https://doi.org/10.48048/asi.2026.287132 RESEARCH ARTICLE

Organization Cybersecurity System of Small and Medium Enterprise in Bangkok Metropolitan

Pattarapon Chummee

Business Administration Program, College of Innovation Management,
Valaya Alongkorn Rajabhat University under the Royal Patronage, Pathum Thani 13180, Thailand

([*]Corresponding author's e-mail: pattarapon@vru.ac.th)

Received: 25 July 2025, Revised: 24 September 2025, Accepted: 1 October 2025, Published: 6 October 2025

Abstract

This study aimed (1) to examine the components related to cybersecurity policy and training, regulatory and government policy, absorptive capacity, the impact of the pandemic, and the cybersecurity systems of small and medium-sized enterprises (SMEs) in Bangkok and (2) to investigate the direct causal influence of cybersecurity policy and training, government oversight and policy effectiveness, absorptive capacity, and the impact of the pandemic on the cybersecurity systems of SMEs in Bangkok. Data were collected from 440 SME entrepreneurs in Bangkok. The statistical methods employed included confirmatory factor analysis (CFA) and structural equation modeling (SEM). The analysis revealed that the structural equation modeling framework demonstrated a good model fit, with Chi-square = 125, df = 89, p-value = 0.001, and RMSEA = 0.022.

The research findings from the CFA confirmed acceptable fit indices for Cybersecurity and Training, Government Regulation and Policy, Absorptive Capacity, Pandemic Impact, and SMEs' Cybersecurity Systems. The SEM results further revealed that Cybersecurity Policy and Training (β = 0.691), Government Regulation and Policy (β = 0.826), Absorptive Capacity (β = 0.680), and Pandemic Impact (β = 0.140) had significant positive effects on SMEs' cybersecurity systems.

Keywords: Cybersecurity system, Regulatory and government policy, Absorptive capacity, Pandemic consequences, Cybersecurity training

Introduction

In today's interconnected world, cybersecurity has become more than just a technical concern it's a fundamental business necessity. At its core, cybersecurity encompasses the technologies, processes, and practices organizations use to defend against cyber-attacks, prevent unauthorized access, and protect their valuable data and systems. For businesses that handle sensitive information daily, having strong cybersecurity measures isn't optional anymore; it's essential for survival. (Advance Research Group, 2022; Sendjaja et al., 2024).

The numbers tell a compelling story about this growing market. According to Analysys Mason's (2024) research, the cybersecurity market for small and medium enterprises (SMEs) in the United States is experiencing remarkable growth, with projections showing a 20% increase between 2023 and 2028. By 2028, this market could reach approximately $170 billion, representing a substantial portion of SME revenue as IT services continue driving business expansion. Internationally, SMEs are already investing heavily in cybersecurity, dedicating around $3.3 billion about 20% of total cybersecurity spending to protect their operations.

Thailand presents a particularly interesting case study in this global trend. Recent reports from Cyber DSA (2025) and Bangkok Post (2024) highlight how Thai SMEs are rapidly adopting digital technologies, which has simultaneously increased their exposure to cyber risks. The Thai cybersecurity market for SMEs is projected to reach $871.71 million by 2029, driven by this digital transformation.

However, there's a concerning gap in preparedness. Many Thai SMEs operate without adequate cybersecurity awareness or robust security frameworks, making them attractive targets for cybercriminals. The statistics are sobering: approximately 65% of SMEs in Thailand have already experienced cyberattacks, highlighting the urgent need for better protection (Cyber DSA, 2025; Bangkok Post, 2024).

This vulnerability has created a surge in demand for cybersecurity expertise. The Asian Business (2024) reported that Thailand's need for cybersecurity professionals is expected to grow by 15% over the next decade. Organizations aren't just looking to fill vacant positions they need skilled professionals who can implement predictive security measures, ensure regulatory compliance, and help businesses adapt to an ever-changing threat landscape.

Bangkok, as Thailand's technological and economic hub, sits at the center of this cybersecurity challenge. SMEs in the Bangkok Metropolitan Area face unique pressures as they balance digital innovation with security concerns. The city's concentration of businesses and technological infrastructure makes it both a target-rich environment for cybercriminals and a critical area where strong cybersecurity practices can make a significant difference.

For SMEs navigating this landscape, the solution lies in implementing practical, effective cybersecurity measures. This includes deploying multi-factor authentication systems, maintaining up-to-date antivirus software, conducting regular employee training programs, encrypting sensitive data, and establishing consistent data backup procedures. These steps, while seemingly basic, form the foundation of a resilient cybersecurity strategy.

As cyber threats continue to evolve and become more sophisticated, organizations must develop comprehensive cybersecurity knowledge to respond quickly and effectively to potential attacks. This understanding goes beyond simply having the right technology it encompasses the ability to protect customer data, prevent information theft, combat online fraud, and safeguard sensitive business information that forms the backbone of modern enterprises.

This study makes a unique contribution by focusing on how small and medium-sized enterprises (SMEs) in Thailand, particularly those in the Bangkok Metropolitan Area, deal with cybersecurity. While many previous studies have looked at cybersecurity adoption in developed countries, there has been little research on the specific challenges faced by Thai SMEs. Unlike earlier work that mainly highlights technology adoption in general, this study examines how government policies, limited resources, and the role of decision-makers influence cybersecurity readiness. By looking at these real-world factors, the research not only adds to academic knowledge but also provides practical insights for policymakers, business leaders, and SME managers. This makes the study original and useful, offering guidance on how SMEs in emerging economies can strengthen their cybersecurity resilience.

Research Objective

1. To examine the components of cybersecurity policy and training, the effectiveness of governance and government policy, absorptive capacity, the impact of the pandemic, and cybersecurity systems of small and medium-sized enterprises (SMEs) in the Bangkok Metropolitan Area

2. To investigate the direct causal influence of cybersecurity policy and training, the effectiveness of governance and government policy, absorptive capacity, and the impact of the pandemic on the cybersecurity systems of small and medium-sized enterprises (SMEs) in the Bangkok Metropolitan Area

Theories and literature reviews

The Technology–Organization–Environment (TOE) framework provides an overarching lens to explain the adoption and implementation of cybersecurity systems in SMEs. Within this framework, the technological context includes the adoption of new security technologies, while the organizational context emphasizes the importance of cybersecurity policy and training as internal resources, and the environmental context highlights external pressures such as pandemic consequences that accelerated digital transformation and heightened cybersecurity vulnerabilities (Tornatzky & Fleischer, 1990). This theory thus allows the study to integrate both internal and external determinants of SME cybersecurity systems. Moreover, the influence of government policy and regulations on organizational practices can be explained through Institutional Theory, which posits that firms are subject to coercive, normative, and mimetic pressures that drive them to comply with state regulations and industry standards to maintain legitimacy (DiMaggio & Powell, 1983). In this view, policies and regulations act as external institutional forces that shape organizational behavior and adoption of new practices. Meanwhile, the concept of absorptive capacity is best understood through the Absorptive Capacity Theory, which highlights an organization's ability to recognize the value of new external information, assimilate it, and apply it for commercial or operational purposes (Cohen & Levinthal, 1990). This perspective explains why some firms can more effectively interpret and implement government regulations into their strategic and operational processes, while others struggle due to limited internal learning capabilities. Finally, the Risk Management Theory is also crucial. It argues that cybersecurity systems can be understood as mechanisms to identify, assess, and mitigate risks associated with information assets (Stoneburner, 2002). From this viewpoint, cybersecurity systems function as organizational responses to manage uncertainties and vulnerabilities in the digital environment by adopting proactive measures such as monitoring, access control, and incident response planning.

Cybersecurity policy and training

Small and medium-sized businesses (SMEs) in Thailand, especially those in the Bangkok Metropolitan Area, display differing degrees of cybersecurity awareness and expertise, according to Ben et al. (2023) adaptive cybersecurity training is essential in this situation. This kind of training is made to fit the abilities, knowledge, and development of each learner, which improves learning efficacy and real-world application. Real-world simulation, gamification, and real-time feedback are important strategies in adaptive training programs. These techniques support long-term knowledge retention in addition to raising learner engagement. Furthermore, because it enables flexible and affordable training options, this strategy is especially well-suited to the limited resources of many SMEs. Consequently, training in adaptive cybersecurity becomes crucial.

According to Arslan and Faisal (2024) cybersecurity policies and training have a significant positive influence on the cybersecurity systems of small and medium-sized enterprises (SMEs). Implementing cybersecurity awareness programs tailored to the specific characteristics of SMEs can significantly reduce security incidents caused by human error. Moreover, Pansuwan et al. (2022) found the relational path analysis, this construct is made up of six observed variables. To strengthen their cybersecurity systems, SMEs in Bangkok must have clear cybersecurity policies and regularly train their employees. The risk of cyber threats can be considerably decreased by well-crafted policies that specify suitable preventive measures. Thus, following prior studies, the hypothesis is presented as below:

Hypothesis 1: Cybersecurity policy and training have a positive influence on the cybersecurity systems of small and medium-sized enterprises (SMEs) in the Bangkok Metropolitan Area

Regulations and Government policy

According to a report by Digital Policy Alert (2024) and Rodriguez-Baca et al. (2023) the Thai government has put specific regulations into place to enhance cybersecurity governance for SMEs. These include new regulations requiring cybersecurity service providers to follow established and standardized practices. The two primary goals are to improve the overall cybersecurity environment and make it easier for SMEs to find reliable and affordable service providers.

The regulations also encourage providers to offer pricing structures that are customized to the size and capabilities of SMEs in the Bangkok Metropolitan Area in order to lessen the financial burden of cybersecurity maintenance. According to Reuters (2024) and AustCham Thailand (2024) these policy initiatives are a focused support mechanism that attends to the unique needs of SMEs, which are very different from those of large enterprises.

The study by Al-Somali et al. (2024) examined the effectiveness of cybersecurity governance and government policies applied to small and medium-sized enterprises (SMEs) in Saudi Arabia. The findings revealed that the regulations and government policy positively influences SMEs' cybersecurity practices, highlighting the necessity of designing policies and measures that align with the distinct cultural and economic contexts. Based on the path analysis carried out by Asiri et al. (2024) this construct comprises three observed variables. The study by Song and Park (2024) also underlined how important government policies and efficient governance are to SMEs' cybersecurity systems in Bangkok. One important example of how regulatory frameworks are being used to improve cyber resilience in the SME sector is the Cybersecurity Act B.E. 2562. Thus, it is proposed that:

Hypothesis 2: The government policy and regulations have a positive influence on the cybersecurity systems of SMEs in the Bangkok Metropolitan Area.

Absorptive capacity

According to a study by Taeratanachai and Wiriyakitjar (2025) the size of the company determines the absorptive capacity of SMEs in Thailand with regard to cybersecurity. Due to resource constraints, smaller SMEs frequently find it difficult to adequately address contemporary cyberthreats. Higher absorptive capacity SMEs, on the other hand, are better positioned to implement cutting-edge and successful cybersecurity strategies.

Rakthin et al. (2024) research supports this finding by showing that SMEs, particularly those that handle sensitive data, like those in the healthcare and finance sectors, have started to develop and use their absorptive capacity to manage threats more effectively. Furthermore, Senivongse (2019) and Rakthin et al. (2024) due to a lack of resources, the majority of SMEs in the Bangkok Metropolitan Area find it challenging to increase this capacity, which makes it challenging to handle sophisticated cybersecurity threats. However, SMEs that have a high capacity for absorption can successfully absorb information from outside sources and incorporate it into modern, appropriate safeguards.

Al-Somali et al. (2024) examined SMEs in Saudi Arabia and found that absorptive capacity exerts a significant positive influence on the development of cybersecurity resilience strategies. SMEs with a high level of absorptive capacity are better positioned to adapt to the dynamic nature of cyber threats, thereby enhancing their overall cybersecurity posture. The study further revealed that absorptive capacity shapes both the strategies and the direction of cybersecurity resilience within SMEs, with four observed variables incorporated into this construct. In line with this perspective, Oroni and Xianping (2023) emphasized that SMEs possessing strong absorptive capacity are more capable of anticipating and mitigating cyber threats, as they are able to learn and adopt emerging cybersecurity technologies and practices. Accordingly, the following hypothesis is proposed:

Hypothesis 3: Absorptive capacity has a positive influence on the cybersecurity systems of SMEs in the Bangkok Metropolitan Area

Pandemic consequences

A study by Benjamin et al. (2024) found that both internal organizational resources and external environmental factors had a big effect on how well SMEs were able to adapt after the pandemic. These factors accounted for as much as 59% of the differences in adaptability. In the meantime, Boston et al. (2024) (2022) found that small and medium-sized businesses (SMEs) in Pathum Thani were affected by the pandemic in a moderate way, such as by changing how many foreign workers they hired as the situation changed.

Benjamin et al. (2024) found a significant impact on the strategic approaches of small and medium-sized enterprises (SMEs) when examining the effects of the pandemic on their strategies. The study revealed a positive and significant relationship between the impacts of the pandemic and the cybersecurity systems of SMEs, indicating that the development of cybersecurity systems plays an essential role in supporting SMEs' strategic responses. Furthermore, this construct is represented by four observed variables. In terms of relational influence, Kassar (2023) found that the pandemic heightened cybersecurity awareness among SMEs, prompting many to invest in more robust cybersecurity systems. Consequently, the disruption caused by the pandemic served as a catalyst for greater cybersecurity readiness and accelerated digital transformation among SMEs. Thus, the following hypothesis is suggested:

Hypothesis 4: The impact of the pandemic consequences has a positive influence on the cybersecurity systems of SMEs in the Bangkok Metropolitan Area

SME Cybersecurity systems

The cybersecurity systems of small and medium-sized businesses (SMEs): In spite of the fact that cybersecurity is essential to their operations, SMEs in the UK usually underinvest in it, according to Arroyabe et al. (2024). Major factors contributing to this include their generally low level of digital maturity and the pervasive perception that cyberthreats are not an urgent concern. As a result, cyberattacks continue to pose a serious risk to these companies' finances and reputation.

An open-source Security Operations Center (SOC) is currently being developed by Thailand's National Electronics and Computer Technology Center (NECTEC), per Statista (2024). This project aims to provide easily accessible and reasonably priced cybersecurity solutions, particularly for Thai SMEs with limited funding that cannot directly invest in state-of-the-art cybersecurity infrastructure.

Conceptual model

Based on an extensive review of the existing literature, including studies conducted by Arslan and Faisal (2024), Al-Somali et al. (2024), Rakthin et al. (2024), Benjamin et al. (2024) and Arroyabe et al. (2024), a comprehensive conceptual framework has been developed. This framework integrates the key variables, theoretical perspectives, and empirical findings identified across these studies, providing a structured representation of the relationships and mechanisms under investigation. The resulting framework, which is illustrated in Figure 1, serves as the foundation for understanding the interactions among the main constructs and guiding the subsequent research design and hypothesis development.

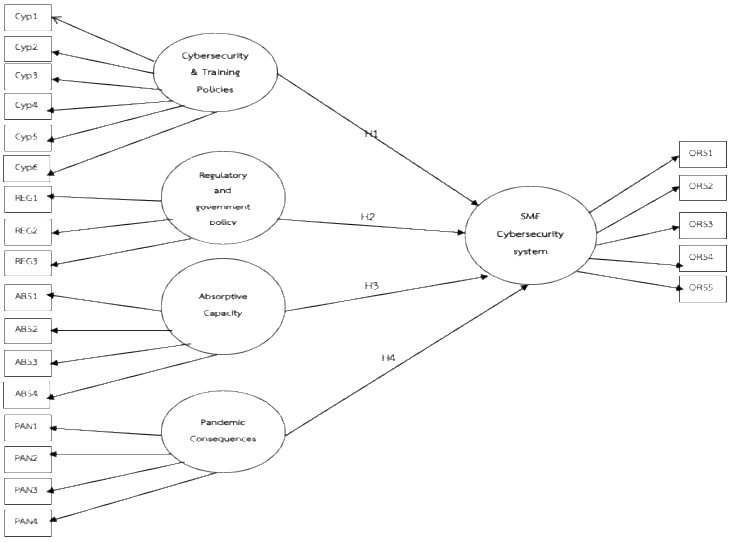


Figure 1 Conceptual framework

Research methods

In this section, the quantitative research methodology is mainly used, using descriptive statistics and analytical statistics to find facts, analyze elements and influences between variables, and supported by qualitative research in small and medium-sized enterprises in Bangkok as the unit of analysis. The research procedure includes:

Research design

This research is applied research, focusing on finding answers in research by searching for facts or finding relationships between data or variables, with the aim of using the research results or findings to create real benefits. Therefore, the research methodology is cross-sectional research for the appropriateness of studying data in businesses that can collect data only once. The researcher uses a quantitative research approach. For the quantitative research, descriptive statistics and inferential statistics are the main research approaches.

Target population and sample group

The target population for this study comprises entrepreneurs of small and medium-sized enterprises (SMEs) operating in Bangkok, which, according to the Office of Small and Medium Enterprises Promotion (2023), includes a total of 521,492 firms. The sample size was determined using Hair et al. (2019) guideline, recommending 5-20 times the number of observable variables. With 22 observable variables related to Cybersecurity and Training (CYP), Regulatory and Government Policy (REG), Absorptive Capacity (ABS), Pandemic Consequences (PAN), and Cybersecurity System (ORS), and applying the upper limit of 20 times, a total sample of 440 respondents was targeted to ensure sufficient statistical power and reliable analysis. Data were collected from managers, individuals with decision-making authority, or representatives of entrepreneurs and companies. A simple random sampling method was employed because it provided every SME in the population an equal chance of being selected, thereby reducing the risk of sampling bias and enhancing the representativeness of the sample. This approach increases the generalizability of the findings to a wider population of SMEs, as the selection process is unbiased and does not depend on predetermined characteristics. To further strengthen the validity of the results, it is important to ensure that the sample size is sufficient to capture the diversity within the SME population and to clearly describe the randomization procedure, which helps maintain the accuracy and credibility of the statistical analysis.

Research instruments

This research used a questionnaire instrument to collect data, consisting of a questionnaire structure with 6 sections: Section 1 General information about the respondents, Section 2 Variables on cybersecurity policy and training, Section 3 Variables on the effectiveness of government supervision and policies, Section 4 Variables on absorptive capacity, Section 5 Variables on the impact of the epidemic, and Section 6 Variables on the cybersecurity system of small and medium-sized enterprises. Whereby Section 1 of the questionnaire consists of open-ended questions, allowing respondents to provide answers freely based on their actual situations. Sections 2-6 consist of closed-ended questions, in which the responses are measured using a Likert scale. In this study, the researcher employed a five-point rating scale (numeric scale), defined as follows: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree.

Validity and reliability

The results of the questionnaire quality assessment in terms of content validity, including coverage, appropriateness, and clarity of language use as evaluated by five experts, revealed item-objective congruence (IOC) values ranging between 0.80 and 1.00. The overall content validity index of the questionnaire was 0.84. Specifically, the sub-dimensions showed the following values: Cybersecurity Policy and Training (CYP) = 0.83, Regulatory and Government Policy (REG) = 0.80, Absorptive Capacity (ABS) = 0.85, Pandemic Impact (PAN) = 0.85, and Organizational Cybersecurity of SMEs (ORS) = 0.88. Reliability was examined using Cronbach's alpha coefficient, following the criteria of Cronbach (1990), which state that alpha coefficients should exceed 0.70. The analysis results indicated that the overall Cronbach's alpha of the questionnaire was 0.85.

Data analysis

Confirmatory factor analysis (CFA) is used to evaluate the measurement model by examining how well each observed variable represents its underlying latent construct. Structural equation modeling (SEM), on the other hand, involves analyzing the relationships between latent constructs and their observed indicators, as well as assessing the structural model that specifies the relationships among the latent constructs themselves. Both CFA and SEM rely on a common set of standard goodness-of-fit indices, which collectively provide an overall evaluation of model adequacy. These indices, including χ^2/df, GFI, AGFI, CFI, NFI, IFI, TLI, RMSEA, and SRMR, are used to determine how well the proposed model represents the collected data, ensuring that the theoretical framework is appropriately reflected in the observed patterns. (Hancock & Mueller, 2001; Schumacker & Lomax, 2016).

Data analysis results

The confirmatory factor analysis (CFA) results for the five latent variables related to cybersecurity in small and medium-sized enterprises (SMEs) in Bangkok are presented in Table 1. These latent variables capture the essential dimensions of cybersecurity readiness and practices among SMEs, encompassing aspects such as policy and training, regulatory effectiveness, absorptive capacity, pandemic impact, and organizational cybersecurity systems. By examining the relationships between observed indicators and their corresponding latent constructs, CFA provides empirical evidence regarding the validity and reliability of the measurement model.

From Table 1, it is evident that the latent variables associated with the cybersecurity systems of SMEs demonstrate a strong level of internal consistency and measurement adequacy. This conclusion is supported by the factor loading values, which are within acceptable thresholds, indicating that each observed variable is a reliable and meaningful representation of its corresponding construct. Additionally, internal reliability scores, as measured by Cronbach's alpha and composite reliability, exceed the recommended benchmark values (Nunnally, 1978; Cronbach, 1990), further confirming the robustness of the measurement model.

Starting with the variable on cybersecurity and training (CYP), the most important observed item is the capability in data recovery (CYP1), with a factor loading of 0.710. This suggests that organizations recognize the importance of being prepared for and recovering from cyber threats. The internal consistency is high, as reflected in a Cronbach's alpha of 0.875, a composite reliability (CR) of 0.904, and an average variance extracted (AVE) of 0.759. The model fit indices are excellent, with χ^2/df equal to 0.036, GFI, AGFI, and CFI all at 1.000, and RMSEA at 0.000.

Next, the variable concerning regulatory and government policy (REG) highlights the presence of supportive government policies for infrastructure (REG3) as its most significant item, with a factor loading of 0.895. Reliability measures also indicate a good level of consistency, with a Cronbach's alpha of 0.790, CR of 0.861, and AVE of 0.676. The model shows good fit, as seen in χ^2/df at 1.94, GFI and AGFI at 1.000, CFI at 1.000, and RMSEA at 0.000.

For absorptive capacity (ABS), the standout observed variable is collaboration with partners in training and assessment (ABS3), which has the highest factor loading of all variables at 0.993. This indicates that organizations actively cooperating with external partners are better equipped to deal with cyber threats. The internal consistency is acceptable, with Cronbach's alpha at 0.754, CR at 0.864, and AVE at 0.681. The model fit indices, including χ^2/df at 0.651, and GFI, AGFI, and CFI all at 1.000, along with RMSEA at 0.000, suggest an excellent model fit.

In the case of pandemic consequences (PAN), the most influential factor is the disruption to business operations (PAN2), which has a factor loading of 0.893. This reflects how the pandemic has pushed businesses to adapt more quickly to digital systems. The Cronbach's alpha is 0.804, CR is 0.888, and AVE is 0.726. The model shows a good fit with χ^2/df at 1.890, GFI at 0.999, AGFI at 0.998, CFI at 0.998, and RMSEA at 0.045.

Finally, the cybersecurity system for SMEs (ORS) is best represented by the availability of protective tools such as firewalls (ORS3), which has a factor loading of 0.914. Internal reliability is strong, with a Cronbach's alpha of 0.778, CR of 0.871, and AVE of 0.693. The model fit is also excellent, as shown by χ^2/df at 0.015, GFI, AGFI, and CFI all at 1.000, and RMSEA at 0.045. Overall, the data support the conclusion that each latent variable meaningfully reflects its underlying observed indicators and that the model fits the data well across all dimensions.

The results of the Structural Equation Modeling (SEM) analysis (Figure 2) show that the external latent variable of the efficiency of regulatory and government policy (REG) has the most influence on the cybersecurity system of SMEs (Organizational Cybersecurity System: ORS), with a path coefficient of 0.826 and a statistical significance level of $p = 0.005$, reflecting that the government's clear, strong policies and effective supervision can have a tangible positive impact on the development and strengthening of the cybersecurity system within the organization, both in terms of structure, standardization, motivation, and enforcement that are consistent with the rapidly changing threat situation in the digital age.

Next, the external latent variable of cybersecurity training and policy (CYP) has a significant positive impact on the cybersecurity system of SMEs, with a path coefficient of 0.691 and a statistical significance level of p = 0. 024, indicating that organizations with clear cybersecurity policies and regular employee training to create the knowledge, understanding, and skills necessary to deal with cyber threats. This will enable effective prevention systems to be created, reduce the risk of personnel errors, and sustainably create a proactive security culture within the organization.

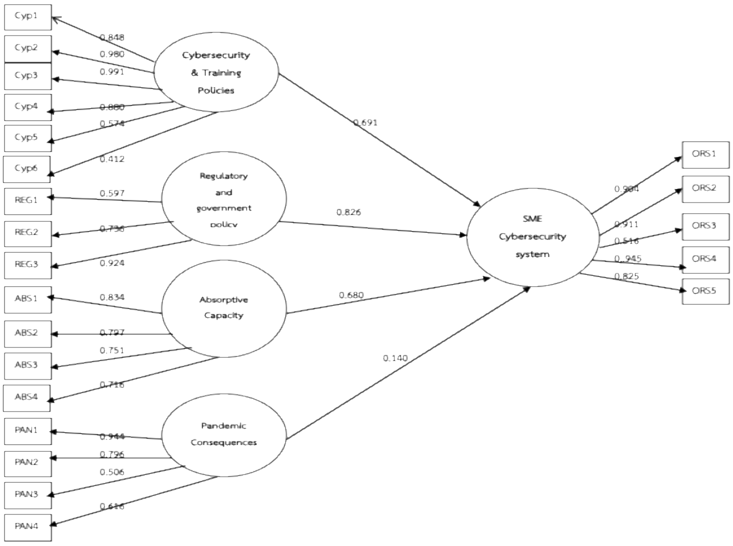
Third, the external latent variable of absorptive capacity (ABS) has a positive effect on the cybersecurity system of SMEs with a path coefficient of 0. 680 and a statistical significance level of p = 0. 014. This means that organizations that can quickly and appropriately learn, interpret, and apply external cybersecurity knowledge, technologies, or management approaches will be able to develop internal security systems that are up-to-date and better respond to complex threats.

Table 1 Result of confirmatory factor analysis

Latent Variable	Item	FaFactor loading	Cronbach's α	CR	AVE
Cybersecurity and Training (CYP)	CYP1	0.710	0.809	0.819	0.754
	CYP2	0.643			
	CYP3	0.433			
	CYP4	0.426			
	CYP4	0.400			
	CYP5	0.372			
	CYP6	0.697			
Regulatory and Government policy (REG)	REG1	0.687	0.837	0.657	0.848
	REG2	0.808			
	REG3	0.895			
Absorptive Capacity (ABS)	ABS1	0.631	0.824	0.531	0.780
	ABS2	0.625			
	ABS3	0.993			
	ABS4	0.640			
Pandemic Impact (PAN)	PAN1	0.669	0.861	0.647	0.875
	PAN2	0.893			
	PAN3	0.874			
	PAN4	0.686			
Cybersecurity System in SME (ORS)	ORS1	0.599	0.883	0.615	0.873
	ORS2	0.713			
	ORS3	0.914			
	ORS4	0.756			
	ORS5	0.877			

Finally, the external latent variable of pandemic consequences (PAN), although it has the lowest path coefficient in the group at 0. 140, has a very high statistical significance level of $p < .001$, indicating that although the driving force from the pandemic situation, such as the COVID- 19 outbreak, has a low direct influence on the cybersecurity system of SMEs, it plays an important role in motivating organizations to accelerate their adaptation, especially in the use of IT systems and telecommunications, which raises awareness of the need to prevent risks and urgently improve their cybersecurity systems.

From Table 2, the analysis of model fit indices indicates that the evaluated model had a Chi-square (χ^2) value of 125 with a corresponding p-value of 0.01. While a p-value less than 0.05 is generally interpreted in statistics as indicating a significant difference between the model and the empirical data, in the context of Structural Equation Modeling (SEM), the Chi-square statistic and its p-value are known to be highly sensitive to sample size. As suggested by Diamantopoulos and Siguaw (2000), a p-value below 0.05 can still be considered acceptable in model fit evaluation.



Chi-square=125, df=89, P-value=0.001, RMSEA=0.022

Figure 2 Synthetic conceptual framework

Table 2 Summary of goodness of fit indices

Fit Index	Criterion	Analysis Result
χ^2	---	125
p-value	< 0.05	0.01
df	---	89
χ^2/df	< 2	1.40
GFI (Goodness of Fit Index)	> 0.90	0.997
AGFI (Adjusted Goodness of Fit Index)	> 0.90	0.996
NFI (Normed Fit Index)	> 0.90	0.903
NNFI (Non-Normed Fit Index)	> 0.90	0.951
CFI (Comparative Fit Index)	> 0.90	0.923
IFI (Incremental Fit Index)	> 0.90	0.914
RFI (Relative Fit Index)	> 0.90	0.914
RMSEA (Root Mean Square Error of Approximation)	< 0.05	0.022
RMR (Root Mean Square Residual)	< 0.05	0.022
Standardized RMR	< 0.05	0.022

When examining other fit indices, the χ^2/df ratio (Chi-square divided by degrees of freedom) was 1.40, which is below the recommended threshold of 2.0, indicating an excellent model fit. Additional indices further confirmed the adequacy of the model: the Goodness of Fit Index (GFI) was 0.997, the Normed Fit Index (NFI) was 0.903, the Comparative Fit Index (CFI) was 0.923, and the Relative Fit Index (RFI) was 0.914, all exceeding the minimum criterion of 0.90. These results suggest that the model explains the variance in the data effectively and demonstrates a high degree of agreement with the observed data. Moreover, error-based indices, including the Root Mean Square Error of Approximation (RMSEA) and the Root Mean Square Residual (RMR), both yielded values of 0.022, well below the maximum acceptable threshold of 0.05, indicating minimal model error and further supporting the statistical adequacy of the model. Overall, although the *p*-value is below 0.05, consideration of other key indices: χ^2/df, GFI, NFI, CFI, RFI, RMSEA, and RMR all of which meet or exceed recommended criteria, confirms that the proposed model demonstrates satisfactory fit with the empirical data.

Table 3 Summary of hypotheses test

No.	Hypothesis	Factor Loading	P-value	Hypothesis Test Result
1	Hypothesis 1: Cybersecurity Policy and Training → Cybersecurity System	0.691	0.024	Supported
2	Hypothesis 2: Regulatory and Government Policy → Cybersecurity System	0.826	0.005	Supported
3	Hypothesis 3: Absorptive Capacity → Cybersecurity System	0.680	0.014	Supported
4	Hypothesis 4: Pandemic Consequences → Cybersecurity System	0.140	< 0.001	Supported

The results of hypothesis testing indicate that the latent variable Regulatory and Government Policy has the strongest positive impact on the cybersecurity system of small and medium-sized enterprises with a factor loading of 0.826 and a p-value of 0.005. This finding supports Hypothesis 2. It demonstrates that the effectiveness of government regulation in establishing guidelines, implementing laws, and providing supportive policies plays a crucial role in enhancing cybersecurity systems. Following this, the variable Cybersecurity Policy and Training also exert a significant positive influence on the cybersecurity system with an estimate of 0.691 and a p-value of 0.024. This result supports Hypothesis 1 and indicates that clear internal policies and employee training in cybersecurity contribute substantially to organizational preparedness to manage and mitigate cybersecurity risks.

The third variable, Absorptive Capacity, shows a slightly lower but still significant effect on the cybersecurity system with a factor loading of 0.680 and a p-value of 0.014. This supports Hypothesis 3 and suggests that organizations capable of learning, adapting, and effectively applying external knowledge are more likely to develop robust cybersecurity systems. Finally, the variable Pandemic consequences, although having the smallest effect, remains statistically significant with an estimate of 0.140 and a p-value less than 0.001. This supports Hypothesis 4 and implies that pandemic events act as a catalyst prompting organizations to improve and strengthen their cybersecurity systems.

Conclusions and discussions

From Objective 1, it was found that the latent variable of cybersecurity and training policies had the most significant component weight in relation to the observed variable of data recovery capability, supported by the quantitative research results. This finding is clearly reinforced by qualitative evidence within the organizational context of Bangkok, where organizations attach great importance to cybersecurity systems, particularly data recovery capability, which is central to recovering from digital threats (National Innovation Agency, 2020).

The results can be discussed as follows: the importance of "data recovery capability" as a key mechanism to strengthen organizational cybersecurity should not be perceived merely as an emergency measure following incidents but should be permanently embedded as part of the organization' score strategic framework. This is especially relevant in Bangkok, a capital city characterized by vast data volumes, high levels of digital connectivity, dense population, and rapidly evolving risks. An effective data recovery plan not only mitigates the impacts of unforeseen disruptions but also enhances proactive adaptability.

Regarding the latent variable of regulatory and government policies, the observed variable with the highest component weight was the presence of government policies to protect infrastructure. This result is supported by the studies of Chatsuwan et al. (2023) and Naw et al. (2023), who found that under increasing regulatory pressures particularly in areas concerning personal data SMEs in Bangkok have adopted internal measures such as appointing Data Protection Officers (DPOs) , organizing cybersecurity training for employees, conducting penetration testing, and establishing incident response plans. These findings indicate that government policies function not merely as regulations but also as a driving force for systematic change in organizational behavior. The discussion highlights that government policy indirectly fosters an organizational culture that emphasizes cybersecurity, extending beyond technology and equipment to encompass employee knowledge, attitudes, and behaviors, as evidenced by initiatives such as systematic awareness training and the integration of ISO standards in government procurement processes.

For the latent variable of absorptive capacity, the observed variable with the highest component weight was cooperation, evaluation, and training with partners. This is consistent with the study of Distanont and Diteeyont (2024), who developed a training program evaluation tool in the hotel industry that measures effectiveness through employee satisfaction and organizational commitment key factors in human resource development for SMEs. Similarly, Phrapratanporn (2019) demonstrated that personnel development practices, such as implementing Individual Development Plans (IDPs) and conducting practical training, significantly enhance employee skills and capabilities, leading to greater satisfaction and organizational commitment. These findings align with the quantitative research results, emphasizing the importance of systematic cooperation and training with partners in driving organizational personnel development.

The results can be further discussed in terms of absorptive capacity: the ability to acquire and apply external knowledge and technology through partner cooperation is essential for strengthening organizational digital resilience. This is particularly important for SMEs, which often face resource and budget constraints. Collaborating with expert partners enables organizations to acquire and implement new knowledge more efficiently, reduce risks from trial-and-error approaches, and enhance competitiveness in rapidly changing markets.

In terms of the latent variable concerning the pandemic consequences, the observed variable with the highest component weight was the impact on business operations. This aligns with the findings of Thanrattanavanich (2022) , who examined SME adaptation during the COVID-19 pandemic in Bangkok. Nearly 90% of entrepreneurs reported experiencing severe economic uncertainty, resulting in reduced business sustainability. Contributing factors included declining consumer demand, supply chain disruptions, and restrictions on business operations. The report also indicated that 84% of SMEs experienced significant declines in revenue and profit, while many faced liquidity challenges and were forced to adopt new strategies, including accelerating digital adoption to maintain business continuity.

The results can be discussed as showing that the pandemic acted as a catalyst for businesses to transform their operating models toward wider digital technology adoption. This shift not only enabled continued operations under social distancing measures but also provided a long-term mechanism for enhancing stability and sustainability. Cybersecurity, in particular, has emerged as a central element in safeguarding business and customer data in an era characterized by increasing reliance on online systems.

For the latent variable of SME cybersecurity systems, the observed variable with the highest component weight was the presence of security protection equipment. This result is supported by the research of Al-Somali (2024) and Thamrongthanakit (2023) , who identified five critical elements for enhancing cybersecurity readiness in SMEs: the adoption of standardized frameworks such as ISO 27001, the appointment of a cybersecurity manager or committee, the development of comprehensive security plans, the improvement of personnel awareness, and the provision of relevant training. The discussion emphasizes that while security protection equipment such as firewalls forms the foundation for protecting organizational data, technological tools alone are insufficient. Equally important is the development of employee knowledge and skills to foster awareness and readiness in responding to cyber threats.

From Objective 2, the results of testing Hypothesis 1 indicated that cybersecurity and training policies have a statistically significant positive influence on SME cybersecurity systems in Bangkok. This finding is supported by Arslan and Faisal (2024) , who demonstrated that tailored security policies and training programs reduced human error-related incidents by 45–65%, while also improving knowledge, awareness, and compliance with cybersecurity protocols. The discussion highlights that among SMEs in Bangkok particularly in service, technology, and manufacturing sectors resource and personnel limitations often hinder the development of comprehensive cybersecurity systems. However, SMEs that implemented context-specific training approaches, such as short workshops of no more than three hours, simulation videos of cyberattacks, and simplified online safety manuals, experienced significant improvements in system security levels.

The results of testing Hypothesis 2 revealed that regulatory and government policies exert a statistically significant positive influence on SME cybersecurity in Bangkok. This is consistent with the findings of Rawindaran et al. (2023), who compared SMEs in Saudi Arabia and the United Kingdom and concluded that government governance and policy frameworks play a pivotal role in enabling SMEs to adopt cybersecurity measures, particularly in contexts where financial, human, and knowledge resources are limited. They also noted that government support significantly reduces resistance to cybersecurity implementation. The discussion suggests that in Bangkok Thailand's digital economy hub most SMEs are aware of cyber threats but remain unprepared to establish systematic protection measures. This is particularly evident among SMEs in online retail, digital services, and logistics sectors, where reliance on IT infrastructure is high. In-depth data collection further revealed that many entrepreneurs struggle to access cybersecurity knowledge and tools, and often lack IT security personnel. Government intervention, therefore, plays a vital role in bridging these gaps.

Hypothesis 3 tested the effect of absorptive capacity and confirmed its statistically significant positive influence on SME cybersecurity systems in Bangkok. This is supported by Utakrit (2023), who found that external knowledge absorption through monitoring cybersecurity news, learning from breaches in other organizations, and participating in collaboration networks enhanced SME adaptability to security technologies and practices. Similarly, Rakthin et al. (2024) emphasized absorptive capacity as a central mechanism for developing context- specific cyber solutions and fostering innovation in risk management. The discussion notes that Bangkok SMEs, particularly those engaged in digital service businesses, e-commerce platforms, and logistics, benefit from promoting internal learning, adopting open knowledge practices, and encouraging employee participation in cybersecurity training and seminars. These approaches help organizations develop more robust cybersecurity systems, particularly in SMEs led by new- generation entrepreneurs who prioritize continuous learning.

Finally, Hypothesis 4 confirmed that the pandemic consequences have a statistically significant positive influence on SME cybersecurity in Bangkok. This result is supported by Bostan et al. (2024) and Leurcharusmee et al. (2024), who found that COVID-19 accelerated the digital transformation of Thai SMEs, forcing greater reliance on information technology for customer engagement, internal management, and online transactions. Consequently, cybersecurity risk management emerged as a critical concern. The discussion indicates that SMEs in Bangkok, many of which quickly adapted to digital business models, are under growing pressure to operate online, particularly in retail, restaurant, and delivery sectors. Businesses in these areas must invest in secure networks, data protection measures, and safer payment systems, underscoring the centrality of cybersecurity in ensuring operational resilience and customer trust.

Recommendations

1. Recommendations for SMEs in Bangkok

SMEs in Bangkok, an area with intensive use of digital technology and facing complex cyber risks, should urgently implement preventive measures and systematically develop cybersecurity systems, starting with setting clear internal security policies and communicating them to employees at all levels, conducting regular training on common threats (e.g. Ransomware, Phishing), and investing in effective prevention tools such as intrusion detection systems (IDS), access control management systems (IAM), and regular backups of data in the cloud.

2. Recommendations for SMEs nationwide

SMEs nationwide should realize that cybesecurity is not an additional cost, but an investment for long-term business security. They should change their mindset from relying on technology only for use to creating a comprehensive cybersecurity management system (Cyber Risk Management System), and should regularly conduct vulnerability assessments of their systems and assign IT security officers, even in small organizations. Businesses that use e-commerce, payment gateway, or online transactions should be encouraged to do so. Data Privacy Policy in line with PDPA.

3. Thailand should accelerate the promotion of a tangible cybersecurity ecosystem for SMEs through the integration of cooperation between government agencies, private organizations, educational institutions, and civil society. A cyber knowledge center for SMEs should be established to provide initial consultation, risk analysis, training, and technical support free of charge to small SMEs. In addition, a national threat database should be created that SMEs can access in real time.

Future Research directions

The findings of this study provide a foundation for advancing the understanding of cybersecurity systems in SMEs; however, several directions remain for future research. First, future studies should expand the geographical scope beyond Bangkok to include SMEs in other regions of Thailand, such as the Eastern Economic Corridor (EEC) or provincial industrial clusters. Comparative studies between urban and non-urban SMEs could yield deeper insights into how contextual factors such as infrastructure, resource availability, and regulatory enforcement influence cybersecurity readiness.

Second, longitudinal studies would be valuable in capturing how SMEs' cybersecurity capabilities evolve over time, particularly in response to external shocks such as new regulatory frameworks, technological advancements, or unforeseen crises similar to the COVID-19 pandemic. This approach would allow researchers to observe dynamic changes rather than relying solely on cross-sectional data.

Third, future research could incorporate mixed-methods approaches with a stronger emphasis on case studies to explore how SMEs internalize absorptive capacity and translate external knowledge into practice. In-depth qualitative evidence may provide richer insights into the mechanisms through which training, partnerships, and government support contribute to sustainable cybersecurity development.

Fourth, cross-national comparative studies should be considered to understand how policy frameworks, cultural norms, and institutional environments influence SMEs' cybersecurity strategies. Such research would not only highlight best practices but also offer practical implications for policymakers aiming to strengthen SME resilience in diverse contexts.

Finally, future research should investigate the role of emerging technologies such as artificial intelligence, blockchain, and big data analytics in shaping cybersecurity systems among SMEs. Examining how these technologies can be integrated into resource-constrained organizations may provide actionable strategies for SMEs to enhance resilience against increasingly complex cyber threats.

References

Advance Research Group. (2022). *Cybersecurity: A business imperative*. Bangkok, Thailand: Advance Research Group Publications.

Analysys mason. (2024). *Cyber security service*. Retrieved from https://www.analysysmason.com/research/content/articles/cyber-incremental-revenue-rdmz0/

Alrawhani, E. M., Romli, A. B., Al-Sharafi, M. A., & Alkawsi, G. (2025). Integrating Information Security Culture and Protection Motivation to

Enhance Compliance with Information Security Policies in Banking: Evidence from PLS-SEM and fsQCA. *International Journal of Human–Computer Interaction*, *14*(19), 1-22.

Al-Somali, S. A., Saqr, R. R., Asiri and Maghrabi (2024), A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability*, *16*(5), 1880.

Arroyabe, M. F., Arranz, C. F., de Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges. *Technological Forecasting and Social Change*, *199*, 123051.

Arslan, H., & Faisal, A. (2024). *Securing SME Digital Frontiers: Designing Cybersecurity Awareness Programs to Minimize Human-Driven Threats*. Retrieved from https://www.researchgate.net/publication/386409772 _Securing_SME_Digital_Frontiers_Designing_Cybersecurity_Awareness_Programs_to_Minimize_Human-Driven_Threats

Asiri, A. M., Al-Somali, S. A., & Maghrabi, R. O. (2024). The integration of sustainable technology and big data analytics in Saudi Arabian SMEs: A path to improved business performance. *Sustainability*, *16*(8), 3209.

AustCham Thailand. (2024). *Thailand lays out new cybersecurity standards*. Retrieved from https://www.austchamthailand.com/thailand-lays-out-new-cybersecurity-standards

Bangkok Post. (2024). *SMEs face growing cybersecurity threats.* Retrieved from https://www.bangkokpost.com

Ben Salamah, F., Palomino, M. A., Craven, M. J., Papadaki, M., & Furnell, S. (2023). An adaptive cybersecurity training framework for the education of social media users at work. *Applied Sciences*, *13*(17), 9595.

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, *19*(2), 134-153.

Bostan Ali, W., Olayinka, J. A., Alam, M. M., & Immelman, A. (2024). Assessing economic implications for micro, small and medium enterprises in Thailand post Covid-19 lockdown. *Plos one*, *19*(2), e0294890.

Brien, E. O., & Hamburg, I. (2014). Supporting Sustainable Strategies for SMEs through Training, Cooperation and Mentoring. *Higher education studies*, *4*(2), 61-69.

Caiazza, R., Phan, P., Lehmann, E., & Etzkowitz, H. (2021). An absorptive capacity-based systems view of Covid-19 in the small business economy. *International Entrepreneurship and Management Journal*, *17*(3), 1419-1439.

Chatsuwan, P., Phromma, T., Surasvadi, N., & Thajchayapong, S. (2023). Personal data protection compliance assessment: A privacy policy scoring approach and empirical evidence from Thailand's SMEs. *Heliyon*, *9*(10), 1-30.

Cronbach, L. J. (1990). *Essentials of psychological testing* (5th eds.). London, United Kingdom: Harper & Row.

Cyber DSA. (2025). *SMEs cybersecurity outlook in Southeast Asia.* Retrieved from https://www.cyberdsa.com

Diamantopoulos, A., & Siguaw, J. A. (2000). *Introducing LISREL: A guide for the uninitiated*. London, United Kingdom: SAGE Publications.

Digital Policy Alert. (2024). *Thailand's cybersecurity policy updates for SMEs.* Retrieved from https://www.digitalpolicyalert.org

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-160.

Distanont, S., & Diteeyont, W. (2024). The Component Analysis of Blended Training Model for SME. *Journal of Business, Innovation and Sustainability (JBIS)*, *19*(1), 187-203.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th eds.). Hampshire, United Kingdom: Cengage Learning.

Hancock, G. R., & Mueller, R. O. (2001). *Structural equation modeling: Confirmatory factor analysis and model evaluation* (pp. 361-389). In Kazdin, A. E. (Ed.). APA handbook of research methods in psychology. New York, USA.: American Psychological Association.

Leurcharusmee, S., Maneejuk, P., Yamaka, W., Thaiprasert, N., & Tuntichiranon, N. (2022). Survival analysis of Thai micro and small enterprises during the COVID-19 pandemic. *Journal of Business Economics and Management*, *23*(5), 1211-1233.

Liu, C., Liang, H., Wang, N., & Xue, Y. (2022). Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender. *Information Technology & People*, *35*(2), 802-834.

Kassar, G. (2023*). Exploring cybersecurity awareness and resilience of SMEs amid the sudden shift to remote work during the coronavirus pandemic: A pilot study* (pp. e107358). In proceeding of the conferences on arpha conference abstracts. Ascencia Business School.

Uthakrit. (2022). A systematic review of organizational readiness guidelines for enhancing cyber security. *Information Technology Journal. 9*(1), 94-102.

National Innovation Agency (2020). *Cloud Computing Adoption in Small and Medium Enterprises (SMEs). National Innovation Agency.* Retrieved from https://nia.or.th

Naw, T. D., & Kohsuwan, P. (2023). Roles of Perceived Knowledge, Risk, and Trust in Cybersecurity Solution Implementation: A Study in Bangkok, Thailand. *Human Behavior, Development & Society*, *24*(3), 81-92.

Office of Small and Medium Enterprises Promotion. (2023). *SMEs statistics report in Thailand, 2023.* Retrieved from https://www.sme.go.th

Oroni, C. Z., & Xianping, F. (2023). Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance. *Journal of Data, Information and Management*, *5*(4), 345-361.

Pansuwan, C., & Chitsawang, S. (2023). Guidelines for governance and response to cyber security threats of organizations in the digital age. *Rajapark Journal*, *17*(53), 103-119.

Phrapratanporn, B., Wararatchai, P., Aunyawong, W., & Rashid, N. R. N. A. (2019). Enhancing supply chain performance of SMEs in Thailand using the integrated personnel development model. *International Journal of Supply Chain Management*, *8*(5), 176-186.

Rakthin, S., Chaithanapat, P., Otakanon, B., & Thananusak, T. (2024). Absorptive capacity for market knowledge and knowledge creation outcomes: the case of Thai SMEs. *Knowledge Management Research & Practice*, *22*(4), 327-339.

Rawindaran, N. (2023). *Impact of cyber security awareness in small, medium enterprises (SMEs) in Wales* (Doctoral dissertation). England: Cardiff Metropolitan University.

Reuters. (2024). *Thailand to pursue new policies to boost and protect digital economy*. Retrieved from https://www.reuters.com/world/asia-pacific/thailand-pursue-new-policies-boost-protect-digital-economy-2024-11-08

Rodriguez-Baca, L. S., Allagi, S., Larrea-Serquen, R., Cruzado, C. F., Alarcon Diaz, M., Garcia-Hernández, S., & Daza Monteiro, J. (2023). Experimental Study based on the Implementation of a Regulatory Framework for the Improvement of Cyber Resilience in SMEs. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(3), 199-205.

RungArun Krasae Sinthu, Wisanupetch Thai, Peeraya Setthaphat, & Klai Rung Krasae Sinthu. (2023). Adaptation of Small and Medium Enterprises (SMEs) Affected by the Outbreak of Coronavirus Disease 2019. *Journal of Innovation in Education and Research, 7*(1), 260-274.

Schumacker, R. E., & Lomax, R. G. (2016). *A beginner's guide to structural equation modeling* (4th eds.). New York, USA.: Routledge.

Sendjaja, T., Rachbini, D. J., Astini, R., & Asih, D. (2024). Beyond Branches: How Fintech and Sustainable Innovation are Reshaping the Banking Landscape in Indonesia. *Applied Business and Administration Journal*, *3*(3), 67-78.

Senivongse, C., Bennet, A., & Mariano, S. (2019). Clarifying absorptive capacity and dynamic capabilities dilemma in high dynamic market IT SMEs. *VINE Journal of Information and Knowledge Management Systems*, *49*(3), 372-396.

Song, J., & Park, M. J. (2024). A system dynamics approach for cost-benefit simulation in designing policies to enhance the cybersecurity resilience of small and medium-sized enterprises. *Information Development*, *0*(0).

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-30.

Taeratanachai, C., & Wiriyakitjar, R. (2025). Cybersecurity Analysis in Thailand: Trends, Challenges, and Policy Insights from Case Studies of SMEs, Mobile Banking, and Port Infrastructure. *National Defense Studies Institute Journal*, *16*(1), 43-61.

Thanrattanavanich, C. (2022). Adaptation of Small and Medium Enterprises (SMEs) Under the Pandemic Situation of the Coronavirus Disease 2019 (COVID -19) in Bangkok Metropolis. *Journal of Humanities and Social Sciences, Rajapruk University*, *8*(3), 296–310.

Thamrongthanakit, T. (2023). *Impacts of cybersecurity practices on cyberattack damage and protection among small and medium enterprises in Thailand* (Master’s Thesis). Sweden: Stockholem University.

The Asian Business. (2024). *Cybersecurity job demand in Thailand to rise 15% over next decade.* Retrieved from https://www.theasianbusiness.com

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation.* Lexington, USA: Lexington Books.

Utakrit, N., & Kaewsa-ard, A. (2023). A systematic review of organizational preparedness approaches to enhance cybersecurity. *Information Technology Journal KMUTNB, 19*(1), 94-102.