Global Business and Management Research: An International Journal
Vol. 15, No. 2 (2023)

Cyber Security Protective Behaviour in Industrial Revolution 4.0 Era: A Conceptual Framework

Saif Hussein Abdallah Alghazo
Abu Dhabi Global Market,
Al Maria Island Abu Dhabi,
United Arab Emirates (UAE)

Norshima Humaidi*
Faculty of Business and Management,
Universiti Teknologi MARA (UiTM) Selangor,
Puncak Alam Campus
42300 Bandar Puncak Alam, Selangor Darul Ehsan, Malaysia
email: norshima958@uitm.edu.my
* *Corresponding Author*

Melissa Shahrom
Faculty of Business and Management,
Universiti Teknologi MARA (UiTM) Selangor,
Puncak Alam Campus
42300 Bandar Puncak Alam, Selangor Darul Ehsan, Malaysia

Nooriha Abdullah
Faculty of Business and Management,
Universiti Teknologi MARA (UiTM) Selangor,
Puncak Alam Campus
42300 Bandar Puncak Alam, Selangor Darul Ehsan, Malaysia

Abstract

Purpose: Cyber security arises due to the weaknesses of employees' behaviours, such as carelessness and failure to adopt good practices in information security. Therefore, this study aims to explore the dimensions that might influence employees' behaviour to adopt good cyber security practices and to develop a new holistic model of cyber security protective behaviour.

Design/methodology/approach: The study reviews the literature in related areas, with a special emphasis on existing theories such as the Protection Motivation Theory (PMT), using scoping review technique.

Findings: In the field of cyber security protective behaviour, the study discovered four major expected findings that need further investigation: cybersecurity protection motivation, procedural information security countermeasures awareness, employee cyber security attitudes, and manager cyber security competence are among the factors to consider.

Research Limitations and Implications: By analysing the impact of security managers' competency in handling cyber security concerns in organisations, the study's findings can help to close a research gap. Future research may also shed light on how employees' perceptions of the

value of cyber security are influenced by their knowledge of the topic. Additionally, the study's results might aid businesses in any sector in developing information security plans and cyber defences that will increase staff adherence to information security policies.
Originality/value: The proposed study model should be statistically verified in the future since the results will be used to inform legislation that will improve employees' behaviour in protecting company information assets, particularly when working in cyberspace and in the IR 4.0 environment.

Keywords: Cyber Security Protective Behaviour, Protection Motivation Theory, Industrial Revolution 4.0, Cyber security Competencies, Cyber security Attitude and Cyber security Awareness

Introduction

The trend of digitization, automation and the increased use of Information and Communications Technology (ICT) has been argued to reflect the main concept of Industrial Revolution (IR) 4.0 (Alaloul et al., 2019). The implementation of IR 4.0 engenders the interconnectedness of every digital device through technological advancements that aid digital devices to operate and share information through cloud computing systems (Alaloul et al., 2019). da Veiga et al. (202) argued that despite the rise in technological advancements, the benefits of IR 4.0 may be hampered by the dangers of cyber security threats. Consequently, without appropriate attention to constant online protection and monitoring of organisations of IoT, organisational data are often lost to cyber security threats (Safa et al., 2019). Recent worldwide security incidents have shown that there is an increase in the complexity and severity of cyber security threats (Yamin et al., 200). They also explained that cyber attackers are becoming more organized. Meanwhile, Grobler et al. (2011) reiterated that organisations with high technology use in IR 4.0 environment are much easily proned to fall victim of several cyberattack vectors. Consequently, existing literature emphasises that it is crucial for IR 4.0 employees to continuously be aware of the importance of cyber security and to consistently develop their cyber security skills in order to expand their knowledge and readiness against the most recent cyber security threats.

Since cyber breach has become a major issue in today's digitalized world, several security experts across the globe recommend the need for improving cyber security behaviour among the employees (Kemper, 2019; Cain et al., 2018) especially when this organisation embraces the IR 4.0 concept. According to Yamin et al. (2020), employees' cyber security protective behaviour should be periodically evaluated to ensure the organisation's cyber health is in optimum condition. This is essential since cases of cyber attack are increasing every year. Many of the cyber attack cases are due to human errors (Chang et al., 2022; Uchendu et al., 2021). Therefore, the study attempts to explore and extend the concepts underpinning prior psychological constructs by also examining the role of security manager competencies and cyber security awareness which are also important elements to sharpen employees' behaviour towards practising good cyber security, especially when all tasks have been done virtually.

According to current studies, several cyber security incidents are related to human error (Wong et al., 2022; Safa et al., 2019; Kemper, 2019). Although many organisations have implemented the latest security technologies, such as biometrics, firewalls, smartcards, and encryption, employees' behaviour towards information security are yet to be influenced by human error, which consequently engenders information security issues (Park et al., 2010). Studies contended that

technological advances cannot completely ensure effective information security if the information security behaviours of employees in organisations are unacceptable. Kemper (2019) lamented that several organisations have lost millions of dollars due to lack of adequate responsiveness to security incidents and careless behaviours of some employees. Equally, several organisations have fallen victim of cyber security breaches due to employee's negligence, and non-compliance with their organisation's information security policies (Ameen et al., 2021; Ani & He, 2018). The employee's negligence, and non-compliance behaviours may be seen in issues like poor password creation, password sharing, leaving internet-connected devices unprotected, login into company systems across unsecured networks, and carelessness when handling organisational data and information (Chang et al., 2022). Kemper (2019) advocated that the struggle most organisations experience with cyber security is often caused by employees who consciously or inadvertently pose as a severe cyber security threat to businesses. To curb this, prior studies accentuated that organisations need to emphasize on advancing employees' awareness of cyber threats and to ensure that employees' cyber security-related behaviour closely aligns with organisational information security policy (Wong et al., 2022).

There are many studies on cyber security, but to the state-of-the-art, there are not many studies conducted to evaluate security manager competencies in IR 4.0 business environments in urban populations, particularly in Malaysia. Cybersecurity threats exist in many business sectors due to a lack of security awareness among employees, poor security skills, poor security monitoring and enforcement, and inappropriate cyber security behaviour (Safa et al., 2019). Employees who have adequate knowledge of cyber security and who understand the consequences of their pro-security actions would be more careful in handling organisational data and information (Kimani et al., 2019). According to Cain et al. (2018), employees must develop their own self-awareness towards the cyber security issue. This can be more effective if the management in the organisation can implement proper information security procedures and guidelines, especially in the IR 4.0 era, when most of the information can be shared on any device at any time through the IoT (Safa et al., 2019). Providing effective information security training and education is essential since many employees are still negligent in complying with information security policies and behave accordingly (da Veiga et al., 2020). Based on these reviews, the study aims to explore the motivational components related to cyber security that can enhance cyber security protective behaviour among the employees. On top of that, this study attempts to explore other possible components that can strengthen the relationship between cyber security protection motivation and cyber security protective behaviour of the employees in the organisation, such as cyber security awareness, attitude, and cyber security competencies among the security managers who play a major role in developing information security strategic planning in the organisation. In doing this, the following research questions have been constructed:

a) What are the predictors of cyber security protection motivation that can shape employees' cyber security protective behaviour in IR 4.0 business environment?

b) What are the security competency components that can play a role in enhancing the relationship between protection motivation and protective behaviour in the aspect of cyber security?

Literature Review

Cyber security Protection Motivation

Protection Motivation Theory (PMT) is anchored on factors triggering several perceived threats

that will motivate people to engage in protective behaviour (Chang et al., 2022; Wong et al., 2022). This theory that has been widely used in human behaviour studies and several of the factors suggested in PMT, such as perceived severity, perceived susceptibility and self-efficacy are fundamentals to predicting human behaviour (Chen et al., 2022; Wu, 2020; Wang et al., 2019;). Few studies have adopted PMT to study users' behaviour towards information security (Chen et al., 2022; Hanus & Wu, 2016). However, these studies only focused on psychological aspects of users but overlooked a comprehensive exploration and further empirical examination of cyber security predictors. Technological developments are always changing, making earlier developments in PMT incomprehensible due to emerging aspects including those ingrained in organisational security culture, social concerns and others (da Veiga et al., 2020).

PMT is based on two (2) main factors that are believed to motivate users to protect themselves, namely threat appraisal and coping appraisal. Threat appraisal assumes that if people have a strong perception concerning the severity and vulnerability of a threat, it can motivate them to avoid security incidences (Younghwa, 2011). Conversely, coping appraisal refers to the ability of people to avoid security risk (response cost perceived barrier) and believe that they can practise the recommended security behaviour successfully (response efficacy, self-efficacy) (Plotnikoff et al., 2009).

In light of growing conflicting juxtapositions of recent research on PMT, it is clear that the theory has been ignored or could not have plausibly aligned their assumptions with today's depth of global digitalization and IR 4.0 during their time of inception (David et al., 2020). Therefore, a dire need to further explore into what these probable and timely predictors influencing users' cyber security protective behaviour are, and empirically to determine how employees' experiences of IR 4.0 influences their behaviours to adopt good cyber security practises. The current study's investigation attempts to fill these significant gaps. Congruently, the current study attempts to identify gaps in earlier research by focusing on a comprehensive review of potential cyber security protective behaviour actors that have been empirically developed.

The current study aims to build upon these actors as a guide to further explore newer and more timely predictors which provoke novel insights that more closely identify with the aims of the study. This will aid in examining how workforce perceptions of and responses to threat appraisal and coping appraisal affect cyber security protective behaviour. It will also help in understanding how the expertise of the cyber security competencies in various fields such as Information Security Intelligence, Cyber Digital Forensics Analysis, Cyber security Risk Assessment, Cyber security Threat Management and Cyber security Strategy Management can influence the cyber security protection motivation. Thereby, the cyber security protective behaviour tends to lean towards a more responsible and positive direction. The role of the cyber security competencies among the security manager was proposed as one of the components in this study, as they are the ones who have the most responsibility as well as authority over steering the cyber security protective behaviour of the employees in the correct direction. How they attempt to do the steering will be a significant portion of the study. It will also allow the study to analyze the gaps in the present attitude and behaviour related to the awareness of employees working in the various organisations operating in the IR 4.0 business environment.

Cyber security Protective Behaviour and Attitude

It is extremely essential for all organisations to ensure that their employees adhere to good cyber security protection behaviours. This includes ensuring that the employees are not allowed to access sensitive data and information through any device or network, unless it has first been verified and

authorized by the Information Technology (IT) specialists at the organisations. It also includes stopping employees from accessing unsafe websites from devices that they use for accessing the data stored in the organisation's databases. These are some of the measures that organisations often take to promote the importance of good cyber security protective behaviour (Mashiane & Kritzinger, 2018). The promotion of good cyber security protective behaviour is an extremely essential motivating factor towards promoting the need for information security intelligence skills and protection motivation amongst the employees of the organisation. This is even more necessary for the organisations that are operating in the public sector. This is because these organisations often handle vast amounts of sensitive information that affects the well-being of the public at large. Likewise, a positive attitude towards cyber security protection is an integral necessity. Organisations must recognize the necessity of a positive cyber security protective attitude of their employees (Jeong & Zo, 2021). Hence, this can lead to good cyber security protective behaviour. It must be noted that the importance of a highly positive cyber security protective attitude is even more required for any organisation that is operating in IR 4.0 environment. It depends on the organisation, how it will instill upon its employees, the importance of a positive cyber security protective awareness. The best way to achieve this is by educating them and making them more aware about the cyber security protection measures as all their various activities can make the data stored in the organisation's database more vulnerable to a cyber security breach (Wong et al., 2022). Knowing more about the things that they should avoid rather than risk has become vulnerable to cyber security breach or attack is a good way to initiate the beginning of enhancing a positive cyber security protective attitude. A highly positive cyber security protective attitude is also responsible for promoting more responsible behaviour on the employees' end (Huang & Pearlson, 2019).

Procedural Information Security Countermeasure Awareness

Awareness about cyber security protection can contribute in great manner towards enabling organisations to be more cautious, hence to ensure that their behaviour in the cyberspace is responsible (Li et al., 2019). Responsible behaviour of employees in the cyberspace will allow for a more protected and less vulnerable workspace. In further support of this proposition, Hadlington (2018) referred the case of workspaces in the United Kingdom (UK), for the analysis of the employees' attitude working in organisations within the UK, concerning the necessity for cyber security and what constitutes as risky online behaviour, in their perspective. He stated that the attitude of the employees working within the organisation can be made more positive with regards to cyber security protective behaviours, only by educating them on the risks that they exposed upon themselves and the organisation through their irresponsible and risky online behaviours. This is also supported by other study which stated that greater awareness about cyber security protection has been seen to be great motivator for good cyber security protective behaviour and more positive cyber security protective attitude (Torten et al., 2018).

Bartnes and Albrechtsen (2016) examined how suitable the approaches are for the industrial safety management, with regards to information security incident management. They alleged that they are highlighting on how effective the recent developments in the theoretical as well as practical fields are in the protection of industrial safety management and measures. They also stated that it is very essential for the organisations implementing these measures to ensure the effectiveness and to enable the organisation to maintain its information security and incident management in better manner.

Additionally, Fruhen et al. (2014) stated the importance of the role that the senior management of the organisation has to play in promoting cyber security protective awareness, thereby stressing on the need for better cyber security protective behaviours and attitudes. According to them, the role of the senior management is indispensable in encouraging the employees to instill the need for good cyber security protective behaviours. The senior management's awareness of cyber security risks has a direct impact on the cyber security behaviours and attitudes of the employees, and they can set a good example for their subordinates.

Cyber security Competencies

Employees who operate within cyber domain should have several cyber security competencies, such as technical skills, domain specific knowledge and social intelligence (Dawson & Thomson, 2018). Defining the knowledge, skills, attributes and other characteristics is not as simple as defining a group of technical skills that people can be trained on; the complexity of the cyber domain makes this a unique challenge. Therefore, this study explores several different cyber security competencies that the security manager should have, as suggested below.

• Information Security Intelligence

This is integral for determining the employees' awareness with regards to the importance of the need for information security intelligence skills. The managers must ensure that the employees are well-aware of the organisation's cyber security infrastructure and can make successful evaluation of all the necessary appraisals, namely threat, coping, risk and strategy appraisals, in order to determine the parameters necessary for instilling the need for highly positive cyber security protective behaviour amongst the employees that are working in the organisation (Zammani & Razali, 2016). This is a valuable ability to be acquired by managers, especially those that are working for organisations operating under the public sector. Such managers can make very valuable contributions towards raising positive cyber security protective behaviour amongst the employees.

• Cyber Digital Forensics Analysis

This is also essential as organisations operating in the public sector must look for in their managers. A manager must be extremely attuned to correctly analyze and appraise the risks involved as well as the strategies being implemented into the running of the organisation's system. They must be able to handle strategy appraisals, identify potential risks and are therefore able to mould the system accordingly. Such managers are more able to instill the necessity and need for a positive cyber security protective attitude amongst the employees that are working for the organisation. This is especially necessary for the organisations operating in the public sector, since more and more of their activities are being digitized (Sharevski, 2015). Managers who possess expertise in cyber digital forensics analysis are therefore needed by the hour especially in the public sector.

• Cyber security Risk Assessment

Cyber security risk assessment can be a valuable asset for managers since most of the transactions and processes of organisations are steadily getting digitized. It is therefore extremely necessary that managers are able to correctly analyze and appraise the risks that are involved. Such managers are able to instill among their subordinates a better sense of what are the parameters that determine what constitutes good cyber security protective behaviour. It is the managers' duty to ensure that the employees in their organisation, understand the risks involved and how their activities will reflect on their cyber security protective behaviour. By doing so, the managers are instilling the

importance of good cyber security protective behaviour amongst their employees (Ganin et al., 2020). Such managers are the necessity of the organisations as they are operating in the public sector. The data that they handle are often very sensitive in nature, and if breached, can have vast and damaging effects on the welfare of the public.

• Cyber security Strategy Management

This is another essential expertise that managers these days must possess. One of the best ways to ensure that the system is well protected from any outside threat is to analyze the implementation of the strategy and how it affects the welfare of the organisation, its employees and the people the organisation serves. It also includes determining ways to minimize the threats that might have arisen after the appraisal of the strategy. Such managers are competent in appraising the organisation's strategy and they chart ways to rectify the flaws that are present in the current system. Their competency in cyber security management is often a very strong determining factor of how strategy appraisals can be effectively utilized in a manner that will promote cyber security protective awareness amongst the employees working in the organisation (Chabinsky, 2010). The necessity of such managers is sought-after in the organisations that are operating in the public sector. This is because they are committed in not only raising and enhancing cyber security protective awareness, but also are responsible in offering valuable insights into what constitutes a better strategy for promoting information security intelligence skills and protection motivators for cyber security behaviour.

Based on the literature reviews discussed above, this study proposed the following model as shown in Figure I.

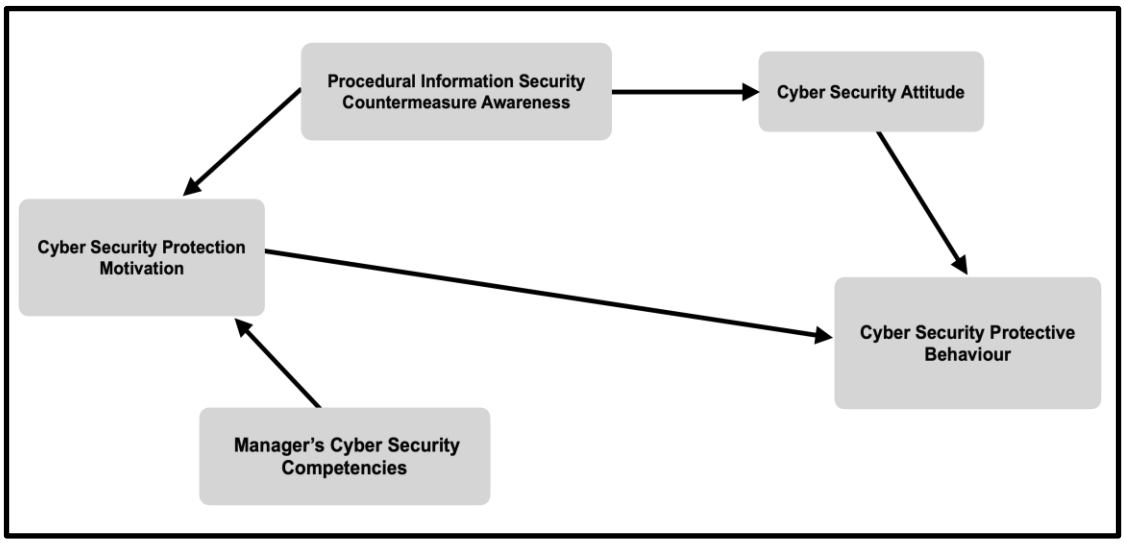

Figure I: The Conceptual Mode

Methodology

A scoping review has been conducted to identify the gaps in the study by searching the available articles related to cyber security protective behaviour and information security compliance behaviour. It has been applied to compile the theories and concepts of information security behaviour from literature, focusing on the articles that have made a significant impact on enhancing employees ability to practice information security behaviour adequately. Additionally,

this method helps the researchers identify the gaps in the particular study and propose a holistic research framework related to cyber security protective behaviour. In doing so, the study follows the scoping review method suggested by Arksey and O'Malley (2005), which consists of several steps as shown in Figure II.

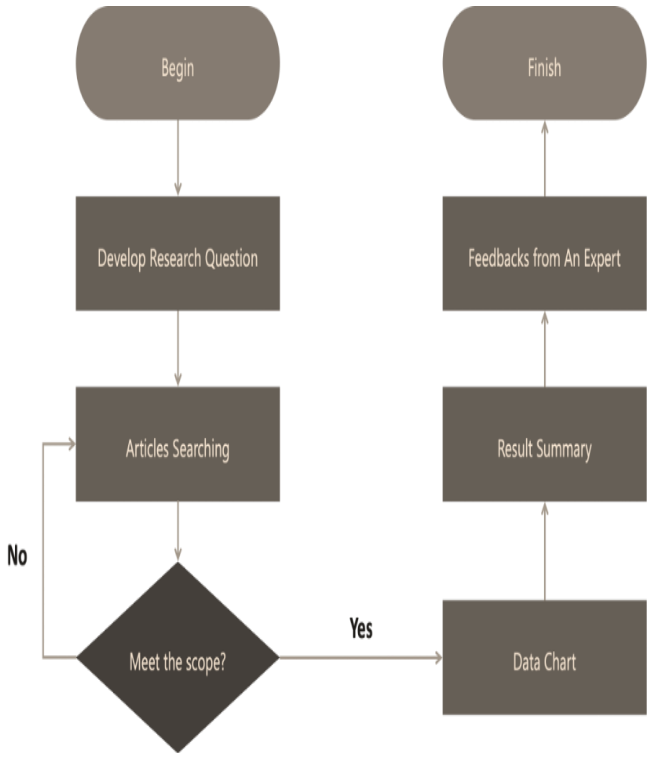

Figure II: Steps in Scoping Review

The study begins by identifying the issues related to cyber security (phase 1). The discussion of this issue helps the researcher construct the research questions related to it. Phase 2 is to identify the relevant studies. This has been conducted by searching related articles from various prestigious databases such as Science Direct, Emerald, and Scopus using a proper searching technique such as using the right keywords or combining the keywords with Boolean operators. Likewise, synonyms and alternative terms should be considered to elicit further information (Grewal et al., 2016). Grewal et al. (2016) also mentioned that spelling is also important when executing search tasks. Most databases use controlled word stock to establish common search terms (or keywords). Some of these alternative keywords can be looked up in the database thesaurus.

Next is Phase 3, to evaluate the articles from the search results. This can be done by identifying the scope of the studies and the inclusion and exclusion criteria for selecting the articles for the study. In this study, for inclusion criteria, any recent empirical research articles related to information security or cyber security protective behaviour were selected. The study also selected any concept paper related to leaders capabilities in managing information security in the organisation. Meanwhile, the study has excluded any articles published in the proceeding, any technical paper, and any publication before the year 2010.

Phase 4 is to extract the relevant information from the articles using the data charting method, while the next phase (5) is summarising the results of the findings. The summary result helps researchers draw the research framework. A preliminary study was implemented in Phase 6 by emailing the structured interview questions to the cyber security experts using the purposive sampling technique. The aims of this preliminary study were to ensure the relevance of the study and to confirm the dimensions that were used to construct the final research framework that will be tested quantitatively in the future.

Implications

The purpose of the study is to demonstrate the need for capable managers in charge of handling and managing organisational cyber security challenges. The subsequent research will make an effort to identify any existing limitations through this research as well. This will make it easier for us to comprehend how reputational harm from cyber security breaches might occur.

This study's theoretical implication is that it seeks to add to the body of knowledge on the subject of cyber security protective behaviour. The study's findings can close a research gap by evaluating the relationship between employees' compliance behaviour with information security practices and managers' competence in resolving cyber security challenges. The results of the study may also shed light on how employees' perceptions of the value of cyber security are influenced by their level of knowledge about it. This research may also aid in determining the variables that influence employees' cyber security behaviour and aid in the creation of theoretical frameworks that explain cyber security behaviour, particularly in digital corporate environments across all industries. Therefore, the study might be used as a starting point for later investigations into cyber security behaviour.

The purpose of this study, on the other hand, is to determine the elements that influence employees' motivation to engage in information security behaviour. Many organisations employ information technology (IT) in today's digital business contexts, especially in IR 4.0 business environments, and a lot of sensitive data can be processed and communicated digitally. The study's conclusions can therefore assist businesses in these new circumstances in developing information security strategic plans and improving their information security programmes to increase employee adherence to information security best actices. The study's findings may also shed light on how employees' perceptions of the value of cyber security are influenced by managers' skills in resolving related situations. This study can assist many organisations in protecting their sensitive data and any organisational information asset from cyber threats by identifying the elements that influence employees' cyber security behaviour. The study's findings will help organisations create security countermeasures that are efficient and reduce future cybersecurity threats.

Conclusions

The current study intends to achieve a few key objectives. First and foremost, the goal is to have a deeper knowledge of what drives employees to adopt appropriate information security behaviours in the IR 4.0 business context. Therefore, it is necessary for future research to make an effort to comprehend the part that the firm's management and cyber security capabilities have to play. This significant role contributes to raising awareness of cyber security and how it affects attitudes and behaviours towards this problem. Additionally, future research must strive to analyse the existing state of affairs in connection with relevant concerns in the IR 4.0 corporate environment, particularly in light of the COVID-19 pandemic and the requirement for cyber security awareness. Future research must also strive to narrow in on ways to fix existing problems

and look for solutions for firms working in the IR 4.0 business environment. In this approach, the overarching goal is to confront the situation more effectively and bring about changes to the way things are now.

Additionally, the upcoming research will contribute to a deeper comprehension of the current problem, especially the significance of cyber security expertise among security experts. Additionally, it might shed light on what drives employees' conduct to safeguard the information assets of the company. This research will also contribute to a greater understanding of the existing situation and potential future advancements in thwarting cyber security attacks. It is intended that the study will be helpful in addressing the numerous problems and can be used to effectively and efficiently resolve any defects that may be present.

Acknowledgment

We would like to express our gratitude to Universiti Teknologi MARA (UiTM) for awarding us this project funding [600-RMC/GPK 5/3 (094/2020)].

References

Arksey, H. & O'Malley, L. (2005). Scoping studies: Towards a Methodological Framework. Interbational Journal of Social Research Methodology, 8, 19-32.

Alaloul, S., Liew, M. S. , Noor Amila Wan Abdullah Zawawi & Kennedy, I. B. (2019). Industrial Revolution 4.0 in the construction industry: Challenges andoppor-tunities for stakeholders. Ain Shams Engineering Journal, 11(1), 225-230.

Ameen, N., Tarhini, A., Mahmood Hussain Shah, Madichie, N., Paul, J. & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cyber security compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114, 1-19.

Ani, U. D., He, H. & Tiwari, A. (2018). Human factor security: evaluating the cyber security capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2-35.

Bartnes, M. & Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. Information and Computer Security, 24, 20-37.

Cain, A., Edwards, M. E. & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36-45.

Chabinsky, S. R. (2010). Cyber security strategy: A primer for policy makers and those on the front line. Journal of National Security Law & Policy, 4(27), 1-13.

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, 1-22.

Chen, Y., Luo, X. R. & Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence. Information & Management, 59(2), 103575.

da Veiga, A., Astakhova, L. V., Botha, A. & Herselman, M. (2020). Defining organisational information security culture – Perspectives from academia and industry. Computers & Security, 92 , 1-23.

David, P. D., Keupp, M. & Mermoud, A. (2020). Knowledge absorption for cyber-security. Computers in Human Behavior, 106, 1-11.

Dawson, J. & Thomson, R. (2018). The Future Cyber security Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Frontiers in Psychology, 9, 1-12.

Fruhen, L. S., Mearns, K. J., Flin, R. & Kirwan, B. (2014). Safety intelligence: An exploration of senior managers' characteristics. Applied ergonomics, 45(4), 967-975.

Ganin, A. A., Quach, P. , Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D. & Linkov, I. (2020). Multicriteria decision framework for cyber security risk assessment and management. Risk Analysis, 40(1), 183-199.

Grewal, A., Kataria, H. & Dhawan, I. (2016). Literature search for research planning and identification of research problem. Indian Journal of Anaesthesia, 60(9), 635-639.

Grobler, M., Dlamini, Z., Ngobeni, S. & Labuschagne W. A. (2011). Towards a Cyber security aware rural community. Information Security South Africa Conference 2011, Hyatt Regency Hotel, Rosebank, Johannesburg, South Africa, August 15-17, 2011. Proceedings, ISSA, Pretoria, South Africa.

Hadlington, Lee, & Murphy, K. (2018). Is media multitasking good for cyber security? exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cyber security behaviors. Cyberpsychology, Behavior, and Social Networking, 21(3), 168-172.

Hanus, B. & Wu, Y. A. (2016). Impact of Users' Security Awareness On Desktop Security Behavior: A Protection Motivation Theory Perspective. Information System Management, 33(1), 2-16.

Huang, K. Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cyber security culture. Proceedings of the 52nd Hawaii International Conference on System Sciences.

Jeong, M. & Zo, H. (2021). Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques. Telematics and Informatics, 63, 101670, 1-17.

Kemper, G. C. (2019). Improving employees' cyber security awareness. Computer Fraud & Security, 2019 (8), 11-14.

Kimani, K., Oduol, V. & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25, 36-49.

Li, L., He, W., Xu, L., Ash, I., Mohd Anwar & Yuan, X. (2019). Investigating the impact of cyber security policy awareness on employees' cyber security behavior. International Journal of Information Management, 45, 13-24.

Plotnikoff, R. C., Trinh, L., Courneya, K. S., Karunamuni, N., & Sigal, R. J. (2009). Predictors of aerobic physical activity and resistance training among Canadian adults with type 2 diabetes: An application of the Protection Motivation Theory. Psychology of Sport and Exercise, 10(3), 320-328.

Mashiane, T. & Kritzinger, E. (2018). Cyber security behaviour: a conceptual taxonomy. IFIP International Conference on Information Security Theory and Practice (pp. 147-156). Springer, Cham.

Park, S., Ruighaver, A. B., & Ahamad, A. (2010). Factors influencing the implementation of information systems security strategies in organization. Paper presented at the International Conference on Information Sciences and Application.

Pang, M-S. & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cyber security risks of organizations: The case of U.S. federal government. Journal of Strategic Information Systems, 31, 101707, 1-19.

Safa, N., Maple, C. Furnell, S., Azad, M., Perera, C., Dabbagh, M. & Sookhak, M (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Generation Computer Systems, 97, 587-597.

Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis. Journal of Digital Forensics, Security and Law, 10(2), 39-54.

Torten, R., Reaiche, C. & Boyle, S. (2018). The impact of security awareness on information technology professionals' behaviour. Computers & Security, 79, 68-79.

Uchendua, B., Jason, R.C.N., Badac, M. & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387, 1-23.

Wang, J., Liu-Lastresb, B., Ritchiea, B. W. & Mills, D. J. (2019). Travellers' self-protections against health risks: An application of the full Protection Motivation Theory. Annals of Tourism Research 78, 102743, 1-12.

Wong, L-W., Lee, V-H., Tan, G. W-H., Ooi, K-B. & Sohal, A. (2022). The role of cyber security and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities, International Journal of Information Management, 66, 1-15.

Wu, D. (2020). Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. Computers in Human Behavior, 105, 1-14.

Yamin, M. M., Katt, B. & Gkioulos, V. (2020). Cyber ranges & security test beds: Scenarios, functions, tools & architecture. Computers & Security, 88, 1-26.

Younghwa, L. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. Decision Support Systems, 50(2), 361-369.

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors. International Journal on Advanced Science Engineering Information Technology, 6(6), 904-913.