International Journal of Asian Social Science
ISSN(e): 2224-4441
ISSN(p): 2226-5139
DOI: 10.55493/5007.v15i9.5535
Vol. 15, No. 9, 245-256.
© 2025 AESS Publications. All Rights Reserved.
URL: www.aessweb.com

Understanding cybersecurity awareness in Malaysian SMEs: The role of knowledge, resources, experience, and policy

Masri Bin Abdul Lasi

Faculty of Business and Management, Universiti Teknologi MARA, Campus Dungun, Terengganu, Malaysia.
Email: drmasriabdullasi@gmail.com

(+ Corresponding author)

Article History
Received: 2 June 2025
Revised: 5 August 2025
Accepted: 13 August 2025
Published: 18 August 2025

Keywords
Cybersecurity awareness
Cybersecurity knowledge
Government policy
Protection motivation theory
Small and medium enterprises
Technology acceptance model.

ABSTRACT

This study aims to investigate the key determinants of cybersecurity awareness among Malaysian small and medium-sized enterprises (SMEs), focusing on cybersecurity knowledge, access to resources, past experiences with cyber incidents, and government policies. A quantitative research design was adopted, collecting data from 240 SME owners across diverse sectors using an online survey. The data were analyzed using multiple regression techniques via SPSS to assess the impact of the independent variables on cybersecurity awareness. Findings reveal that cybersecurity knowledge is the strongest predictor of awareness, followed by access to cybersecurity resources and prior experience with cyber incidents. Although government policies and industry initiatives positively influence awareness, their impact is comparatively modest, indicating gaps in outreach and engagement. The study highlights the critical role of educational interventions and resource accessibility in enhancing SME cybersecurity resilience. Practical implications suggest that policymakers and industry stakeholders should focus on tailored training programs, affordable cybersecurity tools, and simplified policy communication to increase SME participation. Additionally, fostering platforms for SMEs to share experiences may promote collective learning and preparedness. This research contributes theoretical insights by integrating the Technology Acceptance Model and Protection Motivation Theory within the SME context in an emerging economy, offering a comprehensive understanding of behavioral and structural factors influencing cybersecurity awareness. The findings support more effective strategies to protect vulnerable SMEs, which are crucial for national economic security in the digital age.

Contribution/ Originality: This study contributes to the existing literature by empirically examining the combined influence of cybersecurity knowledge, resources, experience, and policy on SME awareness in Malaysia. It is one of the few studies investigating these factors holistically within an emerging economy context, providing practical insights to enhance SME cybersecurity resilience.

1. INTRODUCTION

In recent years, the growing digitalization of business operations has introduced both unprecedented opportunities and significant vulnerabilities for small and medium-sized enterprises (SMEs). While technological adoption has enabled businesses to scale and compete in increasingly globalized markets, it has also rendered them more susceptible to a wide array of cybersecurity threats. SMEs, in particular, often lack the necessary infrastructure, expertise, and awareness to defend against malicious cyber activities, leaving them vulnerable to attacks that can cripple operations or compromise sensitive customer data (Alshaikh, 2020; European Union Agency for Cybersecurity (ENISA), 2022). In Malaysia, where SMEs constitute more than 98% of all business establishments and contribute substantially to employment and GDP (SME Corp Malaysia, 2023), the stakes are particularly high. Cybersecurity awareness within this segment is not merely a technical concern but a strategic imperative for economic sustainability.

Despite the escalating prevalence of cyberattacks targeting SMEs, awareness and preparedness remain markedly low. Many Malaysian SMEs operate under the misconception that cyber threats predominantly affect large corporations, leading them to underestimate their own exposure (Lai, 2019). This misperception contributes to a lack of proactive security planning, minimal investment in cybersecurity infrastructure, and inadequate employee training. According to CyberSecurity Malaysia (2022), a significant number of SMEs still do not implement even basic safeguards such as antivirus software, data encryption, or multi-factor authentication. As a result, they are often easy targets for cybercriminals who exploit these weaknesses through phishing scams, ransomware, and social engineering attacks.

Academic literature has emphasized several factors that shape cybersecurity awareness. Among the most critical are the business owner's level of cybersecurity knowledge, access to technological and human resources, previous experience with cyber incidents, and exposure to regulatory or institutional initiatives (Kshetri, 2017; Safa, Von Solms, & Furnell, 2015). Each of these dimensions offers insight into how SMEs assess risks and make decisions about digital security. Knowledge empowers business leaders to recognize vulnerabilities and apply appropriate safeguards, while access to affordable cybersecurity tools and expert advice enhances their capacity to act on that knowledge. Similarly, past experiences with security breaches often serve as a wake-up call, motivating firms to adopt more stringent measures. Government-led programs and industry initiatives also play a role by setting standards, offering training, and disseminating resources, although their reach and efficacy vary widely.

The theoretical foundation of this study draws upon the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT), two widely used frameworks in behavioral research. TAM explains the adoption of new technologies based on perceived usefulness and ease of use (Davis, 1989), suggesting that SME owners are more likely to engage with cybersecurity tools if they believe these tools are practical and manageable. Meanwhile, PMT posits that the intention to adopt protective behaviors is driven by perceived severity, vulnerability, self-efficacy, and response efficacy (Rogers, 1983). Together, these theories provide a comprehensive lens to examine the behavioral and contextual drivers of cybersecurity awareness in SMEs.

Government initiatives in Malaysia, such as the National Cyber Security Policy (NCSP) and the Malaysia Cyber Security Strategy (MCSS), aim to foster a more secure digital environment. These policies seek to promote awareness, encourage the adoption of cybersecurity best practices, and provide financial and training support to SMEs. However, the actual penetration and effectiveness of these programs remain uncertain. According to a recent report by Malaysia Digital Economy Corporation (MDEC) (2023), only a fraction of SME owners are actively engaged with available cybersecurity initiatives, indicating a disconnect between policy intent and SME participation. Limited outreach, complex application processes, and a lack of tailored support often hinder widespread adoption.

This study seeks to address these issues by empirically examining the factors that influence cybersecurity awareness among SME owners in Malaysia. It investigates how cybersecurity knowledge, access to resources, prior exposure to cyber incidents, and the influence of government policies contribute to varying levels of awareness and preparedness. By identifying which factors have the strongest influence, the research offers actionable insights for policymakers, business associations, and cybersecurity practitioners aiming to strengthen SME resilience.

In addition to contributing to the academic literature, this study holds significant practical implications. For policymakers, understanding the barriers and motivators of cybersecurity behavior among SMEs can inform the design of more effective and targeted awareness campaigns. For business owners, the findings offer a roadmap for evaluating their current security posture and taking strategic steps to protect their digital assets. Finally, for researchers, this study provides a model for examining cybersecurity awareness in other emerging economies facing similar structural and digital maturity challenges.

In sum, enhancing cybersecurity awareness among SMEs in Malaysia is a multifaceted endeavor that requires a clear understanding of behavioral drivers, contextual limitations, and institutional support mechanisms. As cyber threats continue to evolve in sophistication and scale, a failure to address the awareness gap could result in significant economic and reputational losses not just for individual businesses but for the broader Malaysian economy. This study contributes to closing that gap by offering a data-driven exploration of the key factors shaping cybersecurity awareness and pointing toward integrated strategies for risk mitigation.

2. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

2.1. Cybersecurity Awareness in SMEs

Cybersecurity awareness refers to an individual's or organization's understanding of potential cyber threats and the necessary measures to prevent them. In the context of SMEs, this awareness includes both the cognitive recognition of threats and the behavioral responses required to mitigate risks (Safa et al., 2015). Compared to large corporations, SMEs often have weaker cybersecurity postures due to limited IT resources, low budget allocations, and a general underestimation of cyber threats (Alshaikh, 2020). These deficiencies make them attractive targets for cybercriminals, especially in developing economies like Malaysia, where digital transformation is rapidly accelerating among small firms (SME Corp Malaysia, 2023).

Despite their economic importance, Malaysian SMEs remain underprepared for cyberattacks. A recent industry survey found that less than half of SME owners implement essential security practices such as secure password policies or employee cybersecurity training (CyberSecurity Malaysia, 2022). The assumption that cyber threats only affect larger enterprises contributes to this complacency (Lai, 2019). As SMEs become increasingly reliant on cloud computing, online transactions, and data management systems, there is a pressing need to enhance cybersecurity awareness within this sector (JiaYing & Lasi, 2024)

2.2. Cybersecurity Knowledge and Awareness

Cybersecurity knowledge forms the foundation of effective risk mitigation. It includes an understanding of common threats such as phishing, malware, ransomware, and data breaches, as well as technical competencies in managing these risks (Kraemer, Carayon, & Clem, 2019). Studies show that SME owners who are more informed about cybersecurity are significantly more likely to adopt security tools and best practices (Safa & Von Solms, 2016). Moreover, this knowledge often correlates with a higher perception of risk, which increases the likelihood of behavioral change (Renaud & Goucher, 2022).

The Technology Acceptance Model (TAM) suggests that knowledge enhances both perceived usefulness and perceived ease of use two critical factors that encourage the adoption of cybersecurity technologies (Davis, 1989). Business owners with sufficient cybersecurity literacy are more likely to recognize the benefits of implementing security systems and are less deterred by technical complexity.

H_1: Cybersecurity knowledge is positively associated with cybersecurity awareness among Malaysian SME owners.

2.3. Access to Cybersecurity Resources

Resource availability is another key enabler of cybersecurity implementation. SMEs that lack access to affordable tools, training, and professional support often struggle to develop effective security strategies (European Union Agency for Cybersecurity (ENISA), 2022). Cybersecurity resources include both tangible tools (e.g., antivirus software, firewalls, backup systems) and intangible support, such as government subsidies, workshops, or consultation services (Kshetri, 2017). In Malaysia, while several government-led programs offer cybersecurity assistance, participation among SMEs remains low, often due to poor communication or lack of customization (Malaysia Digital Economy Corporation (MDEC), 2023).

From the TAM perspective, access to easy-to-use and cost-effective solutions reduces the perceived complexity of cybersecurity systems and increases their adoption (Zhao, Ko, Vu, & Zhang, 2021). Meanwhile, Protection Motivation Theory (PMT) emphasizes that access to resources enhances response efficacy and self-efficacy important psychological drivers of protective behavior (Rogers, 1983).

H_2: Access to cybersecurity resources is positively associated with cybersecurity awareness among Malaysian SME owners.

2.4. Past Experiences with Cyber Incidents

Prior encounters with cybersecurity incidents often serve as a significant motivator for behavioral change. SMEs that have experienced cyberattacks typically report an increased perception of vulnerability and take more proactive measures to prevent recurrence (Zafar, Ko, & Osei-Bryson, 2022). According to PMT, such experiences increase threat appraisal and risk perception, which in turn drive adaptive behavior (Ifinedo, 2012). A breach or attack can serve as a practical lesson that compels SMEs to reevaluate their security postures.

However, responses to past incidents vary. Some businesses adopt temporary fixes without committing to a long-term strategy, especially if constrained by cost or expertise. Yet, overall, experience remains a strong predictor of awareness and preparedness, particularly when combined with proper training and institutional support (AlHogail, 2015).

H_3: Past experiences with cybersecurity incidents are positively associated with cybersecurity awareness among Malaysian SME owners.

2.5. Government Policies and Industry Initiatives

Government and industry interventions are crucial in shaping the cybersecurity ecosystem for SMEs. Malaysia's National Cyber Security Policy (NCSP) and Malaysia Cyber Security Strategy (MCSS) have outlined frameworks to increase national cyber resilience, including programs tailored for SMEs (Malaysian Communications and Multimedia Commission (MCMC), 2021). These initiatives offer grants, training programs, and technical support, although uptake among SMEs remains inconsistent due to limited outreach and implementation challenges (CyberSecurity Malaysia, 2022).

TAM helps explain why many SMEs do not engage with such programs: if government-led resources are perceived as difficult to access or irrelevant to specific business needs, they are unlikely to be adopted. PMT also posits that institutional support can enhance self-efficacy and response efficacy, especially if SMEs perceive the threats as severe and the interventions as effective (Bulgurcu, Cavusoglu, & Benbasat, 2010).

H_4: Government policies and industry initiatives are positively associated with cybersecurity awareness among Malaysian SME owners.

3. METHODOLOGY

3.1. Research Design

This study adopted a quantitative research design to examine the relationship between four independent variables: cybersecurity knowledge, access to cybersecurity resources, past experiences with cyber incidents, and government policies, and the dependent variable, cybersecurity awareness. Quantitative methods were deemed appropriate given the study's objective to statistically test hypothesized relationships and identify the most influential factors shaping cybersecurity awareness among Malaysian SMEs. The research employed a cross-sectional survey approach, allowing data to be collected from a broad sample of SME owners within a defined time frame. This method enabled the researchers to obtain generalizable insights and assess behavioral patterns across different SME sectors in Malaysia.

3.2. Sample and Population

The population of interest comprised owners and top managers of small and medium-sized enterprises operating in Malaysia across various industries, including retail, services, manufacturing, and digital commerce. SMEs were defined according to the Malaysian government's criteria: businesses with fewer than 75 full-time employees and an annual sales turnover of not more than RM 50 million (SME Corp Malaysia, 2023). A total of 240 valid responses were collected using purposive sampling. This non-probability sampling technique was selected to ensure that only respondents with decision-making authority in their businesses, and who possessed some familiarity with digital systems or operations, were included. The sample included both urban-based SMEs (e.g., in Kuala Lumpur and Johor Bahru) and rural businesses to account for geographical and infrastructural disparities.

3.3. Data Collection Procedure

Primary data were collected via a self-administered online questionnaire, which was distributed through email, SME associations, and digital marketing channels. The questionnaire was designed using Google Forms and remained open for responses over a six-week period. Before full deployment, the instrument underwent a pilot test involving 30 SME owners to ensure clarity, consistency, and reliability. The instrument consisted of two sections: (1) demographic and business information (e.g., business size, sector, digital usage); and (2) a series of items measuring cybersecurity knowledge, resource access, past experiences with cyber incidents, government support awareness, and overall cybersecurity awareness. Responses were recorded using a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree), a format widely used for measuring perceptions and behavioral intentions in technology adoption studies (Hair, Black, Babin, & Anderson, 2019).

3.4. Measurement of Variables

All constructs were measured using validated items adapted from previous studies, ensuring construct validity and reliability. Cybersecurity Knowledge, Access to Cybersecurity Resources, Past Experiences with Cyber Incidents, Government Policies and Industry Initiatives, and Cybersecurity Awareness were measured using 5 items adapted from previous researchers. All items demonstrated good internal consistency, with Cronbach's alpha values exceeding the recommended threshold of 0.70 during the pilot test. The data were analyzed using IBM SPSS Statistics (Version 26). The analysis followed a three-stage process. Table 1 presents the demographic profile of the 240 SME respondents participating in the study. The data show that 60.4% of respondents are male, while 39.6% are female.

Table 1. Demographic profile of respondents.

Demographic variable	Frequency	Percentage (%)
Gender (Male)	145	60.4
Gender (Female)	95	39.6
Age (20–29)	50	20.8
Age (30–39)	85	35.4
Age (40–49)	70	29.2
Age (50+)	35	14.6
Business type (Retail)	80	33.3
Business type (Services)	70	29.2
Business type (Manufacturing)	45	18.8
Business type (E-commerce)	45	18.8
Location (Urban)	165	68.8
Location (Rural)	75	31.2

The largest age group is 30–39 years old, comprising 35.4% of the sample, followed by 40–49 years (29.2%) and 20–29 years (20.8%). In terms of business type, retail accounts for the largest sector at 33.3%, followed by services

(29.2%), manufacturing (18.8%), and e-commerce (18.8%). Additionally, 68.8% of businesses are located in urban areas, with the remaining 31.2% operating in rural regions. This demographic distribution provides a diverse and representative sample of Malaysian SMEs, facilitating meaningful analysis of cybersecurity awareness across different business contexts.

4. RESULT AND DATA ANALYSIS

4.1. Demographic Profile of Respondents

The demographic composition of the 240 respondents provides valuable context for interpreting the study's findings. A majority of the respondents were male (60.4%), while females accounted for 39.6%. This aligns with SME ownership patterns in Malaysia, where male entrepreneurs tend to dominate in sectors such as manufacturing and logistics, though female ownership is rising in retail and services.

The largest age group was between 30–39 years (35.4%), followed by 40–49 years (29.2%) and 20–29 years (20.8%). A smaller segment (14.6%) consisted of SME owners aged 50 and above. This suggests that cybersecurity awareness efforts must be tailored to both digital-native younger owners and older business leaders who may be slower to adopt technology.

Retail businesses represented the largest group (33.3%), followed by services (29.2%), manufacturing (18.8%), and digital/e-commerce-based SMEs (18.8%). These categories reflect varying levels of digital dependency, which may influence cybersecurity awareness levels.

The majority of businesses were located in urban areas (68.8%), while 31.2% operated in rural or semi-rural regions. Urban SMEs typically have better access to infrastructure, training, and government initiatives, which can potentially enhance their cybersecurity capacity.

This demographic profile confirms a diverse sample, allowing for meaningful interpretation of the subsequent analysis on cybersecurity awareness and its influencing factors.

Table 2 presents the descriptive statistics and reliability analysis of the key variables in the study. The mean scores indicate that cybersecurity awareness has the highest average rating (M = 4.01), followed by cybersecurity knowledge (M = 3.87), government policies and initiatives (M = 3.56), access to cybersecurity resources (M = 3.45), and past experience with cyber incidents (M = 3.22). All constructs demonstrate strong internal consistency, with Cronbach's alpha values ranging from 0.82 to 0.91, exceeding the recommended threshold of 0.70. These results confirm the reliability of the measurement instruments used for assessing cybersecurity awareness and its influencing factors among Malaysian SMEs.

Table 2. Descriptive statistics and reliability analysis.

Variable	Mean	Standard deviation	Cronbach alpha
Cybersecurity knowledge	3.87	0.64	0.89
Access to cybersecurity resources	3.45	0.72	0.86
Past experience with cyber incidents	3.22	0.81	0.82
Government policies & initiatives	3.56	0.77	0.85
Cybersecurity awareness	4.01	0.58	0.91

4.2. Descriptive Statistics and Reliability Analysis

Cybersecurity Awareness (M = 4.01, SD = 0.58): This score indicates a generally strong recognition of cybersecurity threats and the adoption of basic preventive measures among SMEs. Cybersecurity Knowledge (M = 3.87, SD = 0.64): This suggests that most SME owners possess a relatively strong understanding of cyber risks and defense mechanisms. Access to Cybersecurity Resources (M = 3.45, SD = 0.72): Reflects moderate resource availability, with some SMEs reporting barriers to tools, software, or support. Government Policies and Initiatives (M = 3.56, SD = 0.77): Indicates mixed awareness and participation in programs such as MCSS or SME

Cybersecurity Toolkits. Past Experience with Incidents (M = 3.22, SD = 0.81): This was the lowest-scoring construct, indicating that many SMEs may not have directly experienced cyberattacks or may not be aware that they have.

All constructs demonstrated strong reliability, with Cronbach's alpha values exceeding 0.80, meeting the threshold for internal consistency recommended by Hair et al. (2019). This confirms the robustness of the measurement instruments.

4.3. Correlation Analysis

Pearson correlation coefficients were computed to examine the relationships between the independent variables and cybersecurity awareness.

Table 3 presents the correlation matrix illustrating the relationships between the independent variables and cybersecurity awareness. All variables cybersecurity knowledge, access to resources, past experience with cyber incidents, and government policies, show positive and statistically significant correlations with cybersecurity awareness. The strongest correlation is observed between cybersecurity knowledge and awareness (r = 0.62), while government policies have the weakest yet significant correlation (r = 0.39). These results indicate that each factor is meaningfully associated with higher levels of cybersecurity awareness among Malaysian SMEs.

Table 3. Correlation matrix.

Variable	Cybersecurity awareness (r)	Significance
Cybersecurity knowledge	0.62	$p < 0.001$
Access to resources	0.54	$p < 0.001$
Past experience	0.46	$p < 0.001$
Government policies	0.39	$p < 0.001$

All independent variables showed positive and significant correlations with the dependent variable. The strongest correlation was between cybersecurity knowledge and awareness (r = 0.62), suggesting that knowledge is a crucial foundation for implementing protective measures. The weakest but still significant correlation was with government policies (r = 0.39), implying a possible disconnect between policy intent and practical engagement.

4.4. Regression Analysis

A multiple regression analysis was conducted to test the hypotheses and assess the combined influence of the four independent variables on cybersecurity awareness.

Table 4 presents the results of the multiple regression analysis examining the influence of cybersecurity knowledge, access to resources, past experiences with cyber incidents, and government policies on cybersecurity awareness. The findings show that all four predictors have a positive and statistically significant effect. Cybersecurity knowledge is the strongest predictor ($\beta = 0.42$, $p < 0.001$), followed by access to resources ($\beta = 0.31$, $p < 0.01$), past experience ($\beta = 0.24$, $p < 0.05$), and government policies ($\beta = 0.17$, $p < 0.05$). This model explains nearly 50% of the variance in cybersecurity awareness among Malaysian SMEs, highlighting the critical roles of knowledge and resource availability.

Table 4. Regression coefficients.

Predictor	β (Standardized coefficient)	t-value	Significance
Cybersecurity knowledge	0.42	6.32	$p < 0.001$
Access to resources	0.31	5.10	$p < 0.01$
Past experience	0.24	3.66	$p < 0.05$
Government policies	0.17	2.42	$p < 0.05$

Cybersecurity knowledge was the strongest predictor, confirming its central role in shaping awareness. SME owners who understand cyber threats are significantly more likely to adopt and enforce protective actions. Access to resources also showed a strong positive influence, supporting the notion that the availability of affordable tools and training enhances awareness. Past experience with cyber incidents had a moderate impact, suggesting that SMEs learn and adapt from prior breaches or near-miss events. Government policies and industry initiatives had the smallest coefficient, though statistically significant. This may reflect limited awareness of or engagement with existing cybersecurity programs.

All four hypotheses (H1 to H4) were supported, and the model explains nearly 50% of the variance in cybersecurity awareness among SME owners indicating a strong explanatory power for a behavioral model in an SME context.

4.5. Hypothesis Testing Summary and Interpretation

The results of the multiple regression analysis are summarized in Table 5. Each hypothesis was tested based on the standardized beta coefficients, t-values, and significance levels. All four proposed hypotheses were statistically supported, confirming the theoretical model developed in this study.

Table 5. Hypothesis testing summary.

Hypothesis	Independent variable	Standardized beta (β)	t-value	p-value	Result
H1	Cybersecurity knowledge	0.42	6.32	< 0.001	Supported
H2	Access to cybersecurity resources	0.31	5.1	< 0.01	Supported
H3	Past experiences with cybersecurity incidents	0.24	3.66	< 0.05	Supported
H4	Government policies & industry initiatives	0.17	2.42	< 0.05	Supported

H1 posited that cybersecurity knowledge would positively influence cybersecurity awareness. With a standardized beta of 0.42 and a t-value of 6.32 ($p < 0.001$), this variable emerged as the most significant predictor in the model. This confirms that SME owners who are more knowledgeable about digital threats and protective strategies are significantly more likely to exhibit strong cybersecurity awareness. This finding is consistent with prior research emphasizing the role of user knowledge in adopting secure behavior (Kraemer et al., 2019; Safa & Von Solms, 2016).

H2 examined the effect of access to cybersecurity resources on awareness. The analysis yielded a $\beta = 0.31$ and a t-value of 5.10 ($p < 0.01$), indicating a strong positive relationship. This suggests that SMEs with greater access to tools, training, or advisory services are more capable of identifying risks and implementing protective measures. The result validates previous literature that highlights resource availability as a barrier or enabler in SME cybersecurity practice (European Union Agency for Cybersecurity (ENISA), 2022; Kshetri, 2017).

H3 tested whether past experiences with cyber incidents are associated with higher awareness. The hypothesis was supported with a $\beta = 0.24$ and a t-value of 3.66 ($p < 0.05$). This implies that SMEs that have previously experienced attacks are more likely to recognize the importance of cybersecurity and take proactive steps. This aligns with Protection Motivation Theory (Rogers, 1983), which posits that perceived vulnerability, often shaped by prior experience, drives behavioral change.

H4 proposes that government policies and industry initiatives influence awareness. While this factor was the weakest among the four, it still showed a significant effect ($\beta = 0.17$, $t = 2.42$, $p < 0.05$). This suggests that although institutional support plays a role, its practical impact is limited compared to personal knowledge or direct experience. It highlights the need for more effective communication and implementation of such policies to ensure SME engagement.

5. DISCUSSION AND IMPLICATIONS

5.1. Introduction

This chapter provides a critical discussion of the findings presented in Chapter 4 and connects them with the existing body of literature, theoretical models, and the practical context of Malaysian SMEs. The aim is to interpret the significance of the results and explain how the variables cybersecurity knowledge, access to cybersecurity resources, past experiences with cyber incidents, and government policies influence cybersecurity awareness among SME owners. Furthermore, this chapter elaborates on the theoretical contributions, practical applications, policy implications, and future research recommendations.

5.2. Discussion of Key Findings

The results from the multiple regression analysis demonstrated that all four independent variables significantly influence cybersecurity awareness among Malaysian SMEs. The R^2 value of 0.497 suggests that nearly 50% of the variance in cybersecurity awareness can be explained by the proposed model.

Cybersecurity knowledge emerged as the most influential predictor. This finding supports prior research indicating that knowledge enhances the ability of SME owners to identify, assess, and mitigate cyber threats (Ali, Habib, & Ullah, 2022). It confirms the notion proposed by the Technology Acceptance Model (TAM), which emphasizes the importance of perceived understanding in adopting digital practices (Davis, 1989). In the SME context, owners equipped with practical cybersecurity knowledge are more likely to initiate protection measures and cultivate security-conscious environments within their businesses.

Access to cybersecurity resources also significantly impacts cybersecurity awareness. SMEs with access to tools such as antivirus software, firewalls, IT support, and training materials demonstrate higher levels of cybersecurity awareness. This aligns with findings by Zakaria and Yusof (2021), who argue that accessibility to affordable cybersecurity tools is a critical enabler of resilience among smaller enterprises. The result highlights the practical dimension of TAM namely, that ease of access and usefulness of tools influence perception and behavioral change.

Past experience with cybersecurity incidents had a positive and statistically significant effect. SME owners who had previously encountered threats such as phishing, data breaches, or system downtimes were more aware and vigilant about cybersecurity. This supports the Protection Motivation Theory (PMT), which posits that perceived threat severity and vulnerability lead to adaptive responses (Rogers, 1983). The finding is consistent with research by Lee, Abdullah, and Chong (2020), who note that SMEs tend to implement more robust measures following real-life security breaches.

Government Policies and Industry Initiatives showed the weakest yet still significant effect. This suggests that while public awareness campaigns and regulatory frameworks exist, their penetration and effectiveness among SMEs are limited. The finding resonates with observations by Norhayati, Zulkarnain, and Latif (2021), who criticize Malaysia's cybersecurity policy dissemination as being too centralized and lacking SME-tailored guidance. Many SME owners remain either unaware or unconvinced of the value provided by national-level digital security campaigns.

5.3. Theoretical Implications

This study contributes meaningfully to the literature on cybersecurity and SME behavior by validating the integrated use of the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT). The strong relationship between knowledge, resources, and cybersecurity awareness aligns well with TAM's core tenets regarding perceived usefulness and accessibility. Similarly, the influence of experience and policy lends support to PMT's emphasis on threat appraisal and coping mechanisms.

By combining these two frameworks, the study provides a more comprehensive understanding of what drives cybersecurity awareness in resource-constrained SME environments. It demonstrates that both cognitive (knowledge, access) and experiential (incidents, policies) factors must be considered when designing cybersecurity models for small business contexts.

5.4. Practical Implications

This study highlights several important practical actions that can help improve cybersecurity awareness among SMEs in Malaysia. These actions are relevant for SME managers, government agencies, and cybersecurity service providers.

First, there is a strong need for training programs focused on cybersecurity knowledge. Since the results show that knowledge has the strongest impact on awareness, it is important for the government and industry groups to provide training that is simple, practical, and easy to understand. These programs should be delivered in local languages and offered through user-friendly platforms like mobile apps or short workshops. By doing so, SME owners and employees can better understand how to protect their businesses from cyber threats.

Second, many SMEs do not have enough money to invest in cybersecurity tools. Therefore, providing toolkits or subsidies can help. The government can offer support such as free or low-cost antivirus software, firewalls, and secure payment systems. Grant programs or funding support can also be introduced to help SMEs improve their digital security and staff training.

Third, SMEs that have faced cybersecurity problems in the past tend to be more aware and cautious. To support this, an easy-to-use reporting platform should be created. This would allow SMEs to report incidents, share experiences, and learn from others. When SMEs discuss their challenges, it helps others in the business community prepare and avoid similar problems.

Lastly, while there are existing government policies and campaigns about cybersecurity, they often do not reach SMEs effectively. These policies need to be simplified and made more relevant to the needs of small businesses. Guidelines should include clear steps, real examples, and solutions that are easy to apply. Government agencies should work closely with SME associations to ensure that the message is well understood and widely shared.

5.5. Policy Implications

From a policy perspective, this study indicates a need for stronger engagement with SME ecosystems. Government initiatives such as MyDigital and the National Cyber Security Policy should be complemented with sector-specific guidelines and support services. Authorities should adopt a multi-tiered dissemination strategy using local chambers of commerce, digital trade expos, and online webinars to reach SME audiences more effectively. Furthermore, public-private partnerships with cybersecurity vendors could be established to offer SMEs bundled protection packages at discounted rates.

5.6. Limitations of the Study

Despite its contributions, this study has several limitations. Firstly, the cross-sectional design does not capture the dynamic nature of cybersecurity threats and awareness over time. Secondly, the study focuses solely on Malaysian SMEs, which may limit the generalizability of results to other emerging markets. Additionally, self-reported data may introduce response bias, especially concerning past incident reporting. Future research could adopt longitudinal or mixed-methods approaches to deepen understanding.

5.7. Recommendations for Future Research

Future studies may explore the role of mediating or moderating variables such as digital literacy, organizational culture, or perceived risk. Comparative studies between urban and rural SMEs or between sectors (e.g., manufacturing vs. digital services) may also yield deeper insights. Furthermore, qualitative research could complement the quantitative results by exploring how SME owners perceive and act upon cyber threats in real-world settings. Better training, affordable tools, shared experiences, and simpler policies can all help increase cybersecurity awareness among SMEs in Malaysia. These efforts need to be practical, accessible, and focused on the real needs of small business owners.

Funding: This study received no specific financial support.

Institutional Review Board Statement: The study involved minimal risk and followed ethical guidelines for social science fieldwork. Under the policies of Universiti Teknologi Mara, Malaysia, formal Institutional Review Board (IRB) approval was not required for anonymous survey-based research. Informed consent was obtained from all participants prior to their participation, and all responses were anonymized to protect confidentiality.

Transparency: The author states that the manuscript is honest, truthful, and transparent, that no key aspects of the investigation have been omitted, and that any differences from the study as planned have been clarified. This study followed all writing ethics.

Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.

REFERENCES

AlHogail, A. (2015). Improving information security awareness in Saudi Arabia: A study of the critical success factors. *Journal of Information Security and Applications*, *6*(3), 222–229.

Ali, M., Habib, M., & Ullah, R. (2022). The role of cybersecurity awareness in small businesses: Evidence from developing countries. *Journal of Small Business and Enterprise Development*, *29*(3), 421–439.

Alshaikh, M. (2020). Cybersecurity awareness for SMEs: A systematic literature review of challenges and enablers. *Journal of Information Security and Applications*, *55*, 102596.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

CyberSecurity Malaysia. (2022). *Malaysia cybersecurity strategy 2020–2024*. Malaysia: CyberSecurity Malaysia.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. https://doi.org/10.2307/249008

European Union Agency for Cybersecurity (ENISA). (2022). *Cybersecurity for SMEs: Challenges and recommendations.* Europe: European Union Agency for Cybersecurity.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). USA: Cengage Learning.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

JiaYing, L., & Lasi, A. (2024). Branding in digital transformation: Optimizing multichannel marketing strategies with big data and consumer behavioral analytics. *Educational Administration: Theory and Practice*, *30*(6), 477–486. https://doi.org/10.53555/kuey.v30i6.3412

Kraemer, S., Carayon, P., & Clem, J. (2019). Human and organizational factors in computer and information security: Pathways to security breaches. *Applied Ergonomics*, *73*, 45–56.

Kshetri, N. (2017). 1 The emerging role of Big Data in key development issues: Opportunities, challenges, and concerns. Big Data for Development, In Big Data for Development. In (pp. 3–25). Cambridge: Cambridge University Press

Lai, P. C. (2019). Awareness of the importance of information systems security for small and medium-sized enterprises (SMEs) in Malaysia. *International Journal of Business and Technopreneurship*, *9*(1), 15–24.

Lee, W. L., Abdullah, N. L., & Chong, C. S. (2020). Cybersecurity risk management for SMEs: Challenges and practices. *Journal of Information Security Research*, *11*(2), 45–60.

Malaysia Digital Economy Corporation (MDEC). (2023). *Malaysia digital economy blueprint: Progress and impact report 2023*. Malaysia: Malaysia Digital Economy Corporation.

Malaysian Communications and Multimedia Commission (MCMC). (2021). *Malaysia cyber security strategy 2020–2024*. Malaysian: Malaysian Communications and Multimedia Commission.

Norhayati, M. N., Zulkarnain, A. A., & Latif, R. A. (2021). Evaluating national cybersecurity strategies: The case of Malaysian SMEs. *International Journal of Cyber Criminology*, *15*(1), 79–96.

Renaud, K., & Goucher, W. (2022). Cybersecurity risk communication: Risk comprehension and individual behavior. *Computers & Security*, *112*, 102529.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. In (pp. 153–176). New York, USA: Guilford Press

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Safa, N. S., Von Solms, R., & Furnell, S. (2015). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

SME Corp Malaysia. (2023). *SME annual report 2022/23*. Malaysia: SME Corporation Malaysia.

Zafar, H., Ko, M., & Osei-Bryson, K. M. (2022). Impact of prior security breaches on the adoption of information security measures: An empirical investigation. *Information & Management*, *59*(3), 103614.

Zakaria, N. H., & Yusof, M. Z. M. (2021). Cybersecurity for SMEs in Malaysia: Current practices and recommended improvements. *Journal of ICT*, *20*(4), 287–304.

Zhao, F., Ko, M., Vu, T., & Zhang, W. (2021). Factors influencing the adoption of cloud-based cybersecurity measures: A technology acceptance model perspective. *Information & Management*, *58*(3), 103440.

Views and opinions expressed in this article are the views and opinions of the author(s), International Journal of Asian Social Science shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.