International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (Apr-23)

http://dx.doi.org/10.12785/ijcds/130153

A Study of Distinguishing Factors between SME Adopters versus Non-Adopters of Cybersecurity Standard

Wipawadee Auyporn[1], Krerk Piromsopa[2] and Thitivadee Chaiyawat[3]

[1]*Technopreneurship and Innovation Management Program (TIP), Graduate School, Chulalongkorn University, Bangkok, Thailand*
[2]*Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand*
[3]*Department of Statistics, Chulalongkorn Business School, Chulalongkorn University, Bangkok, Thailand*

E-mail address: 6087796020@student.chula.ac.th, krerk@cp.eng.chula.ac.th, thitivadee@cbs.chula.ac.th

Received 19 Jan. 2022, Revised 18 Dec. 2022, Accepted 6 Feb. 2023, Published 16 Apr. 2023

Abstract: Digital technology is a vital factor for driving digital business today. In parallel, cybersecurity-related threats are also increasing and may impact the operation of a business. So, the national government in each country may need to encourage digital enterprises to adopt a cybersecurity standard to reduce cybersecurity risks. However, Small and Medium Enterprises (SMEs) have a low rate of cybersecurity standard adoption due to their limitations. This study aims to identify distinguishing factors between SME adopters versus non-adopters of cybersecurity standards in Thailand and provide recommendations for policymakers to improve the adoption of cybersecurity standards in SMEs. A quantitative methodology was used to survey SME IT leaders in Thailand. The data were collected using online questionnaires. The 28 survey items assessed 11 factors in 2 main categories: (1.) demographics characteristics of SMEs and (2.) cybersecurity attitudes of SMEs. This study involved 312 participating SMEs. The major group of SMEs (65.4%) had not adopted any of the cybersecurity standards, and the other group of SMEs (34.6%) had adopted some cybersecurity standards. The Pearson's Chi-Square Test was employed to test what factors were significant differences between responses of these two groups. The results revealed that the significant factors include the size of an organization, the intensity of IT usage, the number of IT staff, the number of IT security staff, the amount of investment in IT, the amount of investment in IT security, the awareness of organizational cybersecurity risks, the perceived cybersecurity needs of customers, and the intention to adopt a cybersecurity standard. Lastly, recommendations for policymakers are provided.

Keywords: SMEs, Cybersecurity Standard Adoption, Policymakers, Cybersecurity Standard Promotion

1. INTRODUCTION

As the uses of digital technologies are growing in this era, on the other hand, cybersecurity-related losses are also increasing [1]. According to the Verizon Data Breach Investigations Report, 28 percent of breaches involved small business victims, especially the APAC region. This region is being targeted mostly by financially motivated factors. And, impacts of ransomware incidents in 2021 range between 69 and 1,155,775 USD per organization [2]. Cyber-attacks might affect the operation of small businesses. According to the Cyber Security Statistics, 60% of small companies go out of business within six months after a cyberattack [3]. Since SMEs are the source of employment and generate a significant part of GDP in many countries. The disruption of small businesses might impact the economic stability of a country. Therefore, the national government in each country may need to increase capability and ensure the stability of SMEs.

However, SMEs have limited resources, less protection, and less standardization of work processes than large organizations [4], [5]. Moreover, hackers might see SMEs as gateways to enter larger organizations. SMEs are usually vendors, outsources, or partners of larger organizations. In many cases, large organizations were affected by the supply chain attack, and we found that SME victims were usually involved in supply chain attacks [2]. Therefore, every party in the supply chain needs to implement good cybersecurity practices to reduce these cybersecurity risks [6].

Adopting a cybersecurity standard is one of the good strategic approaches to reduce cybersecurity risks [7], although SMEs in many countries are not necessary to be certified a cybersecurity standard due to laws and regulations. Cybersecurity standards facilitate sharing of knowledge and best practices by helping to ensure understanding of concepts, terms, and definitions, which prevents errors. Moreover, many standards, for example, the ISO/IEC 27000

series of standards, provide flexibility that can be applied by all types of organizations, regardless of sector, size, or revenue [8]. Thus, implementing cybersecurity standards can help improve cybersecurity practices in any organization, and this will also improve confidence to stakeholders of the implemented organizations, especially customers [9], [10].

In addition, there are many standards that publish for SMEs. For instance, ENISA published an overview study titled "Information security and privacy standards for SMEs". ENISA also states that with the proof of compliance to a cybersecurity standard, SMEs can achieve a possible competitive advantage when dealing with corporate clients from private and public sectors [11]. However, adopting a cybersecurity standard is still challenging for SMEs, because SMEs lack the resources to participate in the implementation, and are often constrained by the budget that is available for use in implementing cybersecurity compliance (which does not generate revenue). While research in cybersecurity practices in SMEs has been under-researched unlike extensive research into IT practices in large organizations [4].

Existing studies are focusing on the personal behaviors of violators of cybersecurity measures. For example, H. U. Khan [12] studied distinguishing factors between violators and non-violators of cybersecurity measures in organizations. R. Khatib [13] and H.P. Shih [14] studied cybersecurity non-compliant behaviors of employees in order to take promotion and prevention mechanisms for cybersecurity in SMEs. However, there had been limited studies about non-compliant organizational characteristics, especially SMEs. Moreover, previous studies usually explored gaps of SMEs toward the adoption of the cybersecurity standard and provided recommendations for SMEs [5], [15]. These studies addressed what efforts shall be made by SMEs. However, there are still rooms for policymakers that can help SMEs to overcome SMEs' constraints. This research not only explores distinguishing factors between SME adopters and non-adopters of cybersecurity standards by using Pearson's Chi-Square Test but also provides implications and recommended actions for policymakers. Therefore, policymakers can use this crucial information to enhance cybersecurity standard promotion strategies for SMEs, and the result of this will increase competitive advantage for SMEs, improve the cybersecurity practices in SMEs, and eventually enhance the cybersecurity overall picture for every business in the supply chain. The conceptual framework of this study is shown in Figure 1.

2. LITERATURE REVIEW

The literature review covers two main categories. The first category is related to the demographic characteristics of SMEs. The second category is related to the cybersecurity attitudes of SMEs. The significant factors would be discussed concerning each of the above categories.

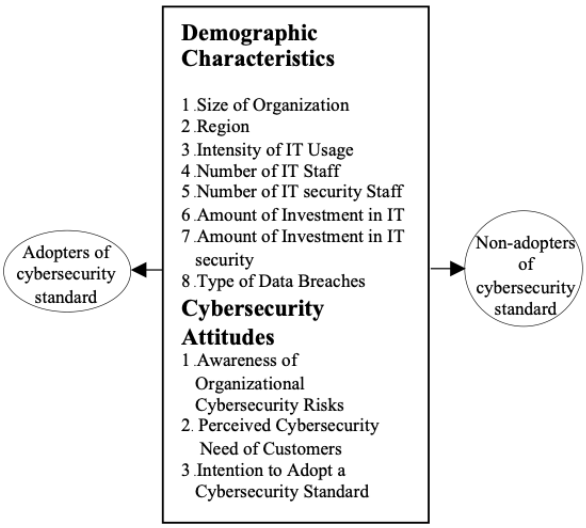

Figure 1. Conceptual framework of this study

A. *Demographic characteristics*

The literature review revealed that various characteristics of SMEs can affect the adoption of cybersecurity standards of SMEs. In this section, many demographic factors were studied. In prior literature, many characteristics can affect SME cybersecurity maturity. According to F. Mijnhardt [16], organizational characteristics influence SME information security maturity. The organizational characteristics include 1. general traits of organizations, 2. IT dependency, and 3. IT complexity. Firstly, the general trait of an organization includes a type of organization. For example, whether the organization is a small or medium enterprise (which is usually classified by the amount of revenue and the number of employees). Secondly, the IT dependency incorporates the intensity of IT usage, which provides an idea of how important IT is in supporting business processes. For example, if a business cannot run for a long period without IT support, that means the business has high intensity of IT usage and has a high dependency on IT. Lastly, the IT complexity incorporates the amount of investment supporting the IT environment and the percentage of annual revenues spent on IT. The IT budget is the quickest and easiest method to determine the complexity of the IT environment in an organization.

According to E. Dzidzah [10], SMEs rarely have a pool of experts; they have a few numbers of IT staff and IT security staff, so the complexity of deploying cybersecurity solutions is an obstacle for SMEs. Some small businesses have IT staff but seldom have IT security staff within the organization dedicated to security [4]. The number of IT staff and IT security staff factors are also in line with F. Mijnhardt's. S. Kabanda [17] also explored that SMEs' internal factors such as IT security budget can also affect SME cybersecurity practices in developing countries. The finding pointed that the lack of adequate IT security investment is one of the issues associated with SMEs lack of having

stringent cybersecurity mechanism. M. Tripathi also studied the impact of types of data breaches on organizations. According to M. Tripathi [18], the type of data breach includes hacking or malware, debit or credit card fraud, accidental disclosure, insider, and physical loss. Therefore, the following hypotheses were framed to the organizational characteristic variables discussed above:

H1: There is a significant difference in the type of organization between adopters and non-adopters of cybersecurity standards.

H2: There is a significant difference in the region between adopters and non-adopters of cybersecurity standards.

H3: There is a significant difference in the intensity of IT usage between adopters and non-adopters of cybersecurity standards.

H4: There is a significant difference in the number of IT staff between adopters and non-adopters of cybersecurity standards.

H5: There is a significant difference in the number of IT security staff between adopters and non-adopters of cybersecurity standards.

H6: There is a significant difference in the amount of investment in IT between adopters and non-adopters of cybersecurity standards.

H7: There is a significant difference in the amount of investment in IT security between adopters and non-adopters of cybersecurity standards.

H8: There is a significant difference in the type of data breaches between adopters and non-adopters of cybersecurity standards.

B. Cybersecurity Attitudes

1) Awareness of Organizational Cybersecurity Risks

The literature about awareness of organizational cybersecurity risks revealed the implications in organizational behaviors and the protection of organizational assets. W. He [19] recommended that enterprises should have cybersecurity training and awareness programs because the awareness of the potential risks of being involved in a negative security event results in precautionary behaviors. And this affects the successful implementation of security procedures and guidelines. The lack of awareness exposes an organization to significant risk in ensuring the security and protection of organizational assets. J. Kaur [20] also found that information security awareness significantly influences CIA (Confidentiality, Integrity, and Availability) of information. Therefore, the following hypothesis can be formed.

H9: There is a significant difference in the awareness of organizational cybersecurity risks between adopters and non-adopters of cybersecurity standards.

2) Perceived Cybersecurity Needs of Customers

The literature revealed that the perceived cybersecurity needs of customers influence organizational behaviors. According to J. Prodanova [9], perceived security and privacy issues of customers affect the repurchase intention of customers. Security and privacy issues reflect customers' belief that their confidential information will not be disclosed, and the online transaction is secure. Therefore, to achieve customers' repurchase intention, an organization must care about customers' needs in security and privacy, and strengthen their cybersecurity practices. A.D. Veiga [21] also said that customer expectation and preferences result in information protection culture; information usage perception results in information attributes. The information usage perception includes the perception of information security and privacy usage requirements. Since today's customers require products or services that are reliable, secure, and protective of the confidentiality of their personal information [10]. Therefore, the following hypothesis can be formed.

H10: There is a significant difference in the perceived cybersecurity needs of customers between adopters and non-adopters of cybersecurity standards.

3) Intention to Adopt a Cybersecurity Standard

The literature also shows that the intention to adopt a cybersecurity standard influences organizational behavior. A.D. Veiga also studied management buy-in including the perception of management buy-in toward information security and the importance attached to the concept by senior managers and executives. The concept of management or the management support adheres to the information security policy [21]. S. Kabanda [17] also addressed that management support influences cybersecurity implementation in South African SMEs. The perception includes the perception of cybersecurity standards that can help enhance the security of an organization's systems. Therefore, the following hypothesis can be formed.

H11: There is a significant difference in the intention to adopt a cybersecurity standard between adopters and non-adopters of cybersecurity standards.

3. RESEARCH METHODOLOGY

The approach of this study is quantitative. Questionnaires were used as a research tool for data collection, and online questionnaires were sent to SME IT leaders. Lists of SMEs were obtained from the Office of Small and Medium Enterprises Promotion (OSMEP), Thailand [22]. The factors about demographic characteristics and cybersecurity attitude were examined.

A. Population and Samples

The population of this study consisted of Thai SMEs mainly focused on IT-related firms. The type of enterprises that participated in the survey was selected from the service sector in three activity groups: (1) information technology

TABLE I. LIST OF SCALE ITEMS

Construct	Measure
1.Awareness of Organizational Cybersecurity Risks (AOCR) (Cronbach Alpha = 0.840)	
AOCR1	Your organization has cybersecurity risks due to the adoption of digital technology
AOCR2	Businesses in your organization's industry have cybersecurity risks.
AOCR3	You have heard that companies in your organization's industry have been exposed to cyber threats.
AOCR4	Cybersecurity threats are evolving, and new threats are emerging.
AOCR5	Today's cybersecurity threats are becoming more severe and growing.
AOCR6	Your organization's executives understand cybersecurity.
AOCR7	Your organization knows and is aware of related information technology laws such as the Personal Data Protection Act or GDPR.
AOCR8	Your organization's employees are aware of cybersecurity risks.
AOCR9	Businesses in your organization's industry regularly provide knowledge or share information about cybersecurity.
AOCR10	Your organization has a documented cybersecurity policy.
2. Perceived Cybersecurity Needs of Customers (PCNC) (Cronbach Alpha = 0.847)	
PCNC1	Your customers need products or services that are reliable.
PCNC2	Your customers have a need for products or services that are secure.
PCNC3	Your customers value the confidentiality of their personal information.
PCNC4	Customer confidence in products or services is important to your business operations
PCNC5	Today's customers in your industry have usage requirement in security and privacy.
3. Intention to Adopt a Cybersecurity Standard (IACS) (Cronbach Alpha = 0.872)	
IACS1	Your organization is interested in implementing cybersecurity standards.
IACS2	Your organization believes that obtaining a cybersecurity standard certification can help increase the level of reliability of its products and services.
IACS3	Your organization believes that following cybersecurity standards can help enhance the security of your organization's systems.
IACS4	Your organization has a need to apply cybersecurity standards.
IACS5	Your organization is currently studying or is interested in studying cybersecurity standards such as ISO / IEC 27001 or NIST to apply to your organization.

service (2) financial service, and (3) insurance service. Since these are the activity groups that are most likely to operate businesses using IT and handle the personal information of customers in IT systems, so they are relevant to cybersecurity issues. The samples were randomly picked up from the database of SMEs in these three activity groups in Thailand. The number of samples was calculated via Hair, Black, Babin, and Anderson [23]. There were 312 SME samples collected, which achieved the minimum requirement of the sample size of 10*28 = 280 samples.

B. Survey Items

The survey had 28 question items in 2 categories: 1.) demographic characteristics, and 2.) cybersecurity attitudes. In category cybersecurity attitudes, we measured 3 factors with 20 questions as shown in Table I, which are 1. perceived organizational cybersecurity risks, 2. perceived cybersecurity needs of customers, and 3. intention to adopt a cybersecurity standard. Each factor included between 5 and 10 statements; whose answers were measured with a 5-point Likert scale ranging from strongly disagree (1) to strongly agree (5). For instance, the following statement was used to measure the perceived organizational cybersecurity risks factor "Your organization has cybersecurity risks due to the adoption of digital technology." On the other hand, "Your customers need products or services that are reliable" was used to measure the perceived cybersecurity needs of customers factor. The statement items were mainly adopted from the prior literature. The list of scale items is shown in Table I.

And, in category demographic characteristics, we measured 8 factors with 8 questions as shown in Table II, which are 1. size of an organization, 2. region, 3. intensity of digital technology usage, 4. number of IT staff, 5. the number of IT security staff, 6. an amount of investment in IT, 7. the amount of investment in IT security, and 8. type of security breaches. The list of the question items is presented in Table II.

C. Reliability and Validity of the Instrument

For the reliability, each variable was tested by Cronbach's Alpha to examine the internal consistency of the questionnaire. For the awareness of cybersecurity risks variable, the reliability for this instrument was acceptable

TABLE II. SAMPLE DEMOGRAPHICS OF THIS STUDY

Variables	N = 312	
	Number of responses	Percentage
Q1. Size of organizations		
Small enterprise	180	57.7%
Medium enterprise	132	42.3%
Q2. Region		
Central	231	74.1%
North	49	15.7%
East	20	6.4%
South	12	3.8%
Q3. Intensity of digital technology usage		
High	186	59.6%
Medium	90	28.8%
Low	36	11.5%
Q4. Number of IT staff		
None	24	7.7%
1-3	162	51.9%
4-10	48	15.4%
More than 10	78	25.0%
Q5. Number of IT security staff		
None	72	23.1%
1-3	150	48.1%
4-5	36	11.5%
More than 5	54	17.3%
Q6. Amount of investment in IT		
Less than 1 million baht per year	201	64.4%
Between 1-2 million baht per year	64	20.5%
More than 2 million baht per year	48	15.4%
Q7. Amount of investment in IT security		
None	108	34.6%
Between 1-500K baht per year	102	32.7%
Between 500K – 1 million baht per year	66	21.2%
More than 1 million baht per year	36	11.5%
Q8. Type of data breaches (more than 1 answer possible)		
malware infection	108	34.6%
Phishing email	29	9.2%
DDoS	18	5.7%
Website defacement	8	2.5%
Data Leakage	6	1.9%
Service down	6	1.9%

TABLE III. SME CYBERSECURITY STANDARD ADOPTION

Adoption of cybersecurity standard	Number of responses	percentage
No	204	65.4%
Yes	108	34.6%

(Cronbach Alpha = 0.840 > 0.7). For the perceived cybersecurity needs of customers, the reliability for this instrument was acceptable (Cronbach Alpha = 0.847 > 0.7). For the intention to adopt a cybersecurity standard, the reliability for this instrument was acceptable (Cronbach Alpha = 0.872 > 0.7). For the validity of variables, the items were reviewed by 3 experts and tested for content validity. Index of item-objective congruence (IOC) by Rovinelli and Hambleton [24] was examined. Next, the items were revised again according to the experts' recommendations. The Indexes of item-objective congruence (IOC) of all items are no less than 0.66.

D. Data Collection Method

This study surveyed SMEs in Thailand. Populations were drawn from SMEs of the service sector in Thailand. The samples were randomly selected. The sample sizes are calculated via Hair, Black, Babin, and Anderson [23]. A total of 600 Sampled SMEs was contacted by mail. Mails were sent to the IT manager, CTO, or CEO, one letter per one organization. And the participating SMEs responded by scanning the QR code of the link to online questionnaires to answer the questions. The calculated response rate was 52 percent. A total of 312 completed surveys were collected.

E. Data Analysis Method

We used IBM SPSS Statistics version 24 on Windows. Descriptive statistics and inferential statistics were used to analyze the data. We examined demographic characteristics of sampled SMEs, and we explored cross-tabulation of SME profiles among variables. Then we used inferential statistics to test our hypotheses. The Pearson's Chi-square Test with the confidence level of 95 percent (p-value of less than 0.05) was used when considering statistical significance in this study.

4. RESULTS AND ANALYSIS

First, we examined the demographic variables using descriptive statistics. A total of 312 completed questionnaires were collected. Table II presents the demographics of the survey participants with the number of responses and percentages.

A. Descriptive Statistics

Table II shows that most of the respondents were small enterprises (57.7%, 180/312). And the majority of respondents were in the central part of Thailand (74.1%, 231/312). Since our samples were drawn from three activity groups: (1) information technology service (2) financial service, and (3) insurance service, the majority of SMEs (59.6%, 186/312) have high intensity of usage in information technologies. The majority of SMEs (51.9%, 162/312) have only between 1 to 3 IT staff, and the majority of SMEs (48.1%, 150/312) have between 1 to 3 IT security staff. The majority of SMEs (64.4%, 201/312) invest in IT less than 1 million baht per year. The majority of SMEs (34.6%, 108/312) have no investment in IT security at all. And the type of security incident that was mostly occurred was malware infection.

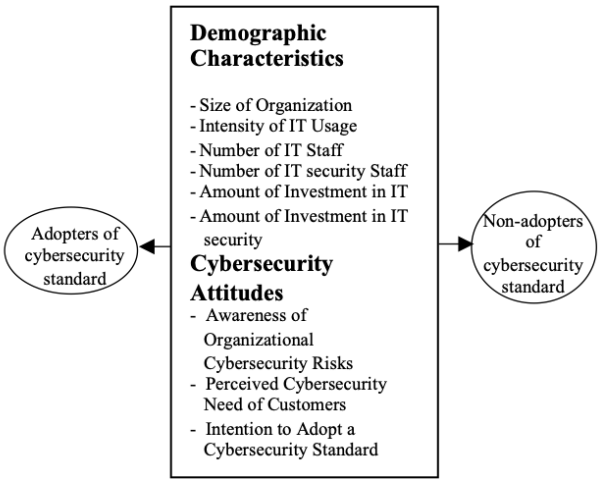

Figure 2. Summary of the significant factors

From Table III, the majority of SMEs (65.4%, 204/312) had not adopted any of the cybersecurity standards, and the other group of SMEs (34.6%, 108/312) had adopted some cybersecurity standards.

B. Testing hypotheses

Next, we tested distinguishing factors between these two groups; SMEs adopters and SMEs non-adopters of cybersecurity standard, using the Pearson's Chi-Square Test. The testing results for demographic factors and attitudes toward cybersecurity factors are shown in Table IV. And, the summary of significant factors is shown in Figure 2.

5. DISCUSSION

According to the statistical analysis (Table IV), larger-size enterprises tends to have a higher chance of implementing cybersecurity standard. Moreover, enterprises with higher usage of information technology, enterprises with a higher number of IT staff or IT security staff, and enterprises with a higher amount of IT or IT security investment will have a higher chance of implementing cybersecurity standards. Additionally, the study found that enterprises, which have awareness of cyber risks, perceive customer needs of implementing a standard, and have the intention to adopt a cybersecurity standard, will have a higher chance of implementing cybersecurity standards. Therefore, this research implies that there are still rooms for policymakers to promote the adoption of the cybersecurity standard in SMEs. More details on recommended actions are provided.

A. Implications for policymakers

From the testing result in Figure 2, there are some implications and recommended actions provided for the policymakers in order to promote the adoption of cybersecurity standards in SMEs as presented in Table V.

6. CONCLUSIONS

This study achieved the objectives by conducting a quantitative study of 312 SME samples. We applied Pearson's

TABLE IV. CHI-SQUARE TESTING RESULTS FOR DEMOGRAPHIC FACTORS AND ATTITUDES TOWARDS CYBERSECURITY EFFECTS

Hypothesis	Factors	Pearson Chi-Square Value	P-Value	Conclusion
Demographic factors				
H1	Size	3.743	.000*	There is a significant difference in the type of organization between adopters and non-adopters of cybersecurity standards.
H2	Region	2.561	.276	There is no significant difference in the region between adopters and non-adopters of cybersecurity standards.
H3	Intensity of IT usage	38.136	.000*	There is a significant difference in the intensity of information technology usage between adopters and non-adopters of cybersecurity standards.
H4	Number of IT staff	57.992	.000*	There is a significant difference in the number of IT staff between adopters and non-adopters of cybersecurity standards.
H5	Number of IT Security Staff	49.416	.000*	There is a significant difference in the number of IT security staff between adopters and non-adopters of cybersecurity standards.
H6	Amount of investment in IT	30.154	.000*	There is a significant difference in the amount of investment in IT between adopters and non-adopters of cybersecurity standards.
H7	Amount of investment in IT security	96.933	.000*	There is a significant difference in the amount of investment in IT security between adopters and non-adopters of cybersecurity standards.
H8	Type of data breaches	2.578	.397	There is no significant difference in the type of data breaches between adopters and non-adopters of cybersecurity standards.
Attitudes towards cybersecurity				
H9	Awareness of organizational cybersecurity risks	162.538	.000*	There is a significant difference in the awareness of organizational cybersecurity risks between adopters and non-adopters of cybersecurity standards.
H10	Perceived cybersecurity needs of customers	26.991	.000*	There is a significant difference in the perceived cybersecurity needs of customers between adopters and non-adopters of cybersecurity standards.
H11	Intention to adopt a cybersecurity standard	53.459	.000*	There is a significant difference in the intention to adopt a cybersecurity standard between adopters and non-adopters of cybersecurity standards.

Chi-Square to test what factors are significant differences between responses of adopters and non-adopters of cybersecurity standards, and the implications for policymakers are provided. The results show that at a 0.05 level of significance, 9 factors are significantly related to the standard adoption as shown in Figure 2. The significant factors consist of the size of an organization, the intensity of digital technology usage, the number of IT staff, the number of IT security staff, the amount of investment in IT, the amount of investment in IT security, the awareness of organizational cybersecurity risks, the perceived cybersecurity needs of customers, and the intention to adopt a cybersecurity standard.

Finally, this research provides recommended actions for policymakers as initial steps to improve the cybersecurity standard adoption in SMEs. The results of this research can be used in various applications to develop various tactics to encourage SMEs to improve their implementation of cybersecurity standards, for example, communicating about cyber risks and customer requirements of security and privacy, providing resources and financial incentives for SMEs, and also developing training programs to produce more IT and IT security professionals. However, there are three limitations in this study that could be addressed in the future study. First, the survey was based on SME IT leaders who were willing to answer the questionnaires, therefore this comprises voluntary bias. Second, the samples were based on SMEs in Thailand, so the results might not be generalized to SMEs in different regions due to different regional features. Future research might study in different regions. Third, this study was conducted using a Cross-

TABLE V. RECOMMENDED ACTIONS FOR POLICYMAKERS

Significant Factors	Implications	Recommended actions for policymakers
Demographic Characteristics		
Size	Larger enterprises have higher chance of implementing standard	•Policymakers should pilot medium-sized enterprises for the cybersecurity standard compliance, then expand to small-sized enterprises. This might be started by, for example, including standard compliance in SME contracts that must be handling personal information.
Intensity of IT usage	Enterprises with higher intensity of IT usage have higher chance of implementing standard	•Policymakers should construct a database of enterprises with an intensity of IT usage. So, policymakers can support the enterprises that have higher IT usage, as they are more likely to implement the cybersecurity standard.
IT investment, IT security investment	Enterprises with higher IT investment or IT security investment have higher chance of implementing standard	•Policymakers may increase financial incentives for IT and IT security investment, for example by reducing the tax from these kinds of investment. So, once they invest in IT and IT security more, then they are more likely to apply cybersecurity standards.
IT staff,IT security staff	Enterprises with higher number of IT staff or IT security staff have higher chance of implementing standard	•Policymakers should survey the demand for IT personnel and IT security personnel and make a prediction of the demand, and at the same time try to produce matching supply of personnel by establishing cybersecurity formal education in colleges or universities, and offering free training courses to develop cybersecurity officers.
Attitudes towards cybersecurity		
Awareness of organizational cybersecurity risks	Enterprises that perceived organizational cybersecurity risks have higher chance of implementing standard.	•Policymakers should promote the implementation of cybersecurity standards by communicating about cyber awareness and cyber risks more often because the awareness of the potential risks will induce precautionary behaviors and the willingness to implement the cybersecurity standard.
Perceived cybersecurity needs of customers	Enterprises that perceived cybersecurity needs of customers have higher chance of implementing standard.	•Policymakers should communicate about customer requirements of cybersecurity and privacy more often. Therefore, when businesses realize that there are such requirements then the business will try to fulfill their customer requirements.
Intention to adopt a cybersecurity standard	Enterprises that intention to adopt a cybersecurity standard have higher chance of implementing standard.	•Policymakers should promote the adoption of cybersecurity standards by communicating about benefits of implementing cybersecurity standards, as it is the first step to draw SMEs' intentions to adopt the cybersecurity standard. •Policymakers should provide expertise resources for standard adoption and also develop implementation guidelines for SMEs to follow easily. •Policymakers may also develop certification that targets SMEs to increase incentives for adopting the cybersecurity standard.

sectional survey within a limited time, however business might change with changing environments over time, so we suggest further research to re-visit this topic again in near future. In addition, this research is the pilot study, which can suggest policymakers take further steps to promote the cybersecurity standard adoption in SMEs. However, to increase the chance of successful implementation of the cybersecurity standard we also need to understand the process of adopting the cybersecurity standards, therefore future research may perform an in-depth interview to further explore this issue.

ACKNOWLEDGMENT

The authors would like to thank the Technopreneurship and Innovation Management Program: the Graduate School, Chulalongkorn University for academic support and financial support. This research is part of the dissertation for Doctor of Philosophy degree in the Technopreneurship and Innovation Management Program, Graduate School, Chulalongkorn University.

REFERENCES

[1] N. Nelson and S. Madnick, "Studying the tension between digital innovation and cybersecurity," *Twenty-third Americas Conference on Information Systems, Boston*, 2017.

[2] Verizon, "2021 data breach investigations report," 2021.

[3] M. Mansfield, "Cyber security statistics: Numbers small businesses need to know," 2020.

[4] E. Dube and S. Flowerday, "Towards a holistic information security framework for south african small and medium enterprises," *2018 1st International Conference on Computer Applications Information Security (ICCAIS)*, 2018.

[5] H. M. J. Abbas and F. Hussian, "Information security management for small and medium size enterprises," 2015.

[6] M. Benz and D. Chatterjee, "Calculated risk? a cybersecurity evaluation tool for smes," business horizons," pp. 531–540, 2020.

[7] L. Y. H. Li and W. He, "The impact of gdpr on global technology development," *Journal of Global Information Technology Management*, 2019.

[8] ISO, "Iso/iec 27001:2013(en) information technology — security techniques — information security management systems — requirements," *the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC)*.

[9] S. M. J. Prodanova and N. Jimenez, "Achieving customers' repurchase intention through stimuli and site attachment," *Journal of Organizational Computing and Electronic Commerce*, vol. 30(3), pp. 187–208, 2020.

[10] K. K. E. Dzidzah and B. Asante, "Security behavior of mobile financial service users," *Information Computer Security*, vol. 28(5), pp. 719–741, 2020.

[11] . ENISA, "Information security and privacy standards for smes," 2016.

[12] H. Khan and K. AlShare, "Violators versus non-violators of information security measures in organizations-a study of distinguishing factors," *Journal of Organizational Computing and Electronic Commerce*, vol. 29(1), pp. 4–23, 2019.

[13] R. Khatib and H. Barki, "An activity theory approach to information security non-compliance," *Information Computer Security*, vol. 28(4), pp. 485–501, 2020.

[14] K.-h. L. T. C. H. P. Shih, X.G., "Taking promotion and prevention mechanisms matter for information systems security policy in chinese smes," 2016.

[15] B. Y. Ozkan and M. Spruit, "Cybersecurity standardisation for smes: The stakeholders' perspectives and a research agenda," *International Journal of Standardization Research*, vol. 17(2), pp. 41–72, 2019.

[16] T. B. F. Mijnhardt and M. Spruit, "Organizational characteristics influencing sme information security maturity," *Journal of Computer Information Systems*, 2017.

[17] M. T. S. Kabanda and C. Kent, "Exploring sme cybersecurity practices in developing countries," *Journal of Organizational Computing and Electronic Commerce*, vol. 28(3), pp. 269–282, 2018.

[18] M. Tripathi and A. Mukhopadhyay, "Financial loss due to a data privacy breach: An empirical analysis," *Journal of Organizational Computing and Electronic Commerce*, vol. 30(4), pp. 381–400, 2020.

[19] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *Journal of Organizational Computing and Electronic Commerce*, vol. 29(4), pp. 249–257, 2019.

[20] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behavior on information security awareness: A case on sme," *International Conference on Research and Innovation in Information Systems*, 2013.

[21] A. Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," *Computer Law Security Review*, vol. 2015(3), pp. 243–256, 2015.

[22] OSMEP, "Annual reports of thai smes 2019," *the Office of Small and Medium Enterprises Promotion (OSMEP)*.

[23] e. a. J. Hair, "Multivariate data analysis: A global perspective," 2010.

[24] R. Rovinelli and R. Hambleton, "On the use of content specialists in the assessment of criterion-referenced test item validity," 1976.

Wipawadee Auyporn is a Ph.D. student at Technopreneurship and Innovation Management Program (TIP), Graduate School, Chulalongkorn University. Her research interests include Cybersecurity and Innovation Management.

Assoc. Prof. Krerk Piromsopa, Ph.D. is a full-time associate professor at the Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University. His research interests include Computer Architecture, Computer Security, Digital Design Verification, Embedded Control Systems.

Assoc. Prof. Thitivadee Chaiyawat, Ph.D. is a full-time associate professor at the Department of Statistics, Chulalongkorn Business School, Chulalongkorn University. Her research interests include Risk Management and Insurance.