# Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia

Siti Fatiha Abd Latif, Noor Suhana Sulaiman, Nur Sukinah Abd Aziz, Azliza Yacob, Akhyari Nasir
Faculty Computer, Media and Technology Management, University College TATI, Malaysia

***Abstract*—This study aims to examine the complex interplay among perceived threat severity, perceived threat vulnerability, fear, perceived response efficacy, perceived self-efficacy, and response cost using Partial Least Squares Structural Equation Modelling (PLS-SEM) via SmartPLS 4.0, grounded in the Protection Motivation Theory (PMT). The analysis is situated within the context of cyber security and information security in Industry Revolution 4.0 (IR 4.0) environments, where interconnected systems are increasingly exposed to cyber threats. Both measurement and structural model assessments were performed, revealing strong indicator loadings, high Cronbach's alpha, composite reliability (CR), and adequate average variance extracted (AVE), confirming the model's reliability and validity. The Fornell-Larcker criterion and heterotrait-monotrait (HTMT) ratio confirmed discriminant validity, while variance inflation factor (VIF) values under 5 and an $R^2$ value of 0.554 indicated no collinearity issues and moderate explanatory power in the structural model. Findings demonstrate that perceived threat severity and vulnerability significantly increased fear, which mediated the threat perception-protection motivation relationship, emphasising the role of emotional responses in decision-making. Coping appraisal components, namely perceived response efficacy and self-efficacy, were strong positive predictors of protection motivation, while response cost negatively influenced protective behaviour intentions. Although intrusion detection systems are essential in mitigating cyber risks, this study highlights the equally critical behavioural component of cyber defence. The outcomes underscore the value of PMT in modelling security behaviour, offering theoretical and practical implications for behavioural interventions, public health strategies, and policy design in IR 4.0 domains. These insights contribute to strengthening cybersecurity and information security culture across digitally-driven industries.**

***Keywords*—Cyber security; information security; intrusion detection; IR 4.0; PLS SEM***

## I. Introduction

The rapid integration of smart devices, artificial intelligence (AI), internet of things (IoT), and big data analytics has led to the emergence of the Fourth Industrial Revolution (IR 4.0). Unprecedented improvements in productivity and decision-making processes have occurred with increased operational efficiency, connectivity, and automation using digital technologies [1]. Nonetheless, the interconnectedness of Industry 4.0 technologies exposes them to cyber threats [2,3]. Digitally-driven companies must increase their employees' cybersecurity awareness and apply viable solutions that address data breaches, cyber-attacks, and system disruptions [4].

Employees in Industry 4.0 environments are responsible for protecting their organisations from cybersecurity breaches via increased cybersecurity awareness and vigilance against cyber threats [5]. Nevertheless, human errors, low awareness, or negligence adversely affect security technologies and cybersecurity despite its sophistication [6]. These cyber incidents call for robust training and awareness programs [7] that educate employees on threat identification, safe data handling, and proactive security measures to establish a strong cybersecurity culture. Cyber security has become a fundamental pillar in safeguarding digital infrastructures within IR 4.0 environments, where interconnected devices increase exposure to cyber threats. Meanwhile, advanced Intrusion Detection Systems (IDS) play a vital role in proactively identifying unauthorised access and potential breaches within Industry 4.0 networks. Intrusion detection mechanisms can complement awareness models by offering real-time monitoring that supports rapid incident response. Information security practices must evolve in tandem with technological advancements to ensure the confidentiality, integrity, and availability of organisational data in smart ecosystems. Ensuring robust information security is critical for maintaining stakeholder trust and business continuity in digitally integrated enterprises.

## II. Protection Motivation Theory

The Protection Motivation Theory (PMT) posits that people assess threats based on perceived severity, vulnerability, response efficacy, and self-efficacy. This psychological framework clearly depicts an individual's motivations to adopt protective cybersecurity behaviours [8]. Companies designing targeted interventions could apply this theory to cybersecurity awareness to inform employees on cyber threats and promote responsible security practices. Studies on the applicability of PMT-based cybersecurity awareness models in Industry 4.0 remain underexplored despite their potential advantages [9]. This knowledge gap necessitates in-depth examination of how PMT constructs can address cybersecurity challenges in digitally-driven industries.

This research proposed a cybersecurity awareness model designed for digital IR 4.0 based on PMT principles to bridge the existing gap. Specifically, the PMT framework and constructs were analysed within existing cybersecurity awareness models. A customised cybersecurity awareness model was developed and evaluated to determine its effectiveness in improving cybersecurity practices among Industry 4.0 employees. Hence, the study enriches the ongoing

discourse on cybersecurity resilience in digital industries and informs industry stakeholders on the importance of securing their data and operations from emerging cyber threats.

Rogers initially developed PMT in 1975 to explain how individuals respond to perceived threats in terms of health behaviour. This framework has since been extended to cybersecurity, environmental behaviour, and organisational safety domains [10]. In theory, people are driven to protect themselves based on their assessment of threats and the coping mechanisms adopted. Two core cognitive processes, known as threat and coping appraisal, underpin the PMT model [11-13]. People are driven to safeguard themselves against a threat, depending on their perceived severity and capability of addressing it.

Threat appraisal involves the evaluation of the seriousness of the threat and likelihood of experiencing the threat, while perceived threat severity denotes the extent to which a threat is perceived to be serious or harmful [14]. The motivation to self-protect increases if the implications are severe (getting diagnosed with a disease or falling prey to a cyberattack). Meanwhile, perceived threat vulnerability implies an individual's assessment of their susceptibility to a threat. Highly vulnerable individuals are more inclined to adopt protective behaviours. Coping appraisal evaluates an individual's ability to prevent a threat, including the effectiveness of those actions and their own self-efficacy [15]. Response efficacy denotes an individual's belief on the effectiveness of the recommended protective behaviours or action in mitigating a threat. People who believe their actions to be successful (installing antivirus software to prevent a cyberattack) would take measures to actualise them. Self-efficacy is an individual's confidence in his or her ability to perform protective behaviours. Those who believe in their ability to successfully execute the action are more likely to do so. Figure 1 depicts the PMT model.

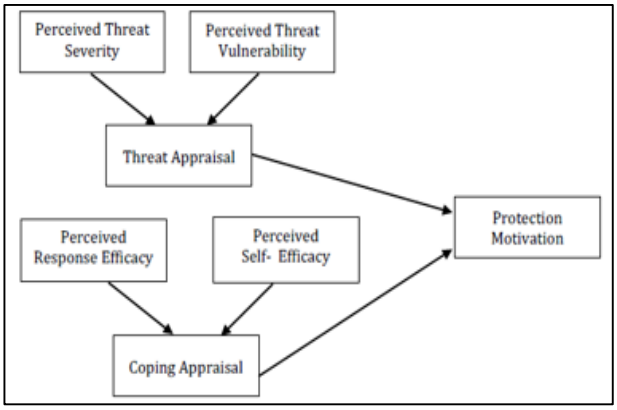


Fig. 1. Protection motivation theory.

Technological advancements via IoT, AI, big data, and cloud computing have led to the emergence of cybersecurity threats [16]. As such, the PMT framework is key to internalising and influencing cybersecurity behaviours in the context of Industry 4.0. Threat appraisal in cybersecurity involves the evaluation of cyber threat severity and likelihood [17-20]. Employees who perceive the potential consequences of a data breach as highly damaging are more inclined to comply with cybersecurity protocols [19]. Likewise, those who believe they are highly vulnerable to cyber threats would adopt protective measures akin to strong password practices and multi-factor authentication [20-21].

Coping appraisal is equally critical in cybersecurity. Perceived response efficacy implies the belief that specific security measures (encryption, regular software updates, and secure network configurations) effectively minimise cyber risks [4,7]. People who trust that these measures can ensure protection against threats would be motivated to implement them. As one's confidence in executing cybersecurity practices (like identifying phishing attempts or managing security settings) increases the likelihood of proactive behaviours, self-efficacy plays a pivotal role in this context [9]. In contrast, high response costs involving perceived complexity, time consumption, or inconvenience of security protocols can prevent individuals from adopting protective actions.

The integration of emotional factors (fear) significantly elevates PMT's explanatory power in cybersecurity. While fear of personal or organisational consequences from cyberattacks can ensure compliance with guidelines, excessive fear without adequate coping mechanisms can instigate avoidance behaviours. This scenario calls for comprehensive cybersecurity training programs [22]. Companies should design interventions that increase their employees' cybersecurity, awareness, self-efficacy, and effectiveness in executing protective measures to establish a resilient cybersecurity culture in Industry 4.0 [23].

## III. Methodology

The research design, population and sample selection, data collection methods, and analysis techniques are presented in this section. Building on PMT, the current work proposed a cybersecurity awareness model designed for digital IR 4.0 by leveraging PMT constructs.

This section also details the population and sample selection process. A diverse and representative group of participants were chosen in this study to increase the outcome generalisability. Empirical data were gathered using a structured questionnaire containing validated PMT constructs to measure key variables of threat appraisal, coping appraisal, self-efficacy, and response efficacy. Furthermore, statistical techniques were used to analyse the correlations between the PMT constructs and cybersecurity awareness behaviours.

A comprehensive model was developed to increase cybersecurity awareness and support regulatory interventions that minimise cyber risks. The insights gained from this research can assist organisations in developing strategies that strengthen their overall security position in digital IR 4.0 and foster a culture of cybersecurity awareness.

### *A. Research Design*

A cross-sectional survey design was employed to systematically collect data on the various factors associated with cybersecurity awareness among digital IR 4.0 employees. This design, which facilitates data collection at a single point in time, proved suitable for examining participants' awareness levels and their perceptions of cybersecurity threats and responses following the research objectives.

The relationships between the PMT constructs were statistically analysed in this study. A structured questionnaire served to gather analyse numerical data via SmartPLS, which facilitates the simultaneous assessment of measurement and structural relationships [24]. Furthermore, SmartPLS offers multiple bootstrapping options to assess the significance of path coefficients and delineate the proposed model correlations.

The survey design was selected to obtain large-scale data from a diverse participant pool and draw meaningful conclusions about the outcome generalisability. A representative sample from various IR 4.0 sectors was chosen to capture a wide range of experiences and perspectives regarding cybersecurity practices. The survey instrument contained validated scales measuring each PMT construct, thus ensuring reliability and validity in the assessment of participants' attitudes and behaviours toward cybersecurity.

Potential associations and patterns among the PMT constructs and cybersecurity awareness were analysed via SmartPLS to determine how perceived threats (threat appraisal) correlate with the ability (self-efficacy) to address them and the perceived effectiveness of their responses (response efficacy).

### B. Specific Research Design

Descriptive and evaluative designs were used in this study. The key PMT constructs in current cybersecurity awareness models were identified and analysed with the descriptive approach [24] to understand the core components of PMT and their role in cybersecurity models based on research question 1.

A structured model development process was applied based on PMT to identify and integrate key PMT constructs into a framework tailored to cybersecurity challenges in digital IR 4.0 environments in Malaysia based on research question 2 [25].

Meanwhile, the proposed model effectiveness was evaluated using the evaluative component to increase cybersecurity awareness in line with research question 3. The recommended model was evaluated based on its ability to improve participants' awareness. Consequently, a survey-based approach served to elicited data on awareness levels pre- and post-exposure to the model. Statistical analyses were performed to quantify model effectiveness and facilitate objective assessment.

### C. Sample and Population

The study population entailed the individuals working in digital IR 4.0-driven companies in Malaysia, including i) cybersecurity experts, ii) IT personnel, and iii) general employees. The first group consists of professionals who are responsible for safeguarding organisational information systems, implementing security strategies, and addressing cyber threats; the second group comprises of employees who are accountable for managing digital infrastructure, ensuring system stability, and implementing security protocols; and the third group encompasses non-technical staff who are responsible for interacting with IR 4.0 technologies and adhering to security policies. The Partial Least Squares Structural Equation Modelling (PLS-SEM) technique was employed to evaluate the hypothesised relationships among PMT constructs and cyber security awareness behaviours.

## IV. Data Collection Methods

This quantitative study used an online survey questionnaire adapted from past research. The PMT constructs relevant to cybersecurity awareness were assessed in this questionnaire.

### A. Content Validity

Five cybersecurity experts reviewed the survey questionnaire for clarity, relevance, and alignment with the study objectives. Content validity ensures that the instrument measures what it is intended to. Their expertise allows for the accurate representation of the study constructs.

### B. Pilot Testing

A pilot test involving 30 respondents was conducted to determine instrument reliability and usability. Internal consistency was confirmed using reliability analysis, while the PMT constructs' effectiveness was ascertained through Cronbach's alpha.

### C. Actual Study of Data Collection

The finalised questionnaire was administered online to 255 respondents across IR 4.0 companies in Malaysia. The elicited data were analysed using SmartPLS to examine relationships between PMT constructs and cybersecurity awareness.

### D. Sample Size Determination

Power analysis was performed using G*Power 3.1 to determine the minimum sample size for the study. A medium effect size ($f^2 = 0.15$), significance level ($\alpha = 0.05$), and statistical power ($1-\beta = 0.80$) generated a sample size of 98. In this study, the sample size of 225 proved sufficient to ensure statistical power for multiple regression analysis.

This research examined cybersecurity awareness using PMT in digital IR 4.0 environments using a structured approach. The cross-sectional nature of the study, validated instruments, and rigorous statistical analysis potentially contribute key insights into enhancing cybersecurity practices and resilience in IR 4.0-driven companies.

## V. Results and Discussion

The respondents' demographic profiles were categorised based on age, gender, organisation/university, race, department/division/unit, education level, and years of experience. Most of the respondents (47.5%) were between 25 and 30 years old, followed by those between 31 and 35 years old (32.9%), below 25 years old (6.3%), and more than 35 years old (13.3%). Regarding gender, 51.0% of the respondents were female, with the remaining 49.0% being male. This finding represents a fairly balanced age distribution.

In terms of organisation/university affiliation, the respondents were employed from a diverse range of industries. A significant proportion of the workers (9.4%) were from Consumer Goods and Retail, followed by Dell Malaysia (8.6%), Fusionex (8.2%), Tenaga Nasional Berhad (TNB) (8.2%), Opcom Holdings Berhad (7.1%), and Vitrox Corporation Berhad (7.5%). Other companies revealed smaller representations, with some contributing under 1% each.

Concerning race, Chinese respondents constituted the largest group (44.7%), followed by Malay (32.5%), and Indian (22.7%).

The respondents were also distributed across various departments, with the highest representation in administration (20.4%), followed by accounts (18.1%), marketing (15.7%), and human resources (13.7%). Other departments such as finance (8.6%) and content creation/creative (6.7%) also demonstrated notable participation. Meanwhile, specialised units resembling cybersecurity, environment, and procurement revealed minimal representation.

Based on educational qualifications, many respondents were Degree holders (31.0%), followed by Diploma holders (27.1%), Master's degree holders (22.4%), and Ph.D. holders (10.6%). A smaller percentage (9.0%) of them had a Certificate-level education. Regarding work experience, the respondents were well-distributed across different experience levels. Most of the individuals worked between 5-9 years (22.0%), followed by 20-24 years (19.6%), 10-14 years (17.6%), and 15-19 years (14.5%). A smaller group were employed for more than 25 years of experience (11.4%). Approximately 14.9% of them had 1-4 years of experience. This diversity highlights a broad representation of professionals from various industries, educational backgrounds, and experience levels.

The SEM was employed using Smart PLS 4.0 to examine the relationships among perceived threat severity, perceived threat vulnerability, fear, perceived response efficacy, perceived self-efficacy, and response cost in the PMT framework. A two-stage analysis involving measurement and structural model assessment was performed. The former involves evaluating construct reliability and validity, while the latter entails examining the path coefficients, explanatory power ($R^2$), effect sizes ($f^2$), and predictive relevance ($Q^2$).

TABLE I. OUTER LOADING

| Items | Outer Loading | Items | Outer Loading |
|---|---|---|---|
| Fear | | Perceived Self-Efficacy | |
| FOC1 | 0.91 | PSE1 | 0.764 |
| FOC2 | 0.853 | PSE2 | 0.8 |
| FOC3 | 0.882 | PSE3 | 0.8 |
| FOC4 | 0.79 | PSE4 | 0.697 |
| Perceived Response Efficacy | | Perceived Threat Vulnerability | |
| PRE1 | 0.853 | PTV1 | 0.833 |
| PRE2 | 0.83 | PTV2 | 0.895 |
| PRE3 | 0.826 | PTV3 | 0.894 |
| Response Cost | | Perceived Threat Severity | |
| RC1 | 0.797 | PTS1 | 0.822 |
| RC2 | 0.862 | PTS2 | 0.8 |
| RC3 | 0.869 | PTS3 | 0.758 |
| Protection Motivation Theory | | | |
| PM1 | 0.867 | | |
| PM2 | 0.874 | | |
| PM3 | 0.797 | | |

Several statistical tests were used in measurement model assessment to determine construct reliability and validity. With all the outer loadings exceeding the recommended threshold of 0.60 (0.697-0.910), indicator reliability was established (see Table I). Cronbach's alpha and CR values, both of which exceeded 0.70, confirmed strong internal consistency reliability. The AVE values exceeding 0.50 confirmed the convergent validity. Hence, each construct effectively measured the intended latent variables. The Fornell-Larcker criterion, cross-loadings, and HTMT ratio met the required thresholds, confirming discriminant validity of each construct. Overall, the theoretical constructs and measurement model were accurately captured and validated, respectively.

The VIF values below 5 indicate the absence of multicollinearity in the structural model assessment [26]. Represented by the $R^2$ value for protection motivation (0.554), the model's moderate explanatory power suggests that 55.4% of the variance was explained by the independent variables. Path coefficient analysis highlighted the statistical significance of most of the hypothesised relationships based on the theoretical assumptions of PMT [27]. With some of the constructs denoting strong effects and others reflecting moderate to small effects on protection motivation, the $f^2$ results varied. The positive $Q^2$ values highlight the model's ability to predict future data and applicability in behavioural works.

The current results evidence the key determinants of protection motivation. The significant positive influence of perceived threat severity and vulnerability on fear implies that people who perceive a threat as severe might experience higher levels of fear and, subsequently, the motivation to engage in protective behaviours. Fear played a strong mediating role in the relationship between perceived threat (severity and vulnerability) and protection motivation. As such, emotional responses must be seriously considered in the decision-making process [28-29]. The significant relationship between perceived response efficacy, self-efficacy, and protection motivation confirms that people who believe in the effectiveness of a protective measure and trust in their ability to perform it would engage in protective behaviours. In contrast, the negative influence of response cost implies that people who perceive protective actions as too costly or difficult would be less inclined to adopt them [30]. This finding highlights the need to mitigate the perceived barriers to protective behaviours via policy interventions and awareness campaigns.

The validation of PMT's applicability in a new context enriches the theoretical understanding of PMT. Including fear as a mediator increases the theory's explanatory power while delineating how individuals assess risk and make protective behaviour-related decisions [31]. In practice, the study results have significant implications for public health campaigns, policy interventions, and behavioural change strategies. Risk communication efforts should prioritise threat severity and self-efficacy for enhanced protective behaviours. For example, policymakers should aim at alleviating financial barriers or inconvenience (response costs) to facilitate the adoption of protective measures [32]. Educational programs should also incorporate skills-building workshops. These self-efficacy strategies can empower individuals to take proactive risk mitigation measures.

This study highlighted the significant influence of threat appraisal (severity, vulnerability), coping appraisal (response efficacy, self-efficacy), and emotional factors (fear) on protective behaviour intentions based on PMT. The current outcomes underscore the significance of addressing fear, self-efficacy, and response costs in behavioural interventions [33-34]. Future works could consider examining longitudinal effects and cultural differences to increase the outcome generalisability. 10 research hypotheses were tested based on the proposed framework. McGuire et al. (2017) [27] and Hair et al. (2020) [28] asserted that structural model assessment facilitates the identification of significant and influential pathways that validate the hypotheses and demonstrate the model's predictive capability.

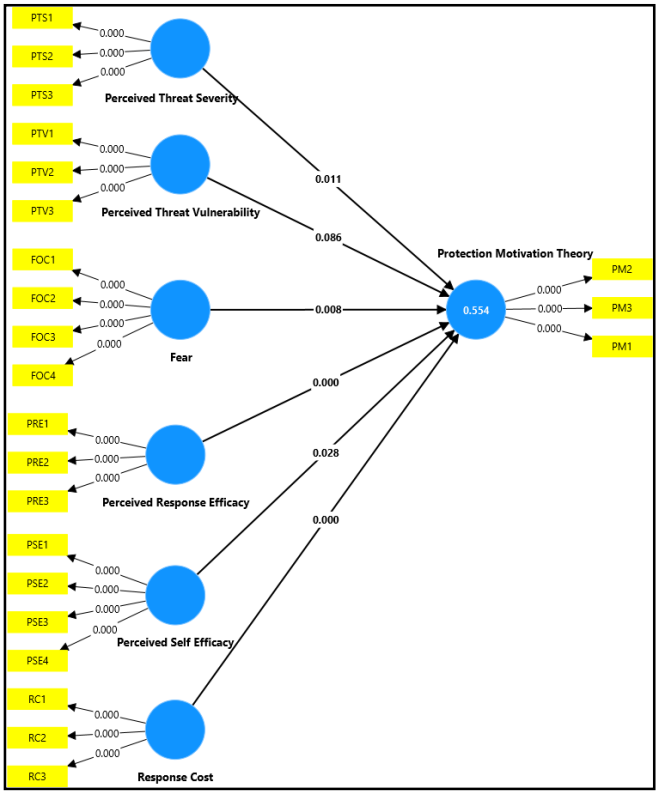


Fig. 2. Structural model.

Figure 2 illustrates the PMT framework and its key components, which are divided into two key cognitive processes: threat and coping appraisal. Perceived threat severity and its impact on individuals' motivation to take protective action were evaluated under threat appraisal [32].

Perceived threat severity, which implies an individual's assessment of how serious or dangerous a threat is, and fear, an emotional response stemming from the threat's perceived severity, influenced the motivation to adopt protective measures [33]. Coping appraisal assesses an individual's ability to effectively address the threat. This includes perceived response efficacy, where taking protective action effectively minimises the risk; perceived self-efficacy, which denotes the confidence in one's ability to perform the protective behaviours successfully; and response cost, which represents the perceived barriers or costs (related to taking the protective action [34]. These factors contribute to PMT, ultimately determining whether an individual is driven to take protective actions in response to a perceived threat (as in Figure 3).

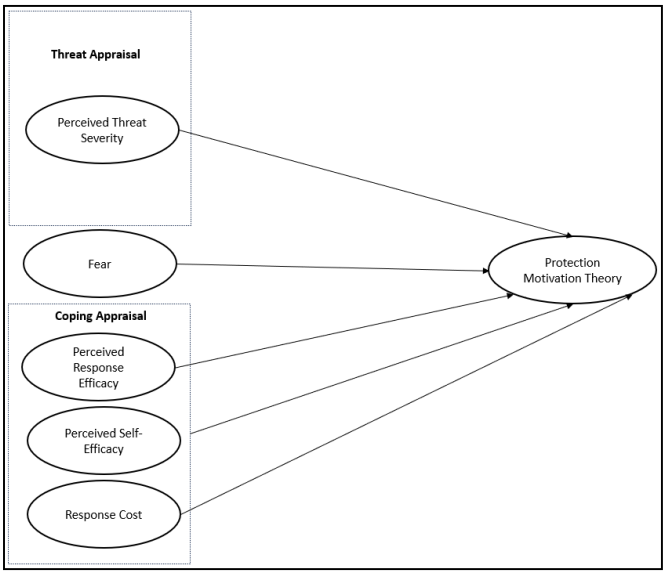


Fig. 3. Final model of cybersecurity awareness model based on PMT.

## VI. Conclusion

This study empirically validated PMT by highlighting the significance of threat appraisal, coping appraisal, and emotional responses in influencing protective behaviour intentions. Perceived threat severity and vulnerability positively impacted the levels of fear, which played a strong mediating role between the threat perception-protection motivation relationship. The finding underscores the critical role of emotional responses in behavioural decision-making processes. Furthermore, coping appraisal components strongly and positively influenced protection motivation. Individuals who believed in the effectiveness of the protective action and trusted in their ability to perform it were more driven to engage in protective behaviours. Meanwhile, the negative influence of response suggested that higher perceived barriers decreased the likelihood of adopting protective measures. These results validated PMT in a new context while also enhancing its explanatory power via the mediating effect of fear. The theoretical and practical study implications provided meaningful insights that will benefit public health strategies, policy development, and behavioural change interventions.

Public health campaigns must consider the severity and vulnerability associated with threats to evoke appropriate levels of fear that motivate protective actions. Notably, this correlation must be balanced to avoid inducing excessive fear and defensive mechanisms. Educational programs could introduce skill-building workshops and training sessions to boost individuals' confidence in their ability to effectively perform protective behaviours. Meanwhile, communication strategies should demonstrate the effectiveness of protective measures using evidence-based information. Such actions can significantly mitigate risks. Policymakers could consider alleviating the perceived barriers to protective behaviours through financial subsidies, simplified procedures, and publicly accessible

protective resources. Furthermore, behavioural interventions could account for emotional responses (particularly fear) by providing supportive messages that guide individuals from awareness to action without causing unnecessary anxiety. Potential scholars should conduct longitudinal studies to explore the long-term effects of protection motivation factors. Examining cultural differences can enhance the outcome generalisability to diverse populations. Stakeholders who apply these recommendations can develop more robust strategies that improve protective behaviours, public health outcomes, and risk management practices.

## VII. LIMITATION

Despite providing valuable insights into cybersecurity awareness in IR 4.0 environments, this study is subject to several limitations. Firstly, the use of a cross-sectional design limits the ability to observe changes in cybersecurity awareness or protective behaviours over time; hence, longitudinal studies are recommended for future research to gain a deeper understanding of behavioural dynamics and causality. Secondly, the reliance on self-reported data introduces potential biases, such as social desirability effects, where participants may have overestimated their awareness or adherence to cybersecurity practices to align with perceived expectations. Additionally, the study's generalisability is limited due to its focus on Malaysian IR 4.0-based organisations; extending this research to other cultural and geographical contexts could enhance the applicability of the findings. The theoretical scope was also constrained, as the study concentrated solely on core Protection Motivation Theory (PMT) constructs—namely threat appraisal, coping appraisal, and fear—without considering other influential factors like peer influence, organisational culture, or support systems, which may further enrich the model. From a technical perspective, while the behavioural aspects of cybersecurity were well addressed, the study did not explore technical dimensions such as intrusion detection systems (IDS), encryption tools, or information security protocols. Incorporating these elements through a mixed-methods approach could offer a more holistic understanding of cybersecurity readiness. Lastly, although PLS-SEM was appropriately used for its predictive and exploratory capabilities, it does have methodological constraints, including sensitivity to model specifications and potential path estimation biases. Future work may benefit from comparing PLS-SEM outcomes with those derived from covariance-based SEM for validation and robustness.

## REFERENCES

[1] R. Swamy and R. Kota, "Applications and implications of IoT in daily life and industry," 2020.

[2] A. Rikalovic, I. Cosic, and D. Lazarevic, "Additive manufacturing technologies in smart factories," Additive Manufacturing Journal, vol. 50, art. no. 102563, 2022.

[3] E. Rivera and D. Gonzalez, "The adoption of cyber-physical systems in small and medium enterprises," 2021.

[4] A. Vance, M. Siponen, and S. Pahnila, "The impact of fear on cybersecurity behavior: A systematic review of the literature," 2021.

[5] W. Tsai, Q. Li, and D. Nguyen, "Cyber threat mitigation in IoT-based smart factories: Exploring human factors and PMT constructs," International Journal of IoT Security, vol. 27, no. 2, pp. 33–56, 2021.

[6] L. Turner and S. Park, "Big data analytics for quality control in Industry 4.0," 2019.

[7] A. Vance, P. B. Lowry, and D. Eggett, "Using accountability to reduce access policy violations in information systems," Journal of Management Information Systems, vol. 29, no. 4, pp. 263–290, 2012.

[8] F. Tao, "The dual focus of PMT on health-compromising and health-promoting behaviors," 2022.

[9] T. Sommestad et al., "A meta-analysis of PMT in predicting information security behaviors," 2016.

[10] J. Mou et al., "Refining PMT with additional contextual constructs and coping factors," 2022.

[11] Y. Li et al., "Peer influence and danger perception: Extending PMT in employee cybersecurity," 2016.

[12] B. McLean and C. Torres, "Role of IoT in enhancing the performance of smart logistics systems," 2022.

[13] P. Miller and K. Kim, "The role of digital twins in optimizing smart factories," 2019.

[14] S. Mohamed and T. Ali, "Cybersecurity awareness in Malaysia: Trends, challenges, and future directions," Journal of Southeast Asian Technology Studies, vol. 18, no. 2, pp. 102–123, 2022.

[15] R. Khanna and A. Kaur, "IoT devices: Collecting and transmitting environmental, behavioral, and operational data," 2020.

[16] M. Khorassani, Q. Li, and D. Smith, "Collaborative robotics in smart manufacturing: Opportunities and challenges," Robotics and Autonomous Systems, vol. 128, art. no. 103763, 2022.

[17] J. Kim et al., "A comparative analysis of PMT and other health behavior theories," 2021.

[18] L. Kim and J. Jordan, "Data privacy and security concerns in Industry 4.0 environments," 2019.

[19] S. Kim et al., "Customization and flexibility enabled by CPS in manufacturing," 2022.

[20] S. Kim, H. Li, and W. Zhang, "Perceived cybersecurity risks and behaviors in smart factory environments: Applying PMT constructs," Industrial Cybersecurity Journal, vol. 28, no. 3, pp. 45–68, 2022.

[21] J. Kokina and S. Blanchette, "Service robots in healthcare and domestic environments," 2019.

[22] R. Kothe et al., "Subjective Expected Utility Theory and its implications for behavioral choices," 2019.

[23] C. Kowalski and D. Black, "Cost-benefit paradigms in health behavior theory," 2020.

[24] K. Kritikos et al., "Cloud computing essentials: The NIST framework and beyond," 2019.

[25] K. Kritikos et al., "Enabling remote monitoring and control through cloud computing in Industry 4.0," 2019.

[26] R. Lal, A. Gupta, and S. Arora, "Industry 4.0: Revolutionizing operations with AI, IoT, and robotics," Journal of Technology and Innovation, vol. 29, no. 1, pp. 45–67, 2023.

[27] W. J. McGuire, M. D. Slater, and J. P. Dillard, "Fear appeals and protective behaviors in cybersecurity: The moderating role of perceived self-efficacy," 2017.

[28] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, Multivariate Data Analysis, 7th ed. Pearson Education, 2011.

[29] R. Huang, L. Chen, and P. Zhang, "Understanding vulnerability perception in cybersecurity: A model of risk awareness," 2021.

[30] S. Huang and P. Cooper, "Using augmented reality for training and maintenance in Industry 4.0," 2021.

[31] J. Hughes and M. Wang, "Cyber-physical systems in agriculture: Enhancing productivity and sustainability," 2021.

[32] R. Ibrahim, "International cooperation in addressing global cybersecurity challenges," 2021.

[33] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory," Computers & Security, vol. 31, no. 1, pp. 83–95, 2012.

[34] A. Janelesch et al., "AI-driven systems for predictive maintenance and process optimization in Industry 4.0," 2021.