding for decision-making, and the further representation of results in better understood formats like charts, graphs, and tables for time-critical decision-making. These are necessary to improve security posture and assurance within the industrial operating environment, without which top management is unable to retain high degrees of confidence about the security of their industrial asset (Evans *et al.*, 2016).

3. Related Works

The assessment of cyber security capability of human agents (workforce) is quite helpful towards achieving an efficient workforce security consciousness (Navarro, 2007). There are few researches which explored this area to propose schemes for assessing cybersecurity postures from the workforce perspectives.

A Human Factor Vulnerability Analysis (HFVA) framework is presented by Kraemer & Carayon (Kraemer and Carayon, 2003). The framework presents a three-stage process (identification, analysis, and solution) for determining human-factor vulnerabilities connected to technical vulnerabilities. The framework is presented as a process that follows a system/network-wide technical audit conducted after the discovery of technical vulnerabilities that bear human-factor underpinning. The HFVA model is limited in that it depends on the existence of technical vulnerabilities, and evaluates how well human network administrative experts are able to classify and appropriate respond to technical security vulnerabilities. Thus, it assumes human-factor vulnerabilities to be solely dependent on technical vulnerabilities. This is not entirely true with changing attack patterns, where social engineering attacks forms are employed to exploit and compromise systems and networks even when clear technical vulnerabilities have not been identified. The human agent itself is an asset that can have exploitable vulnerabilities, and can be independent of any technical vulnerabilities.

Human agents with varied levels of knowledge and experience in cyber security can demonstrate different perceptions of cyber security. Typically, higher security proficiencies imply better capability as experience can influence decision-making capability levels (Asgharpour, Liu and Camp, 2007). Advanced knowledge and previous experience could enhance the sensitivity to security threats and the performance of incident response. The researchers in (Goodall, Lutters and Komlodi, 2009) highlighted that domain knowledge in information and network security, as well as situated environmental knowledge grounded in an analyst's unique environment; are required to boost the expertise for effective intrusion detection by an analyst. The domain knowledge includes: theoretical knowledge acquired through formal education, training, or certification (Chi, 2006), and practical knowledge cultured through hands-on practice and experience with tools, methods of operation, and work- flows. The situated environmental knowledge is acquired through continued interactions with a specific operating environment (Goodall, Lutters and Komlodi, 2004). Researchers have used interviews and questionnaires to drive easy understanding of both mental models and security workforce workflows (D'Amico and Whitley, 2008; Paul and Whitley, 2013).

Wang (2013) explored an assessment of cyber security knowledge and behaviour using an anti-phishing scenario. The study investigated the relationship between evaluated users' knowledge of cyber security risks

and solutions (in relations to phishing), and their attitude and intention towards adopting and using cyber security solution. The outcome showed a positive correlation which implied that the extent of security knowledge influenced the attitude and intention towards adopting cybersecurity solutions. Another significant finding indicated a positive correlation between direct assessment answers and self-assessment responses. Wang (2013) also recommended security training and assessment tools surveys and questionnaires.

The Cybersecurity Capability Maturity Model (CCMM) (Christopher et al., 2014) describes an assessment framework, consisting of a set of characteristics, indicators or patterns that embody capability and progression which can be contextualised to various disciplines. CCMM provides a flexible guide to help organisations establish and enhance their security capability using corporate-level abstractions. More common studies focus on the impacts of human perception (Bulgurcu, Cavusoglu and Benbasat, 2010; Siponen, Adam Mahmood and Pahnila, 2014), attitudes, and behaviour (Parsons et al., 2014; Evans et al., 2016) to organisational security capacities, and policy implementations. These works have emphasised the relevance of social human attributes to effective security outcomes and performances. While these attributes are quite relevant and influential in deriving security conclusions in terms of capacities and controls, security knowledge and skill levels of individuals can influence the outcome of each attribute. Thus, it is rational to consider the primary influencing factors and how they impact resulting security capacities and controls.

Beautement et al (2016) argued that effective security management required that security managers were able to evaluate the effectiveness of prescribed policies, as well as the impact of employee behaviour. They proposed a Productive Security (ProdSec) methodology for aggregating huge datasets on employee behaviour and attitudes using scenario-based surveys. The approach was designed to ensure repeatable and scalable data collection, from which better insights can be deduced about security-related issues facing employees, their response behaviours, and attitudes. Results indicated that that business area, age, and geographical location, all provide axis of differentiating response maturity levels of employees, as well as intra-population group of employees. Details as these can influence efficient planning of future trainings, communications, and policy-making. It can also support proactive targeted interventions (remediation) on specific employees, which can save from inclusions in non-targeted interventions and reduce the expense on employee compliance budgets (Beautement, Sasse and Wonham, 2009).

Ben-Asher and Gonzalez (2015) investigated the security capacity differences between security experts and novices within an organisational setup. The study evaluated the expertise of cyber security analysts with specific application to intrusion detection, and the use of intrusion detection systems (IDS). Using emulated scenarios, the researchers used the IDS response approach to evaluate the general performance of both expert and novice security analysts outside conventional operational environments. The outcome showed that experts performed slightly than novices. Results also suggested that theoretical knowledge as being completely independent of practical knowledge. The dissociation was more noticeable in the expert analysts' group than in the novice group.

Generally, the use of quantitative tools and measures of performance relating to intrusion detection scenarios provided an effective means of evaluating and characterising security control capacities of the expert groups as desired (Ben-Asher and Gonzalez, 2015). Quantitative analysis could provide an easy approach to evaluating the security capability of a user in relations to cyber-attacks, as it can help both senior managers and general infrastructure users to intuitively understand the status of their cyber security capability. A quantitative approach also simplifies result presentation and interpretations. Quantitative approaches allow for consistent results, the production of trend interpolations and forecasts, quicker situational understanding for decision-making, and the further representation of results in better understood in formats like charts, graphs, and tables for time-critical decision-making. These are necessary to improve security capacity and assurance within the industrial operating environment, and without which top management is unable to retain high degrees of confidence about the security of their industrial asset (Evans et al., 2016). This work provides the baseline for our research and contribution.

Some clear points picked from the above reviews include security capabilities can be evaluated through interviews (structured and semi-structured) (D'Amico et al., 2005), questionnaires (Botta et al., 2007), observations and gamifications (Paul and Whitley, 2013; Adams and Makramalla, 2015; Ben-Asher and Gonzalez, 2015), penetrations testing (Aloul, 2012), etc. While a body of works exists around understanding the security posture of organisations, there is little research that has proffered a clear quantitative scheme for evaluating and attributing security capacities to individuals within an organisation, and use such individual

aggregations to derive overall organisational security capability. The CCMM scheme focuses on organisation-wide dispositions rather than workforce-focused dispositions.

Cyber security knowledge and practical security response skills are two direct attributes of workforce security capability which are invaluable towards achieving a secure industrial operating environment. These can be quite distinct as well. However, the effective input of security knowledge and skills should be built on; a clear understanding of existing measures of capability, and the identification of capability shortfalls that reveal user vulnerabilities (weaknesses) to cyber attackers. This can be achieved through evaluations. Existing researches on security performance evaluation of human agents within organisations typically focused on comparative analysis of security perceptions, with emphasis the security staff (analysts) who had the duty of securing a system. There is no research on other operational human agents such as found in the ICS domain and their performance and contribution to overall system security. We have not yet seen research in identifying potential workforce's weakest links, potential weak security capability areas, and the discrete but informative adoption of security measures. This work will fill the gaps.

4. Proposed Evaluation Model

The lack of familiarity with digital security concepts observed in ICS workforce opens a great deal of security vulnerabilities that could be easily exploited through social engineering by intelligent intruders. These adversaries exploit human characteristics and attitudes, such as ignorance, desire for gain, rewards, being helpful and responsible to coax actions, and (or) inactions from targeted workforce, to enable non-resistant access to systems and infrastructures, which could otherwise yield resistance when and if accessed directly. The number and capability of organisation-resident cybersecurity professionals, who have responsibility for system security in an enterprise is typically inadequate to completely protect the organisation. Every single ICS OT personnel presents an equal access point to the ICS, and the defence capacity of each ICS personnel contributes to an overall security status.

4.1 Security Capability

In this study, workforce security capability is considered as the combined, normalised, and (or) harmonised expression of security proficiencies in knowledge (domain and situational) and practical skills of a human agent (user) for appropriate actions, reactions, and (or) inactions for effective security of operational systems. Thus, industrial workforce security capability is modelled in terms of their knowledge and skill levels. These two attributes are considered as dominant factors in the security proficiency of operators in the ICS environment. Security knowledge level is defined as the measure of theoretical information that an individual has about cyber threats, vulnerabilities, attack patterns and impacts on a host system. Skill level outlines the ability to use accrued hands-on techniques and(or) tools to detect or recognise cyber-attack attempts, patterns and techniques, and to respond timely with appropriate countermeasures. Knowledge and skills in digital security concepts, evolving threats, vulnerabilities, attack intelligence, and the practical security response skills of each ICS personnel, allow a better understanding of the inherent security level of the entire workforce in an industry enterprise. This will help create the essential threshold of organisational security.

ICS workforce typically include IT security experts, IT operations personnel, and OT personnel (field operators, automation engineers, SCADA and telemetry engineers, corporate management, etc). All of them contribute directly and (or) indirectly, actively or passively in control system process activities, and their individual security capabilities contribute directly and indirectly to the threshold of general workforce security capacity. The threshold of general workforce security capability refers to the harmonised security status-derivative in relations to all evaluated workforce security capabilities in the organisation. Thus, the commitment of workforce to protecting an organisation and operational infrastructure is a critical factor of a strong cybersecurity defence. The approach of appraising and enhancing workforce cybersecurity capabilities as a means of emphasising a positive security culture is necessary. As knowledge levels indicate the degree of awareness to potential cybersecurity threats, vulnerabilities, attacks patterns, and damaging impacts, the evaluation of knowledge seeks to verify if, and how much an individual is acquainted with prevailing ICS security trends and intelligence in a specific working environment. It is an attempt to ascertain (and to what degree) if the industrial workforce knows what to do, and (or) what not to do to guard against successful breaches from cyber-attacks.

In contrast, skill levels can help build the ICS personnel some degree of practical social and technical strengths for hands-on, efficient and appropriate actions and reactions to potential security attacks, such that industry workforce is able to prevent cyber-attacks or mitigate attack impacts. Thus, cybersecurity capability evaluation

should encompass information gathering in all aspects of security relating to ICS safety, availability, integrity, confidentiality, and accountability. Assessment scopes should cover typical areas such as personnel security responsibilities, prevalent attack patterns, signatures, and appropriate response modes, adherence to adopted security policies, standards, and best practice solutions, samples of ICS security failures and impacts, updated security threat and vulnerability intelligence, and observed/discovered capability gaps in individual personnel, security initiative, and adherence to global standards (Parsons *et al.*, 2010; PA Consulting Group, 2015).

4.2 The Weakest Link

The statistics enumerating the successes of cyber incidents influenced by the ability of attackers to easily con human actors to behave or respond inappropriate to attack and compromise scenarios within their work domains add to the evidence that suggests that human actors are potentially the weakest links (Ashford, 2016). Clearly, all other things being equal including well instituted technical security measures, the record of cyber incidents described in section 2 also demonstrate facts that intelligent attackers motivated by potential financial gains tend to direct their malicious effort toward less-protected targets (Pan, Zhong and Mei, 2015). The attackers aim to compromise potential targets (human actors) with poor or weak abilities to defend infrastructure and information systems from attacks. "The weakest link" refers to the most poorly protected asset. "The weakest link" asset has become a key factor to determine the security level of the chain. If these corporations want to improve the security level of the whole information systems and optimize security chain integration, they must improve the security level of "the weakest link" (Pan, Zhong and Mei, 2015) . The question left to be answered remains; how to find the weakest link?

An attempt to address this is demonstrated in a previous work (Ani, He and Tiwari, 2016) from a human-factor security perspective. An approach is proffered for identifying the weakest link in security capability of ICS human workforce. *'Humans',* also referred to as *'workforce',* often present the weakest link in an operational security chain (Mitnick and Simon, 2003), and an organisation security capacity is as weak as its weakest link. Understanding workforces' security capabilities inferred from knowledge and skill measures, deriving a workforce-focused organisational security posture, and the identification of specific most vulnerable workforce constituents (weakest link) in the system are important for evaluating an overall ICS security posture (Bulgurcu, Cavusoglu and Benbasat, 2010; Aloul, 2012; Pan, Zhong and Mei, 2015). A weakest link refers to the personnel with least knowledge and practical proficiency in security for the implementation of ICS security objectives. Essentially, the weakest link is the least security-capable individuals in the operational domain, who demonstrate the highest likelihood of becoming victims of cybersecurity attacks (Aloul, 2012; Vishwanath, 2016). Such human elements represent the easiest attack vectors, and provide the weakest penetrable entry point to a system irrespective of whatever other safeguards in place. Identifying these weakest points through evaluation presents an essential line of action towards security assurance. Identifying and strengthening weakest links is equivalent to raising the bar of security capability of an organisational workforce. This work explores further this concept of human security capability evaluation (Ani, He and Tiwari, 2016), and proposes a quantitative approach to characterising workforce security capability, and identifying potential weak-links in an ICS operational domain. It also explores how the security weaknesses of the workforce members can influence the implementation of a priority-driven control strategy.

4.3 The Model

As an extension of prior work on human cybersecurity capability evaluation (Ani, He and Tiwari, 2016) where organisational security level is derived from the combined average for knowledge and skills security capacity for all human actors within an evaluation context. Further research has proffered more clarity and rational against initial assumptions that capabilities in individuals are interdependent such that average values can be used to represents a harmonised overall security capacity. It is more rationale to view each user as independent and a potential entry point into the system irrespective of the presence of others. Thus, an improvement in the weakest link attribute is introduced to the capability evaluation process where harmonised security capability ratings implicitly express measures of weakness or susceptibility to attacks. The collection of varied values in a set of capability ratings is indicative of the varied, independent susceptibilities or weak points that can allow successful cyber-attacks. The multiplicity of capability values indicates the variety of potential attack surfaces, and implies the multiplicity of corresponding human vulnerability weak-points for possible initiation and (or) accomplishment of cyber-attacks. In a set of capability rating scores, higher values suggest higher defensive surfaces and lesser vulnerable surfaces in relations to a defined security baseline, and vice versa.

The concept of security defence combined with vulnerability baselines, and the quantitative representation could support easy and clear identification, articulation, and attribution of potential weak-links. The least

capability value together with its corresponding vulnerability rating suggests the most vulnerable surface, and points to an associated human actor (user) with the greatest likelihood of successfully falling for a human-factor cyber-attack event. Hence, represents the weakest link. The new evaluation scheme presents a five-stage activity process of evaluating workforce cybersecurity capability, which include: *definition, data collection, formulation, representation,* and *attribution* as presented in Figure 1. Each stage provides a list of sub-stages, which form an overall security capability evaluation of ICS workforce.

4.3.1 Definition

This involves the definition of knowledge and skills security capability requirements, and the outline of desirable security capability baselines.

A. Security requirements

Workforce security evaluation should be built upon defined security policies and requirements, compliant with relevant standards and best practices, and contextual objectives of the specific operational environment. There exist several standards focusing on security in the ICSE, most of which are domain-specific, and do not cover all ICS types, security functionalities and requirements. For instance, the UK '10 Steps to Cyber Security' guideline (UK-Cabinet-Office, 2012), NIST SP 800-53 Revision 4 - guidance on security and privacy controls for systems and organisations (NIST, 2013), NIST SP 800-82 Revision 2 - guide on industrial control system security, etc., all have sections that advise on requirements and guidelines regarding personnel security awareness and training. Combining recommendations from these standards can provide a better reference for situational security requirements to guide capability evaluations considering the specific features of the system/environment under consideration.

B. Security Baseline

Security baseline defines desirable the status of the metrics/measures, representing varied capabilities and their corresponding attribute ratings from security requirements. It can be considered as the point of ideal capabilities of all workforce members. Any status lower than this ideal capability is considered a non-ideal capability.

In the proposed model, a capability ratio is introduced with value range of [0, 1]. We adopt the FIPS 199 (NIST, 2004) security categorisation recommendations to define three levels of capabilities: low, moderate, and high levels. For this, a three-group ratio is defined where a one-step incremental ratio is used to derive respective upper bounds: 1/3, 2/3, and 3/3 for the three levels (low, moderate, and high) within the defined range 0-1 as earlier prescribed. The capability ranges for the three groups/levels of classification are presented in Table 1. This capability ratio is used to provide capability categorisations for which the workforce and their associated capability evaluation values that would be classified. This way, human agent security capacities are grouped according to closely related scores/ratings to indicate the personnel that share similar of very close capability traits and proficiencies, and to support better decision-making on appropriate responses.

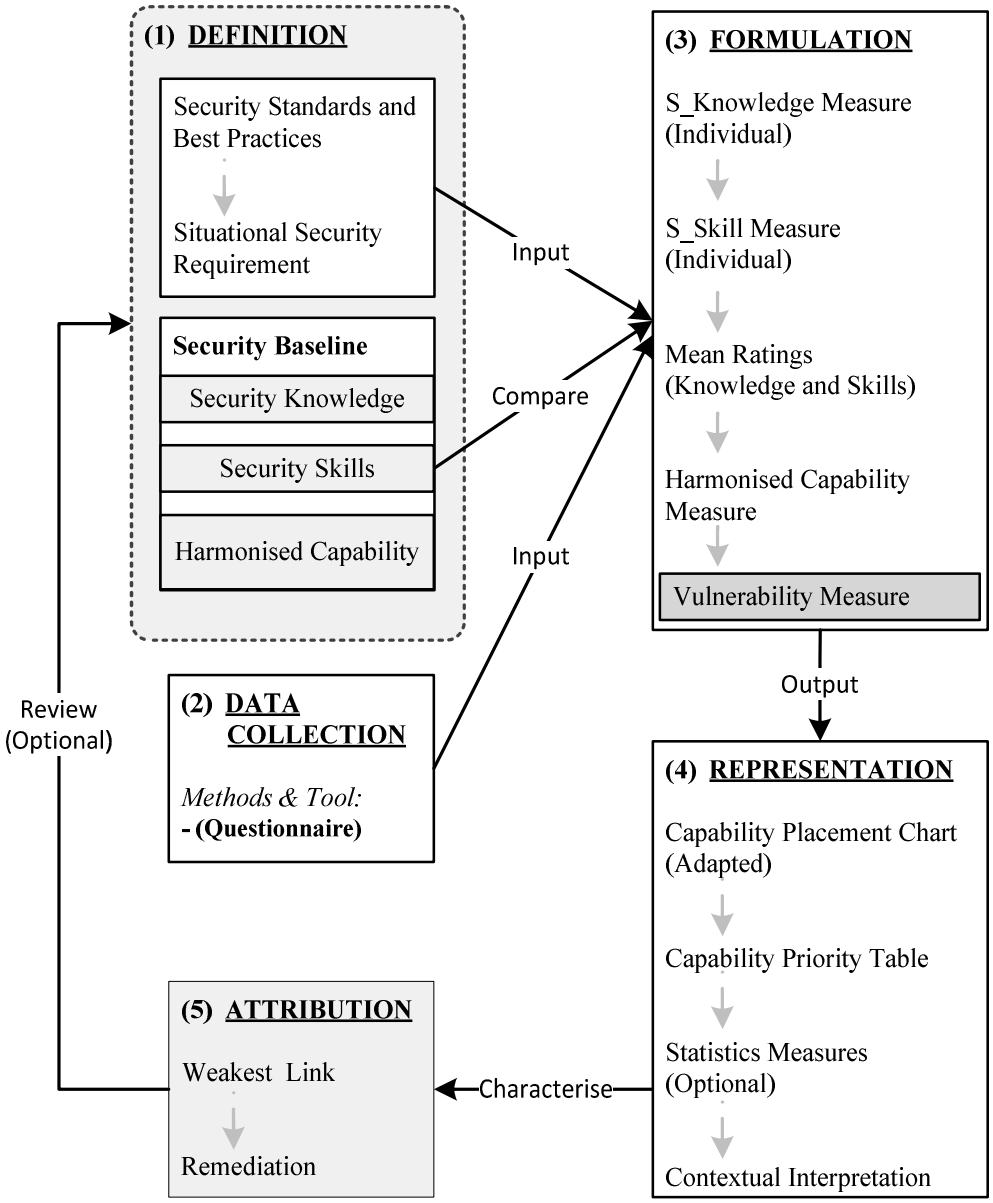

Figure 1: Human Workforce Security Capability Evaluation Scheme

This is not adopted as a closed scheme, but rather, it represents a way of achieving categorisations for security capabilities. Following a similar approach, other grouping schemes may be adopted with a t-level categorisation, where *t* can be 2, 3, 4, or 5, and defining the number of capability categorisation desired from an evaluation scheme. Depending on the value of *t*, the number of PSC, ratio, fractional limits, capability range, and priority ratings would be proportionate to *t*, and will corresponding number of classifications to represent dispersed or closely-related security capacities of human agents under evaluation. For instance, if *t*=5, it means 5-level classification is used. Upper bounds for the classes include; 1/5, 2/5, 3/5, 4/5, and 5/5, which is still between 0 and 1. The values for capability variables (knowledge and skills) will then be spread among the 5 groups. In comparison with *t*=3, using *t*=5 will imply that workforce capabilities are classed into 5 groups instead of 3. The 3 groups will break off to form independent groups to make up the 5 groups. The implication is that the specific capability value for each workforce would remain unchanged since the same range [0,1] is used, and the evaluation tool (questionnaire) characteristics (questions, multichoice answers and score allocations) also remain unchanged. Only the values' classification in capability range and priority ranking may change. The capability ratings are applied to knowledge, skills, and harmonised capability metrics accordingly, and the range is used for ranking the level of workforce capabilities. A priority order for security response/control is defined which is the reverse order of the security capability levels for security arrangement.

Table 1: Capability - Priority Range Table

Capability Rating	Capability Range	Priority Rating *(Security Response)*
Low *(l)*	$0 \leq l \leq \frac{1}{3}$	High
Moderate *(m)*	$\frac{1}{3} < m \leq \frac{2}{3}$	Moderate
High *(h)*	$\frac{2}{3} < h \leq 1$	Low

4.3.2 Data Collection Methods and Tools

To determine the status of an entity in the light of prescribed security requirements, it is necessary to extract the information of the entity. It is pertinent for the workforce security capacity evaluation to aggregate the data of the response or reactions of ICSE workforce members to cyber threats, attacks and/or incidents through active and/or passive, direct and/or indirect security capability investigation. The investigation should reflect prescribed ICSE security policy guidelines, objectives, evaluation timeline, a targeted workforce size, and quality of expected feedback.

For this evaluation, the test-based questionnaire tool is used for data collection following similar approaches observed in related literatures. This approach is typically used to determine if a tested subject qualifies in relations to certain prescribed standards as in this case; the UK Cyber Security Essentials (10 Steps to Cyber Security). Feedback data are collected and characterised to clearly represent attributes of individuals in the evaluated group. Score ratings are attributed based on the coded response/feedbacks in relations to the organisation's view of the security risk implications of each response to the security objectives. These quantitative feedback data then serve as inputs to the computation stage of the evaluation model.

4.3.3 Formulation

At this stage, mathematical procedures are applied on collected data to determine possible workforce capability values. Following the description of workforce security capability as a function of security knowledge and skills of a workforce, two groups of data corresponding to security knowledge and skills evaluations are derived.

Assuming p is an element in set P of ICS workforce personnel, whose security capacity will be evaluated, and N implies the total number of members in the set. Depending on the evaluation technique, let $K = \{k_1, k_2, \ldots, k_N\}$ represents the set of evaluation questions (from capability data collection tool which can be a survey) for knowledge capability. Every element in K contains a multi-choice list of evaluation (survey) response options each having a corresponding score allocation based on expert judgment on the implications of the choice to an overall assurance of security of the ICS. A response knowledge score allocation (x) range of 1 to 5 is proposed, 1 implying a lower potential and 5 implying a higher potential of resistance to the prescribed security scenario. Each response to an element in K therefore has a value range: $\{x|\ 1 \leq x \leq 5\}$. The variety of feedbacks in K will yield varied occurrence of x during the data aggregation. Hence, the cumulative knowledge capacity (CKC) for every $p \in P$, as the measure of the total quantitative knowledge capability (Kc) scores of a single workforce member. This is represented in equation 1. Note that equation 1 represents the computational model for deriving the security knowledge capability score of a single workforce (human agent) obtained from the score allocations associated to the individual's responses in the evaluation tool.

$$Kc_p = CKC_P = \left[\sum_{x=1}^{5}(x.n_x)\right]_p, \forall\, p \in P \qquad (1)$$

where n_x is the number of occurrences of respective response allocation x (i.e., 1-5)

Similarly, the cumulative skill capability (CSC) of $p \in P$ can also be derived from a set S of skills capability evaluation questions (from capability data collection tool which can be a survey), using similar scheme and range for skill score (y) as in knowledge score (x), i.e. 1-5. The total quantitative skill capability (Sc) rating of

a single workforce member p can be denoted as equation 2. This represents the computational model for deriving the security skill capability score of a single workforce (human agent) also obtained from the score allocations associated to the individual's responses in the evaluation tool.

$$Sc_p = CSc_P = \left[\sum_{y=1}^{5}(y.n_y)\right]_p, \forall\, p \in P \qquad (2)$$

Equations 1 and 2 can be used to compute corresponding knowledge and skill capabilities of each workforce member p in the group P of the workforce under evaluation. The harmonisation of *Kc* and *Sc* values yields a *personalised security capability* (*PSC*) computed via a Geometric Mean (GM) technique of the knowledge and skills capability score associated with a single individual. This is presented as Equation 3. GM offers the strength of being less submissive to the vast skewness influence of a very large values in a range of distribution (Manikandan, 2011), through normalising quantities to ensure that no singular quantity alone perpetually dominates the weighing of a final result. A set of *PSCs* will be generated, corresponding to all members, $p \in P$, and fed into the representation stage of the evaluation process.

$$PSC_p = \left(Kc_p \times Sc_p\right)^{1/2}, \forall\, p \in P \qquad (3)$$

4.3.4 Representation

The visualisation of workforce capacity should drive easy and better understanding of security perspectives, especially by top management and decision-makers who are often less technically savvy. To achieve this visualisation, Capability Placement Chart (CPC) and Capability Priority Table (CPT) are proposed as effective methods that can be used as shown in Figure 2 (a) and (b), respectively.

The CPC embodies a scattered diagrammatic representation and placement of a set of derived *PSC* values. The values would typically be between the potential minimum and maximum capability ratings for the group of workforces, and which depict the status of security capacity for workforce members evaluated. High capability value would mean a high knowledge and skills potentials with respect to outlined security baseline. A range of priorities attributed to each *PSC* outline the magnitude of security attention and concern that should be attributed to each *PSC* value in line with the capability-priority rating range outlined in Table 1. The order of priority for security control effort is in the reverse order of security capacity. Workforce members with high *PSC* values retain a relatively high degree of security awareness and practical proficiencies, implying a higher likelihood to respond appropriately to potential security incidents, at least within the scope defined in the evaluation tool. *PSC* values that fall within the moderate capability ratings imply a moderate priority rating, and those within the low capability rating imply a high priority rating. These particularly indicate low level security awareness and (or) skills, and thus a higher need for security control measures that can improve their capacities to an acceptable level and within the prescription of the evaluation objectives.

The CPT presents *PSC* values alongside corresponding *Kc* and *Sc* values; helping to provide a holistic detail and comparative provisioning for the evaluation process. It provides a means of easily identifying both initial and successive weakest links in an array of *PSC* values. In the case where further or deeper insights are required about each metric or the harmonised format, capability priority table also provides a means for the optional analysis of derive measures using conventional statistical paradigms, such as measures of central tendency and dispersion. It can also support a test of hypothesis where necessary to compare or consolidate on findings and conclusion from initial evaluation results.

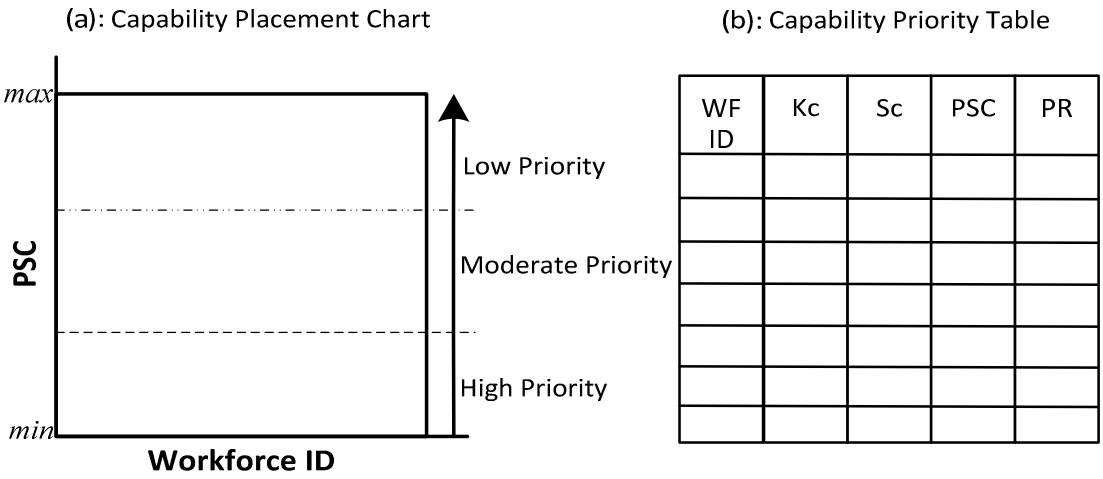

Figure 2: Capability Representation Formats

The interpretation of result involves a contextualised mental clarification of the significance of the results in the representation stage. This tie real meanings and implications to derived quantities and measures in both knowledge and skills evaluations in relations to security threats, vulnerabilities, attacks capability gaps in the ICS workforce. Such interpretations simplify the understanding of the points of high risk, the scale of risks and potential impacts from workforce perspective. It contributes to an understanding of what is expected of workforce members towards an overall operations security of ICS.

4.3.5 Attribution

This involves the clear identification of the weakest link attribute to a relative workforce member or group in line with a prescribed attribute function. In the approach proposed, the weakest link attribute implies the workforce or group with the least possible capability rating value and highest possible priority rating value in the capability priority table (CPT). The focus is typically on the *PSC* array, however, depending on the targeted objective, *Kc* and *Sc* arrays can also be used to attribute weakest link. Assuming *Z* represent the set of *PSC* values in the CPT, the weakest link (*WL*) attribute can be determined with simple mathematical minimum function as;

$$WL = min(Z) \qquad (3)$$

The characterisation of the weakest link also guides the process of determining the specific security vulnerabilities demonstrated by workforce members, and potential control solutions as a means of remediating identified capability gaps. The results and inferences from the evaluation process gives an understanding of the security incidence response and control measures that can be engaged. This typically tilts towards security capability areas where workforce members demonstrate a low degree of knowledge and skills.

5 Scenario-Based Testing

A scenario-based testing and validation technique is used to explore the usability and workability of the proposed approach.

5.1 Evaluation Tool (Survey) Design

An online questionnaire evaluation tool is adopted as a means towards achieving scalable collections of evaluation data. The reason for this validation was to assess the suitability of the proposed method for achieving efficient quantitative evaluations of ICSE workforce cybersecurity capability. To ascertain its effectiveness towards the identification of; potential weakest link(s), predominant security vulnerability areas, and relevant control measures. The defined security objectives for the assessment included: (i) evaluate the knowledge and skills security capability of the industrial workforce in relations to prescribed security guides, (ii) ascertain the weakest link from computed workforce personalised security capability values, and (iii) identify possible weak capability security themes and control areas in the workforce.

The purpose for adopting an online questionnaire approach was to efficiently reach large numbers of industrial workforce respondents, while allowing for participation in the assessment from any geographical location. This way, the demand constraints for participation is reduced, and response rates likelihoods potentially increased. It was also meant to create more realistic unsupervised assessment scenarios that will yield realistic data collection. The assessment questionnaire was circulated via email links to forum members of the UK IoT Security Foundation. It was opened to those who shared concerns about human-factor security vulnerabilities, and desired a way of determining specific security capabilities of respective workforce member within their industrial organisations, to support security decision-making. The evaluation contents shared contained clear description of the security capability evaluation questionnaire and its purpose.

In line with the model approach proposed, the evaluation was made following some recommended security control attributes and requirements for enabling cyber-attack defence, effective security within a digital system like ICS, as contained in NIST SP 800-82 v2 (Stouffer *et al.*, 2015), and UK 10 steps to Cybersecurity (UK-Cabinet-Office, 2012) good practice guide. Specific areas considered include: privacy and access control, system/network security monitoring, user awareness and training, secure configurations, removable media protection, personnel/credential security, home and mobile security, email security, malware protection, incident response, updates and patch management.

5.2 Capability Evaluation Tool (Survey) Testing and Refining

Survey questions were designed to evaluate the level of respondents' knowledge and skills in relations to the above-listed security themes. The broad security themes outlined in 5.1 also reflected similar security focus areas enumerated by Parson et al (2014) that provide valid themes for evaluating human aspect of information security. Questions were designed in scenario-based formats to evaluate the level of respondents' knowledge and skills in relations to these varied security theme. Initial assumptions included that the workforce members involved already had prior awareness and guidance on adherence to the prescribed security guides and essentials. The assessment was thus to ascertain the extent to which workforce members are holding up or improving on the security knowledge and skills already imparted by organisations. In structuring the questions, the design objectives were to: (i) present realistic and familiar security scenarios to participants, and (ii) proffer answer options that are realistic and familiar to the participants.

The initial evaluation tool (survey) comprised of two sets of questions covering knowledge and skills respectively. Each set comprised of 30 questions (3 questions per security theme) and focused on direct evaluations of security capability via applying the proposed model. Each question had 5 multiple-choice answers. This initial survey tool was subjected to quality testing using one-to-one interviews with 3 cyber security professionals (2 IT security experts and 1 ICS security expert) not included in the general capability evaluation sample. The inputs from experts were used to evaluate the validity and reliability of the survey tool in relations to its representativeness of all the security themes adopted in 5.1. Each expert answered questions relating to: if the survey tool was measuring what is intended, i.e., workforce security knowledge and skills. If the questions captured all the security themes of interest? If there was a need to add or cut down on questions, and rank the 3 questions in each security theme according to relevance. Each expert was to revise (where necessary) and provide ranking score allocations to the multiple-choice answers in each question based on the expert's perceived severity or implication of each response to an overall cyber-attack susceptibility.

In response to recommendations from the expert on the survey evaluations, significant and necessary improvements were achieved. The number of questions for each security theme was reduced to 2 for both the knowledge and skills sets. For each security theme, the top two most relevant questions identified by experts were selected. This reduced the number of questions in each set from 30 to 20. Following expert recommendations, a third set (comprising of 6 questions) was introduced to capture additional respondent demographic data (gender, age, work group, and possession of security certification) and a security self-evaluation rating. Score allocations for each of the multiple-choice answers were obtained by taking the average of the scores for each choice allocated by the experts. Where there were ties, further interaction was engaged with the experts to understand their viewpoints and use that to resolve score allocation ties amongst choice answers.

Thus, the capability evaluation tool (survey) output of this testing yielded 3 sets of questions: set A for respondents' demographics and self-evaluations (6 questions), set B for respondents' security knowledge evaluations (20 questions), and set C for security skills evaluations (20 questions). Each question in sections

B and C has 5 multiple-choice answers with respective score allocations, corresponding to the perceived severity or implication of each answer to an overall cyber-attack susceptibility and potential risk posed. The accompanying multi-choice answers is to represent varied security susceptibility levels (from high to low) for a respondent. The score allocation range is from 1 to 5, where an answer that implies a least security implication has a highest score of 5, while that with a highest implication has a least score of 1. A respondent's (knowledge or skills) capability is inferred from the choice answer for every question by the respondent.

The revised evaluation tool was pilot-tested with a team of six researchers at the manufacturing informatics centre in Cranfield University undertaking a research project for the development of a similar physical demonstrator of cyber security in manufacturing. The pilot test was built on the assumption: (i) the team represents a small-scale industrial (manufacturing) workforce, (ii) all the members of the team had equal action potentials to ensure the attainment of prescribed objectives of the project. The revised evaluation tool was administered to each team member and responses analysed using the workforce capability evaluation approach. The corresponding knowledge and skills capability ratings were derived using the appropriate evaluation functions as prescribed in the model. For this, the capability priority rankings include: $20.00 \leq h \leq 33.33$ for *high,* $33.33 < m \leq 66.67$ for *moderate, and* $66.67 < l \leq 100.00$ for *low.* The *low* priority range of scores represented the *'Ideal state' I* of the metric quantities. The evaluation yielded different levels of capabilities for knowledge, skills, and normalised capability ratings for the team members. The evaluation provided quantitative value reflections of the team members security capabilities, from which the weakest link can be identified. Based on the model description, the weakest link capability is attributed to the team member ID *WF03 (Kc = 23, and Sc = 48)* with a normalised capability rating $CR = 33.23$. A further look into the demographic profile of WF03: not having any form of security certification, product development process designer (not belonging to a security workgroup), and not having any form of work experience; all combine to suggest an element of true representation of the security state of the weakest link in comparison with others in the team.

The revised survey tool was again passed through the experts for another testing for quality in terms of identifying poor question wording and ordering, as well as errors in rationale layout, multichoice answers and associated score allocations to improve the quality and credibility of response and results. With minimal alterations, the final evaluation tool was used for the actual evaluation with real external target audience. Security knowledge capability survey was captured through structured questions that query respondent's awareness relative to their work environments and trends about certain threats, vulnerabilities, attacks or control details or features. For example, the question below is one of the knowledge capability questions that queries on 'system/network monitoring':

'The risk of your industrial process/operational environment becoming a victim of a cyber-attack has increased in the past year, and you are conscious of this while undertaking your routine duties in the workplace. To what extent do you agree or disagree with the following statement?'

A.	***Totally agree***	***[5]***	
B.	***Tend to agree***	***[4]***	
C.	***Tend to disagree***		***[3]***
D.	***Totally disagree***		***[2]***
E.	***Don't Know***	***[1]***	

<u>Rational for score allocations</u>

The numbers represent the score allocation that represent the relative security capability effort for each of the corresponding responses chosen. Employees who choose "E" are obviously unaware of the evolving industrial security trends, and are least likely to notice or sense security anomalies on their work end, hence the least '1' score allocation. Those who choose "D" are the next least likely sense security since they do not believe that there is any security risk around their work place. Their score allocation is "2", followed by those who choose "C" with a "3" score allocation. However, the employees that chose "A" are most likely to notice or sense security anomalies given their initial acknowledgment of proliferating attacks, hence, their score allocation of "5" which implies a highest knowledge capability. This is followed by those who tend to agree, choosing "B" with a "4" score allocations. Depending on the response chosen, the potential knowledge capability of the respondent can easily be assumed.

Security skills capability survey was captured through structured questions that query the practical actions or reactions of respondents in the face certain cyber compromise conditions. For the skills example:

'Outside the scheduled/planned maintenance period, you receive an email or pop-up notification on your workstation to urgently initiate a 'critical' security update or patch that you are not sure has been tested but addresses certain security flaws on your ICS node. How would you respond to this?'

- ***A. Do not install the update/patch, and leave the security flaw [4]***
- ***B. Quickly install the update/patch to enhance the security of your ICS node. [2]***
- ***C. Test the acceptability of the patch yourself, and install when satisfied [3]***
- ***D. Seek and verify the approval and accountability for the update/patch from technical support [5]***
- ***E. Neither install or verify patch since your system is not breached and is working normal [1]***

<u>Rational for score allocations</u>
Employees who choose "E" obviously bear careless security attitude, pose higher cyber-attack exposure, and highly unlikely to respond appropriately to cyber-attacks. Those that choose "B" also retain significant likelihood susceptibility to malware or Trojan attacks. Those that choose "D" might present the best likelihood of reaching appropriate solution by their actions, as their actions can ensure proper verification and response. Those with option "A" bear slight security risk, especially when the updates are genuine but ignored. for appropriate and timely response to cyber-attack potential. Those with choice "C" offers a slight cyber-attack risk doing the job themselves without formal reporting that could be helpful to others, but might proffer a better and suitable operational solution for the company. Similarly, depending on the response chosen, the potential skill capability of the respondent can easily be assumed.

Note that the score allocations are not directly included in the questionnaire, but only coded in the internal setup, captured from responses and used to evaluate security capabilities after responses are collated. They are only included here for clearer understanding of the evaluation scheme and process proposed. Table 2 presents the summary of baseline definitions in line with earlier discussed capability classification ratios and groups. A minimum capability rating is feasible assuming that all responses for one workforce member have the same least allocation score of 1. A maximum capability rating is derivable if all the responses each have the highest allocation score of 5. Response bias is a typical issue attributed to online surveys and questionnaires. It exemplifies a phenomenon where respondents provide answers they consider most acceptable, or expected from them, rather than a true expression of their personal views. To avert this, short and precise scenario-based questions with close-ended Likert-style answers were used to avoid potentials response biases that can emerge from too long and unclear questions. The interval scale (1-5) implied coding of responses was designed to help the acquisition of more accurate responses. The answer options were mostly structured into short and concise sentences to forestall the difficulty of evaluating their meanings by respondents. Response bias from incomplete set of answers was resolved through introducing answer options. For example, the answer option "Don't Know" was used to cover other possible response options not included in the interval list, to avoid getting 'false-positive' answers due to the absence of desirable options.

Table 2: Scenario Baseline Definitions

From Response Allocation Score, min = 20.00, and max = 100.00		
	Priority Class	**Range**
Capability Priority Rankings	High Priority Range (h)	$20.00 \leq h \leq 33.33$
	Moderate Priority Range (m)	$33.33 < m \leq 66.67$
	Low Priority Range (l)	$66.67 < l \leq 100.00$

5.3 Results Presentation

A total of 37 industrial professionals participated in the evaluation with each having a unique identifier. The feedback data were collected and used to compute the knowledge, skills, and harmonised capabilities of corresponding workforce members using Equations (1), (2), and (3), respectively.

A summarised capability-priority classification of the results is presented in Table 3. Figure 2 presents the capability placement chart (CPC), and Table 4 presents the CPT of the first 15 least capability (highest priority) ratings, while Figure 3 shows a chart showing the *Kc*, *Sc*, and *PSC* representations of the 15 least capability (highest priority) workforce members.

5.3.1 Demographics and Reliability Testing Results

The ages of the respondents were grouped into three: Group 1 (20-35 years), Group 2 (36-50 years), and Group 1 (51-66 years). There were 18 respondents in Group 1, 18 in Group 2, and 1 respondent in Group 3. The average age of the respondents was 36. More than half of the respondents (workforce) were between ages 30 and 40. More precisely, 48.6% of the sample workforce were under 35 years of age, and over three quarters (91.9%) are under 45 years of age. These suggest that that most of workforce evaluated were mid-age range. There were more male (33) than female (4) respondents, which suggests that there are potentially eight times more male than female human workers in operational ICS domains. Similarly, there were more OT personnel (34) than IT personnel (3), which provides an indication that that there are potentially more OT personnel than IT in the ICSE.

Initial validity and internal consistency reliability test of the measurement scale for knowledge capability (*Kc)* yielded Cronbach's $\alpha = 0.868$, which suggests a good measure of reliability. However, a good measure of reliability for the Skills capability *(Sc)* - Cronbach's $\alpha = 0.803$ was achieved in response to the need to remove one of the questions/assessment case items from the skills measurement scale. This item affected the reliability of the scale, and needed to be excluded to achieve the minimum recommended level of reliability. A Pearson's *r* data analysis of the modified data revealed a low positive correlation, $r = 0.018$ between *PSC* and workforce *Age* with significantly highly chances (0.914) of occurrence. This indicates a slight convergent validity, and suggests that although workforce *PSC* and workforce *Age* were two separate constructs that measured distinct properties about the workforce, there existed high likelihood of slight increase in *PSC* as *Age* increases. This means that older industrial workforce personnel were more likely to be more knowledgeable and skilled in security response and incident management in the ICSE. Possible influences on this correlation could be attributed to years of experience working within the ICS domain and the corresponding incidents that may be encountered, resolved, and learnt over the years.

The above results coincides with the findings by Beautement *et al* (2016) about a positive influence of *Age* on employee security maturity levels. Other measures that indicated slightly positive correlations to *PSC* include: *Workforce Group* with $r = 0.130$, and *Capability Group* with $r = 0.416$. The likelihoods of occurrence for both measures were quite lower than that of *Age*. The results generally aligned with Wang's (Wang, 2013) conclusion of a positive correlations between directly evaluated (computational) and self-evaluated responses of workforce security evaluations. This suggested that measures derived from directly evaluating capabilities most often follows similar results pattern as measures from self-evaluated responses of the same workforce.

5.3.2 Direct Evaluation Results

As shown in Figure 4, results indicated only 3 (8.1%) respondents from the *'security professional'* group, and 34 (91.9%) came from the *'general ICS operations group'*. This potentially reflects the typical rationing of workforce members in the industrial environment, where there is by a greater proportion of the industrial workforce, engaging general process operations, than that working for the maintenance of security. The result of the normalised individual security capability scoring of sampled respondents, in line with the priority grouping ratios prescribed in the capability evaluation model, indicates that more than half of the respondents (23) representing 62.2% were classed to be of *'low priority'* regarding their combined knowledge and skills conforming to the prescribed security standards and best practices. 12 (32.4%) respondents fell onto the 'moderate priority', and 2 (5.4%) fell in the 'high priority' group. The latter group identifies the respondents with high-risk weaknesses in cyber security, and which needed a quite urgent attention in terms of education and security capacity building. Contextually, the weakest link (*WL*) typically emerges from this group, and is attributed to the personnel with workforce ID ***WF014*** with an approximate harmonised capability rating of 32.47 ($i.e., WL = min(Z) = min(PSC_1 \ldots PSC_n) = 32.47$). This workforce individual had a knowledge capability rating of 34, and a skill capability rating of 31.

Table 3: Capability-Priority Classification for Test Scenario

Cap.	Priority	Freq	Percent	Valid Percent	Cumm. Percent
Low	High	2	5.4	5.4	5.4
High	Low	23	62.2	62.2	67.6
Moderate	Moderate	12	32.4	32.4	100.0
	Total	**37**	**100.0**	**100.0**	

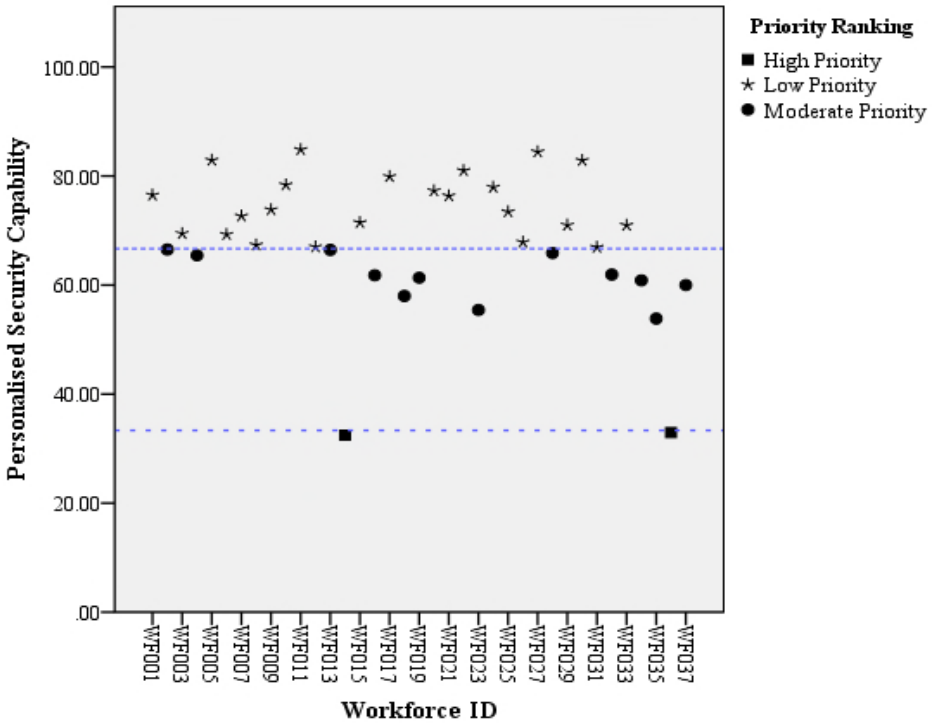

Figure 3: Workforce Capability Evaluation Placement Chart (37-User Classification)

Table 4: Priority Ranking for the 15 workforce members with the lowest security capacity

WF ID	Kc	Sc	PSC	Priority Ratings
WF014	34	31	32.47	High
WF036	31	35	32.94	High
WF035	58	50	53.85	Moderate
WF023	64	48	55.43	Moderate
WF018	58	58	58.00	Moderate
WF037	60	60	60.00	Moderate
WF034	65	57	60.87	Moderate
WF019	66	57	61.34	Moderate
WF016	57	67	61.80	Moderate
WF032	71	54	61.92	Moderate
WF004	68	63	65.45	Moderate
WF028	70	62	65.88	Moderate
WF013	64	69	66.45	Moderate
WF002	59	75	66.52	Moderate
WF031	70	64	66.93	Low

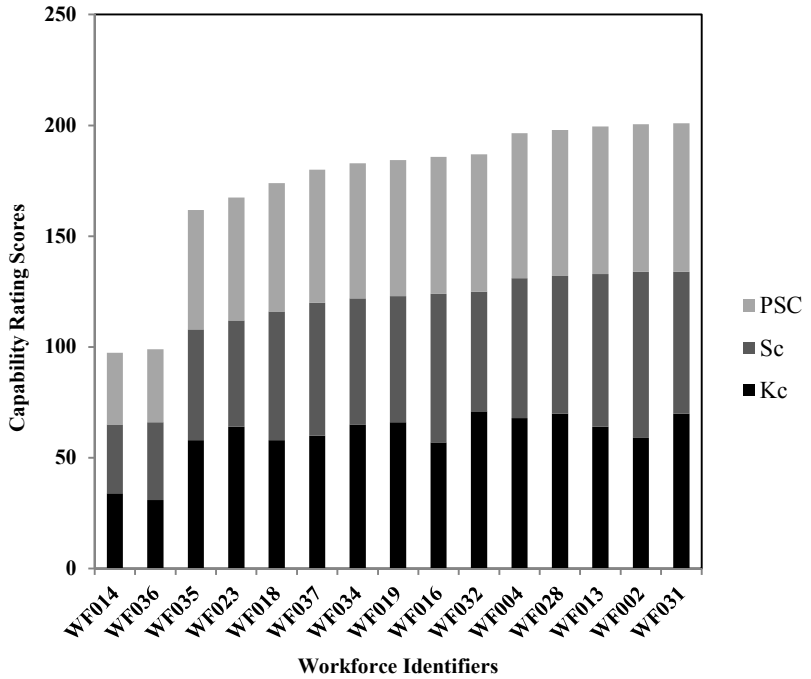

Figure 1: 15 Lowest Capability Workforce Representation (Kc, Sc, and PSC Contributions)

In assessing the areas of potential security weaknesses inherent the workforce evaluated, the cumulative capability rating (CCR) of each of the security questions was evaluated. The best-case scenario represents the maximum CCR (CCR_{max}), with a value of 185, if the highest capability score of 5 is assigned by all workforce responses to a specific question. The CCR value for the specific question is the product of the uniform score and the number of respondents (i.e., 5 x 37 = 185). The worst case represents the minimum CCR (CCR_{min}), which is 37 (i.e. representing the scenario where a uniform score of 1 is obtained by all responses to a specific question). The 15 least CCR values are presented in Figure 5, the records indicate that the first 3 least CCRs were from the skills evaluation questions, 10 (66.67%) of the least 15 CCRs compared came from the skills

(*Sc*) evaluation questions (Table 5), and only 5 (33.33%) of the least 15 CCR values came from the knowledge (*Kc*) questions (Table 6).

Table 5: The Least 10 Skills Cumulative Capability Ratings (CCR)

Skills Capability Weakness Areas		
Question ID	**Questions**	**Security Evaluation Areas**
Q37:	*How often do you change/review your account password assuming organisational security policy is in place*	***Credential (Password) Management Policies***
Q27:	*How do you respond to either of the following; the mouse on your workstation screen begins to move around on its own and click things, or the controls on your monitoring station (HMI) get activated on their own?*	***Malware (Virus) Attack Response and Controls***
Q23:	*How do you access and exchange files and documentations within your industrial system/organisation (Enterprise Management and Industrial networks)?*	***Removable Media Protection***
Q40:	*How often are you able to detect cyber intrusions, attacks, compromise, or malware (virus, Trojan, spyware, etc.) when they occur on your work system/station (industrial equipment, computing device, network, etc).*	***Malware (Virus) Attack detection***
Q30:	*Two different offices in your workplace are working to straighten out an error in your Single Sign-On Account (Login) Configurations and Bank payments details. Office 1 asks you to email your correct account details. You send the requested details via email to office 1, which is subsequently forwarded via email to office 2. Office 2 confirms to have straightened the error out. What do you think could be wrong here?*	***Credential Management and email security***
Q22:	*How do you access and exchange files and documentations within your industrial system/organisation (Enterprise Management and Industrial networks)?*	***Updates and patch management in ICS***
Q28:	*In your opinion, which of these offers a stronger and more secure password type to adopt?*	***Credential (password) security deployment***
Q34:	*It is festivity time; you receive an electronic greeting card (e-card) to your work email from a friend. The mail requires you to click on the attachment to view the electronic card. What should you do?*	***Email security (phishing) attack management***
Q24:	*Knowing and following the channels and modes for incident reporting in the event of being a victim of a (suspected) cyber-attack/intrusion/infection.*	***Incidence Response***
Q29:	*Because you are keen on enhancing your cyber security knowledge and skills, you subscribed to a number of free online ICS/SCADA Security Magazines. To activate your free subscription, you are required to register with your work email. One magazine asks for your year of birth, a second asks for your month of birth, a third asks for your mother's maiden name. How do you respond to these queries?*	***Identity and Privacy Security***

Table 6: The Least 5 Knowledge Cumulative Capability Ratings (CCR)

Knowledge Capability Weakness Areas		
Question ID	**Questions**	**Security Evaluation Areas**
Q1:	*How well secure do you feel about your industrial equipment, networks, operations and(or) critical infrastructure against cyber vulnerabilities, threats and attacks?*	***Security Controls Availability***
Q17:	*It is the sole responsibility of the information security department to protect company assets by engineering protection and proper use of information assets, deploying security technologies for securing industrial processes, and developing proper security practices for daily activities*	***Proper Attribution of Security Responsibilities***
Q12:	*You have good knowledge and understanding of your duties and role expectation pertaining the following; awareness and training, home and mobile working, configuration management, removable media protection, user credential security and management, incident response and management, privacy controls, monitoring, malware protection, audits, accountability, authentication and authorisation, physical and environmental security, and contingency planning, for the protection of industrial computing assets and critical infrastructures as contained in any of (i) CPNI Good Practice Guide, (ii) ISO/IEC 27002, (iii) IEC 62443 (ISA-99), (iv) NIST SP 800-82 v2, (v) COBIT 5*	***Awareness of respective Roles in Security***
Q18:	*Which statement best describes your knowledge of potential solutions available for addressing cyber security threats to ICS/SCADA infrastructure and(or) enterprise network?*	***Knowledge of Available security controls***
Q2:	*How often do you monitor process and activity log data, and tune the usage statistics of your Industrial Control Systems and IT critical infrastructure?*	***Security Monitoring Frequency***

Furthermore, the demographics of ***WF014*** personality indicates an age of 29, no form of certification in information or cyber security, and self-rated assessment of security capability 1, which implies a *least capability* rating. This suggests a relatively young age of work and perhaps experience, considering that three-quarters of the workforce were over 30 years. Self-rated assessment of security capability is likely to change as this personnel's age and experience in the ICS environment increases.

The mean capability ratings for knowledge and skills are 69.43 and 62.97 respectively. The standard deviation for the knowledge capability scores is 12.39, while that of the skill capability score is 11.69. In relations to the security requirements adopted and evaluated, it implied that the workforce generally demonstrated higher theoretical knowledge than practical skills. It could also be because of the perceived lack of keenness for security skills in industrial workforce, who often assume that enforcing security should be solely left to the IT security specialists. The standard deviation values indicated that there were slightly more capability dispersions in security knowledge than security skill amongst the workforce. That is, most of the workforce had very closely the same level of practical skills in ICS security than they were closely levelled in awareness (knowledge) of ICS Security. In general, the results suggest some measure of capability gaps amongst the workforce which may be influenced by their interactions, information sharing, personal capability enhancement engagements, and possibly organisational policies on security. Out of the 37 workforce members; 34 (91.9%) belonged to the General ICS operations class, 3 (8.1%) belong to ICS Security class. 36 (97.3%) did not have any security training or certificate, only 1 (2.7%) has a form of security training. This reflects the potential typical rationing of workforce members in the industrial environment. There is by far a greater proportion of the industrial workforce engaged with other industrial responsibilities other than the maintenance or assurance of security.

5.3.3 Self-Evaluation Results

In the aspect of self-evaluated capabilities, more than half (19) or (62.2%) rated themselves as *'low capability'* in ICS security proficiencies. This contrasts with the computed capability score class that showed 2 (5.4%) respondents under low capability. This suggests a significant variation between individual and organisational views about security capability expectations, and further suggest that the respondents appear to have a higher capability rating disposition than that adopted by the organisation (used in the evaluation). To investigate and expound further on this capability variations, statistical hypothesis testing was applied with a Null assertion (A/H_o): *There is no difference in priority rating levels of the workforce amongst the self-rated security capability groups*. The self-rated security capability attributes used in the evaluation tool (questionnaire) included: 1= least capability, 2= low capability, 3 = moderate capability, 4 = high capability, and 5 = highest capability.

.

Table 7: Statistical Crosstab for Security Capability by Priority Ranking

Security Capability * Priority Ranking Crosstabulation

			Priority Ranking			Total
			High Priority	*Low Priority*	*Moderate Priority*	
Security Capability	*Least Capability*	Count	2	1	1	4
		Expected Count	.2	2.5	1.3	4.0
	Low Capability	Count	0	12	7	19
		Expected Count	1.0	11.8	6.2	19.0
	Moderate Capability	Count	0	9	2	11
		Expected Count	.6	6.8	3.6	11.0
	Higher Capability	Count	0	1	2	3
		Expected Count	.2	1.9	1.0	3.0
Total		Count	2	23	12	37
		Expected Count	2.0	23.0	12.0	37.0

Table 8: Statistical Crosstab for Workforce Group by Priority Ranking

Workforce Group * Priority Ranking Crosstabulation						
			Priority Ranking			
			High Priority	*Low Priority*	*Moderate Priority*	**Total**
Workforce Group	*General ICS Operations*	Count	2	21	11	34
		Expected Count	1.8	21.1	11.0	34.0
	Security Professional	Count	0	2	1	3
		Expected Count	.2	1.9	1.0	3.0
Total		Count	2	23	12	37
		Expected Count	2.0	23.0	12.0	37.0

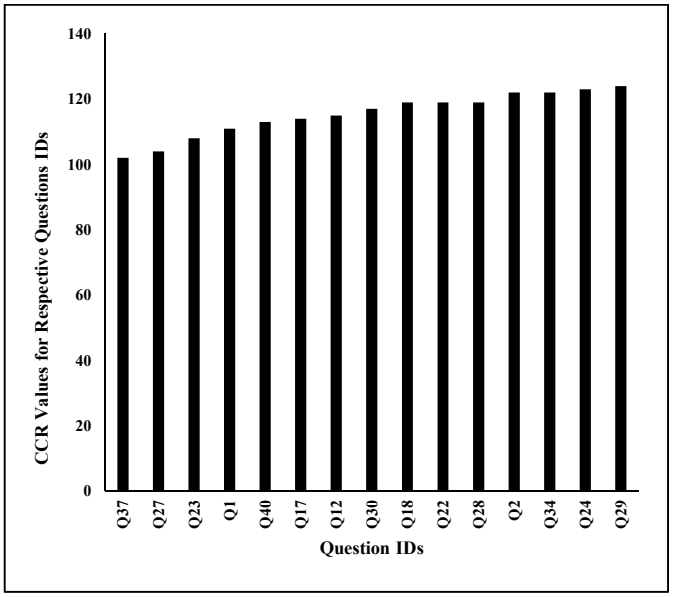

Figure 2: The Least 15 cumulative capability rating (CCR)

As observed in Table 7, 2 of 37 workforce members are in the high priority group, same 2 rated themselves as having least capability. Similarly, 23 of 37 workforce members are in low priority, and of the 23, 9 self-rated themselves as having moderate capability, 12 having low capability, and 1 each having least and highest capabilities. Since our work focuses on weakest link, focused analysis is undertaken on the least capability – high priority intersection. The row totals revealed 4 workforce members self-rated under least capability, the column total shows 2 workforce individuals on high priority ranking. A Pearson's chi-square (x^2) value of 20.431 was obtained for these statistics with a 0.002 significance level. The crosstab statistics in Table 8 suggests that there is a rather large difference between the count and expected count in the sample if all self-rated least capability workforce reactively behaved in like manner of high priority as other grouped workforce members. However, a 0.002 significance level on the chi-square (x^2) value implies the possibility of rejecting the null hypothesis with only 0.2% chance of being wrong (i.e., less than 1 in 1000 chances of being wrong). The Null hypothesis could be rejected, and an alternative hypothesis alternative hypothesis (A/H_i): *There is a difference in priority rating levels of the workforce amongst the self-rated security capability groups* could be considered. It can thus be assumed that the workforce self-rated under least capability are more in high priority ranking group than in others. In the event of such variations, it becomes important to engage with, and determine the workforce's view about security capability expectations, and work towards updating and bringing-up the seemingly low-rated organisation security rating benchmark for personnel to a higher acceptable level.

Also, testing a second hypothesis (B/H_o) that *there is no difference in priority ranking level between the general ICS operations and security professional workforce* yielded a Pearson's chi-square (x^2) value of 0.188 with

0.910 significance level. The crosstab on Table 8 suggested very negligible difference between the real and expected priority ranking behaviours of the general ICS operations group. The security group also behaved in like manner. As expected, the results in the table 8 crosstabs indicated no security professional emerged in the high priority (low capability) group. Thus, a 0.910 significance suggests a 91% chance of being wrong if we reject the null hypothesis. This huge likelihood of being wrong informed our basis for not rejecting the null hypothesis that there is no difference in priority ranking level between the general ICS operations and security professional workforce.

5.4 Discussion

The above results suggest that irrespective of the number of high security-proficient cybersecurity professionals in the workforce members in an industrial control environment, the presence of other general operations ICS workforce members with inherently low capabilities can decrease overall organisational human-oriented security capacity. Circumstantially, this phenomenon follow similar patterns and disposition in prior works (Nikolakopoulos, 2009) where human agents (ICS workforce members) with low security capability (knowledge and skills) ratings are likely to be weak-links, since they pose more conspicuous targets of attacks.

If all of the workforce evaluated all belong to the same organisation, then the workforce individual with identity number ***WF014*** represents the security capability of the organisation. Notwithstanding the security capability strengths of all other workforce members, the organisation can easily be penetrated and compromised to the security and defence capability of ***WF014*** workforce individual. The organisation would be considered as weakly penetrable as the capability of ID WF014, who in this context and based on evaluation result is considered the weakest link. This represents the straw portion of whatever security fences or capability enabled or imbibed in the entire workforce, and figuratively, a *'straw'* portion in a brick wall suggests the weakest and most vulnerable point of breach. Reactively or proactively raising the capability ratings of potential weakest link (via appropriate control measures) implies raising or strengthening organisational security capability. Also, a low capability rating in any of knowledge or skills potentially upsets an eventual PSC, and by extension an organisational capability. A low capability in both attributes suggests an even worse phenomenon. Essentially, a workforce individual with high security knowledge rating indicates being abreast with evolving industrial cyber security landscape, but with low security skills rating, indicating a lack or gap in practical (responsive) proficiency to ensure security within his/her domain, is nearly as weak as the workforce who is skilled in responding to primordial cyber security threats and attacks but does not constantly keep up with updates and changes in the security landscape. This is a possible scenario within ICS organisations where adequate emphasis is not placed on human-factored cyber security assurance. This point re-echoes an earlier disposition (Beautement *et al.*, 2016), asserting that for security management to be effective, it remains valuable to evaluate the impact of employee security capability, susceptibility and behaviour, more so, in a way that supports identifying and ranking capability and susceptibility levels, as well as common security weak areas.

A related phenomenon is seen to play out in the contrast between self-rated and computed capabilities of the workforce. The outcome indicates that more industrial workforce members were more aware of cyber-attack trends and issues than they have the skills to respond appropriately to eventual incidences, despite that most of the workforce had not undergone any formal education and(or) training on security concepts, norms, and best practices, an information that would help them acquire appropriate knowledge and skills in the assurance of cyber security within their working environments. It suggests that while the organisation might feel comfortable about certain qualities and proficiency levels, personal workforce convictions might not represent the same opinion. This could result from a lack of updated details in emerging cyber security threat landscape on the part of the organisation, which is reflected in the test for old and widely known security capabilities. To avoid such precarious situations, organisations must continually keep abreast with the changing security trends, and updates evaluations in the light of those changes. Reviews and refinements of the security risk landscape should be continuous to capture any new or left out changes. Comparing the two results helps the balancing of security efforts between organisational view and workforce view about security capability.

The analysis of prime security-vulnerable areas reveals an interesting pattern inherent the workforce. The cumulative capability rating (CCR) of each of the security questions/parameters for all respondents can guide the identification of prime security knowledge and skill vulnerable areas. A lower CCR value indicates a gap or weakness in capability, and vice versa. It is therefore presumed that security weaknesses or vulnerabilities would typically widen or increase with decrease in CCR values. In the analysis of the least 15 CCR values

selected, the first 3 least CCR values emerged from skill evaluation parameters, and 10 out of the least 15 CCR values also came from skill evaluation parameters. These suggest a potentially more incapacity and security gaps in skill than in knowledge of the workforce evaluated. This also presents a correlated perspective when compared with the overall knowledge and skill capability averages, which indicated a higher average security knowledge than security practical skill in the workforce.

Grouping the security areas of the least 10 skill CCRs into related family of security controls reveals that the workforce evaluated are weak in 4 broad areas of security control. These include: Credentials (Password) Management and Security, Malware (Virus) Detection and Management, Removable Media and Email Security, and Patch (update) management. The broad areas of theoretical knowledge weaknesses include; awareness of available security control measures, and knowledge of self-duties and responsibilities towards overall system security. Most of the identified workforce vulnerability areas are in their weakest states in the security capability characterisation of the identified weakest link workforce individual (i.e., WF014). In this context, rather than engage all workforce members in practice training and awareness in all conceivable security areas, a strategic, cost, time, and resource-effective implementation of control measures for enhancing cyber security assurance would involve focussed awareness and practical training of selected purported weaker (more vulnerable) workforce members in the 'low capability' areas enumerated. Security assurance improvement should involve inculcating security proficiencies (knowledge and skills) that are observed to be lacking, as it may be a waste of time, money, and other resource giving the workforce what they already have.

It is apparent that a single human-factor attribute such as security knowledge alone does not provide sufficient landscape and information to effectively characterise and represent a human agent's security aptitude. Industrial organisations need to cultivate and maintain a culture of continually improving their corporate security posture and capacity through evaluating and growing the security capacity of their employees (workforce). This must be driven by an understanding that effective security starts and ends with each human-agent (workforce) involved with their industrial infrastructure, processes, operations, and services. A better representation of security capability can be obtained by combining multiple human-factor (workforce) attributes such as knowledge and skills as demonstrated in the results obtained. A low capability rating in any of knowledge or skills potentially upsets an eventual PSC, and by extension an organisational capability. Thus, workforce security capability should be a priority for organisation, for when technical security capacities are ineffective, fail, or non-available, the security capability of the human agents can provide the last line of dense.

6 Conclusion and Future Work

Amidst evolving security trends that places human industrial actors as prime vectors of industrial cyber-attacks, human-factored security efforts are required to manage and control the menace of prevailing attacks. Considering that cyber security knowledge and skills capabilities of the industrial workforce (people) is crucial and strategic towards building a more effective and cybersecurity-compliant workforce. Inordinate records demonstrate that most successes in the security compromises of industrial control system and network environments have target and exploited the security capability weaknesses of the human (people) constituents of industrial/operational environments, especially those with low aptitudes. Securing ICS domains and networks is no longer the sole responsibility of cybersecurity professionals within the industries, it is a responsibility shared by all workforce members in the industry. Particularly, the non-security-savvy industrial operations personnel needs to be considerably knowledgeable and skilled in the act of appropriate and effective security behaviours and responses, as they are currently more targeted than the security experts.

Directed cyber-attacks on the workforce become effective due to a couple of reasons; like weak or lack of sufficient cyber security knowledge and skills, negligence, misinformation, all of which can spur inappropriate behaviour (actions and inactions) enough to neutralise cyber-malicious actions. Technology-based security solutions alone may not be able to enforce the desired security in the system if the people constituents fail to recognise and maintain their roles in overall organisation/system security. A lack of cyber security knowledge is as bad as a lack of cyber security skill, and it is a matter of an organisation and(or) system being as strong as its weakest link. Potentially, the weaker links in the system/organisation, the lower the potential security capacity or posture. One way to reduce organisation security vulnerability or risk potential is to enhance security capability through improving security awareness and training, identifying specific personnel with security weaknesses, and the specific knowledge or training needs. Humans will always be in the loop (directly or indirectly), and their competencies would seldom come into play towards achieving certain security objectives. The application of systematic and strategic analysis of workforce security capacities can spur the

ICS-driven organisations towards good and well-informed cyber hygiene, and help maintain effective responses to possible cyber security factors, through removing or reducing weak links in the system. Human-factored security evaluations is a step towards building robust and resilient cybersecurity capacity in the people elements of a digital system.

The research provides an approach to identify the security-compliant weakest link in a group of workforce members. It proffers the first line of defence against potential security threats by activating security consciousness in the workforce. It also offers a starting point for security evaluators and top management towards understanding individual workforce security postures, in relations to defined security objectives and expected baselines. It can (i) help analyse and reveal potential variations in security capability among the workforce of organisations, (ii) be used to assess organisations' workforce over or under performance in security capacity, and (iii) persuade and promote an up-to-date disposition in security expectations and requirements, (iv) aid the identification of cyber security threats and vulnerabilities that are unique to their environments. Overall, the evaluation approach proffers a means of measuring the effectiveness of continuous cybersecurity control and remediation efforts, and speeds-up problem-solving. It also demonstrates potential to guide organisations into adopting cost-efficient means of thinning and appropriating security remediation outlines to meet evolving needs, security assurance scopes, and resources without undue wastes or redundancies. A limitation of the proposed model points to subjectivity where score allocations for responses in the evaluation tool rely on expert evaluations of perceived risks attributed to any response disposition. It would be interesting to explore a way of achieving the same allocation via a standardised evaluation approach and tool to eliminate high-level subjectivity and potential inconsistencies in value allocations. Other future work in this area also includes developing an automated evaluation tool that can be used to replicate and quicken the processes outlined in the proposed approach. It would be interesting to consider incorporating further human attributes like cognitive and behavioural patterns and characteristics to the evaluation scheme. Work will be done on the incorporating the human-factored attributes into a larger risk-based critical impact point method for enhancing cyber security assurance.

References

Abe, S. *et al.* (2016) 'Security Threats of Internet-reachable Industrial Control System (ICS)', in *Society of Instrument and Control Engineers of Japan (SICE) Annual Conference 2016*. Tsukuba: IEEE Xplore, pp. 750–755. doi: 10.1109/SICE.2016.7749239.

Adams, M. and Makramalla, M. (2015) 'Cybersecurity Skills Training : An Attacker-Centric Gamified Approach', *Technology Innovation Management Review*, (January), pp. 5–14. Available at: https://timreview.ca/sites/default/files/article_PDF/AdamsMakramalla_TIMReview_January2015.pdf.

Aloul, F. a. (2012) 'The Need for Effective Information Security Awareness', *Journal of Advances in Information Technology*, 3(3), pp. 176–183. doi: 10.4304/jait.3.3.176-183.

Amin, S. and Sastry, S. (2015) '1 Introduction 2 Analysis of the Secure Control Problem', *Control*, pp. 1–14.

Ani, U. P. D., He, H. M. and Tiwari, A. (2016) 'Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure', in Nicholson, D. (ed.) *Advances in Human Factors in Cyber Security: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA*. Florida: Springer International Publishing, pp. 169–182. doi: 10.1007/978-3-319-41956-5.

Asgharpour, F., Liu, D. and Camp, L. J. (2007) 'Mental models of security risks', in Dhamija, R. (ed.) *Lecture Notes in Computer Science*. Berlin; Heidelberg: Springer, pp. 367–377. doi: 10.1007/978-3-540-77366-5_34.

Ashford, W. (2016) 'Lack of cyber security awareness putting UK organisations at risk', *ComputerWeekl.com Online Article*, March. Available at: http://www.computerweekly.com/news/4500278074/Lack-of-cyber-security-awareness-putting-UK-organisations-at-risk.

Badie, N. and Lashkari, A. H. (2012) 'A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP', *Journal of Basic and Applied Scientific Research*, 2(9), pp. 9331–9347.

Beautement, A. *et al.* (2016) 'Productive Security: A scalable methodology for analysing employee security behaviours', in *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*. Denver: www.usenix.org, pp. 1–18. Available at: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement.

Beautement, A., Sasse, M. and Wonham, M. (2009) 'The compliance budget: Managing security behaviour in organisations', in *Proceedings of the 2008 Workshop on New Security Paradigms*. Lake Tahoe, California, USA: ACM New York, NY, USA, pp. 47–58. doi: 10.1145/1595676.1595684.

Ben-Asher, N. and Gonzalez, C. (2015) 'Effects of cyber security knowledge on attack detection', *Computers in Human Behavior*. Elsevier Ltd, 48(June), pp. 51–61. doi: 10.1016/j.chb.2015.01.039.

Botta, D. *et al.* (2007) 'Towards understanding IT security professionals and their tools', in *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security*. Pittsburgh, PA, pp. 100–111. doi: http://doi.acm.org/10.1145/1280680.1280693.

Brassso, B. (2016) *Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories*, *FireEye Online Security Blog*. Available at: https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html (Accessed: 24 April 2017).

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information Security Policy Compliance: An Emperical Study of Rationality-based Beliefs and Information Security Awareness', *MIS Quarterly*, September, pp. 523–548. Available at: http://130.18.86.27/faculty/warkentin/BIS9613papers/MISQ_SpecialIssue/BulgurcuCavusogluBenbasat2010_MISQ34_RationalityAwareness.pdf.

Chen, P.-C. *et al.* (2012) 'Experience-based cyber situation recognition using relaxable logic patterns', in *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*. New Orleans, LA: IEEE Xplore, pp. 243–250. doi: 10.1109/CogSIMA.2012.6188392.

Chi, M. T. H. (2006) 'Two approaches to the study of experts' characteristics', *The Cambridge handbook of expertise and expert performance*, pp. 21–30. doi: 10.1017/CBO9780511816796.002.

Christopher, J. D. *et al.* (2014) *Cybersecurity Capability Maturity Model (C2M2)*, *Department of Homeland Security*. Available at: https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program.

CLOUDMARK (2016) *Survey Reveals Spear Phishing as a Top Security Concern to Enterprises*, *Website Blog Inforgraph*. Available at: https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/ (Accessed: 25 April 2017).

D'Amico, A. *et al.* (2005) 'Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts', in *Proceedings of the Human Factors and Ergonomics Society Annual*

Meeting. DoD, pp. 229–233. doi: 10.1177/154193120504900304.
D'Amico, A. and Whitley, K. (2008) *VizSEC 2007 : The real work of computer network defense analysts*, *Proceedings of the Workshop on Visualization for Computer Security*. Edited by J. R. Goodall, G. Conti, and K.-L. Ma. Springer Berlin Heidelberg. doi: 10.1007/978-3-540-78243-8.
Debo, C. (2015) *Preventing Cyberattacks and Data Breaches via Employee Awareness Training and Phishing Simulations*, *Website Article*. Available at: http://www.schneiderdowns.com/preventing-cyberattacks-data-breaches-employee-awareness-training-phishing-simulations (Accessed: 14 July 2015).
Drias, Z., Serhrouchni, A. and Vogel, O. (2015) 'Analysis of Cyber Security for Industrial Control Systems', in *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. Shanghai, China: IEEE, pp. 1–8. doi: 10.1109/SSIC.2015.7245330.
Evans, M. *et al.* (2016) 'Human Behaviour as an aspect of Cyber Security Assurance', *arXiv preprint arXiv:1601.03921*, pp. 1–22. Available at: http://arxiv.org/abs/1601.03921.
Fan, X. *et al.* (2015) 'Overview of cyber-security of industrial control system', in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 - Proceedings*. IEEE Xplore, pp. 1–7. doi: 10.1109/SSIC.2015.7245324.
Gonzalez, C. *et al.* (2014) 'Cognition and Technology', *Cyber Defense and Situational Awareness*. Edited by A. Kott, C. Wang, and R. F. Erbacher. Springer Publishers: Advances in Information Security 62, pp. 93–117. doi: 10.1007/978-3-319-11391-3.
Goodall, J. R., Lutters, W. G. and Komlodi, A. (2004) 'I Know My Network: Collaboration and Expertise in Intrusion Detection', in *ACM conference on Computer supported cooperative work*. Illinois, USA: ACM, pp. 342–345. doi: http://doi.acm.org/10.1145/1031607.1031663.
Goodall, J. R., Lutters, W. G. and Komlodi, A. (2009) 'Developing expertise for network intrusion detection', *Information Technology & People*, 22(2), pp. 92–108. doi: 10.1108/09593840910962186.
Harp, D. and Gregory-Brown, B. (2016) *SANS 2016 State of ICS Security Survey*. Available at: https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067.
Hershberger, P. (2014) *Security Skills Assessment and Training: The "Make or Break" Critical Security Control*, *SANS Institute InfoSec Reading Room*. Available at: https://uk.sans.org/reading-room/whitepapers/leadership/security-skills-assessment-training-critical-security-control-break-o-35637.
Howarth, F. (2014) 'The Role of Human Error in Successful Security Attacks', *Security Intelligence Website*. IBM Security Intelligence. Available at: http://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/#.VYee7Pmqqko.
IRM (2015) *Amateyrs attack technology. Professional hackers target people*, *Website Article*. Available at: https://www.irmplc.com/issues/human-behaviour/ (Accessed: 15 June 2015).
Johansson, E., Sommestad, T. and Ekstedt, M. (2009) 'Issues of cyber security in SCADA-systems-On the importance of awareness', *The 20th International Conference on Electricity Distribution CIRED*, (0969), pp. 1–4. doi: 10.1049/cp.2009.1099.
Kaspersky-Labs (2015) *Kaspersky-Labs: Empowering Industrial Cyber Security*. Available at: http://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Empowering-Industrial-Cyber-Security.pdf.
Knowles, W. *et al.* (2015) 'A survey of cyber security management in industrial control systems', *International Journal of Critical Infrastructure Protection*. Elsevier, 9, pp. 52–80. doi: 10.1016/j.ijcip.2015.02.002.
Kraemer, S. and Carayon, P. (2003) 'A Human Factors Vulnerability Evaluation Method for Computer and Information Security', in *Human Factors and Ergonomics Society Annual Meeting*. SAGE Publications, Inc, pp. 1389–1393. doi: 10.1177/154193120304701202.
Luallen, M. (2014) *Breaches on the Rise in Control Systems : A SANS Survey*.
Macaulay, T. and Singer, B. L. (2012) 'ICS Vulnerabilities', in *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton, FL: CRC PRESS : Taylor & Francis Group, pp. 81–124. Available at: https://www.crcpress.com/Cybersecurity-for-Industrial-Control-Systems-SCADA-DCS-PLC-HMI-and/Macaulay-Singer/9781439801963.
Mandiant (2017) *M-Trends 2017: A View From the Front Line*. Available at: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.
Manikandan, S. (2011) 'Measures of central tendency: The mean', *Journal of Pharmacology and Pharmacotherapeutics*, 2(2), p. 140. doi: 10.4103/0976-500X.81920.
Mirashe, S. P. and Kalyankar, N. V (2010) 'Cloud Computing', *Communications of the ACM*. Edited by N. Antonopoulos and L. Gillam. ACM (Informatik im Fokus), 51(7), p. 9. doi: 10.1145/358438.349303.
Mitnick, K. D. and Simon, W. L. (2003) *The Art of Deception: Controlling the Human Element in Security*, *BMJ: British Medical Journal*. New York, New York, USA: ACM. doi: 0471237124.

Murphy, G. B. (2015) 'Cybersecurity in the Chemical Industry', in Leclair, J. (ed.) *Protecting Our Future, Volume 2: Educating a Cybersecurity Workforce*. Hudson Whitman/ ECP, p. 234. Available at: https://books.google.co.uk/books?id=CzcnCgAAQBAJ&pg=PT31&lpg=PT31&dq=industrial+attacks+that+target+human+elements&source=bl&ots=q1PoLJtHBm&sig=h77CQEvTXIaeO0RbqL5Khm8tzpk&hl=en&sa=X&ved=0ahUKEwiFioqCrKnWAhWEK8AKHepCCrQQ6AEIODAD#v=onepage&q=industrial att.
Navarro, L. (2007) 'Train employees - your best defense - for security awareness', *SC Magazine Online*. Available at: http://www.scmagazine.com/train-employees--your-best-defense--for-security-awareness/article/34589/.
Nicholson, A. *et al.* (2012) 'SCADA security in the light of Cyber-Warfare', *Computers & Security*, 31(4), pp. 418–436. doi: 10.1016/j.cose.2012.02.009.
Nikolakopoulos, T. (2009) 'Evaluating the Human Factor in Information Security', *Masters Thesis*. Oslo University College, pp. 1–88. Available at: http://folk.uio.no/eivindkv/ek-thesis-2003-05-12-final-2.pdf.
NIST (2004) *Standards for security categorization of federal information and information systems*, *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*. Gaithersburg, Maryland. doi: 10.6028/NIST.FIPS.199.
NIST (2013) *Security and Privacy Controls for Federal Information Systems and Organizations*, *SP-800-53A Rev 4*. National Institute of Standards and Technology (NIST). doi: 10.6028/NIST.SP.800-53Ar4.
PA Consulting Group (2015) *Security for Industrial Control Systems : Framework Overview - A Good Practice Guide*. London: The Crown. doi: Retrieved June 30, 2015, from http://www.21stcenturyskills.org/ index.php?option=com_content&task=view&id= 254 &It emid=120.
Paganini, P. (2016) *The number of ICS Attacks continues to increase worldwide*, *Security Affairs Website*. Available at: http://securityaffairs.co/wordpress/54792/security/ics-attacks-2016.html (Accessed: 24 April 2017).
Pan, C., Zhong, W. and Mei, S. (2015) 'Finding the Weakest Link in the Interdependent Security Chain Using the Analytic Hierarchy Process', *Journal of Advances in Computer Networks*, 3(4), pp. 320–325. doi: 10.18178/JACN.2015.3.4.190.
Parsons, K. *et al.* (2010) *Human Factors and Information Security : Individual, Culture and Security Environment*, *Science And Technology*. Edinburgh South Australia. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf.
Parsons, K. *et al.* (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers and Security*. Elsevier Ltd, 42, pp. 165–176. doi: 10.1016/j.cose.2013.12.003.
Paul, C. L. and Whitley, K. (2013) 'A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness', in Marinos, L. and Askoxylakis, I. (eds) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer, Berlin, Heidelberg, pp. 145–154. doi: 10.1007/978-3-642-39345-7-16.
Ralston, P. A. S., Graham, J. H. and Hieb, J. L. (2007) 'Cyber security risk assessment for SCADA and DCS networks.', *ISA transactions*, 46(4), pp. 583–94. doi: 10.1016/j.isatra.2007.04.003.
Ramakrishnan, S. and Testani, M. (2011) 'People , Process , Technology - The Three Elements for a Successful Organizational Transformation', *IBM Path Forward to Business Transformation*. IBM Centre for Learning and Development, pp. 1–21. Available at: http://www.iienet2.org/Details.aspx?id=24456.
Robert, H. (2015) *Humans "often the weakest link" when it comes to cyber security*, *NCC Group Website: New Room*. Available at: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/news/2015/july/humans-often-the-weakest-link-when-it-comes-to-cyber-security/ (Accessed: 10 September 2015).
Russell, C. (2002) *Security Awareness - Implementing an Effective Strategy*. Available at: https://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418.
Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information and Management*. Elsevier B.V., 51(2), pp. 217–224. doi: 10.1016/j.im.2013.08.006.
Stouffer, K. *et al.* (2015) *Guide to Industrial Control Systems (ICS) Security - NIST.SP.800-82r2*. Available at: http://dx.doi.org/10.6028/NIST.SP.800-82r2.
Tobias, S. (2014) *2014: The Year in Cyberattacks*, *Newsweek*. Available at: http://www.newsweek.com/2014-year-cyber-attacks-295876 (Accessed: 23 November 2016).
UK-Cabinet-Office (2012) *10 Steps to Cyber Security*, *Cyber Security Strategy*. Available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary (Accessed: 26 March 2015).

Vishwanath, A. (2016) ‘Cybersecurity ’ s weakest link is humans’, *The Conversation*, May, pp. 2016–2018. Available at: https://techxplore.com/news/2016-05-cybersecurity-weakest-link-humans.html%0AThis.
Wang, P. A. (2013) ‘Assessment of Cybersecurity Knowledge and Behavior : An Anti-phishing Scenario’, in *ICIMP 2013: The Eighth International Conference on Internet Monitoring and Protection*. Rome, Italy: IARIA, pp. 1–7. Available at: https://www.thinkmind.org/index.php?view=article&articleid=icimp_2013_1_10_30003.
Workman, M., Bommer, W. H. and Straub, D. (2008) ‘Security lapses and the omission of information security measures: A threat control model and empirical test’, *Computers in Human Behavior*, 24(6), pp. 2799–2816. doi: 10.1016/j.chb.2008.04.005.

Human factor security: evaluating the cybersecurity capacity of the industrial workforce

Ani, Uchenna Daniel

2019-03-11

Ani U, He H, Tiwari A. (2019) Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, Volume 21, Issue 1, March 2019, pp. 2-35

https://doi.org/10.1108/JSIT-02-2018-0028