International Journal of Information Technology and Language Studies (IJITLS)

Conceptualizing a Framework to Enhance Information Security Culture and Compliance Behavior in Organizations through Protection Motivation Theory

Ebrahim Mohammed Alrawhani and Awanis Binti Romli
Faculty of Computer, University Malaysia Pahang Al-Sultan Abdullah, Pahang, Malaysia
abrahem7@gmail.com; awanis@ump.edu.my

Article Information

Article type: Article

Article history:

Received: July 31, 2024
Revised: August 24, 2024
Accepted: September 05, 2024

Keywords:

Information Security Policy
Information Security Culture
Conceptual Framework
Compliance Behavior
Organization Culture
Protection Motivation Theory

Abstract

Ensuring information security compliance is essential for securing organizational data. However, comprehending the factors that impact employees' compliance behavior remains challenging. Scholars have proposed that an established Information Security Culture (ISC) in organization may impact employee compliance with policies of information security. Existing models often address only partial aspects of Information Security Culture (ISC) or lack integration of comprehensive behavioral theories. The aim of this study is to propose an enhanced conceptual framework that identifies all elements of ISC and their influence on employees' compliance with the policies of information security. Aligning with well-established concepts of organizational culture and ISC, the framework was developed by incorporating important elements from the literature. The employees' information security behavior was explained by the Protection Motivation Theory (PMT) to offer comprehensive insights about compliance behavior. It is believed that this conceptual framework will provide more precise results on the correlations between ISC and compliance behavior of employees towards information security regulations.

1. Introduction

There has been an evolution in the past years towards incorporating human and technical factors into information security programs, such as protecting, detecting, mitigating, and recovering from information security threats (Hassandoust et al., 2022). Organizations may face internal risks in preventing information security threats, particularly due to employees' inadvertent or deliberate leaking of sensitive information (Alghamdi, 2021). Based on the research, individuals are the most vulnerable aspect of cyber security and are responsible for a significant percentage of security breaches in the organization (Torten et al., 2018; Yuryna Connolly et al., 2017). Technology methods alone is insufficient to address the human elements of information security (Nel & Drevin, 2019). Scholars in the present literature have given significant emphasis to the human aspect of information security. As a result, researchers have seen an increasing tendency in discusses on the factors that drive human intention to comply with information security policies (Amankwa et al., 2022). In that, research indicate that the establishment of an information security culture (ISC) is crucial for transforming workers' noncompliant behavior into compliance with information security regulations Ali et al. (2021). Thus, experts have advocated for the development of a robust ISC model in organizational context to stimulate employees' willingness to adhere to information security policies (Solomon & Brown, 2021).

According to recent research, there is an increasing recognition that ISC may significantly influence workers' self-protective behavior and their willingness to comply with information security policies policy (Amankwa et al., 2022). In particular, Nasir et al. (Nasir et al., 2017) has proposed a comprehensive ISC model that comprises of seven dimensions. The model incorporates the Theory of Planned Behavior to examine workers' adherence to security regulations. Furthermore, it was recommended that other behavioral theories should be explored in order to have a comprehensive understanding of the ISC concept within the context of information security (Nasir, Abdullah Arshah, et al., 2019).

Despite advancements in integrating human and technical factors into information security programs, there remains a significant gap in understanding the behavioral elements influencing employee compliance with security regulations. Existing models often fail to address the full complexity of human behavior, which is crucial given that employees are a major source of security breaches, addressing this issue is the primary motivation behind this study. This research study aims to present a conceptual framework that comprehensively explains the behavior of employees towards information security regulations within an organizational setting.

2. REVIEW OF LITERATURE AND THEORETICAL FOUNDATIONS

This section will provide an in-depth review of the ISC construct and all of its dimensions. Furthermore, a thorough examination of the suggested conceptual framework will be provided. Finally, a discussion of the contribution of this research is presented.

2.1 The ISC dimensions in Adherence to ISP

The establishment of an information security culture was essential because of the human actions that pose substantial many risks to the security of a company's information assets. In previous research studies, various dimensions have been utilized to illustrate the concept of ISC and its correlation to ISP compliance (Nasir, Arshah, et al., 2019). Also, in several research related to ISC, numerous conceptual models of ISC have been proposed (AlHogail & Mirza, 2014). A variety of concepts and theories, including organizational behavior (Martins & Eloff, 2002) and organizational culture (Elehinle, 2024), were used in developing these models. In addition, (Nasir, Arshah, et al., 2019) reviewed the concepts and dimensions of ISC and found that most of the studies conceptualized ISC using Schein's organizational culture concepts compared to other concepts. They also provides a comprehensive overview of the main factors and dimensions related to the ISC, including but not limited to Information Security Risk Analysis and Assessment, Top Management Commitment, Trust, Belief, Information Security Training, Security Policy, and others (Nasir, Arshah, et al., 2019).

2.2 Adapted ISC Dimensions

This research defines ISC as a set of different factors that describe this concept and contribute to the formation of its basic assumptions. (Nasir, Arshah, et al., 2019) synthesized many terms used in the literature to describe ISC and put up a complete model for the ISC concept. The model consisted of the following components: Information Security Knowledge Sharing (ISKS), Proceduaral Countermeasures (PCM), Top Management Commitment (TMC), Security Monitoring (SM), Risk Management (RM), Information Security Knowledge (ISK), and Security Education, Training, and Awareness (SETA). Their findings indicate that all ISC dimensions, were found to be reliable and made a substantial contribution to the ISC. Moreover, ISC has a significant impact on the inclination to adhere to IS policy. Hence, this study follows (Nasir, Abdullah Arshah, et al., 2019) conceptualization and regard ISC as a set of seven measurable dimensions that constitute ISC, i.e., ISKS, PCM, TMC, SM, RM, ISK, and SETA. The following sections describe each dimension and expound upon the value of each within the organizational culture.

2.2.1 Procedural Countermeasures (PCM)

PCM stands for individuals' comprehension of the organization's information system policies (Nasir, Abdullah Arshah, et al., 2019). Organizations must implement technical controls and countermeasures to mitigate security risks. These measures should include the development of security culture policies that raise knowledge about a broad range of potential security threats (Hassandoust et al., 2022). In addition, (Nasir, Abdullah Arshah, et al., 2019) explain that PCM is apparent via the presence of official policies that define individual authority and access levels for computer systems, regulations that control the use of computer resources, and rules that determine proper conduct using email. Implementing effective countermeasures against risks ensures that individuals have a clear understanding of organizational rules and are proactive in responding to and protecting themselves and the organization against security threats (Torten et al., 2018).

2.2.2 Risk Management (RM)

RM is the process of examining and controlling any risks to information assets by customizing security measures according to the value of the assets and the magnitude of prospective threats (Nel & Drevin, 2019). The same study argued

that it is crucial for organizations to identify and evaluate elements that might create security risks (Nel & Drevin, 2019). Additionally, the study emphasized the need to identify potential threats to each organizational asset and prioritize risks in order to execute security solutions efficiently. Nasir et al. (Nasir, Abdullah Arshah, et al., 2019) define risk management as the effective implementation of risk assessment processes to identify potential threats that can impact information systems. Risk management also involves the ability to understand the security threats, vulnerabilities, and risks associated with a company's information assets, as well as the establishment of a strong security culture. Furthermore, risk management may have motivating impact on employees, encouraging them to adopt precautionary measures and demonstrate compliant behavior (Alsaad & Al-Okaily, 2022). Security risk management assists the company and its workforce in identifying potential security threats and improves the firm's response efficacy, hence enhancing security compliance (Tolah et al., 2021).

2.2.3 Security Education, Training and Awareness (SETA)

SETA is an acronym that stands for workers' perceptions of security training activities inside an organization. These activities include security education, training, and programs aimed at increasing awareness (Nasir, Abdullah Arshah, et al., 2019). The objective of SETA is to provide workers with comprehensive security knowledge and abilities, improve their understanding of the significance of security protection, and enhance their awareness of security concerns (Cram et al., 2019, p. 540). Nasir et al. (Nasir, Abdullah Arshah, et al., 2019) stated that SETA involves instructing individuals on their responsibilities regarding computer security and providing training to enhance their comprehension of computer and information system risks. Hassandoust et al. (Hassandoust et al., 2022) also emphasize the significance of educating workers about the potential consequences of unauthorized modification of computerized material and the legal implications of accessing computer systems without permission. Training and education in information systems may enhance staff's knowledge about security concerns and address any existence of severity fear. It can help motivate staff to comply with information system processes, as highlighted by (Balapour et al., 2020). Therefore, it is important for organizations to provide their workers comprehensive training and awareness courses to ensure their readiness in complying with security of information regulations (Chul et al., 2018). This supports the prior evidence of the significance of the SETA factor in improving the ISC in organizations.

2.2.4 Top Management Commitment (TMC)

Top management commitment (TMC) stands for workers' interpretation of top management's clear dedication to information securities, demonstrated by their behaviors (Solomon & Brown, 2021). TMC is seen as a vital focus for organizations. It requires the active participation of all levels of management in important security activities, a strong dedication to the security program, and the allocation of enough training resources to ensure compliance with information security standards (Tolah et al., 2021). In order to maximize the advantages of information security education courses and promote compliance behavior, it is crucial for management to effectively communicate the importance of information security compliance to their personnel via their actions (Flores & Ekstedt, 2016). According to (Nord et al., 2020), when top management demonstrates a strong commitment to security compliance, it may effectively increase the awareness of security concerns among all staff members, help them understand the basic principles of security, and enable them to use technologies properly.

2.2.5 Security Monitoring (MON)

Security monitoring is relevant to the perception of workers that their computer actions are being actively and retrospectively watched and examined (Solomon & Brown, 2021). Monitoring is a useful method for evaluating staff response efficacy and affecting their compliance intentions positively (Masrek et al., 2018). In addition, (Nasir, Abdullah Arshah, et al., 2019) defines security monitoring as a means of identifying the presence of unauthorized software on the company's computers and monitoring the computing activity of employees. Key elements of security monitoring are regularly analyzing logs of staff's computing activities and monitoring any modifications made by staff to computerized data. According to Amankwa et al. (2022), including monitoring into information security policies increases its effectiveness by notifying staff members that all computerized activities are being watched to ensure compliance with security measures. Furthermore, the presence of security monitoring discourages staff from participating in non-compliant activity simply because of fear of facing penalties (Moore et al., 2018). Thus, the dimension of security monitoring serves an essential element in influencing the culture of information security in organizations.

2.2.6 Information Security Knowledge (ISK)

ISK represents workers' belief of the organization's knowledge of information security (Nasir, Abdullah Arshah, et al., 2019). Nasir et al. (Nasir, Abdullah Arshah, et al., 2019) suggest that ISK encompasses the presence of a security specialist who enforces information security controls, a comprehensive procedures manual to safeguard information assets, a high level of awareness in implementing information security programs, and the ability to improve staff security knowledge and skills. The acquisition of sufficient ISK is crucial for the development of a strong ISC. Lacking of ISK, a firm

may be unable to provide complete information security solutions (Amankwa et al., 2022). Based on the research conducted by Sas et al. (Sas et al., 2021), staff with a higher level of security awareness have a more positive attitude towards security-related matters and demonstrate more secure behavior. Staff with security expertise demonstrate good compliance behavior, including reporting information security offences and suspicious conduct, identifying emergency circumstances related to information security, and acquiring preventive security recommendations (McCormac et al., 2017).

2.2.7 Security Knowledge Sharing (ISKS)

Information security knowledge sharing (ISKS) represents workers' subjective understanding and recognition of the need of sharing security information inside the organization (Nasir, Abdullah Arshah, et al., 2019). Sharing knowledge about information security is crucial for fostering ISC to guarantee that the knowledge can be distributed, shared, and disseminated to make it accessible for the individuals who need it (Hassan et al., 2013). ISKS encompasses the exchange of experiences, thoughts, and information with others to safeguard information resources inside organizations. This includes activities such as knowledge sharing meetings, mailing lists, and specialized online conferences (Moody et al., 2018). The ISKS is an efficient way to increase awareness and mitigate security risks, while also reducing the financial burden of information security in companies (Pérez-González et al., 2019).

3. CONCEPTUAL FRAMEWORK

Building upon the discussed sections previously, the proposed conceptual framework is illustrated in Figure 1. Generally, it proposed how the development of ISC, formed by the seven dimensions (ISKS, PCM, TMC, SM, RM, ISK, and SETA), would affect the employees' compliance behavior toward information security policies in companies. The seven dimensions are the unique aspects that will thoroughly construct the culture of information security in the organization. Nasri et al. (Nasir et al., 2017) established the seven dimensions based on the broadly acknowledged aspect of Organizational Culture as described by (Schein, 2009, 2010), and connected them with the ISC layered model as proposed by (Van Niekerk & Von Solms, 2006). In order to guarantee that the aforementioned dimensions accurately represent the ISC concept, they were developed after careful consideration of all relevant literature on ISC factors. An employee's behaviors that are following the information security policies of an organization will be impacted by the ISC that is comprised of these seven dimensions.

Building upon the discussed sections previously, the proposed conceptual framework is illustrated in Figure 1. It outlines how the development of Information Security Culture (ISC), comprised of the seven dimensions (ISKS, PCM, TMC, SM, RM, ISK, and SETA), affects employees' compliance behavior toward information security policies in organizations. These seven dimensions represent critical aspects of constructing a robust information security culture. According to Nasri et al. (2017), these dimensions are grounded in the well-established framework of Organizational Culture as described by Schein (2009, 2010) and linked with the ISC layered model proposed by Van Niekerk and Von Solms (2006). Recent studies further reinforce this framework by evaluating how these dimensions impact security behaviors and compliance. For instance, Singh and Gupta (2023) examined the seven dimensions of information security culture across various industries, highlighting their influence on organizational practices. Chen and Lee (2023) developed a framework based on these dimensions, exploring their effects on employee behaviors and policy compliance. Patel and Kumar (2023) investigated the impact of these dimensions on compliance, offering insights into their practical application. These studies collectively validate that an ISC comprised of these seven dimensions significantly impacts employees' adherence to information security policies (Singh & Gupta, 2023; Chen & Lee, 2023; Patel & Kumar, 2023).

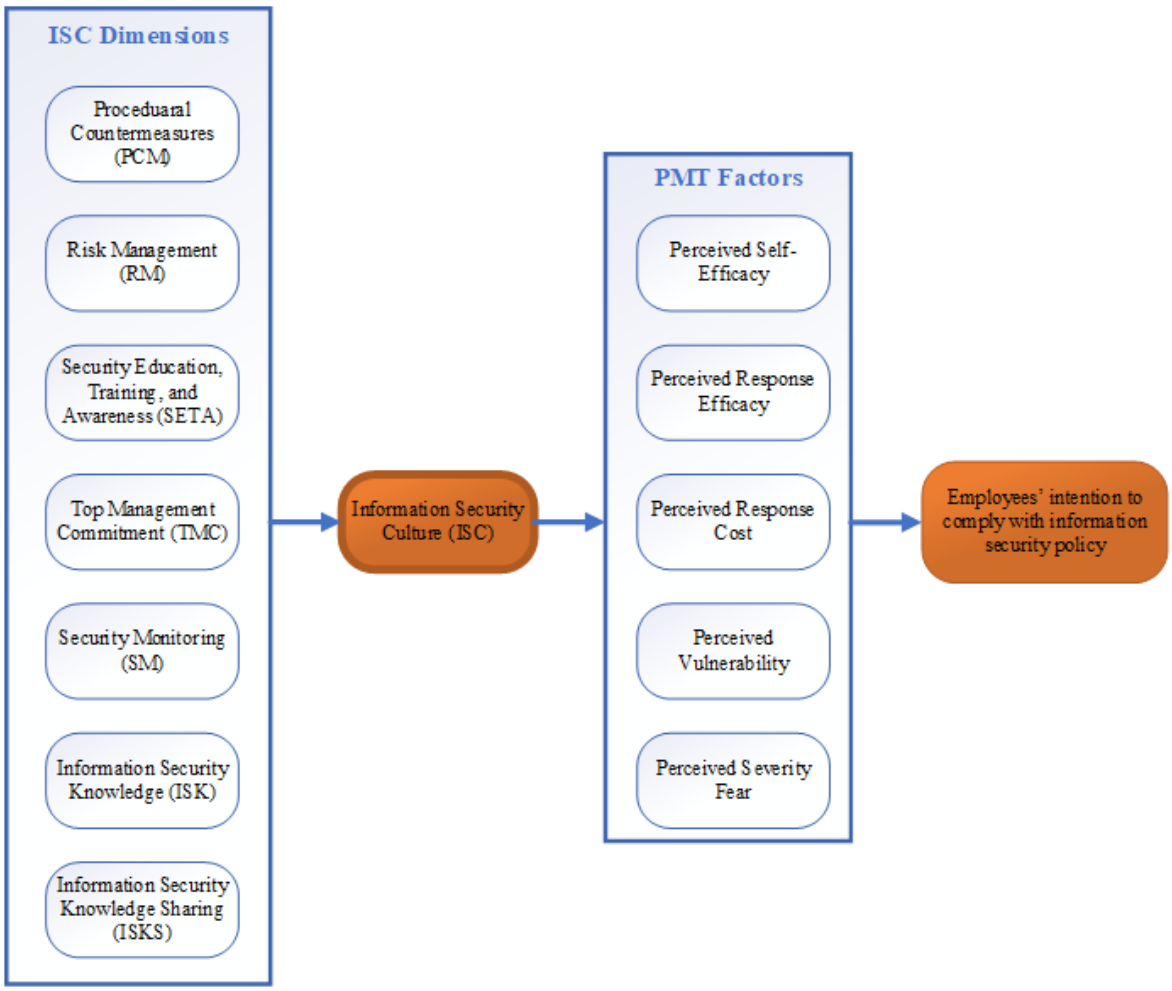

Figure 1. Teacher distribution related to their ICT profile.

To get an in-depth understanding of employee behavior and reveal further insights, especially on ISP compliance behavior, this framework incorporates the Protection Motivation Theory (PMT) developed by (Rogers, 1975), a well-recognized behavior theory. According to the PMT, there are two mechanisms or procedures that individuals use to safeguard themselves (Ogbanufe et al., 2023). The PMT hypothesis emphasizes the interconnected processes of threat assessment and coping assessment, which are believed to influence an individual's protective behavior (Alsaad & Al-Okaily, 2022). Threat assessment refers to the evaluation of the intensity and susceptibility to harmful events, which consists of two factors Perceived Vulnerability and Perceived Severity Fear. Coping assessment (Perceived Self-Efficacy, Perceived Response efficacy, and Perceived Response Cost) is a process that evaluates an individual's effectiveness, efficiency of response, and the associated costs of prospective adaptive behavior (Chang et al., 2022). In other words, a threat assessment focuses on the nature of the danger, whereas a coping evaluation pertains to the ability to effectively respond to that threat (Van Bavel et al., 2019). An individual's "protective motivation," the desire to protect oneself from the perceived risks in the threat assessment, is a result of the combined processes of the threat evaluation and the coping evaluation, as described by PMT (Boss et al., 2015). Based on PMT theory, the level of motivation to perform preventive action is influenced by the degree of protection motivation. Thus, protective motivation may be seen as a mediating variable between fear perceptions and behavioral intention (Rogers, 1975). Prior research has consistently shown that the intention to adhere to information security policies is impacted by factors related to protection motivation (e.g., Fan et al., 2022; Neisi et al., 2020; Zhu et al., 2022).

PMT offers a more comprehensive explanation compared to other theories such as the Theory of Planned Behavior (TPB), Theory of Reasoned Action (TRA), and Diffusion of Innovation (DOI) due to the fact that PMT distinguishes itself by integrating two key processes: threat assessment and coping assessment. Threat assessment involves evaluating perceived vulnerability and severity, while coping assessment evaluates perceived self-efficacy, response efficacy, and response cost.

This dual-process model allows for a detailed understanding of how individuals assess risks and their ability to manage those risks, influencing their protective behaviors (Alsaad & Al-Okaily, 2022; Chang et al., 2022).
In contrast, TPB and TRA primarily focus on behavioral intentions based on attitudes, subjective norms, and perceived behavioral control (Ajzen, 1991; Fishbein & Ajzen, 1975), which may not fully capture the complexity of threat perception and response strategies. DOI emphasizes the spread of innovations and adoption rates, which is less focused on the individual's motivational processes related to specific threats (Rogers, 2003). Therefore, PMT's emphasis on motivational factors driven by threat and coping evaluations provides a more precise and actionable framework for understanding ISP compliance behaviors, highlighting why it is a more suitable theoretical foundation for this study, the main factors of PMT have a more substantial impact on the intentional behavior of individuals, as compared to other behavioral theories like Theory, of Reasoned, Action, (TRA) and Diffusion of Innovation theory (DOI).

4. ANTICIPATED CONTRIBUTIONS

In this study, insights will be provided on how the compliance behavior of employees in an organization might be impacted by the development and implementation of ISC inside the organization. Additionally, this study will add to the current knowledge on the topic of ISC by shedding light on the effects of the seven dimensions (ISKS, PCM, TMC, SM, RM, ISK, and SETA) that form the ISC in organization. Furthermore, more in-depth knowledge of employees' compliance behavior to information security policies will be gained by including the PMT theory as the fundamental behavior theory in the proposed framework. The literature has shown that the PMT theory and its main factors of Perceived Vulnerability, Perceived Severity Fear Perceived Self-Efficacy, Perceived Response efficacy, and Perceived Response Cost are significant factors in understanding and predicting compliance behavior with information security regulations. Apart from that, information security managements might the proposed framework to structure and execute an organization's information security controls. This will guide the organization's employees to work in a way that complies with the organization's information security policies.

5. CONCLUSION

This research provided a conceptual framework based on the ISC that comprehensively explains the behavior of workers towards information security regulations in organizational context. The framework used the ISC concept, which was established by taking into account all the crucial factors of ISC found in literature. Additionally, this model used PMT, one of the most popular and important protection behavior theories, to depict how an employee acts in regards to information security. Future empirical investigations studying the connections between ISC and information security culture compliance behavior may be guided by this conceptual framework. New indications and a more thorough knowledge of how ISC effects workers' compliance behavior with information security culture are provided by this research, which defines ISC to be a multidimensional construct comprising seven dimensions. This investigation is essential in the domain of information security, as ISC is often defined differently across among research studies, varying in both its number of dimensions and integrations with other theories.

References

Alghamdi, M. I. (2021). Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. *Materials Today: Proceedings*. https://doi.org/https://doi.org/10.1016/j.matpr.2021.04.093

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. 2014 World Congress on Computer Applications and Information Systems (WCCAIS),

Ali, R., Panneer Selvam, D. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, *11*, 3383. https://doi.org/10.3390/app11083383

Alsaad, A., & Al-Okaily, M. (2022). Acceptance of protection technology in a time of fear: the case of Covid-19 exposure detection apps. *Information Technology & People*, *35*(3), 1116-1135. https://doi.org/10.1108/ITP-10-2020-0719

Amankwa, E., Loock, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors. *Information & Computer Security*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ICS-10-2021-0169

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems*, *39*(4), 1-72. https://doi.org/10.25300/MISQ/2015/39.4.5.

Chang, H. H., Wong, K. H., & Lee, H. C. (2022). Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators. *Electronic Commerce Research and Applications*, *54*, 101176. https://doi.org/https://doi.org/10.1016/j.elerap.2022.101176

Chen, Y., & Lee, H. (2023). "The Role of Organizational Culture in Shaping Information Security Behaviors: A Framework Based on Seven Dimensions." International Journal of Information Technology & Learning Sciences, 22(2), 115-130.

Chul, W. Y., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–540. https://doi.org/10.25300/MISQ/2019/15117.

Elehinle, E. (2024). Impact of organizational culture on on information security: A case of SMEs in Nigeria. In.

Fan, A., Kline, S. F., Liu, Y., & Byrd, K. (2022). Consumers' lodging intentions during a pandemic: empirical insights for crisis management practices based on protection motivation theory and expectancy theory. *International Journal of Contemporary Hospitality Management*, *34*(4), 1290-1311. https://doi.org/https://doi-org.ezproxy.utm.my/10.1108/IJCHM-07-2021-0889

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26-44. https://doi.org/10.1016/j.cose.2016.01.004.

Hassan, N. H., Ismail, Z., & Maarop, N. (2013). A conceptual model for knowledge sharing towards information security culture in healthcare organization. 2013 International Conference on Research and Innovation in Information Systems (ICRIIS),

Hassandoust, F., Subasinghage, M., & Johnston, A. C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. *Information & Management*, *59*(1), 103574. https://doi.org/https://doi.org/10.1016/j.im.2021.103574

Martins, A., & Eloff, J. (2002). Assessing Information Security Culture. ISSA,

Masrek, M., Harun, Q., & Sahid, N. (2018). Assessing the information security culture in a government context: The case of a developing country. *International Journal of Civil Engineering and Technology (IJCIET)*, *9*(8), 96–112.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-322.

Moore, A. P., Samuel, P. J., Jennifer, C., Collins, M. L., Cassidy, T. M., & Nathan, V. (2018). The critical role of positive incentives for reducing insider threats. *Computer Emergency Response Team*, *7*, 1-66. https://doi.org/10.1184/R1/6585104.v1.

Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, *28*(3), 55-80.

Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework. Proceedings of the 2017 international conference on information system and data mining,

Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12-22.

Neisi, M., Bijani, M., Abbasi, E., Mahmoudi, H., & Azadi, H. (2020). Analyzing farmers' drought risk management behavior: Evidence from Iran. *Journal of Hydrology*, *590*, 125243. https://doi.org/https://doi.org/10.1016/j.jhydrol.2020.125243

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*, *27*(2), 146-164. https://doi.org/10.1108/ICS-12-2016-0095

Nord, J. H., Koohang, A., Floyd, K., & Paliszkiewiez, J. (2020). Impact of habits on information security policy compliance. *Issues in Information Systems*, *21*(3), 217-226. https://doi.org/10.48009/ 3_iis_2020_217-226

Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers & Security*, *124*, 102960. https://doi.org/https://doi.org/10.1016/j.cose.2022.102960

Patel, R., & Kumar, S. (2023). "Understanding the Impact of Cultural Dimensions on Information Security Compliance: A Seven-Dimensional Approach." International Journal of Information Technology & Learning Sciences, 22(3), 143-160.

Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. (2019). Organizational practices as antecedents of the information security management performance. *Information Technology & People*, *32*(5), 1262-1275. https://doi.org/10.1108/ITP-06-2018-0261

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *19*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803.

Sas, M., Reniers, G., Ponnet, K., & Hardyns, W. (2021). The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. *Safety Science*, *144*, 105447. https://doi.org/https://doi.org/10.1016/j.ssci.2021.105447

Schein, E. H. (2009). *The corporate culture survival guide* (Vol. 158). John Wiley & Sons.

Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2). John Wiley & Sons.

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), 1203-1228. https://doi.org/10.1108/JEIM-08-2019-0217

Singh, A., & Gupta, N. (2023). "Evaluating the Seven Dimensions of Information Security Culture: Insights from a Multi-Industry Study." International Journal of Information Technology & Learning Sciences, 22(1), 87-102.

Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security*, *108*, 102354. https://doi.org/https://doi.org/10.1016/j.cose.2021.102354

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. https://doi.org/https://doi.org/10.1016/j.cose.2018.08.007

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39.

Van Niekerk, J., & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. ISSA,

Yuryna Connolly, L., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour. *Information & Computer Security*, *25*(2), 118-136. https://doi.org/10.1108/ICS-03-2017-0013

Zhu, Y., Wen, X., Chu, M., & Sun, S. (2022). Consumers' intention to participate in food safety risk communication: A model integrating protection motivation theory and the theory of reasoned action. *Food Control*, *138*, 108993. https://doi.org/https://doi.org/10.1016/j.foodcont.2022.108993