Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8, 105-128
2026
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v10i8.13459

Assessing the barriers to cybersecurity readiness among Malaysian non-IT SMEs: An exploratory qualitative study

Zymul Z[1*], Hafizan Matsom[2], M Fadzil Hassan[3]
[1,2,3]Faculty of Science, Management and Computing, Universiti Teknologi PETRONAS, Malaysia;
zymul_24002432@utp.edu.my (Z.Z.) hafizan.msom@utp.edu.my (H.M.) mfadzil_hassan@utp.edu.my (M.F.H.).

Abstract: Malaysian non-IT SMEs that are subject to cyberattacks are still vulnerable and lack a strong cybersecurity infrastructure. This study explores the cybersecurity barriers among Malaysian non-IT SMEs, assesses their organizational cybersecurity readiness, and provides insights for strengthening their cybersecurity readiness posture. It uses a qualitative approach to examine the barriers to cybersecurity readiness of Malaysian non-IT SMEs and identifies the factors impacting it. Data were gathered by adopting purposive sampling, using self-administered, open-ended questionnaires, and thematic analysis was performed to find themes and produce insights about organizational, infrastructural, and human factors influencing cybersecurity readiness. The findings identified that the main obstacles Malaysian SMEs face include security exposure due to infrastructure and knowledge gaps, awareness and policy gaps, limited preventative measures and recovery plans, financial restrictions, and inadequate cybersecurity awareness and strategic oversight. The actionable guidelines include government initiatives for SMEs, outsourced security solutions, security assessment, and cybersecurity skill development; these are some practical recommendations. Overall, by highlighting the significance of organizational perception among Malaysian non-IT SMEs, this study adds to the body of literature on cybersecurity readiness. It also offers practical recommendations for SME owners, policymakers, and non-technical staff to identify cybersecurity-related vulnerabilities and implement efficient cybersecurity measures.

Keywords: *Cybersecurity readiness, Malaysian organizations, Non-IT SMEs, Organizational barriers, Small and medium enterprises.*

1. Introduction

Cybersecurity can be defined as the application of tools, technologies, processes, and controls to protect and preserve systems, networks, programs, devices, and data from malicious use and cyber-attacks [1]. Cybersecurity has become an increasingly critical issue in current times as more businesses are heavily dependent on IT infrastructure [2]. Small and medium enterprises (SMEs) are more exposed to all sorts of cyber-attacks and data breaches, such as theft of sensitive data, unauthorized access, identity theft, Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS), malicious insiders, man-in-the-middle attacks, hacking, social engineering, spoofing, keylogging, cookies, backdoor trojans, SQL injection, web-based attacks, human error, phishing emails, spear phishing attacks, malware, spam, etc. [2, 3]. Cybercriminals now have more opportunities than ever before, attributed to the digitalization of enterprises, remote labor, and overuse of digital tools and technologies [4, 5]. Non-IT SMEs are more vulnerable because they lack the technical knowledge and adequate infrastructure to counter cyberattacks. Despite the growing body of research and models proposed for cybersecurity measures, various studies show that malware is still evolving and poses a crucial threat to SMEs. Ali et al. [6], highlighting the same issue, investigated the factors that influence the implementation of cybersecurity infrastructure for SMEs, emphasizing the need for adequate

History: Received: 20 May 2026; Revised: 17 July 2026; Accepted: 22 July 2026; Published: 18 August 2026
* Correspondence: zymul_24002432@utp.edu.my

cybersecurity infrastructure to detect and mitigate malware attacks. The study identified and categorized factors into organizational, technical, and environmental challenges, proposing a preliminary model for malware mitigation in Malaysian SMEs. The author identified numerous factors influencing the implementation of cybersecurity infrastructure in SMEs by conducting extensive literature reviews. It emphasizes that SMEs are most vulnerable to malware attacks because of insufficient resources, lack of expertise, lack of effective tools, and lack of awareness, which leads to a high number of cyber incidents. Therefore, having a strong cybersecurity readiness posture is crucial for survival in the digital space.

Organizational cybersecurity readiness refers to "the evaluation of an organization's cybersecurity capabilities to avoid, proactively secure, address, and recover from cyber incidents" [7]. It includes security policies, processes, and procedures implemented in an organization to manage cyber threats [3]. SMEs are the biggest contributors to a country's economy, creating more employment opportunities and significantly contributing to a country's Gross Domestic Product (GDP) [8]. According to studies, SMEs rank among those most susceptible to cyber threats, mainly because of a lack of cyber resilience [9]. Almost 90% of businesses worldwide are SMEs, providing more than 50% of employment opportunities [10]. In Malaysia, SMEs are considered the backbone of the nation's economy [8, 11]. In 2023, 1,101,725 SMEs were recorded in Malaysia, accounting for 96.9% of all businesses [12]. "According to the Malaysia Cybersecurity Insights 2024 report, Ransomware-as-a-Service (RaaS) attacks have increased by 45%, primarily targeting SMEs. Moreover, 72% of Malaysian businesses experienced supply chain attacks in 2022. Malaysia lost approximately USD 9,000 million to cybercriminals between 2002 and 2012, with an average of 30 users being victims of cybercrimes daily [13], and this amount has significantly increased since then. By July 2022, ASEAN had lost USD 2.87 million due to cyberattacks [1]. In 2023, there were 5,917 cyber incidents reported to the Malaysian Emergency Response Team (MyCERT) [14]. In Penang, a technology company called "Exabyte" was targeted and asked for US$900,000 in cryptocurrency [15]. These statistics highlight the growing risks SMEs face in the digital landscape [8].

As more Malaysian businesses accelerate their digital transformation by embracing Web 3.0 and cloud architecture, stronger cybersecurity defenses against enterprise ransomware attacks are fundamentally required [16]. Malaysian companies must stay up to date with digital transformation and maintain a strong cybersecurity infrastructure to boldly enter Web 3.0 and seek growth in the digital era if they are to fully grasp the promise of the country's digital economy.

This study will address these challenges and limitations. By identifying and evaluating the readiness factors and measures, as well as the limitations of cybersecurity infrastructures of SMEs in detecting and mitigating enterprise ransomware attacks, the proposed research study's primary goal is to examine the cybersecurity readiness of Malaysian SMEs. Given that cybercriminals are increasingly choosing Malaysia, it also looks at the impact and adoption of these criteria by Malaysian enterprises to strengthen their cybersecurity infrastructures [17]. These issues will further be addressed in this study, and actionable insights will be generated to improve and strengthen the cybersecurity readiness posture of Malaysian non-IT SMEs as a provided solution.

1.1. Problem Statement

Cybersecurity has become a crucial pillar for businesses and organizations in this digital era. With heavy reliance on the internet for businesses and social activities, cybersecurity readiness has become a significantly important aspect of digital security. With the revolution of digitization and the constant advancements in technology, cyberattacks have also become more prevalent, more sophisticated, and stronger than ever before. Larger organizations keep cybersecurity at the top of their priority list, but Small and Medium Enterprises (SMEs) struggle to comply with complex cybersecurity policies and regulations, mainly because of limited resources, insufficient awareness, and inadequate technical skills. According to recent studies, SMEs face more cybersecurity-related challenges compared to larger organizations and struggle to combat cybercrimes because they lack adequate cybersecurity

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

infrastructure. According to studies, since most large organizations rely on SMEs for their services, attackers typically target SMEs to gain access to larger companies. The average ransomware payment over the last three years was roughly US$250,000, according to IDC. Given their low budgets and inadequate security infrastructure, SMEs find this to be a remarkably outrageous sum. It is more difficult for non-IT SMEs to counter cybercrimes since there is a huge knowledge and awareness gap. IBM reports over 700,000 attacks against SMEs in 2020, which caused approximately $2.8 billion in damages. Recent studies have noted that approximately 85% of Malaysian SMEs have faced cyberattacks, of which 75% have experienced repeated incidents. While many studies have investigated cybersecurity for SMEs, the focus has been on hardware, software, or network level. However, there is a lack of discussion regarding cybersecurity readiness among non-IT SMEs. Not enough research is available on cybersecurity readiness in an organizational context for non-IT SMEs. Specifically, the topic of the Malaysian context in this regard and Malaysian non-IT SMEs is heavily under-researched. Non-IT SMEs could boost their operational efficiency if provided with easy-to-follow guidelines and proper strategies and better defend themselves against cybercrimes. This study explores the barriers that Malaysian non-IT SMEs face in their cybersecurity posture, assesses the organizational cybersecurity readiness infrastructure, and provides implementable insights and practicable recommendations tailored specifically for non-IT Malaysian SMEs to strengthen their cybersecurity readiness posture.

1.2. Research Objectives

1. To explore the infrastructural barriers encountered by Malaysian non-IT SMEs influencing their cybersecurity readiness.
2. To identify the factors contributing to organizational limitations that hinder the cybersecurity readiness posture of Malaysian non-IT SMEs.
3. To suggest strategies to improve the cybersecurity readiness of Malaysian non-IT SMEs.

1.3. Research Questions

1. What are the technical/infrastructural barriers encountered by Malaysian non-IT SMEs affecting cybersecurity readiness?
2. What are the factors contributing to organizational limitations that hinder the cybersecurity readiness posture of Malaysian non-IT SMEs?
3. What strategies can improve the cybersecurity resilience of Malaysian non-IT SMEs?

1.4. Contributions of the Study

This study contributes to the understanding of the cybersecurity readiness posture of Malaysian non-IT SMEs in an organizational context by identifying the barriers and restrictions that hinder the effective implementation of cybersecurity readiness strategies or techniques and proposing context-specific, insightful, implementable improvement strategies as a cybersecurity readiness checklist. Theoretically, this study contributes by expanding the existing literature on cybersecurity readiness in the context of non-IT Malaysian SMEs, which is a topic that remains heavily underexplored. Practically, this study helps SME owners, policymakers, managers, and cybersecurity practitioners understand the major organizational factors influencing cybersecurity readiness, and the findings may assist organizations in developing targeted cybersecurity training programs, allocating resources more accurately for a more efficient cybersecurity readiness posture, and strengthening their internal operational workflow and cybersecurity practices.

1.5. Related Works

1.5.1. Cybersecurity and Cybersecurity Readiness

Cybersecurity and cybersecurity readiness have received significant attention from academicians and researchers in recent years, due to becoming an integral part of business operations in organizations

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

of all sizes and natures [3]. Cybersecurity readiness for organizations could be described as "the assessment of the cybersecurity capabilities of organizations to prevent, prepare for, respond to, and recover from cyber incidents." [18]. In recent years, a considerable number of research studies have been conducted on cybersecurity, and numerous articles have been published about assessing cybersecurity readiness, which reflects the rising importance of needing proactive cybersecurity practices for organizational safety and digital security [19]. To understand the current state of cybersecurity in Malaysia, Chief Chapree [20] and the National Entrepreneur and MSME Development Council [21] discussed three factors that govern cybersecurity protection in Malaysia, i.e., technology, organizational, and human factors. To enhance overall cybersecurity protection, as these factors are deeply interrelated, if one of them gets neglected, the whole cybersecurity posture would collapse. The purpose of this section is to provide a thorough overview of the current state of knowledge on this topic by synthesizing findings and ideas from a few notable research articles. Cybersecurity breaches have become increasingly common against companies at a fast pace [3]. As Malaysia is progressing to develop its digital infrastructure and economy, cybersecurity is becoming increasingly crucial. Non-IT SMEs in Malaysia face the challenge of a lack of adequate resources, knowledge, and expertise, and with the prevalence of cybercrimes, non-IT SMEs immediately need to prioritize cybersecurity readiness, because low awareness of cybersecurity in Malaysian non-IT SMEs is a significant struggle and the risk of falling victim to cyberattacks is far more prominent in non-IT SMEs than in other sectors [14].

1.5.2. Cybersecurity Challenges in Malaysia

According to the Malaysia Computer Emergency Response Team (MyCERT), based on 2021 to 2022 data, a total of 8 comparative categories of attacks occurred in Malaysia, which were vulnerability reports, denial of services, intrusion attempts, spam, fraud, content-related, and malicious codes that happened every month [7]. Studies report that Malaysian businesses faced the most disruptive cyber-attacks in the ASEAN region in 2022. According to Alwashali et al. [22], 44% of SMEs in Malaysia are using cloud computing; however, most of them do not use cloud software ERP to further update and advance their business processes, especially non-IT SMEs, which often have simpler business processes, making them more vulnerable to cyber-attacks. According to a survey conducted by Kappe et al. [2], 40% of the participants stated that the topic of cybersecurity is not dealt with enough in the company. It is apparent that most SMEs do use IT security measures such as backups, firewalls, or two-factor authentication; it is noticed that the level of awareness among companies is substantially low, which can lead them to be more vulnerable to cyber threats [2], which denotes that these small companies are not in a good position to invest in comprehensive security services.

An overview of ransomware attack analysis and its countermeasures is discussed by Sharma and Shanker [23] in a review paper, providing infection mechanisms and effective prevention and mitigation strategies, where the authors highlight that the human factor is a very critical aspect for the organization being attacked, as 59% of infections originate from phishing emails and 24% from malicious websites, which emphasizes the weak link between humans and cybersecurity architecture. The authors painted a picture of the common reasons for ransomware attacks being weak points: lack of regular system vulnerability patches, the absence of adequate security policies, and system vulnerabilities. The study then provides various countermeasures ranging from fundamental preventative strategies for proactive defense, like programmed updates, regular backups, and antivirus installation, to much more advanced techniques, such as utilizing tools for ransomware family detection, deploying honeypots, monitoring system traffic, and monitoring event logs.

A survey conducted by the European Union Agency for Cybersecurity showed that only 10% of SMEs have a formal cybersecurity strategy implemented, while the majority of SMEs rely on outdated basic measures when it comes to cybersecurity. The SMEs that were surveyed were asked about their confidence levels in their cybersecurity preparedness; only 25% considered themselves confident in their ability to counter cyber-attacks, while 45% of SMEs reported being neutral, and 30% indicated lacking confidence [24]. Participants in this study mentioned three key challenges, which are financial

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

constraints (38%), limited technical expertise (32%), and insufficient employee awareness (30%). A lot of research studies emphasize that employees play an important role in cybersecurity risk management [19]. Employee awareness and cybersecurity training programs play an important part in mitigating human-related hazards, such as social-engineering attacks. Recent studies show that, in Malaysia, 48% of cyber incidents were caused by human or administrative errors, with the most frequently breached information being consumer information; 40% of businesses reported a customer file leak, and 35% of businesses were affected by ransomware attacks and malicious email phishing [25]. According to Syauqi et al. [8], SMEs frequently use a logging and alerting system but give less priority to employee awareness training; low levels of physical security increase the risk of cyber-attacks, and sensitive data becomes vulnerable.

A conceptual framework was proposed for Levels of Cybersecurity Controls where SMEs can keep progressing toward Cybersecurity Maturity, lowering Cyber Risks with each level up. The authors Pawar and Palivela [26] in this study conducted a survey among 115 SMEs to assess their current cybersecurity posture according to cybersecurity control implementation. They identified the main challenges that SMEs reported facing as: lack of resources, lack of financial investment, unclear roadmap, too many controls operating in existing frameworks, etc. The authors also argue that many SMEs do not need (or cannot afford) all controls suggested in heavy frameworks; rather, a minimal but effective set of controls (least controls) tailored specifically for SMEs is more practical and convenient to adopt. The proposed solution in this study is termed LCCI (Least Cybersecurity Control Implementation), "a conceptual framework of Levels of Cybersecurity Controls where SMEs can keep proceeding toward Cybersecurity Maturity, lowering Cyber Risks with each level up," designed specifically for SMEs. It identifies the critical assets that are important to their business, then maps those assets to the CIA (Confidentiality, Integrity, Availability) triad to decide which security principles align most with their business. The framework also combines threat-based risk assessment to assess which threats are more relevant to them. The framework is built around multiple 'levels': business-level, administrative-level, and employee-level. It provides tier-based solutions for particular threat types such as phishing, malware, and web-based attacks; a legal component that guides data protection regulations and cyber insurance; a support/community component where SMEs are encouraged to collaborate and share solutions; and a practical tool is also proposed, e.g., a URL classifier to help SMEs identify malicious links and other types of attack vectors. Although the framework is a comprehensive solution, it lacks real-world empirical validation, and pilot studies are suggested. Furthermore, the LCCI might differ across different SME sectors, as each environment might need a different set of controls, so the effectiveness of the LCCI framework remains uncertain, as it has not been validated and its real-world effectiveness remains in doubt.

Discussing the challenges SMEs face, [8] mentions that one of the major challenges for SMEs is the lack of resources and expertise to implement robust cybersecurity systems. Another challenge is a lack of awareness among SME management about the severity of cybersecurity risks, which leaves them ill-equipped to handle cyber-threats effectively. Specifically, non-IT SMEs lack adequate cybersecurity knowledge to employ effective cybersecurity measures. Many SMEs operate on limited budgets, facing financial constraints that prevent them from covering advanced security solutions, staff training, or hiring cybersecurity specialists, which weakens SMEs' overall organizational cybersecurity posture [8]. Several international studies have emphasized that organizational culture significantly influences the effectiveness of cybersecurity policies and practices employed in the company [27].

1.5.3. Cybersecurity Models in the literature

The cybersecurity culture for effective cybersecurity strategy implementation is emphasized immensely in the literature. The NIST Cybersecurity Framework (NIST) is recognized for its comprehensive approach and five primary functions to address cyber incidents: identify, protect, detect, respond, and recover. This framework emphasizes the creation of a cybersecurity culture and highlights incorporating cybersecurity into an organization's broader risk management [19]. Furthermore, the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

ISO/IEC 27001 standard (ISO) offers a systematic approach to information security management, including risk assessment, risk management, and ongoing improvement for information security.

Al-Matari et al. [28] proposed a novel security maturity model, derived from the Information Security Management Maturity Model (ISM3), to categorize organisations into five security levels. The primary objective of the model was to identify and bridge critical cybersecurity gaps relating to talent, technology, financial aspects, organisational units, and management & operations, to measure and enhance an organisation's security status with a structured approach.

Asad and Oscar [29] offer a unique perspective on how SMEs can enhance their cybersecurity resilience while minimizing complexity and cost using a theoretical approach. This study explores the implementation of AI automation strategies in cloud security of SMEs and emphasizes how AI-driven automation, intelligent threat response, and proactive monitoring are key components that can transform the cybersecurity status of SMEs. These components are then described as redefining security by containing breaches, providing continuous visibility, and streamlining critical security operations such as anomaly detection, system patching, firewall configuration, identity management and verification, and data encryption, which makes it more convenient for SMEs to manage their security without extensive resources. While the reported suggested strategies advance understanding of SMEs' need for improving cybersecurity posture, they are also constrained by certain factors that limit the broader applicability of the research, such as the fact that the study does not show any experimental performance metrics or real-world testing of the data; the emphasis that AI can "minimize complexity and cost" is not backed by financial modelling or budgeting guidance; and it outlines generic AI capabilities rather than specifying concrete cloud platforms, AI models, or integration pipelines, leaving practitioners without any technical actionable insights.

Curtin et al. [9] addressed SMEs' limited cybersecurity expertise and resources in their study and highlighted significant gaps in SMEs' cybersecurity practices, revealing that up to 67% of participants do not test their backups, and 83% of participants were unsure of their response in case a cyber incident occurred in Irish SMEs. The authors then proposed an easy-to-understand, user-friendly cyber-risk assessment tool designed for SMEs to enhance their cybersecurity awareness and resilience to counter cyber threats. The authors employed a systematic review methodology to examine existing international risk assessment tools and best cybersecurity practices to form the basis of the tool's development. The tool was developed using an iterative approach, involving co-creation with SME owners who provided feedback to refine the tool's accessibility and relevance. Furthermore, the tool's usability and effectiveness were evaluated through focus groups and surveys with SMEs, allowing for feedback on the tool's effectiveness. The tool's contents were designed, applying thematic coding to analyse cybersecurity guidance documents. The overarching themes of the tool's content included software updates, data backup, access management, antivirus, network security, device management, cloud risk, data security, website and social media security, remote working, third-party risks, cyber-awareness training and culture, cyber incident response and business continuity planning, and cyber governance. The tool simplifies complex cybersecurity concepts into non-technical language to make it accessible for non-experts in SMEs, enhancing the cyber resilience of SMEs by aiding them in identifying specific cybersecurity vulnerabilities through stakeholder engagement and testimony. Although the study provides valuable insights into the current cybersecurity landscape by identifying critical cybersecurity vulnerabilities and areas of risk for SMEs in Ireland, such as data protection and incident preparedness, and the research contributes to the development of a national cybersecurity risk assessment tool for Irish SME owners, despite these contributions, a few limitations restrict the generalisability of the study, such as potential bias from participants volunteering for the study, as they may already be aware of and have an interest in the subject; the presence of a researcher during the user studies, which may hinder the outcome of the activity by participants feeling self-conscious or awkward, as the authors acknowledged in the study; and also the study's proposed risk assessment tool was criticised for being less user-friendly than others because of the need for downloading and the use of technical language.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

In another study, Perozzo et al. [30] addressed the cybersecurity vulnerabilities of SMEs, particularly after the COVID-19 pandemic, and proposed a Cybersecurity Readiness Model (CSRM) to assess SMEs' cybersecurity readiness from a socio-technical systems approach and suggested strategies to strengthen their cybersecurity resilience posture. The study employed a qualitative approach, conducting four semi-structured interviews and adopting a multiple-case-study methodology to evaluate their cybersecurity readiness through the Cybersecurity Readiness Model (CSRM). The analysis included developing individual case reports to derive comprehensive insights from multiple case studies. The study revealed that existing cybersecurity models have various limitations, with some being overly technical and not suitable for SME-specific needs. Interviews conducted during the study identified different stereotypes of SMEs, which can be used as a reference model to understand their cybersecurity posture. The model was applied in a multiple-case-study setting, focusing on three Italian SMEs in the manufacturing sector and demonstrating its practical implications. Although the study contributed greatly to the cybersecurity readiness literature, its findings should be interpreted with caution due to some of its limitations; this study's empirical basis is limited to three Italian companies in the manufacturing sector, which does not encompass all possible business realities inside or outside Italy; further exploration and validation of the Cybersecurity Readiness Model (CSRM) are needed, and the findings cannot be generalized to other sectors because of the focus on the manufacturing sector only.

Collectively, existing literature places significant emphasis on cybersecurity readiness and cybersecurity risk management. However, most cybersecurity advice is presented in a general format, focusing on large organizations or SME in general; thus, the non-IT SME perspective is often overlooked. The literature focuses on generic cybersecurity strategies, and the models discussed in the literature need further validation through testing in diverse organizational cultures. There is limited research on cybersecurity readiness in non-IT SMEs. Moreover, very few studies address the Malaysian context of cybersecurity readiness among non-IT SMEs. This study addresses these research gaps by adopting a qualitative approach to explore the barriers to cybersecurity readiness among Malaysian non-IT SMEs.

2. Methodology

The research methods are selected considering that the exploratory research aims to generate rich qualitative insights. The main aim of this study is to identify the experiences and perspectives of non-IT SMEs and the barriers to cybersecurity readiness. Overall, this study explores the cybersecurity readiness of Malaysian non-IT SMEs, focusing on the organisational context, and suggests actionable insights and guidelines to strengthen the cybersecurity readiness of Malaysian non-IT SMEs. "Unpublished."

2.1. Research Design

This study is part of a larger comparative investigation regarding cybersecurity readiness among Malaysian IT and non-IT SMEs, which uses an exploratory design to concentrate on the research aims. This study primarily focuses on non-IT SMEs only and employs a qualitative method as the overall study. Qualitative research aims to provide context-specific, focused understanding of a phenomenon based on the person experiencing it, without bias and generalization. It provides a deep understanding of a specific case through comprehensive exploratory studies to extract better-quality responses [31, 32]. To further identify cybersecurity readiness among Malaysian non-IT SMEs, an exploratory, qualitative approach was selected. The research paradigm used in this study is interpretivism. To obtain thorough insights into cybersecurity readiness among Malaysian non-IT SMEs, the research questions are also developed utilizing exploratory methodologies, emphasizing context depth above context breadth. As a result, this architecture enables a comprehensive examination of the common causes of organizational constraints and infrastructure impediments and helps produce practical findings that serve as a conceptual foundation and guidelines for SMEs and future research. Since the inductive

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

technique seeks to investigate participant experiences and produce rich, contextual insights from their views rather than testing hypotheses or a preset theory, it is thought to be the most appropriate research methodology for this qualitative study.

This study employed a non-probability sampling methodology known as "Maximum Variation Purposive Sampling," which is a form of purposive sampling technique. Because it allows the researcher to carefully choose respondents who can provide rich, perceptive, and contextual information on difficulties related to enterprise ransomware from SMEs' experiences, this sampling approach is suitable for a qualitative exploratory study such as this one. Participants include non-IT SME employees to obtain a variety of viewpoints regarding the general level of cybersecurity readiness awareness.

The unit of analysis in this study is Malaysian non-IT SMEs functioning across various sectors in Malaysia. Each SME is treated as a single entity; the study focuses on organisational factors affecting cybersecurity readiness rather than individual behaviours alone, hence the selection of SMEs as one unit. Within each SME, the individuals purposely selected for data collection include:

- Head of Department
- Senior Engineer
- Company Owner/CEO
- Managing Director

The study's participant requirements are consistent with the Malaysian government's definition of SMEs. The following standards are used by the SME Corporation Malaysia to define SMEs: the number of employees (all paid workers working at least six hours a day) and sales turnover (total revenue including other earnings) [33]. If a company fits under one of the two designated qualifying criteria, it is considered an SME. SMEs are further divided into two sectors based on the magnitude of their operations:

- In the manufacturing sector, a business is classified as an SME if it has fewer than 200 full-time employees or a sales turnover of less than RM50 million.
- The SME definitions for the service and other industries are as follows: either the number of full-time employees should not exceed 75, or sales turnover should not exceed RM20 million.
- Microenterprises in all sectors have fewer than five full-time employees or a sales turnover of less than RM300,000.

2.2. Participant Inclusion Criteria

- The company is based in Malaysia and fits the country's definition of a small and medium-sized business.
- The participant must work for a non-IT SME in Malaysia.
- The SME's main business is not related to cybersecurity services or IT operations.
- With informed consent, the subject is willing to take part in the study and provide the required information.

To guarantee that the data being gathered is pertinent, trustworthy, and in line with the study's objectives, temporary employees without decision-making authority and organizations that do not fit the national SME requirements were removed. These factors are essential to consider to better understand Malaysian non-IT SMEs' overall cybersecurity readiness landscape and to pinpoint the obstacles and constraints SMEs have when it comes to their organizational cybersecurity readiness.

This study targeted a sample size of approximately 8 SMEs, consisting of four IT SMEs and four non-IT SMEs, which will be sufficient to reach data saturation during thematic analysis. In a qualitative study, a small and purposively selected sample can be implemented with the objective of increasing the depth (in contrast to breadth) of understanding Braun and Clarke [34]. Cheang [35] and Malecki [36] also mentioned that there is no one-size-fits-all approach and that there are several case studies in which

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

they assessed transcripts from previous studies. In one of the cases, they noted code, theme, and development to evaluate whether 6 interviews generated as much data as 12, 18, or 24 interviews.

This study aimed for a sample size of four non-IT SMEs. The goal of a small, purposefully chosen sample in a qualitative study is to increase the depth (as opposed to the breadth) of understanding [34]. Additionally, Cheang [35] and Patricia and Ness [37] cited several case studies in which they evaluated transcripts from earlier research; in one instance, they examined coding topics and development to determine whether six interviews produced as much data as twelve, eighteen, or twenty-four interviews. 73% of the codes were found in the first six interviews, and 92% were found in the first twelve. In another instance, they discovered that the first focus group contained 60% of their 94 codes, the first three groups contained 84%, and the six groups contained 90%. The majority of codes and themes were found in small samples; however, additional examples gave recognized themes more complexity [35].

Each participant was chosen based on their capacity to offer pertinent information about the cybersecurity posture of their companies. No personally identifying information was used to protect participant anonymity; instead, participants were given unique identifiers, such as N-IT1 to N-IT4. In the section that follows, text samples from participant quotes are presented using these identities. The participant classification is shown in Table 1 below.

Table 1.
Participant Classification.

Participant ID	Industry Type	Company Size	No. of Employees
N-IT1	Education	Microenterprise	3
N-IT2	Geospatial Information Technology	Small	10
N-IT3	Pharmaceutical	Small	60
N-IT4	Automotive	Medium	120

2.3. Data Collection and Analysis

Self-administered and open-ended questionnaires were designed to collect data; this method was chosen because of its flexibility, as the open-ended questions allow participants to express their beliefs freely. The questions were designed to identify the factors, measures, infrastructural limitations, and the perception of cybersecurity readiness against ransomware attacks, making it accurate for determining attitudes, beliefs, and practices. The open-ended questionnaire has been formulated by adapting it to the objectives and the participants' positions to get accurate information and identify and allow new themes and patterns to emerge. The questions were divided into categories covering the following factors:

Open-ended, self-administered questionnaires were created to gather data; this approach was selected due to its versatility, as the open-ended questions let participants freely express their opinions. To accurately determine the attitudes, beliefs, and behaviors required, the questions were developed to identify the barriers, infrastructural limitations, and the perception of cybersecurity readiness of non-IT SMEs. To obtain reliable data and to detect and permit the emergence of new themes and patterns, the open-ended questionnaire was developed by tailoring it to the objectives and the positions of the participants. The following factors were covered by the categories into which the questions were divided:

- Adopted preventive measures against ransomware.
- Limitations encountered in the cybersecurity space.
- Employee training.
- Cybersecurity awareness.
- The budget and IT tools utilized.
- Previous experiences with ransomware attacks.
- Coping mechanisms and disaster recovery plans.
- Threat identification.
- Vulnerability assessment.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

Participants were contacted by phone and email, and they received information about the study's objectives. All participants gave their informed consent; ethical guidelines were strictly followed during the data collection process, and data privacy precautions were implemented to ensure participant confidentiality.

Thematic analysis was used to analyse the data. Themes emerged directly from the empirical data through the analysis's inductive methodology. This study's data analysis was carried out using the procedures outlined in the six-phase protocol by Pereira da Silva and Bobbert [38].

The first phase involved reading and rereading the responses to become acquainted with the complete set of data. After importing the raw data files into the qualitative analysis program NVivo, recurrent patterns were found. Creating preliminary codes by methodically arranging the data was the second phase. Since the study did not use pre-established codes, interpretative coding was used in the initial coding phase. The questionnaire responses were then coded line-by-line to extract pertinent data consistent with each research topic [39]. After that, Microsoft Excel was used to create categories using the detected codes.

Following that, related codes were grouped into categories based on the evaluation's objectives. A particular text fragment that represents each code was then labelled for each category, and this label was then recognized as a single theme, while the clustered categories were recognized as sub-themes.

Following the development of the themes, the next stage involved reviewing, refining, and expanding the themes found in the preceding step, as well as carefully re-evaluating whether they made sense considering the study's research questions. Each topic was mapped to pertinent study questions, carefully analyzed, and supported by data from participant answer excerpts. As recommended by the National Institute of Standards and Technology [39], the results of inductive thematic analysis are presented as themes as the primary headings and categories as the sub-headings or sub-themes.

The codes and categories created during the first data analysis utilizing thematic analysis in relation to the study topics for non-IT SMEs are displayed in Table 2.

Table 2.
Code Categorization Table.

Categories	**Codes**
Category 1: Awareness and technical limitations	• Insufficient IT infrastructure • Limited staff training frequency • Attempts at cyber attacks • Poor awareness of advanced technology • Unestablished policies
Category 2: Weak security measures	• No ransomware preventative measures • Lack of automated security systems • Insufficient security filters • Weak disaster recovery plans
Category 3: Financial limitations	• Budgetary constrictions
Category 4: Lack of knowledge and strategic planning	• Lack of advanced knowledge • Overlooking cybersecurity needs
Category 5: Government support for non-IT SMEs	• Cybersecurity training programs by government • Government support through incentives
Category 6: Outsourcing Security	• Protective measures & tools • Outsourcing services to save time
Category 7: Cyber-assessment	• Risk assessment • Vulnerability assessment
Category 8: Need for cybersecurity skills	• Specialized training

2.4. Trustworthiness of the Study

Several tactics were used to increase this study's credibility. The information gathered throughout the study process is triangulated against a variety of data sources, such as comparing replies from various participants in various circumstances and pre-existing information from an evaluation of the literature [27]. Following the initial phase of data collection and analysis, member verification was carried out; informal follow-up correspondence was conducted online with each participant to confirm the precision and reliability of the data interpretations. The goal of these follow-up discussions was to make sure that the information they supplied was appropriately interpreted and represented their viewpoints and experiences. The organizational, technological, and infrastructure elements that surfaced from the preliminary data analysis were open to comments and clarifications from participants. By refining the researcher's interpretations, member checking strengthened the data-gathering and analysis methods employed in this study and increased the reliability of the results. To verify that the interpretations of the results were accurate, the study supervisor also examined how categories, topics, and results were developed [13].

Rich, in-depth descriptions of the individuals and Malaysian non-IT SME context are provided to improve the study's transferability. Because a purposive sampling technique was used, we were able to obtain more accurate and insightful information from the qualitative data answers. The study's findings apply to different contexts to investigate preventive strategies against enterprise ransomware in SMEs, as demonstrated by the comprehensive presentation of the conditions and research settings [13].

Throughout the data gathering and analysis, reliability was guaranteed by upholding a methodical research methodology. To create a clear data audit trail that was routinely examined by the research supervisor, every step of the sampling rationale, coding choices, transcript edits, and theme creation processes was documented and kept in a research journal. To reduce discrepancies and guarantee methodological robustness, the researchers conducted independent coding. The study supervisor also conducted an intercoder assessment of the merged codes and themes.

It is crucial to recognize that the findings and their interpretations in this study are directly derived from the data gathered for the investigation and are not the product of the researcher's imagination. First, during the entire study process, an audit trail was kept, recording all analytical choices and changes. To reduce potential bias throughout the analysis, the researcher used bracketing and reflexive journaling to record any assumptions or preconceptions. To improve confirmability, the research supervisor assessed the coding, topic development, and interpretations. Additionally, the results were bolstered by quotes from participants to show that the interpretations appropriately represented their viewpoints. These metrics confirmed that the study's results were precisely in line with its objectives and research questions.

3. Results and Discussion

The study's conclusions are shown in this section. The research questions this study seeks to address serve as a guide for how the themes are presented. Themes and sub-themes are examined separately under each research question.

The thematic analysis yielded a total of nine themes and fifteen sub-themes emerging from non-IT SMEs. The themes included: (1) Security Exposure due to Infrastructure and Knowledge Gaps, (2) Awareness and Policy Gaps, (3) Restricted Preventive Measures and Recovery Plans, (4) Financial Restrictions, (5) Inadequate Cybersecurity Awareness & Strategic Oversight, (6) Government Initiatives & Incentives for SMEs, (7) Protective & Outsourced Security Solutions, (8) Security Exposure Assessment, and (9) Targeted Cybersecurity Skill Development.

3.1. Thematic Findings Addressing RQ1

Research Question 1 (RQ1): What technical and infrastructural barriers do Malaysian non-IT SMEs encounter that affect cybersecurity readiness?

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

This section presents the three key themes identified under RQ1, discussing the eight sub-themes in detail.

Theme 1: Security Exposure due to Infrastructure & Knowledge Gap

Theme 1 discusses gaps in cybersecurity infrastructure and awareness within non-IT SMEs and highlights the vulnerabilities, limitations, and challenges non-IT SMEs face within their organizations. This theme captures non-IT SMEs' perspectives on cyber risks and weaknesses, lack of cybersecurity awareness, and inadequate infrastructure, comprising the following three sub-themes: (1) Limited IT infrastructure, (2) Limited Staff Training Frequency, and (3) Attempts at cyber-attacks.

Sub-theme 1: Limited IT infrastructure

Sub-theme 1 captures the adoption of IT infrastructure for the organizational operations of non-IT SMEs. It reflects the non-IT SMEs' perspective on implementing IT infrastructure for their cybersecurity needs and highlights their cybersecurity literacy and practices within the organization. When discussing this aspect, N-IT2 expressed:

"We absolutely operate our daily business using an IT infrastructure. Currently, our business employs on-premises systems where we require direct control, specific hardware, or deal with sensitive data. Our office network, including routers, switches, and Wi-Fi access points, is managed in-house to ensure reliable connectivity for all our workstations and devices. Essential office equipment, like multifunction printers and other peripherals, is managed locally."

Consistent with this account, N-IT3 noted:

"We have basic IT infrastructure that comprises traditional desktops, laptops, printers, and scanners. We have a server, but it is used only for quality-control laboratory instrumental-analysis data."

These accounts indicate the adoption of basic IT infrastructure as a foundation for cybersecurity within non-IT SMEs, which reflects their limited level of cybersecurity literacy.

Sub-theme 2: Limited Staff Training Frequency

Sub-theme 2 illustrates the contrast in the occurrence of staff training activities within non-IT SMEs related to cybersecurity, reflecting their cyber awareness. When discussing the aspect of educating the employees and training them about ransomware and cybersecurity threats, N-IT2 stated:

"Every new employee receives mandatory cybersecurity awareness training as part of their initial onboarding process. This covers our core policies, common threats, and how to report suspicious activity, setting the foundation from day one. In response to specific, emerging threats (e.g., a new, highly prevalent phishing scam making the rounds, or a public advisory from a cybersecurity agency), we issue immediate alerts and provide focused guidance or mini-training sessions."

This excerpt from N-IT2 reflects their understanding of the significance of cybersecurity training and the risks of cyber threats. Contrastingly, other SMEs reflected a lack of prioritization of employee awareness and training. N-IT1, when discussing the frequency of employee training within their organization, stated:

"Once a year."

Discussing the same context, N-IT4 similarly noted:

"It is on our yearly training plan (annually)."

N-IT3 in this regard expressed:

"No training is carried out."

These accounts indicate the lack of awareness and prioritization of cybersecurity knowledge within non-IT SMEs. As one SME noted, no training activities are carried out within their organization, while others mentioned annual training activities. Only one SME indicated a higher level of cybersecurity awareness and emphasized the significance of employee training activities.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

Sub-theme 3: Attempts at Cyber-Attacks

This sub-theme emerged across both IT and non-IT SMEs; it describes non-IT SMEs' experiences with cyber-attacks and their approach to handling cyber threats. Discussing their perspectives and experiences with cyber-attacks, N-IT1 expressed:

"We had experience of attacks or spam/scams on our Facebook ad system. They use it to market their products using our FB. They hack the system and deduct the money from our credit card."

This excerpt highlights the SME's experience with cyber threats, discussing the same aspect N-IT2 indicated a good understanding of cybersecurity vigilance against ransomware. N-IT2 expressed:

"Fortunately, we can state that a direct, successful ransomware attack has not occurred at our company that led to data encryption or system compromise. However, we have certainly experienced threats and attempts on a regular basis, which reinforces our understanding and vigilance. We routinely encounter sophisticated phishing emails designed to trick our employees into clicking malicious links or opening infected attachments. These emails often impersonate well-known services, financial institutions, or even internal communications."

These accounts indicate non-IT SMEs' experiences with cyber-attacks, highlighting contrasts in their awareness levels that contribute to security exposure risks.

Theme 2: Awareness & Policy Gaps

Theme 2 reflects non-IT SMEs' cybersecurity awareness and the implementation of cybersecurity knowledge within their organizational security landscape. It demonstrates the different perspectives of non-IT SMEs regarding cybersecurity awareness levels, illustrated in two focused sub-themes: (1) Limited Awareness of Advanced Technology and (2) Unestablished Policies.

Sub-theme 1: Limited Awareness of Advanced Technology

From the perspective of non-IT SMEs, this sub-theme captures their awareness of advanced technologies for implementing a secure cybersecurity status within the organization. When discussing this aspect, N-IT1 mentioned:

"Currently, we use OnPay, Drive, Canva, Facebook, and ChatGPT on our premises. We also use Zoom for online classes."

This excerpt indicates the SME's limited awareness of advanced technology implementation for digital safety needs. Moreover, discussing the implementation of IT infrastructure for cybersecurity needs, N-IT3 expressed:

"We do not really understand the requirements. This makes it complex to begin with."

These accounts indicate the lack of awareness regarding basic or advanced technology within non-IT SMEs, highlighting the limitations they face in implementing adequate cybersecurity infrastructure.

Sub-theme 2: Unestablished Policies

Sub-theme 2 outlines non-IT SMEs' perspectives on organizational policies related to cybersecurity within their organizations. A contrast emerged from this sub-theme; N-IT2 described this aspect as follows:

"While we might not face the same complex regulatory landscape as a large multinational corporation, maintaining a robust framework of policies and adhering to relevant compliance standards is crucial for our risk management and business integrity."

This excerpt suggests a sufficient level of awareness regarding the significance of organizational policies within SMEs for maintaining an adequate digital security infrastructure. Conversely, other non-IT SMEs expressed different perspectives, discussing policy establishment within their organizations; N-IT1 mentioned:

"We don't have any."

Consistent with this account, N-IT3 expressed:

"We have not been regulated yet, but we hope to get regulated in this area. We do not have such a policy in place. We do not have any compliance issues as of now."

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

These accounts indicate a lack of cybersecurity policies within the SME, contributing to organizational limitations within non-IT SMEs.

Theme 3: Restricted Preventative Measures & Recovery Plans

This theme depicts the limited preventative measures adopted within non-IT SMEs for ransomware protection. It illustrates the different perspectives and experiences of non-IT SMEs regarding protective strategies and measures implemented to highlight their organizational cybersecurity preparedness. One of the non-IT SMEs indicated a high level of understanding regarding the adoption of adequate preventative measures, while others articulated alternative views discussing this aspect. N-IT2 mentioned implementing effective and suitable preventative measures. N-IT2 noted:

"To achieve near real-time predictive threat prevention and detection, Automated containment and remediation, AI-Powered Behavioral Analytics is adopted by us for Instantaneous and Immutable Data Recovery with Zero Downtime"

This account suggests relevant preventative measures were taken within the SME; however, this theme is further categorized into three sub-themes to better outline the depth and clarity of the different perspectives of the aspects discussed in it. The sub-themes outlined in this theme are: (1) Insufficient Security Filters, (2) Lack of Automated Security Systems, and (3) No Ransomware Preventative Measures.

Sub-theme 1: Insufficient Security Filters

Sub-theme 1 reflects the limited security filters implemented by non-IT SMEs and highlights the insufficient preventative measures for cybersecurity readiness within non-IT SMEs. Discussing this aspect, N-IT1 noted:

"All of our products have their own passwords."

This excerpt indicates a lack of appropriate cybersecurity awareness related to adopting suitable preventative measures to safeguard the organization in cyberspace. Consistent with this account, N-IT3 expressed:

"For now, we have only antivirus software installed. All our staff have been briefed to avoid opening suspicious emails or communications."

These accounts indicate the insufficient security filters adopted by non-IT SMEs, reflecting the adoption of weak preventative measures for ransomware protection.

Sub-theme 2: Limited Adoption of Automated Security Systems

This sub-theme captures the inadequate strategies and measures implemented by non-IT SMEs; it highlights the lack of proactive and automated security systems within non-IT SMEs. While discussing this aspect, non-IT SMEs mentioned that there is a lack of proactive systems and expressed interest in adopting automated security systems in the future. N-IT2 noted:

"To achieve near real-time predictive threat prevention and detection, Automated containment and remediation, AI-Powered Behavioral Analytics. Instantaneous and Immutable Data Recovery with Zero Downtime. Proactive Cybersecurity Culture Driven by Advanced Training."

This excerpt reflects SMEs' intention to implement automated security systems despite the absence of advanced technologies. Echoing similar views, N-IT4 stated:

"Implement real-time threat detection, periodic infrastructure audits, and simulations."

These accounts indicate the deficiency of automated systems and non-IT SMEs' intentions to implement such technologies in the future to enhance their protective measures for cybersecurity preparedness.

Sub-theme 3: Inadequate Ransomware Preventative Measures

This sub-theme captures the divergent perspectives of non-IT SMEs on ransomware preventative measures. While most non-IT SMEs lacked adequate preventative measures, one indicated appropriate awareness of implementing suitable measures for cybersecurity preparedness. Discussing this aspect, N-IT2 expressed:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

"We evaluate our infrastructure through regular vulnerability assessments and routine health checks of critical systems, ensuring security configurations remain optimal and default settings are hardened."

This account highlighted strong cybersecurity knowledge and the implementation of effective ransomware-prevention measures. Conversely, other non-IT SMEs shared different views while discussing the implementation of effective measures for cybersecurity readiness; N-IT1 expressed:

"We have not done it yet, but are planning to."

Similarly, N-IT3 mentioned:

"We have the infrastructure and desire to implement cybersecurity initiatives. It's just that we do not know where to begin."

These accounts demonstrate varying perspectives on the adoption of preventative measures within non-IT SMEs to prevent ransomware, while only one of the SMEs showed effective implementation of these measures; others reflected a lack of adequate ransomware preventative measures.

3.2. Summary of Themes Under RQ1

The primary themes and particular sub-themes found in non-IT SMEs under research question 1 (RQ1) were summarized in this section. The results showed a range of organizational adoption of cybersecurity implementation and emphasized the viewpoints of non-IT SMEs regarding IT infrastructure and cybersecurity awareness levels, adoption of technology and security landscape policies, and limitations in ransomware prevention measures.

3.3. Thematic Findings Addressing RQ2

Research Question 2 (RQ2): What are the organizational factors that hinder the cybersecurity readiness posture of Malaysian non-IT SMEs?

This section outlines the two key themes and two sub-themes derived in relation to RQ2.

Theme 1: Financial Restrictions

This theme highlights that financial restrictions are a key barrier for non-IT SMEs investing in robust cybersecurity infrastructure. When discussing this aspect, N-IT1 expressed:

"We don't have enough money to cover the cost for the time being."

This excerpt shows that the SME faces financial limitations in fulfilling the organization's needs for investing in robust IT infrastructure. Consistent with this view, N-IT2 mentioned:

"Implementation costs can strain an SME's budget. We need to be very judicious about where we allocate our limited funds. Cybersecurity requires continuous investment in software updates, hardware refreshes, and dedicated manpower. These recurring costs can add up quickly."

These accounts indicate that non-IT SMEs face significant financial challenges in implementing adequate infrastructure. Overall, it is clearly depicted that budgetary limitation is a key barrier for non-IT SMEs investing in robust cybersecurity infrastructure.

Theme 2: Inadequate Cybersecurity Awareness & Strategic Oversight

Theme 2 captures the gaps in cybersecurity awareness within non-IT SMEs. It outlines the limited cybersecurity knowledge that SMEs possess and how it affects the implementation of appropriate strategies. It highlights how a lack of cybersecurity knowledge affects organizational strategies and cybersecurity posture. This theme is further divided into two sub-themes, namely: (1) Lack of Advanced Knowledge and (2) Overlooking Cybersecurity Needs.

Sub-theme 1: Lack of Advanced Knowledge

This sub-theme reflects non-IT SMEs' limited cybersecurity knowledge and the lack of awareness regarding advanced IT tools and technologies, and how this affects an SME's cybersecurity culture. While discussing ransomware and its prevention, utilizing appropriate tools and techniques, N-IT3 stated:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

"We are aware of the idea and only have basic information about ransomware attacks."

This excerpt indicates the SMEs' limited awareness regarding ransomware and its prevention, highlighting a strategic gap. Consistent with this account, when discussing preventative strategies, N-IT4 mentioned:

"Yes, we have an ERP system, email with a specific domain, servers, network, and data sharing."

These accounts reflect that non-IT SMEs' delineated basic knowledge of IT infrastructure and preventative strategies highlights the lack of advanced cybersecurity knowledge within non-IT SMEs.

Sub-theme 2: Overlooking Cybersecurity Needs

Sub-theme 2 captures non-IT SMEs' tendency to deprioritize and underestimate cybersecurity requirements within their organizations. Most non-IT SMEs indicated that cybersecurity was not viewed as an urgent concern proactively and was often overlooked due to other operational priorities. Discussing the aspect of incorporating cybersecurity into organizational planning and the importance of implementing cybersecurity infrastructure, N-IT1 stated:

"We haven't done it yet."

This excerpt indicates a lack of prioritization and urgency regarding cybersecurity needs. Echoing similar views on cybersecurity requirements within the organization, N-IT3 expressed:

"As we have not started anything yet, we would also like to weigh the costs and their implications for the total bottom line before implementation."

These accounts reflect that cybersecurity was treated as a secondary consideration rather than an integral component and a top priority within an organizational context of non-IT SMEs.

3.4. Summary of the Themes Under RQ2

The main topics and sub-themes from non-IT SMEs that were pertinent to research question 2 (RQ2) were outlined in this section. The results showed gaps in the adoption of sufficient cybersecurity infrastructure and emphasized the cybersecurity knowledge and awareness of non-IT SMEs, as well as their viewpoint on budgetary constraints and the organization's adoption of cybersecurity strategies. The non-IT SMEs revealed gaps in organizational cybersecurity strategy and financial resources, as well as a lack of advanced cybersecurity knowledge and limited understanding of the deployment of advanced tools and procedures.

Thematic Findings Addressing RQ3

Research Question 3 (RQ3): What strategies can improve the cybersecurity resilience of Malaysian non-IT SMEs?

This section presents four themes derived from non-IT SMEs under Research Question 3, comprising five context-specific sub-themes.

Theme 1: Government Initiatives & Incentives for SMEs

This theme highlights the role of government initiatives and financial support in non-IT SMEs' cybersecurity adoption. SMEs mentioned that programs led by the government, such as grants, training sessions, awareness campaigns, and subsidies, help non-IT SMEs alleviate resource constraints and invest in security solutions to enhance the cybersecurity posture within the organization. Discussing the aspect of government involvement through incentives for non-IT SMEs' cybersecurity robustness, N-IT3 mentioned the important factors that need investment as:

"The most important requirement for creating a robust system is gaining and sharing knowledge. Subsequently, it is important to maintain and upgrade it constantly."

This excerpt indicates that government initiatives play a critical role in enhancing non-IT SMEs' cybersecurity readiness. Furthermore, these aspects are discussed in two sub-themes, namely: (1) Cybersecurity Training Programs by the Government and (2) Government Support through Incentives.

Sub-theme 1: Cybersecurity Training Programs by the Government

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

This sub-theme underscores the importance of government-provided cybersecurity training programs as crucial to enhancing non-IT SMEs' cybersecurity awareness and technical capabilities. Discussing this aspect, N-IT1 expressed:

"Non-IT organizations would benefit from more accessible cybersecurity training programs and guidelines tailored to their industry."

Consistent with this view, N-IT4 mentioned:

"Non-IT SMEs would benefit from subsidized access to cybersecurity audits and training programs."

These accounts indicate that non-IT SMEs acknowledged that government-led programs offered structured learning opportunities and updated knowledge of current cybersecurity trends, which highlighted non-IT SMEs' perspective on government cybersecurity training programs as a positive contributing factor in enhancing their organizational cybersecurity preparedness.

Sub-theme 2: Government Support through Incentives

This sub-theme highlights the role of government-provided incentives in encouraging non-IT SMEs to invest in appropriate cybersecurity measures. SMEs mentioned that government support through subsidies, grants, and tax relief reduces the cost burden associated with cybersecurity infrastructure implementation and provides relief to non-IT SMEs from the existing budgetary constraints they face. Discussing this aspect, N-IT1 expressed:

"Government support through incentives for cybersecurity investments and stronger regulations could also drive more companies to prioritize security."

Consistent with this view, N-IT2 also noted:

"As a non-IT organization, we critically depend on external support to strengthen our cybersecurity posture. Direct financial assistance from government agencies or matching grants specifically for cybersecurity investments would help."

These accounts indicate that government support through incentives was perceived to encourage non-IT SMEs to prioritize and invest in robust cybersecurity infrastructure.

Theme 2: Protective & Outsourced Security Solutions

Theme 2 highlights non-IT SMEs' reliance on outsourced services and adopted protective measures to manage security threats. SMEs mentioned using external security solutions by adopting third-party services and outsourcing services that required specialized knowledge or training. However, a contrast was observed among the SMEs: specific SMEs mentioned facing budgetary constraints in adopting third-party services and implementing relevant protective measures, while some mentioned an interest in implementing such measures in the future. This aspect is further discussed in two sub-themes, which are: (1) Outsourcing Services to Save Time, and (2) Protective Measures & Tools.

Sub-theme 1: Outsourcing Services to Save Time

This sub-theme describes non-IT SMEs' reliance on external outsourced services to save time and reduce operational burden within the organization. A contrast was noticed in non-IT SMEs' perspectives on outsourcing services to enhance cybersecurity preparedness. Discussing this aspect, N-IT2 expressed:

"Yes, we typically outsource services that require continuous monitoring, specialized knowledge, or significant infrastructure. Implementing and managing cybersecurity measures takes time away from immediate business objectives, which can be a struggle for busy teams in a fast-paced environment."

This excerpt indicates the use of external, third-party services to reduce time constraints and enhance operational efficiency. Conversely, another excerpt discussing this aspect stated:

To begin with, we may outsource it to an external service provider or vendor, as we are not subject-matter experts and do not have thorough knowledge in-house.

These accounts indicate a contrast in outsourcing external services, as some SMEs indicated a low level of awareness regarding cybersecurity, while others highlighted outsourcing services to save time as an efficient strategy to enhance the organizational cybersecurity posture within non-IT SMEs.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

Sub-theme 2: Protective Measures & Tools

This sub-theme captures how non-IT SMEs adopted technical measures and tools to safeguard their organizations' cybersecurity posture. SMEs mentioned using firewalls, antivirus software, cloud infrastructure, and regular backups to prevent and mitigate cyber incidents. Discussing this aspect, N-IT2 expressed:

"Regular Backups, Offsite/Cloud Backups, Offline Backups (Air-Gapped), Antivirus and Anti-Malware, Firewall protection, and Email Security Gateway/Filtering."

However, a contrast was observed in the adoption of protective measures. As mentioned in previous sections, some non-IT SMEs indicated that adopting preventative measures was essential to supporting a robust cybersecurity operational environment within the organization.

Theme 3: Security Exposure Assessment

This theme focuses on non-IT SMEs' organizational practices in identifying and evaluating potential vulnerabilities within their systems. SMEs mentioned conducting regular audit trails, routine health checks, and risk assessments within their organization to assess their operational efficiency. Discussing the aspect of exposure assessment for potential threat checks, N-IT4 stated:

"It is part of our business risk management monitoring."

This excerpt indicates that fundamental evaluation metrics are considered within non-IT SMEs. This aspect is further discussed through a single sub-theme: (1) Risk & Vulnerability Assessment.

Sub-theme 1: Risk & Vulnerability Assessment

This sub-theme highlights the importance of regular security assessments by prioritizing, identifying, and analyzing cybersecurity risks within the organization's systems and operations. SMEs mentioned planning digital activities according to the organization's cybersecurity priorities, conducting regular risk assessments, and configuring systems according to the organization's cybersecurity needs. Discussing this aspect, N-IT2 expressed:

"Yes, our organization at least considers cybersecurity in the planning of new digital activities or systems. Before committing to a new system, we conduct an initial assessment to identify potential cybersecurity risks. We evaluate our infrastructure through regular vulnerability assessments and routine health checks of critical systems, ensuring security configurations remain optimal and default settings are hardened."

This account indicates that non-IT SMEs perceive routine risk and vulnerability assessment as essential for effective risk management and proactive cybersecurity preparedness.

Theme 4: Targeted Cybersecurity Skill Development

This theme captures non-IT SMEs' focus on prioritizing specialized training and targeted cybersecurity skill development to strengthen organizational cybersecurity robustness. Although, as mentioned in the previous sections, a contrast was observed in non-IT SMEs' staff-training priorities, the organizations acknowledged the importance of specialized cybersecurity training for skill development and enhancing employees' cybersecurity capabilities. Discussing this aspect, N-IT2 expressed:

"Every new employee receives mandatory cybersecurity awareness training as part of their initial onboarding process. This covers our core policies, common threats, and how to report suspicious activity, setting the foundation from day one."

This account indicates that such targeted cybersecurity skill development and focused training were perceived to enhance organizational security efficiency and reduce vulnerabilities associated with staff skill gaps.

3.5. Summary of the Themes Under RQ3

The primary themes and particular sub-themes found in non-IT SMEs under RQ3 were summarized in this section. The results showed that protective and outsourced security solutions, security exposure assessments, and targeted cybersecurity skill development are essential measures to be implemented within non-IT SMEs to enhance organizational cybersecurity capabilities. They also revealed that government initiatives for SMEs are critical to developing cybersecurity capabilities of

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

non-IT SMEs. The organizations recognized the implementation aspects and identified government measures as crucial for non-IT SMEs' cybersecurity development, despite the fact that there was a disparity in cybersecurity awareness among non-IT SMEs.

4. Discussion

Using a qualitative thematic approach, this study identified the barriers to cybersecurity readiness among a limited number of Malaysian non-IT SMEs and highlighted variations in how they experience cybersecurity readiness in an organizational setting. Figure 1 summarizes the barriers to cybersecurity readiness among non-IT SMEs in a barrier model, as shown below.

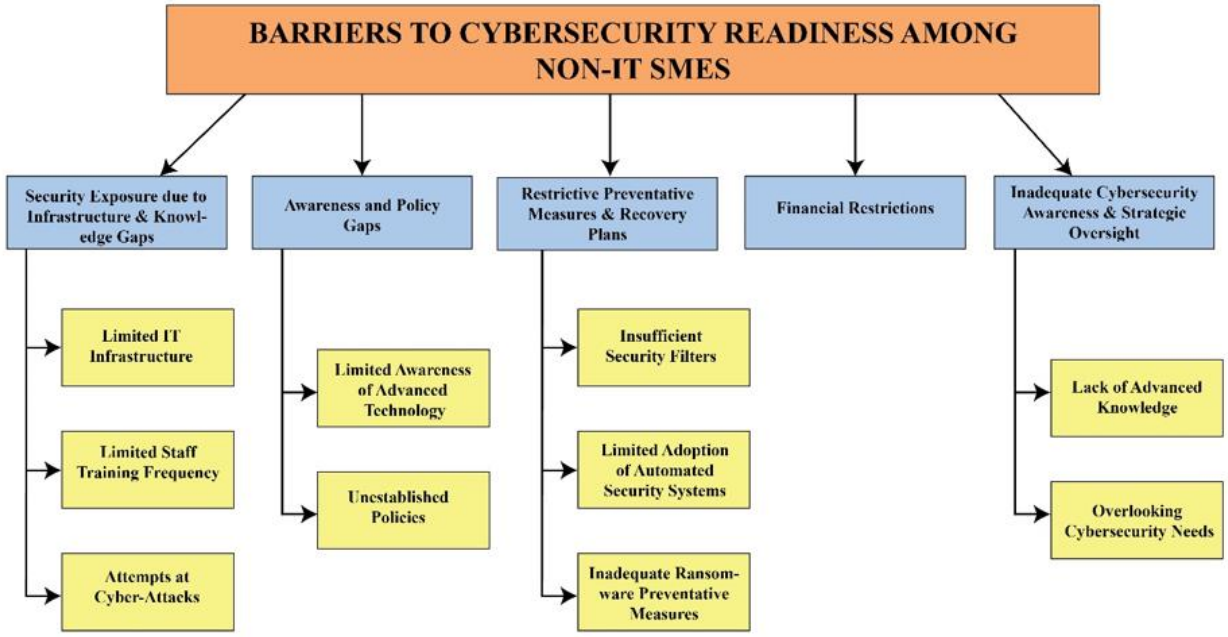

Figure 1.
Barrier Model.

In relation to RQ1, several barriers were noted, including limited staff-training frequency within SMEs, a lack of advanced cybersecurity knowledge, and resource and capacity constraints. However, the predominance of the themes restrictive preventative measures and recovery plans, awareness and policy gaps, and strategic oversight highlights how inadequate employee awareness regarding cybersecurity weakens the organizational security posture because non-IT SMEs with less awareness of cyber threats tend to fall into ransomware traps more easily because they lack the necessary human error is a critical weak link between humans and cybersecurity architecture [40]. The relationship between insufficient cybersecurity awareness and strategic oversight security exposure due to infrastructure and knowledge gaps points to a vicious cycle in which a lack of expertise discourages proactive strategy implementation. This is consistent with Kappe et al. [2], who found that SMEs with low awareness were reactive rather than proactive in strategy implementation, and Huzaizi et al. [25], which emphasizes that having a solid understanding of cybersecurity is essential for businesses to use effective cybersecurity strategies.

Regarding RQ2, the results show that financial constraints are a common cause of inadequate cybersecurity infrastructure and strategies in non-IT SMEs. SMEs with financial constraints reported that their tight budgets prevent them from investing in strong cybersecurity technologies, which is the primary cause of non-IT SMEs' inadequate preventive measures, as McBride [41] identified a lack of

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

resources and financial investment as the primary challenges that SMEs face. In other words, non-IT SMEs reported having an unclear roadmap and a lack of cybersecurity investment planning within the organization, which is consistent with what [41] discussed regarding some of the main challenges faced by SMEs. Non-IT SMEs clearly reported having no budget assigned for cybersecurity, which stems from two reasons: one is having a lower level of awareness compared to IT SMEs regarding cybersecurity, which results in non-IT SMEs having no idea where or how to invest in cybersecurity.

Regarding RQ3, practically speaking, the results indicate that non-IT SMEs should implement cybersecurity awareness programs for technical training centred on risk management and cybersecurity-related decision-making. By highlighting the significance of organizational prioritization and managerial decision-making on cybersecurity practices across Malaysian SMEs, this study theoretically expands the literature on cybersecurity readiness. The current findings emphasize the dangers and constraints of adopting a reactive approach to cybersecurity preparation and recommend the deployment of proactive cybersecurity measures, whereas previous research mostly concentrated on technical controls and compliance methods.

The breadth of this study is limited by a few restrictions, which should be taken into account despite its methodological robustness. First, the study is derived from a wider investigation on cybersecurity readiness of Malaysian IT and non-IT SMEs and used a multi-variation purposive sampling strategy with a comparatively small sample size of four non-IT SMEs. The study's target population, which consists of a small number of Malaysian non-IT SMEs, is highly specialized and narrowly defined, which may limit the findings' applicability in different contexts. However, rather than reaching statistical generalization, this strategy was in line with the exploratory nature of the study, which seeks to obtain in-depth, context-specific insights on an understudied topic. Second, because the data were gathered using self-administered, open-ended questionnaires based on participants' self-reported experiences and perceptions, personal bias may be introduced because respondents may give answers that are socially acceptable. Participants were encouraged to express their opinions honestly and impartially in order to reduce the possibility of personal bias, which increased the data's reliability. Third, the results may not be as applicable to other industries or nations due to the regulatory, cultural, and organizational characteristics unique to Malaysian non-IT SMEs. Additionally, only a few organizational characteristics were taken into account, mostly due to the reluctance of businesses that are subject to enterprise ransomware attacks to disclose their organization's profile or attack data. However, the limitations are a feature of qualitative research and are consistent with the study's objectives, which were to obtain a deep, comprehensive understanding of participants' perspectives rather than to produce results that could be applied broadly. Finally, the study's findings are exploratory, and instead of producing results that are generally applicable, the exploratory, context-specific findings are meant to offer enhanced analytical insights that may be useful in similar contexts like Malaysian non-IT SMEs.

The study recommends that appropriate incident management and recovery plans, such as timely incident response, incident documentation and review, backup, and disaster recovery mechanisms, should be essential components of cybersecurity practices as defined by Jamaludin et al. [7] based on five core functions: identify, protect, detect, respond, and recover. This is also covered by Alwashali et al. [22] in their incident management plan, which consists of the following: a, preparation; b, detection; c, analysis and containment; and d, recovery, if ransomware is detected. Considering the uneven implementation of cyber strategies by SMEs, implementing automated security systems, centralized visibility systems across all networks, continuous system monitoring, and regular security updates and checkups within routine operations, as suggested by Kasih [1], the findings highlight the need for proactive cybersecurity approaches and operational governance. By redefining security by containing breaches, providing continuous visibility, and streamlining critical security operations like anomaly detection, system patching, firewall configuration, identity management and verification, and data encryption, it becomes easier for SMEs with limited resources to manage their security without making significant resource investments. SMEs should prioritize cybersecurity awareness and resource

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

investment in security infrastructure for a safe and sound cyberspace in accordance with the awareness and knowledge gaps. This is in line with Malaysia's cybersecurity resilience goals, which are defined in Gupta and Ramteke [42] as "Strengthen community-level cybersecurity awareness, literacy, and resilience" and "Integrate cybersecurity education across all levels of education," as also mentioned by Young and Casey [43]. According to some surveys, 90% of people are unfamiliar with the term. Given the cybersecurity exposure, SMEs should conduct security exposure assessments on a regular basis because ransomware attacks are more frequent in SMEs with unaddressed vulnerabilities. This aligns with one of the strategic goals in Gupta and Ramteke [42], which is defined as "Strengthen cybersecurity maturity capability and cyber risk management." This aspect is also covered by Mukhopadhyay and Jain [40]. Common causes of ransomware attacks include weak points in systems, a lack of regular system vulnerability patches, inadequate security policies, and system vulnerabilities. As a result, SMEs must continuously assess vulnerabilities to limit security exposure. And lastly, specifically, non-IT SMEs should focus on the basics of cybersecurity readiness first and then slowly and continually progress towards advanced cybersecurity measures, starting slowly with investing in protective and outsourced security solutions, investing in and building the base for cybersecurity readiness, like outsourcing protective tools and services from trusted third-party SaaS vendors to save time and operational burden, as defined by ISO/IEC 27001, focusing on establishing, maintaining, and continually improving an information security management system. Enitan [24] also suggested, as suggested by McBride [41], in their proposed solution called LCCI (Least Cybersecurity Control Implementation). Table 3 summarizes the actionable guidelines presented for enhancing cybersecurity readiness to prevent ransomware attacks among Malaysian SMEs.

Table 3.
Summary of the Actionable Guidelines.

Guidelines	Target Actor	Linked Theme
Integrate robust security infrastructure	SME owners	Security exposure due to infrastructure and knowledge gap
Regulate incident management plans	SME managers	Restrictive preventative measures and recovery plans
Prioritize proactive cybersecurity approach	SME owners, policymakers	Inadequate cybersecurity awareness and strategic oversight
Promote cybersecurity awareness and resource investment	Policymakers, SME managers, and government institutes	Security exposure due to infrastructure and knowledge gaps
Perform security exposure assessments	SME managers/directors	Inadequate cybersecurity awareness and strategic oversight
Facilitate protective and outsourced security solutions	SME owners	Restrictive preventative measures and recovery plans

5. Conclusion

Using a qualitative thematic analysis approach, this study examined the barriers to cybersecurity readiness among Malaysian non-IT SMEs in an organizational context, identified the organizational and infrastructure barriers and limitations Malaysian non-IT SMEs face, and offered actionable recommendations to improve cybersecurity readiness for Malaysian non-IT SMEs. The results showed that organizational, technological, and human variables all work together to shape an organization's cybersecurity readiness. The constraints and inadequacies that Malaysian SMEs encounter regarding awareness, tools, technology, strategies, policies, resources, and budget were brought to light by this study. Additionally, it outlined the significance of resource-driven decision-making, managerial knowledge, and organizational prioritization in enhancing the cybersecurity preparedness of non-IT SMEs. This study provides qualitative, in-depth insights from an understudied context to the literature and advances a more nuanced understanding of cybersecurity readiness in resource-constrained situations by providing rich, context-specific insights for Malaysian non-IT SMEs. While the study offers insightful information about organizational cybersecurity preparedness, a number of limitations

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459

may affect the findings' generalizability and transferability. One of the study's main limitations is that its findings are exploratory and context-specific to a small number of Malaysian SMEs. Additionally, the suggested guidelines are not validated through practical implementation and must be tested in real-world scenarios in order for the findings to be verified, which restricts the study's transferability, dependability, and generalizability. Despite the aforementioned constraints, this study offers insightful and relevant information about the cybersecurity preparedness of a limited number of Malaysian non-IT SMEs. To the best of our knowledge, this is the first exploratory study that identifies the barriers to cybersecurity readiness specifically for Malaysian non-IT SMEs. Overall, by highlighting the significance of organizational perception among a small number of Malaysian non-IT SMEs, this study adds to the body of literature on cybersecurity readiness. It also offers practical recommendations for SME owners, policymakers, and non-technical staff to identify cybersecurity-related vulnerabilities and implement efficient cybersecurity measures in SMEs. In particular, future research should use a mixed-methods approach to assess the generalizability of the themes discovered across a larger non-IT SME population with a larger sample size. Our study indicates several significant possibilities for future research and practice. Longitudinal studies could also examine how Malaysian non-IT SMEs' cybersecurity preparation procedures change over time in response to the changing technology environment. Furthermore, more investigation is required to verify the conceptual models' validity for the "best practices" for Malaysian SMEs' cybersecurity preparedness. Overall, the results highlight how crucial it is to include cybersecurity considerations in a larger organizational context with strategic prioritization in order to improve resilience against the ever-changing landscape of cyber threats.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Acknowledgments:

Ethical approval to conduct the research involving human participation during the data collection and interview session was granted by the university at the beginning of the research project.
We would like to acknowledge the Centre for Graduate Studies, Universiti Teknologi PETRONAS (UTP) for partially funding this research paper and publication.

Copyright:

References

[1] M. C. Kasih, "Fostering ASEAN's digital future through cybersecurity policies and human empowerment," Policy Brief, Economic Research Institute for ASEAN and East Asia (ERIA), Jakarta, Indonesia, 2023.

[2] M. Kappe, R.-C. Härting, C. Karg, and D. Deffner, "Cybersecurity in SMEs–drivers of cybercrime, insufficient equipment and prevention," *Procedia Computer Science*, vol. 225, pp. 3631-3640, 2023. https://doi.org/10.1016/j.procs.2023.10.358

[3] M. H. Shah, R. Muhammad, and N. Ameen, ""Cybersecurity readiness of e-tail organisations: A technical perspective," in *Information and Communication Technology for Sustainable Development: Proceedings of ICT4SD 2020, vol. 12066, Lecture Notes in Computer Science*, 2020.

[4] P. F. Tamyez, *The challenges and solutions of cybersecurity among Malaysian companies. Industry 4.0 and hyper-customized smart manufacturing supply chains.* Hershey, PA, USA: IGI Global Scientific Publishing, 2019.

[5] National Cyber Security Agency, *Malaysia cyber security strategy 2025–2030.* Kuala Lumpur, Malaysia: National Cyber Security Agency, National Security Council, Prime Minister's Department, 2025.

[6] A. B. A. Ali, R. K. Ayyasamy, R. Akbar, V. Ap Ponnusamy, and L. E. Heng, "Cybersecurity infrastructure adoption model for malware mitigation in small medium enterprises (sme)," in *2022 IEEE 5th International Symposium in Robotics and Manufacturing Automation (ROMA) (pp. 1-6). IEEE*, 2022.

[7] N. Jamaludin, U. A. Rauf, and N. Awang, "Awareness of cybersecurity: A case study in a logistics organizations," *JOIV: International Journal on Informatics Visualization*, vol. 9, no. 2, pp. 753-760, 2025. https://dx.doi.org/10.62527/joiv.9.2.3349

[8] M. Syauqi *et al.*, "Cybersecurity threats among SMEs in Malaysia: Risks and challenges," *Journal of Information and Knowledge Management*, vol. 15, no. SI1, pp. 218–225, 2025.

[9] M. Curtin, B. Sheehan, M. Gruben, G. O'Carroll, and H. Murray, "Enhancing cybersecurity awareness in small and medium enterprises through a user-friendly risk assessment tool," in *2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P) (pp. 209-226). IEEE*, 2025.

[10] G. Guest, E. Namey, and M. Chen, "A simple method to assess and report thematic saturation in qualitative research," *PloS One*, vol. 15, no. 5, p. e0232076, 2020. https://doi.org/10.1371/journal.pone.0232076

[11] International Organization for Standardization, *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, 3rd ed. Geneva, Switzerland: International Organization for Standardization, 2022.

[12] SME Corporation Malaysia, "SME definition. SME Corp. Malaysia," 2013. https://www.smecorp.gov.my

[13] N. S. M. Mizan, M. Y. Ma'arif, N. S. M. Satar, and S. M. Shahar, "CNDS-cybersecurity: Issues and challenges in ASEAN countries," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1.4, pp. 1-7, 2019. https://doi.org/10.30534/ijatcse/2019/1781.42019

[14] N. Ghazali, I. Suryani, and S. Z. S. Idrus, "Challenges and opportunities of cybersecurity education for non-technical majors," *Journal of Communication in Scientific Inquiry (JCSI)*, vol. 6, no. 1, pp. 47-55, 2024. https://doi.org/10.58915/jcsi.v6i1.873

[15] M. Carlton and Y. Levy, "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals," in *SoutheastCon 2015 (pp. 1-6). IEEE*, 2015.

[16] R. A. Ross, "The ongoing threat of ransomware to small businesses: A qualitative case study on the impediments to the application of preventative, detective, and corrective controls," Ph.D. Dissertation, Northcentral University, 2023.

[17] A. Ganesin, L. Supayah, and J. Ibrahim, "An overview of cyber security in Malaysia," *Arabian Journal of Business and Management Review*, vol. 6, no. 4, pp. 12-20, 2016. https://doi.org/10.65453/ajbmr.v6i4.956

[18] S. Campbell *et al.*, "Purposive sampling: Complex or simple? Research case examples," *Journal of Research in Nursing*, vol. 25, no. 8, pp. 652-661, 2020. https://doi.org/10.1177/1744987120927206

[19] J. Parsola, "Cybersecurity risk assessment and management for organizational security," *NeuroQuantology*, vol. 20, no. 5, pp. 5330–5337, 2022. https://doi.org/10.48047/nq.2022.20.5.nq22815

[20] Chief Chapree, "Exabytes falls victim to ransomware attack: Causes disruptions to certain services. Lowyat.net," 2021. https://www.lowyat.net/2021/253244/exabytes-ransomware-attack/

[21] National Entrepreneur and MSME Development Council, *MSME insights 2023/24*. Kuala Lumpur, Malaysia: SME Corp. Malaysia, 2024.

[22] A. A. M. A. Alwashali, N. A. Abd Rahman, and N. Ismail, "A survey of ransomware as a service (RaaS) and methods to mitigate the attack," in *2021 14th International Conference on Developments in eSystems Engineering (DeSE) (pp. 92-96). IEEE*, 2021.

[23] N. Sharma and R. Shanker, "Analysis of ransomware attack and their countermeasures: A review," presented at the 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022.

[24] O. I. Enitan, "Enhancing cybersecurity readiness in SMEs: Addressing resource constraints and policy gaps through scalable solutions and IT investments," *International Journal*, vol. 14, no. 1, pp. 1–6, 2025. https://doi.org/10.30534/ijmcis/2025/011412025

[25] A. H. A. Huzaizi, S. Tajuddin, K. A. Bahari, K. A. Manan, and N. N. Abd Mubin, "Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs," *Asian Culture and History*, vol. 13, no. 2, pp. 1-20, 2021. https://doi.org/10.5539/ach.v13n2p20

[26] S. Pawar and H. Palivela, "LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)," *International Journal of Information Management Data Insights*, vol. 2, no. 1, p. 100080, 2022. https://doi.org/10.1016/j.jjimei.2022.100080

[27] F. D. Orellana, "Cybersecurity incident response capabilities in the Ecuadorian small business sector: A qualitative study," Ph.D. Dissertation, Northcentral University, 2020.

[28] O. M. Al-Matari, I. M. Helal, S. A. Mazen, and S. Elhennawy, "Adopting security maturity model to the organizations' capability model," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 193-199, 2021. https://doi.org/10.1016/j.eij.2020.08.001

[29] F. Asad and E. Oscar, "Building secure clouds for SMEs: AI automation, threat response, and proactive monitoring," 2025. https://doi.org/10.13140/RG.2.2.13671.56485

[30] H. Perozzo, A. Ravarini, and F. Zaghloul, "Assessing cybersecurity readiness within SMEs: Proposal of a socio-technical based model," presented at the Int. Workshop on Socio-Technical Perspective in Information Systems Development (STPIS), 2022.

[31] H. H. Alharahsheh and A. Pius, "A review of key paradigms: Positivism VS interpretivism," *Global Academic Journal of Humanities and Social Sciences*, vol. 2, no. 3, pp. 39-43, 2020.

[32] A. Georgiadou, S. Mouzakitis, K. Bounas, and D. Askounis, "A cyber-security culture framework for assessing organization readiness," *Journal of Computer Information Systems*, vol. 62, no. 3, pp. 452-462, 2022. https://doi.org/10.1080/08874417.2020.1845583

[33] H. K. B. Mustafa, "Managing operational risk among SMEs: The Malaysian perspective," Ph.D. Dissertation, Universiti Utara Malaysia, 2021.

[34] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006. https://doi.org/10.1191/1478088706qp063oa

[35] S. Cheang, "Conceptual model for cybersecurity readiness assessment for public institutions in developing country: Cambodia," presented at the 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009.

[36] F. Malecki, "Best practices for preventing and recovering from a ransomware attack," *Computer Fraud & Security*, vol. 2019, no. 3, pp. 8-10, 2019. https://doi.org/10.1016/S1361-3723(19)30028-4

[37] I. Patricia and L. R. Ness, *Are we there yet? Data saturation in qualitative research.* Minneapolis, Minnesota, USA: Walden Faculty and Staff Publications, 2015.

[38] A. D. Pereira da Silva and Y. Bobbert, "Cybersecurity readiness: An empirical study of effective cybersecurity practices for industrial control systems," *Scientific Journal of Research and Reviews*, vol. 2, no. 3, 2019. https://doi.org/10.33552/SJRR.2019.02.000536

[39] National Institute of Standards and Technology, *The NIST cybersecurity framework (CSF) 2.0.* Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024.

[40] A. Mukhopadhyay and S. Jain, "A framework for cyber-risk insurance against ransomware: A mixed-method approach," *International Journal of Information Management*, vol. 74, p. 102724, 2024. https://doi.org/10.1016/j.ijinfomgt.2023.102724

[41] D. Y. McBride, "An analysis of cybersecurity curriculum designs, workforce readiness skills, and applied learning effectiveness," Ph.D. Dissertation, Capitol Technology University, 2021.

[42] N. Gupta and V. Ramteke, "A study on defacing ransomware: Are we aware and ready?," *International Journal of Computer Science and Information Technologies*, vol. 8, no. 2, pp. 311–317, 2017.

[43] D. S. Young and E. A. Casey, "An examination of the sufficiency of small qualitative samples," *Social Work Research*, vol. 43, no. 1, pp. 53-58, 2019. https://doi.org/10.1093/swr/svy026

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 8: 105-128, 2026
DOI: 10.55214/2576-8484.v10i8.13459