Cyber Risk Analysis and Causal Factors Influence the Cybersecurity Readiness Capability for Small and Medium Enterprises in Thailand

Wilas Witheeprai , Prasan Wongkitisopon , Chanapatt Pattaramaetakul , Benjaporn Sathanarugsawait , Prasong Praneetpolgrang *

Posted Date: 3 July 2025

doi: 10.20944/preprints202507.0267.v1

Keywords: cyber risk; cybersecurity; small and medium enterprises (SMEs); cybersecurity readiness

 doi:10.20944/preprints202507.0267.v1

Article

Cyber Risk Analysis and Causal Factors Influence the Cybersecurity Readiness Capability for Small and Medium Enterprises in Thailand

Wilas Witheeprai, Prasan Wongkitisopon, Chanapatt Pattaramaetakul, Benjaporn Sathanarugsawait and Prasong Praneetpolgrang *

School of Information Technology, Sripatum University, Bangkok 10900

* Correspondence: prasong.pr@spu.ac.th

Abstract

This research examines the challenges faced by Small and Medium Enterprises (SMEs) in Thailand concerning cybersecurity, primarily stemming from resource limitations that impair their capacity to effectively mitigate cyber threats. Such constraints often result in heightened vulnerability to cyber attacks, underscoring need for a comprehensive understanding of risk landscape. To achieve this, study employs Fuzzy Analytic Hierarchy Process, engaging fifteen experts to evaluate and prioritize the key categories of cyber risks encountered by SMEs. The analysis reveals that financial risks constitute the most critical concern, followed by operational, regulatory, human-related, and reputational risks. Utilizing Structural Equation Modeling, the study identifies technology readiness as the most influential factor, with organizational processes and human factors also playing significant roles. Additionally, Exploratory Factor Analysis is applied to develop a measurement scale for cybersecurity readiness, pinpointing fifteen indicators classified into three overarching categories. The culmination of this research is the proposal of a comprehensive framework aimed at enhancing cybersecurity preparedness within SMEs. This framework integrates the identified indicators with established standards from the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022, ensuring relevance across organizational levels from leadership to operational staff. Expert evaluations suggest that the framework is both practical and feasible for implementation in real-world SME contexts.

Keywords: cyber risk; cybersecurity; small and medium enterprises (SMEs); cybersecurity readiness

1. Introduction

In the contemporary digital landscape, organizations are increasingly reliant on technological systems to enhance operational efficiency and productivity. While this technological integration offers significant advantages, it concurrently exposes organizations to a spectrum of cyber threats that have become an omnipresent concern in modern business environments. Recent trends indicate a surge not only in the frequency of cyberattacks but also in their complexity—partly fueled by advancements in Artificial Intelligence (AI), which enable attackers to develop more sophisticated and harder-to-detect methods. Such threats can lead to severe repercussions, including operational disruptions, exfiltration of sensitive data, and erosion of customer trust. Therefore, alongside leveraging digital innovations, organizations must prioritize robust cybersecurity strategies to mitigate potential risks [1].

Small and Medium Enterprises (SMEs) in Thailand represent a crucial segment of the national economy, contributing approximately 35% to the Gross Domestic Product (GDP). Despite their economic significance, many SMEs face challenges related to resource constraints, limited cybersecurity expertise, and low awareness of cyber risks, which frequently result in inadequate preparedness. Furthermore, some SMEs tend to underestimate their vulnerability, assuming their

 doi:10.20944/preprints202507.0267.v1

small size shields them from targeted cyberattacks [2]. As digital reliance grows, SMEs heavily engaged in online operations and digital platforms remain particularly vulnerable to cyber threats. According to the Kaspersky Cyberthreat Live Map (January 2025), Thailand experiences approximately 28,000 cyberattacks daily, with the incidence steadily increasing. This underscores the importance of strengthening cybersecurity resilience within SMEs to safeguard their continuity and growth [3].

In response to these issues, this study centers on exploring internal factors influencing cybersecurity preparedness among Thai SMEs, articulated through four primary objectives. First, it assesses cyber risk factors across financial, operational, governance, personnel, and reputational dimensions using the Fuzzy Analytic Hierarchy Process (Fuzzy AHP) approach [4], facilitating the prioritized allocation of resources. Second, it examines how internal organizational components—specifically personnel, processes, and technology—affect cybersecurity readiness, guided by the Resource-Based View (RBV) theory [5], which emphasizes the strategic value of internal resources. Third, the research develops measurable indicators for evaluating cybersecurity preparedness within these key areas. Lastly, it proposes a tailored framework aimed at enhancing SMEs' cyber resilience by integrating insights derived from internal factor analysis with established international standards, notably the NIST Cybersecurity Framework 2.0 [6] and ISO/IEC 27001:2022 [7], considering the resource limitations often faced by SMEs.

Achieving these objectives promises significant contributions to advancing cybersecurity readiness in SMEs, especially within developing economies. These include: (1) providing a prioritized cyber risk profile through Fuzzy AHP to support effective risk management; (2) identifying critical internal factors influencing cybersecurity capacity; (3) establishing foundational indicators for assessing organizational preparedness across personnel, processes, and technology; and (4) presenting a comprehensive, standards-aligned framework specifically adapted to the context and constraints of SMEs.

2. Literature Review

2.1. Cybersecurity Readiness of SMEs

Compared to larger enterprises, SMEs generally demonstrate lower levels of cybersecurity readiness. Research by [8] reveals that SMEs with more advanced adoption of digital technologies and stronger cybersecurity preparedness often utilize technological measures such as malware protection, encryption techniques, firewalls, and routine software updates to safeguard their systems. Conversely, SMEs with limited digital engagement tend to rely mainly on basic protections like software patches and firewall implementation, which are insufficient to address the full spectrum of cyber threats.

Despite these differences, both groups commonly lack comprehensive cybersecurity management frameworks. This includes gaps in staffing dedicated to security, the execution of audit mechanisms, formal cybersecurity policies, and the practical application of cybersecurity standards. These shortcomings largely stem from a lack of sufficient information and limited commitment from management to establish and maintain resilient cybersecurity practices.

To improve cybersecurity readiness in SMEs, there is a need to strengthen internal organizational components. [9] highlighted five essential internal factors that can drive effective cybersecurity readiness in SMEs within developing countries: adequate operational funding, strong organizational support from management, cybersecurity knowledge and expertise, appropriate information technology infrastructure, and adherence to personnel-related policies and regulations.

Drawing upon the Resource-Based View (RBV) theory [5], which suggests that organizations gain competitive advantages by leveraging valuable, rare, inimitable, and non-substitutable resources, this study focuses on analyzing internal factors specifically through the lenses of personnel, processes, and technology. These elements represent critical internal resources that enable SMEs to craft cybersecurity strategies that are not only effective but also efficient. Emphasizing these

 doi:10.20944/preprints202507.0267.v1

three aspects helps ensure that SMEs can maximize the use of their existing assets in a cost-effective manner, thus unlocking greater organizational potential [10].

2.2. Cyber Risks of SMEs

While digital technologies offer opportunities for SMEs to gain competitive advantages, they also expose these businesses to various cyber threats. Cybercriminals constantly refine and enhance their attack techniques, often focusing on SMEs due to their comparatively weaker defenses, making them easier targets than larger firms. [11] emphasize that one of the primary reasons SMEs face elevated cyber risks is their limited awareness of these threats. Many SMEs do not fully recognize or prioritize cyber risks, lack the necessary knowledge to protect themselves adequately, and struggle to establish effective cybersecurity programs. Resource limitations further hamper their ability to sustain robust cybersecurity measures.

This study analyzes cyber risks faced by SMEs using two key frameworks: the Risk Assessment in Practice framework by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) [12] and the ISO/IEC 27005:2018 standard, which provides guidelines on information security risk management [13]. Building upon these frameworks, the research identifies SME-relevant risk factors covering financial risk, operational risk, governance risk—including compliance with laws and regulations—personnel risk, and reputational risk. These identified risks are then systematically evaluated and ranked using the Fuzzy Analytic Hierarchy Process (Fuzzy AHP) technique to prioritize their impact.

2.3. Fuzzy Analytic Hierarchy Process

The Fuzzy Analytic Hierarchy Process (Fuzzy AHP) is a hybrid decision-making method that merges the traditional Analytic Hierarchy Process (AHP) with principles from Fuzzy Set Theory to better handle uncertainty and ambiguity in evaluations [14,15]. This method proves especially valuable when experts or decision-makers find it difficult to assign exact numerical values—known as crisp numbers—during pairwise comparisons, and instead express their preferences as intervals or degrees of confidence [16].

Fuzzy Set Theory introduces the idea of a "degree of membership," which ranges continuously from 0 to 1, allowing for the representation of imprecise or vague information [15]. In Fuzzy AHP applications, the Triangular Fuzzy Number (TFN) is widely used to capture uncertainty in a simple triangular form, defined by three parameters: the lower bound (l), the most likely or median value (m), and the upper bound (u) [17].

2.4. Factors Influencing the Cybersecurity Readiness Capability

2.4.1. Personnel Readiness

Personnel are fundamental to building a robust cybersecurity system since organizational operations involve the interaction of people with digital technologies and online platforms. The attitudes, beliefs, and behaviors of employees have a strong impact on the overall cybersecurity posture of an organization [18]. Employees lacking awareness of cyber threat severity can inadvertently expose their organizations to risks. Even when some staff members possess high awareness, operational challenges may still occur—such as the accidental leakage of confidential information—demonstrating what is known as the "knowing-doing gap," where individuals' actions do not align with their knowledge [19]. Thus, improving cybersecurity awareness and skills through targeted training programs equips employees to use technology more securely and helps reduce errors caused by human factors [20].

Moreover, fostering a collaborative culture within the organization's research and development network, especially when working alongside external partners like government agencies and academic institutions, encourages ongoing learning and the sharing of information about cybersecurity practices and new threats. This collaboration supports the continual adaptation and

 doi:10.20944/preprints202507.0267.v1

enhancement of cybersecurity strategies, boosting their overall effectiveness [21]. Based on this, the study proposes the following hypothesis:

H1. *Personnel readiness has a positive effect on the cybersecurity readiness capability of SMEs.*

2.4.2. Process Readiness

Organizations that heavily depend on digital technologies and online platforms tend to show higher cybersecurity readiness. However, simply having superior resources or cutting-edge technology does not automatically translate into a competitive edge from cybersecurity efforts [22]. To effectively counter cyber threats, organizations need well-designed cybersecurity management systems that maximize the use of their resources and technological tools [23].

Strong operational processes play a key role in achieving organizational success [24]. Effective cybersecurity processes help reduce risks from attacks that could interrupt business operations or cause harm, while also building confidence among customers and business partners. [25] argue that cybersecurity efforts should go beyond mere prevention and adopt a proactive stance. This includes establishing a resilient infrastructure, maintaining flexibility, continuously monitoring for threats, and being able to adapt and improve over time. Furthermore, aligning operational strategies with recognized cybersecurity frameworks can help SMEs overcome limitations in resources and expertise, enabling them to detect weaknesses and strengthen their security posture [26]. Based on these points, the following hypothesis is proposed:

H2. *Process readiness positively affects the cybersecurity readiness capability of SMEs.*

2.4.3. Technology Readiness

Technology is a vital component in managing cybersecurity effectively, as it equips organizations to address cyber threats more efficiently. The development of an organization's personnel and processes related to cybersecurity should be aligned with its level of technology readiness. Organizations that combine skilled human resources with competent technology management tend to achieve stronger cybersecurity results [1]. Research by Berlilana et al. (2021) highlights that higher technology readiness can significantly decrease cybersecurity risks, thereby boosting operational security, enhancing the organization's reputation, and increasing customer confidence. On the other hand, many SMEs suffer from limited technological expertise or insufficient proficiency, which negatively impacts their cybersecurity capabilities [27].

SMEs with well-developed technological readiness gain several advantages, such as smoother digital operations and the ability to create products that better satisfy customer needs with improved quality and lower costs [28], alongside stronger cybersecurity defenses. Based on this understanding, the following hypothesis is proposed:

H3. *Technology readiness positively influences the cybersecurity readiness capability of SMEs.*

3. Methodology

This research was carried out in four consecutive phases. The first phase focused on ranking cybersecurity risks faced by SMEs using the Fuzzy Analytic Hierarchy Process (Fuzzy AHP). In the second phase, structural equation modeling (SEM) was employed to analyze internal factors—specifically personnel, processes, and technology—that affect SMEs' cybersecurity readiness capabilities. The third phase involved developing measurement indicators for cybersecurity readiness related to personnel, processes, and technology through Exploratory Factor Analysis (EFA). Finally, in the fourth phase, a framework for enhancing cybersecurity readiness was created by integrating these indicators with the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022 standards.

 doi:10.20944/preprints202507.0267.v1

3.1. Fuzzy AHP

The prioritization of cybersecurity risks for SMEs using the Fuzzy Analytic Hierarchy Process was conducted in four stages: (1) Planning, (2) AHP Execution, (3) Fuzzy Calculations, and (4) Ranking [29].

3.1.1. Planning

The identification of cybersecurity risk factors relevant to SMEs was based on guidelines from the Risk Assessment in Practice framework [12] and the ISO/IEC 27005:2018 standard for information security risk management [13]. Five key categories of cyber risk were selected: financial, operational, governance, personnel, and reputational risks. To validate these factors, detailed interviews were conducted with cybersecurity professionals, chosen via purposive sampling with criteria including: (1) cybersecurity expertise, (2) experience with SME operations, and (3) educational background in information technology. The interview findings supported the relevance of the five identified risk categories.

3.1.2. AHP Execution

Experts performed pairwise comparisons of the five risk factors to assess their relative importance, with results presented in Table 1. The consistency of these evaluations was verified using the Consistency Ratio (CR), where values below 0.1 indicate acceptable consistency.

Table 1. The pairwise comparison scale used to assess the importance levels of factors through pairwise comparisons, rated according to [30].

Intensity of Importance	Description
1	Equal importance
3	Moderate importance
5	Strong importance
7	Demonstrated important
9	Extreme importance
2,4,6,8	Intermediate values between two adjacent judgments

AHP Operation includes the following procedure:

1. Pairwise Comparison: Experts evaluate the relative importance of each risk factor by comparing them in pairs. When one risk (risk i) is judged to be more significant than another (risk j), a numerical value representing this importance is assigned to the corresponding cell at row i, column j. Conversely, the reciprocal of this value is placed in the cell at row j, column i. An example of this comparison matrix is shown in Table 2.

Table 2. Pairwise comparison.

RISK	i	j	….
i	1	5	7
j	1/5	1	3
….	1/7	1/3	1

2. Calculation of the Consistency Ratio (CR)

- Calculate the sum of each column as shown in equation (1).

$$\sum_{i=1}^{n} a_{ij} \qquad \forall i, j \tag{1}$$

where

a_{ij} is the importance value comparing criterion i with criterion j

n is total number of criteria

Normalization as shown in equation (2).

 doi:10.20944/preprints202507.0267.v1

$$a'_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \qquad \forall i,j \tag{2}$$

Where

a'_{ij} is normalized value

Calculate the eigenvector by computing the average of each row to obtain the weights of the factors, as shown in the equation (3).

$$w_i = \frac{\sum_{i=1}^{n} a'_{ij}}{n} \tag{3}$$

Where

w_i is the weight or relative importance of the criterion i

Calculate eigenvalue λ_max as shown in the equation (4).

$$\lambda_{max} = \sum_{i=1}^{n} \frac{Aw_i}{nw_i} \tag{4}$$

Where

A is the original pairwise comparison matrix

w is the weight vector obtained from the equation (3)

Aw_i is the value obtained from multiplying matrix A by vector w

Calculate the consistency ratio according to equation (5).

$$CR = \frac{\lambda_{max} - n}{RI\ (n - 1)} \tag{5}$$

Where

λ_{max} is maximum eigenvalue

n is matrix size (number of criteria)

RI is random consistency index as shown in the Table 3

Table 3. Random consistency index.

n	1	2	3	4	5	6	7	8	9	10
RI	0.00	0.00	0.52	0.89	1.12	1.26	1.36	1.41	1.46	1.49

3.1.3. Fuzzy Operation

In the fuzzy operation step, Triangular Fuzzy Numbers (TFN) are used to convert the uncertain opinions of experts or decision-makers into data in the form of fuzzy numbers, as shown in Table 4.

Table 4. Standard scale for comparing the importance between factors.

Level of Importance	TFNs	Explanation
1	(1,1,1)	Equally important
3	(1,3,5)	Little less important
5	(3,5,7)	More important
7	(5,7,9)	Much more important
9	(7,9,9)	Maximum important

Aggregation of Fuzzy Matrix Sums

This is a crucial step in calculating the sum of each column for the lower (L), middle (M), and upper (U) values of the Fuzzy Pairwise Comparison Matrix. These sums represent the overall fuzzy importance level of each factor and are calculated as shown in equation (6).

For column j in Fuzzy Matrix

 doi:10.20944/preprints202507.0267.v1

$$L_{\text{sum},j} = \sum_{i=1}^{n} L_{ij}\,, M_{\text{sum},j} = \sum_{i=1}^{n} M_{ij}\,, U_{\text{sum},j} = \sum_{i=1}^{n} U_{ij} \tag{6}$$

Where

$L_{\text{sum},j}$ is the sum of the lower (L) values of column j

$M_{\text{sum},j}$ is the sum of the middle (M) values of column j

$U_{\text{sum},j}$ is the sum of the upper (U) values of column j

Fuzzy Normalization

Is the process of adjusting the fuzzy values (L, M, U) in the Fuzzy Pairwise Comparison Matrix to be within the range of 0 to 1, in order to prepare for the calculation of the fuzzy weights of each factor, as shown in equation (7).

For the position (i, j) in the fuzzy matrix,

$$L_{\text{norm},ij} = \frac{L_{ij}}{U_{\text{sum},j}}\,,\; M_{\text{norm},ij} = \frac{M_{ij}}{M_{\text{sum},j}}\,,\; U_{\text{norm},ij} = \frac{U_{ij}}{L_{\text{sum},j}} \tag{7}$$

Where

$L_{ij}\,, M_{ij}\,, U_{ij}$ is fuzzy value (L, M, U) in the position of i, j

$L_{\text{sum},j}, M_{\text{sum},j}, U_{\text{sum},j}$ is the sum of lower value (L), middle value (M), and higher value (U) of column j

Meaning of the Equation

$L_{\text{norm},ij}$ is normalize value of lower value (L) for the factors of (i, j)

$M_{\text{norm},ij}$ is normalize value of middle value (M)

$U_{\text{norm},ij}$ is normalize value of higher value (U)

Fuzzy Weights Calculation

This is a crucial step in the Fuzzy AHP process, which enables the determination of the relative weights of each factor in the form of Triangular Fuzzy Numbers (TFNs). Using the Normalized Fuzzy Matrix obtained from the previous step, the weights can be calculated as shown in equation (8) for each factor i.

$$L_{\text{weight},i} = \frac{\sum_{j=1}^{n} L_{\text{norm},ij}}{n}\,,\; M_{\text{weight},i} = \frac{\sum_{j=1}^{n} M_{\text{norm},ij}}{n}\,,\; U_{\text{weight},i} = \frac{\sum_{j=1}^{n} U_{\text{norm},ij}}{n} \tag{8}$$

Where

$L_{\text{weight},i}$ is the lower weight (L) of factor i

$M_{\text{weight},i}$ is the middle weight (M) of factor i

$U_{\text{weight},i}$ is the upper weight (L) of factor i

3.1.4. Ranking

Defuzzification of Fuzzy Weights

This step in the Fuzzy AHP process involves converting values expressed as Triangular Fuzzy Numbers (TFNs) (L, M, U) into a single specific value (Defuzzified Weight), which is then used to rank the importance of the factors, as shown in equation (9).

$$\text{Defuzzified Weight}_i = \frac{L_{\text{weight}} + M_{\text{weight}} + U_{\text{weight}}}{3} \tag{9}$$

Where

L_{weight} is the lower weight of the factor.

M_{weight} is the middle weight of the factor.

U_{weight} is the higher weight of the factor.

3.2. Structural Equation Modeling Analysis

 doi:10.20944/preprints202507.0267.v1

This research employed Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (SEM) using Jamovi software, version 2.6.44.0. The process began by assessing construct validity and discriminant validity of the measurement model, followed by hypothesis testing and detailed presentation of the results.

3.2.1. Population and Sample

The target population consists of SMEs across Thailand, divided into four main industry categories: trade (1,346,641 units), services (1,304,004 units), manufacturing (515,759 units), and agriculture (59,339 units), totaling 3,225,743 SMEs. The sample size was determined by applying the rule of thumb suggesting a minimum of ten times the number of questionnaire items [31]. With 18 items included in the survey, a minimum sample size of 180 participants was set. To reflect the proportional distribution of SMEs across these sectors, the Probability Proportional to Size (PPS) sampling technique was used, resulting in quotas of 75 for trade, 73 for services, 29 for manufacturing, and 3 for agriculture.

In total, 313 valid responses were gathered from SME employees with IT or digital roles, surpassing the initially required sample size. The breakdown of respondents by sector was as follows: 124 from trade, 111 from services, 73 from manufacturing, and 5 from agricultural businesses.

3.2.2. Instrument

The survey instrument consisted of an 18-item questionnaire measured on a 5-point Likert scale ranging from 1 (Strongly disagree) to 5 (Strongly agree). The items assessed four latent constructs: Personnel readiness was evaluated using 3 items adapted from [32]; Process readiness was measured with 6 items adapted from [32–34]; Technology readiness comprised 6 items adapted from [32,33]; and Cybersecurity readiness of SMEs was assessed with 3 items.

3.3. Indicator Development

The creation of indicators measuring the cybersecurity capability readiness of Thai SMEs was carried out through Exploratory Factor Analysis (EFA), which verified the construct validity and reliability of these measures. A total of 15 items, representing the latent constructs of personnel readiness, process readiness, and technology readiness, were examined using EFA with a fresh sample drawn from Thai SMEs [35]. This analysis aimed to explore the internal relationships among items within each construct, identifying those that best reflect their designated categories for effective practical use.

3.4. Development of the Capability Readiness Framework for Cybersecurity Protection

Following the establishment of readiness indicators, and through a comprehensive review of established cybersecurity frameworks—including the NIST Cybersecurity Framework 2.0 [6] and ISO/IEC 27001:2022 [7] —the researcher designed an actionable framework to bolster cybersecurity preparedness in SMEs. This framework structures the organization into three distinct levels:

- **Tier 1: Management System**, aligned with ISO/IEC 27001:2022, targeting senior leadership and governance roles;
- **Tier 2: Operational System**, derived from the NIST Cybersecurity Framework 2.0, focusing on day-to-day cybersecurity operations and procedures;
- **Tier 3: Internal Enablers**, addressing the management of resources necessary to support readiness.

To ensure the framework is clear and practical for real-world application, redundant and overlapping elements across these tiers were carefully streamlined, producing a coherent and manageable model for SMEs to implement.

4. Results

 doi:10.20944/preprints202507.0267.v1

4.1. Cybersecurity Risk Analysis Results

Fifteen experts assessed the relative importance of five cybersecurity risk categories: financial, operational, governance, personnel, and reputational risks. Their pairwise comparison data were transformed into Triangular Fuzzy Numbers (TFNs) to capture uncertainty in judgments. These fuzzy values were then combined, normalized, weighted, and defuzzified to generate definitive weights for each risk factor. The outcome is a ranked hierarchy of cybersecurity risks derived using the Fuzzy Analytic Hierarchy Process (Fuzzy AHP), aimed at guiding improvements in cybersecurity defenses.

The average priority rankings from the pairwise comparisons of the five risk factors are summarized in Table 5.

Table 5. Averaged pairwise comparison matrix.

Factor	Finance	Operation	Monitoring	People	Reputation
Finance	1.0	1.6022	2.5822	2.0473	2.8300
Operation	1.6466	1.0	2.1022	2.0906	2.8928
Monitoring	1.2400	1.0188	1.0	1.5062	1.9967
People	2.1372	2.4101	2.1711	1.0	2.8667
Reputation	1.4463	1.6309	1.7806	0.4455	1.0

Results of Converting the Pairwise Comparison Matrix into a Fuzzy Pairwise Comparison Matrix

The researcher converted the Averaged Pairwise Comparison Matrix into a Scaled Pairwise Comparison Matrix using Saaty's scale. This Scaled Pairwise Comparison Matrix was then transformed into Triangular Fuzzy Numbers (TFNs) to address uncertainty in the data. The results are presented in Tables 6–8.

Table 6. Scaled pairwise comparison matrix.

Factor	Finance	Operation	Monitoring	People	Reputation
Finance	1	3	5	3	5
Operation	3	1	3	3	5
Monitoring	1	1	1	3	3
People	3	3	3	1	5
Reputation	1	3	3	1	1

Table 7. Triangular Fuzzy Numbers.

Value in Metrix	TFNs (Lower, Middle, Upper)
1	(1, 1, 1)
3	(1, 3, 5)
5	(3, 5, 7)
7	(5, 7, 9)
9	(7, 9, 9)

Table 8. Fuzzy pairwise comparison matrix.

Factor	Finance	Operation	Monitoring	People	Reputation
Finance	(1, 1, 1)	(1, 3, 5)	(3, 5, 7)	(1, 3, 5)	(3, 5, 7)
Operation	(1, 3, 5)	(1, 1, 1)	(1, 3, 5)	(1, 3, 5)	(3, 5, 7)
Monitoring	(1, 1, 1)	(1, 1, 1)	(1, 1, 1)	(1, 3, 5)	(1, 3, 5)
People	(1, 3, 5)	(1, 3, 5)	(1, 3, 5)	(1, 1, 1)	(3, 5, 7)
Reputation	(1, 1, 1)	(1, 3, 5)	(1, 3, 5)	(1, 1, 1)	(1, 1, 1)

Results of the aggregation of fuzzy matrix sums are presented in Table 9.

 doi:10.20944/preprints202507.0267.v1

Table 9. Results of the aggregation of fuzzy matrix sums.

Factor	L_{sum}	M_{sum}	U_{sum}
Finance	5	9	13
Operation	5	11	17
Monitoring	7	15	23
People	5	11	17
Reputation	11	19	27

Results of fuzzy normalization of values in the fuzzy matrix are presented in Table 10.

Table 10. Results of fuzzy normalization calculations.

Factor	Finance (L, M, U)	Operation (L, M, U)	Monitoring (L, M, U)	People (L, M, U)	Reputation (L, M, U)
Finance	0.0769, 0.1111, 0.2	0.0588, 0.2727, 1	0.1304, 0.3333, 1	0.0588, 0.2727, 1	0.1111, 0.2632, 0.6364
Operation	0.0769, 0.3333, 1	0.0588, 0.0909, 0.2	0.0435, 0.2, 0.7143	0.0588, 0.2727, 1	0.1111, 0.2632, 0.6364
Monitoring	0.0769, 0.1111, 0.2	0.0588, 0.0909, 0.2	0.0435, 0.0667, 0.1429	0.0588, 0.2727, 1	0.0370, 0.1579, 0.4545
People	0.0769, 0.3333, 1	0.0588, 0.2727, 1	0.0435, 0.2, 0.7143	0.0588, 0.0909, 0.2	0.1111, 0.2632, 0.6364
Reputation	0.0769, 0.1111, 0.2	0.0588, 0.2727, 1	0.0435, 0.2, 0.7143	0.0588, 0.0909, 0.2	0.0370, 0.0526, 0.0909

Results of the fuzzy weights calculation are presented in Table 11.

Table 11. Fuzzy weights calculation.

Factor	L_{weight}	M_{weight}	U_{weight}
Finance	0.0872	0.2506	0.7673
Operation	0.0698	0.2320	0.7101
Monitoring	0.0550	0.1399	0.3995
People	0.0698	0.2320	0.7101
Reputation	0.0550	0.1455	0.4410

The results of defuzzifying the fuzzy weights are presented in Table 12.

Table 12. Results after defuzzification.

Factor	Defuzzified Weight
Finance	0.3684
Operation	0.3373
Monitoring	0.1981
People	0.3373
Reputation	0.2138

Summary of analysis results (Conclusion)

From the analysis of the prioritization of cybersecurity risks affecting Thai SMEs using the Fuzzy AHP decision-making process, it was concluded that financial risk is the most significant. This is followed in descending order by operational risk, personnel risk, reputational risk, and Monitoring risk, as shown in Table 13.

 doi:10.20944/preprints202507.0267.v1

Table 13. Results of the prioritization of cybersecurity risk factors.

Order of Importance	Factor	Defuzzified Weight
1	Finance	0.3684
2	Operation	0.3373
2	Personnel	0.3373
4	Reputation	0.2138
5	Monitoring	0.1981

4.2. Results of the Analysis of Internal Factors Affecting SMEs' Cybersecurity Readiness Capability

4.2.1. Validity and Reliability

To ensure the robustness and accuracy of the constructed model and hypotheses, the validity and reliability of the study's variables and questionnaire items were thoroughly examined. The model includes four latent variables: Personnel Readiness (PP), Process Readiness (PC), and Technology Readiness (TR) as independent (exogenous) variables, and SME Cybersecurity Readiness (SMER) as the dependent (endogenous) variable. The PP variable comprises 3 questionnaire items, PC has 6 items, TR includes 6 items, and SMER contains 3 items.

All 18 questionnaire items underwent validity and reliability testing by evaluating Factor Loadings, Average Variance Extracted (AVE), Composite Reliability (CR), and Cronbach's Alpha. The findings confirmed that each item satisfied the established statistical thresholds, as detailed in Table 14.

Following this, discriminant validity was assessed through the Heterotrait-Monotrait ratio (HTMT) and the Fornell-Larcker criteria. The HTMT evaluates the correlation between indicators across different constructs and within the same construct, with acceptable values below 0.90. Meanwhile, the Fornell-Larcker criterion requires that the square root of each variable's AVE exceed its correlation coefficients with other variables. Table 15 illustrates that all variables conform to these criteria, demonstrating satisfactory discriminant validity.

Table 14. Factor analysis, validity and reliability statistics.

Factors	Items	Loadings	AVE	CR	Alpha
Thresholds		*> 0.7*	*> 0.5*	*> 0.7*	*> 0.7*
People Readiness (PP)			.668	.858	.858
	PP1	.785			
	PP2	.812			
	PP3	.854			
Process Readiness (PC)			.673	.925	.931
	PC1	.814			
	PC2	.794			
	PC3	.801			
	PC4	.819			
	PC5	.841			
	PC6	.853			
Technology Readiness (TR)			.719	.939	.942
	TR1	.852			
	TR2	.844			
	TR3	.843			
	TR4	.891			
	TR5	.842			
	TR6	.813			
SME's Cybersecurity Readiness (SMER)			.672	.860	.852
	SMER	.812			

 doi:10.20944/preprints202507.0267.v1

	SMER	.773		
	SMER	.872		

Table 15. HTMT and Fornell-Larcker criterion.

	PP	**PC**	**TR**	**SMER**
HTMT				
PP				
PC	.857			
TR	.711	.782		
SMER	.852	.871	.802	
Fornell-Larcker criterion				
PP	*.817*			
PC	.767	*.821*		
TR	.642	.737	*.848*	
SMER	.726	.775	.705	*.820*

4.2.2. Hypothesis Testing

Structural Equation Modeling (SEM) analysis was performed using Jamovi version 2.6.44.0, as depicted in Figure 1. The findings reveal that personnel readiness significantly and positively influences cybersecurity readiness (Estimate = 0.184, p = 0.019), providing support for hypothesis H1. Similarly, process readiness shows a significant positive effect on cybersecurity readiness (Estimate = 0.351, p = 0.001), confirming hypothesis H2. Furthermore, technology readiness also demonstrates a significant positive impact on cybersecurity readiness (Estimate = 0.438, p = 0.001), thereby supporting hypothesis H3. Model fit was evaluated using multiple indices: Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), Non-Normed Fit Index (NNFI), Relative Noncentrality Index (RNI), Normed Fit Index (NFI), Relative Fit Index (RFI), and Incremental Fit Index (IFI), with values above 0.90 to 0.95 considered indicative of a good fit. Additionally, Standardized Root Mean Square Residual (SRMR) and Root Mean Square Error of Approximation (RMSEA) values below 0.08 signify acceptable fit [36,37]. The Parsimony Normed Fit Index (PNFI) exceeding 0.50 suggests improved model parsimony [38], and a chi-square to degrees of freedom ratio (χ^2/df) under 3 is indicative of good model fit. Detailed model fit indices are summarized in Table 16, while the hypothesis testing outcomes are presented in Table 17.

 doi:10.20944/preprints202507.0267.v1

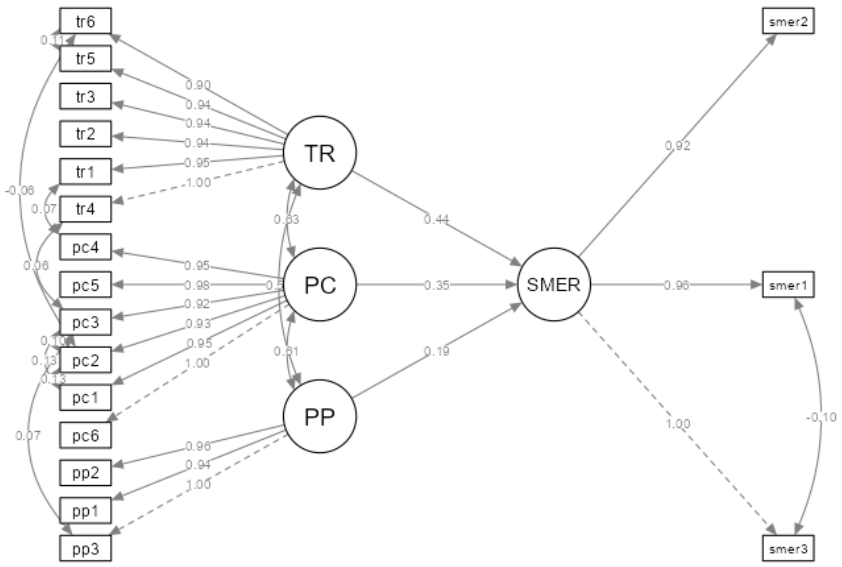

Figure 1. The results of the structural equation modeling analysis.

Table 16. The results of the model fit index analysis.

	X^2	df	p-Value
Model tests			
User model	355	120	<.001
Baseline model	5246	153	<.001
Fit indices			
CFI	0.954	NFI	0.932
TLI	0.941	RFI	0.914
NNFI	0.941	IFI	0.954

Table 17. Results of hypothesis testing.

Hypothesis	Paths	Estimate	β	z	p	Decision
H1	PP -> SMER	0.185	0.183	2.35	0.019	Support
H2	PC -> SMER	0.351	0.354	3.91	<.001	Support
H3	TR -> SMER	0.438	0.554	7.39	<.001	Support

In Table 18, the Measurement Model presents the unstandardized factor loadings of the items. The factor loadings for items in the PP construct range from .787 to .846, those in the PC construct range from .792 to .857, items in the TR construct range from .814 to .893, and items in the SMER construct range from .784 to .849. Considering the z-statistics and p-values, all item loadings are shown to be statistically significant.

Table 18. Measurement model.

			95% Confidence Intervals			
Latent	**Observed**	**β**	**Lower**	**Upper**	**z**	**p**
PP	pp3	0.846	1.000	1.000		
	pp1	0.787	0.821	1.052	15.9	<.001

 doi:10.20944/preprints202507.0267.v1

	pp2	0.807	0.846	1.075	16.5	<.001
PC	pc6	0.857	1.000	1.000		
	pc1	0.812	0.843	1.051	17.9	<.001
	pc2	0.797	0.827	1.037	17.4	<.001
	pc3	0.792	0.816	1.026	17.2	<.001
	pc5	0.842	0.882	1.083	19.1	<.001
	pc4	0.816	0.851	1.057	18.2	<.001
TR	tr4	0.893	1.000	1.000	22.2	
	tr1	0.864	0.865	1.032	20.9	<.001
	tr2	0.841	0.849	1.025	21.1	<.001
	tr3	0.845	0.854	1.029	20.9	<.001
	tr5	0.843	0.851	1.027	19.5	<.001
	tr6	0.814	0.807	0.987		<.001
SMER	smer3	0.849	1.000	1.000		
	smer1	0.818	0.840	1.086	15.3	<.001
	smer2	0.784	0.811	1.034	16.2	<.001

4.3. Indicators of Cybersecurity Readiness Capability for SMEs

The validity and reliability of 15 indicators measuring the cybersecurity readiness capability of SMEs were evaluated using Exploratory Factor Analysis (EFA) across three core components. The assessment criteria included Factor Loadings greater than 0.5, a Kaiser–Meyer–Olkin (KMO) value exceeding 0.7, and a significant Bartlett's test of sphericity ($p < 0.05$). All indicators satisfied these criteria, with each item demonstrating a Factor Loading above 0.5. The overall KMO measure was 0.949, and Bartlett's test indicated statistical significance ($\chi^2 = 4201$, $p < .001$), confirming the data's suitability for factor analysis.

Collectively, these indicators explained 72.3% of the total variance, reflecting strong correlations among the items within each construct, as detailed in Table 19. Interestingly, one indicator initially assigned to the Process Readiness component showed a higher Factor Loading in the Technology Readiness component, prompting its reassignment.

Accordingly, the final set of cybersecurity readiness capability indicators for SMEs comprises 3 indicators for Personnel Readiness, 5 for Process Readiness, and 7 for Technology Readiness.

Table 19. Presents the detailed results of the structural examination of these indicators.

	Item	Factor		
		1	2	3
	Factor 1: People Readiness			
1.	SME: Promotes raising cybersecurity awareness among their personnel.	0.545		
2.	SME: Encourages personnel to undergo training in internationally recognized cybersecurity courses.	0.741		
3.	SME: There is research and development in cybersecurity within organizations and network agencies.	0.631		
	Factor 2: Process Readiness			
1.	SME There are strategies, policies, and planning related to cybersecurity.		0.728	
2.	SMEs continuous monitoring and evaluation of cybersecurity operations.		0.806	
3.	SMEs utilize internationally standardized cybersecurity frameworks as the foundation for their cybersecurity operations.		0.718	

 doi:10.20944/preprints202507.0267.v1

4.	SMEs seek collaboration with external agencies to develop, enhance, and strengthen their cybersecurity capabilities.	0.664	
5.	SMEs have continuously developed and improved their cybersecurity measures.	0.693	
	Factor 3: Technology Readiness		
1.	SMEs have sufficient cybersecurity technology in terms of both quantity and quality.		0.780
2.	SMEs use modern and effective cybersecurity technologies.		0.690
3.	Most of the equipment used by SMEs is installed with cybersecurity software (such as antivirus or malware protection programs).		0.763
4.	SMEs possess cybersecurity technologies capable of rapidly and accurately detecting and responding to cyber threats.		0.761
5.	The tools, equipment, and technologies of SMEs are regularly updated.		0.825
6	SME personnel have access to tools and equipment that can support operations when encountering cyber threats or attacks.		0.788
7.	SMEs have sufficiently quality management processes for critical cybersecurity infrastructure systems.		0.589

4.4. Framework for Developing Cybersecurity Readiness Capability for SMEs

Based on the analysis of cybersecurity risks and readiness, the researcher developed a framework to enhance the cybersecurity readiness capability of SMEs to address risks arising from cyber threats. The framework comprises three interconnected levels that encompass and link the operations of SMEs, beginning with policy formulation at the management level (TIER 1: Management System), and the development of resource capabilities foundational to operations (TIER 3: Internal Enablers), which connect to the implementation of cybersecurity operations (TIER 2: Operational System). This framework is illustrated in Figure 2., with detailed guidance on its application provided in Table 20.

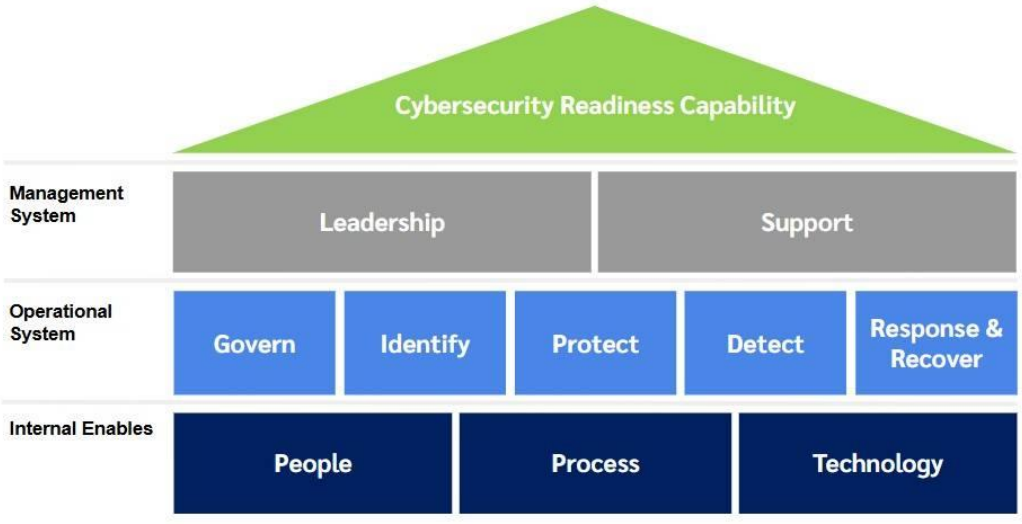

Figure 2. Framework for developing cybersecurity readiness capability for SMEs.

 doi:10.20944/preprints202507.0267.v1

4.4.1. Description of Framework Implementation

Table 20. Description of framework implementation.

Framework	Description
TIER 1: Management System	
Leadership	
• Leadership and Commitment	Senior management must demonstrate leadership and prioritize the implementation of the cybersecurity management system by establishing policies and objectives aligned with the SME's strategic direction. They should integrate the system into various processes, allocate necessary resources, communicate the importance of the system, support personnel, promote continuous improvement, and encourage other managers to fulfill their respective roles.
• Organizational roles, responsibilities and authorities	Senior management must ensure that clear roles, responsibilities, and authorities related to cybersecurity within the SME are defined and communicated. They should delegate these responsibilities to designated individuals who can ensure the system's compliance with requirements and appropriately report the system's performance to senior management.
Support	
• Resources	SMEs must allocate sufficient and appropriate resources to support the implementation, maintenance, and continuous improvement of the cybersecurity system to ensure effective and sustainable outcomes.
• Competence	SMEs must define, assess, and develop the competencies of personnel responsible for information security to ensure they possess appropriate knowledge, skills, or experience through continuous training and development, while maintaining documented evidence to verify competencies in accordance with requirements.
• Communication	SMEs must establish clear communication guidelines both internally and externally regarding the cybersecurity system, specifying what information will be communicated, when, by whom, and through which channels, to ensure understanding and effective implementation.
• Documented information	SMEs must create, control, and maintain documented information related to the cybersecurity system to support operations and demonstrate compliance with requirements. This includes ensuring that the documentation is appropriate, comprehensive in detail, properly formatted, stored securely, approved, and accessible, as well as controlling against loss, alteration, or unauthorized use.
TIER 2: Operational System	
Govern	
• Organizational Context	SMEs must understand the organization's mission and use it as a guideline for managing cyber risks. They need to identify and comprehend the expectations of both internal and external stakeholders, including relevant legal requirements, and clearly communicate the SME's context to these stakeholders.
• Risk Management Strategy	SMEs must establish a clear approach to cyber risk management by defining the objectives of risk management, setting the acceptable risk levels (Risk Appetite), and determining risk tolerance levels. These must be communicated effectively to employees and relevant stakeholders to ensure a shared understanding. Additionally, risk management activities should align with organizational policies and take into account the potential cyber impacts on business operations.
• Oversight	The monitoring and evaluation of risk management and cybersecurity performance must be conducted regularly. The outcomes of risk management

 doi:10.20944/preprints202507.0267.v1

	strategies should be communicated to relevant stakeholders and used to inform improvements in the organization's strategies and direction, ensuring alignment with actual circumstances. Existing strategies must be continuously reviewed and developed.
• Cybersecurity Supply Chain Risk Management	SMEs should establish clear guidelines for managing cybersecurity risks within the supply chain, especially concerning external service providers or partners. This includes defining roles and responsibilities, clearly communicating cybersecurity requirements, establishing agreements or contracts that comprehensively address security issues, continuously monitoring and evaluating partner performance, as well as developing response and recovery plans in the event of an incident.
Identify	
• Asset Management	SMEs should maintain a comprehensive asset inventory covering hardware, software, systems, data, services, and personnel related to business operations. This inventory must identify all assets relevant to cybersecurity risk management, be regularly updated, and categorize assets to facilitate access control and management. Additionally, the importance of each asset should be assessed to prioritize risks accordingly.
• Risk Assessment	SMEs should conduct systematic cybersecurity risk assessments to identify weaknesses or vulnerabilities in assets, personnel, and operational systems. They should regularly monitor cyber threat intelligence from reliable sources and evaluate potential impacts on both business operations and organizational reputation. Furthermore, emphasis should be placed on risk prioritization, response planning, thorough inspection of software and hardware to ensure no critical vulnerabilities exist, and assessment of third-party service providers.
• Improvement	SMEs should establish guidelines for the continuous improvement of processes, workflows, and activities related to cybersecurity. This should be based on assessment results, user feedback, and lessons learned from past security incidents. Additionally, the outcomes of these improvements must be clearly communicated to all relevant stakeholders.
Protect	
• Identity Management, Authentication, and Access Control	SMEs must define and control access to systems, data, and services, granting permissions only to authorized personnel or systems. This requires systematic user account management, assigning access rights based on roles and responsibilities, and enforcing multi-factor authentication to enhance security. Clear policies for access rights management should be established, periodic access reviews conducted, unauthorized access prevented, and permissions promptly revoked when no longer needed.
• Data Security	SMEs must implement measures to ensure the confidentiality, integrity, and availability of data, such as encryption, access control, and validation of data accuracy before use. Additionally, storage systems should be tested regularly to ensure they are operational when needed. Any data transferred outside the organization's systems must be protected according to its level of sensitivity.
• Platform Security	SMEs must establish clear guidelines for managing the security of platforms, including hardware, software, operating systems, and applications. They should define and implement secure configuration practices and regularly maintain, update, and replace outdated equipment or software. Additionally, SMEs should retain log data to enable timely analysis of anomalous events and ensure that only licensed software is installed.
• Technology Infrastructure Resilience	SMEs should establish a flexible technology infrastructure that can continuously withstand threats or disruptions. Equipment, systems, and environments must be protected against unauthorized access. Additionally,

 doi:10.20944/preprints202507.0267.v1

	preparedness for emergencies such as power outages, system failures, or natural disasters should be in place. This includes having backup resources or alternative solutions available for temporary use to enable rapid recovery and resumption of operations.
Detect	
• Continuous Monitoring	SMEs should have continuous monitoring and anomaly detection systems in all parts of their infrastructure, including networks, endpoints, environments, and user behaviors, to promptly identify indicators of compromise and enable rapid response actions.
• Adverse Event Analysis	SMEs should have a systematic approach for analyzing cybersecurity incidents or anomalies. When a suspicious event or potential attack occurs, relevant data should be thoroughly collected and analyzed to identify the cause, origin, and impact of the incident, as well as to assess any connections with other threats.
Response & Recover	
• Incident Management	SMEs must develop a response plan for potential cybersecurity incidents, clearly specifying the response procedures, events that require notification, and responsible personnel. When an incident occurs, there should be systematic reporting, investigation, and response processes in place, including thorough management of evidence and assessment of the incident to prioritize its severity.
• Incident Recovery Plan Execution	SMEs should have a clear and actionable recovery plan to restore systems and services to normal operation following a cybersecurity incident. The recovery plan should clearly define roles and responsibilities, prioritize the assets that need to be recovered first, and include regular drills or tests to assess preparedness.
TIER 3: Internal Enablers	
People Readiness	
• Awareness	SMEs must promote cybersecurity awareness among personnel at all levels by organizing training sessions or providing information about cyber threats. They should clearly communicate organizational policies and practices, regularly conduct educational activities or awareness campaigns, and continuously evaluate employees' understanding.
• Training & Learning	SMEs must promote continuous training and learning for personnel in cybersecurity, focusing on developing skills, knowledge, and competencies aligned with their roles. For example, technical training should be provided for IT staff, while security best practice training should be offered to general users.
• Research & Development	SMEs should promote research and development in cybersecurity by collaborating with research institutes, universities, or external organizations to exchange knowledge. This enables personnel to stay updated on new technologies, emerging threat trends, and modern prevention approaches, which can then be applied to their operations.
Process Readiness	
• Policy, Strategy & Plan	The formulation of policies, strategies, and plans for cybersecurity must be clear. Policies should demonstrate the management's commitment to protecting information and information systems. Strategies should align with the SME's objectives, and plans must specify operational actions within defined timeframes, such as risk assessment, prevention, incident response, and system recovery. This ensures that cybersecurity efforts are purposeful and continuous.
• Cybersecurity Evaluation	Cybersecurity assessments must be conducted regularly to measure the levels of risk, vulnerabilities, and the effectiveness of implemented measures. These

 doi:10.20944/preprints202507.0267.v1

	assessments may include system testing (e.g., penetration testing), vulnerability analysis, compliance audits with policies or standards, and ongoing performance
• Cybersecurity Framework	SMEs should establish a clear and systematic cybersecurity management framework that at minimum encompasses the approaches for prevention, detection, response, and recovery from cyber incidents. This framework should be based on international standards or best practices tailored to the specific characteristics of each SME, ensuring that cyber risk management is conducted in a structured manner, aligned with business operations, and practically implementable.
• Cybersecurity Coordination	SMEs should ensure effective coordination of cybersecurity efforts both within their organization and with relevant external agencies to enable a rapid and consistent response to threats. This coordination should include clearly defined roles and responsibilities, incident notification, joint incident management, and continuous communication of security-related information to strengthen defense systems and minimize risks arising from communication gaps.
• Cybersecurity Improvement	The improvement and development of the cybersecurity system must be carried out continuously, based on evaluation results, identified vulnerabilities, incidents that have occurred, and changes in technology or threats. These improvements should encompass policies, processes, technology, and personnel.
Technology Readiness	
• Quality & Quantity	The allocation of tools, equipment, and technology used for cybersecurity must be sufficient in quantity and appropriate in quality, such as computers with antivirus software, backup systems, and monitoring tools.
• Modern & Efficient	The devices, tools, and technologies used must be capable of responding rapidly to emerging threats. Utilizing modern and efficient technologies and equipment enhances the effectiveness of cybersecurity defenses and allows for future improvements as needed.
• Protecting Devices	SMEs must have measures in place to protect devices such as computers, servers, and network equipment by installing antivirus systems, firewalls, encryption software, and access controls. These measures help prevent attacks, data leaks, and unauthorized use, thereby reducing the risk of devices becoming vulnerabilities for cyber threats.
• Detect & Response	SMEs should have systems and processes that support the rapid detection of cyber incidents or anomalies, along with a clear response plan when threats are identified. This is to limit the impact, restore operations, and prevent recurrence.
• Updating Devices	Digital devices and tools must have their software and operating systems regularly updated to close security vulnerabilities that could be exploited by cyber threats. Updates should be continuous and up-to-date for both core systems and supporting programs to ensure that all devices remain secure and function efficiently.
• Accessible devices for personnel	SMEs must allocate secure and appropriate devices and systems that personnel can access conveniently, both during normal operations and in the event of a security threat. Access controls should be in place, such as secure authentication and permission settings, to prevent unauthorized access to data or systems.
• Cybersecurity Infrastructure	SMEs must have appropriate infrastructure to support cybersecurity, such as secure network systems, intrusion prevention systems, data backup, and

 doi:10.20944/preprints202507.0267.v1

	secure data storage. This infrastructure should effectively support threat prevention, incident detection, and system recovery.

4.4.2. Evaluation Results of the Capability Development Framework for Cybersecurity Readiness for SMEs

The capability development framework for cybersecurity readiness for SMEs that was developed has been evaluated in terms of suitability, acceptance, and feasibility for implementation by six experts. These experts specialize in cybersecurity across the public sector, private sector, and academia. The evaluation results show that the developed framework is the most suitable, has the highest level of acceptance, and has highly feasibility for implementation, as presented in Table 21.

Table 21. Evaluation results of suitability, acceptance, and feasibility of the capability development framework for cybersecurity readiness for SMEs.

	Questions	Assessment	
1.	Suitability of the Capability Development Framework for Cybersecurity Readiness for SMEs	4.50	The most
2.	Acceptance of the Capability Development Framework for Cybersecurity Readiness for SMEs	4.67	The most
3.	Feasibility of Implementing the Capability Development Framework for Cybersecurity Readiness for SMEs	4.17	Very much
	The sum of average	**4.44**	**The most**

5. Conclusions

The analysis of cyber risks affecting small and medium-sized enterprises (SMEs) using the Fuzzy Analytic Hierarchy Process (Fuzzy AHP) reveals the prioritization of risks posed by cyber threats, which have the potential to significantly impact SMEs across financial, operational, human resource, reputational, and governance dimensions, respectively. Despite this, SMEs continue to encounter substantial challenges in managing cyber risks and ensuring cybersecurity, primarily due to a shortage of skilled personnel, limited resources, and the absence of a formal cybersecurity strategy [39].

To address these constraints, this study examines internal factors—specifically personnel, processes, and technology—that influence SMEs' cybersecurity readiness. The findings underscore the critical importance of internal resource management within SMEs [40], particularly in enhancing technological readiness, which has been found to significantly affect operational performance [41]. Furthermore, modernizing operational processes to respond to increasingly sophisticated cyber threats can contribute to risk reduction and improved operational efficiency [42]. Concurrently, developing employees' cybersecurity knowledge and skills not only supports threat mitigation and seamless operations but also fosters workforce advancement in the digital technology landscape [43].

Thai SMEs, in particular, face difficulties in accessing and adopting advanced technologies due to inadequate knowledge and institutional support [44]. Therefore, strengthening technological capability is a pressing concern, as competitiveness in today's market increasingly depends on the effective deployment of advanced technologies. However, such technologies often entail complexity and potential security vulnerabilities, especially when used without proper monitoring or maintenance. Conversely, the well-regulated and systematic implementation of modern, sufficient technological tools not only mitigates cybersecurity risks but also enhances confidence that business operations will comply with standards and timelines. This, in turn, facilitates the development of secure and sustainable operational systems [45].

Amid the rapid expansion of technology and electronic devices, organizations—including Thai SMEs—are integrating digital tools to enhance competitiveness. This growing reliance on technology has raised awareness of potential damage from cyberattacks and prompted the adoption of

 doi:10.20944/preprints202507.0267.v1

cybersecurity measures. Nevertheless, Thai SMEs still face constraints in adopting standardized cybersecurity frameworks, such as NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022. According to [46], key barriers include insufficient financial resources, lack of specialized expertise, and inadequate tools. To overcome these challenges, SMEs must urgently evaluate the adequacy of their existing cybersecurity measures, plan the development of digital infrastructure, and consider engaging external experts to address security vulnerabilities.

In addition to technological and process readiness, human resource development is essential for fostering a culture of cyber-safe practices—particularly in SMEs that have not yet achieved digital maturity. This immaturity often leads to complacency and unsafe use of digital tools in the workplace [47]. Therefore, SMEs should promote cybersecurity awareness, conduct targeted training programs, and seek knowledge and resources for workforce development through collaborative external networks.

Cyber threats are evolving rapidly in complexity and resilience, representing external factors beyond SMEs' control. Moreover, each SME operates within a unique context, with differing needs in protecting critical assets [48]. This study proposes a framework for enhancing SMEs' cybersecurity readiness, integrating SME-specific indicators with internationally recognized standards, namely the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022. This framework embeds cybersecurity measures throughout the organizational structure—from executive management to operational and support levels—and has been assessed as highly appropriate, acceptable, and feasible for practical implementation.

References

1. Neri, M.; Niccolini, F.; Pugliese, R. Assessing SMEs' Cybersecurity Organizational Readiness: Findings from an Italian Survey. *Open J. Adv. Knowl. Manag*. **2022**, *10*, 1–22.
2. Perozzo, H.; Zaghloul, F.; Ravarini, A. CyberSecurity Readiness: A Model for SMEs Based on the Socio-Technical Perspective. *Complex Syst. Inform. Model. Q.* **2022**, *33*, 53–66.
3. Szedlak, C.; Reinemann, H.; Hatzelmann, S. Ensuring Cybersecurity Compliance: Assessing SME Awareness and Preparedness for the Cyber Resilience Act. In Proceedings of the International Conference on Industrial Engineering and Operations Management; IEOM Society International: Tokyo, Japan, September 10 2024.
4. Van Laarhoven, P.J.M.; Pedrycz, W. A Fuzzy Extension of Saaty's Priority Theory. *Fuzzy Sets Syst*. **1983**, *11*, 229–241.
5. Barney, J. Firm Resources and Sustained Competitive Advantage. *J. Manag.* **1991**, *17*, 99–120.
6. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024; p. NIST CSWP 29.
7. International Organization for Standardization; International Electrotechnical Commission. *ISO/IEC 27001:2022—Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*; ISO/IEC: Geneva, Switzerland, 2022.
8. Arroyabe, M.F.; Arranz, C.F.A.; Fernandez De Arroyabe, I.; Fernandez De Arroyabe, J.C. Exploring the Economic Role of Cybersecurity in SMEs: A Case Study of the UK. *Technol. Soc.* **2024**, *78*, 102670.
9. Kabanda, S.; Tanner, M.; Kent, C. Exploring SME Cybersecurity Practices in Developing Countries. *J. Organ. Comput. Electron. Commer*. **2018**, *28*, 269–282.
10. Durst, S.; Hinteregger, C.; Zieba, M. The Effect of Environmental Turbulence on Cyber Security Risk Management and Organizational Resilience. *Comput. Secur*. **2024**, *137*, 103591.
11. Junior, C.R.; Becker, I.; Johnson, S. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. *arXiv* **2023**, arXiv:2309.17186. Available online: https://arxiv.org/abs/2309.17186 (accessed on 18 June 2025).
12. Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Risk Assessment in Practice*; COSO: Durham, NC, USA, 2012.

 doi:10.20944/preprints202507.0267.v1

13. International Organization for Standardization (ISO); International Electrotechnical Commission (IEC). *ISO/IEC 27005:2018—Information Technology—Security Techniques—Information Security Risk Management*; ISO: Geneva, Switzerland, 2018.
14. Saaty, T.L. A Scaling Method for Priorities in Hierarchical Structures. *J. Math. Psychol*. **1977**, *15*, 234–281.
15. Zadeh, L.A. Fuzzy Sets. *Inf. Control* **1965**, *8*, 338–353.
16. Chang, D.-Y. Applications of the Extent Analysis Method on Fuzzy AHP. *Eur. J. Oper. Res*. **1996**, *95*, 649–655.
17. Buckley, J.J. Fuzzy Hierarchical Analysis. *Fuzzy Sets Syst*. **1985**, *17*, 233–247.
18. Vishwanath, A.; Neo, L.S.; Goh, P.; Lee, S.; Khader, M.; Ong, G.; Chin, J. Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests. *Decis. Support Syst*. **2020**, *128*, 113160.
19. Kearney, W.D.; Kruger, H.A. Can Perceptual Differences Account for Enigmatic Information Security Behaviour in an Organisation? *Comput. Secur*. **2016**, *61*, 46–58.
20. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Comput. Secur*. **2014**, *42*, 165–176.
21. Aldabbas, H.; Oberholzer, N. The Influence of Transformational and Learning through R&D Capabilities on the Competitive Advantage of Firms. *Arab Gulf J. Sci. Res.* **2024**, *42*, 85–102.
22. Makridis, C.A.; Smeets, M. Determinants of Cyber Readiness. *J. Cyber Policy* **2019**, *4*, 72–89.
23. Hasan, S.; Ali, M.; Kurnia, S.; Thurasamy, R. Evaluating the Cyber Security Readiness of Organizations and Its Influence on Performance. *J. Inf. Secur. Appl.* **2021**, *58*, 102726.
24. Salah, A.; Çağlar, D.; Zoubi, K. The Impact of Production and Operations Management Practices in Improving Organizational Performance: The Mediating Role of Supply Chain Integration. *Sustainability* **2023**, *15*, 15140.
25. Kumar, M.; Yadav, U.; Kumar, S.; Kumar, K. Enhancing Cyber Resilience through Synergistic Cybersecurity and Cyber Defence Strategies. In Proceedings of the 11th International Conference on Cutting-Edge Developments in Engineering Technology and Science (ICCDETS 2024), India, 2024; pp. 862–866.
26. Calvo-Manzano, J.A.; San Feliu, T.; Herranz, Á.; Mariño, J.; Fredlund, L.-Å.; Colomo-Palacios, R.; Moreno, A.M. Towards an Integrated Cybersecurity Framework for Small and Medium Enterprises. In *Systems, Software and Services Process Improvement*; Springer Nature Switzerland: Cham, Switzerland, 2024; Volume 2179, pp. 231–244.
27. Shaikh, A.A.; Syed, A.A.; Shaikh, M.Z. A Two-Decade Literature Review on Challenges Faced by SMEs in Technology Adoption. *Acad. Mark. Stud. J.* **2021**, *25*, 3. Available online: https://ssrn.com/abstract=3823849 (accessed on 18 June 2025).
28. Saad, S.M.; Bahadori, R.; Jafarnejad, H. The Smart SME Technology Readiness Assessment Methodology in the Context of Industry 4.0. *J. Manuf. Technol. Manag.* **2021**, *32*, 1037–1065.
29. Tukimin, R.; Mahmood, W.H.W.; Nordin, M.M. Application of Fuzzy AHP for Supplier Development Prioritization. *Int. J. Adv. Appl. Sci.* **2022**, *9*, 125–134.
30. Saaty, T.L. Decision Making with the Analytic Hierarchy Process. *Int. J. Serv. Sci. Manag. Eng*. **2008**, *1*, 83. https://doi.org/10.1504/IJSSCI.2008.017590
31. Hair, J.F.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed.; SAGE: Los Angeles, CA, USA, 2017; ISBN 9781483377445.
32. Berlilana; Noparumpa, T.; Ruangkanjanases, A.; Hariguna, T.; Sarmini Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. *Sustainability* **2021**, *13*, 13761.
33. Neri, M.; Niccolini, F.; Martino, L. Organizational Cybersecurity Readiness in the ICT Sector: A Quanti-Qualitative Assessment. *Inf. Comput. Secur*. **2024**, *32*, 38–52.
34. Badi, S.; Nasaj, M. Cybersecurity Effectiveness in UK Construction Firms: An Extended McKinsey 7S Model Approach. *Eng. Constr. Archit. Manag*. **2024**, *31*, 4482–4515.

 doi:10.20944/preprints202507.0267.v1

35. Tweheyo, G.; Abaho, E.; Verma, A.M.; Musenze, I. The Mediating Role of Transformational Leadership in the Relationship Between Institutional Pressures and Collaboration with Commercialization of University Research Output: A Pilot Study. *Int. J. Innov. Technol. Manag*. **2024**, *21*, 2450008.
36. Hu, L.; Bentler, P.M. Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives. *Struct. Equ. Model*. **1999**, *6*, 1–55.
37. Kline, R.B. *Principles and Practice of Structural Equation Modeling*, 4th ed.; The Guilford Press: New York, NY, USA, 2016; ISBN 9781462523351.
38. Newsom, J.T. Some Clarifications and Recommendations on Fit Indices. *USP* **2012**, *655*, 123–133.
39. Hoppe, F.; Gatzert, N.; Gruner, P. Cyber Risk Management in SMEs: Insights from Industry Surveys. *J. Risk Finance* **2021**, *22*, 240–260.
40. Rustiarini, N.W.; Bhegawati, D.A.S.; Mendra, N.P.Y.; Vipriyanti, N.U. Resource Orchestration in Enhancing Green Innovation and Environmental Performance in SME. *Int. J. Energy Econ. Policy* **2023**, *13*, 251–259.
41. Chege, S.M.; Wang, D. The Influence of Technology Innovation on SME Performance through Environmental Sustainability Practices in Kenya. *Technology in Society* **2020**, *60*, 101210.
42. Castillo-Vergara, M.; García-Pérez-de-Lema, D. Product Innovation and Performance in SME's: The Role of the Creative Process and Risk Taking. *Innovation* **2021**, *23*, 470–488.
43. Howe-Walsh, L.; Kirk, S.; Oruh, E. Are People the Greatest Asset: Talent Management in SME Hotels in Nigeria during the COVID-19 Crisis. *Int. J. Contemp. Hosp. Manag*. **2023**, *35*, 2708–2727.
44. Sartamorn, S.; Oe, H. Cyberspace Communication in the SME Business Context: Exploring Ways to Improve Technological Readiness and Capability of Thai SMEs. In *Proceedings of the 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*; IEEE: Tenerife, Canary Islands, Spain, 19 July 2023; pp. 1–6.
45. Mohammadian, H.D.; Alijani, O.; Moghadam, M.R.; Ameri, B. Navigating the Future by Fuzzy AHP Method: Enhancing Global Tech-Sustainable Governance, Digital Resilience, & Cybersecurity via the SME 5.0, 7PS Framework & the X.0 Wave/Age Theory in the Digital Age. *AIMS Geosci*. **2024**, *10*, 371–398
46. Jonathan, G.; Thamrongthanakit, T. Cybersecurity Management Practices in Thai SMEs. In *Proceedings of the Nineteenth Midwest Association for Information Systems Conference (MWAIS 2024)*, Peoria, IL, USA, 16–17 May 2024; pp. 1–5.
47. Van Haastrecht, M.; Sarhan, I.; Shojaifar, A.; Baumgartner, L.; Mallouli, W.; Spruit, M. A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. In *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021), Vienna, Austria, 17 August 2021*; ACM: New York, NY, USA, 2021; pp. 1–12.
48. Ajmi, L.; Hadeel; Alqahtani, N.; Ur Rahman, A.; Mahmud, M. A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia. In *Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, May 2019; IEEE: New York, NY, USA, 2019; pp. 1–9.