

Impacts of Cybersecurity Practices on Cyberattack Damage and Protection Among Small and Medium Enterprises in Thailand

Thanintorn Thamrongthanakit

Department of Computer
and Systems Sciences

Degree project 30 HE credits
Computer and Systems Sciences
Degree project at the master level
Spring term 2023
Supervisor: Gideon Mekonnen Jonathan
Reviewer: Mohamed Sobih Aly El Mekawy



Stockholm
University

Abstract

Small and medium enterprises (SMEs) are a significant factor that drives the global economy, especially in developing countries such as Thailand, where SMEs contribute more than one-third of the Thai GDP. With digital transformation allowing businesses to access new technologies easily, most SMEs have shifted from traditional businesses to digital businesses. However, adopting technologies without any protections could make SMEs become a target of cyberattacks. This study, therefore, aims to explore cyber securities that are used to protect against cyberattacks in Thai SMEs and also the challenges of implementing cybersecurity frameworks and controls in SMEs. The research questions of this study are “How do SMEs in Thailand protect their organization from cyberattacks?” and “What challenges do SMEs in Thailand face during implementing cybersecurity frameworks or controls?” A mixed method combining surveys for quantitative data and interviews for qualitative data was used in this study. The online survey questionnaires were used to find out the overview of cybersecurity in SMEs, followed by the semi-structured interview to investigate the challenges of implementing cybersecurity in SMEs. There were 75 SMEs participating in the survey along with three respondents working for SMEs and an IT consultant for SMEs participating in in-depth interviews. The quantitative data were analyzed with descriptive statistics, while the thematic analysis was used to analyze the qualitative data. The findings indicate that SMEs in Thailand implement some cybersecurity controls to protect their organization instead of complying with the cybersecurity standards or frameworks, such as ISO2700X series, NIST, and PCI DSS. However, SMEs are also concerned about the laws, including Thailand’s PDPA, Computer Crime Act, and Personal Information Act, to which they have to comply. In addition, the biggest challenge of implementing cybersecurity frameworks and controls in SMEs is lack of financial resources, as cybersecurity frameworks and controls require a lot of budget, tools, and also experts or consultants to implement.

Keywords: SMEs in Thailand, Cybersecurity Frameworks, Cybersecurity Controls

Synopsis

Background	SMEs in Thailand are one of the most important factors that drive Thai's economy. SMEs have adopted many new technologies to drive their business because of the digital transformation, so recently, many SMEs have shifted from traditional business to digital business. However, the adoption of new technology in a short time with little knowledge and skills could easily become a target of cyberattacks.
Problem	SMEs have very limited resources. They usually invest money in the technologies that could help them improve their business, but try to ignore cybersecurity. Therefore, SMEs could easily be a target of cyberattacks. In addition, most cybersecurity frameworks are not suitable for SMEs.
Research Questions	This study aims to explore cybersecurity in SMEs and the challenges of implementing cybersecurity frameworks and controls to protect their organization. Therefore, the research questions of this study are <ul style="list-style-type: none">• How do SMEs in Thailand protect their organization from cyberattacks?• What challenges do SMEs in Thailand face during implementing cybersecurity frameworks or controls?
Method	The mixed method combining the quantitative and qualitative data was used in this study. The online survey questionnaires were conducted in this study to explore the overview of cybersecurity in SMEs, followed by the semi-structured interview to investigate the challenges of implementing cybersecurity in SMEs.
Result	Most of the SMEs in this study implement cybersecurity controls to protect their organizations instead of comply with the cybersecurity standard or framework. However, there are many challenges of implementing cybersecurity frameworks and controls in SMEs, including lack of financial resources, human resource, and knowledge.
Discussion	This study contributes to the findings of cybersecurity in SMEs, which confirms the findings of former related research. The findings also implicated that cybersecurity is not considered as important as other business priorities to SMEs. However, there are some limitations, including the number of participants, the background of participants, and the biases of the researcher, that could affect the credibility, dependability, and confirmability of the finding. Moreover, the findings in this study do not create any negative ethical consequences and can be used to develop a cybersecurity model that is suitable for SMEs.

Acknowledgement

I am deeply grateful to my supervisor, Gideon Mekonnen Jonathan, for his support and guidance throughout my Master's thesis and my reviewer, Mohamed Sobih Aly El Mekawy, for his invaluable advice and feedback throughout the research. Their expertise and encouragement helped me to complete this research.

I would also like to thank all participants from both the survey and interview for sharing their experiences and insights, which were invaluable to my research and have helped to make this thesis a success. Thank you for your time and contribution.

Table of Contents

1	Introduction	1
1.1	Background.....	1
1.2	Research Problem	2
1.3	Aim and Research Questions	3
1.4	Delimitation of Study	3
1.5	Thesis Structure	3
2	Extended Background	4
2.1	Confidentiality, Integrity, and Availability (CIA) Triad for SMEs	4
2.2	Cybersecurity Controls.....	5
2.3	Challenges of implementing cybersecurity controls in SMEs.....	7
3	Methodology	9
3.1	Research Strategy	9
3.2	Data Collection	9
3.3	Sampling	10
3.4	Data Analysis Method.....	11
3.5	Application of Method	12
3.5.1	Data Collection Procedure.....	12
3.5.2	Data Analysis Procedure	12
3.6	Quality Criteria	14
3.6.1	Credibility.....	14
3.6.2	Dependability	14
3.6.3	Transferability	14
3.6.4	Confirmability	14
3.7	Ethical Consideration	14
4.	Result	15
4.1	Survey Result.....	15
4.1.1	Demographic and Companies' Background.....	15
4.1.2	Cybersecurity in SMEs.....	16
4.1.2	Application of Cybersecurity Framework.....	18
4.2	Interview Result	22
4.2.1	Cyberattacks in SMEs	22
4.2.2	Cybersecurity concern	23
4.2.3	Cybersecurity frameworks and controls.....	23
4.2.4	Reasons for not applying for a cybersecurity certificate and full controls.....	24
5.	Discussion	25
5.1	Why do only a few SMEs in Thailand have cybersecurity frameworks?	25
5.2	Cybersecurity controls in SMEs	25
5.3	Challenges of implementing cybersecurity frameworks and controls in SMEs.....	26
6.	Conclusion	27

6.1	How do SMEs in Thailand protect their organizations from cyberattacks?.....	27
6.2	What challenges do SMEs in Thailand face during implementing cybersecurity controls?	27
6.3	Contribution	27
6.4	Limitation	28
6.5	Future Research	28
6.6	Ethical and Societal Consequences.....	28
	<i>References.....</i>	<i>29</i>
	<i>Appendix A – Survey and Interview Questions.....</i>	<i>35</i>
	<i>Appendix B – Survey Responses</i>	<i>39</i>
	<i>Appendix C – Transcripts.....</i>	<i>40</i>
	<i>Appendix D – Consent Form</i>	<i>41</i>
	<i>Appendix E – Reflection.....</i>	<i>43</i>

List of Figures

Figure 1: CIA Triad.....	4
Figure 2: Demographic and Companies' Background.....	15
Figure 3: Result of Cybersecurity Knowledge and Awareness in SMEs.....	16
Figure 4: Result of Behavior and Current Cybersecurity Measure.....	17
Figure 5: Use of Cybersecurity Frameworks in SMEs.....	18
Figure 6: Security Controls in SMEs.....	18
Figure 7: Physical, Technical, and Administrative Security Controls in SMEs.....	19
Figure 8: Cybersecurity Training in SMEs.....	20
Figure 9: Challenges of Implementing Cybersecurity Controls in SMEs.....	20
Figure 10: Cyberattacks Faced by SMEs.....	21

List of Tables

Table 1: Size of SMEs in Thailand.....	1
Table 2: Example of Cybersecurity Controls	6
Table 3: Overview of Interviews	12
Table 4: Thematic Analysis.....	12
Table 5: Statistic Result of Cybersecurity Knowledge and Awareness in SMEs	17

List of Abbreviations

SMEs	Small and Medium Enterprises
SMBs	Small and Medium Businesses
GDP	Gross Domestic Product
IOT	Internet of Things
NIST	National Institute of Standards and Technology
COBIT	Control Objectives for Information Technologies
ISACA	Information Systems Audit and Control Association
DDoS	Distributed Denial-of-Service
PCI DSS	Payment Card Industry Data Security Standard
AI	Artificial Intelligence
CC	Common Criteria
SSE-CMM	Systems Security Engineer-Capability Maturity Model
PDPA	Personal Data Protection Act
NDA	Non-Disclosure Agreement
SaaS	Software as a Service

1 Introduction

This chapter presents the study background, research problem, aim and research questions, delimitation of this study, and the structure of this paper.

1.1 Background

Small and Medium Enterprises (SMEs) or Small and Medium Businesses (SMBs) are recognized as significant factors contributing to global economies, especially in developing countries. According to World Bank (2022), SMEs not only contribute to national income but also create jobs for employees and produce up to 40% of national income, with the prediction of SMEs' job creation at approximately 600 million jobs by 2030. In Thailand, there were 3.19 million SMEs in 2021, which increased by 0.06 million SMEs from the previous year (Statista, 2022). SMEs are responsible for the majority of national income in Thailand. The OSMEP (2022) found that the Gross Domestic Product (GDP) of SMEs in Thailand increased by 3% from 2022, accounting for 34.6% of the total Thai GDP. The size of SMEs in Thailand can be defined by the number of employees, income as well as types of business, as shown in Table 1. Although Thai SMEs are the backbone of the Thai economy, they are also disturbed by digital transformation.

Table 1: Size of SMEs in Thailand (OECD, 2022)

Type of Business	Size	Employees	Annual Income (Million baht)
Manufacturing	Micro	≤ 5	≤ 1.8
	Small	≤ 50	≤ 100
	Medium	≤ 200	≤ 500
Services and Merchandising	Micro	≤ 5	≤ 1.8
	Small	≤ 30	≤ 50
	Medium	≤ 100	≤ 300

Digital transformation drives SMEs to shift from traditional to digital business, especially during the Covid-19 epidemic. Many SMEs have invested a lot of money to adopt new advanced technologies, including smart robots, Bigdata, Cloud Computing, and IOT, to approach Industry 4.0 (I4.0) (Davies, 2015). Although businesses nowadays try to use technology to drive their businesses, they still lack awareness and knowledge of cybersecurity, especially SMEs. For example, according to Wipawadee et al. (2020), Thai SMEs were aware of cybersecurity, but they still lacked knowledge of using technology and how to identified and manage cybersecurity risks.

Cybersecurity is the practices that are designed to protect systems, mobile devices, servers, networks, and data from cyber-attacks (Kaspersky, 2023). Cybercrimes tend to attack SMEs not only the company's systems but also every mobile device to take some benefits from business such as private data, money, and reputation. Therefore, not only advanced technologies but also IT infrastructure, social media, email, and mobile devices used in companies should be protected from cyberattacks or cybercrimes. In SMEs, poor cybersecurity can cause business vulnerability, raising the tendency to be

targeted by cybercrime. The recent statistics from Verizon (2022) reported that 61% of SMEs were attacked by cybercrime in 2021, and Asian-Pacific had the highest number of incidents accounting for 4,114 incidents of cybercriminal attack.

According to Kleck (2022), the global cost of cybercrime rose from 0.86 trillion U.S. dollars in 2018 to 8.44 trillion U.S. dollars in 2022, and it is predicted to skyrocket to 23.82 trillion U.S. dollars in 2027. It is noticeable that the impacts of cybercrime cost a lot of money, especially on SMEs. The statistics showed that the average cost of cybercrime per incident in SMEs was between 826 and 653,587 U.S. dollars (Verizon, 2021). Most SMEs are weak in defending themselves against cyber threats due to the limited financial and expertise resources. The cybercrime found commonly among SMEs include Social Engineering Scams (phishing, smishing, baiting, etc.), Distributed Dos attacks (DDoS), Malware, SQL Injection and Web Application Attacks, and Botnets. Take an incident as an example: The software startup company called "Cygilant " was attacked by Netwalker Ransome, which was able to hack into the system's victims and downloaded data to the hacker's server. Cygilant's customers' data was encrypted and posted on the website for negotiation (AI TechPark, 2020).

However, to reduce the high cost and damage from cybercrime, there are some cybersecurity standards, frameworks, and controls that could help SMEs to protect their business. For example, ISO 27001 is one of the widely used overall cybersecurity standards for any enterprise, which describes the practices for Information Security Management Systems (ISMS) (ISO, 2022). NIST is another cybersecurity framework that provides practices and activities to help organizations identify and manage cybersecurity risks, suitable for small and medium enterprises (SMEs) (Mahn et al., 2021). The COBIT framework provides a set of guidelines, measures and best practices that are developed by ISACA. It aims to help companies to optimize IT management and develop controls on information system management (Bernard, 2012). Although cybersecurity frameworks and practices could help organizations to protect their systems and data, these frameworks are by no means suitable for every type of organization, especially SMEs. Therefore, SMEs should have a framework for least cybersecurity controls to help them protect their organizations.

In Thailand, many SMEs have also encountered cybersecurity issues during their attempts to adopt new technologies to move toward Industry 4.0. The root cause of widespread cyber crimes found among SMEs, according to Potjanajaruwit (2022), is that Thai SMEs not only lack the financial resources to invest in hardware and software protection but also have insufficient skills and awareness of cybersecurity when the new technologies are adopted. Therefore, Thai SMEs have become a target of cybercriminals. Recently, as many as 65% of Thai SMEs have been suffering from the damage of the attacks, while phishing and malware are the top two common cyberattacks in SMEs (Leesa-nguansuk, 2021). However, there are many cybersecurity standards, practices, and frameworks that have been applied by SMEs in Thailand, such as ISO27001, NIST, and PCI DSS, which help guide them to protect the confidentiality, integrity, and availability (CIA) of their data.

1.2 Research Problem

Thai SMEs tried to adopt advanced technologies to improve their business operations and services and also move toward industry 4.0. According to Masood and Sonntag (2020), the technologies in Industry 4.0, including cloud computing, IoT, AI, and Bigdata, have been developed for or by larger organizations or multinational enterprises (MNS), so it requires both financial and technical resources to implement. In addition, SMEs, which normally have limited budgets and cash flow, tend to be leery of investment in technology and training of employees on its technology and security compared to larger companies that strictly obey standards like ISO (Lee et al., 2010; Julien & Ramangalahy, 2003).

Due to such weakness, SMEs have become the main target of cybercriminals in Thailand, including malware, phishing, DDoS, and spamming. In 2021, 65% of Thai SMEs reported being attacked by cyber criminals of all forms (Leesa-nguansuk, 2021). One of the areas in computer and systems sciences that could help SMEs from cyberattacks, which affect not only companies' finances but also confidential

data, reliability, and reputation among clients and industries, cybersecurity requires knowledge and considerable time to be an expert.

Worse than that, most of the available cybersecurity frameworks, guidelines, or practices are not suitable for SMEs. In a study conducted by Alqatawna (2014), it was found that the security standards such as Common Criteria (CC), Systems Security Engineer-Capability Maturity Model (SSE-CMM), and ISO27001 did not provide the starting point and implementation steps for SMEs, and implementing these standards cost a lot of money and time-consuming, while SMEs usually wanted to move forward fast and had limited resources. Therefore, SMEs had to select and tailor the cybersecurity standards to apply to their businesses.

Moreover, there is not much research focusing on the challenges of implementing cybersecurity controls in SMEs (Alqatawna, 2014). According to Sangani & Vijaayakumar (2012), prior studies focus exclusively on large organizations implementing many controls and advanced tools to protect their organizations. Besides, most cybersecurity studies attempted to identify cybersecurity risks (e.g., Alahmari and Duncan (2021)). Thus, this study addresses the lack of knowledge about cybersecurity controls in SMEs, including common frameworks, the reason behind such choices, and challenges.

1.3 Aim and Research Questions

The aim of this study was to explore the methods that SMEs in Thailand apply to deal with cybercrimes based on their levels of technology adoption. While most of the research focuses on challenges of cybersecurity in large companies, this study tried to explore the roles of cybersecurity in SMEs. To serve this aim, the research questions have been formed:

- How do SMEs in Thailand protect their organization from cyberattacks?
- What challenges do SMEs in Thailand face during implementing cybersecurity controls?

1.4 Delimitation of Study

This study investigates the current situation of cybersecurity in SMEs and the cybersecurity controls that are used in SMEs to protect their IT assets as well as the issue of implementing cybersecurity controls. Therefore, the focus of the cybersecurity framework would be only on the controls that are available and ubiquitous in Thailand, including ISO27001, NIST, PCI DSS, Thailand's Personal Data Protection Act (PDPA), and CIS control.

1.5 Thesis Structure

This thesis is organized in 5 chapters. Chapter 1 presents the introduction and background of the study, including research problems, research problem, aim and research question and delimitation. Chapter 2, review literature, presents the evolution of cybersecurity in SMEs in Thailand, some cybersecurity frameworks, current cybersecurity threats, impacts, and solutions. Chapter 3 is methodology, which shows the subject, the questionnaire and its development, data collection process, and analysis methods. The result of data analysis is illustrated in Chapter 4, followed by Chapter 5, which provides conclusion, discussion, recommendations, and significance of this study.

2 Extended Background

This chapter presents an extended background of the Confidentiality, Integrity, and Availability triad for SMEs and cybersecurity control, as well as the challenge of implementing cybersecurity in SMEs.

2.1 Confidentiality, Integrity, and Availability (CIA) Triad for SMEs

When cyber threats have become serious issues in any organization, cybersecurity is implemented to prevent and reduce the damage of cyberattacks. Although there are many cybersecurity frameworks and standards used to protect data in organizations, such as ISO 2700X series, COBIT, and other cybersecurity-related frameworks, most of them are not suitable for SMEs due to the limited resources and challenges of implementing cybersecurity (Mijnhardt et al., 2016). However, there is a CIA triad model that is broadly used for cybersecurity to identify confidentiality, integrity, and availability of information assets, such as data, information, software, hardware, or other information resources (Warkentin & Orgeron, 2020). Confidentiality, integrity, and availability are the essential elements of building a cybersecurity model, so many standards, including the International Organization for Standardization 27001 series (ISO27001), the National Institute of Standards and Technology (NIST), and the Information Systems Audit and Control Association (ISACA) were also constructed based on CIA triad (Gashi et al., 2022). None of the cybersecurity models can be constructed without the CIA triad.

The CIA triad has been used as a fundamental security model for almost four decades. It is used in many security models, such as Bell-La Padula Model, Biba Model, and Denning intrusion-detection model. The CIA focuses first on protecting confidentiality, then on integrity, followed by availability:

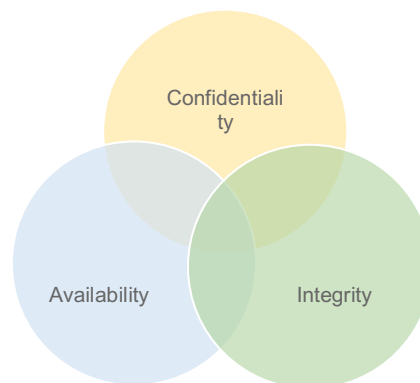


Figure 1: CIA Triad

Confidentiality refers to the ability to protect the data from those who do not have the authorization to view it (Andress, 2011). Lopes and Oliveira (2014) maintained that the information should be restricted to legitimate entities only, or authorized by the information owner before accessing them as a meaning of confidentiality. In other words, the data should be kept private and can be accessed by those who only have permission to access it. Confidentiality is a core concept of information security, which is rooted in the military mindset of maintaining a top-down authority and control over those who have access to data (Samonas & Coss, 2014). Therefore, some methods, including encryption, password policies, and access control, can help companies to maintain confidentiality. In addition, the intersection between confidentiality and integrity is regarded as trust. Trust is one of the basically significant attributes of confidentiality, but it also relates to data access, which can have an impact on data integrity in terms of both data accuracy and non-redundancy (Samonas & Coss, 2014).

Integrity is the ability to ensure that data are not altered in unauthorized or undesirable manners (Andress, 2011). Technical definition wise, the U.S. code defines integrity as the prevention of improper information modification or destruction and is also associated with information authenticity and non-repudiation (Solms & Niekerk, 2013). Moreover, integrity can be seen as ethicality and responsibility in key elements of security and the concept of integrity in the CIA triad (Hedström et al., 2010). According to Samonas and Coss (2014), integrity can be not only the ethical behavior of employees but also the responsibilities of their job roles and participation in an organization. In addition, the intersection of Integrity and availability can refer to the correctness of specification, which is the basis of robust and coherent access control that is related to the availability of data (Samonas & Coss, 2014).

Availability is the ability to access data by authorized users when needed (Andress, 2011). This means that the system should be accessible at any time by authorized users and should be protected from disruptions such as Denial-of-Service attacks, botnets, natural disasters, or other unintentional actions. Furthermore, availability also usually relates to the usability of the system, but it could conflict with security because users typically prefer usability and convenience to security; for instance, people prefer single-factor authentication because of its ease of use although two-factor authentication is more secure (Gunson et al., 2011). Despite no previous study discussing the intersection of availability and confidentiality, the intersection of three elements at the center of the CIA triad can refer to identity management (Samonas & Coss, 2014).

Many studies have shown that confidentiality is the key element of the CIA triad, and organizations should give first priority to satisfy it. However, when organizations try to satisfy one of the elements in the CIA triad, they may also serve the other smaller parts of the elements, as seen in Figure 1. Therefore, confidentiality, integrity, and availability of the information assets usually are protected even when organizations only focus on one part of them.

2.2 Cybersecurity Controls

Cybersecurity controls are not only used to mitigate the risks of cyber threats but also prevent the system from cyber criminals. Cybercrimes noticeably increase during the last five years, and the cost of the impact of cybercrime is also very high. Although there are some laws and regulations are enacted by the government to protect data, for example, the Thai government has introduced a new law called the “Personal Data Protection Act (PDPA)” in 2019 to control and protect privacy data (Phakdeetham, 2022), these could protect only some parts of information assets in SMEs. Therefore, cybersecurity controls should be urgently considered for implementation in companies, especially SMEs. The aim of implementing cybersecurity controls is to protect the confidentiality, integrity, and availability of the data. According to Andress (2011), cybersecurity controls are divided into 3 categories. First is physical control, which protects the physical environment such as fences, gates, CCTV, and so on. It seems not to be related to cybersecurity, but it is the first layer to protect the system from attackers accessing the physical information assets. Secondly, logical controls or technical controls prevent the networks, systems, storage, etc., from attackers. Encryption, password, access control, firewall, or intrusion detection systems could be applied to protect information assets. Logical or technical control tends to protect information from unauthorized users or attackers by using software and hardware (Soomro et al., 2016). Thirdly, administrative controls refer to policies, procedures, or guidelines to deal with cybersecurity threats. The administrative controls are significantly vital because they also affect the success of physical and technical controls (Yaokumah, 2017). In addition, according to Tsegaye & Flowerday (2014), there are 3 types of control which are preventive, detective, and corrective controls used to deal with cyber threats. Preventive controls use to prevent security incidents from occurring at the early stage. Policies, security training, firewalls, intrusion prevention systems, antivirus software, penetration testing, and patches, for example, can be the solution for preventive controls. Detective

controls are used to protect the system when cyber threats are able to bypass preventive controls. This type of control tends to reduce the impact of cyber threats by ensuring that they are identified and detected early. Intrusion prevention systems, antivirus software, intrusion detection systems, and honeypots could help to detect cyber threats. Corrective controls are used when the incident already occurs to respond to cyberattacks as early as possible. Antivirus software, disaster recovery plan, and Zombie Zapper are applied to respond to cyberattacks. SMEs should try to map cybersecurity controls to their different information assets to minimize the risks of cyber threats and satisfy the CIA triad.

Table 2: Example of Cybersecurity Controls (Pawar & Palivela, 2022)

Control types/methods	Preventive Control	Detective Control	Corrective Control
Physical	Fences, Gates, Locks, Security guards, Door access systems, Biometrics systems, etc.	CCTV, Surveillance cameras, Smoke detections, Alarm systems, Temperature detections, Monitoring systems, etc.	Repair Physical Damages, Re-Issue access cards, Disaster recovery sites, etc.
Technical or Logical	Firewalls, Antivirus software, Intrusion prevention systems (IPS), Encryptions, Passwords, Multi-factor authentication, Data backup, regularly update patches, penetration testing, etc.	Intrusion detection system (IDS), Logs, system utilization, system monitors, Honeypots, Antivirus software, Network diagnosis tools, etc.	Data restoration, High availability system detection (HA failure), Redundant network, Reboot system, Vulnerability patching, Antivirus software, Quarantine virus, etc.
Administrative	policies, laws, regulations, security training, Data classification, Access control policies, Risk management, Disaster preparedness and recovery plan, etc.	Review access rights, Audit logs, Cybersecurity Audits, Risk assessment, etc.	Business continuity plan, Disaster recovery plan, Incident responsible plan, cybersecurity insurance, etc.

However, from Table 2, it is noticeable that there are some overlap controls in a few functions that could protect against cyber threats in different ways. For example, antivirus software can protect the system from many kinds of viruses from their signatures before they pass through the systems, but also be able to detect and quarantine viruses when they already access systems. The antivirus software can fulfill the preventive, detective, and corrective controls to protect the CIA triad of information assets. Therefore, SMEs could be able to select only one control but can protect many functions of their systems from cyberattacks.

2.3 Challenges of implementing cybersecurity controls in SMEs

It is undeniable that SMEs are the target of cyber attacks due to the weakness of cybersecurity in organizations, underestimating the value of their data, and less IT infrastructure complex. According to Kabanda et al. (2018), SMEs believed that they were not a target of cybercrimes because of their size, less complex IT system, and legacy system. They also thought that SMEs have only a few assets and are easy to maintain compared to large companies, and only large and complex IT systems need to be secured. Moreover, SMEs also underestimate the value of their data, which is low value compared to data from large enterprises. Many attackers currently focus on SMEs instead of large organizations. In Thailand, SMEs are also the target of cyberattacks. More than 60% of SMEs in Thailand experienced cyberattacks in 2022 (Baumgartner, 2023). Therefore, cybersecurity controls are important for SMEs to protect their systems and information assets. Nevertheless, it is not easy for SMEs to implement cybersecurity controls because there are many critical factors that SMEs encounter.

Top Management Support is very important for SMEs. According to Wipawadee et al. (2020) found that some SMEs in Thailand, which are supported by the top management in cybersecurity, will have good cybersecurity policies and strategies to protect their organizations. While SMEs that lack management support will not have them. Therefore, if the top managements consider cybersecurity as important as other business functions, the companies will have low risks of cyberattacks and plan to deal with cybersecurity issues. In addition, top management supports not only impacts policies and strategies in organizations but also resource allocation such as human resources, financial resources, and cybersecurity tools. According to Kabanda et al. (2018), SMEs' top management supports who consider cybersecurity as a critical issue will allocate the appropriate budget for cybersecurity and other related IT resources for their organizations.

Organizational Characteristics also have an impact on implementing cybersecurity controls, including the size of organizations, number of employees, and revenue. SMEs usually think that they are small and not a target of cyberattacks. According to Kabanda et al. (2018), one of the SMEs in this study was concerned about security only when writing code because they thought that they were small and could not be a target easily. Furthermore, most SMEs do not dedicate staff to the IT team that could take responsibility for cybersecurity in their organization due to the limited number of employees and low income (Chidukwani et al., 2022). In addition, the revenue also impacts the budget of companies. The study of Wipawadee et al. (2020) found that SMEs in Thailand, which have high revenue, would invest in cybersecurity more than SMEs with lower revenue.

Lack of Financial Resources is one of the most important factors in implementing cybersecurity controls. SMEs have very limited financial resources compared to large companies, so some SMEs decided to ignore cybersecurity controls to save their budgets, and they thought that they were small and not a target of cyberattacks (Kabanda et al., 2018). Moreover, the low budget for cybersecurity in SMEs also affects the security tools. Kabanda et al. (2018) found that SMEs usually use open-source software for logging and detecting intrusion instead of IPS/IDS with licensing because of the cost and ease of implementation and maintenance, although the IPS/IDS with licenses have high quality, more features, and better supports. Therefore, SMEs could have high risks and vulnerabilities in cybersecurity if they do not have appropriate cybersecurity tools to protect their organizations.

Lack of Cybersecurity Knowledge and Skills is a common factor in implementing cybersecurity frameworks among SMEs. Although there are many cybersecurity frameworks that could apply to small businesses, most of the frameworks require knowledge and skills to start implementing them. According to Alqatawna (2014), most SMEs do not have IT experts in their organizations to help them implement and maintain cybersecurity, so it is very difficult for them to follow the guidelines of cybersecurity frameworks because most of the cybersecurity frameworks do not have a starting point of implementation step for SMEs. Not only cybersecurity practices but also cybersecurity tools are also required knowledge and skills in implementation and maintenance. SMEs also struggle with some monitoring tools and security systems because of their complexity and skills, and knowledge

requirements (Chidukwani et al., 2022). Moreover, SMEs have difficulty assessing the capabilities of their IT service providers, so SMEs cannot ensure that their systems are fully protected (McLaurin, 2021). SMEs which have a high level of cybersecurity knowledge and skills tend to be more successful in implementing cybersecurity than others. According to Wipawadee et al. (2020), SMEs in Thailand encounter poor cybersecurity risk management due to a lack of knowledge in cybersecurity and poor risk management in organizations. Nevertheless, SMEs with knowledge of cybersecurity could become a success factor in their organization. Therefore, training in cybersecurity awareness and educating employees in IT are highly recommended for SMEs.

Although technologies are essential for SMEs to drive their businesses, there are some cyber threats that SMEs should not underestimate. There are many signs showing that SMEs are not aware of cyber threats. According to Kabanda et al. (2018), SMEs believed that they were not a target of cybercrimes because of their size, less IT complex system, and legacy system. They also thought that SMEs have only a few assets and are easy to maintain compared to large companies, and only large and complex IT systems need to be secured. Moreover, SMEs also underestimate the value of their data, which is low value compare to data from large enterprises. This lead to undefence and risk of cyberattacks. In Thailand, SMEs are also the target of cyberattacks. More than 60% of SMEs in Thailand experienced cyberattacks in 2022 (Baumgartner, 2023).

3 Methodology

This chapter presents research strategy, data collection, samplings, data analysis method and quality criteria of this study.

3.1 Research Strategy

The research strategies are used to support the aim and answer the research questions. This study would like to find out about the standard or frameworks of cybersecurity that are used in SMEs in Thailand and the challenges of implementing them. According to Denscombe (2014), there are many types of research strategies, such as surveys, case studies, systematic reviews, experiments, mixed methods, etc. Each strategy is used according to the purpose of the research. The case study was used to investigate a specific situation in a particular circumstance. This strategy is usually used for small-scale research that needs in-depth information, but it takes time and focuses on the processes rather than the result, which is not suitable for the aim and research questions of this study. The systematic review is the summary of all available primary research literature that is related to the topic of the study. This strategy usually applies to the research topic that already exists, and the accuracy of the result depends on the sources of previous research. However, this study does not have many previous studies focusing on SMEs in Thailand, so this systematic review was rejected. The experiment uses to investigate the situation under control of the environment, but this study wants to explore the real situation among SMEs in Thailand. Therefore, the experiment was not aligned with this study.

This study is an exploratory research that aims to find out the overview of cybersecurity among SMEs in Thailand and then seek in-depth detail about the factors that affect implementing cybersecurity controls. Therefore, the mixed method is the most suitable research strategy for this study. According to Denscombe (2014), the mixed method combines the qualitative and quantitative elements within a single study, for example, qualitative and quantitative research, qualitative and quantitative data, or qualitative and quantitative methods. The survey strategy with online questionnaires and interviews is used in this research. A survey strategy can be used to find information that is related to a large number of people at a specific time and also can examine some specific details of research interest (Igwenagu, 2016). The online questionnaires in this survey were used to find out the current situation regarding cybersecurity among SMEs in Thailand in the form of quantitative data to be analyzed, followed by the interview used for further investigation about the causes and challenges in implementing cybersecurity controls in SMEs. The results of the interview are qualitative data. Therefore, the quantitative and qualitative data are combined in this study. This method was also used in a study by Wong et al. (2022), who explained, "Survey strategy was used to find the common roles of cybersecurity in the organization, then the semi-structured interview was used to further investigate the result."

3.2 Data Collection

Data collection methods are varied, and each has its own merits and drawbacks (Denscombe, 2014). Some of the possible methods that can be used in this study include documents, observation, questionnaires, and interviews. The document is used as a source of data, including text, social networks, photos, and videos, as evidence. Although this method is easy to access the data and inexpensive, the data should be evaluated for quality and come from reliable sources. Due to the limited cybersecurity information in Thailand, it tends to be difficult to find accurate data from reliable sources. By contrast, using the observation method, researchers will receive data directly because they can have direct contacts with the research participants. However, this method focuses on what is happening in that situation but not the cause of the situation. Therefore, these two methods are not suitable for this research.

However, to collect precise data, this study decided to use both questionnaires and interviews to collect data. According to Denscombe (2014), it is possible to combine the method because the weakness of one method can be fulfilled by the strength of another method. Questionnaires were used to collect the overview of the data about the current situation of cybersecurity in SMEs in Thailand. Questionnaires contained a list of questions and included multiple choices and a Likert scale for the possible answers. Although the questionnaires are provided with limited answers, they save cost and time, are easy to access, and are standardized. In the past years, with the emergence and ubiquity of the internet, more and more people can regularly access it online, which makes it possible for organizations and researchers to collect data via online questionnaires. According to Kumar (2019), the online questionnaire is developed from normal questionnaires by using technologies to create questions, collect data, and analyze data. Moreover, it can be easily sent to respondents via the internet, not to mention the fact that the data were ready for analysis after collection.

However, there were limited answers in the questionnaires due to the choices that the researcher provided, so the online interview was conducted to fulfill this gap. Online interview is very useful for anyone with access to a computer and the internet: cost-saving, easy to record, and reduces embarrassment because of no direct interaction compared to face-to-face interview (Denscombe, 2014). The semi-structured interview was used in this study. According to Denscombe (2014), a clear list of questions is prepared for the semi-structured interview, but the interviewees are also allowed to develop their ideas to answer freely and can be able to point out their views of interest. Therefore, the online semi-structured interview was the best choice to be used to investigate in-depth the issues of cybersecurity controls among Thai SMEs.

3.3 Sampling

This study focuses on participants who work in small and medium enterprises. However, it was not possible to include everyone in this study, so the sampling techniques were applied to select the proper participants. According to Denscombe (2014), there are two primary types of sampling techniques: probability and non-probability. The probability technique is used to randomly select members from the population pool for the research, while the other is used when the researcher wants a specific group of people. Therefore, probability sampling was used to select participants to answer the online questionnaire in the survey, while non-probability was used to select participants for the interviews.

According to Denscombe (2014), there are many types of probability samples: systematic sample uses of statistics to create intervals for selecting a population; cluster sample divides the population into multiple groups and randomly selects the sub-groups; or stratified sample selects the population based on characteristic. However, these three samples are time-consuming and need the specific skill of researchers. Therefore, the simple random sampling was selected for this research to reach out to the potential respondents online, as a researcher wants to randomly select a small number of samples to represent a large group of the population based on the assumption that anyone from the population pool can equally represent it (Acharya et al., 2013), whereas the others, stratified sampling, and cluster samplings, focus on a specific group of people based on the division of the population in a smaller sub-group and a group clustering in the same geography, respectively.

For the interview, non-probability was the most suitable to select participants because this study needs to investigate participants' perspectives related to cybersecurity and IT assets in SMEs, so the participants were selected based on their roles and responsibilities in their organizations. According to Denscombe (2014), there are many non-probability sampling techniques that be able to used in this study. Quota sampling selects participants based on specific criteria such as gender, age, and status, while convenient sampling selected samples based on the convenience of the researchers. Snowball sampling is the selection of participants that are referred from the previous participants. Moreover, theoretical sampling selected the samples that have the potential to provide new evidence to develop a theory in the research. Lastly, purposive sampling selects participants based on their knowledge and the relevance of the research. However, quota, convenience, snowball, and theoretical sampling were

rejected because this study needs participants who could provide the specific information about cybersecurity in their organizations and do not want to develop any theories.

Therefore, the most suitable technique for this study was purposive sampling, which selects the participants who have knowledge and experience related to the field of study, as the participants in this study should have basic knowledge about cybersecurity and be able to describe rules, policies, or controls of cybersecurity that applied in their organizations.

The online survey was sent out to 100 SMEs in Thailand by chat application, but only 75 participants responded to the survey. After that, 4 interviewees were selected from the respondents. The first interviewee is the product manager of an IT company, and the second interviewee is the chief executive officer of a game developer company. Both companies have not implemented cybersecurity frameworks. The third interviewee is the manager of e-commerce platform company with a cybersecurity framework in the organization. The last interviewee is a cloud service delivery manager of a service provider company working closely with SMEs. The research decided not to find more interviewees due to the data saturation. According to Francis et al. (2010), the interviews reached data saturation when there are no new themes appearing during the interview.

3.4 Data Analysis Method

This study collected quantitative data from the questionnaire and qualitative data from the interviews. Therefore, the different types of data needed different methods of analysis.

For quantitative data, the results of online questionnaires were exported in the form of a table, so the data would be easy to analyze. There are a few statistical methods that could be used in this study. Regression analysis is used to find the relationship between variables in terms of cause and effect, while correlation statistics are used to investigate the connection between two variables (Denscombe, 2014). However, this study did not focus on the connection of variables or the cause and effect, so these two methods were rejected. Therefore, descriptive statistics were used in this study to find the pattern of the data. The mean, median, mode, range, and standard deviation were used to describe sample data and present them in the form of pie and bar charts.

For qualitative data, the interview data would be transcribed for ease of analysis. According to Denscombe (2014), although the transcribing of the audio records could be time-consuming, it makes the researchers close to the data and can analyze them more reflectively. The transcripts analysis can be conducted in many ways. Content analysis tends to find the hidden aspect of the text by counting the frequency of using texts or phrases that are mentioned in the transcripts (Denscombe, 2014), while grounded theory focuses on developing theories or concepts based on the analysis of empirical data (Johannesson & Perjons, 2014). However, this study did not focus on either the quantifying of text or developing theory, so they were rejected. By contrast, thematic analysis is very useful to identify and analyze insight into the pattern of the data (Braun & Clarke, 2012). There were six phases that the researchers had to follow. The first phase was getting familiar with the data. The researcher had to read transcripts and understand the data before analysis. The second phase was coding data to identify and label the set of data. The third phase was finding the themes. After coding, the codes were sorted and the pattern of the data emerged, and the potential themes could be developed. The themes were reviewed and verified to ensure the quality of them in phase 4. In phase 5, defining and naming themes were applied. The last phase was writing and presenting them.

3.5 Application of Method

3.5.1 Data Collection Procedure

The online questionnaires were designed to take a maximum of 10 to 15 minutes per participant to complete the survey. Google Forms was used to conduct this survey. The questions in the survey were inspired by previous studies. The format of the survey was very simple to answer. The researcher already provided multiple choices for possible answers. Therefore, the participants only selected the best answer that fit their views. There were three parts of the survey; the first part was demography and companies' background; the second part conducted the data related to the current situation regarding cybersecurity in the organizations. The third part was the cybersecurity controls in SMEs.

The interview was designed to take approximately 15 to 30 minutes per participant. The questions for the interview were also separated into three parts: demography of interviewees and their organizations, cyber threats, and cybersecurity framework applied in SMEs. The interview questions were extended from the result of the survey. Before the interview, the consent form was sent to the participants to allow them to understand the aim of this study. The interviews were conducted online via the Zoom application. The overview of the interview is shown in Table 3.

Table 3: Overview of Interviews

Participants	Participants Roles	Date	Duration
Interviewee case 1 (C1)	Product manager of Software as a Service company	2023-05-08	22 minutes
Interviewee case 2 (C2)	Chief Executive Officer (CEO) of the game development company.	2023-05-03	15 minutes
Interviewee case 3 (C3)	General manager of the e-commerce platform	2023-05-05	30 minutes
Interviewee case 4 (C4)	Cloud Services Delivery Managers in ICT company	2023-05-09	20 minutes

3.5.2 Data Analysis Procedure

For the quantitative data, Google form provides the data in the form of graphs and tables, so it is easy to transfer to SPSS for analysis. The data were exported automatically to Google Spreadsheet and then transformed the variables into numbers as shown in Appendix B. The SPSS was used to analyze the data by using descriptive statistics, including max, min, and standard deviations, and they were presented in the graph format for ease of understanding.

For the qualitative data, the records were transcribed into texts by using online Microsoft Word in O365 and re-checked by the researcher. Some interviews were conducted in Thai language and translated to English by the researcher. In the thematic analysis, the researcher had to read and tried to understand all data in the transcripts, and transcripts were coded and grouped into themes and categories as shown in Table 4

Table 4: Thematic Analysis

Theme	Category	Code
1. Cyber attacks in SMEs	Cause of cyber attacks	C2: "direct access to the project files"

		C3: “business competitors”, “username and password leaked” C4: “insecure password”
	Prevention against cyber attacks	C1: “spam filter”, “web app firewall”, “dashboard” C2: “sign a NDA” C3: “sign NDA”, “monitoring system”, “Cloudflare services” C4: “backup”
	Action against cyber attacks	C1: “create new instance” C3: “scaled out”
2. Cybersecurity concerns	Legal concern	C1: “PDPA” C4: “PDPA and computer crimes”, “personal information”, “personal information act”
3. Cybersecurity frameworks and controls	Reasons for specific cybersecurity frameworks and controls	C3: “best practice”, “trust my consultant” C4: “experience”, “focus on CIA”, “basic of cybersecurity”
	Preparation before implementing cybersecurity frameworks or controls	C2: “assessment of our current security posture”, “invest in necessary resources” C3: “using SaaS” C4: “know what is the pain point”
	Benefits of using cybersecurity frameworks and controls	C1: “not that important” C3: “no effect in terms of marketing”, “feel relieved” C4: “standards affect our customers”, “need to hire a consultant”
4. Reasons for not applying for a cybersecurity certificate and full controls	A lot of time and resources required	C2: “requires a significant amount of financial resources” C4: “put a lot of afford”, “budget is the most concern”, “requires more staffs, tools, and technologies”
	Reliance on managed services	C1: “include many protections”, “comply with the sets of standards” C4: “complied with these standards”
	Trust in teams	C1: “second nature” C3: “transfer the best practices”
	No request from customers	C3: “never asked about the certificates”

3.6 Quality Criteria

3.6.1 Credibility

Credibility is to identify that the data are accurate and appropriate (Denscombe, 2014). The result of the research should be credible and reliable. Credibility is vital in this study as it confirms that the findings can be trusted: not false, fake, or deviant from facts provided by the subjects. To strengthen credibility, the transcripts of the interview are reviewed by the researchers and participants. When the study is finished, the participants can check and review the result of the study. In addition, the triangulation could be applied to see others' perspectives in balance.

3.6.2 Dependability

Dependability refers to the consistency of the result or the stability of findings. In other words, The study always produces the same result, even different researchers do (Denscombe, 2014). This criterion is important because it verifies the consistency of findings and the raw data of this study. To strengthen dependability, the research process and decision-affected process are described clearly in this research. In addition, the audio records, transcripts, and survey records are kept in the cloud storage, so they are able to track and audit if needed.

3.6.3 Transferability

Transferability is about the result of the research that can be transferred to other contexts or settings (Korstjens & Moser, 2017). This means the readers could be able to use the findings of this research to transfer to their future research. In addition, the findings should be able to be applied in reality as a guideline for those related to SMEs to understand their attitude and choices of cybersecurity frameworks in their organizations. Therefore, the findings and conclusions of this study are described clearly so that the readers are able to understand and transfer them to their future studies.

3.6.4 Confirmability

The finding of the research could be able to prove that there is only the result from data analysis without the bias of researchers (Denscombe, 2014). Confirmability is used in this study to prove the interpretation of findings is accurate and free from the researcher's bias. Therefore, to address this issue, the data analysis and findings are described elaborately, as well as the research methodology to provide all specific detail to readers. In addition, the researcher is also aware of the bias that could occur during the study.

3.7 Ethical Consideration

The principle of research ethics, according to Johannesson and Perjons (2014), consists of 4 principles. First, to protect the Interests of participants and ensure participants should not be harmed both physically and mentally, the participants were informed in the consent form the rights to quit at any time during the survey and interview. Second, to ensure that participation is voluntary and based on informed consent and that participants have rights to decide whether to join the research or not, the consent forms were sent to participants before the interview and survey, so they could decide whether to participate in this study or not. Third, to operate openly and honestly, the purpose of the study was informed clearly to participants in the consent form and before the interview, the finding of this study is sent to the participants for checking before the study is submitted. Lastly, to comply with the laws of the country where the research is being conducted, the researcher reviewed the laws of both Thailand, where the participants are residents, and Sweden, where the study is to be submitted, to ensure that all processes are legal.

4. Result

This chapter provides the findings of the survey as well as the results of the interviews, which are divided into 4 parts, including Cyberattacks in SMEs, Cybersecurity Concerns, Cybersecurity Frameworks and Controls, and Reasons for not applying for a cybersecurity certificate and full controls.

4.1 Survey Result

The results of questionnaires from Appendix B in the survey consist of 3 parts: Part 1, Demographic and Companies' Background; Part 2, General cybersecurity in SMEs; and Part 3, Cybersecurity frameworks apply.

4.1.1 Demographic and Companies' Background

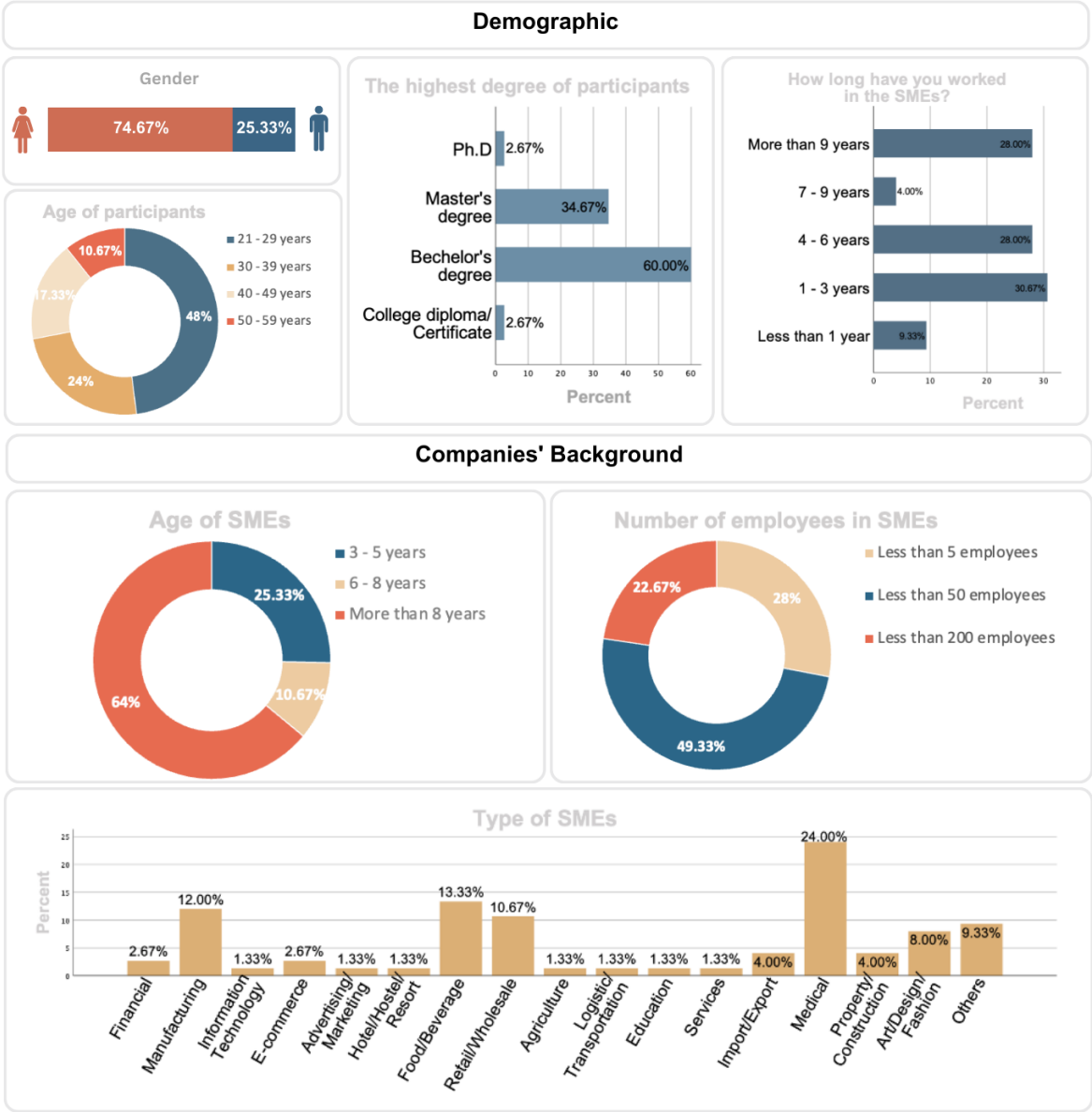


Figure 2: Demographic and Companies' Background

There were 75 participants from different SMEs participating in this study. Figure 2 shows that most of the respondents are female, at 74.67%, while only 25.33% are male. The 21-29-year-old group of respondents was the majority, at 64%, while the age group of 30-39, 40-49, and 59-60 years account for 24%, 17.33%, and 10.67%, respectively. The majority of respondents, 60%, hold a bachelor’s degree, followed by 25% holding a Master’s degree, while a PhD and diploma/certificate account equally for 2.67% of respondents. Approximately 30% of respondents have worked in SMEs for 1-3 years, followed by those working for 4-6 years and more than 9 years, each at 28%. Most of the SMEs in this study, accounting for 64%, have been established for more than 8 years, while the rest of the SMEs were older than 3 years old. The small businesses (fewer than 50 employees) account for 49.33%, while the figure for micro-businesses (fewer than 5 employees) stands at 28%, and the proportion of medium businesses (fewer than 200 employees) is 22.67%. The top 3 SMEs involved in this survey are medical, food/beverage, and manufacturing businesses, at 24%, 13.33%, and 12%, respectively.

3.7.1 Cybersecurity in SMEs

This part consists of 2 sub-sections: Part 2.1 is Cybersecurity Knowledge and Awareness in SMEs, including items scored from 1 (strongly disagree) to 5 (strongly agree) on the Likert scale; and Part 2.2 is Behaviour and Current Cybersecurity Measures, including 10 questions, which can be answered by “true,” “false,” and “do not know.”

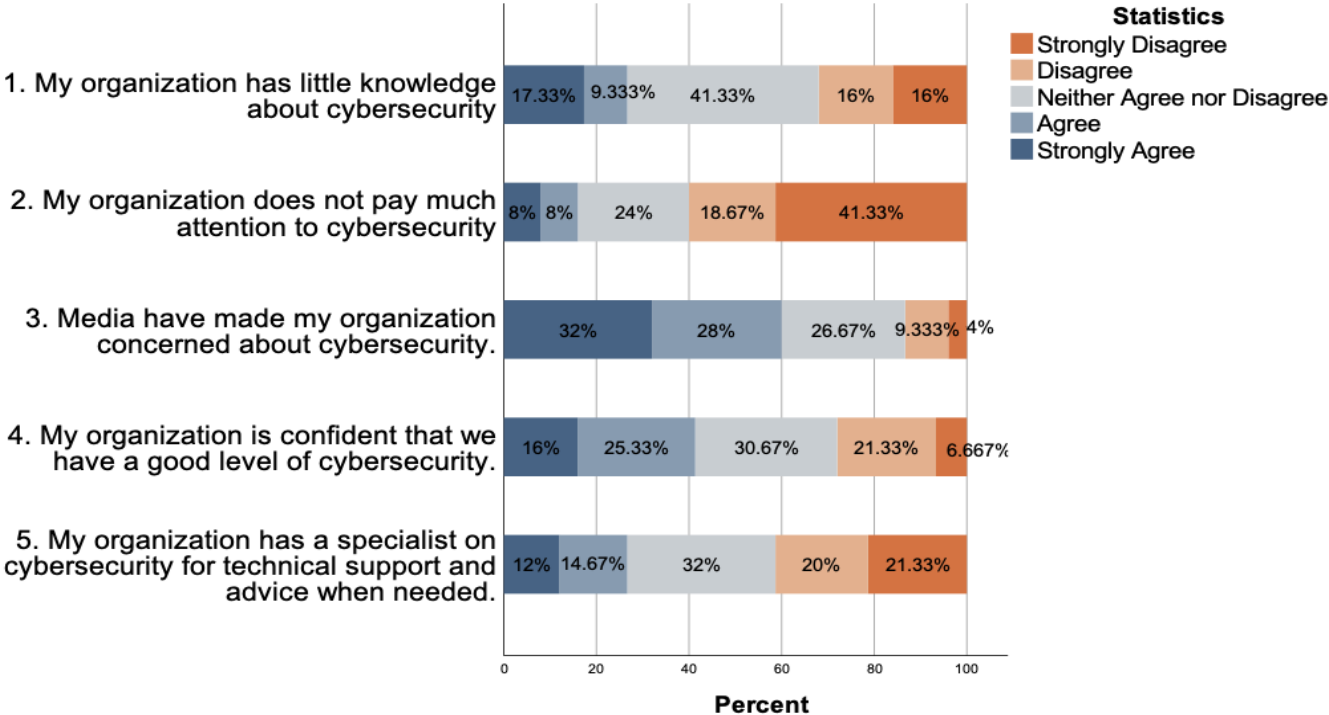


Figure 3: Result of Cybersecurity Knowledge and Awareness in SMEs

Table 5: Statistic Result of Cybersecurity Knowledge and Awareness in SMEs

Statements (S)	N	Minimum (Strongly disagree)	Maximum (Strongly agree)	Mean	Std. Deviation
1. My organization has little knowledge about cybersecurity	75	1	5	2.96	1.267
2. My organization does not pay much attention to cybersecurity	75	1	5	2.23	1.290
3. Media have made my organization concerned about cybersecurity.	75	1	5	3.75	1.128
4. My organization is confident that we have a good level of cybersecurity.	75	1	5	3.23	1.158
5. My organization has a specialist on cybersecurity for technical support and advice when needed.	75	1	5	2.76	1.282
Valid N (listwise)	75				

The result of Part 2.1, Cybersecurity Knowledge and Awareness in SMEs in Thailand, is presented in Figure 3 in percentage, while Table 3 presents statistical results, including max, min, mean, and standard deviation. Overall, all the statements receive mild responses and the standard deviation of all statements ranges from 1.128 to 1.29, at an average of 1.225. S3 ($x = 3.75$, $s = 1.128$) and S4 ($x = 3.23$, $s = 1.158$) are met with just “agree”, while S1 ($x = 2.96$, $s = 1.267$), S2 ($x = 2.23$, $s = 1.290$) and S5 ($x = 2.76$, $s = 1.282$) are rated averagely with “disagree”.

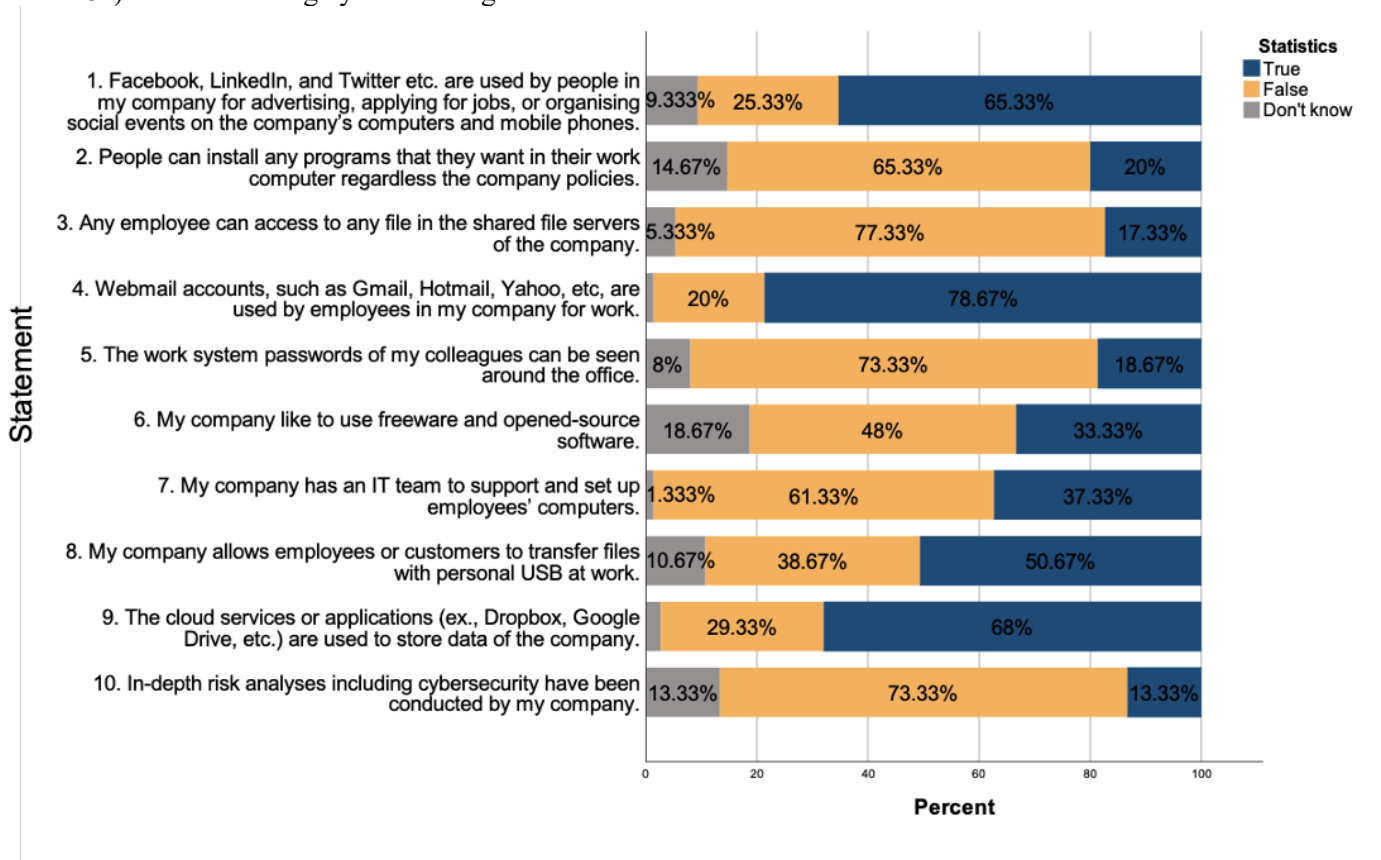


Figure 4: Result of Behavior and Current Cybersecurity Measure

The results of Part 2.2 (Behavior and Current Cybersecurity Measures) are presented in Figure 4. The majority of the respondents answered “true” to S1 (65.33%), S4 (74.67%), and S9 (68%), while more than 73% of respondents answered “false” to S3, S5, and S10. In addition, S2 (65.33%) and S7 (61.33%) were responded to as “false.” Moreover, for S6, 48% of respondents answered “false,” 33.33% answered “true,” and 18.67% were uncertain. However, for S8, 50.67% of respondents answered “true,” 38.67% of respondents answered “false,” and 10.67% answered “do not know.”

4.1.2 Application of Cybersecurity Framework

This section of the survey consists of 12 multi-choice questionnaires, for some of which (Q1, Q4, Q6, Q8, Q10, and Q12) more than 1 answer can be selected.

- **Cybersecurity Frameworks have been applied in SMEs**

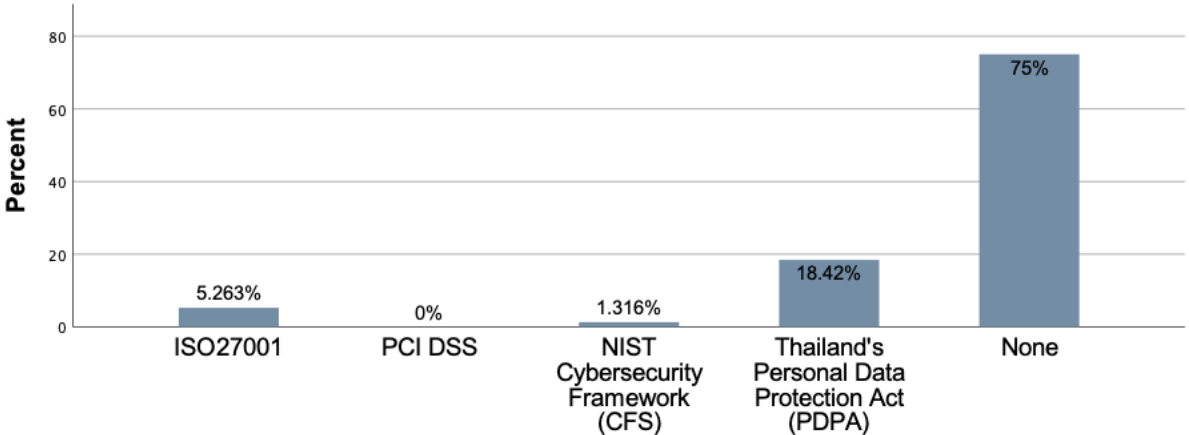


Figure 5: Use of Cybersecurity Frameworks in SMEs

According to Figure 5, the majority of SMEs in Thailand (75%) do not implement cybersecurity standards or frameworks. The most common cybersecurity framework used by the SMEs that have it is Personal Data Protection (PDPA), at 18.42%, followed by ISO27001 and NIST, at 5.263% and 1.316%, respectively. No respondents chose PCI DSS.

- **Use of Cybersecurity Controls in SMEs**

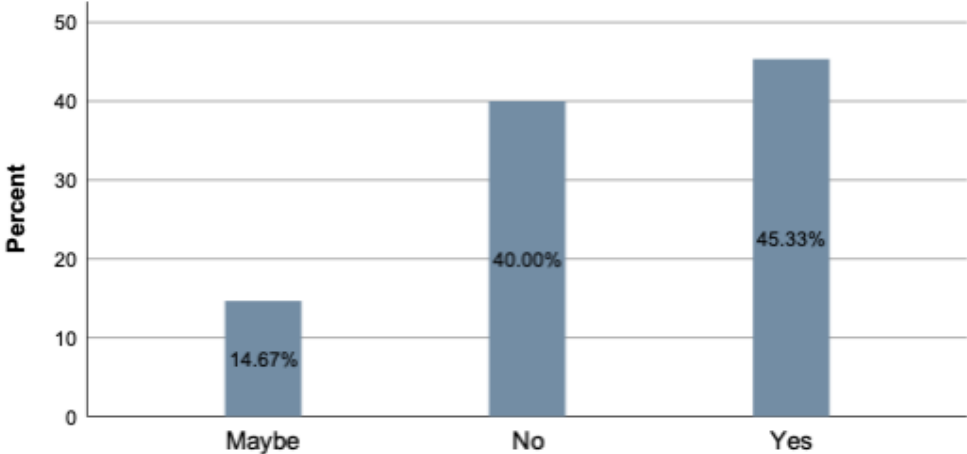


Figure 6: Security Controls in SMEs

Figure 6 shows that 45.33% of SMEs have security controls implemented in their organizations, while 40% of SMEs do not have any security controls to protect their organizations, and 15% of them are not sure about their security controls in their organizations.

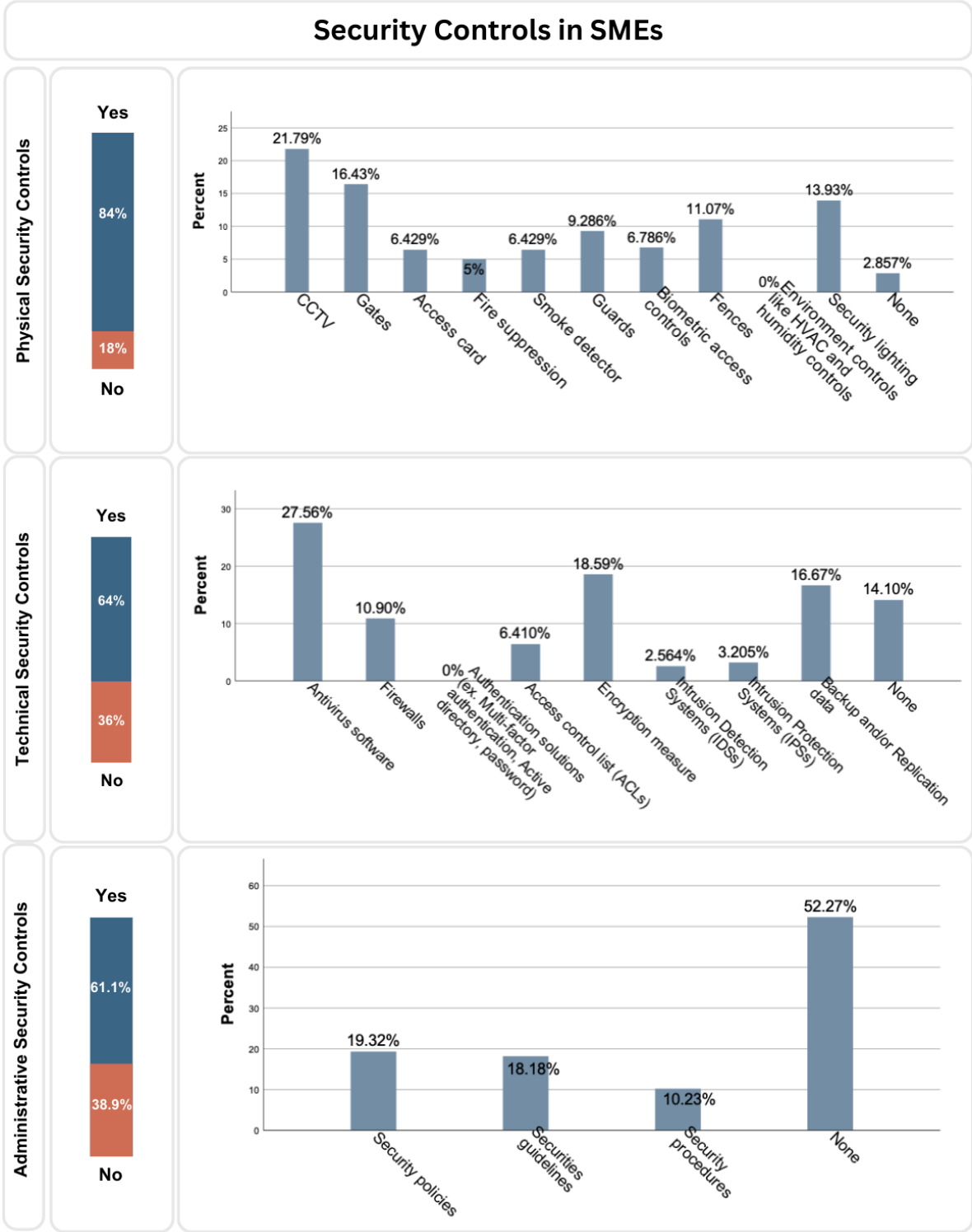


Figure 7: Physical, Technical, and Administrative Security Controls in SMEs

Figure 7 shows that 84% of the SMEs have physical controls implemented in their organizations: the top 3 common physical controls are CCTV (21.79%), gates (16.43%), and security lights (13.93%). Moreover, less than 65% of the SMEs have implemented technical controls. The most common technical

security controls are antivirus software (27.56%), encryption measures (18.59%), and backup and/or replication data (16.67%), while none of the SMEs have authentication solutions. Furthermore, 60% of the SMEs have administrative controls, but only 19.32% of them have security policies, 18.18% have security guidelines, and 10.23% have security procedures.

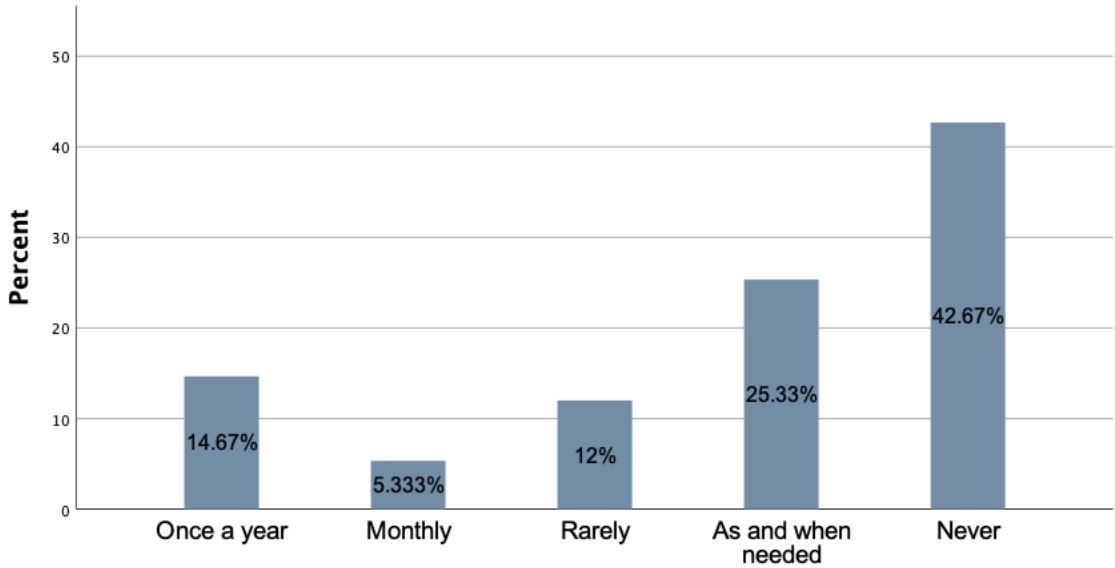


Figure 8: Cybersecurity Training in SMEs

Figure 8 shows that the majority of the SMEs (42.7%) have not trained their employees in cybersecurity awareness, while only 25% of the SMEs have trained their employees when needed. 14.7% of them have trained their staff once a year, but 12% rarely have cybersecurity training, and only 5.3% have trained their staff every month.

- Challenges of implementing Cybersecurity Controls in SMEs

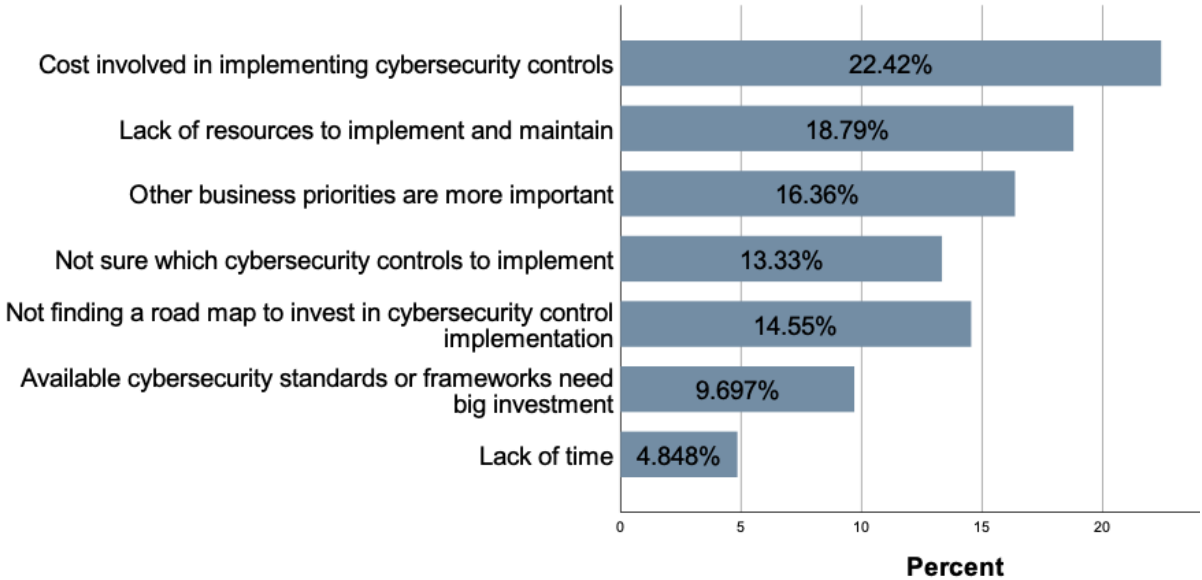


Figure 9: Challenges of Implementing Cybersecurity Controls in SMEs

Figure 9 presents that many SMEs face the challenges of implementing cybersecurity controls in their organizations. The majority of the SMEs (22.42%) have financial problems as the challenge, followed

by lack of resources (18.79%), and other essential business priorities (16.36%). Lack of time is the least important factor for implementing cybersecurity controls, at almost 5%.

- **Cyberattacks faced by SMEs**

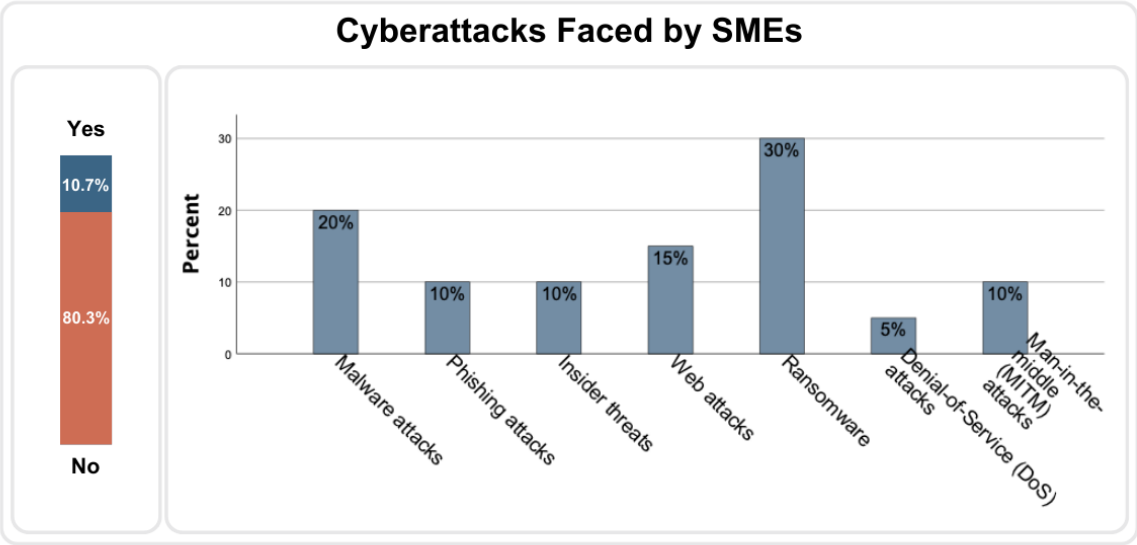


Figure 10: Cyberattacks Faced by SMEs

Figure 10 shows that only 10.7% of SMEs have been a target of cyberattacks. The most common cyberattacks are ransomware (30%), malware at 20% and web attacks (15%). Phishing attacks, insider threats, and Man-in-the-middle (MITM) attacks have the equal proportion, at 10%, while Denial-of-Service (Dos) attacks are least encountered by SMEs, at 5%.

To Sum up, the majority of respondents in this study are female within the age range of 21-29 years old. Most of them hold bachelor’s degrees. They have been working for the SMEs for at least 1-3 years. Most SMEs in this study have been established for more than 8 years with fewer than 50 employees in their company, so they can be classified as small businesses. The top 3 industries for the SMEs in this study are medical, food/beverage, and manufacturing.

Most of the respondents disagreed that SMEs have little knowledge about cybersecurity and do not pay much attention to cybersecurity. However, the media have made them strongly concerned about cybersecurity. Although the majority of SMEs are quite confident with their level of cybersecurity, only a few SMEs in this survey have specialists in cybersecurity for technical support and advice.

Most SMEs in this study allow employees to use social media for promoting or advertising events on the companies’ computers or phones. Moreover, webmail accounts (e.g. Gmail, Hotmail, Yahoo, etc.) are used by most of the SMEs for work instead of using business email accounts. The SMEs usually store data in the cloud service, including Google Drive, Dropbox, etc., and personal USB drives are allowed to be used to transfer data in most of the SMEs. However, many SMEs do not allow their employees to install any programs out of their works regarding the policies and freeware, and open-source software are not likely to be used in the SMEs. Almost all SMEs in this study tend not to allow any employees to access their shared file servers. In addition, most SMEs are able to keep their work system password safe in order to be seen by others. On the other hand, only some of the SMEs in this study have done risk analysis, including cybersecurity risks.

Although the majority of SMEs tend not to implement cybersecurity in their companies, they still have some controls to protect their systems and information. Physical, technical, and administrative controls are commonly used in the SMEs, but most of the SMEs have not trained their employees about cybersecurity. The biggest challenges of SMEs to implement cybersecurity controls are the cost of

implementing, other essential business priorities, and a lack of resources. However, only a minority of the SMEs in this study have been attacked by cyber threats: the top 3 attackers are ransomware, malware, and web attacks.

4.2 Interview Result

In the 2nd part of the study are findings from interviews with 4 respondents related with cybersecurity in SMEs, two managers of SMEs, a CEO, and a manager of a cloud computing team in a service provider company that works with SMEs. The thematic analysis has yielded 4 themes: cyber attacks in SMEs, cybersecurity concern, cybersecurity frameworks and controls, and no cybersecurity certificate and full controls applied as shown in Table 4. The transcripts of all interviewees are shown in the Appendix C.

4.2.1 Cyberattacks in SMEs

Cyberattacks in SMEs can be further divided into 3 categories.

- **Cause of cyber attacks:** the common causes of cyberattacks as mentioned by all the respondents are account hijacking, insider threats, and DDoS. To clarify, the causes of such attacks mentioned were username and password leak through multiple account administrators, direct access to the project files, and business competitor attacks.

“Our customers were attacked by account hijacking [...] Our system was designed so that one online store can be managed by many administrators, so the username and password can be leaked. [...] There are conflicts among our stores. They try to hinder one another by using DDoS attacks.” (C3)

- **Prevention against Cyber attacks:** According to the respondents, SMEs usually resort to such tools as spam filters used to detect spam email, web app firewall to protect against web attacks, monitors checking the status of systems, and backups.

“[...]for email spam, we use the spam filters. Regarding the applications, they are running on the cloud, so we use the web app firewall or WAF. [...] Yes, we have. The backup of everything, including data and code, runs automatically. [...] for the data, the service that we use already provides a daily snapshot.” (C1)

Moreover, some SMEs apply general security policies to prevent any internal leaks and potential cyber attacks, such as Non-Disclosure Agreement (NDA).

“[...]all full-time employees are required to sign a NDA, which includes a provision for the protection of our confidential information.” (C2)

- **Actions taken against cyber attacks:** SMEs in this study deal with malicious attacks such as ransomware and malware by creating new instances.

“[...] we had to solve this problem. So, we released that server and created the new instance instead. But we had to run and install everything again.” (C1)

In addition, to deal with DDoS attacks, the servers can be scaled out to be durable.

“If someone tries to flood our servers, the servers will be scalable to defend themselves [...] to make the system stable to use [...] can continue working.” (C3)

4.2.2 Cybersecurity concern

- **Legal concern**, including Thailand's PDPA, Computer crimes, and personal information act was a common concern for SMEs

"[...] there are some laws, including PDPA and computer crimes, so every private company has to follow them. Personal information, or personal information act are considered more [...]" (C4)

Especially, regarding Thailand's PDPA, similar to GDPR, which protects personal data from being used or disclosed, the SMEs need to be concerned about how to store, encrypt, and use data.

"But, most of them are more afraid or more concerned about PDPA. OK. How do we store data, how do we encrypt data? How do we store data, how do we encrypt data? Is it encrypted on the files? Is it encrypt at rest or encrypt on the flight like all these things are most of the questions which we get asked data masking as well all these things are most of the questions which we get asked data masking as well." (C1)

4.2.3 Cybersecurity frameworks and controls

- **Reasons for specific cybersecurity frameworks and controls** are trust for consultants because most SMEs in this study have only basic knowledge of cybersecurity.

"Because it is the best practice. I think cybersecurity is very important. However, I do not have much technical knowledge, so I trust my consultant, who suggests that SaaS should have cybersecurity controls." (C3)

Moreover, some SMEs decided to implement the cybersecurity frameworks and controls based on their previous experiences with cyberthreats and positive perception towards chosen cybersecurity frameworks/controls.

"Customers (SMEs) usually use many services because they have some experience with losing their files or encountering viruses [...]" (C4)

- **Preparation before implementing cybersecurity frameworks or controls:** the SMEs and the consultant in this study suggested using SaaS rather than their own infrastructure, investing in necessary resources, and doing assessment to find potential vulnerabilities because SMEs thought that managing IT infrastructure is too complex and costly.

"I would suggest using SaaS. [...] because SMEs usually do not want to manage the system, but they use the system to help them work more efficiently. [...] If they have their own infrastructure, they will have more work to do. Moreover, the cost will be increased." (C3)

- **Benefits of using cybersecurity frameworks and controls** are not apparent in terms of marketing, but significant in terms of assurance for SMEs and their clients. In the case of SMEs working in IT business, according to an interviewee, its customers do not care whether cybersecurity is provided or not, but focus on functions and the value of the products.

"[...] I think cybersecurity is not the first thing which comes to mind. So, to answer your question in terms of marketing, I think it's secondary. Not that important. [...] they'll just ask me about the features. How is it hosted? Is the backup being done? All these things are being asked [...]" (C1)

4.2.4 Reasons for not applying for a cybersecurity certificate and full controls.

- **A lot of time and resources required** is the common challenge of implementing a cybersecurity framework or controls for SMEs in this study.

“So, uh, to establish a cyber security framework is like requires a significant amount of financial resources. So, we are like a startup game company. We have to focus on investing our limited resources towards our game development and expanding our client base.” (C2)

In addition, most cybersecurity frameworks are difficult to implement because of the interpretation, so SMEs need the consultant or experts to help them.

“If it is the ISO standards, I think they need to hire a consultant to help them. It is very difficult to understand these standards and follow them. [...] It is not only documenting everything, but It may require more staff to do operation, more tools for checking systems, and also technologies to help them reduce the vulnerabilities and human errors.” (C4)

- **Reliance on managed services**, SMEs in this study thought that managed services already comply with all cybersecurity frameworks and controls, so they can be used without any cybersecurity concerns.

That’s why I do not concern much about cybersecurity frameworks because we usually use the managed service. [...] The cost of managed services is high but worth it because they also include many protections [...]” (C1)

- **Trust in teams**, SMEs in this study, especially IT business though that most of their staffs are aware of cybersecurity because their staffs have many experiences in IT and knowledge of cybersecurity.

“[...] we think the staff are mostly aware of cyber threat because these are IT people, right? So, it's something which is like second nature to them.” (C1)

- **No request from customers**, the result of penetration test can assure the level of cybersecurity, which can replace a cybersecurity certificate. Therefore, SMEs in this study thought that the cybersecurity is not necessary if the penetration test can clarify their security.

“So, when we receive a job request from our customers, such as banks or other customers. Even though we do not have the cybersecurity certificate, we show the result of penetration testing. They always accept the result without any concerns.” (C3)

5. Discussion

This chapter presents the Discussion of the Result that is divided into two parts; Why do only a few SMEs in Thailand have adopted cybersecurity frameworks, cybersecurity controls, and challenges of implementing cybersecurity frameworks and controls as well as limitations and ethical considerations in this study.

5.1 Why do only a few SMEs in Thailand have cybersecurity frameworks?

According to Baumgartner (2023), the majority of SMEs in Thailand have been a target of cyber attacks such as internal threats, DDoS, malware, and social engineering. However, this study found that only some SMEs had an experience with cyber attacks. The common cyber attacks that SMEs encountered were ransomware, malware, and web attacks. Many participants in this study think that these types of cyberattacks are very common, so they do not have to implement a cybersecurity framework against them. This finding is supported by the suggestion of Kabanda (2018) that SMEs have simple business processes and systems, so they do not need stringent cybersecurity measures.

According to Mijnhardt et al. (2016), cybersecurity frameworks are not suitable for SMEs because of the complexity of implementations and require a lot of resources. The systems of most SMEs in this study are not very complex, so they just need some cybersecurity controls to prevent some kinds of cyberattacks that have a strong effect on their business, for example, a web app firewall to filter, monitor and block some malicious traffic or DDoS attacks. An exception is only some SMEs that work in the areas of IT and finance, which have implemented cybersecurity frameworks. However, the main reason to implement cybersecurity frameworks mentioned by the SMEs in this study is not because of security but mostly related to customer requirements, law enforcement, and their own assurance. Moreover, privacy and security of data are the biggest concern for SMEs to adopt cloud computing services, including IaaS, SaaS, and PaaS (Isma'ili et al., 2016). However, most SMEs in this study rely on managed services because they believe that the services already comply with cybersecurity standards and laws. Therefore, they do not have to implement their own cybersecurity frameworks in their organizations.

5.2 Cybersecurity controls in SMEs

Although SMEs in this study tend not to adopt cybersecurity frameworks in their organizations, they have implemented cybersecurity controls, including physical, technical, and administrative controls, to protect their organizations. The finding shows that SMEs implemented at least physical controls, including CCTV, gates, and security lights, to protect unauthorized people from accessing their buildings, which is in accordance with Andress (2011), who stated that physical controls are the first layer to protect attackers from accessing the systems.

Moreover, this study found that not only security policies, guidelines, and procedures but also Non-Disclosure Agreements (NDA) are commonly used in SMEs. NDA is a legal contract that prevents sensitive information from being shared with others for certain purposes. This means that NDA will automatically impact the physical and technical controls that are used to protect the confidentiality of data in their organizations. Similar to the finding of Yaokumah (2017) that administrative controls usually affect the success of physical and technical controls. In addition, the purpose of the controls is not only to prevent the systems from cyberattacks but also to detect and deal with them (Tsegaye & Flowerday, 2014). The SMEs in this study have implemented some controls, such as antivirus, and web application firewalls, that can be both preventive and detective controls. This means some controls can have many functions that can act as different types of controls.

5.3 Challenges of implementing cybersecurity frameworks and controls in SMEs

There are many challenges to implementing cybersecurity controls in SMEs. First is top management support. According to Wipawadee et al. (2020), if cybersecurity is supported by the top management in SMEs, they would have good cybersecurity policies and strategies to protect their organizations. This study found that most top management in SMEs considers cybersecurity as an important factor for their business, so they usually invest in cybersecurity tools and policies to help mitigate risk. For example, some SMEs in this study have a policy to change the password of the system every 6 months to keep their systems more secure. Secondly, organization structure, including size, number of employees, and revenue, usually affect cybersecurity. SMEs in this study usually do not hire the IT or cybersecurity team to manage their own IT assets, but they usually have some employees who also have the ability in IT to manage them. Similar to the previous study from Chidukwani et al. (2022), the SMEs have a limited number of employees and low income, so they do not dedicate staff to the IT team. Thirdly, the finding shows that a lack of financial resources is the biggest challenge for SMEs. SMEs in this study think that implementing cybersecurity frameworks and controls required a lot of budget compared to their revenue.

According to Kabanda et al. (2018), SMEs have very limited financial resources, and investing in cybersecurity lacks immediate return on investment, so they try to ignore the importance of cybersecurity controls. This study shows that cybersecurity in terms of marketing is not the first priority factor for clients of SMEs to decide to use their services. The last challenge is the lack of cybersecurity knowledge and skills. Most of the staff in SMEs in this study were not trained in cybersecurity, but they still have awareness and basic knowledge of cybersecurity. According to Alqatawna (2014), most cybersecurity frameworks usually do not have a starting point for implementing steps for SMEs, so it is difficult to implement them without advice from experts. Therefore, only a few SMEs, especially IT businesses, are able to implement cybersecurity frameworks and controls because they usually hire staff who are IT or cybersecurity experts or have good knowledge and skills in cybersecurity. However, most of the SMEs in this study think that using managed services is the best way to comply with cybersecurity without a huge investment and afford.

6. Conclusion

This chapter presents the conclusion of the result and answers the research questions of this study as well as future research.

6.1 How do SMEs in Thailand protect their organizations from cyberattacks?

The finding shows that most SMEs in this study do not comply with cybersecurity frameworks or standards, but they have implemented some cybersecurity controls instead. To illustrate, the SMEs in this study, especially IT businesses, consider cyberattacks, including malware, ransomware, and web attacks, as common, so they just use antivirus or web application firewalls against cyber attacks without the need for cybersecurity frameworks. The common controls that are used in SMEs are physical controls (e.g., CCTV, gates, security lights), technical controls (e.g., antivirus, encryption measures, and backup and replication data), and administrative controls (e.g., security policies, security guidelines, and NDA).

6.2 What challenges do SMEs in Thailand face during implementing cybersecurity controls?

The findings show that the biggest challenge faced by the SMEs in this study is to adopt cybersecurity controls is a lack of resources, including a budget, knowledge, and human resources, while the top management support and characteristics of the organization are not the main issues. As a result, the SMEs in this study usually do not implement cybersecurity controls following the cybersecurity standards or frameworks, but they have decided to use some services from managed services to reduce the cost of implementation and maintenance. SMEs in this study also believed that services from service providers such as Azure, AWS, and Google have already complied with cybersecurity standards, so they do not have to worry about any securities.

To sum up, Thai SMEs in this study tend not to concern themselves much with cybersecurity. The SMEs usually implement only some tools that could help them protect their organizations instead of complying with cybersecurity frameworks or standards. In addition, managed services such as IaaS, SaaS, and PaaS are used by SMEs to help them manage and maintain the security of their systems. However, some SMEs in this study have complied with cybersecurity standards because of customer requirements, law enforcement, and their own assurance instead of security. In addition, due to the limited resources of SMEs in this study, the SMEs would invest money in other business priorities that could immediately return on investment more than cybersecurity.

6.3 Contribution

This study provides in-depth data in cybersecurity in Thai SMEs as well as the trend of technologies that are used in SMEs to protect their organizations and the challenges of implementing cybersecurity controls. Since the lack of the previous research focusing on cybersecurity in SMEs, this study could fulfil the gap in the cybersecurity research area. For the practical contribution, the findings of this study could be helpful for the service providers, consultants, and outsourcing companies who design the cybersecurity solutions or implement cybersecurity frameworks and controls for SMEs. In addition, this study also makes SMEs aware of cyberattacks and also presents some security controls that could help SMEs protect their organizations.

6.4 Limitation

The study has some limitations that might affect the findings of the research in terms of credibility, dependability, and confirmability. Firstly, due to the time limit of this study, the sample size of participants in the survey is quite small. This study could not manage to select the participants from different types of businesses equally. Secondly, cybersecurity is a specific topic that needs participants who already have basic cybersecurity knowledge for the interview, but most of the participants are at the management level with some IT background. Therefore, the results of the interview are more of a business view than a technical view. Thirdly, the study is difficult to reproduce because of the semi-structured interview. The participants were allowed to answer freely and elaborate on their own points of interest. This, therefore, leads to non-uniformity in the interviews. Lastly, it is not possible to eliminate all researcher's biases from this study since only one researcher works on this study, even if the researcher is already aware of it during the study.

6.5 Future Research

This study only investigated why SMEs have adopted cybersecurity frameworks in their organization and the challenges of implementing cybersecurity frameworks and controls. Finding the answers to these questions pointed out some gaps and ideas that could be studied in future research. Future research can focus more on the types of businesses and business cultures because both can affect the technologies and policies that are used in SMEs. This study has very limited time, so future research should increase the number of participants in both surveys and interviews to get more accurate data from a larger population pool to increase representativeness. Moreover, this study provides a deep understanding of cybersecurity controls in SMEs and the challenges of implementing them, so future research could use the findings of the study to create a cybersecurity model that is suitable for SMEs in Thailand.

6.6 Ethical and Societal Consequences

This study investigated cybersecurity in Thai SMEs. It is an overview of the use of cybersecurity frameworks or control in SMEs in Thailand and the issues when Thai SMEs have adopted them, which is not considered a sensitive topic. The data collection in this study has been done in accordance with the consent form, which includes the practice of keeping data confidential and participants anonymous. The data from the online survey cannot be tracked back to the participants. Therefore, this study does not have an ethical concern.

References

- Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. (2013). Sampling: Why and How of it? *Indian Journal of Medical Specialities*, 4(2), 330-333.
- AI TechPark. (2020). *Cygilant Threat Detection Company attacked by NetWalker Ransomware*. AI-TechPark. Retrieved January 25, 2023, from <https://ai-techpark.com/cygilant-threat-detection-company-attacked-by-netwalker-ransomware/>
- Alahmari, A. A., & Duncan, R. A. (2021). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1-6. 10.1109/ECAI52376.2021.9515166
- Alqatawna, J. (2014). The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises. *Journal of Software Engineering and Applications*, 7(10). <http://dx.doi.org/10.4236/jsea.2014.710079>
- Andress, J. (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Elsevier Science. <https://doi.org/10.1016/C2010-0-68336-2>
- Baumgartner, K. (2023, February 6). *Top cyberthreats to small business*. Bangkok Post. Retrieved February 7, 2023, from <https://www.bangkokpost.com/business/2500801/top-cyberthreats-to-small-business>
- Bernard, P. (2012). *COBIT 5 - A Management Guide* (1st ed.). van Haren Publishing.
- Braun, V., & Clarke, V. (2012). Thematic Analysis. *APA handbook of research methods in psychology*, 2.
- Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, 10. 10.1109/ACCESS.2022.3197899
- Dandge, A. (2020). *How Soon Should a Startup be Profitable?* LinkedIn. Retrieved March 19, 2023, from <https://www.linkedin.com/pulse/how-soon-should-startup-profitable-amod-dandge/>

- Davies, R. (2015). Industry 4.0: digitalisation for productivity and growth. *European Parliamentary Research Service*.
[https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI\(2015\)568337_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf)
- Denscombe, M. (2014). *The Good Research Guide: For Small-scale Social Research Projects* (5th ed.). McGraw-Hill/Open University Press.
- Fleck, A. (2022). *Cybercrime Expected To Skyrocket in Coming Years*. Statista. Retrieved January 24, 2023, from <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>
- Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology & Health, 25*(10), 1229-1245.
<https://doi.org/10.1080/08870440903194015>
- Gashi, L., Luma, A., & Aliu, A. (2022). A comprehensive review of cybersecurity perspective for Wireless Sensor Networks. *International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 392-395. 10.1109/ISMSIT56059.2022.9932788
- George, D., & Mallery, P. (2018). *IBM SPSS Statistics 25 Step by Step: A Simple Guide and Reference* (15th ed.). Taylor & Francis.
- Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security, 30*(4). <https://doi.org/10.1016/j.cose.2010.12.001>
- Hedström, K., Dhillon, G., & Karlsson, F. (2010). Using Actor Network Theory to Understand Information Security Management. *IFIP Advances in Information and Communication Technology, 330*, 43–54. https://doi.org/10.1007/978-3-642-15257-3_5
- Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science, 8*(1). <https://doi.org/10.1186/s40163-019-0097-9>
- Igwenagu, C. (2016). *Fundamentals of Research Methodology and Data Collection*. Lap Lambert Academic Publishing.

- Isma'ili, S. A., Li, M., Shen, J., & He, Q. (2016). Cloud computing adoption determinants: an analysis of Australian SMEs. *Pacific Asia Conference on Information Systems 2016 Proceedings*, 1-17.
- ISO. (2022). *ISO/IEC 27001:2022(en) Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. Retrieved 2023, from <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en>
- Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. Springer International Publishing. 10.1007/978-3-319-10632-8
- Julien, P., & Ramangalahy, C. (2003). Competitive strategy and performance of exporting smes: An empirical investigation of the impact of their export information search and competencies. *Entrepreneurship Theory and Practice*, 27(3), 227-245. <https://doi.org/10.1111/1540-8520.00013>
- Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 269-282. <https://doi.org/10.1080/10919392.2018.1484598>
- Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3). <https://doi.org/10.1080/10919392.2018.1484598>
- Kaspersky. (2023). *What is Cyber Security? | Definition, Types, and User Protection*. Kaspersky. Retrieved January 23, 2023, from <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- Korstjens, I., & Moser, A. (2017). Practical guidance to qualitative research. *European Journal of General Practice*, 24(1), 120-124. <https://doi.org/10.1080/13814788.2017.1375092>
- Kumar, R. (2019). *Research Methodology: A Step-by-Step Guide for Beginners* (5th ed.). SAGE Publications.
- Lee, S., Park, G., Yoon, B., & Park, J. (2010). Open innovation in SMEs—An intermediated network model. *Research Policy*, 39(2), 290-300. <https://doi.org/10.1016/j.respol.2009.12.009>

- Leesa-nguansuk, S. (2021). *Most SMEs under digital attack over past year*. Bangkok Post. Retrieved January 27, 2023, from <https://www.bangkokpost.com/business/2197995/most-smes-under-digital-attack-over-past-year>
- Lopes, I., & Oliveira, P. (2014). Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. *New Perspectives in Information Systems and Technologies, 1*, 277–286. https://doi.org/10.1007/978-3-319-05951-8_27
- Mahn, A., Marron, J., Quinn, S., & Topper, D. (2021). *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide | NIST*. National Institute of Standards and Technology. Retrieved January 26, 2023, from <https://www.nist.gov/publications/getting-started-nist-cybersecurity-framework-quick-start-guide>
- Masood, T., & Sonntag, P. (2020). Industry 4.0: Adoption challenges and benefits for SMEs. *Computers in Industry, 121*. <https://doi.org/10.1016/j.compind.2020.103261>
- McLaurin, T. (2021). A Study on the Efficacy of Small Business Cybersecurity Controls. *Marymount University ProQuest Dissertations Publishing*.
- Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems, 56*(2), 106-115. <https://doi.org/10.1080/08874417.2016.1117369>
- Nylander, S., Wallberg, A., & Hansson, P. (2017). Challenges for SMEs Entering the IoT World – Success is about so Much More than Technology. *Proceedings of the Seventh International Conference on the Internet of Things*. <https://doi.org/10.1145/3131542.3131547>
- OECD. (2022). *Financing SMEs and Entrepreneurs 2022: An OECD Scoreboard*. OECD Publishing. <https://doi.org/10.1787/e9073a0f-en>
- OSMEP. (2022). White Paper on MSME 2022. *MSME 2022*. https://sme.go.th/upload/mod_download/download-20220930104411.pdf
- Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights, 2*(1), <https://doi.org/10.1016/j.jjime.2022.100080>.

- Phakdeetham, J. (2022). *Explainer: What is PDPA, Thailand's new data law?* Bangkok Post. Retrieved March 9, 2023, from <https://www.bangkokpost.com/business/2319054/explainer-what-is-pdpa-thailands-new-data-law->
- Potjanajaruwit, P. (2022). Technology Risk Assessment in Small-and-Medium-Sized Enterprises (SMEs) in Thailand. *Journal of Southwest Jiaotong University*, 57(4), 149-155. 10.35741/issn.0258-2724.57.4.13
- Qureshi, S., & Kamal, M. (2011). Role of Cloud Computing Interventions for MicroEnterprise Growth: Implications for Global Development. *Proceedings of the Fourth Annual SIG GlobDev Workshop*.
- Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity, and Availability in Security. *Journal of Information System Security*, 10(3).
- Sangani, N. K., & Vijaayakumar, B. (2012). Cyber Security Scenarios and Control for Small and Medium Enterprises. *Informatica Economică*, 16(2).
- Solms, R. V., & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225. <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>
- Statista. (2022). *Thailand: number of MSMEs 2021*. Statista. Retrieved January 20, 2023, from <https://www.statista.com/statistics/1337417/thailand-number-of-msmes/>
- Tsegaye, T., & Flowerday, S. (2014). Controls for protecting critical information infrastructure from cyberattacks. *2014 World Congress on Internet Security (WorldCIS 2014)*. <http://dx.doi.org/10.1109/WorldCIS.2014.7028160>
- Verizon. (2021). *2021 SMB Data Breach Statistics*. Verizon. Retrieved January 24, 2023, from <https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>
- Verizon. (2022). *2022 Data Breach Investigations Report*. Verizon. Retrieved January 23, 2023, from <https://www.verizon.com/business/resources/reports/dbir/#resources>

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, 52.

<https://doi.org/10.1016/j.ijinfomgt.2020.102090>

Wipawadee, A., Auyorn, W., Piromsopa, K., & Chaiyawat, T. (2020). Critical Factors in Cybersecurity for SMEs in Technological Innovation Era. *ISPIM Conference Proceedings*.

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66.

<https://doi.org/10.1016/j.ijinfomgt.2022.102520>

World Bank. (2022). *World Bank SME Finance: Development news, research, data*. World Bank.

Retrieved January 20, 2023, from <https://www.worldbank.org/en/topic/smefinance>

Yaokumah, W. (2017). Modelling the Impact of Administrative Access Controls on Technical Access Control Measures. *Information Resources Management Journal (IRMJ)*, 30(4), 53-70.

<http://dx.doi.org/10.4018/IRMJ.2017100104>

Appendix A – Survey and Interview Questions

- Survey questions

Questions	Motivation
<p>Gender? Age? What is the highest level of school you have completed or the highest degree you have received? How long have you worked in this small and medium enterprise? What is your role within your company? How old are your small and medium enterprises (SMEs)? What industrial sectors is your company in? How many people are in your company?</p>	<p>Introduction questions were used to ask for an understanding of the background of the participants and their companies.</p>
<p>Your Cyber Security Knowledge and Awareness 12. Please rate how these statements apply to you (Strongly Agree; Agree; Neither Agree or Disagree; Disagree; Strongly Disagree)</p> <ul style="list-style-type: none"> a) My organization has little knowledge about cybersecurity b) My organization does not pay much attention to cybersecurity c) Media have made my organization concerned about cybersecurity. d) My organization is confident that we have a good level of cybersecurity. e) My organization has a specialist on cybersecurity for technical support and advice when needed. 	<p>General cybersecurity questions were used to investigate the level of cybersecurity knowledge of participants in this study</p>
<p>Are these statements true or false in your company? (true; false; don't know)</p> <ul style="list-style-type: none"> a) Facebook, LinkedIn, Twitter, etc., are used by people in my company for advertising, applying for jobs, or organizing social events on the company's computers and mobile phones. b) People can install any programs that they want in their work computer regardless the company policies. c) Any employee can access to any file in the shared file servers of the company. d) Webmail accounts, such as Gmail, Hotmail, Yahoo, etc, are used by employees in my company for work e) The work system passwords of my colleagues can be seen around the office. 	<p>Behavior and current cybersecurity measure questions were used to explore the level of knowledge and awareness of cybersecurity in SMEs.</p>

<ul style="list-style-type: none"> f) My company like to use freeware and opened-source software. g) My company has an IT team to support and set up employees' computers. h) My company allows employees or customers to transfer files with personal USB at work. i) The cloud services or applications (ex., Dropbox, Google Drive, etc.) are used to store data of the company. j) In-depth risk analyses including cybersecurity have been conducted by my company. 	
<p>Are any standards or frameworks below applied in your organization? (Can select more than one)</p> <p>Are there any security controls implemented in your organization?</p> <p>Are there any PHYSICAL security controls implemented in your organization?</p> <p>If the answer from the previous question is YES, please select the PHYSICAL security controls that are implemented in your company. (Can select more than one)</p> <p>Are there any TECHNICAL security controls implemented in your organization?</p> <p>If the answer from the previous question is YES, please select the TECHNICAL security controls that are implemented in your company. (Can select more than one)</p> <p>Are there any ADMINISTRATIVE security controls implemented in your organization?</p> <p>If the answer from the previous question is YES, please select the ADMINISTRATIVE security controls that are implemented in your company. (Can select more than one)</p> <p>How often does your company train employees about cybersecurity awareness?</p> <p>Which of the following are the main problems of implementing cyber security in your organization? (Can select more than one)</p> <p>Has your company ever been a target of cyber attacks?</p> <p>What kind of the cyber attacks that your company has encountered with? (Can select more than 1)</p>	<p>Cybersecurity frameworks and controls questions are used to find the overview of using cybersecurity frameworks and controls in SMEs</p>

- **Interview questions**

Questions	Motivation
<p>What does your company do? What is your role in the company? How long have you been working for this company?</p>	<p>Introduction questions were used to ask for understanding of the background of the participants and their companies.</p>
<p>Have your company encountered cyber threats? Which type of cyber threats did your company encounter? How often? Which cyber threat is the most difficult to deal with? Why? How did your company deal with it?</p>	<p>Cyberattack questions were used to explore the cyberattack experiences of SMEs in Thailand</p>
<p>Does your company have a cybersecurity framework? (Yes) Why does your company decide to have a cybersecurity framework? Which cybersecurity framework does your company use? Why did your company use this framework? How does the company prepare before implementing a cybersecurity framework? Does your company have any problems when implementing this framework? Do you have any team responsible for implementing and maintaining cybersecurity? What are the challenges of implementing this cybersecurity framework? What are the benefits of using them? Does your company train the staff in cybersecurity? How do you maintain the level of cybersecurity in your organization? If other SMEs would like to implement a cybersecurity framework, what do you recommend? What do they consider?</p>	<p>Questions about cybersecurity framework applied in SMEs were used to investigate the reasons, processes, and issues of implementing cybersecurity frameworks in SMEs</p>
<p>Does your company have a cybersecurity framework? (No) Why does your company not have any cybersecurity framework? How does your company protect your systems and information in terms of confidentiality, integrity, and availability? Do you think the security controls that are used in this company are enough for protecting your systems and information from cyber threats? Why?</p>	<p>Questions about no cybersecurity frameworks applied in SMEs were used to investigate how SMEs protected their organizations</p>

<p>Does your company train the staff in cybersecurity? Do you think the staff in your company are aware of cyber threats? Why? Have you done anything to encourage them to be aware? Does your company have any plans to implement cybersecurity in the future? What should your company prepare before implementing cybersecurity?</p>	
---	--

Appendix B – Survey Responses

- Survey responses

https://drive.google.com/drive/folders/1Nxgfp9CfhpvH4VSWw_JUk03dS2SoOJzg?usp=sharing

- SPSS

Part1-2-Data.sav [DataSet1] - IBM SPSS Statistics Data Editor

Visible: 22 of 22 Variables

	Gender	Age	Highest Education Level	YearOfWorking	CompanyAge	IndustrySector	Number OfEmployee	Part2.1.1	Part2.1.2	Part2.1.3	Part2.1.4	Part2.1.5	Part2.2.1	Part2.2.2	Part2.2.3	Part2.2.4	Part2.2.5	Part2.2.6
1	Female	21 - 29 y...	Beachelor'...	Less than...	More tha...	Import/E...	Less than...	Strongly A...	Agree	Strongly A...	Strongly ...	Strongly ...	False	False	False	True	True	Fals
2	Female	40 - 49 y...	Master's ...	More tha...	More tha...	Food/Bev...	Less than...	Strongly A...	Strongly ...	Neither A...	Strongly ...	Strongly ...	True	False	False	False	False	Fals
3	Female	40 - 49 y...	Beachelor'...	More tha...	More tha...	Manufact...	Less than...	Neither A...	Disagree	Agree	Agree	Agree	True	False	False	True	True	Fals
4	Female	30 - 39 y...	Master's ...	7 - 9 years	6 - 8 years	Food/Bev...	Less than...	Agree	Agree	Agree	Disagree	Disagree	True	True	False	True	True	Tru
5	Female	21 - 29 y...	Beachelor'...	4 - 6 years	More tha...	Property/...	Less than...	Neither A...	Disagree	Agree	Agree	Agree	True	False	False	True	False	Fals
6	Female	21 - 29 y...	Master's ...	1 - 3 years	3 - 5 years	Medical	Less than...	Neither A...	Disagree	Strongly ...	Neither A...	Neither A...	True	False	False	True	True	Fals
7	Female	30 - 39 y...	Beachelor'...	4 - 6 years	More tha...	Retail/Wh...	Less than...	Disagree	Disagree	Neither A...	Agree	Agree	False	False	False	True	True	Fals
8	Male	40 - 49 y...	Beachelor'...	More tha...	More tha...	Import/E...	Less than...	Neither A...	Neither A...	Neither A...	Agree	Neither A...	Don't know	False	True	True	True	Tru
9	Female	21 - 29 y...	Master's ...	1 - 3 years	More tha...	Medical	Less than...	Strongly A...	Neither A...	Neither A...	Disagree	Strongly ...	True	False	False	True	True	Tru
10	Male	21 - 29 y...	Beachelor'...	4 - 6 years	More tha...	Manufact...	Less than...	Strongly A...	Strongly ...	Strongly A...	Disagree	Disagree	True	Don't know	False	True	False	Fals
11	Male	30 - 39 y...	Beachelor'...	More tha...	More tha...	Food/Bev...	Less than...	Disagree	Strongly ...	Agree	Agree	Agree	False	False	False	True	False	Fals
12	Female	30 - 39 y...	Beachelor'...	Less than...	3 - 5 years	Financial	Less than...	Strongly ...	Strongly ...	Strongly A...	Strongly A...	Strongly A...	Don't know	False	False	True	False	Fals
13	Male	50 - 59 y...	Beachelor'...	More tha...	More tha...	Medical	Less than...	Disagree	Strongly ...	Strongly A...	Strongly A...	Strongly A...	Agree	True	False	True	False	Fals
14	Male	50 - 59 y...	Beachelor'...	4 - 6 years	More tha...	Informati...	Less than...	Strongly ...	Strongly ...	Strongly A...	Strongly A...	Strongly A...	True	False	False	False	False	Tru
15	Female	21 - 29 y...	Beachelor'...	1 - 3 years	3 - 5 years	Medical	Less than...	Disagree	Disagree	Agree	Neither A...	Disagree	True	True	False	True	False	Tru
16	Male	30 - 39 y...	Beachelor'...	More tha...	More tha...	Others	Less than...	Neither A...	Strongly ...	Agree	Disagree	Strongly ...	True	True	False	True	False	Tru
17	Female	21 - 29 y...	Master's ...	Less than...	More tha...	Hotel/Ho...	Less than...	Strongly ...	Strongly ...	Strongly A...	Strongly A...	Neither A...	True	False	False	False	False	Fals
18	Male	40 - 49 y...	Beachelor'...	More tha...	More tha...	Property/...	Less than...	Agree	Agree	Agree	Agree	Agree	True	Don't know	False	True	False	Fals
19	Female	21 - 29 y...	Beachelor'...	4 - 6 years	6 - 8 years	Medical	Less than...	Agree	Strongly A...	Disagree	Disagree	Disagree	True	True	Don't know	Don't know	False	Fals
20	Female	21 - 29 y...	Beachelor'...	4 - 6 years	3 - 5 years	Medical	Less than...	Disagree	Disagree	Neither A...	Agree	Neither A...	True	False	False	True	False	Fals
21	Female	21 - 29 y...	Beachelor'...	1 - 3 years	3 - 5 years	Medical	Less than...	Disagree	Strongly ...	Strongly A...	Neither A...	Neither A...	True	Don't know	True	True	False	Tru
22	Female	21 - 29 y...	Beachelor'...	4 - 6 years	3 - 5 years	Medical	Less than...	Neither A...	Disagree	Strongly ...	Agree	Disagree	True	False	True	True	False	Don't kno
23	Female	21 - 29 y...	Beachelor'...	1 - 3 years	6 - 8 years	E-comme...	Less than...	Neither A...	Strongly ...	Agree	Neither A...	Disagree	True	False	True	True	True	Tru
24	Female	30 - 39 y...	Beachelor'...	4 - 6 years	3 - 5 years	Medical	Less than...	Neither A...	Strongly ...	Agree	Strongly A...	Neither A...	True	False	False	True	False	Tru
25	Male	40 - 49 y...	Master's ...	4 - 6 years	6 - 8 years	Others	Less than...	Neither A...	Strongly ...	Strongly A...	Disagree	Disagree	True	False	True	True	True	Tru

Data View Variable View

Part1-2-Data.sav [DataSet1] - IBM SPSS Statistics Data Editor

Visible: 22 of 22 Variables

	Gender	Age	Highest Education Level	YearOfWorking	CompanyAge	IndustrySector	Number OfEmployee	Part2.1.1	Part2.1.2	Part2.1.3	Part2.1.4	Part2.1.5	Part2.2.1	Part2.2.2	Part2.2.3	Part2.2.4	Part2.2.5	Part2.2.6
1		2	1	4	1	3	15	2	5	4	5	1	1	2	2	2	1	1
2		2	3	5	5	3	7	2	5	1	3	5	1	1	2	2	2	2
3		2	3	4	5	3	2	3	3	2	4	4	3	1	2	2	1	1
4		2	2	5	4	2	7	2	4	4	4	2	2	1	1	2	1	2
5		2	1	4	3	3	17	2	3	2	4	4	3	1	2	2	1	2
6		2	1	5	2	1	16	1	3	2	5	3	3	1	2	2	1	1
7		2	2	4	3	3	8	2	2	2	3	4	4	2	2	2	1	1
8		1	3	4	5	3	15	2	3	3	3	4	3	3	2	1	1	2
9		2	1	5	2	3	16	2	5	3	3	2	1	1	2	2	1	1
10		1	1	4	3	3	2	2	5	1	5	2	2	1	3	2	1	2
11		1	2	4	5	3	7	3	2	1	4	4	4	2	2	2	2	2
12		2	2	4	1	1	1	2	1	1	5	5	5	3	2	2	1	2
13		1	4	4	5	3	16	2	2	1	5	5	4	1	2	2	1	2
14		1	4	4	3	3	3	3	1	1	5	5	5	1	2	2	2	2
15		2	1	4	2	1	16	2	2	2	4	3	2	1	1	2	1	2
16		1	2	4	2	3	19	2	3	1	4	2	1	1	1	2	1	2
17		2	1	5	1	3	6	3	1	1	5	5	3	1	2	2	2	2
18		1	3	4	5	3	17	2	4	4	4	3	4	1	3	2	1	2
19		2	1	4	3	2	16	2	4	5	2	2	2	1	1	3	3	2
20		2	1	4	3	1	16	1	2	2	3	4	3	1	2	2	1	2
21		2	1	4	2	1	16	1	2	1	5	3	3	1	3	1	1	2
22		2	1	4	3	1	16	1	3	2	5	4	2	1	2	1	1	2
23		2	1	4	2	2	4	2	3	1	4	3	2	1	2	1	1	1
24		2	2	4	3	1	16	1	3	1	4	5	3	1	2	2	1	2
25		1	3	5	3	2	19	1	3	1	5	2	2	1	2	1	1	1

Data View Variable View

Appendix C – Transcripts

- **Interview case 1**

https://docs.google.com/document/d/1LQccDef7ubzS4C2qHOYILebk3ZKwMovD/edit?usp=share_link&oid=118024162287022499197&rtpof=true&sd=true

- **Interview case 2**

<https://docs.google.com/document/d/1qLDCM36im3AsuAOsbpyAyAzwyBt1ClAy/edit?usp=sharing&oid=118024162287022499197&rtpof=true&sd=true>

- **Interview case 3**

<https://docs.google.com/document/d/1XIUu6HxV959t4mhLZkfxe9UDrDQBS13O/edit?usp=sharing&oid=118024162287022499197&rtpof=true&sd=true>

- **Interview case 4**

https://docs.google.com/document/d/1aZc6zNCZclennAPVvWrqj5_oj3hIrsmk/edit?usp=sharing&oid=118024162287022499197&rtpof=true&sd=true

Appendix D – Consent Form

- Survey Consent Form

CONSENT TO PARTICIPATE IN RESEARCH Impacts of Cybersecurity Practices on Cyberattack Damage and Protection Among Small and Medium Enterprises in Thailand

Purpose To discover which cybersecurity controls that Thai SMEs adopted to protect their organizations and what are the challenges of implementing cybersecurity controls.

You are invited to the research study. This research is conducted by Thanintorn Thamrongthanakit, who is a Master's student from the Department of Computer and Systems Sciences (DSV), Stockholm University.

If you agree to take part in this study, you will be asked to complete an online survey. During this survey the first part of the survey will ask about your demographic, such as gender, age, education, and so on. You will also be asked about general knowledge and practices of cybersecurity in your organization. The last part is about the cybersecurity controls that are used in your organization. Completing this questionnaire will take about 10 - 15 minutes. To take part in this study, you must work in micro, small, or medium enterprises in Thailand. Your participation in this study is completely voluntary. You feel free to stop or withdraw from the study at any time without any consequence or reject to answer any particular questions for any reason.

Inclusion criteria

1. Participants have to work in small and medium enterprises(SMEs).
2. Working for a small and medium enterprise that has been established for more than 3 years.
3. Participants should have knowledge about cybersecurity in their organizations.

Confidentiality: This anonymous online study is being conducted through the Google Form. Only the researcher who has authority can access the data of the survey. This survey is designed to be anonymous. Therefore, the data such as email, phone no., and IP address that can track back will not be collected.

Further Information: If you have any questions regarding the survey or would like additional information about this study, please contact thth9984@student.su.se

Consent: Clicking the “Next” entry below means that you understand the information on this form and voluntarily agree to participate.

- Interview Consent Form

CONSENT TO PARTICIPATE IN RESEARCH

Impacts of Cybersecurity Practices on Cyberattack Damage and Protection Among Small and Medium Enterprises in Thailand

Purpose: To discover which cybersecurity controls that Thai SMEs adopted to protect their organizations and what are the challenges of implementing cybersecurity controls.

You are invited to the research study. This research is conducted by Thanintorn Thamrongthanakit, who is a Master's student from the Department of Computer and Systems Sciences (DSV), Stockholm University.

If you agree to take part in this study, you will also be asked about general knowledge and practices of cybersecurity in your organization. The interview will take about 20-30 minutes. To take part in this study, you must work in micro, small, or medium enterprises in Thailand. Your participation in this study is completely voluntary. You feel free to stop or withdraw from the study at any time without any consequence or reject to answer any particular questions for any reason.

Inclusion criteria

1. Participants have to work in/related with small and medium enterprises (SMEs).
2. Working for a small and medium enterprise that has been established for more than 3 years.
3. Participants should have knowledge about cybersecurity in their organizations.

Confidentiality: The online interview is being conducted and recorded on Zoom. The recorded files will be stored in the cloud storage that can be accessed by the researcher, who has the authority only. The online interview also will be transcribed, and it will be included in the report. In case of not accepting the recording of the interview, the researcher should be noticed from the beginning of the interview. The taking notes will be used instead of recorded, and they will be approved by the interviewee before using them.

Further Information: If you have any questions regarding the survey or would like additional information about this study, please contact thth9984@student.su.se

Consent: In case you wish to stay anonymous, the researcher will mention neither your name nor your organization in the report and also your contact information or any other information that reveals your and the organisation's identity. Therefore, the researcher is responsible for taking away all of your and the organization's identity from the report. Otherwise, you can give them the authority to publish the name of your organization, your name and your contact information.

Therefore, I would like to request your authorization to conduct a research study and collect data in your organization regarding the purpose of the study that I mentioned above.

Please check one of the boxes below:

- I agree to be interviewed, and the information concerning my organization and also the contact information can be published.
- I agree to be interviewed but do not publish the information of my organization and also the contact information.

Signature of the interviewee,

Date

Appendix E – Reflection

During the master's thesis study, I had learnt a lot about cybersecurity and the processes of doing thesis. This study explored the cybersecurity in SMEs in Thailand and identified the challenges of implementing cybersecurity controls in Thai SMEs. The Information Security in Organization motivated me to do a master thesis in this area. The Risk Management course also gave the idea of how to manage risks in the organization that are very useful for the cybersecurity controls in this study, and the Scientific Communication and Research Methodology course also provided the steps of doing research for this study. In addition, this study was also inspired by and adapted from previous studies that focus on cybersecurity in SMEs, including the ideas of research, and methodology. Many previous cybersecurity literature and statistical data were included in the background to show the situation of cybersecurity in SMEs. Moreover, I also considered the ethical and societal aspects as an important part of the thesis, so the consent forms were used to protect the sensitive data of participants and the data were stored in the proper storage. The findings were compared with the previous studies to find the similarity and difference of the result. The arguments and important points were written in the discussion. The findings show that SMEs in Thailand only pay attention to some cybersecurity controls that could help them protect their organization from harmful cyberattacks. In addition, I was able to summarize and present this study in the final seminar within 20 minutes and defend my points of view with the participants and opponents in the seminar.

The plan of this study was designed at the beginning of the master thesis, diving in to 3 main phases which are introduction, result and discussion, and presentation. The introduction phase, including background, aim and research questions and methodology, took a bit longer than expected because the research questions were more than 2 questions, and not clearly formulated. So, I had to reformulate and find more literature to support the questions. After that the online questionnaires and interviews were conducted. The most challenging part in the phase was finding the interviewee who is working in SMEs that implemented cybersecurity framework in the organization because most SMEs in Thailand still lack implementing cybersecurity framework in their organization. Only a few types of SMEs, including financial, IT, and medical businesses, considered the cybersecurity framework as an important factor for their businesses. Moreover, the data had to be analyzed very quickly to get back on track following the plan. Then, the findings were discussed, and concluded smoothly. Therefore, this study was presented in the final seminar before the deadline even though the processes were a bit delayed at the beginning.

Furthermore, I was very satisfied with the result of this study because the results of this study were similar to the previous study, but still had their own points of view. For example, most SMEs in this study have implemented cybersecurity controls instead of frameworks to protect their organizations, and most of them are more about the law rather than technical concern and cost of implementing cybersecurity controls. The findings in this study contributed to cybersecurity research, which is one of the important areas in computer and systems sciences providing the knowledge of protecting both organizations and individuals from cyber threats. This study could benefit consultants and service providers to find the cybersecurity solutions for SMEs as well as reminding SMEs to avoid and protect their organizations from cyberattacks. For future research, I would suggest focusing more on the type of SMEs, increase the number of participants, and try to send out the online survey to them equally to get more accurate data. The findings of this study already provide a depth understanding about cybersecurity in Thai SMEs and the challenges of implementing cybersecurity controls, so the future research could focus on creating cybersecurity framework for Thai SMEs.