Utilising Manager's Competency, Employee's Awareness and Motivation for Promoting Cybersecurity Protective Behaviour

Saif Hussein Abdallah Alghazo, Norshima Humaidi and Nooriha Bt Abdulla
Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia

saif.alghazo@gmail.com
norshima958@uitm.edu.my
nooriha.abdullah@gmail.com

https://doi.org/10.34190/ejkm.23.2.3895

Abstract: Technological developments have seen a rapid evolution in the last decade. The complexity and cyber-attacks increase within the advancement of technology and artificial intelligence, this creates pressures for corporations to adopt the necessary methods to ensure they function in a safe environment. This study attempts to assess the role of managers' informational security intelligence (MISI) along with procedural information security countermeasure awareness (PCM) and cybersecurity protection motivation in promoting cybersecurity protective behaviour among employees in the public sector within the context of UAE. The study employs quantitative cross-sectional design with primary data collected from 520 employees in nine listed organisations in the public sector of Abu Dhabi, UAE. The data is analysed using Partial Least Square Structural Equation Modelling (PLS-SEM). The findings indicated that perceived threat susceptibility, self-efficacy, information security problem-solving, and social competence significantly affect cybersecurity protective behaviour. Additionally, MISI positively influences PCM, which in turn affects cybersecurity protection motivation. Finally, attitude moderates the relationship between self-efficacy and cybersecurity protective behaviour. The study extended the protection motivation theory by investigating the capabilities and competences of managers related to information security in addition to adding the attitude as a moderating variable. The findings offer valuable insights for policy makers in the aspect of ensuring the implementation of cyber security national strategies; for managers in organisations in the aspect of promoting awareness and capabilities among themselves and among their employees through educational and training programs to enhance their cybersecurity practices and mitigate risks.

Keywords: Cybersecurity protective behaviour, Information security, Cybersecurity, Public sector, Information security intelligence, Information security competency

1. Introduction

Technological developments have seen a rapid evolution in the last decade. As technology evolves, business practices and methods have also drastically changed. In this direction, organisations now carry out their online transaction in a manner that achieves better performance, customer satisfaction and safety and security assurance. For this, they store their data digitally (Shaban, Farhan and Ahmed, 2022). Along with the efficiency of storing such data to be accessible anytime and anywhere, their vulnerability remains as a key issue in information security (Mohammed, 2019). In this context, organisations rely on clouds to store their data (Jang-Jaccard and Nepal, 2014) which implies that cybersecurity is the need of the hour.

The complexity and cyber-attacks increase within the advancement of technology and artificial intelligence (Siponen, Adam Mahmood and Pahnila, 2014; Li *et al.*, 2019). It is evident in the literature that the lack of attention to security measures and underestimating cybersecurity threats significantly influence the effect of security policies (Han, Kim and Kim, 2017; Li *et al.*, 2019). Further, exposure to cybersecurity training and knowledge does not necessarily result in higher extent of cybersecurity behaviour (Zwilling *et al.*, 2022).

Security behaviour have been studied in research from different perspectives such as behaviour of management leadership on employee's security behaviour (Guhr, Lebek and Breitner, 2019), employees' resilience in dealing with Information Technology (IT) security threats (Liang *et al.*, 2019) and cybersecurity policy awareness on employee's cybersecurity behaviour (Li *et al.*, 2019).

As more and more organisations become increasingly concerned about the cybersecurity threats in the workplace and have invested huge resources to tackle such issues, especially in the new environment after the pandemic where adopting technology became more essential (Vahdat, 2022).

In the UAE context, there is a remarkable growth in adopting technology among organisation due to the focus of the government and organisations in the United Arab Emirates (UAE) on innovation and technology investments

Cite this article: Alghazo, S.H.A., Humaidi, N. and Abdulla, N.B., 2025. "Utilising Manager's Competency, Employee's Awareness and Motivation for Promoting Cybersecurity Protective Behaviour", *The Electronic Journal of Knowledge Management,* 23(2), pp 14-40, https://doi.org/10.34190/ejkm.23.2.3895

to improve firm performance and achieve growth (Almehairbi, Jano and Mosali, 2022). Further, the establishment of smart government was one of the significant steps to support adopting technology in UAE business environment (Haddad *et al.*, 2020). When it comes to technological innovation in the public sector, UAE leads the Arab world globally in the aspect of open government, big data, mobile government and cloud computing as emerging tools to promote the performance of the public sector (Ahmat *et al.*, 2024). Further, Al Sayegh et al. (2023) indicate that in the UAE, smart government is an outcome of e-government initiative led by the government. In this context, the services of e-government include government to citizen, employee, business and to government to government (G2G). For instance, residents obtain smart pass ID number that can used to access all the portals of government to avail the available services. In the aspect of G2G services, better utilization of public resources is aimed by connecting all the public institutions and grouping all the services together under a single e-government portal (Eid, Selim and El-Kassrawy, 2021; Al Sayegh *et al.*, 2023).Under the current circumstances, more than 82% of organisations in the UAE's public sector have faced one or more cyber-attacks in the year of 2019 alone (Younies and Al-Tawil, 2020). Research also reveals that common cybersecurity such as password hacking, falling prey to phishing attacks, accessing malicious links on company systems, and mishandling of sensitive information are responsible for these cybersecurity breaches (Ocasio and Joseph, 2018).

The UAE has become a major target for cyberattacks due to its strong economy and widespread internet use, with 85% of the population active online (Al-Kumaim and Alshamsi, 2023). Cyberattacks in the UAE surged by 71% in 2021 compared to 2020, with organisations facing an average of 925 attacks per week in the fourth quarter of 2021, up from 408 in 2020. Phishing attempts reached 1.1 million, and ransomware incidents affected 59% of organisations, with an encryption rate of 46% (Adam, 2022; SOCRadar, 2022; Alalawi, 2024).

Several high-profile cyberattacks have targeted UAE industries over the years, employing tactics like ransomware, data encryption, and phishing. In 2023, LockBit ransomware used double extortion to encrypt and threaten to leak sensitive data (SOCRadar, 2022). Similarly, the Conti ransomware attack in 2022 encrypted files and threatened to release stolen information unless a ransom was paid (SOCRadar, 2022). Due to this, the importance is geared towards the competences, skills and capacities of managers in respect to information security intelligence (Y. Connolly and Wall, 2019). Managers' information security intelligence (MISI) competencies make them exhibit familiarity with wide range of information security skills such as security and network architectures, systems and frameworks, and compliance related skills. Intelligence skills necessary for the security of information and the protection motivation for cybersecurity behaviour become an essential competency (Campbell, 2017). In this aspect, questions are raised regarding the role of such skills related to information security possessed by managers in addition to protection motivation and countermeasures awareness in promoting employees' cybersecurity protective behaviour. More particularly, the following questions are stated: (1) What is the role of cyber security protection motivation, countermeasures awareness and MISI competencies in promoting employee's cyber security protective behaviour, (2) How does the employees' attitude moderate the role of motivation in embracing protective behaviour?

Research show that UAE had the highest number of phishing attacks in the Middle East, with over 38% of attacks aimed at stealing money (Al Neaimi, Ranginya and Lutaaya, 2015a; Al-Kumaim and Alshamsi, 2023). While the government entities in Abu Dhabi have invested in various types of software and hardware technologies to mitigate cybersecurity risks, there has been an increase in ransomware attacks in Abu Dhabi, with 33% of the targeted companies being based in the UAE, according to a report by Group-IB (Ahmed Hassan and Ismail, 2022). The report by the Telecommunications Regulatory Authority (TRA) in the UAE also highlights a 250% increase in cyber-attacks in the country in the first five months of 2021 compared to the same period in the previous year (Tubaishat and AlAleeli, 2024). These statistics emphasise the need for both government and private sectors to invest heavily in cybersecurity technology and upgrade it periodically to match the onslaughts of cybercrime.

Public and private sectors in the UAE are actively engaged in cybersecurity. However, the public sector tends to have stricter regulations and a more centralised approach due to national security concerns, but in the private sector challenges my face smaller companies having weaker security practices. This variance between the two sectors, highlights the level of compliance to cybersecurity practices regulated by the government. The National Electronic Security Authority (NESA) focuses on maintaining effective rules and regulations data protection measures for critical infrastructure and government systems (UAE, 2022; Alalawi, 2024). This creates an untapped area for this study in the aspect of investigating the protection behaviour among employees towards cybersecurity within the public sector in the UAE context.

Furthermore, with the rapid advancements in technology and the growing reliance on digital platforms for business operations necessitated storing data in digital forms. This transformation contributed to business and

performance development and also exposed organisations to cyberattacks threats. Cybersecurity threats escalated in the UAE during the last five years (Younies and Al-Tawil, 2020; SOCRadar, 2022). Research indicates that regardless of investments in cybersecurity infrastructure, persistent cyber threats such as phishing, ransomware, and data breaches continue to challenge organisations. In this context, traditional cybersecurity training and awareness programs do not always lead to effective protective behaviours among employees (Zwilling *et al.*, 2022).

Prior research has explored various determinants of CPB, including cybersecurity policy awareness and protection motivation in promoting protective behaviour while dealing with cyber threats. However, limited research is observed in investigating the role of information security intelligence skills among managers and how they lead protection motivation towards embracing protective behaviour among employees.

Given the UAE's rapid digital transformation and the increasing cyber threats faced by its public sector, there is a need to explore how managers' information security intelligence, protection motivation, and countermeasure awareness shape employees' cybersecurity protective behaviour. Further, understanding the role of cybersecurity attitude in moderating the role of motivation can provide sufficient insights into how employees' perceptions and willingness to comply with security measures influence their actual behaviour. Investigating this area will offer sufficient insights into the strategic role of managerial competencies in fostering a security-conscious organisational culture, ultimately improving cybersecurity resilience in public organisation in the UAE context.

Due to the aforementioned issues, this study aims to evaluate how do manager's information security intelligence (MISI) competencies affect organisations' management of information security programs and how these MISI competencies influence CPB alongside dimensions of cybersecurity protection motivation. Additionally, the study examines how does employees' attitude toward practicing cybersecurity can enhance the relationship between their cybersecurity protection motivation and CPB as their awareness of this subject increases.

2. Literature Review and Hypothesis Development

The study is based on the Protection Motivation Theory (PMT) which explains employees' motivation in responding to warnings about threats. It is the most relevant theory in assessing the attention of engaging in protective cybersecurity actions (Li *et al.*, 2019).

PMT is based on five factors that are believed to motivate employees to protect themselves, and these factors are severity, vulnerability, response cost, and response efficacy. These factors are divided into two categories: threat appraisal (perceived threat severity and perceived threat susceptibility) and coping appraisal (self-efficacy and response efficacy). The PMT theory is selected due to its relevance in assessing behavioural change through persuasive messages and explaining how compelling communication might be constructed successfully (Rogers, 1975).

PMT has been used in the literature pertaining to examining employees' understandings on cybersecurity threats and develop coping responses (Vance, Siponen and Pahnila, 2012). Using the PMT paradigm, compelling communication, often known as emotional appeals, may forecast behavioural change (Renaud and Dupuis, 2019).

Within the application of PMT, Li, Xu and He (2022) extended it by incorporating organisational efforts such as information security efforts and employee awareness as antecedent factors for employee cybersecurity behaviour. Based on this, the study extends by extending PMT by including MISI as a key factor influencing the awareness as well as the behaviour of employees towards cybersecurity protective behaviour.

2.1 Cybersecurity Protection Motivation and Cybersecurity Protective Behaviour

Threat appraisal along with coping appraisal of PMT components are essential for organisations, especially in the public sector in order to ensure the adherence of employees to guidelines pertaining to cybersecurity protective behaviours (CPB) (Li, Xu and He, 2022). It also involves making sensitive data inaccessible for employees through unverified and unauthorised devices to ensure such protection. In addition to that, excluding access to unsafe websites from the devices used to access the data stored in the organisation is considered one of the measures adopted by organisations to promote the importance of good cybersecurity protective behaviour (Mashiane & Kritzinger, 2018).

Rogers (1975) opine that both affective and psychological reactions to threats play a substantial role in perceived behavioural control. It is evident that people are motivated by fear arousal (Ruiter, Abraham and Kok, 2001) which led to more investigation on the role of fear on behaviour intention (Cooper, Goldenberg and Arndt, 2014). Since motives are directly affected by fear, this study hypothesises that:

H1a: *Perceived Severity positively influences CPB.*

H1b: *Perceived Susceptibility positively influences CPB.*

In coping appraisal, a person's self-efficacy and response efficacy are influenced by their judgment of the proposed actions' efficiency and capacity to carry them out. Response efficacy and self-efficacy have improved behavioural intentions (Zajdel and Helgeson, 2020).

The individual's belief that their protective measures are effective is the definition of response efficacy (Alkhazi *et al.*, 2022), the absence of such belief results in abandoning such protective behaviours (Shillair, 2018). Fears and motives form the efficacy cognition when considering cybersecurity protective behaviour (Johnston and Warkentin, 2010). Therefore, the response efficacy is the individuals' belief in their ability in facing cybersecurity risks (Vance, Siponen and Pahnila, 2012). An optimization is required to promote response efficiency when it comes to cybersecurity (Zhang, Zhang and Jiang, 2023). Qiu et al. (2023) argue that response efficacy positively affects the preparedness for crisis and disasters.

The possibility that response efficacy leads the protective behaviour is evident in previous research, yet self-efficacy plays as a key factor in utilizing such capability to respond towards certain concerns (Thrasher *et al.*, 2016). The same is applicable when considering accepting technology (Zhang *et al.*, 2017). This indicates their effect on behavioural intentions (Rainear and Christensen, 2022).

Self-efficacy act as a key factor in promoting cybersecurity behaviour (Zainal, Puad and Sani, 2021), as it is evident that security self-efficacy leads to adopting security behaviour (Verkijika, 2020).

Further, the associated cost must be considered while ensuring protection. According to Bax, McGill and Hobbs (2021), the response cost is considered a significant influential factor on maladaptive and protective behaviours pertaining to cybersecurity while Bolívar and Dallery (2020) argue that the resurgence of human behaviour is affected by the response cost punishment.

H1c: *Response efficacy positively influences CPB.*

H1d: *Self-efficacy positively influences CPB.*

H1e: *Response cost negatively influences CPB.*

2.2 Procedural Information Security Countermeasure Awareness and Cybersecurity Protection Motivation of the Employees

Awareness about cybersecurity protection is the first and most integral motivator for promoting cybersecurity protection motivation. The employees working in an organisation must understand the threats they face when accessing the data and information present in the company's database.

High procedural information security countermeasure awareness is an essential factor that organisations must focus on including their employees (Zwilling *et al.*, 2022). This is primarily a critical necessity for organisations operating in the public sector. Mabitle and Kritzinger (2021) state the necessity for proper education and awareness as a contributing factor towards ensuring enhanced and greater procedural information security countermeasure awareness. Further, cybersecurity behaviour can be enhanced by the effort of educational institutions in their curricula (Deraman *et al.*, 2021).

It Is evident that PCM significantly and positively affects CPB In terms of attitude and intentions (Bulgurcu, Cavusoglu and Benbasat, 2009; Kim, Hovav and Han, 2019). Further, perceiving PCM as a negative tool result in exhibiting less protective behaviour (Kim, et al., 2019). Li et al. (2019) argue that awareness about cybersecurity protection can greatly enable organisations to be more cautious towards ensuring that their behaviour in cyberspace is responsible. Hence, for employees, responsible organisations are being exposed (Hadlington and Murphy, 2018). Therefore, greater awareness is considered a greater motivation for organisations towards adopting CPB. Hence, the study hypothesises:

H2a*: PCM positively influences Perceived Threat severity among employees.*

H2b*: PCM positively influences Perceived Threat susceptibility.*

H2c*: PCM positively influence response efficacy.*

H2d*: PCM positively influence self-efficacy.*

H2e*: PCM positively influence response cost.*

2.3 Managers' Information Security Intelligence (MISI) in an Organisation

The Managers' Information Security Intelligence (MISI) is responsible for ensuring that all the dependencies that have been defined above are correctly followed (Kim, Hovav and Han, 2019). MISI is relevant to all the activities of employees in respect to cyber security. MISI ensures that employees have a high sense of cybersecurity protective awareness which requires certain steps and procedures to be followed in the organisation (Humaidi and Abdallah Alghazo, 2022).

Safety Intelligence is the extent to which employees believe their managers are committed to safety, it is associated positively with organisational success (Clarke, 1999). This is affected by the perception of employees towards supervisory behaviours (Christian *et al.*, 2009).

Fruhen et al. (2014b) argue that safety intelligence of managers can have subcomponents such as safety knowledge, personality, regulatory commitment, social competence, and problem-solving abilities. Moreover, security managers are required to constantly develop skills such as problem-solving skills in order to be able to appropriately analyse and appraise the risks involved correctly. Cultivating such abilities among employees would reflect on their cybersecurity protective behaviour (Yoon, Arik and Pfister, 2020).

Further, knowledge of safety and cybersecurity of managers is essential especially for organisations in the public sector (Kim, Hovav and Han, 2019). Possessing such knowledge enable them to ensures systems and strategies adopted in the organisation are protected and functioning effectively along with ensuring cybersecurity is maintained.

Competency in safety knowledge among managers plays a crucial role in effectively utilizing strategy appraisals to enhance cybersecurity protective awareness among employees (Van Niekerk, 2018). This is particularly important in the public sector, where managers are pivotal in raising and enhancing cybersecurity awareness in the organisation (Prabhu and Thompson, 2022). Implementing effective safety management measures is essential for organisations to ensure their contribution to maintaining information security and managing security incidents effectively (Line and Albrechtsen, 2016).

Perceived information security knowledge is defined as the degree to which employees believe senior managers comprehend information security risks (Finkelstein, 1992). Embracing knowledge mechanisms among employees and managers is essential to promote cybersecurity in the organisation (Mady, Gupta and Warkentin, 2023). Information security knowledge is promoted by education and experience (An *et al.*, 2023). Therefore, possessing awareness positively leads to increasing information security knowledge among employees and managers (Alkhazi *et al.*, 2022). Organisation adopt certain approaches to promote their information security knowledge and awareness such as theoretical models, gamification and constructivist approaches (Khando *et al.*, 2021). Utilising data and resources promotes information knowledge in the organisation (Żywiołek and Schiavone, 2021). Hence, having the necessary knowledge acts as a motivation towards promoting cybersecurity in the organisation (Herbert, Schmidbauer-Wolf and Reuter, 2020; Alhogail, 2021).

Perceived information security problem solving skill is described as an employee's impression of the capacity of senior management to recognise information security concerns, suggest solutions, and develop action plans to overcome these difficulties (Kim, Hovav and Han, 2019). Following certain procedures allows managing predictable dangers (Spagnoletti and Resca, 2008). When considering cybersecurity protection motivation, problem-solving abilities contribute to senior managers commitment to safety (Fruhen *et al.*, 2014a). This supports the regular improvement in the organisation (Abdul Hamid *et al.*, 2015). Further, manager safety problem-solving abilities is a key factor in training employees in the organisation for information security (Fruhen *et al.*, 2014a) and safety-related regulations (Hamid et al., 2015). This implies that utilising information security problem solving acts as a motive to contribute towards maintaining cybersecurity in the organisation (Hu *et al.*, 2012).

Managers' competencies in managing information security programs within organisations have a positive influence on improving their employees' motivation toward information security (Taufan and Basalamah, 2021). Managers' connections with their employees motivates information security in the organisation (Liu, Wang and Liang, 2020). Furthermore, managers competencies are crucial for ensuring organisational performance (Szczepańska-Woszczyna and Gatnar, 2022). The enhancement of managers' social competencies leads to improved work and increased motivation among employees to practice cybersecurity behaviour (Oppong and Zhau, 2020).

According to Fruhen et al. (2014a), the role of the senior management is indispensable in encouraging the employees about the need for good cybersecurity protective behaviours. Hence, these employees can be led by

example, and the cybersecurity protective awareness of the senior management reflects directly upon the cybersecurity behaviours and attitudes of the employees. Based on these reviews, the following hypotheses were constructed:

H3a: *Perceived information security knowledge positively influences PCM.*

H3b: *Perceived social competence positively influences PCM.*

H3c: *Perceived information security problem-solving skills positively influence PCM.*

2.4 The Relationship Between MISI and CPB

In addition to this, MISI has three main components, Perceived Information Security Knowledge (PISK) which explains the extent to which senior managers are understand information security issues in the organisation; Perceived Information Security Problem Solving (PISP) which explains the extent of mitigating the issues faced in relevance to information security in the organisation; and perceived social competencies (PSC) which implies the capabilities utilised by senior managers to establish strong relationship with employees through communication to improve their performance and competitive advantage (Han and Ryu, 2016; Kim, Hovav and Han, 2019; Alghazo, Humaidi and Noranee, 2023).

The growth in the dependence of technology and Internet creates the need for sufficient knowledge, skills and capabilities to be utilised for better performance and information security. According to Zwilling et al. (2022), the increase of cybersecurity knowledge and awareness contributes to the increase of cybersecurity protective behaviour. Similarly lacking such knowledge and capabilities will negatively affect adopting the appropriate behaviour related to information technology. The literature provide evidence that the three dimensions of MISI are influential on the intention and behaviour related to information security (Kim, Hovav and Han, 2019; Alghazo, Humaidi and Noranee, 2023).

Security leaders are required to be participative in the organisation when it comes to cybersecurity management. Research shows that organisation should strategically invest in human capital and technology to promote cybersecurity management (Abraham, Chatterjee and Sims, 2019).

Mashiane and Kritzinger (2021) argue that even if organisations provide the necessary support for information security knowledge and competencies of employees and managers remain essential for its success. It is evident that employees' information security compliance intention behaviour can be promoted through information security knowledge and problem-solving skills (Chen *et al.*, 2021). This implies that managers remain the key player in promoting information security behaviour among employees (Hong and Furnell, 2021). Further, weak cybersecurity knowledge and skills among the security leaders would impact security decision-making quality and lead to decreased information security management performance.

Previous studies support this and found a positive effect of top management participation on information security awareness programs (Hasan *et al.*, 2021). Khando et al. (2021) also argued that the shared understanding amongst employees is influenced by how they perceive the role of management and the persuasiveness of communication by the security managers.

According to Whitman and Mattord (2019), the MISI's are also responsible for determining what constitutes good cybersecurity behaviour for the employees working at the organisation. The most important role of the MISI's is to promote a positive cybersecurity protective attitude amongst the employees. They achieve this by educating the employees, training them, and organizing workshops. In addition to that, they are responsible for ensuring that the necessity for information security intelligence and the protection motivation for cybersecurity behaviour are instilled amongst the organisation's employees. The role of the MISI's is even more crucial for organisations operating in the public sector since the data they deal with concerns the public welfare at large.

H4a: *Perceived information security knowledge positively influences CPB.*

H4b: *Perceived social competence positively influences CPB.*

H4c: *Perceived information security problem-solving skills positively influence CPB.*

2.5 The Moderating Role of Cybersecurity Attitude

Safa et al. (2015) and Parsons et al. (2017) stated that a person's (or an employee) views and feelings are directly influenced by what they know about information security countermeasures. Therefore, attitude is related to what a person believes and feels. The way a person practises security can be influenced both directly and indirectly by

their attitude and expertise. Attitude has explicit and implicit dimensions: a) explicit attitude, refers to that the employees are aware of the effect of their behaviour; and b) implicit attitude, refers to that the employees are not conscious of the effect of their behaviour (Yeng, Fauzi and Yang, 2022).

Previous studies on information security suggest that manger's support significantly influences employees' attitude and intentions toward security (Kankanhalli *et al.*, 2003; Chan, Woon and Kankanhalli, 2005; Knapp *et al.*, 2006). Managers can provide legitimacy to employees' information security policies and standards compliant behaviour by shaping their beliefs, norms, and attitudes toward new programs, initiatives or policies (Hu *et al.*, 2012). According to Bulgurcu, Cavusoglu and Benbasat (2010), the attitude and intentions of employees toward information security compliance are positively impacted by their perceptions of PCM. Based on this, the current study hypothesises that

> ***H5:*** *Employee's cybersecurity attitude moderates the effect of the dimensions of protection motivation on CPB.*

Although Protection Motivation Theory (PMT) has been extensively explored in terms of evaluating responses to cybersecurity threats (Vance, Siponen, & Pahnila, 2012; Li et al., 2019), there is a notable gap in the investigation of the role of managers' intelligence in the realm of information security (Fruhen et al., 2014a; Kim, Hovav, & Han, 2019). Additionally, research has highlighted the role of procedural countermeasure awareness in motivating employees to adopt cybersecurity protective behavior (Mabitle & Kritzinger, 2021; Zwilling et al., 2022), but the role of managers' skills in promoting this awareness remains underexplored. Furthermore, while previous research has examined the moderating role of attitude in similar contexts related to employee behavior (Safa et al., 2015; Parsons et al., 2017), there is a lack of investigation into how employees' attitudes influence the effect of motivation on adopting CPB. Moreover, while studies have explored cybersecurity and employee protective behavior in the private sector (Johnston & Warkentin, 2010; Li, Xu, & He, 2022), there is limited research on these aspects within the public sector. This gap provides an opportunity for this study to explore how managers' information security intelligence, cybersecurity protection motivation, and cybersecurity procedural countermeasure awareness influence the practice of adopting cybersecurity protective behavior among employees in the public sector within the context of the UAE.

3. Research Method

3.1 Research Design

This study employed quantitative cross-sectional design with an exploratory approach. It relies on a research questionnaire as the main instrument to process the collected data in numerical form for analysis.

3.2 Measurement and Survey Instrument

This section provides a brief description about the measurement of the study variables while a complete list of the variables with their measurement items can be found in Appendix (1).

Managers' Information Security Intelligence Skills (MISI) is measured with 14 items adopted from (Kim, Hovav and Han, 2019) and divided into three dimensions Perceived Information Security Knowledge (5 items) a sample item of it is "senior managers of my company know about information security", Perceived Information Security Problem-Solving (4 items) a sample item of it is "senior managers of my company maintain a balance between information security management and its costs", and Perceived Social Competence (5 items) a sample item of it is "senior managers of my company operate an open-door policy".

Cybersecurity Protection Motivation (CPM) was measured with 18 items based on (Mousavi *et al.*, 2020; Li, Xu and He, 2022), they are divided into five dimensions, which are Threat Severity (4 items) with a sample item "if my information released to unauthorised people, it would be very bad for me", Threat Susceptibility (5 items) with a sample item "my information is at risk for being released to unauthorised people", Self-efficacy (3 items) with a sample item "it is easy for me to use privacy assurance mechanisms", Response Efficacy (3 items) with a sample item "complying with the information security policies in my organisation will keep security breaches down" and Response Cost (3 items) with a sample item "".

Five items were adapted from (Simonet and Teufel, 2019) to measure Procedural Information Security Countermeasure Awareness (PCM) with a sample item "i recognise that safe security practices are needed to deal with cybersecurity threats and risks". Finally, five items adopted from (Li *et al.*, 2019) to measure Cybersecurity Protective Behaviour (CPB) with a sample item "I keep the anti-virus software on my computer up-to-date", and

another five items adopted from (Hadlington, 2017) were used to measure Cybersecurity Protective Attitude (CTA) with a sample item "it is inconvenient to check the security of an email with attachments".

3.3 Sampling and Data Collection Procedures

Three categories of respondents are targeted: IT staff, administrative staff and management/leadership as explained in Table 1. The sampling frame indicates that the total number of units in nine listed corporations in the public sector in Abu Dhabi is 3415. Based on the total the three categories are identified and the sample calculation is conducted based on their weight against the total population.

Stratification is followed to draw the sample from the study population based on the size of the population. In the listed organisations, three strata of respondents are highlighted, IT staff, administrative staff and management staff. Out of these strata, the targeted sample size is determined where management and leadership staff account for 40% of the population, while IT staff and administrative staff accounted for 30% each. Several resources are consulted in respect of the sufficient sample size which yielded that 400 to 500 responses are considered sufficient for such population (Hair *et al.*, 2010). In the case of power analysis, 189 was recommended as the minimum sample size for 13 predictors and effect size of 0.15.

The research questionnaire was distributed in print to minimise the potential for bias. However, in cases where delivering a hard copy was difficult (211 cases), email communication was used. A Google Forms link was sent to respondents after obtaining their consent to participate in the study. The distribution was carried out through random selection from the sampling frame, and respondents were given 30 days to complete the questionnaire. Approximately 27% of respondents received two reminders to ensure timely submission. The questionnaire was available in both English and Arabic to ensure better clarity. The translation was supervised by professors from the UAE and India, and validated through back translation. Out of 600 distributed forms, 520 were completed, resulting in a response rate of 86.6%.

Table 1: Demographic characteristics of respondents

Variable	Category	Frequency	Percent
Gender	Male	184	35.4
	Female	336	64.6
Age	18-24 Years	6	1.2
	25-34 Years	52	10.0
	35-44 Years	294	56.5
	45-54 Years	152	29.2
	55 or above	16	3.1
Qualification	Master Degree	191	36.7
	Bachelor Degree	233	44.8
	High School	82	15.8
	PhD or Higher	14	2.7
Experience	1-3 years	83	16.0
	4-6 years	154	29.6
	7-10 years	245	47.1
	More than 10 years	22	4.2
	Less than 1 year	16	3.1
Position	Entry-level employee	85	16.3
	Mid-level employee	141	27.1
	Senior-level employee	163	31.3
	Managerial/Supervisory position	131	25.2
Institution	Department of Digital Authority	108	20.8
	Abu Dhabi Judicial Department	118	22.7

Variable	Category	Frequency	Percent
	Abu Dhabi Security Exchange	64	12.3
	Abu Dhabi Chamber	74	14.2
	Abu Dhabi Investment	53	10.2
	Department of Finance	29	5.6
	Federal Authority for Identity and Citizenship	41	7.9
	Statistics Center Abu Dhabi	33	6.3
Cybersecurity attacked before	Yes	101	19.4
	No	419	80.6
Using mobile phone for work	No	136	26.2
	Yes	384	73.8
Allowed to work remotely	No	287	55.2
	Yes	233	44.8
Total		520	100.0

3.4 Data Analysis

Partial least square structural equation modelling (PLS-SEM) approach by using SmartPLS software version 4 was used to analyse the final data. In this analysis the measurement model is assessed for reliability and validity of the research model, then the structure model is assessed for path coefficient assessment and moderation analysis. PLS-SEM has become a significant tool in management and information system research. It differs from covariance-based SEM (CB-SEM) by being a non-parametric test for multivariate factor analysis. According to Rouse and Corbitt (2008), applying PLS-SEM in information system research requires careful attention due to misuse, lack of training and reliability and validity concerns. However, in recent research, PLS-SEM has developed to become more acceptable in information system research along with the awareness of research applying advanced tools (Cepeda *et al.*, 2024). Further, PLS-SEM is more adopted among researchers in Industrial Management and Data Systems (IMDS) due to the ability to handle model complexity and improving prediction assessment along with other advanced features (Sabol *et al.*, 2023). Research articles present methodological guidance for researchers in information system (Al-Emran, Mezhuyev and Kamaludin, 2019). Finally, Hair et al. (2017) argue that PLS-SEM increased maturity in information system research due to model complexity and formative, measurement rather than just focusing on small sample data and non-normal data. Hence, PLS-SEM is selected to analyse the data for the current study.

4. Results

4.1 Data Coding and Screening

Data was screened and managed to ensure its appropriateness for analysis. In this process, incomplete responses were excluded; valid responses were coded to ease the analysis. In addition, normality assessment was conducted to ensure the homogeneity of the responses through ensuring Skewness and Kurtosis are within 2 and -2 (Kim, 2013).

4.2 Common Method Variance

Common method bias was assessed to ensure there is no bias that can compromise the responses accuracy and negatively impact the research outcome (MacKenzie and Podsakoff, 2012; Kock, 2017). Harman's single-factor which yielded a cumulative variance explained of 41.2% which is below 50%. Further, marker variable was conducted (Miller and Simmering, 2023) where the coefficients are compared before and after adding the marker variables and the results indicates that there are no remarkable differences between both set of coefficients.

Multicollinearity is assessed to ensure data is free from multicollinearity issues. Variance Inflation Factor (VIF) is followed to do so and the results indicated that VIF values range between 1 and 2.906 which is below the limit (3.33) (Hair *et al.*, 2019).

Non-response bias (de Winter *et al.*, 2005) which assesses the difference between the first and last 20 responses using variance analysis which indicated that there is no significant difference between the first and last 20 responses ($p > 0.05$)

4.3 Assessment of the Measurement Model

In the process of establishing the research model reliability and validity, the PLS-SEM approach is used to identify the measures of reliability and discriminant validity (Hair, Ringle and Sarstedt, 2011).

Factor loading values are assessed to ensure the contribution of the items in each latent variable in the research model. The results indicates that they range from 0.715 to 0.918 which is considered sufficient according to the threshold of 0.708 recommended in scholarly research (Hulland, 1999; Hair *et al.*, 2016).

The reliability measures assessed are Cronbach's Alpha (a) and composite reliability (CR), where are the values were found to exceed 0.70 (Hair *et al.*, 2019). Further, the values of average variance extracted (AVE) have to exceed 0.50 which was also evident in the study results by exceeding 0.50 (Hair *et al.*, 2021). The details of the results are presented in Table 2.

Table 2: Reliability assessment

	Mean	Std. Deviation	Loading
Perceived information security knowledge a = 0.835, CR = 0.839 and AVE = 0.604			
PISK1	3.92	1.368	0.715
PISK2	3.96	1.352	0.818
PISK3	4.07	1.325	0.814
PISK4	4.16	1.177	0.799
PISK5	4.23	1.131	0.734
Overall	4.0685	0.98853	
Perceived social competence a = 0.872, CR = 0.873 and AVE = 0.664			
PSC1	4.16	1.353	0.821
PSC2	4.26	1.226	0.866
PSC3	4.30	1.206	0.835
PSC4	4.19	1.239	0.822
PSC5	4.32	1.134	0.725
Overall	4.2454	1.00585	
Perceived information security problem-solving a = 0.849, CR = 0.849 and AVE = 0.689			
PISP1	4.06	1.245	0.819
PISP2	4.18	1.157	0.846
PISP3	4.14	1.252	0.862
PISP4	3.99	1.309	0.791
Overall	4.0913	1.01093	
Procedural Information Security Countermeasure Awareness (PCM) a = 0.855, CR = 0.859 and AVE = 0.635			
PCM1	4.15	1.149	0.739
PCM2	4.19	1.203	0.772
PCM3	4.26	1.126	0.830
PCM4	4.17	1.193	0.850
PCM5	4.10	1.218	0.789
Overall	4.1758	0.93756	
Cybersecurity Protective Attitude (CTA) a = 0.866, CR = 0.867 and AVE = 0.653			
CTA1	4.03	1.245	0.772
CTA2	3.94	1.312	0.839

	Mean	Std. Deviation	Loading
CTA3	4.06	1.218	0.839
CTA4	4.05	1.282	0.847
CTA5	4.20	1.175	0.736
Overall	4.0542	1.00713	
Threat Severity a = 0.868, CR = 0.869 and AVE = 0.718			
SEV1	4.22	1.086	0.816
SEV2	4.20	1.201	0.877
SEV3	4.14	1.187	0.877
SEV4	4.16	1.128	0.817
Overall	4.1774	0.97557	
Threat Susceptibility a = 0.877, CR = 0.878 and AVE = 0.671			
SUSC1	4.21	1.115	0.789
SUSC2	4.20	1.106	0.813
SUSC3	4.27	1.121	0.871
SUSC4	4.25	1.117	0.848
SUSC5	4.15	1.216	0.771
Overall	4.2162	0.92786	
Self-efficacy a = 0.859, CR = 0.86 and AVE = 0.781			
SE1	3.96	1.303	0.885
SE2	3.94	1.342	0.896
SE3	3.85	1.327	0.869
Overall	3.9135	1.16980	
Response Efficacy a = 0.844, CR = 0.847 and AVE = 0.764			
RE1	3.825	1.326	0.894
RE2	3.844	1.326	0.907
RE3	3.775	1.372	0.818
Overall	3.814	1.17	
Response Cost a = 0.856, CR = 0.863 and AVE = 0.776			
RC1	3.838	1.292	0.918
RC2	3.969	1.279	0.838
RC3	3.775	1.23	0.885
Overall	3.861	1.116	
Cybersecurity Protective Behaviour (CPB) a = 0.904, CR = 0.906 and AVE = 0.723			
CPB1	3.86	1.333	0.824
CPB2	3.84	1.323	0.838
CPB3	3.83	1.330	0.886
CPB4	3.87	1.281	0.883
CPB5	3.89	1.309	0.817
Overall	3.8608	1.11759	

For discriminant validity, Fornell and Larcker (1981) yielded satisfactory outcome where the correlation values of each variable are found below the square root values of the average variance extracted of the same variable (Table 3). Similarly, Heterotrait Monotrait criteria (HTMT) yielded acceptable outcome by having the similarity values across all variables below 0.85. This implies the establishment of discriminant validity. No violations were detected when observing cross loading values as well (Table 4).

Table 3: Discriminant validity of reflective constructs (F&L).

Constructs	CPB	CTA	PCM	PISK	PISP	PSC	RC	RE	SE	SEV	SUSC
CPB	***0.850***										
CTA	0.550	***0.808***									
PCM	0.529	0.731	***0.797***								
PISK	0.529	0.623	0.669	***0.777***							
PISP	0.571	0.617	0.577	0.680	***0.830***						
PSC	0.513	0.613	0.606	0.654	0.662	***0.815***					
RC	0.403	0.479	0.565	0.479	0.459	0.493	***0.881***				
RE	0.536	0.491	0.493	0.545	0.529	0.422	0.594	***0.874***			
SE	0.423	0.485	0.460	0.482	0.500	0.516	0.375	0.427	***0.883***		
SEV	0.464	0.680	0.634	0.573	0.525	0.602	0.450	0.431	0.367	***0.847***	
SUSC	0.567	0.662	0.709	0.594	0.563	0.571	0.51	0.517	0.392	0.711	***0.819***

Resource: Responses analysis.

Table 4: Discriminant validity of reflective constructs (HTMT).

Constructs	CPB	CTA	PCM	PISK	PISP	PSC	RC	RE	SE	SEV	SUSC
CPB											
CTA	0.619										
PCM	0.604	0.846									
PISK	0.607	0.733	0.790								
PISP	0.650	0.717	0.674	0.808							
PSC	0.577	0.704	0.700	0.767	0.770						
RC	0.449	0.549	0.651	0.564	0.529	0.563					
RE	0.613	0.576	0.581	0.651	0.624	0.493	0.705				
SE	0.479	0.561	0.535	0.571	0.583	0.594	0.436	0.501			
SEV	0.521	0.784	0.734	0.67	0.610	0.692	0.516	0.504	0.423		
SUSC	0.634	0.761	0.816	0.692	0.652	0.653	0.580	0.601	0.452	0.815	

Resource: Responses analysis

4.4 Assessment of the Structural Model

The research outcome related to assessing the significance of the relationships across the research model are depicted in Table 5 and Figure 1. As illustrated in Table 5, the R^2 values of 0.479 explains the variance in CPB that is influenced by managers' information security intelligence Procedural Information Security Countermeasure Awareness, protection motivation dimensions were above the 0.26 value as suggested by Cohen (1988) indicating a solid model.

As for the effect of protection motivation dimensions on CPB, the results indicate that protective behaviour (CPB) is significantly influenced by perceived threat severity (β = -0.093, f^2 = 0.006, p = 0.120), perceived threat susceptibility (β = 0.237, f^2 = 0.037, p = 0.001) and response efficacy (β = 0.241, f^2 = 0.048, p = 0.001), while no significant effect on self-efficacy (β = 0.079, f^2 = 0.007, p = 0.130) and response cost (β = -0.076, f^2 = 0.003, p = 0.167) (Table 5).

As for the effect of PCM on protection motivation dimensions, the results indicates that PCM is found to be a significant factor in influencing perceived threat severity (β = 0.634, f^2 = 0.672, p = 0.001), perceived threat susceptibility (β = 0.709, f^2 = 1.010, p = 0.001), self-efficacy (β = 0.460, f^2 = 0.269, p = 0.001), response efficacy (β = 0.493, f^2 = 0.322, p = 0.001), and response cost (β = 0.565, f^2 = 0.468, p = 0.001).

When investigating the effect of MISI on PCM, the result unveiled that PCM is significantly and positively affected by perceived information security knowledge (β = 0.421, f^2 = 0.166, p = 0.001), perceived information security

problem-solving (β = 0.127, f^2 = 0.015, p = 0.009), and perceived social competence (β = 0.247, f^2 = 0.060, p = 0.001).

Similarly, investigating the effect of MISI on CPB revealed that CPB is not significantly influenced by perceived information security knowledge (β = 0.024, f^2 = 0.001, p = 0.695), while it is found to be significantly influenced by perceived information security problem-solving (β = 0.187, f^2 = 0.029, p = 0.002) and perceived social competence (β = 0.109, f^2 = 0.009, p = 0.045).

When assessing the moderating role of employee's cybersecurity attitude in moderating the effect of protection motivation on their cybersecurity protective behaviour. The results unveiled that the role of CAT on all the concerned relationships is found insignificant except one association involving employees' self-efficacy and its effect on their behaviour which was insignificant. This implies that the attitude does not play any moderating role over these relationships.

Table 5: Assessment of paths significance

Path	β1	B2	t	P	2.50%	97.50%
R^2	(0.479)					
Effect of MISI on CPB						
PISK -> CPB	0.024	0.028	0.392	0.695	-0.099	0.144
PISP -> CPB	0.187	0.184	3.048	0.002	0.065	0.304
PSC -> CPB	0.109	0.105	2.003	0.045	0.008	0.220
Effect of MISI on PCM						
PISK -> PCM	0.421	0.421	6.81	0.001	0.300	0.541
PISP -> PCM	0.127	0.127	2.155	0.031	0.011	0.243
PSC -> PCM	0.247	0.247	3.738	0.001	0.117	0.377
Effect of PCM on Protection motivation dimensions						
PCM -> SEV	0.634	0.633	14.659	0.001	0.539	0.710
PCM -> SUSC	0.709	0.709	19.696	0.001	0.630	0.771
PCM -> SE	0.46	0.459	10.011	0.001	0.365	0.545
PCM -> RE	0.493	0.493	11.002	0.001	0.400	0.576
PCM -> RC	0.565	0.564	13.517	0.001	0.476	0.639
The effect of Protection motivation dimensions on CPB						
SEV -> CPB	-0.093	-0.09	1.554	0.12	-0.211	0.026
SUSC -> CPB	0.237	0.233	3.868	0.001	0.116	0.356
SE -> CPB	0.079	0.083	1.514	0.13	-0.024	0.179
RE -> CPB	0.241	0.242	4.089	0.001	0.127	0.357
RC -> CPB	-0.076	-0.074	1.382	0.167	-0.181	0.032
The moderating role of CTA on the effect of Protection motivation dimensions on CPB						
CTA x SEV -> CPB	-0.048	-0.038	0.958	0.338	-0.151	0.046
CTA x SUSC -> CPB	0.046	0.038	0.853	0.394	-0.068	0.142
CTA x RE -> CPB	0.01	0.019	0.17	0.865	-0.105	0.115
CTA x SE -> CPB	0.081	0.076	2.036	0.042	0.006	0.163
CTA x RC -> CPB	-0.06	-0.063	1.123	0.261	-0.178	0.033

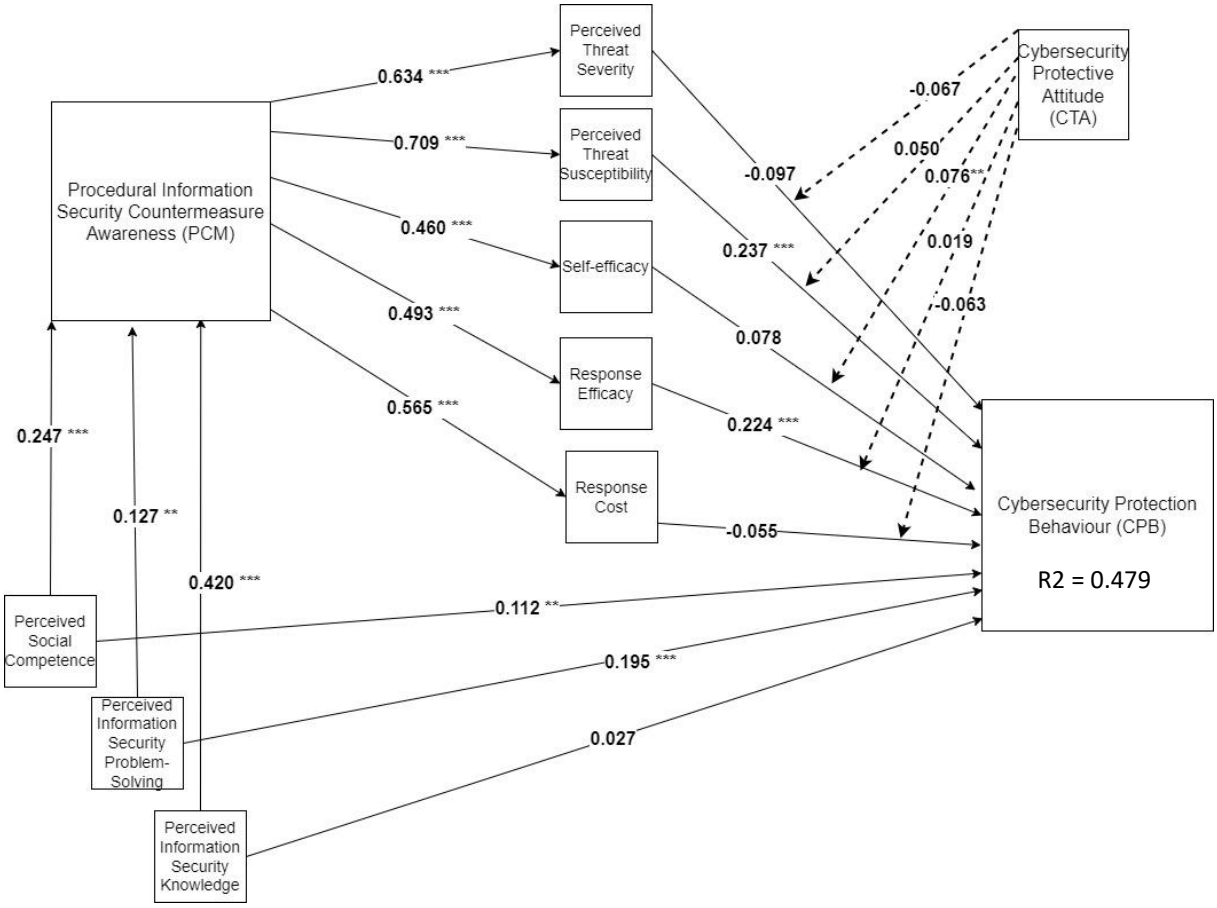

Figure 1: Research model with hypothesis assessment

When considering the explanatory power of the research model, the value of R^2 is assessed for the main dependent variable which is CPB, the value of R^2 is found to be 0.479, which is considered substantial (Cohen, 1988; Chin, 1998; Hair *et al.*, 2010). Further, Applying PLS predict technique to compare the prediction errors between the PLS model and the LM model unveiled that the mean absolute errors (MAE) are less in three of the five indicators of CPB which indicates that the research model has a medium predictive power

5. Discussion

In the current study, the presence of females in the public sector is highlighted (64.6% of respondents), this indicates a high extent of women's participation in the job market and economic development in the UAE context which is a growth supported by the government policies regarding the importance of women's inclusion and empowerment through the public sector (Othman *et al.*, 2025). Furthermore, when it comes to the qualification, only 15.8% of respondents have diplomas lower than a university degree, while 44.8% possess Batchelor's degree and 39.4% possess Masters or PhD qualifications. Similarly, when it comes to work experience, 16% of the respondents indicated having work experience lower than three years. This implies the need to focus on low qualified employees and less experienced employees to ensure they possess the necessary knowledge and awareness of cybersecurity. This highlights the need for publicizing the initiatives such as Salim, Cyber-Pulse which are launched by the government to spread knowledge and awareness about cybersecurity and promoting knowledge-based economy along with supporting the investments in the digital economy and aiming to improve resilience in both the private and public sectors. Additionally, the strategies established for promoting cybersecurity in the country such as the UAE's National Cyber Security Strategy and Dubai Cyber Security Strategy (UAE, 2022).

In the position category, the majority are of higher levels of managerial hierarchy, while 16% of the respondents are entry level employees and 27.1% are mid-level employees. Considering the extent of awareness and adoption of best practice regarding cybersecurity protective behaviour, the improvement of knowledge and experience among this category of employees is considered essential as it is evident that cybersecurity attacks are associated

with the lack of sufficient knowledge and experience in dealing with the digital work environment (Aliebrahimi and Miller, 2023).

When assessing the nature of work environment, the results indicated that 19.4% of respondents already experienced cybersecurity attacks such as losing access to data stored digitally. Further, the majority of respondents (73.8%) indicate that they use mobile systems to perform their work tasks and responsibilities. In this context, almost half of respondents (44.8%) conduct such activities remotely from home. This highlights the importance of maintaining cybersecurity awareness and protective behaviour to promote safety and productivity in the public sector. This can be improved by referring to the relevant policies, strategies and initiatives sponsored in the UAE to ensure employees in such categories are well equipped with the necessary awareness and knowledge allowing them to perform their tasks and responsibilities effectively and safely in such digital work environment (UAE, 2022).

The results indicate that three dimensions of protection motivation (threat severity, self-efficacy and response cost) are not influential on CPB. Previous literature presents that perceived threat severity as an influential factor on behaviour where individuals seek help, take protective actions or choosing to ignore (Chen and Zahedi, 2016). Furthermore, De Kimpe et al. (2022) report that perceived severity is a significant key factor leading the creation of the intention to take protective action. The difference in these results could be attributed to the lack of experiencing the actual threats when it comes to information security and protection. It is expected that the actual knowledge of the security would results in a significantly planned behaviour towards information protection and the opposite occurs when such language is lacked. Regardless of the reported facts that the UAE is ranked the fifth globally when it comes to cyber safety and digital security (UAE, 2022), in addition to that, having good and effective laws and regulation related to maintaining and developing cybersecurity in the country (Othman *et al.*, 2025), efforts are needed to promote the extent of embracing cybersecurity among individuals in corporations to ensure individual and organisational compliance is achieved.

On top of that, self-efficacy significantly influences the behaviour of individuals when it comes to cybersecurity (Edwards, 2015). It affects information security and the behaviour relevant to it (Pizam *et al.*, 2024). Further, self-efficacy is presented as an optimum factor that builds and changes the individual behaviour (Kamboj, Matharu and Shukla, 2024). The inconsistency of this results in the aspect of the current study could be attributed to the status of lacking the sufficient level of training and awareness of the effect of the threats on their personal and organisational performance. Hence, believing that the organisation is the first protector of their information regarding cybersecurity may make them expressing low level of self- efficacy when it comes to protecting their personal information at workplace. The availability of the strategies, initiatives and regulations related to promoting cybersecurity in the public sector in the UAE does not necessarily imply that all employees possess the determination related to utilizing cybersecurity to avoid any relevant threat while working digitally. This also highlights the need of corporation authority to maintain a closer look in monitoring the extent of capabilities and determination among their employees across different categories to ensure that the level of their skills, capabilities and determination is compatible with unpredicted nature of digital work environment.

Response cost is a proven negative contributor to the intention and behaviour regarding information security (Zhang, Zhang and Jiang, 2023). According to Mills, Todorova and Zhang (2024), the high level of response cost triggers the action to use specific tools in the domain of information technology. Gillam and Foster (2020) concluded that perceived response cost is a significant predictor of risky cybersecurity behaviours among employees. Further, the perceived response cost leads to changing the individual behaviour and actions with respect to cybersecurity protection (Woon, Tan and Low, 2005). The absence of its significance in this study could be attributed to the lack of occurrence of the threat as well as the awareness relating the measures to be taken to conquer potential threats in cybersecurity and information protection. Therefore, when the response cost is high or low, it would certainly affect the tendency or behaviour in the organisation towards information protection.

In the same vein, perceived threat susceptibility and response efficacy are found influential on CPB. Fan et al. (2024) stated that the individual threat susceptibility is associated with appropriate online security habits. Safaei and Head (2024) argue that improving the human computer interaction can help in mitigating the threat susceptibility which could contribute towards enhancing the adopted protection behaviour. Further, Ribeiro, Guedes and Cardoso (2024) indicate that the more ability of the individuals with respect to cybersecurity threats, the threat susceptibility gets reduced which implies improving the personal abilities in this aspect.

Mwakatage and Golyama (2024) reported that perceived response efficacy significantly shapes the attitude of the individuals towards action or prevention. According to Mills, Todorova and Zhang (2024), the perception of coping

and response efficacy helps in understanding how to cope effectively towards the threats. Further, Choi et al. (2024) argued that response efficacy is associated with the uptake of actions when it comes to using technology in response to emergencies. According to the theory of protection motivation, appraisal is necessary for threats as well as for the coping abilities and strategies. The UAE public sector has a significant infrastructure with technology and information system which is considered effective in facilitating such evaluation related to the threats and coping strategies (UAE, 2022). Compliance to the national strategies promoting cyber security is considered an essential step towards nurturing protection motivation among employees in the public sector (Al-Kumaim and Alshamsi, 2023). What promotes this motivation among employees is the focus on training and regular monitoring within the organisation to ensure best practices regarding cybersecurity are embraced by them (Al Neaimi and Lutaaya, 2018).

PCM is significantly associated with all the dimensions of cybersecurity protection motivation. This is confirmed in previous research as the literature presents evidence that procedural security countermeasure awareness positively influences protection motivation components, except for self-efficacy (Humaidi and Abdallah Alghazo, 2022). Further, Hassandoust and Techatassanasoontorn (2020) argue that procedural security countermeasure awareness positively affects response efficacy, response efficacy and response cost. This is also confirmed by Oruc, Chowdhury and Gkioulos (2024) who concluded that the lack of awareness leads to the occurrence of many cybersecurity attacks. However, along with lacking the awareness, the lack of policies and practices are also associated with the protection motivation (Sultan, Laias and El Saiti, 2024). In addition to this, Alyami et al. (2024) confirm that gaining education and awareness with respect to information security is considered effective in promoting the tendency in organisation towards cybersecurity protection. This requires regular improvement in the awareness process Shakti and Hidayanto (2024) in order to ensure that the awareness remains at a good level to promote the activities of individuals in organisations towards information security development Indrakusuma and Hidayanto (2024).

In the context of UAE, education and training are considered the major factor to promote encounter measure awareness among individuals regarding cyber security threats and attacks. In the aspect of education, educational institutions in the UAE can play a significant role in shaping the extent of knowledge and awareness among graduates about cybersecurity and the challenges associated with working in a digital work environment. This role can be guided by the national strategies launched to promote cyber security in the country (AlDaajeh *et al.*, 2022). Based on this, graduates could be prepared to be equipped with the necessary knowledge and capabilities that positively contribute to the motivation of employees to adhere to the best practices related to maintaining cyber security and preventing its attacks and managing its challenges (AlDaajeh *et al.*, 2022; UAE, 2022; Aliebrahimi and Miller, 2023).

When it comes to the role of knowledge and awareness in triggering the motive for information protection, knowledge sharing promotes self-efficacy among employees (Islam and Asad, 2024; Islam *et al.*, 2024). Further, knowledge and awareness improve the threat undesirability which is proven to be influential on protection motivation (Mady, Gupta and Warkentin, 2023). Finally, training and education can promote the protection motivation among individuals (Khan *et al.*, 2023).

The three dimensions of Managers' Information Security Intelligence (MISI) have significant and positive effect on the Procedural Information Security Countermeasure Awareness (PCM) of employees. This is consistent with previous literature. The support of management with respect to policy and problem solving can play a significant role towards building information security culture which in turns form the intention and behaviour of individuals towards cybersecurity protection (Tenzin, McGill and Dixon, 2024). Further, the activities of managers with respect to monitoring are helpful regarding solving the challenges that hinder the activities of cybersecurity protection (Ahmadi, 2024).

Alghazo, Humaidi and Noranee (2023) demonstrate that the dimensions of information security competences significantly influence the PCM among individual. The study done by Kim, Hovav and Han, 2019 has reported that perceived information security knowledge (PISK) and perceived information security problem (PISP) solving significantly influences PCM.

Similarly, Kirwan (2008) report that MISI is a significant factor in promoting PCM. However, the literature presents a different point of view when it comes to perceived social competence (PSC) which was found insignificant in affecting PCM (Alghazo, Humaidi and Noranee, 2023).

Therefore, the competencies possessed by managers can play a significant role in their awareness and knowledge related to information security. This implies that the development of the abilities and skills of the managers can

lead to developing their knowledge and awareness measured dedicated for information security. The cybersecurity protective behaviour is not found significantly influenced by perceived information security knowledge which is inconsistent with previous literature due to the lack of the sufficient knowledge and awareness that could have an effect on the protection motivation. The literature presents evidence that the managers abilities regarding knowledge and problem solving are considered influential when it comes to taking actions and behaviour (Korzynski and Protsiuk, 2024; Nguyen *et al.*, 2024).

Improving the capabilities of managers in the digital aspect in the UAE context is essential to avoid the negative effects of cybersecurity threat. When considering the aspect of the organisational that have already experienced cybersecurity attacks, the role of managers skills and capabilities should be considered in a more serious extent due to the role that can be played by utilizing the skills and capabilities among managers in implementing the guidelines and recommendations highlighted in the national strategies and initiatives targeting the promotion of cyber security awareness and best practices associated with maintaining safety and productivity in the public sector (AlDaajeh *et al.*, 2022; UAE, 2022; Aliebrahimi and Miller, 2023).

In addition, the results showed that cybersecurity protective behaviour is found to be significantly and positively influenced by PISP and PSC. The result is in line with previous research (Zwilling *et al.*, 2022; Butera, Dompnier and Darnon, 2024). Previous research indicates that the increase of the PSC leads to increasing the adoption of CPB (Carroll *et al.*, 2020; Özerk, Özerk and Silveira-Zaldivara, 2021; Zwilling *et al.*, 2022). Social competences and social support are significant in promoting the behaviour of individuals (Sinha and Sarkar, 2024). Further, the social competence and social influence are significant in improving the achievement of goals (Butera, Dompnier and Darnon, 2024) which can be applicable in the aspect of information security. According to Zwilling et al. (2022), even though individual possess the knowledge related to cybersecurity, they are found to apply only minimum protection measures which are considered common and simple to use. Furthermore, when employees possess the required knowledge, awareness and competences, their behaviour towards applying the procedures improves (Li *et al.*, 2019).

The moderating effect is unsupported in this study which is inconsistent with previous research. The literature presents evidence that the positive attitude towards cybersecurity leads to less perception of risky behaviour (Hadlington, 2017), which is also associated with adopting certain protective behaviours. This iterates that the change in cybersecurity attitude among the employees does not have an effect in the role played by protection motivation in the behaviour of induvial regarding cybersecurity protection. Expressing attitude towards information security influences the decision of students to protect their privacy on social media (Sales *et al.*, 2024), this is also confirmed by the argument of Baltuttis, Teubner and Adam (2024) that higher attitude affects the decisions towards information security protection is more common with the experience of working with information security domain. When the cybersecurity attitude is low, the association between protection motivation and protection behaviour could be rendered to a low effect association (Lechuga Sancho, Martín-Navarro and Ramos-Rodríguez, 2020; Sun *et al.*, 2022; Koloba and Surtie, 2023).

The enhancement of attitude towards cybersecurity among public sector employees in the UAE context is closely linked to raising awareness and education, particularly within educational institutions. Implementing managerial development programs for the public sector employees can significantly improve their understanding of the country's cybersecurity strategies and policies, encouraging better compliance with practices related to CPB. Additionally, on the job training plays a crucial role in fostering positive attitude among public employees, emphasizing the importance of cybersecurity in maintaining a safe and productive work environment. Research by Al Neaimi, Ranginya and Lutaaya (2015b), Al Shamsi (2019) and Ismail and Alrabaee (2024) supports the view that continuous training and education are essential for promoting strong cybersecurity practices among the employees.

5.1 Research Implication

The study implication is summarised by providing significant evidence for managers and authorities in corporations within the Emirati context by setting strategies and policies that are dedicated to ensuring the protection practices that contribute to the performance improvement among individuals as well as corporations; identifying the chances for improvement when it comes to information security protection; and utilising digital assets of the organisation for better protection. Policymakers can utilise the research outcome to address organisational and individual cybersecurity concerns by incorporating cyber threat severity awareness into a wider and national campaigns to promote security protection. The main rule that can be played by policy makers is to ensure the implementation of the established strategies targeting safer work environment in the public sector through

ensuring the compliance of individuals as well as organisations in the public sector towards having safer and effective work environment in the UAE.

Managers and executive should utilise the research outcome in fostering a culture of continuous learning and improving personal abilities for the purpose of mitigating susceptibility and protective behaviour improvement. Managers can support the development of knowledge and awareness about cybersecurity among themselves and among their employees. The first necessary aspect that can be embraced by public sector managers is to engage in managerial development programs to ensure they are aware of the best practices to maintain security measures to ensure a safe work environment in their administrations. Furthermore, managers can enhance cybersecurity knowledge and awareness among their employees by supervising on-the-job training sessions and programs, particularly for those who lack experience or understanding in dealing with cybersecurity threats.

Finally, policymakers should address organisational and individual cybersecurity concerns by incorporating cyber threat severity awareness into a wider and national campaigns to promote security protection.

When considering knowledge and awareness, educational institutions can play a key role in promoting the knowledge and awareness of the public towards cybersecurity and its importance in maintaining a safe work environment. Universities can utilise the outcome of this research in initiating managerial development programs for the employees in the public sector with the coordination of the relevant public institutions to ensure that the level of knowledge and awareness about cyber security and its threats is well maintained among students, graduates and employees. This is considered effective in improving the caution level among employees in dealing with responsibilities and tasks conducted in digital platforms in the public sector.

Theoretically, this research extends the theoretical understanding of the role played by the skills and abilities of managers in driving both the awareness as well as the behaviour of employees in respect to cyber security. The contribution of this research towards knowledge and theory is summarised by highlighting the role of support, awareness, managers' capabilities and resources in promoting cybersecurity in the public sector within the UAE context. Similarly, the individual' attitude and perception does not emerge as a key contributor towards promoting cybersecurity within the UAE context.

6. Conclusion

The study assessed how protection motivation promotes cybersecurity protective behaviour through measuring the aspect of employees in the public sector in the UAE. The study highlighted that perceived threat severity and perceived threat susceptibility should be improved through actual knowledge and experience to shape individual skills towards enhancing cybersecurity protective behaviour. Moreover, the importance of cybersecurity awareness in promoting protection motivation is highlighted, such awareness can be fostered through utilizing managerial competencies in the organisations. The study highlighted that cybersecurity protective behaviour is dependent on enhancing the managerial capabilities, awareness and motivation among employees towards embracing cybersecurity best practices. Finally, the attitude of employees towards cybersecurity may not be a fundamental driver for employing their motivation towards adopting cybersecurity best practices.

It is concluded that the attention should be focused towards enhancing the knowledge and awareness about information security, along with competences and skills of managers promoting the protection motivation factors and that leads to improving the cybersecurity protective behaviour among employees. The study recommends conducting educational sessions and awareness programs with respect to information security and protection; setting clear strategies as well as objectives related to employee information protection through using optimum tools; and coordinating the effort between the organisations with their employees with the governmental institutions in order to ensure that cybersecurity policies and practices are established.

Regardless of the effort made by the researchers, the study is still limited due to focusing on the listed corporation in Abu Dhabi, hence generalizing the results should take into consideration the shared characteristics; targeting managers and administrative members in such companies which creates a gap for further research to be widened in respect of sample and population. Further research can include organisations beyond the listed companies, further, comparative studies between the public and private sector can bring different insight contributing policy and practice. In addition to this, qualitative research method can be employed to investigate the perspective of managerial experts in organisations about managing cybersecurity attacks.

Acknowledgement

The authors would like to express their sincere gratitude to the Faculty of Business and Management, Universiti Teknologi MARA (UiTM), Selangor, Puncak Alam Campus, for their continuous support and encouragement throughout this study. Further, We would like to thank the anonymous reviewers for their time and effort in enhancing this publication's quality. Finally, we would like to thank employees and administrators in the nine selected companies in the public sector of Abu Dhabi for their time and effort in filling out the study forms.

AI Statement: The authors declare that this work is original content prepared by them and no technology (e.g. AI) was used to generate all or part of its content. Further, the authors declare that this work is not under publication or presentation considerations elsewhere.

Ethics Statement: This study was approved by the Institutional Research Ethics Committee (REC). Informed consent was obtained from all participants.

Conflict of Interest: The authors declare that they have no competing interests.

Data Availability: The datasets generated and analysed during the current study are available in the corresponding author repository.

Funding: This research was self-funded.

References

Abraham, C., Chatterjee, D. and Sims, R.R. (2019) 'Muddling through cybersecurity: Insights from the U.S. healthcare industry', *Business Horizons*, 62(4), pp. 539–548. Available at: https://doi.org/10.1016/j.bushor.2019.03.010.

Adam, S. (2022) *The State of Ransomware 2022 Explore the real-world ransomware experiences of 5,600 IT professionals working at the frontline*. Available at: https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/ (Accessed: 26 February 2025).

Ahmadi, S. (2024) 'Challenges and Solutions in Network Security for Serverless Computing', *International Journal of Current Science Research and Review*, 07(01), pp. 218–229. Available at: https://doi.org/10.47191/ijcsrr/V7-i1-23.

Ahmat, N.N. *et al.* (2024) 'Impact of Digital Transformation on Smart Government in United Arab Emirates: A Review', *International Journal of Academic Research in Business and Social Sciences*, 14(8), pp. 3398–3415. Available at: https://doi.org/10.6007/IJARBSS/v14-i8/22772.

Ahmed Hassan, D.M. and Ismail, A.S. (2022) 'Cybersecurity for UAE Digital Banks Suggested Strategy According to the Terms of the Abu Dhabi Global Market.', *Ajman Journal of Studies & Research*, 21(2).

Al Neaimi, A. and Lutaaya, P. (2018) 'The Role of Culture in the Design of Effective Cybersecurity Training and Awareness Programmes. A Case Study of the United Arab Emirates (UAE)', in, pp. 131–139. Available at: https://doi.org/10.1007/978-3-319-98827-6_11.

Al Neaimi, A., Ranginya, T. and Lutaaya, P. (2015a) 'A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE)', *International Journal of Cyber-Security and Digital Forensics*, 4(1), pp. 290–301.

Al Neaimi, A., Ranginya, T. and Lutaaya, P. (2015b) 'A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE)', *International Journal of Cyber-Security and Digital Forensics*, 4(1), pp. 290–301.

Al Sayegh, A.J. *et al.* (2023) 'Factors affecting e-government adoption in the UAE public sector organisations: the knowledge management perspective', *Journal of Knowledge Management*, 27(3), pp. 717–737. Available at: https://doi.org/10.1108/JKM-09-2021-0681.

Al Shamsi, A.A. (2019) 'Effectiveness of cyber security awareness program for young chiAbdul Hamid, H. *et al.* (2015) 'An Overview of the Management Commitment to Safety Elements for Mitigating Accidents in the Construction Industry', *Jurnal Teknologi*, 74(2), pp. 1–8. Available at: https://doi.org/10.11113/jt.v74.4517.

Alalawi, M.H. (2024) *Enhancing Cybersecurity Awareness in the United Arab Emirates: An Assessment of Current Practices and the Development of an AI-Enhanced Mobile Application*. Masters' Dissertation. United Arab Emirates Unversity.

AlDaajeh, S. *et al.* (2022) 'The role of national cybersecurity strategies on the improvement of cybersecurity education', *Computers & Security*, 119, p. 102754. Available at: https://doi.org/10.1016/j.cose.2022.102754.

Al-Emran, M., Mezhuyev, V. and Kamaludin, A. (2019) 'PLS-SEM in Information Systems Research: A Comprehensive Methodological Reference', in, pp. 644–653. Available at: https://doi.org/10.1007/978-3-319-99010-1_59.

Alghazo, S.H.A., Humaidi, N. and Noranee, S. (2023) 'Assessing Information Security Competencies of Firm Leaders towards Improving Procedural Information Security Countermeasure: Awareness and Cybersecurity Protective Behavior', *Information Management and Business Review*, 15(1 (I) SI), pp. 1–13.

Alhogail, A. (2021) 'Enhancing information security best practices sharing in virtual knowledge communities', *VINE Journal of Information and Knowledge Management Systems*, 51(4), pp. 550–572. Available at: https://doi.org/10.1108/VJIKMS-01-2020-0009.

Aliebrahimi, S. and Miller, E.E. (2023) 'Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles', *Transportation Research Part F: Traffic Psychology and Behaviour*, 96, pp. 82–91. Available at: https://doi.org/10.1016/j.trf.2023.06.010.

Alkhazi, B. *et al.* (2022) 'Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior', *IEEE Access*, 10, pp. 132132–132143. Available at: https://doi.org/10.1109/ACCESS.2022.3230286.

Al-Kumaim, N.H. and Alshamsi, S.K. (2023) 'Determinants of Cyberattack Prevention in UAE Financial Organisations: Assessing the Mediating Role of Cybersecurity Leadership', *Applied Sciences*, 13(10), p. 5839. Available at: https://doi.org/10.3390/app13105839.

Almehairbi, K.M.S.S., Jano, Z. and Mosali, N.A. (2022) 'Structural relationship of technology adoption and performance factors in UAE manufacturing industry', *International Journal of Sustainable Construction Engineering and Technology*, 13(4), pp. 320–337.

Alyami, A. *et al.* (2024) 'Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives', *Information & Computer Security*, 32(1), pp. 53–73. Available at: https://doi.org/10.1108/ICS-08-2022-0133.

An, Q. *et al.* (2023) 'How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates', *International Journal of Information Security*, 22(2), pp. 305–317. Available at: https://doi.org/10.1007/s10207-022-00637-z.

Awareness: Case Study At Financial Institution', *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, 9(2), pp. 172–179.

Baltuttis, D., Teubner, T. and Adam, M.T.P. (2024) 'A typology of cybersecurity behavior among knowledge workers', *Computers & Security*, 140, p. 103741. Available at: https://doi.org/10.1016/j.cose.2024.103741.

Bax, S., McGill, T. and Hobbs, V. (2021) 'Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs', *Computers & Security*, 106, p. 102278.

Bolívar, H.A. and Dallery, J. (2020) 'Effects of response cost magnitude on resurgence of human operant behavior', *Behavioural Processes*, 178, p. 104187. Available at: https://doi.org/10.1016/j.beproc.2020.104187.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009) 'Roles of information security awareness and perceived fairness in information security policy compliance', *AMCIS 2009 proceedings*, p. 419.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS quarterly*, pp. 523–548.

Butera, F., Dompnier, B. and Darnon, C. (2024) 'Achievement Goals: A Social Influence Cycle', *Annual Review of Psychology*, 75(1), pp. 527–554. Available at: https://doi.org/10.1146/annurev-psych-013123-102139.

Campbell, R.J. (2017) 'The smart grid and cybersecurity: Regulatory policy and issues', *Current Politics and Economics of the United States, Canada and Mexico*, 19(2), pp. 169–200.

Carroll, A. *et al.* (2020) 'Who benefits most? Predicting the effectiveness of a social and emotional learning intervention according to children's emotional and behavioural difficulties', *School Psychology International*, 41(3), pp. 197–217. Available at: https://doi.org/10.1177/0143034319898741.

Cepeda, G. *et al.* (2024) 'Emerging opportunities for information systems researchers to expand their PLS-SEM analytical toolbox', *Industrial Management & Data Systems*, 124(6), pp. 2230–2250. Available at: https://doi.org/10.1108/IMDS-08-2023-0580.

Chan, M., Woon, I. and Kankanhalli, A. (2005) 'Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior', *Journal of Information Privacy and Security*, 1(3), pp. 18–41. Available at: https://doi.org/10.1080/15536548.2005.10855772.

Chen, B. *et al.* (2021) 'Cybersecurity of Wide Area Monitoring, Protection, and Control Systems for HVDC Applications', *IEEE Transactions on Power Systems*, 36(1), pp. 592–602. Available at: https://doi.org/10.1109/TPWRS.2020.3022588.

Chen, Y. and Zahedi, F.M. (2016) 'Individuals' internet security perceptions and behaviors', *Mis Quarterly*, 40(1), pp. 205–222.

Chin, W.W. (1998) 'The Partial Least Squares Approach to Structural Equation Modeling', in *Modern Methods for Business Research*. Psychology Press, pp. 295–336.

Choi, S.L. *et al.* (2024) 'Telehealth uptake among middle-aged and older Americans during COVID-19: chronic conditions, social media communication, and race/ethnicity', *Aging & Mental Health*, 28(1), pp. 160–168. Available at: https://doi.org/10.1080/13607863.2022.2149696.

Christian, M.S. *et al.* (2009) 'Workplace safety: A meta-analysis of the roles of person and situation factors.', *Journal of Applied Psychology*, 94(5), pp. 1103–1127. Available at: https://doi.org/10.1037/a0016172.

Clarke, S. (1999) 'Perceptions of organisational safety: implications for the development of safety culture', *Journal of organisational behavior: the international journal of industrial, occupational and organisational psychology and behavior*, 20(2), pp. 185–198.

Cohen, J. (1988) 'Statistical Power Analysis for the Behavioral Sciences, 2nd Edn. Hillsdale, NJ: Erlbaum.'

Cooper, D.P., Goldenberg, J.L. and Arndt, J. (2014) 'Perceived efficacy, conscious fear of death and intentions to tan: Not all fear appeals are created equal', *British Journal of Health Psychology*, 19(1), pp. 1–15. Available at: https://doi.org/10.1111/bjhp.12019.

De Kimpe, L. *et al.* (2022) 'What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context', *Behaviour & Information Technology*, 41(8), pp. 1796–1808. Available at: https://doi.org/10.1080/0144929X.2021.1905066.

de Winter, A.F. *et al.* (2005) 'Evaluation of non-response bias in mental health determinants and outcomes in a large sample of pre-adolescents', *European Journal of Epidemiology*, 20(2), pp. 173–181. Available at: https://doi.org/10.1007/s10654-004-4948-6.

Deraman, N.A. *et al.* (2021) 'Mining social media opinion on online distance learning issues during and after movement control order (MCO) in Malaysia using topic modeling approach', *International Journal of Advanced Technology and Engineering Exploration*, 8(75), pp. 371–381. Available at: https://doi.org/10.19101/IJATEE.2020.762136.

Edwards, K. (2015) *Examining the security awareness, information privacy, and the security behaviors of home computer users*. Nova Southeastern University.

Eid, R., Selim, H. and El-Kassrawy, Y. (2021) 'Understanding citizen intention to use m-government services: an empirical study in the UAE', *Transforming Government: People, Process and Policy*, 15(4), pp. 463–482. Available at: https://doi.org/10.1108/TG-10-2019-0100.

Fan, Z. *et al.* (2024) 'Investigation of Phishing Susceptibility with Explainable Artificial Intelligence', *Future Internet*, 16(1), p. 31. Available at: https://doi.org/10.3390/fi16010031.

Finkelstein, S. (1992) 'Power in top management teams: Dimensions, measurement, and validation', *Academy of Management journal*, 35(3), pp. 505–538.

Fornell, C. and Larcker, D.F. (1981) 'Evaluating Structural Equation Models with Unobservable Variables and Measurement Error', *Journal of Marketing Research*, 18(1), pp. 39–50. Available at: https://doi.org/10.1177/002224378101800104.

Fruhen, L.S. *et al.* (2014a) 'Safety intelligence: An exploration of senior managers' characteristics', *Applied Ergonomics*, 45(4), pp. 967–975. Available at: https://doi.org/10.1016/j.apergo.2013.11.012.

Fruhen, L.S. *et al.* (2014b) 'Skills, knowledge and senior managers' demonstrations of safety commitment', *Safety Science*, 69, pp. 29–36. Available at: https://doi.org/10.1016/j.ssci.2013.08.024.

Gillam, A.R. and Foster, W.T. (2020) 'Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study', *Computers in Human Behavior*, 108, p. 106319. Available at: https://doi.org/10.1016/j.chb.2020.106319.

Guhr, N., Lebek, B. and Breitner, M.H. (2019) 'The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory', *Information Systems Journal*, 29(2), pp. 340–362. Available at: https://doi.org/10.1111/isj.12202.

Haddad, A. *et al.* (2020) 'The impact of technology readiness on the big data adoption among UAE organisations', in *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 2*. Springer, pp. 249–264.

Hadlington, L. (2017) 'Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours', *Heliyon*, 3(7), p. e00346. Available at: https://doi.org/10.1016/j.heliyon.2017.e00346.

Hadlington, L. and Murphy, K. (2018) 'Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors', *Cyberpsychology, Behavior, and Social Networking*, 21(3), pp. 168–172. Available at: https://doi.org/10.1089/cyber.2017.0524.

Hair, J. *et al.* (2017) 'An updated and expanded assessment of PLS-SEM in information systems research', *Industrial Management & Data Systems*, 117(3), pp. 442–458. Available at: https://doi.org/10.1108/IMDS-04-2016-0130.

Hair, J.F. *et al.* (2010) 'Multivariate data analysis: A global perspective (Vol. 7)'. Upper Saddle River, NJ: Pearson.

Hair, J.F. *et al.* (2016) 'A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)'. Sage.

Hair, J.F. *et al.* (2019) 'When to use and how to report the results of PLS-SEM', *European business review*, 31(1), pp. 2–24.

Hair, J.F. *et al.* (2021) *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*. Cham: Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-80519-7.

Hair, J.F., Ringle, C.M. and Sarstedt, M. (2011) 'PLS-SEM: Indeed a Silver Bullet', *Journal of Marketing Theory and Practice*, 19(2), pp. 139–152. Available at: https://doi.org/10.2753/MTP1069-6679190202.

Han, J., Kim, Y.J. and Kim, H. (2017) 'An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective', *Computers & Security*, 66, pp. 52–65. Available at: https://doi.org/10.1016/j.cose.2016.12.016.

Han, J.Y. and Ryu, H.-S. (2016) 'The Effect of Managerial Information Security Intelligence on the Employee's Information Security Countermeasure Awareness', *Information Systems Review*, 18(3), pp. 137–153.

Hasan, S. *et al.* (2021) 'Evaluating the cyber security readiness of organisations and its influence on performance', *Journal of Information Security and Applications*, 58, p. 102726. Available at: https://doi.org/10.1016/j.jisa.2020.102726.

Hassandoust, F. and Techatassanasoontorn, A.A. (2020) 'Understanding users' information security awareness and intentions', in *Cyber Influence and Cognitive Threats*. Elsevier, pp. 129–143. Available at: https://doi.org/10.1016/B978-0-12-819204-7.00007-5.

Herbert, F., Schmidbauer-Wolf, G.M. and Reuter, C. (2020) 'Differences in IT security behavior and knowledge of private users in Germany'.

Hong, Y. and Furnell, S. (2021) 'Understanding cybersecurity behavioral habits: Insights from situational support', *Journal of Information Security and Applications*, 57, p. 102710. Available at: https://doi.org/10.1016/j.jisa.2020.102710.

Hu, Q. *et al.* (2012) 'Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organisational Culture*', *Decision Sciences*, 43(4), pp. 615–660. Available at: https://doi.org/10.1111/j.1540-5915.2012.00361.x.

Hulland, J. (1999) 'Use of partial least squares (PLS) in strategic management research: a review of four recent studies', *Strategic Management Journal*, 20(2), pp. 195–204. Available at: https://doi.org/10.1002/(SICI)1097-0266(199902)20:2<195::AID-SMJ13>3.0.CO;2-7.

Humaidi, N. and Abdallah Alghazo, S.H. (2022) 'Procedural Information Security Countermeasure Awareness and Cybersecurity Protection Motivation in Enhancing Employee's Cybersecurity Protective Behaviour', in *2022 10th*

International Symposium on Digital Forensics and Security (ISDFS). IEEE, pp. 1–10. Available at: https://doi.org/10.1109/ISDFS55398.2022.9800834.

Indrakusuma, K.K.A. and Hidayanto, A.N. (2024) 'Information Security Awareness Analysis on Digital Bank Customer Using Analytic Hierarchy Process: Case Study at XYZ Application from Bank ABC', *Walisongo Journal of Information Technology*, 5(2), pp. 103–128.

Islam, T. and Asad, M. (2024) 'Enhancing employees' creativity through entrepreneurial leadership: can knowledge sharing and creative self-efficacy matter?', *VINE Journal of Information and Knowledge Management Systems*, 54(1), pp. 59–73. Available at: https://doi.org/10.1108/VJIKMS-07-2021-0121.

Islam, T. *et al.* (2024) 'How knowledge sharing encourages innovative work behavior through occupational self-efficacy? The moderating role of entrepreneurial leadership', *Global Knowledge, Memory and Communication*, 73(1/2), pp. 67–83. Available at: https://doi.org/10.1108/GKMC-02-2022-0041.

Ismail, M. and Alrabaee, S. (2024) 'Empowering Future Cyber Defenders: Advancing Cybersecurity Education in Engineering and Computing with Experiential Learning', in *2024 IEEE Frontiers in Education Conference (FIE)*. IEEE, pp. 1–9.

Jang-Jaccard, J. and Nepal, S. (2014) 'A survey of emerging threats in cybersecurity', *Journal of Computer and System Sciences*, 80(5), pp. 973–993. Available at: https://doi.org/10.1016/j.jcss.2014.02.005.

Johnston and Warkentin (2010) 'Fear Appeals and Information Security Behaviors: An Empirical Study', *MIS Quarterly*, 34(3), p. 549. Available at: https://doi.org/10.2307/25750691.

Kamboj, S., Matharu, M. and Shukla, Y. (2024) 'Examining the effect of perceived risk, self-efficacy and individual differences on consumer intention to use contactless mobile payment services', *Journal of Science and Technology Policy Management* [Preprint]. Available at: https://doi.org/10.1108/JSTPM-05-2023-0073.

Kankanhalli, A. *et al.* (2003) 'An integrative study of information systems security effectiveness', *International Journal of Information Management*, 23(2), pp. 139–154. Available at: https://doi.org/10.1016/S0268-4012(02)00105-6.

Khan, N.F. *et al.* (2023) 'Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model', *Computers & Security*, 125, p. 103049. Available at: https://doi.org/10.1016/j.cose.2022.103049.

Khando, K. *et al.* (2021) 'Enhancing employees information security awareness in private and public organisations: A systematic literature review', *Computers & Security*, 106, p. 102267. Available at: https://doi.org/10.1016/j.cose.2021.102267.

Kim, H.L., Hovav, A. and Han, J. (2019) 'Protecting intellectual property from insider threats', *Journal of Intellectual Capital*, 21(2), pp. 181–202. Available at: https://doi.org/10.1108/JIC-05-2019-0096.

Kim, H.-Y. (2013) 'Statistical notes for clinical researchers: assessing normal distribution (2) using skewness and kurtosis', *Restorative dentistry & endodontics*, 38(1), pp. 52–54.

Kirwan, B. (2008) 'From safety culture to safety intelligence', in *Probabilty Safety Assessment and Management Conference, PSAM9*, pp. 18–23.

Knapp, K.J. *et al.* (2006) 'Information security: management's effect on culture and policy', *Information Management & Computer Security*, 14(1), pp. 24–36.

Kock, N. (2017) 'Common Method Bias: A Full Collinearity Assessment Method for PLS-SEM', in *Partial Least Squares Path Modeling*. Cham: Springer International Publishing, pp. 245–257. Available at: https://doi.org/10.1007/978-3-319-64069-3_11.

Koloba, H.A. and Surtie, S.S. (2023) 'Acceptance of Mobile Marketing Amongst Generation Z Students in South Arica: The Moderating Role of Attitude', *Acta Universitatis Danubius. Œconomica*, 19(5), pp. 100–113.

Korzynski, P. and Protsiuk, O. (2024) 'What leads to cyberloafing: the empirical study of workload, self-efficacy, time management skills, and mediating effect of job satisfaction.', *Behaviour & Information Technology*, 43(1), pp. 200–211. Available at: https://doi.org/10.1080/0144929X.2022.2159525.

Lechuga Sancho, M.P., Martín-Navarro, A. and Ramos-Rodríguez, A.R. (2020) 'Will they end up doing what they like? the moderating role of the attitude towards entrepreneurship in the formation of entrepreneurial intentions', *Studies in Higher Education*, 45(2), pp. 416–433. Available at: https://doi.org/10.1080/03075079.2018.1539959.

Li, L. *et al.* (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', *International Journal of Information Management*, 45, pp. 13–24. Available at: https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Li, L., Xu, L. and He, W. (2022) 'The effects of antecedents and mediating factors on cybersecurity protection behavior', *Computers in Human Behavior Reports*, 5, p. 100165. Available at: https://doi.org/10.1016/j.chbr.2021.100165.

Liang, H. *et al.* (2019) 'What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective', *MIS Quarterly*, 43(2), pp. 373–394. Available at: https://doi.org/10.25300/MISQ/2019/14360.

Line, M.B. and Albrechtsen, E. (2016) 'Examining the suitability of industrial safety management approaches for information security incident management', *Information & Computer Security*, 24(1), pp. 20–37. Available at: https://doi.org/10.1108/ICS-01-2015-0003.

Liu, C., Wang, N. and Liang, H. (2020) 'Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organisational commitment', *International Journal of Information Management*, 54, p. 102152. Available at: https://doi.org/10.1016/j.ijinfomgt.2020.102152.

Mabitle, K. and Kritzinger, E. (2021) 'Predicting Schoolteachers' Intention and Behaviour of Promoting Cyber-Safety Awareness', *International Journal of Information and Education Technology*, 11(3), pp. 119–125. Available at: https://doi.org/10.18178/ijiet.2021.11.3.1499.

MacKenzie, S.B. and Podsakoff, P.M. (2012) 'Common Method Bias in Marketing: Causes, Mechanisms, and Procedural Remedies', *Journal of Retailing*, 88(4), pp. 542–555. Available at: https://doi.org/10.1016/j.jretai.2012.08.001.

Mady, A., Gupta, S. and Warkentin, M. (2023) 'The effects of knowledge mechanisms on employees' information security threat construal', *Information Systems Journal*, 33(4), pp. 790–841. Available at: https://doi.org/10.1111/isj.12424.

Mashiane, T. and Kritzinger, E. (2021) 'IDENTIFYING BEHAVIORAL CONSTRUCTS IN RELATION TO USER CYBERSECURITY BEHAVIOR', *EURASIAN JOURNAL OF SOCIAL SCIENCES*, 9(2), pp. 98–122. Available at: https://doi.org/10.15604/ejss.2021.09.02.004.

Miller, B.K. and Simmering, M.J. (2023) 'Attitude Toward the Color Blue: An Ideal Marker Variable', *Organisational Research Methods*, 26(3), pp. 409–440. Available at: https://doi.org/10.1177/10944281221075361.

Mills, A., Todorova, N. and Zhang, J. (2024) 'The role of threat and coping appraisals in motivating the use of personalised mobile emergency alert systems', *Information Technology & People* [Preprint]. Available at: https://doi.org/10.1108/ITP-04-2021-0297.

Mohammed, I.A. (2019) 'Cloud identity and access management–a model proposal', *International Journal of Innovations in Engineering Research and Technology*, 6(10), pp. 1–8.

Mousavi, R. *et al.* (2020) 'Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory', *Decision Support Systems*, 135, p. 113323. Available at: https://doi.org/10.1016/j.dss.2020.113323.

Mwakatage, B. and Golyama, B. (2024) 'Examining the Role of Attitudinal Factors in Shaping Fire Prevention Intentions: A Study of Response Efficacy in Public Markets of Tanzania', *South Asian Journal of Social Studies and Economics*, 21(1), pp. 10–20.

Nguyen, N.N. *et al.* (2024) 'Examining effects of students' innovative behaviour and problem-solving skills on crisis management self-efficacy: Policy implications for higher education', *Policy Futures in Education*, 22(1), pp. 1–20. Available at: https://doi.org/10.1177/14782103221133892.

Ocasio, W. and Joseph, J. (2018) 'The Attention-Based View of *Great* Strategies', *Strategy Science*, 3(1), pp. 289–294. Available at: https://doi.org/10.1287/stsc.2017.0042.

Oppong, R.F. and Zhau, W. (2020) 'The Influence Of Competence On Performance With Motivation As An Intervening Variable On Medical Employees In America Public Service Department', *Medalion Journal: Medical Research, Nursing, Health and Midwife Participation*, 1(2), pp. 63–70.

Oruc, A., Chowdhury, N. and Gkioulos, V. (2024) 'A modular cyber security training programme for the maritime domain', *International Journal of Information Security*, 23(2), pp. 1477–1512. Available at: https://doi.org/10.1007/s10207-023-00799-4.

Othman, S.N. *et al.* (2025) 'The impact of cybersecurity law in the middle east', *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, (23), pp. 392–420.

Özerk, G., Özerk, K. and Silveira-Zaldivara, T. (2021) 'Developing Social Skills and Social Competence in Children with Autism', *International Electronic Journal of Elementary Education*, 13(3), pp. 341–363. Available at: https://doi.org/10.26822/iejee.2021.195.

Parsons, K. *et al.* (2017) 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies', *Computers & Security*, 66, pp. 40–51. Available at: https://doi.org/10.1016/j.cose.2017.01.004.

Pizam, A. *et al.* (2024) 'The role of perceived risk and information security on customers' acceptance of service robots in the hotel industry', *International Journal of Hospitality Management*, 117, p. 103641. Available at: https://doi.org/10.1016/j.ijhm.2023.103641.

Prabhu, S. and Thompson, N. (2022) 'A primer on insider threats in cybersecurity', *Information Security Journal: A Global Perspective*, 31(5), pp. 602–611. Available at: https://doi.org/10.1080/19393555.2021.1971802.

Qiu, D. *et al.* (2023) 'The role of response efficacy and self-efficacy in disaster preparedness actions for vulnerable households', *Natural Hazards and Earth System Sciences*, 23(12), pp. 3789–3803. Available at: https://doi.org/10.5194/nhess-23-3789-2023.

Rainear, A.M. and Christensen, J.L. (2022) 'Examining Pre-existing Environmental Beliefs: Using a PSA to Investigate the Role of Self-Efficacy and Response Efficacy on Behavioral Intentions', *Communication Studies*, 73(2), pp. 151–170. Available at: https://doi.org/10.1080/10510974.2022.2026426.

Renaud, K. and Dupuis, M. (2019) 'Cyber security fear appeals', in *Proceedings of the New Security Paradigms Workshop*. New York, NY, USA: ACM, pp. 42–56. Available at: https://doi.org/10.1145/3368860.3368864.

Ribeiro, L., Guedes, I.S. and Cardoso, C.S. (2024) 'Which factors predict susceptibility to phishing? An empirical study', *Computers & Security*, 136, p. 103558. Available at: https://doi.org/10.1016/j.cose.2023.103558.

Rogers, R.W. (1975) 'A Protection Motivation Theory of Fear Appeals and Attitude Change1', *The Journal of Psychology*, 91(1), pp. 93–114. Available at: https://doi.org/10.1080/00223980.1975.9915803.

Rouse, A. and Corbitt, B. (2008) 'There's SEM and "SEM": A Critique of the Use of PLS Regression in Information Systems Research', in *19th Australasian Conference on Information Systems*. Christchurch, pp. 845–855.

Ruiter, R.A.C., Abraham, C. and Kok, G. (2001) 'Scary warnings and rational precautions: A review of the psychology of fear appeals', *Psychology & Health*, 16(6), pp. 613–630. Available at: https://doi.org/10.1080/08870440108405863.

Sabol, M. *et al.* (2023) 'PLS-SEM in information systems: seizing the opportunity and marching ahead full speed to adopt methodological updates', *Industrial Management & Data Systems*, 123(12), pp. 2997–3017. Available at: https://doi.org/10.1108/IMDS-07-2023-0429.

Safa, N.S. *et al.* (2015) 'Information security conscious care behaviour formation in organisations', *Computers & Security*, 53, pp. 65–78. Available at: https://doi.org/10.1016/j.cose.2015.05.012.

Safaei, B. and Head, M. (2024) 'Investigating Age-Related Factors in Phishing Susceptibility: A Focus on Decision-Making Processes in HCI Context'.

Sales, J.N. *et al.* (2024) 'Personal Privacy and Cyber Security: Student Attitudes, Awareness, and Perception on the Use of Social Media: Student Attitudes, Awareness, and Perception on the Use of Social Media', *International Journal of Curriculum and Instruction*, 16(1), pp. 175–190.

Shaban, A.I., Farhan, M.A. and Ahmed, S.R. (2022) 'Building a Smart System for Preservation of Government Records in Digital Form', in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, pp. 1–6. Available at: https://doi.org/10.1109/HORA55278.2022.9800034.

Shakti, F.N. and Hidayanto, A.N. (2024) 'Measurement Of Employee Information Securityldren: A case study in UAE', *Int. J. Inf. Technol. Lang. Stud*, 3(2), pp. 8–29.

Shillair, R.J. (2018) *Mind the Gap: Perceived Self-Efficacy, Domain Knowledge and Their Effects on Responses to a Cybersecurity Compliance Message*. Michigan State University.

Simonet, J. and Teufel, S. (2019) 'The Influence of Organisational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users', in, pp. 194–208. Available at: https://doi.org/10.1007/978-3-030-22312-0_14.

Sinha, A. and Sarkar, R. (2024) 'Social Influence on Management Education in Contemporary India', in *Managing India*. London: Routledge India, pp. 32–47. Available at: https://doi.org/10.4324/9781032724461-4.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information & Management*, 51(2), pp. 217–224. Available at: https://doi.org/10.1016/j.im.2013.08.006.

SOCRadar (2022) *Threat Landscape Report United Arab Emirates*. Available at: https://socradar.io/wp-content/uploads/2024/10/SOCRadar-UAE-Threat-Landscape-Report-2022.pdf (Accessed: 26 February 2025).

Spagnoletti, P. and Resca, A. (2008) 'The duality of Information Security Management: fighting against predictable and unpredictable threats', *Journal of Information System Security*, 4(3), pp. 46–62.

Sultan, A., Laias, E. and El Saiti, A. (2024) 'Investigating Practices of Information Security Awareness: Perspectives from Government Entities in Libya', *International Journal of Computer Applications*, 186(1), pp. 9–15.

Sun, T. *et al.* (2022) 'Association Between Self-Perceived Stigma and Quality of Life Among Urban Chinese Older Adults: The Moderating Role of Attitude Toward Own Aging and Traditionality', *Frontiers in Public Health*, 10. Available at: https://doi.org/10.3389/fpubh.2022.767255.

Szczepańska-Woszczyna, K. and Gatnar, S. (2022) 'Key competences of research and development project managers in high technology sector', in *Forum Scientiae Oeconomia*, pp. 107–130.

Taufan, M.Y. and Basalamah, A. (2021) 'Implementation of teacher social competence in improving student learning motivation', *Golden Ratio of Social Science and Education*, 1(1), pp. 25–36.

Tenzin, S., McGill, T. and Dixon, M. (2024) 'An Investigation of the Factors That Influence Information Security Culture in Government Organisations in Bhutan', *Journal of Global Information Technology Management*, 27(1), pp. 37–62. Available at: https://doi.org/10.1080/1097198X.2023.2297634.

Thrasher, J.F. *et al.* (2016) 'Influences of Self-Efficacy, Response Efficacy, and Reactance on Responses to Cigarette Health Warnings: A Longitudinal Study of Adult Smokers in Australia and Canada', *Health Communication*, 31(12), pp. 1517–1526. Available at: https://doi.org/10.1080/10410236.2015.1089456.

Tubaishat, A. and AlAleeli, H. (2024) 'A Framework to Prevent Cybercrime in the UAE', *Procedia Computer Science*, 238, pp. 558–565. Available at: https://doi.org/10.1016/j.procs.2024.06.060.

UAE (2022) *Cyber safety and digital security*. Available at: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security (Accessed: 26 February 2025).

Vahdat, S. (2022) 'The role of IT-based technologies on the management of human resources in the COVID-19 era', *Kybernetes*, 51(6), pp. 2065–2088. Available at: https://doi.org/10.1108/K-04-2021-0333.

Van Niekerk, B. (2018) 'The Cybersecurity Dilemma: considerations for investigations in the Dark Web', *Acta Criminologica: African Journal of Criminology & Victimology*, 31(3), pp. 132–148.

Vance, A., Siponen, M. and Pahnila, S. (2012) 'Motivating IS security compliance: Insights from Habit and Protection Motivation Theory', *Information & Management*, 49(3–4), pp. 190–198. Available at: https://doi.org/10.1016/j.im.2012.04.002.

Verkijika, S.F. (2020) 'Employees' Cybersecurity Behaviour in the Mobile Context: The Role of Self-Efficacy and Psychological Ownership', in *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. IEEE, pp. 1–5. Available at: https://doi.org/10.1109/IMITEC50163.2020.9334097.

Whitman, M.E. and Mattord, H.J. (2019) *Management of information security*. Cengage Learning.

Woon, I., Tan, G.-W. and Low, R. (2005) 'A protection motivation theory approach to home wireless security'.

Y. Connolly, L. and Wall, D.S. (2019) 'The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures', *Computers & Security*, 87, p. 101568. Available at: https://doi.org/10.1016/j.cose.2019.101568.

Yeng, P.K., Fauzi, M.A. and Yang, B. (2022) 'A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals', *Information*, 13(7), p. 335. Available at: https://doi.org/10.3390/info13070335.

Yoon, J., Arik, S. and Pfister, T. (2020) 'Data valuation using reinforcement learning', in *International Conference on Machine Learning*. PMLR, pp. 10842–10851.

Younies, H. and Al-Tawil, T.N. (2020) 'Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)', *Journal of Financial Crime*, 27(4), pp. 1089–1105. Available at: https://doi.org/10.1108/JFC-04-2020-0055.

Zainal, N.C., Puad, M.H.M. and Sani, N.F.M. (2021) 'Moderating effect of self-efficacy in the relationship between knowledge, attitude and environment behavior of cybersecurity awareness', *Asian Social Science*, 18(1), p. 55.

Zajdel, M. and Helgeson, V.S. (2020) 'Communal coping: A multi-method approach with links to relationships and health', *Journal of Social and Personal Relationships*, 37(5), pp. 1700–1721. Available at: https://doi.org/10.1177/0265407520903811.

Zhang, H., Zhang, S. and Jiang, X. (2023) 'Response efficiency optimisation of data cube online analysis for network user's behaviour', *International Journal of Autonomous and Adaptive Communications Systems*, 16(3), pp. 270–283. Available at: https://doi.org/10.1504/IJAACS.2023.131623.

Zhang, X. *et al.* (2017) 'User acceptance of mobile health services from users' perspectives: The role of self-efficacy and response-efficacy in technology acceptance', *Informatics for Health and Social Care*, 42(2), pp. 194–206. Available at: https://doi.org/10.1080/17538157.2016.1200053.

Zwilling, M. *et al.* (2022) 'Cyber Security Awareness, Knowledge and Behavior: A Comparative Study', *Journal of Computer Information Systems*, 62(1), pp. 82–97. Available at: https://doi.org/10.1080/08874417.2020.1712269.

Żywiołek, J. and Schiavone, F. (2021) 'The Value of data sets in Information and Knowledge Management as a Threat to Information Security', *Garcia-Perez, Alexeis*, pp. 882–891.

Appendix 1: Table

Managers' Information Security Intelligence Skills (MISI) - Adapted from (Kim et al., 2019).		
Perceived Information Security Knowledge		
PISK	PISK1	Senior managers of my company know about information security.
	PISK2	Senior managers of my company understand information security issues.
	PISK3	Senior managers of my company are trained in information security.
	PISK4	Senior managers of my company understand information security management.
	PISK5	Senior managers of my company understand information security impacts.
Perceived Social Competence		
PSC	PSC1	Senior managers of my company operate an open-door policy.
	PSC2	Senior managers of my company ask their employees questions.
	PSC3	Senior managers of my company have good communication skills.
	PSC4	Senior managers of my company capture all views.
	PSC5	Senior managers of my company engage people at the floor level.
Perceived Information Security Problem-Solving		
PISP	PISP1	Senior managers of my company maintain a balance between information security management and its costs.
	PISP2	Senior managers of my company make decisions regarding the company's information security after consultation.
	PISP3	Senior managers of my company are ready to understand information security problems.
	PISP4	Senior managers of my company make informed decisions about information security problems.
Global	GI	Overall, senior managers of my company have a good information security skills
Procedural Information Security Countermeasure Awareness (PCM) - Adapted from (Simonet & Teufel, 2019)		
PCM	PCM1	I recognize that safe security practices are needed to deal with cybersecurity threats and risks.
	PCM2	I understand that following safe security practices are essential to protect my firm against cyberattacks.

	PCM3	I have the knowledge and capability to recognize and respond to cybersecurity threats and risks.
	PCM4	I am mindful of the cybersecurity threats and risks I face when doing my job.
	PCM5	I recognize that I have to take security protection measures to protect my firm's information assets against cyberattacks.
Cybersecurity Protective Attitude (CTA) – Adapted from (Hadlington, 2017)		
CTA	CTA1	I think that management have the responsibility to ensure a company is protected from cyber crime.
	CTA2	I am aware of my role in keeping the company protected from potential cyber criminals.
	CTA3	I believe everyone in the company has a role to play in protecting against threats from cyber criminals.
	CTA4	I can help protect the organisation from cyber crime.
	CTA5	I have the right skills to be able to protect the organisation from cyber crime.
Cybersecurity Protection Motivation (CPM) – Adapted from (Mousavia et al, 2020)		
Threat Severity		
SEV	SEV1	If my information released to unauthorized people, it would be very bad for me.
	SEV2	If my information released to unauthorized people, it would be a serious danger.
	SEV3	If my information released to unauthorized people, it would be significant danger.
	SEV4	If my information be available to unauthorized users, it would be risky.
Threat Susceptibility		
SUSC	SUSC1	My information is at risk for being released to unauthorized people.
	SUSC2	It is likely that my information will become available to unauthorized people.
	SUSC3	It is possible that my Information will become available to unauthorized people.
	SUSC4	It is likely that others get access to my information without my permission.
	SUSC5	It is probable that others get access to my information without my permission.
Self-efficacy		
SE	SE1	It is easy for me to use privacy assurance mechanisms.
	SE2	It is convenient for me to use privacy assurance mechanisms.
	SE3	I am able to use privacy assurance mechanisms without much effort.
Response Efficacy		
RE	RE1	Complying with the information security policies in my organisation will keep security breaches down.
	RE2	If I comply with information security policies, the chance of information security breaches occurring will be reduced.
	RE3	Careful compliance with information security policies helps to avoid security problems.
Response Cost		
RC	RC1	It is inconvenient to check the security of an email with attachments.
	RC2	Changing the privacy setting on social media sites is inconvenient.
	RC3	Backing up a computer regularly is inconvenient.

Cybersecurity Protective Behaviour (CPB) – Adapted from (Li et al, 2019)		
CPB	CPB1	I keep the anti-virus software on my computer up-to-date.
	CPB2	I watch for unusual computer behaviours/responses (e.g., computer slowing down or freezing up, pop-up windows, etc).
	CPB3	I always act on any malware alerts that I receive.
	CPB4	It is inconvenient to check the security of an email with attachments.
	CPB5	Changing the privacy setting on social media sites is inconvenient.

