A Comprehensive Framework for Understanding Security Culture in Organizations

Alaa Tolah, Steven M. Furnell, Maria Papadaki

A Comprehensive Framework for Understanding Security Culture in Organizations

Alaa Tolah[1-2][0000-0001-8917-9382], Steven M.Furnell[1-3-4]and Maria Papadaki[1]

[1] University of Plymouth, Plymouth, United Kingdom
[2] Saudi Electronic University, Riyadh, Saudi Arabia
[3] Nelson Mandela University, Port Elizabeth, South Africa
[4] Edith Cowan University, Joondalup, Australia
{alaa.tolah,steven.furnell,maria.papadaki}@plymouth.ac.uk

Abstract. Organizational security is exposed to internal and external threats, with a greater level of vulnerabilities coming from the former. Drawing upon findings from prior works as a foundation, this study aims to highlight the significant factors that influence the security culture within organizations. Phase one of the study reports upon an interview-based investigation undertaken with thirteen experienced, knowledgeable security specialists from seven organizations. The main findings confirmed the importance of the identified factors from the previous work. The focus to emerge from the interviews concludes that continuously subjecting employees to targeted training and awareness development improves security culture. Indeed, there was a clear lack of awareness and compliance regarding the implementation and clarity of security policies in organizations. Also, the inefficient training program and limit to specific employees in organizations leads to a lack of awareness and compliance.

Keywords: Security Culture, Human Factors, Qualitative study.

1 Introduction

Nowadays, a knowledge-based economy has become more dynamic than at any time in history, which continues to progress. Technology enables all business operations and information technology to develop into a central concept for most aspects of life. However, information technology developments continually initiate new risks to the security of information assets. The use of ICT can make the violation of information security easier, while many technical approaches to security and counter-measures have augmented in organizations; although this development needs to increase, as many researchers perceive security to be both a "people" and "technical" issue [2, 4]. Nonetheless, technology is less likely to cause problems than human error, which is a cause of the majority security breaches (75% of organizations suffer security breaches by insiders) [13]. Therefore, organizations need to focus on employees' behavior to achieve information security, as many studies examined the human factors and their relation to information security with social psychology issues that determine reasons for unacceptable behavior that leads to security breaches [12]. One approach the or-

ganization can take to manage the security would be developing strategies that enhance security culture [1, 7].

A positive security culture contributes to support organizations in guiding employees to follow security policies, which lowers the potential risk of harmful information interaction by employees, as they develop knowledge and advance their skills correctly, and behave securely in their working environments [2, 17]. The culture that promotes secure human behavior through knowledge, values, and assumptions is better than regulations that merely mandate employees' behavior [1]. Various studies suggest that organizational security culture could lead an employee to act as a "human firewall" [18]; where acting correctly is commonplace [14]. Consequently, organizations are required to use understandable guidelines to develop a culture of security awareness, which utilizes various approaches to improve comprehension [2, 17].

The proposed paper extends the proposed framework by [16], which facilitates an understanding of security culture and its elements. It initially assists in comprehending whether the level of security culture enhances the security of information assets, and also assesses the relationship between influential factors and factors that constitute security culture.

The development of an initial framework is based on Alnatheer's model and a review of academic literature in the security culture. In the proposed framework, the security culture comprises several factors, as the components are structured into: factors that influence security culture (top management, security policy, security education and training, security risk assessment and analysis, and ethical conduct); factors that constitute security culture (security awareness, security ownership and security compliance); and factors of organizational behavior that contribute to workplace behaviors and could influence the security culture (personality traits and job satisfaction) (see Fig. 1). These factors appear to be the most influential factors and are considered as part of the security culture's conceptualization. By understanding the influential factors or reflection factors, it is possible to aid in directing the interaction of humans with information security. These factors provide management with a means to implement adequate security management approaches that include the guidance provision and control implementation in the assessment of security culture.

As this study relied on prior literature to develop an initial security culture framework and to explore a detailed perception and understanding of human behavior, it was considered that using an interview method would enable in-depth information from employees involved in an organization's information security, and understand factors affecting security culture with which are more critical from the perspective of participants. The main aims of the interview were to explore whether all the ten factors within the proposed framework are necessary; which factors are the most important, whether new factors should be incorporated, and to identify new issues that had not previously been considered to alter security culture potentially.

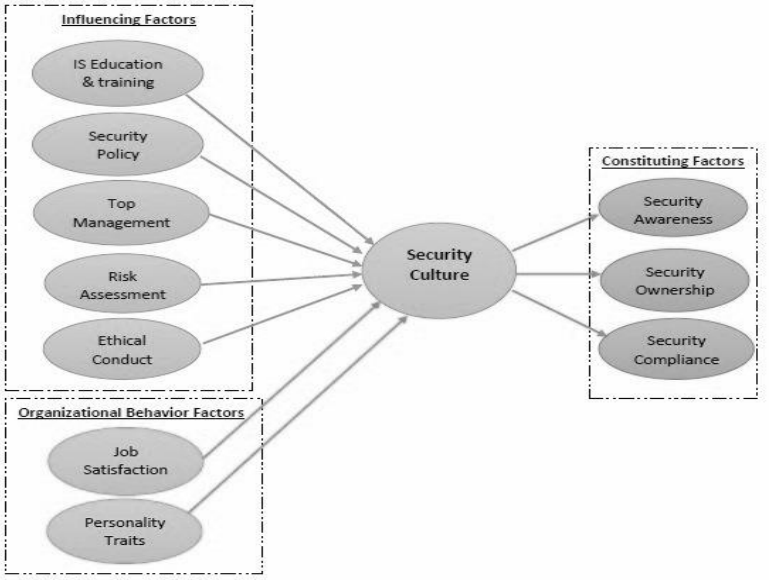

Fig. 1. The comprehensive security culture framework [16]

Therefore, this paper presents the findings from exploratory interviews with IT/security professionals and combines these with the literature review to investigate whether the identified factors are vital for organizations and to determine a base for more comprehensive research through quantitative techniques. The paper initially provides a review of related work for security culture frameworks. Subsequently, the current research method is described with the analytical approaches used to interpret the results. The paper concludes by outlining the research implications and future research.

2 Literature Review of Existing Security Culture Approaches

Instilling an effective culture is vital to create adequate levels of information security. Various studies have focused on security culture, while literature reviews offer an overview that focuses on security culture (Alhogail [2]; Glaspie and Karwowski [8]). Their literature analyzes concluded that most investigated issues in security culture relate to: the conceptualization of culture to identify concepts and factors that affect security culture, the creation of security culture, or an assessment of security culture to measure whether it is an adequate level. Many studies provide various approaches and models that highlight security culture's importance, promote its benefits and provide guidelines to create and assess security culture. The literature analysis showed that most studies demonstrated various essential factors that may shape or change security culture [2]. A comprehensive review of security culture was conducted to gain an overview of the current security culture frameworks, which focused on studies that assess security culture, which presented essential knowledge with regards to fac-

tors that assist in developing security culture [16]. Thirteen research perspectives relate to the creation of security culture and five studies incorporate an assessment of security culture. The security culture is a product of various factors, such as security policy and security training that affect the individual's behavior in organizations [16]. These studies have developed comprehensive security culture models and contributed to how organizations potentially create and maintain acceptable security culture levels.

Studies by Alnatheer [3] and Da Veiga and Eloff [7] provide an approach that utilizes the same framework to assess security culture, which both provide statistically sound assessment instruments to perform security culture assessment. Few studies have provided reliable and valid security culture assessment instruments; Schlienger and Teufel [14] designed a questionnaire to detail how proper rules impact upon employees' security behavior, while Da Veiga and Eloff [7] designed a security culture assessment tool. Moreover, there is minimal coverage of other influential factors, such as individual difference variables and job satisfaction. The positive impacts of these factors on workplace behaviors had proven by studies from D'Arcy and Greene [5] and McCormac [11]. The literature review illustrated that there is a need for more investigation in the area to provide comprehensive frameworks and the best practices of security culture cultivation and assessment. Hence, this study proposed an initial framework that integrates the most important factors that influence security culture. The interview method was adopted to explore and examine the identified factors.

3 Methodology

This study used the pragmatic philosophical approach with mixed methods of data collection. The initial phase was a qualitative design to acquire sufficient information regarding security culture from IT/security specialists in organizations and to explore influential factors. The second phase will be quantitative data for a survey with a minimum sample size of 250 employees from several organizations to develop an understanding of the relationship between factors and to test the framework's validity. The findings from the qualitative phase will be incorporated with the literature review to identify constructs that influence security culture and related survey items. To enhance theoretical propositions, an exploratory interview was adopted to investigate whether all identified factors are necessary for organizations, which also assist in the survey design.

3.1 Sample

It is essential to select organizations from a broad range of sectors and industries, which may require various levels of security. It will help organizations to make individual decisions regarding security culture programs and guide investments in security awareness and training sessions [15]. Access to appropriate organizations was difficult, as certain organizations are restricted against discussing security management. The initial choice of organizations' location was in the UK, due to the study's loca-

tion. However, the low number of respondents in the UK resulted in an invitation e-mail being sent to international organizations' members that had cooperated on past occasions in Saudi Arabia and the USA. The study managed to interview seven individual organizations: two in the UK, one in the USA, and four in Saudi Arabia, which covered private, public and semi-public sectors, and included various industries: four in education, and one insurance, law, and mining, respectively. These organizations have the security infrastructure in place; have technology adoption, and used security management practices. However, the diversity of organizations' geographical locations would assist in advancing the understanding of security culture from varied backgrounds.

A semi-structured was utilized in an exploratory manner, and there was no restriction in sample size. This study does not aim to demonstrate the representation of security culture; it aims to identify factors of more critical importance within organizations. This exploratory study could provide indications of the validity of factors intended in the framework. The results cannot be generalized, although it is possible that the findings from the quantitative survey in the next phase could be generalizable. Access to people with relevant knowledge and experience of organizations' security was sufficient. Nevertheless, only thirteen participants from the IT/Information security department agreed to participate in the interview; experience and knowledge of respondents yield rich data. Table 1 below lists the demographic features for participant organizations.

Table 1. Organizations demographic profile

Org	Type	Size	Location	Sector	No. of interviewees	Interviewees position
A	Public	4000	SA	Education	3	IT assistance director and IT specialists
B	Public	5000	SA	Education	2	IT specialists
C	Private	6000	USA	Education	2	IT specialists
D	Public	5000	UK	Education	1	Enterprise security architect
E	Private	400	SA	Insurance	3	IT supervisor and IT specialists
F	Semi-Public	4000	SA	Mining	1	Security manager
G	Private	1500	UK	Law	1	Security manager
Total					13	

3.2 Data Collection

The primary method for collecting data for discourse analysis was individual interviews from October 2017-January 2018, conducted face to face or through Skype. An interview guide was designed and utilized during the interview to ensure data consistency and minimize bias. The interview questions consisted of four parts, with the first part on demographics and a general overview of participants. The second part

included questions with open-ended answers related to organizations' security practices, how employees are educated and acquire security regulations' awareness. The third part includes questions with open-ended answers that determine security culture behaviors, knowledge, and practices of employees; and part four enabled interviewees to construct individual interpretations.

A pilot study with three respondents was conducted to ensure that the interview guide was appropriate, and participants understood the questions. Subsequently, the language was either in English or Arabic, depending on the preference of each interviewee, although the transcripts were transcribed in English. The average interview time was twenty-five minutes, while certain interviewees refused to have their interviews recorded, due to the perceived sensitive nature of their information, even though the identity of the interviewees and the data were kept confidential.

3.3 Data Analysis

A within-case analysis was used for data analysis, which includes detailed interviews. Each interview assists in providing insight into the identified factors and how different constructs are perceived within real life situations. The interviews provided data regarding security culture in the form of a narrative discussion, instead of analyzed interpretation. The understanding was obtained by reviewing the significant findings and reflecting upon personal views following a review of past literature. The data analysis process in the study includes developing a coding scheme to capture the data's critical content; applying the coding scheme to each identified comment made by the interviewee; and exploring the results' frequencies and patterns, where pieces are taken individually from the analysis and compared with other forms of data to determine which parts are similar or different to establish data correlations.

During the analysis, both explicit and implicit results derived from the interviews. By coding the data, the interviews were sufficiently analyzed, as this was a repetitive process that involved determining consistency and providing data links to the framework's constructs. The data from this repetitive process were correlated and coded into constructs during the analysis stage and resulted in data points for further analysis. Furthermore, data categories were identified, which are: top management, policy, education and training, ethical conduct, risk assessment and analysis, awareness, compliance, ownership and job satisfaction. The selected comments focused on various levels of analysis, such as the comments' structure, the overall content of what was said, and the vocabulary.

4 Results

The interview analysis depicted the perception of employees towards security culture. The findings of the interviews illustrated the relevant signify factors and correlation regarding security culture. The participants responded to the interview questions concerning their organization's practices: the security culture practices, the employee security behavior patterns, and the perceptions for improving security culture. Quota-

tions are used to highlight explanations of the findings, followed by a symbol that denotes the organization's name and the participant's number [A1].

4.1 Security Culture Practices

This section determines information regarding security practices; how employees educate; and acquire the awareness of related security regulations and risks.

- **The Main Information Security Practices and Rules used in the Organization.** Interviewees provided the main security practices used in organizations, which indicated that all seven participating organizations use general security practices, such as security policies, security training, physical and technical measures.
- **Security Education and Training Courses in the Organization.** Interviewees reported whether their organizations provide security training sessions. Eight participants from organizations located in Saudi Arabia and the USA reported an absence of security training programs. Five participants reported security training courses in their organizations: two organizations located in the UK and one in Saudi Arabia. Each organization informed its members regarding information security matters through induction training.
- **Different Methods of Security Awareness and Training Sessions.** The participating organizations use various channels to distribute related security awareness to employees, such as sending e-mails' notification, conducting seminar and training courses, sending text message notification, using posters or displaying information security in the organization website. Organization A usually uses e-mails, text message and training sessions to make the members aware of any security issues. While participants from organizations B and C reported that e-mails and posters are the main security awareness activities utilized in their organizations. In organization D, the main security awareness methods are e-mails, training courses and displaying information security on the organization website. Organizations E and F adopted the same security awareness activity of e-mails. Finally, organization G uses e-mails, text messages, training courses, and displays information security on the organization website as the main awareness methods.
- **Alerting Regularly about Risks and Dangers in the Organization.** Three interviewees reported that their organization's employees are not alert to any security risks, such as B and G. Ten interviewees reported that all employees in the organization are alert to security risks and dangers inherited in the work environment.
- **Information Security Level in the Organization.** To attain quantifies data, interviewees rated the level of information security in their organizations. Six participants believed that their organizations have a moderately acceptable level of information security; four participants believed a slightly acceptable level of information security; two participants claimed a very acceptable level; and one believed that it is completely acceptable.

4.2 Employee Security Behavior Patterns

This section attempts to uncover information regarding the employee's security culture behavior, knowledge, and practices in organizations.

- **Employee's General Security Behaviors.** Participants rated the employee's security behavior to obtain a broad picture. Eight participants believed that the security behavior in their organizations is "OK"; whereas four participants thought it to be "poor or very poor"; one believed it to be "good".
- **Identification of the Most Effective Security Practices on Employee's Security Behavior.** Interviewees were given several security practices to rank the level of effectiveness, including: top management, IT department initiatives, technical security countermeasure and personal values and beliefs regarding information security. Eight respondents stated top management involvement as a high priority. Following the IT department's initiatives, there was a priority for technical security countermeasures, and less priority for personal values and beliefs.
- **Perceptions of an Effective Security Culture.** Participants made a range of statements that aimed to form an effective security culture. All thirteen participants stated that conducting security training programs would be effective upon acceptable levels of security culture in organizations. Nine participants affirmed this statement: "Educating employees about the information security to increase their knowledge and make the right decision is important to have an adequate level of security culture." [B1]. The comparative analysis demonstrated that participants from the USA and Saudi Arabia organizations agreed and indicated that developing security policies and support from all levels of leadership are essential to develop an effective security culture. Participant C7 highlighted this: "To create or expect an efficient security culture, there should be an active, continuous engagement and endorsement of the information security by all levels of leadership and managers in the company". The participants from the UK and Saudi Arabia organizations stated that increasing security awareness is necessary for security protection that supports security culture. Four participants from Saudi Arabia organizations suggested that enhancing security ownership in employees would help to promote an acceptable level of security culture.
- **The Main Contributory Factors Establishing Security Culture**. There has been an agreement among participants from the UK and Saudi Arabia organizations that a security training program is one of the most important factors in security culture. Nine participants revealed that developing security training sessions for employees in the organization is one of the highest contributory factors in establishing security culture. Participant A2 assured this: "the security training program is one of the key factors for educating employees to adopt security and influence the employee behavior which will lead to establishing the security culture". Seven participants indicated that developing clear security policies as a second top contributing factor; they affirmed the effectiveness impact of security policy in security culture. Participant E3 commented that: "implementing security policies in the company will be efficient because it helps employees to clarify and get a detailed understanding about the security requirements, and the way to comply with the security rules".

Five participants mentioned that increasing security awareness is a third factor that supports security culture; while three participants signified that a periodical risk analysis is another factor that has to be considered. Two participants revealed that security culture could be effective if there is support from top management, as well as employee's compliance with security policy. One participant stated that understanding the ethical obligations of the organization and employees' job satisfaction are also vital in improving security culture.

A comparative analysis illustrated that four participants from the US and Saudi Arabia organizations believed that top management support and employees' security compliance are contributory factors in developing security culture; participant E3 stated that: "the security culture can be established effectively if all members of the company comply with security policy and regulations". Five participants from the Saudi Arabia organizations considered additional factors, such as security risk analysis, ethical conduct and job satisfaction, to contribute to the security culture. As participant A3 stated that: "Understanding the risk involved with information security and more importantly conducting a periodical risk assessment is a vital key for establishing the security culture environment". Participant B4 affirmed the effectiveness of ethical conduct policies in advancing an organization's security culture: "understanding the ethical codes and obligations is essential to improving security culture". Participant E10 suggested that job satisfaction can motivate employees to comply with organizations' security requirements: "one of the issues that should be considered in a company is the employee's job satisfaction; when the employee has a positive feeling, he/she will be more likely to comply with company security policies".

- **The Main Barriers to Achieving Improved Security Compliance.** The findings indicated that nine participants considered that the lack of awareness and training programs to be the first obstacle; the lack of clear direction in security policies was second; followed by a lack of leadership support and ownership. Two participants signified certain obstacles related to faulty human behavior by misunderstanding the ethical obligations and having no consequences to employees who fail to comply with security procedures. There has been some agreement among seven participants' perceptions of organizations in the UK and Saudi Arabia regarding the main obstacles. Seven interviewees believed that the security training sessions tend to achieve security compliance with the security policy of organizations; participant F1 stated that: "we have simple security policies, but most of the employees lack relevant training and hardly follow any security policies; the training program is vital in educating all employees to comply with security rules and guidelines". The comparative analysis illustrated that four participants from the USA and Saudi Arabia organizations expressed that the absences of clear security policies contribute significantly to the lack of compliance with information security. Three participants revealed that some of the organizations' top management lack the appropriate commitment to promote security policies; participant C2 stated that: "in my company, I have not observed any serious commitment from the top management to enforce enhancing security". One participant from Saudi Arabia considered ethi-

cal conduct as an additional factor, while one in the USA focused on the lack of security compliance.

4.3 Perceptions for Improving the Security Culture

The Participants had different recommendations that aimed to develop a security culture. There was some agreement among participants' perceptions of organizations in the UK, the USA and Saudi Arabia. Four participants agreed that the top management support in enhancing information security in organizations would improve security culture. Eight participants from the UK and Saudi Arabia organizations considered implementing security awareness as useful in developing security culture. Nine participants in the USA and Saudi Arabia organizations signified that conducting security training sessions and developing clear security policies are the most positive factors that help in improving security culture. Four participants from Saudi Arabia suggested additional factors, such as enhancing the sense of security ownership, developing ethical conduct, conducting a periodical risk assessment, and enhancing the employees' job satisfaction. Meanwhile, one USA participant suggested the importance of improving security compliance. Moreover, three participants from the UK and Saudi Arabia organizations stated the need for a tool or a model that could be used as guidance in implementing the required security culture factors that are targeted at the appropriate tiers of employee behavior, and to inculcate acceptable levels of security culture.

5 Discussion

Internal threats continue to exist within organizations. It was evident that factors identified in previous research continue to be significant. Phase one in this study provides rich data from thirteen experienced and knowledgeable respondents in seven organizations in the UK, the USA, and Saudi Arabia. The interview also revealed an apparent gap in the efficiency of providing training programs and security policies. Participants stated the requirement for periodic security training, as information security is mentioned once on induction day when the employee starts working for an organization. Participant A1 disclosed that: "education and training are not memorized for long; once the new employee finishes the first week of training, information security is forgotten." There was also concern regarding the limitations of training programs to key managers and IT members. They concluded the need for a structured training program aimed at all the organization's members.

Moreover, respondents suggested that they were unclear how their policies were implemented and updated, which is important due to the changing nature of threats. There was concern about the possible clarity of organizational policies to follow. Participant C1 suggested that: "the threats are always changing, the environment is always changing, and information security is always changing. Hence, it is vital for a company to have clear policies that are clearly described; improve the security poli-

cies by reviewing it continuously and maintain it up to date". Thus, phase two takes these points into consideration when constructing the questionnaire.

However, a comparative analysis suggested some differences in the data sets, including data collected in the UK, the USA and Saudi Arabia. In particular, there are both similarities and differences among the participants' perceptions based on their country regarding the main factors in terms of cultivating an effective security culture. There has been an agreement among the participants' perceptions regarding the important factors in establishing organizations' security culture. Based on the findings, it appears that security education and training programs, as well as security awareness and the security policy are the most significant factors that contribute toward security culture. Security education and training are considered as the most important factors to influence security culture's effectiveness. It is essential to implement and conduct periodic security training sessions in organizations to develop security culture and to improve employee's awareness, which tends to encourage security compliant behavior [7]. Additionally, it was indicated that in three organizations the security lessons had been learned following specific incidents.

The interviews indicated the importance of security awareness in promoting security culture. Both security education programs and security policy encourage compliant behavior by increasing employees' security awareness. The findings show that some organizations viewed security awareness as important in establishing a common understanding of security culture. It helps structure how employees think about information security and provides the common language and base of useful knowledge when discussing various security-related topics. Participant G1 indicated that: "it is important to create a mindset within employees; you have to develop active awareness programs, and that will give the employee a high level of awareness". Three participants stressed that sometimes security awareness might be inadequate if members are not aware of possible consequences of security breaches and cannot see the value of their security role in the organization's holistic security work. Demonstrating a high level of security awareness would lead to security-cautious behavior, which tends to encourage security compliance, while also improving security culture [6]. The findings also demonstrate that clear and sufficient security policy could promote security-cautious behavior through security awareness and establish an acceptable level of security culture. Four participants stated that security policy is an important measure, although it might be insufficient if members are not well-informed about the existing security policies.

The interviews revealed other factors that should be considered in establishing organizations' security culture: top management support and security ownership. Respondents from the UK, the USA and Saudi Arabia agreed that gaining top management commitment and support is significant in increasing organizations' security effectiveness. The support and commitment from top management help to form organizational security and predict security culture quality [9]. There were concerns regarding the failure of top management in enhancing security culture through developing appropriate training sessions, as an organization can subsequently face major issues in daily operations. Participant E2 indicated that: "employees in the company understand the importance of security; although we do not yet have a robust security

policy because of that the top management is still in the process of establishing the company security activities and structures". Also, respondents from the UK and Saudi Arabia revealed that when employees understand security responsibilities and personal ownership, they comprehend security risks and behave more securely, which tends to increase security awareness and compliance; thus, better security culture [3]. Participant B1 asserted: "we do not expect to establish the security culture if our employees do not understand the importance of protecting information and it is their responsibility."

The participants from Saudi Arabia and the USA suggested three factors: security risk analysis and assessment; ethical conduct; and security compliance. The findings demonstrated that security risk assessment and analysis tend to assist organizations and employees to become capable of understanding potential damage to security, which helps to increase awareness and knowledge of security culture [3, 10]. The interview also suggested that ethical conduct is a vital factor that influences security culture, as it supports employees to integrate ethical behavior, ensuring the security of information and what is accepted by the organization [3, 10]. The findings illustrated the importance of improving security compliance in security culture creation to increase an organization's security and ensure that employee behavior complies with security policy. Participant C1 stated that: "employees are often unaware of the consequences of security breaches caused by their actions; the company should have a method that ensures employees' behavior continues to be monitored to the compliance program's effectiveness". Furthermore, another vital factor that was suggested by one respondent from Saudi Arabia is employee job satisfaction tends to promote security-cautious behavior, which develops security culture [5].

Interview analysis supports other studies and highlights the significance of factors that have an impact upon employees' security behavior and is important to be considered as part of security culture conceptualization. These factors have a positive influence on each other, and thus, have a positive influence on the security culture. The possible relationships between factors will be tested statistically in order to determine whether the proposed framework is valid. However, personality traits have received little attention from researchers, despite indications that personality traits directly affect individual behavior [11]. This is important for future research and will be an essential factor in the construction of the survey items. This paper provides some insights, although cannot be generalizable, as additional investigations are required. The study will be expanded to develop a statistical framework that would identify the correlations between factors. Knowledge management would be integrated to develop a framework that would help organizations to create the culture efficiently and predict how the security culture could be improved. Consequently, the study adopts a quantitative survey on a range of different sizes of organizations with sample size range from 250 to 300 employees.

6 Conclusion and Future Work

This study has aimed to build further comprehension of various factors that positively assist with organizations' security culture from employees' perspectives. Existing literature states factors regarding security culture adoption, while all top factors should be considered to create an environment that promotes better security culture. The study conducted an exploratory interview to present important factors that potentially affect organizational security culture and to identify existing gaps in what employees are aware of. The interviews comprised of thirteen experienced and knowledgeable security specialists from different organizations located in the USA, the UK and Saudi Arabia. These interviews were analyzed to highlight the significant factors in security culture stemming from participants' experiences.

The findings from this study contribute to the existing knowledge by providing factors that are significant in affecting human behavior and vital in security culture. The information gained from interviews provided further knowledge of how different factors were viewed regarding reality settings. The findings also revealed an apparent gap in the organizational policies' implementation and ineffective training programs that lead to a lack of awareness and compliance. The result of this study cannot be generalizable but can be viewed to be indicative. In addition, the findings from this study demonstrate certain limitations, such as the how it cannot test the security culture framework's non-logical validity; the initial influence of factors on security culture; or factors that define security culture. However, the findings from the qualitative phase produced variables that are utilized in the quantitative phase to test the development framework's validity. In order to design the survey, the specific operational elements involved were measurable to the literature review, which were incorporated with the findings from the qualitative phase to identify constructs and related survey items that influence security culture.

References

1. Alhogail, A., Mirza, A., Bakry, S.: A Comprehensive Human Factor Framework for Information Security in Organisations. Journal of Theoretical and Applied Information Technology. 78(2), 201-211 (2015).
2. Alhogail, A.: A Framework for the Analysis and Implementation of an Effective Information Security Culture Based on Key Human Factor Elements and Change Management Principles. King Saud University (2016).
3. Alnatheer, M., Chan, T., Nelson, K.: Understanding and Measuring Information Security Culture. In: Proceedings of the 16 th Pacific Asia Conference on Information Systems. PACIS 2012 Proceedings (2012).
4. Connolly, L.Y., Lang, M., Gathegi, J., Tygar, D.J.: Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. Information and Computer Security, 25(2), 118–136 (2017).
5. D'Arcy, J., Greene, G.: The Multifaceted Nature of Security Culture and Its Influence on End User Behaviour. In: Proceedings of IFIP TC 8 International Workshop on Information Systems Security Research, 145-157 (2009).

6. Da Veiga, A.: The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. In: Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance, 22-33 (2015).
7. Da Veiga, A., Eloff, J.: A framework and assessment instrument for information security culture. Computers and Security. 29(2), 196-207 (2010).
8. Glaspie, H.W., Karwowski, W.: Human Factors in Information Security Culture: A Literature Review. In: International Conference on Applied Human Factors and Ergonomics, 269-280. Springer, Cham (2017). DOI 10.1007/978-3-319-60585-2 25
9. Martins, N., Da Veiga, A.: An Information Security Culture Model Validated with Structural Equation Modelling. In: Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance, 11–21 (2015).
10. Martins, A., Eloff, J.: Assessing Information Security Culture. Information for Security for South-Africa 2nd Annual Conference, 1-14 (2002).
11. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M.: Individual Differences and Information Security Awareness. Computers in Human Behavior. 69, 151-156 (2017).
12. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers and Security, 66,40-51 (2017).
13. Pwc.co.uk. (2015). [online] Available at: https://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf [Accessed 25 Feb. 2017].
14. Roer, K., Petric, G.: Indepth insight into the Human factor: The Security Culture Report 2017. 1st ed. CLTRe North America, Inc (2017).
15. Schlienger, T., Teufel, S.: Information Security Culture-from analysis to change. South African Computer Journal. 2003(31), 46-52 (2003).
16. Tolah, A., Furnell, S., Papadaki, M.: A Comprehensive Framework for Cultivating and Assessing Information Security Culture. In: Proceedings of the Eleventh International Symposium on Human Aspects of Information Security and Assurance, 52-64 (2017).
17. W, E. (2017). Growing positive security cultures – National Cyber Security Centre. [online] Ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures [Accessed 22 Feb. 2019].