

Can humans be patched?

A short current state review.

Karan Luthra

Ledarskap & Organisation HT19
Kandidatuppsats
15 hp
VT20
Handledare: Sissi Ingman

Can Humans Be Patched?

Karan Luthra

Malmö University

Supervisor:

Sissi Ingman

Abstract

Information security is a growing concern among organisations. A large number of security breaches involve employee negligence as human activity is considered as a critical factor in information security. Therefore, organisations must cultivate an information security culture (ISC). The purpose of this study is to enhance our understanding of information security culture and elucidate the human's role in information security. A qualitative systematic literature review from 2015 to 2019 yielded 27 journal articles which identified key concepts within the research field. Results demonstrate four sets of concept categories; Understanding ISC, Information Security Policy (ISP) compliance, Cognition and Awareness. 26% attempted to conceptualise measure ISC, 44.4% discussed ISC as compliance with ISP, 22.2% points out security behaviour with cognitive models, and finally 7.4% attribute awareness training as motivating factor for ISC. These findings suggest that ISC is a nascent field and that human behaviour goes above and beyond policy compliance. Academics suggest that social science approaches provide a deeper understanding of human organisational behaviour towards security. Organisations should cultivate ISC by encouraging employees to behave securely rather than behave as directed by policies.

Keywords: Information security, Information security culture, Information security behaviour, organisational security behaviour, Information security policy, compliance

Sammanfattning

Informationssäkerhet är ett växande problem bland organisationer. Ett stort antal säkerhetsöverträdelser innefattar vårdslöshet bland anställda eftersom den mänskliga uppförande anses vara den viktigaste faktorn för informationssäkerhet. Därför är det avgörande för organisationer att utveckla en informationssäkerhetskultur. Syftet med denna studie är att öka vår förståelse av informationssäkerhetskulturen och belysa människans roll i informationssäkerhet. En kvalitativ systematisk litteraturöversikt från 2015 till 2019 gav 27 journalartiklar som identifierade nyckelkoncept inom forskningsområdet. Resultatet uppvisar fyra olika konceptkategorier; Förstå informationssäkerhetskultur, Informationssäkerhetspolicy lydighet, Kognition och medvetenhet. 26% försökte definiera och conceptualisera och även mäta informationssäkerhetskultur. 44,4% diskuterade Informationssäkerhetskultur som lydighet med ISP, 22,2% påpekar säkerhetsbeteende med hjälp av kognitiva modeller, och slutligen 7,4% kännetecknar kunskap och medvetenhet som motiverande faktor för informationssäkerhetskultur. Dessa resultat tyder på att informationssäkerhetskultur är ett framväxande område och att mänskligt beteende går utöver policy lydighet. Akademiker föreslår att samhällsvetenskapliga tillvägagångssätt ger djupare förståelse för mänskligt organisatoriskt beteende mot säkerhet. Organisationer bör därför kultivera ISC genom att uppmuntra anställda att bete sig informationssäkert snarare än att bete sig enligt policyriktlinjer.

Acknowledgements

This bachelor's thesis was by Karan Luthra, during the autumn of 2019 and is the final part of the course Leadership and Organisation (OL110A) at Malmö University. I would like to extend my gratitude towards the most significant contributors and supporters. First, I would like to thank my academic supervisor Sissi Ingman, whose guidance and feedback have been very helpful during the thesis process. I am upmost grateful for all the guidance and encouragement that I have received throughout the period, it has been a great learning experience. Secondly, I would also want to express my gratitude to all the course leaders, Jonas Lundsten and Maria Appelqvist for sharing your ideas, knowledge, and experience. I would also like to express my appreciation to Malmö university for allowing me to develop my knowledge in leadership and organisational science. Lastly, I am truly grateful for all the support I have received from my friends and family.

Malmö, 2020-01-19

Karan Luthra

Table of Contents

| | |
|---|-----------|
| <i>Abstract</i> | 2 |
| <i>Sammanfattning</i> | 3 |
| <i>Acknowledgements</i> | 4 |
| <i>Can Humans Be Patched?</i> | 7 |
| <i>Introduction</i> | 7 |
| Theoretical background | 9 |
| Information security. | 9 |
| Information security culture | 9 |
| Organisational compliance and information security policies. | 11 |
| Related research..... | 11 |
| Purpose | 12 |
| Research questions | 13 |
| Delimitations | 13 |
| <i>Methodology</i> | <i>14</i> |
| Search and evaluation | 16 |
| Methodology critique | 17 |
| <i>Results</i> | <i>18</i> |
| Understanding information security culture | 19 |
| Compliance to policies | 21 |
| Cognition | 25 |
| Education, training and awareness | 27 |

Discussion31

Conclusion33

References34

Appendix42

Can Humans Be Patched?

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards -- and even then, I have my doubts. - Eugene H. Spafford

Introduction

In recent years, the spread of digital technologies has provided individuals, organisations, and societies in general with new opportunities. It has contributed to vast interconnectivity and globalisation among organisations. With the emergence of the Internet of Things, organisations are getting even more digitised. Like electricity, information is therefore considered as an essential commodity (Van Niekerk & Von Solms, 2010). In the world we live in unfortunately, information is a lot more valuable than other basic commodities. It is highly doubtful that a disgruntled person in a different part of the world can affect a company's electricity. The same cannot necessarily be said about valuable information. The proliferation of data makes them rich targets for criminals. Thus, organisations must ensure their access to information by protecting their assets. Organisations will be unable to do business without their access to their information resources. Protecting the information resources has no direct return on investment for a company (Van Niekerk & Von Solms, 2010). Safeguarding information resources does rarely generate income for organisations. Therefore, executives and organisations, in general, are rarely interested in information security as it is often seen as detrimental to business goals because it makes systems less usable.

Most of research in the field of information security has concluded that humans are the main cause of security incidences (Mahfuth et al., 2017; Tolah et al., 2017). As technology has advanced exponentially over the past decade so has threats towards organisations. When information is regarded as a highly valuable asset that needs to be protected from those threats.

Many organisations have lost billions as a result of information security violations (PricewaterhouseCoopers, 2018). Both, internal and external risks continuously evolve and often result in breaches which lead to negative effects on customer trust. In many cases, employee behaviour is the main cause of several security incidents and privacy breaches (Da Veiga & Martins, 2015). A survey conducted by PricewaterhouseCoopers (2018) found that current employees (30%) and former employees (26%) contribute to top information security incidents compared to hackers (23%) and competitors (20%). Employee behaviour that causes security

breaches could be a result of error, negligence or intentional. Slips and mistakes, whether intentionally or lack of knowledge, employees are the greatest threat to information security as it can result in privacy breaches and management of human errors should be prioritised (Da Veiga & Martins, 2015; Mitnick et al., 2013). An organisation's information security strategy should systematically address this human factor.

In general, the human element is considered the weakest link in information security (Mahfuth et al., 2017). Several studies indicate that information security cannot be achieved by technology alone, as the system is operated and managed by the humans (Glaspie & Karwowski, 2018; Karlsson et al., 2015; Van Niekerk & Von Solms, 2006; Van Niekerk & Von Solms, 2010). Human error and negligence are the cause of various security violations where technology is less likely to cause problems within organisations. Research emphasises that employee behaviour should be addressed to protect information assets and it is important to remember that not only is trusted technical infrastructure needed but also good corporate governance (Da Veiga & Eloff, 2010). On one hand, employees attribute a prominent role in creating threats to an organisation, and the other hand play a key part in protecting against or preventing such violations" human firewall" (Drogkaris & Bourka, 2019; Mahfuth et al., 2017).

The information security studies that address the problem of human being for the most part from engineering disciplines alternative to social sciences (Drogkaris & Bourka, 2019). Technological solutions are insufficient for organisational security. Managing employees to behave securely are approached in a technical fashion for them to comply with organisational directives. Multiple sources debate the lack of human involvement in security project, for instance how they interact and relate to security (Pfleeger et al., 2014; Stewart & Jürjens, 2017). In their seminal research, Dhillon and Backhouse (2001) explain that the information is predominantly viewed as a functionalistic and technical perspective. In their work, the authors criticize the information systems and security research field for having a simplistic view of the individual regardless of the complex nature of humans and organisations (Dhillon & Backhouse, 2001). Their critique lays the basis for an interpretive/socio-organisational perspective in managing security issues.

As several authors concur, a holistic information security management approach underlines the significance of the human element when ensuring information throughout the organisation (Dhillon & Backhouse, 2001; Rocha Flores et al., 2014). This accounts for

employees' attitudes, beliefs, norms, behaviour, leadership, culture, employee awareness. For this reason, cultivating a good information security culture is therefore vital for information security.

The rest of the paper is structured as follows. The following section will present theoretical foundation describing information security culture and information security policy. Shortly after, related research and the purpose will be presented. The methodology section presents the evidence gathering process which is done by using a systematic literature review. The section that follows presents the findings from the review process. Here, a summary from all the literature is described to answer the research questions. Finally, the paper ends with a discussion of the results and conclusions drawn with future research.

Theoretical background

In this section, an overview of the main concepts and theories that are important for this study will be provided.

Information security.

Information that is managed by an organisation must be safeguarded. Information security is the practice of protecting and mitigating risks from the information. Its main concern is protection of information systems from unauthorised access, use, disclosure, disruption, modification or destruction (Adéle Da Veiga & Martins, 2015; Nieves et al., 2017). It maintains the (CIA) Confidentiality; preventing unauthorised users, Integrity; completeness, accuracy and validity of information and Availability; access to the information at any point in time without impeding on productivity (Da Veiga & Martins, 2015).

As information is regarded as an essential asset for a given organisation, protecting it is crucial to ensure the stability of the organisation by maintaining the CIA of that information. Some researchers argue that security of information can be protected and managed if an effective information security culture is taken into account and the employees can recognise and manage their perceptions about securing their organisation's assets.

Information security culture

Schein (2009) defines organisation culture as "a pattern of basic assumptions invented, discovered, or developed by a given group as it learns to cope with its problems of external

adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems”. This way of approaching culture is widely accepted in information security (Van Niekerk & Von Solms, 2006).

Schein’s (2009) model delineated three different levels of culture. Artefacts; are what can be observed, seen heard and felt in an organisation i.e. what occur in the organisation without any necessary skills. Espoused values; are the organisation’s official viewpoints that encompass values, principles and visions. These values are communicated with mission statements, strategy documents, code of conduct and other documents that describe the organisation’s values. Shared tacit assumptions; consists of beliefs and values of employees that have been adopted from the organisation’s success over time. The values, assumptions and beliefs have shared and accepted among the employees (Schein, 2009).

Researchers characterise ISC as a subculture of organisation culture as it supports these three aforementioned levels. It includes the daily activities, guidelines and practices of the employees to them protect the information assets and reduce risk. However, without knowledge information security cannot be ensured (Van Niekerk & Von Solms, 2010).

In this study, ISC is defined as “Shared patterns of thought, behaviour, and values that arise and evolve within a social group, based on communicative processes influenced by internal and external requirements, are conveyed to new members and have implications on information security” (Hallberg et al., 2015). It guides behaviour when interacting with information technology systems and avoids jeopardising of information assets.

Creating an information security culture within an organisation has the potential to minimize the harmful interactions of employees towards the organisation’s information assets. Further, it will reduce the risk of employee misbehaviour when they interact with such assets (Van Niekerk & Von Solms, 2010).

Numerous studies indicate that the employees’ attitude and lack of security awareness are the most significant contributors to security incidents. A robust information security culture can aid at minimising the risk from employee behaviour when interacting and processing information. To reduce the risk of security failures, organisations should focus more on employee behaviour and promoting a security-aware culture (Da Veiga & Eloff, 2010). Despite being a potential problem, employees have the capacity in reducing the risk towards information assets

(Nel & Drevin, 2019). An important aspect to strengthening information security is to have high compliance among employees with the security rules and regulations (Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015; Karlsson et al., 2015).

Organisational compliance and information security policies.

Compliance is an organisational term to understand the level of employee's commitment to organisational directives. The directives are manifested as policies in the organisation. ISP is defined as "directives, regulations, rules, practices that prescribe how an organisation manages, protects and distributes information" (Nieles et al., 2017). The ISP guides the organisation's approach to information security and provides a structure for setting objectives and controls, including risk assessment and risk management (ISO/IEC 27001, 2013). It governs the protection of information through and is regarded as best practice by the International Organisation of Standardisation. According to the standard it aids "to provide management direction and support for information security following business requirements and relevant laws and regulations" (ISO 27001 Controls and Objectives, Annex IX). ISP is designed to communicate security procedures in which assigns clear roles and responsibilities to provide employees with guidance during incidents (Sommestad, 2018).

Since information security has shifted its attention from technology to human aspects, many authors have investigated the effect ISP has on information security culture (Sommestad et al., 2014). Organisations are required to have an ISP integrated. These policies set mandatory guidelines to form favourable behaviour when managing information assets along with complying with organisations objectives (Sommestad, 2018). When policies are complicated and ambiguous, can lead to difficulties for employees to understand or even follow, which in turn leads to negative attitudes and unwanted behaviour.

Related research.

Studies covering the past two decades have provided important information on the complex nature of ISC.

Karlsson et al. (2015) conducted an extensive state-of-the-art review ranging between 2000 and 2013 through classifying ISC studies based on four main categories: Research topic, Underlying theory, Purpose and methodology. The study provided a clear summary of the

particular themes investigated, including the theories and concepts that influence the concept of ISC. Findings show that the research was mostly descriptive or theoretical, it was difficult for practitioners to adopt the framework or measuring tools which have not been empirically tested (Karlsson et al., 2015). However, Karlsson et al. (2015) fail to focus on how these underlying theories influenced the ISC.

Recently, Nasir et al., (2019) conducted a review between 2000-2017, of all the literature regarding the dimensions of ISC. Although there are numerous studies in this area there is a lack of widely accepted dimensions for ISC as different perspectives and concept are used (Nasir et al., 2019). The proposed framework and models lacked in generalisability. The authors suggest that the field has no unifying foundation that captures the essence concretely. These reviews show that there is no consensus, which indicate a nascent field and lacks the propensity of the human element.

Purpose

Given the evidence of immature information security culture, the purpose of this study is to elucidate the human aspect in information security. More specifically, the review aims to clarify the current research on human behaviour regarding information security because information security behaviour cultivates ISC (Da Veiga & Eloff, 2010). The motivation for conducting this review is that current research fails to develop a unanimous conclusion that is generalisable across organisations (Karlsson et al., 2015; Mahfuth et al., 2017; Nasir et al., 2019). Therefore, some researchers have determined the field of information security culture as nascent, and the subject of culture and human behaviour is complicated. This paper will focus on the organisational cultural aspects regarding information security. Specifically, how the current research field addresses the human aspect of information security in organisations. The research will be reviewed through an organisation theoretic perspective to shine a different light on the problem.

The present study also aims to benefit the field in future ISC-related studies by contributing to the nascent field. It has the potential to clarify the importance of information security culture for organisations and aid practitioners to deepen their understanding of complex human organisational behaviour.

Research questions

To examine how ISC is viewed in current research and what role the human plays in the literature, the study used the following research questions:

What is the current state of research field regarding information security culture? How is ISC defined by researchers?

How do the researchers address the information security issues stemming from the human? How are humans discussed in their research? How come humans are the weakest link?

Delimitations

This review will only focus on the human behavioural aspects of information security regarding organisational science, in other words, the culture. It does not seek to address the definition of information security nor discuss organisation culture. The current state of information security culture literature will be discussed in a descriptive fashion and thus not focus on practical considerations. Thus, how literature addresses the concept of the human role in information security as the “weakest link”.

Methodology

As previously mentioned, the field is quite nascent and immature. Meta studies ranging from 2000 to 2017 have concluded a disagreement among researchers and there lacks a stable generalisable model that can explain the complex nature of human behaviour towards information security (Karlsson et al., 2015; Mahfuth et al., 2017; Nasir et al., 2019). Any empirical research without a solid theoretical foundation might be considered fruitless. Therefore, the present review will examine the current research field following a systematic literature review strategy discussed by Denscombe (2014, p. 132).

A systematic literature review is a method to identify, evaluate, and interpret research relevant to the research question or area of interest. It provides a summary of what has been published on a research topic, in this case, ISC. The most common reasons for conducting a systematic literature review are, summarizing existing evidence, identify gaps in current research or background for new research. It is beneficial in broad research areas where many publications exist (Denscombe, 2014, p. 133). Systematic literature reviews are used by a range of practitioners who want to get a reliable overview of the evidence that is currently available on a specific topic. It aims to arrive at a conclusion about the state of knowledge on a topic based on a rigorous and unbiased overview of all the research that has been undertaken on that topic (Denscombe, 2014, p. 132). A main key point is the rigorous search for data and transparency in the review methods. According to Denscombe (2014, p. 134) five criteria must be met in order for a systematic review to work well.

1. The topic of interest must be clearly defined and narrowly focused.
2. A sizable body of research findings must already exist on the topic.
3. The available evidence must come from studies that use similar methods.
4. The evidence must lend itself to measurement, comparison and evaluation.
5. The findings are usually based on quantitative data.

Though there has been some attention of including qualitative research within systematic reviews. In social sciences, qualitative research is more likely to equate to quantitative research, offering its contribution to knowledge (Denscombe, 2014, p. 134). Rather than comparing and evaluating methodologies and their results, qualitative systematic literature reviews the findings through qualitative analysis methods (Denscombe, 2014, p. 134). Therefore, the present study employed a concept-centric approach to the literature, which focused on highlighting key

constructs and relationships in each article. Categorising research around key concept enables an enhanced synthesis of the literature (Webster & Watson, 2002).

Since the research on ISC is regarded as nascent by researchers and contains heaps of research across various disciplines, mostly functionalistic/technical perspective, the present study conducted a systematic literature review using an inductive approach to answer the research questions. The reason being that it enables concepts to emerge from the literature and thoroughly understand the current state of ISC in the research field and determine the human aspect regarding information security.

The present study adopted Denscombe's (2014, p. 135) seven main stages to describe both the process of conducting the review and the reporting process:

1. Scope of the study

The chosen subject has to be specific and narrow to delineate the content of the search. Systematic reviews are inadequate with broad and vague topics since it would make it difficult to decide what research findings to search for and which evidence to consider (Denscombe, 2014, p. 135). All significant choices during the process need to be described and justified for full transparency.

2. Search process

Search terms that accurately describe the chosen topic should be considered. Similarly, relevant academic databases should be well selected to produce best search results. Besides published articles, the search should include unpolished reports and conference papers for the topic to be as comprehensive as possible. However, small-scale research is likely to focus primarily on published work (Denscombe, 2014, p. 135).

3. Quality evaluation

Here, the exclusion and the inclusion criteria are defined, and research is filtered out that are unrelated to the topic. The process needs to be made explicit and justifiable criteria for decisions (Denscombe, 2014, p. 136).

4. List of sources included in the review

In this stage, the search process is illustrated with a simple flowchart diagram indicating the number of studies included and excluded at each stage of the review. Furthermore, a table of the bibliographic detail is provided which allows researchers to find the source and check the contents (Denscombe, 2014, p. 138).

5. Descriptive summary

The review from the final stage of the process is categorised and descriptively summarised. When and where the studies were conducted, which research method was used and by which institution was responsible for it (Denscombe, 2014, p. 139).

6. Analysis

The literature is thoroughly analysed to with an aptly chosen approach to identify emerging patterns in research. In this case, concept-centric analysis enables academics to highlight key ideas and characteristics of the research, such as the methodology and theoretical frameworks (Webster & Watson, 2002).

7. Conclusion

The study should provide with a clear practical value and conclusions. It should also provide a clear description of current state of the topic and suggest future research for the topic (Denscombe, 2014, p. 141).

Search and evaluation

A review plan was developed for this study following the seven stages mentioned above. To capture the quality of the issue in organisational theoretical perspective, specific search terms were selected. Therefore, interest lies in the organisation cultural aspect in the domain of information security. In this case, management relates to practical actions to create and maintain information security, in contrast to a culture which are patterns of basic assumptions developed by a group to cope with external problems in the organisation (Schein, 2009). For this reason, management will be disregarded.

With the pace which technology is growing, the date range for publication will include the past 5 years, ranging from 2015 to 2019. To narrow the search further, sources such as

conference papers and non-peer review articles were excluded. Peer review articles ensure credible research compared to non-peer reviewed articles (Denscombe, 2014, p. 231). It reduces the likelihood for biases and errors since multiple experts in the field review the publications. However, there are some drawbacks concerning the prolonged reviewing processes which can lag behind the technological development which might render the research inadequate.

Three leading electronic databases were selected for identifying potential articles, ProQuest, Emerald and Scopus. The search was conducted on the keywords “information security culture” from the period 2015 until 2019. The search was further narrowed down to exclude non-peer reviewed studies to have valid and confirmed studies with verified results from multiple sources. Articles other than the English language were excluded.

Scopus provided with 44 results; emerald with 52 results and ProQuest with 102 results, a total of 198 articles. The title and abstract studies were then screened, and irrelevant studies were excluded along with duplicates. Filtering it down to 36 potential candidates. Articles that did not discuss the human aspect of information security were excluded. These articles were technical in nature and focused on computer systems design. Also, articles that were specific in context, for example, ISC during organisational mergers, whistleblowing or specific cyber threats were excluded. One article was removed due to lack of full-text access. Final filtering excluded research which discussed different management methods, such as knowledge sharing practices and the lack of sufficient management towards information security. Twenty-seven articles met the requirements and are eligible for analysis. For a full overview see flow diagram in Figure 1 in the Appendix. During the analysis stage, all 27 articles were thoroughly read through at least two times with the research questions in mind. Concepts that emerged from the analysis were discussed with the supervisor. Four different categories of concepts distinguished the 27 articles, a comprehensive table was created during the examination presented in Table 1 in the next results section. These concepts demonstrate how the human aspect is portrayed by the research article in regard to information security.

Methodology critique

There is three limitations to consider. Firstly, publication bias, where studies are conducted with the primary reason for getting published and for that reason not all findings do get published. As Nasir et al. (2019) noted that majority of dimensions of information security

culture are contextual and low generalizability, which indicates complex nature of the problem or even a bias towards reporting significantly positive results. The method is based on published findings and cannot cover finding from unavailable sources (Denscombe, 2014, p. 143).

The second limitation concerns incomparability in social science research. Studies are related to the subject but are rarely the same topic. Hence, there is less possibility of comparing and evaluating data from different studies (Denscombe, 2014, p. 143).

Lastly, systematic literature reviews are designed for quantitative data where research experiments and randomised controlled trials produce objective conclusions. However as previously noted by Denscombe (2014), qualitative analysis can bring a different perspective equally valuable provided that the review adheres to the systematic method.

Results

In total, 27 articles were reviewed. Three of them were published within the field of information systems, three articles were from a management journal, another three were from technology and human behaviour research fields, and lastly, 18 were from information and computer security journals.

Analysis of the 27 research articles revealed four sets of delineating categories. The first set contained seven articles discussing information security culture which attempts to identify and operationalise ISC to propose frameworks to do so. Twelve of the articles discussed employee compliance with information security policies and designing effective policies. Six articles explain human behaviour through other psychological and cognitive models as the basis for security issues and attitudes regarding information security. Lastly, two articles illustrate the importance of awareness and training programs to support security behaviour among employees.

The summary depicts the research attention among different disciplines. Agreeing to some extent that ISC is predominantly influenced by functionalistic/technical perspectives.

The following section will illustrate the different categories where a summary of each research will be presented. The reason is to give a transparent view of the current research field in ISC.

Understanding information security culture

As previously mentioned, seven articles of 27 attempts to grasp the concept of ISC. Due to the fragmented and limited view of information security culture framework (Karlsson et al., 2015; Nasir et al., 2019), AlHogails (2015) work aims to present a comprehensive framework that guides organisations and practitioners to create an effective ISC. The proposed framework attempts to combine many organisational variables in one comprehensive framework. It integrates the human, organisation and technology which consists of five different dimensions; strategy, technology, organisation, people and environment (STOPE). The framework also integrates change management principles that guide the ISC (AlHogail, 2015). According to AlHogail (2015) the proposed ISC framework provides with a full system for organisations to develop an effective ISC to minimise information risk and protect assets. To validate the STOPE framework, AlHogail, (2015) implements the framework with an empirical study using three case studies pertaining a survey and interview data. The research aims to illustrate the effectiveness of the framework in describing and explaining ISC within an organisation (Hogail, 2015). The author addresses the problem of the lack of a complete framework in previous literature and suggests a comprehensive framework that encompasses the majority of organisational aspects. To specifically address the human dimension, AlHogail (2015) proposes the Human Factor Diamond which consists of four domains and influences security behaviour; preparedness, responsibility, management, society and regulations. For example, awareness and training, monitoring and sanctions, policies and practices, and social aspects issues.

Moreover, Nel and Drevin (2019) investigated ISC in South Africa and identify key elements that constitute ISC. The authors reviewed the literature concerning security culture and information security. Twenty-one unique security culture elements were identified from six different most cited framework studies. Four additional elements were identified and added from survey results of 113 respondents (Nel & Drevin, 2019). The authors conclude that the elements are the main factors to ensure a strong ISC within an organisation. For instance, the top five key aspects were; Accountability, Ethical conduct, Managerial trust/security leadership, Policy and Fairness towards employees.

The following two articles investigate the cultivation of ISC and the identification of protruding subcultures. The researchers apply Information Security Culture Assessment (ISCA) tool to quantify and measure ISC to identify underlying influencing factors. (Da Veiga & Eloff, 2010). Their tool surveys the employees' attitude and behaviour in organisations.

Da Veiga and Martins (2015) advocate the effectiveness of the ISCA tool to determine inadequacies in an organisations ISC. In a period of eight years across 12 countries, the authors used the ISCA with multivariate analysis to establish whether the awareness training interventions for ISC improved between assessment periods. Their result indicated that awareness and training implementation was critical for cultivating ISC.

Furthermore, Da Veiga and Martins (2017) addressed the characteristic of subcultures that operate in a microlevel within workgroups. Dominant ISC encapsulates the entire organisation originating from the top level of the hierarchy, where information security subculture is defined as a distinctive group of employees that share security values, perceptions and policy principles that deviate from those shared by the majority of the organisation's members (Da Veiga & Martins, 2017). In other words, workgroups can have incongruent values and beliefs due to other cultural factors such as nationality, geographical area, work environment and peer group behaviour.

The authors validated their ISCA tool and provide empirical evidence that ISC can be influenced confidently by the tool, thus implement appropriate actions to increase ISC. These two studies attempt to validate a measurement tool that has the ability to operationalise and capture ISC.

As mentioned previously, the majority of ISC research builds its definition of culture from Schein's (2009) three level model. However, Tang, Li and Zhang (2016) approach ISC through a different model. As ISC being a critical part of an organisations culture, the authors explain ISC through Hofstede's organisation culture framework. They propose a relationship map of Hofstede's organisation culture and propose four dimensions of ISC; Compliance, communication, accountability and governance. These dimensions concluded to be a causal linkage and suitable for explaining the connection between the cultures which could provide a more practical measure for practitioners. Here, the research attempts to conceptualise ISC using Hofstede's six dimensions rather than Schein's (2009) to further our understanding of ISC.

Recently, Wiley, McCormac and Calic (2019) questioned the relationship between ISC and organisation culture, that the interplay between the cultures has not been empirically examined. The authors measured 508 Australian employees Information Security Awareness using Human Aspects of Information security Questionnaire; organisation culture using Denison Organisational Culture Survey and security culture using Organisational Security Culture Measure. Their result from mediation analysis concluded that security culture played an important mediating relationship between organisation culture and information security awareness. The authors suggest that organisations should focus on security culture rather than organisation culture to improve awareness. In contrast to the previous study in the topic, the quantitative analysis suggested that security culture should be addressed separately from organisation culture as it has a stronger mediating effect on awareness than OC (Wiley et al., 2019). The author's conclusion demonstrates the incongruent conceptualisation of ISC. In their view, ISC should be managed irrespective of the organisation's culture.

The seven articles illustrate a representative sample of the current state of ISC. Academics are still undecided on a universal framework for understanding and managing ISC. However, there are indications of common ideas that define ISC in organisational terms i.e. top-level engagement, awareness training among others.

Compliance to policies

Having a security policy alone does not ensure compliance. Twelve of 27 studies addressed security issues as user noncompliance with ISP. The following 13 article is categorised similarly due to one common preconceiving assumption. The authors base their research question on policies being adequate to address information security and that user compliance to policy is desirable to lower security risk (Sommestad et al., 2019). ISC is therefore regarded as a product of employee compliance behaviour with information security policies. However, two of the 13 challenge the assumption of adequacy and discuss the issue of policies being insufficient in communicating its purpose and the reason for security risk.

Parsons et al. (2015) demonstrated the importance of information security culture regarding information security decision making. Their survey of 500 Australian employees revealed a significant positive relationship between information security decision making and information security. By improving security culture in an organisation will result in a positive increase in behaviour of employees and thus improve compliance. Their study indicates the value of ISC in shaping user's behaviour and decision making. The research describes the cultural influence on decision making which primarily advocates "right" decisions as compliant behaviour.

Hwang, Kim, Kim and Kim (2017) conducted an empirical study to answer the question "Why not comply with information security?". They investigated the negative causal relationships between security factors and noncompliance motives. 415 survey responses from employees at organisations with implemented policies were examined. The author's result corroborates with compliance being negatively affected by work impediment, security system anxiety and non-compliance behaviour of peers. Further, the authors conclude that security systems, security education and security visibility reduce both system anxiety and noncompliance behaviours of peers. For work impediment, only security systems reduced employees the hinderance. Thus, the study suggests the importance of security systems, education and visibility in order to reduce non-compliance (Hwang et al., 2017).

Da Veiga (2016) research on comparing policy readers, determine to answer two simple questions. First, do employees who read the policy impact ISC compared to those who have not. Second, if a stronger ISC is established over time for those who have read the policy. ISCA questionnaire was used over eight years across 12 countries and concluded that ISC average score was significantly more positive form policy readers compared to non-readers. Also, ISC had improvement overtime for employees who had read the security policies. It is important to note that awareness is with ISP and compliance rather than awareness towards the security threats itself.

Stewart and Jürjens's (2017) work explain the importance of the human aspect and the lack of it in information security management. Their aim is primarily to encourage management to recognise employees playing a major role in information security. The authors highlight the absence of human influence in security projects which can, in turn, induce noncompliance with

ISP among employees. Furthermore, they propose a set of principle that enhances information security management by identifying human conduct and security related issues.

According to Doherty and Tajuddin (2018) user-centric approach to information security involves perceiving the value of the information the employees are managing. From 55 interviews and seven focus groups, the authors of this study concluded that users take into account their views from their immediate workgroup and other factors concerning to education and ethics (Doherty & Tajuddin, 2018). In particular, users' perception of information value has a clear impact on their motivation to comply with security policies. The authors suggest to proactively educate users that information they are managing is a valuable asset for the organisation and thus increase the willingness to comply with the ISP.

Two following studies addressed the non-compliance issue as a value conflict between information security and other organisational demands.

The difficulties for security managers to understand the rationalities behind employee's non-compliant behaviour is a complex problem (Kolkowska et al., 2017). To address this limitation, Kolkowska, Karlsson and Hedström, (2016) suggested a Value-Based Compliance analysis method and a set of principles for methodically examine different rationalities among employees. Their method seeks to identify differences in values among employees for information security and why they do not comply with security policies. Similarly, Karlsson and Karlsson, (2017) investigated the difference between compliance measures of value-monistic and value-pluralistic measure. A survey from 600 white-collar workers resulted that value-monistic measure determined compliance as a function of employees' intentions, self-efficacy and awareness of ISP. However, when changed to value-pluralistic measure, the results suggested that compliance was a result of the occurrence of conflicts between information security and other organisational demands and values (Karlsson, Karlsson, et al., 2017). The authors suggest that when measuring compliance, practitioners should be aware of underlying values influencing employee compliance. In short, the two research indicate noncompliance issues that can occur due to conflicting values between the individual and the organisation.

The following two studies point out issues regarding policy design. The researchers argue the cause of noncompliant behaviour being inadequate ISP.

Cram, Proudfoot and D'Arcy (2017) took upon the task to synthesise the current state of knowledge regarding organisational ISPs. A systematic literature review of 114 papers identified five different sets of relationships; design and implementation of policies; security policies on the organisation and employees; organisation and employee factors on policy compliance; policy compliance on organisational objectives, and lastly adjustments on the policy design (Cram et al., 2017). The authors outline a framework that combines the construct linkages within the current literature regarding policy design. Similarly, Karlsson, Hedström and Goldkuhl (2017) conducted a practice-based discourse analysis of information security policies in healthcare in Sweden through studying hospitals ISP texts, conducted observations and held interviews. The studies aimed to demonstrate the usefulness of practice-based discourse analysis method for understanding ISP design. Also, to provide a set of criteria for ISP in healthcare. The authors concluded that ISP with high communicative quality has the potential to be a practical and useful tool for information security management.

To summarise, these studies highlight policy design as a factor for noncompliant behaviour among employees. In short, highly communicative ISP has the potential to increase compliance and thus minimise information risk.

The issue of non-compliance can be approached from different directions. Amankwa, Looock and Kritzingler (2018) proposed to tackle the problem by highlighting the importance of an information security policy compliance culture. By nurturing a culture specifically towards policy compliance, could potentially decrease non-compliance among employees in organisations. An empirical survey from a sample of 500 found that certain factors such as supportive organisational culture and employee involvement significantly influenced attitudes towards compliance with ISP (Amankwa et al., 2018).

Finally, Alotaibi, Furnell and Clarke (2019) introduced a point-based system for reporting and dealing with policy compliance. The framework responds by grading employee behaviour both compliance and non-compliance behaviour. The authors suggest practical user monitoring and scoring to enhance compliance and catch non-compliant users.

Cognition

Six research articles approached the human aspect of information security in a social cognitive and psychological perspective. These following studies provide a deeper understanding of human behaviour concerning information security.

Many researchers have concluded multiple times that humans are the weakest link (Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015; Mitnick & Simon 2013). As illustrated previously, a common approach is for users to comply with the ISP to decrease information security risks.

Ashenden (2018) conducted a qualitative interview study to understand employees' attitude towards information security. The author found two different perspectives among users. The first group felt that the organisation was proactive to protect its information and the employees took personal responsibility to keep the information secure. The first group also felt that the risks were exaggerated, and their colleagues were overly cautious. The second group believed that the information security specialist were the ones who were responsible for the information, even though they felt that risks were justified and that colleagues took many risks (Ashenden, 2018). Ashenden's (2008) research illustrate the employees perspective give an intricate picture of how information security is perceived.

The two following articles propose different alternatives for security behaviour. Snyman and Kruger (2017) elaborate on the issue with behaviour thresholds in group dynamics by performing an exploratory investigation. Behavioural thresholds explain that preferences, norms or beliefs are formed by the environment and interactions with others in the immediate group. Humans have an inherent threshold for acceptance of behaviours in groups (Snyman & Kruger, 2017). For example, a peaceful non-violent person can commit violence if enough people in the group commit violence. In an organisational setting, if a new ISP is getting implemented by the managers and want to generate acceptance among employees by impacting a specific number of employees. The authors argue that behavioural thresholds analysis can provide help to determine which security issues are prone to peer pressure or influenced by group behaviour. It can identify key issues on which to focus on security awareness training (Snyman & Kruger, 2017).

Another, research article points out another a human behaviour pattern named “escalation of commitment”. Escalation of commitment involves an individual or a group facing a negative outcome from a decision or action and continuing with that action instead of changing it (Chulkov, 2017). In an organisational context, an employee decides to breach security policies to complete a failing task. Or if managers continue economical investment in security policies and solutions that are ineffective (Chulkov, 2017). The author presents underlying irrational theories or biases that influence information security i.e. Sunk cost effect; where managers continue to invest in projects that are already been heavily invested, Self-justification theory; internal or external justification of a persons’ past mistake in their decisions, either as a psychological defence mechanism or towards co-workers and supervisors. Chulkov (2017) highlight the cognitive irrationalities that could potentially be detrimental to an organisation’s information security. The author suggests a rotation of duties and a change in management to mitigate escalation.

The two following studies examine information security behaviour through social cognitive theories.

Ahmad et al. (2019) research illustrated the importance of security monitoring and social learning factors on security assurance behaviour. Security assurance behaviour is defined as employees’ intentional and effortful actions that are aimed towards protecting and defending information systems (Ahmad et al., 2019). The authors used an online questionnaire to determine the importance of security monitoring to ensure non-negligence among employees. Since learning is a result of observation, the authors suggest the importance of role models supporting the learning process. The research highlights the human as an active participant in safeguarding information asset and ensuring security.

Self-efficacy the ability to believe in oneself to perform a specific action. An individual’s perception of their capability to act exceeds the belief in the action itself, which in turn makes the self-efficacy to perform a secure behaviour a critical predictor of secure behaviour (Mutchler, 2019). Through a web-survey of 211 valid responses, their result indicated that self-efficacy was found to be a significant predictor of behavioural intention to perform a response towards security threats. The author suggests that organisations should make their employees aware of

information security issues so that they can perform secure behaviour and thus comply with the ISP (Mutchler, 2019).

Wong et al. (2019) highlight the importance of ISC in mitigating information leakage in organisations with weak internal control for managing information. Their study addresses the cognitive perspective of accidental leakers as employees can unintentionally disclose information to an unauthorized party. The authors conclude that the human factors deserve more research attention so managers and practitioners could take appropriate strategies to avert information leakage to achieve efficient and effective information sharing (Wong et al., 2019).

These six articles exhibit different theoretical viewpoints that extend beyond policy compliance. The sociological and psychological underpinnings place the human as an autonomous complex entity that requires different approaches than compliant behaviour.

Education, training and awareness

The last two articles point out the security awareness training programs efficacy in promoting secure employee behaviour. These program aims to educate employees on information security and threats to increase awareness. Thus, increasing the protection of valuable information assets (Da Veiga & Martins, 2015).

An article from Chen et al. (2015) addressed the impact of information security awareness programs on ISC. A commonly used program named SETA (Safety Education, Training, Awareness) has long been widely established in many organisations to aid the protection of information systems and assets. The authors aimed to elucidate the relationship between the impact of SETA on the information security culture. A measurement scale was developed and obtained 100 valid responses. Between security policies, SETA programs and security monitoring, SETA programs were significantly more effective in promoting security culture than policies and monitoring. It provides evidence that well-designed and implemented SETA programs can change employees' perceptions of attitude and beliefs on information security (Chen et al., 2015).

Kirova and Baumöl (2018) conduct a similar literature review on identifying factors that affect the success of security education programs such as SETA. The authors aimed to identify which human factors influence SETA effectiveness and summarise a conceptual classification. The classification According to the authors, their research will aid in design and develop SETA programs and establish suitable conditions for integrating them into the organisations (Kirova & Baumöl, 2018).

SETA involves educating employees to understand information security and the dangers of it. These two articles highlight the effectiveness of awareness training as well as the importance it has to shape behaviour and therefore cultivating ISC.

The findings of the present review illustrate the current state of information security culture in the research field over the last five years. Table 1 demonstrates the concept categories found in the literature. It is evident that the majority of the articles, 44.4%, explain secure human behaviour as compliance with ISP. These studies demonstrate the positive effects policies have on lowering information security risks and that obedient employees work best for the organisation's safety. These 12 studies, address non-compliance behaviour from different perspectives such as monitoring employees, creating compliance culture, investigating conflicting values and even the design of policy itself.

The second-largest category, 26% of the articles attempts to conceptualise and quantify ISC through frameworks and assessment tools. AlHogail (2015) and Hogail (2015) proposes a framework for design validation for ISC and verifies his framework with an empirical study. Furthermore, Da Veiga and Martins (2015, 2017) investigate ISC as to identify influencing microlevel subcultures that could be detrimental for organisations, and improving ISC through monitoring and awareness training interventions. Both studies use and validate ISCA tool and suggest ways of cultivating a positive ISC in an organisation with the help of their tool. Furthermore, Nel and Drevin (2019) synthesise a list of important key from the six most cited ISC frameworks. Their research illustrates 21 important factors of ISC. Lastly, Wiley et al. (2019) challenge the tight relationship between organisation culture and security culture, where they recommend that organisations should specifically concentrate on security culture rather than organisation culture.

The third category, 22.2% discussed human error proneness using cognitive and social psychological models for an explanation. These six articles addressed the human regarding its cognition and its limitations. Escalation of commitment, self-efficacy and security assurance behaviour, the behavioural threshold in peer groups, and lastly, employee attitudes and information leakage. To summarise, these researches approached the issue with the human as an active role in managing information security. The cognitive approach highlights complex human behaviour that needs attention.

Finally, the fourth category, 7.4% which are two of the 27 articles, specifically address education, training and awareness. Both review articles exclusively approach security awareness and training as an effective method for increasing security in the organisation.

Regarding ISC, each of the categories places the human's role differently. Majority of the research indicates that compliance to policies is a reliable approach for cultivating ISC. A valid explanation for this trend might be that ISC is a complex phenomenon. Researchers have attempted to propose comprehensive frameworks that could potentially manage ISC. On one hand, this review has found a consensus among researches in defining ISC as a concept relating to organisational culture. On the other hand, there exists little evidence that the comprehensive frameworks have high generalisability (Karlsson et al., 2015; Mahfuth et al., 2017; Nasir et al., 2019). Contextual factors have a significant influence on organisations. The nascency and complexity of ISC introduce a variety of issues. This could explain the popularity of compliance as it provides with a simple and manageable answer for cultivating to ISC. In organisations, practical methods with tangible results for shaping employee behaviour are more appealing.

However, looking at the publication years in Table 1 indicates a shifting trend. More contemporary research is putting interest in social sciences as support for understanding secure behaviour in organisations.

Table 1

Concept categories

| Understanding Culture (7) | Policy compliance (12) | Cognition (6) | Awareness (2) |
|------------------------------|---------------------------|------------------------|--------------------|
| AlHogail (2015) | Parsons et al. (2015) | Chulkov (2017) | Chen et al. (2006) |
| Hogail (2015) | Da Veiga (2016) | Snyman & Kruger (2017) | Webb et al. (2018) |
| Da Veiga & Martins (2015) | Cram et al. (2017) | Ashenden (2018) | |
| Da Veiga & Martins (2017) | Hwang et al. (2017) | Ahmad et al. (2019) | |
| Tang et al. (2016) | Karlsson et al. (2017) | Mutchler (2019) | |
| Nel & Drevin (2019) | Karlsson et al. (2017) | Wong et al. (2019) | |
| Wiley et al. (2019) | Kolkowska et al. (2017) | | |
| | Stewart & Jürjens (2017) | | |
| | Amankwa et al. (2018) | | |
| | Doherty & Tajuddin (2018) | | |
| | Sommestad (2018) | | |
| | Alotaibi et al. (2018) | | |

Note: Twenty-seven research articles categorised into four concepts during the analysis stage.

Discussion

Information security has exclusively focused on securing systems and communication infrastructure that manage information. Humans are treated as components where behaviour can be determined through security policies and controlled through security processes. The security processes are generally inadequate, as even trained and motivated users could not use email encryption correctly nor follow password policies correctly (Adams & Sasse, 1999; Whitten & Tygar, 1999). Since then, further studies have revealed and explained the ineffectiveness security warnings (Herley, 2009) and security awareness and education (Bada, Sasse & Nurse, 2019). According to Bada et al. (2019) SETA programs have not had the desired impact due to the lack of psychological perspective in these programs. Information security has identified human as the “weakest link” and attempts to create security more usable and looked to social sciences to inform the design of policies and procedures (Drogkaris & Bourka, 2019).

Moreover, a fundamental disconnect exists between what security professionals seek from behavioural sciences, and the guidance the professionals offer. Security professionals often attribute noncompliance user behaviour as faulty and searching for interventions to behave to comply with security policies. Thus, many adopt psychology or behavioural models for the purpose to motivate humans and take security seriously. Another set of efforts seeks to reduce human error by application factors and usability principles (Stewart & Jürjens, 2017).

In a modern interconnective society where workers are regarded as responsible agents, organisations need to foster adherence rather than compliance and empower employees’ to encounter the threats (Drogkaris & Bourka, 2019). Employees and users are driven by capabilities and limitations e.g. passwords and they are autonomous agents driven by their goals, values and norms. As Pfleeger et al. (2014) point out, treating humans as the weakest link and directing them to follow directives does not lead to compliant behaviour by employees. Blaming people who not comply with policies is counterproductive.

Awareness of a security measure with the intention to comply and self-efficacy leads to secure behaviour unless the employee finds that such behaviour conflicts with other organisational values and cause decreased productivity (Karlsson, Karlsson, et al., 2017; Kolkowska et al., 2017).

The current state of ISC is still fragmented which suggest that there are no widely accepted dimensions among academics and is still an evolving area. The variations of suggested

frameworks indicate that our understanding of ISC is still nascent (Karlsson et al., 2015; Nasir et al., 2019). Majority of academics emphasise on the important connection of ISC as a subculture of an organisations culture, which according to Wiley et al. (2019) is not the case.

Drogkaris and Bourka (2019) meta-analysis revealed that most results are unreliable as only a quarter of the studies met basic criteria for scientific survey research (Drogkaris & Bourka, 2019; Nasir et al., 2019). The surveys often made adjustments to the validated instruments without revalidating them. Drogkaris and Bourka (2019) state that most of these investigations are an exercise in trying to find something in employees that can be blamed for their non-compliant behaviour and used by organisations to fix it. The majority of these studies cannot be regarded as reliable due to inconsistent results (Drogkaris & Bourka, 2019; Nasir et al., 2019).

The lack of qualitative research approaches overlooks an important facet of human behaviour. Insecure behaviour is mostly due to complicated security procedures as interviewee explained (Ashenden, 2018). There is a growing interest among researchers to investigate human as a central role in information security. Psychological and social cognitive theories promise new insight into our understanding of humans behaving securely and thus cultivating an information security culture.

Although this review makes important contributions to the research field, it does so with certain limitations. by limiting to only five past years ignores previous work that has laid the foundation of ISC. The thoroughness of the review search, the exclusion and inclusion criteria and search keywords could be revised. Only using one key phrase ignores certain concepts for instance “cyber” security culture. Recent research is moving from managing information risk towards managing the cyber space, where humans are regarded as information assets (Gcaza et al., 2017). Additionally, more publication databases could be used, and more keywords would have given a more comprehensive description of the research field. The reviewing process involves subjective justification of articles which needs to be classified into concept categories. This process has not been straightforward, and a chance of some crucial information being overlooked. Additionally, the limitations discussed in the methodology chapter are still concerned.

Can humans be patched? The short answer is NO. But we should stop trying to fix humans and instead cultivate trust. Giving employees the right knowledge and trusting their abilities to perform securely can turn them from weakest link to the strongest firewall.

Conclusion

With the prevalence of information technology, organisations would benefit from having a good information security culture in the long run. The present study has revealed the current state of the research field regarding information security culture. The results of this review reflect on previous research finding in this topic. However, the present study indicates that humans in information security research are more regarded as objects for organisations to manage rather than autonomous subjects. This is largely due to the lack of social science perspective in the research field as the majority of the research are derived from engineering or technical disciplines.

The growing body of literature indicates a shift from policy compliance to understanding human dynamics, where humans have a central role in security development. Cognitive theories have the potential to elucidate threat perception and attitudes towards security, which could provide deeper insight. Simply put, to deal with the “weakest link” humans should behave securely rather than behave with policies. More academics emphasising humans as being a part of the information system. Instead of managing information assets, employees are assets as well as the valuable information they are managing. This, in turn, is redefined as “cybersecurity” where humans cannot be blamed for blunders since they are a part of the cyberspace.

I firmly believe that future direction in ISC studies should attempt to address the human as the responsible person for ensuring the safety of information assets. Researchers should continue studying self-efficacy and self-belief as a motivating factor for cultivating information security. Technology is evolving and so are the threats, as researchers, we must continue to find the answer.

References

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. <https://doi.org/10.1145/322796.322806>
- Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information and Computer Security*, 27(2), 165–188. <https://doi.org/10.1108/ICS-10-2017-0073>
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575. <https://doi.org/10.1016/j.chb.2015.03.054>
- Alotaibi, M. J., Furnell, S., & Clarke, N. (2019). A framework for reporting and dealing with end-user security policy compliance. *Information and Computer Security*, 27(1), 2–25. <https://doi.org/10.1108/ICS-12-2017-0097>
- Amankwa, E., Looock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information and Computer Security*, 26(4), 420–436. <https://doi.org/10.1108/ICS-09-2017-0063>
- Ashenden, D. (2018). In their own words: Employee attitudes towards information security. *Information and Computer Security*, 26(3), 327–337. <https://doi.org/10.1108/ICS-04-2018-0042>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *ArXiv:1901.02672 [Cs]*. <http://arxiv.org/abs/1901.02672>
- Chen, Y., Ramamurthy, K. (Ram), & Wen, K.-W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems*, 55(3), 11–19. <https://doi.org/10.1080/08874417.2015.11645767>

- Chulkov, D. V. (2017). Escalation of commitment and information security: Theories and implications. *Information and Computer Security*, 25(5), 580–592.
<https://doi.org/10.1108/ICS-02-2016-0015>
- Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, 26(6), 605–641. <https://doi.org/10.1057/s41303-017-0059-9>
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207.
<https://doi.org/10.1016/j.cose.2009.09.002>
- da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162–176. <https://doi.org/10.1016/j.cose.2014.12.006>
- da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70, 72–94.
<https://doi.org/10.1016/j.cose.2017.05.002>
- Da Veiga, Adéle. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information and Computer Security*, 24(2), 139–151. <https://doi.org/10.1108/ICS-12-2015-0048>
- Da Veiga, Adéle, & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), 243–256. <https://doi.org/10.1016/j.clsr.2015.01.005>

- Denscombe, M. (2014). *The good research guide: For small-scale social research projects* (5. ed). Open University Press.
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153.
<https://doi.org/10.1046/j.1365-2575.2001.00099.x>
- Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People*, *31*(2), 348–367.
<https://doi.org/10.1108/ITP-08-2016-0194>
- Drogkaris, P., & Bourka, A. (2019). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. *European Union Agency for Network and Information Security (ENISA)*.
<https://doi.org/10.2824/324042>
- Gcaza, N., von Solms, R., Grobler, M. M., & van Vuuren, J. J. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information and Computer Security*, *25*(3), 259–278. <https://doi.org/10.1108/ICS-12-2015-0046>
- Glaspie, H. W., & Karwowski, W. (2018). Human Factors in Information Security Culture: A Literature Review. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (Vol. 593, pp. 269–280). Springer International Publishing. https://doi.org/10.1007/978-3-319-60585-2_25
- Hallberg, J., Andersson, T., Berndtsson, J., Frostenson, M., Hansson, S. O., Hedström, K., Hellberg, S., Johansson, B., Johansson, P., Karlsson, F., Karlsson, M., Karlzén, H., Kolkowska, E., Lundgren, B., Möller, N., Olovsson, T., Posette, A., Prenkert, F., Räisänen, K., ... Ödman, S. (2015). *Definition of information security culture* (Memo

FOI Memo 5253).

<https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%205253>

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 Workshop on New Security Paradigms*

Workshop - NSPW '09, 133. <https://doi.org/10.1145/1719030.1719050>

Hogail, A. A. (2015). Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study. *International Journal of Security and Its Applications*, 9(7), 163–

178. <https://doi.org/10.14257/ijisia.2015.9.7.15>

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, 41(1),

2–18. <https://doi.org/10.1108/OIR-11-2015-0358>

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information and Computer Security*, 23(3), 246–285.

<https://doi.org/10.1108/ICS-05-2014-0033>

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, 67, 267–279.

<https://doi.org/10.1016/j.cose.2016.12.012>

Karlsson, F., Karlsson, M., & Åström, J. (2017). Measuring employees' compliance – the importance of value pluralism. *Information and Computer Security*, 25(3), 279–299.

<https://doi.org/10.1108/ICS-11-2016-0084>

Kirova, D., & Baumöl, U. (n.d.). *Factors that Affect the Success of Security Education, Training, and Awareness Programs: A Literature Review*. 19(4), 28.

- Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, 26(1), 39–57. <https://doi.org/10.1016/j.jsis.2016.08.005>
- Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6. <https://doi.org/10.1109/ICRIIS.2017.8002442>
- Mitnick, K. D., Simon, W. L., & Wozniak, S. (2013). *The art of deception: Controlling the human element of security*. Wiley. <http://rbdigital.oneclickdigital.com>
- Mutchler, L. A. (2019). Response awareness and instructional self-efficacy: Influences on intent. *Information & Computer Security*, 26(4), 489–507. <https://doi.org/10.1108/ICS-05-2018-0061>
- Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, 44, 12–22. <https://doi.org/10.1016/j.jisa.2018.11.003>
- Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information and Computer Security*, 27(2), 146–164. <https://doi.org/10.1108/ICS-12-2016-0095>
- Nieves, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security* (NIST SP 800-12r1; p. NIST SP 800-12r1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-12r1>
- Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information

- Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117–129. <https://doi.org/10.1177/1555343415575152>
- Petticrew, M., & Roberts, H. (2006). M. Petticrew and H. Roberts. *Systematic Reviews in the Social Sciences: A Practical Guide*. Oxford: Blackwell 2006. 352 pp. ISBN 1 4051 2110 6. *Counselling and Psychotherapy Research*, 6(4).
<https://doi.org/10.1080/14733140600986250>
- Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*, 11(4). <https://doi.org/10.1515/jhsem-2014-0035>
- PricewaterhouseCoopers. (2018). *The Global State of Information Security® Survey 2018*. The Global State of Information Security® Survey 2018.
<https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html>
- Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90–110.
<https://doi.org/10.1016/j.cose.2014.03.004>
- Schein, E. H. (2009). *The corporate culture survival guide* (New and rev. ed). Jossey-Bass.
- Snyman, D., & Kruger, H. (2017). The application of behavioural thresholds to analyse collective behaviour in information security. *Information and Computer Security*, 25(2), 152–164. <https://doi.org/10.1108/ICS-03-2017-0015>

- Sommestad, T. (2018). Work-related groups and information security policy compliance. *Information and Computer Security*, 26(5), 533–550. <https://doi.org/10.1108/ICS-08-2017-0054>
- Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 22(1), 42–75. <https://doi.org/10.1108/IMCS-08-2012-0045>
- Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems*, 59(4), 344–353. <https://doi.org/10.1080/08874417.2017.1368421>
- Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, 25(5), 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>
- Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, 17(2), 179–186. <https://doi.org/10.1007/s10799-015-0252-2>
- Tolah, A., Furnell, S. M., & Papadaki, M. (2017). *A Comprehensive Framework for Cultivating and Assessing Information Security Culture*. 13.
- Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476–486. <https://doi.org/10.1016/j.cose.2009.10.005>
- Van Niekerk, J., & Von Solms, R. (2006). *Understanding Information Security Culture: A Conceptual Framework*. 10.

- Webster, J., & Watson, R. T. (2002). *Analyzing the Past to Prepare for the Future: Writing a literature Review*. 11. <https://doi.org/10.2307/4132319>
- Whitten, A., & Tygar, J. D. (n.d.). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. 15.
- Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88, 101640. <https://doi.org/10.1016/j.cose.2019.101640>
- Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M.-L. (2019). Human factors in information leakage: Mitigation strategies for information sharing integrity. *Industrial Management & Data Systems*, 119(6), 1242–1267. <https://doi.org/10.1108/IMDS-12-2018-0546>

Appendix

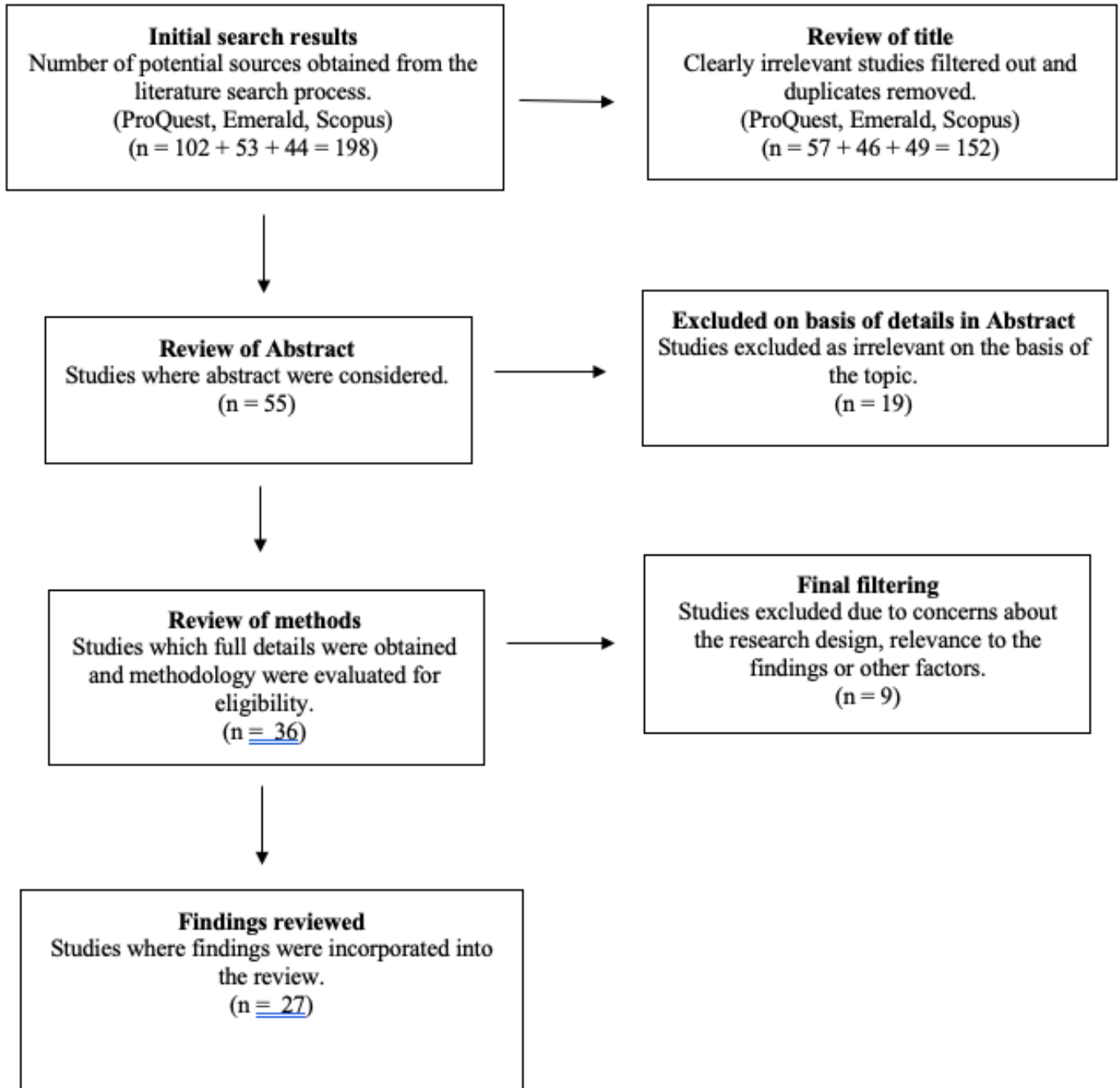


Figure 1. Flowchart of inclusion and exclusion criteria of studies from the review inspired by Petticrew & Roberts (2006).

