INFORMATION SECURITY FRAMEWORK FOR CRITICAL INFORMATION INFRASTRUCTURE IN SME

ZHANG LULU

UNIVERSITI KEBANGSAAN MALAYSIA

INFORMATION SECURITY FRAMEWORK FOR CRITICAL INFORMATION INFRASTRUCTURE IN SME

ZHANG LULU

PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE DEGREE OF MASTER OF CYBER SECURITY

FACULTY OF INFORMATION SCIENCE & TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2023

KERANGKA KESELAMATAN MAKLUMAT UNTUK INFRASTRUKTUR MAKLUMAT KRITIKAL DI PKS

ZHANG LULU

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEHI IJAZAH
SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI
2023

DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

23 August 2023

ZHANG LULU
P117754

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the following individuals and organizations who have contributed greatly to the completion of my project. First and foremost, I would like to express my deepest appreciation to my supervisor, Dr. Umi Asma' binti Mokhtar, for her guidance, support, and valuable insights throughout the research process. Without her assistance, this work would not have been possible. I would also like to extend my thanks to the Program Coordinator, lecturers, and staff from the Faculty of Information Science & Technology, for their constant support and encouragement during my academic journey.

Last but not least, I would like to express my heartfelt gratitude to my family and friends for their unwavering support and encouragement throughout my academic journey. Their love and encouragement have been a constant source of motivation and inspiration for me.

Once again, I express my sincere thanks to all those who have contributed to this work in one way or another. My hope is that this study will, to some extent, contribute to the field of research and serve as a reference for future researchers.

ABSTRAK

Internet membawa orang ramai ke masa depan yang lebih baik, dan disebabkan IoT, aktiviti harian menjadi mudah. Bagaimanapun, isu keselamatan kerap berlaku apabila orang ramai menikmati kemudahan dan faedah daripada kehidupan yang penuh dengan teknologi. Infrastruktur kritikal mungkin mengalami kegagalan dalam tahap keterukan yang berbeza-beza akibat daripada kelemahan fizikal dan logik, dan kerana terdapat banyak saling bergantung antara infrastruktur kritikal, walaupun kegagalan kecil mungkin mempunyai kesan yang serius kepada pengguna. Projek ini membincangkan kerangka keselamatan maklumat untuk perlindungan infrastruktur kritikal dalam perusahaan kecil dan sederhana. Perusahaan kecil dan sederhana tidak mempunyai penyelesaian yang sempurna untuk melindungi infrastruktur kritikal dan maklumat. Kajian ini mengenal pasti kerangka keselamatan maklumat sedia ada dan meraih pengalaman dan kelemahan daripadanya. Selain itu, kajian ini akan membangunkan kerangka keselamatan maklumat yang sesuai untuk infrastruktur maklumat kritikal dalam PKS. Setiap sektor dan pengurusan akan menyokong PKS dengan lebih baik. Projek ini memberi tumpuan kepada infrastruktur maklumat kritikal dalam syarikat yang berkaitan dengan beberapa pertahanan dan pencegahan sistem untuk syarikat meneruskan perniagaan yang dijalankan dalam talian. Memandangkan beberapa kerangka keselamatan maklumat versi lama untuk infrastruktur maklumat kritikal tidak lagi sesuai untuk syarikat kecil dan sederhana semasa, adalah penting untuk mencadangkan yang baharu untuk menyediakan perkhidmatan yang berkaitan. Kajian ini menemui faktor berkaitan yang berkaitan dengan kerangka keselamatan maklumat untuk infrastruktur maklumat kritikal daripada kajian literatur dan amalan sebenar dalam PKS. Ia akan membantu mencapai pengalaman dan mengelakkan beberapa isu atau keburukan sambil mencadangkan rangka kerja keselamatan maklumat baharu untuk infrastruktur maklumat kritikal. Metodologi yang digunakan untuk melancarkan kajian adalah kualitatif dan menggunakan temu bual untuk mengumpul data amalan PKS. Kajian ini menggunakan analisis kandungan dan pendekatan induktif untuk menganalisis data yang dikumpul berdasarkan konsep, tema, model dan sebagainya. Rangka kerja keselamatan maklumat yang dicadangkan untuk infrastruktur maklumat kritikal akan berdasarkan kelemahan dan pengalaman sedia ada daripada penyelidikan dan analisis.

ABSTRACT

The internet brings people to a better future, and due to IoT, daily activities have become convenient. However, security issues occur frequently when people enjoy the convenience and benefits of a life fulling of technology. Critical infrastructure may have failures of varying degrees of severity as a result of physical and logical vulnerabilities, and because there are many interdependencies among critical infrastructure, even minor failures may have serious effects on users. This project discusses the information security framework for critical infrastructure protection in small and midsize enterprises. Small and midsize enterprises do not have impeccable solutions to protect their critical and information infrastructure. Some malicious threats influencing relevant systems in companies will be discussed. This research study identifies the threats and vulnerabilities existing in critical infrastructure and critical information infrastructure such as nature disasters, cyber-attacks, human errors and so on. Also, this study develops the suitable information security framework for critical information infrastructure in SMEs. Each sector and management will support SMEs better. The scope of this study is on the critical information infrastructure in companies that relate to some defence and prevention of systems for the company to proceed with business running online. Since some old version information security framework for critical information infrastructure are no longer suitable for current small and midsize companies, it is significant to propose the new one to provide relevant services. The findings of relevant factors related to information security framework for critical information infrastructure from literature review and real practices in SMEs that helps to achieve experience and avoid some issues or disadvantages while propose the new information security framework for critical information infrastructure. The methodology used to launch the study is qualitative and use interview to collect practice data of SMEs. The study uses content analysis and inductive approach to analyse the data collected based on concepts, themes, models and so on. A proposed information security framework for critical information infrastructure will base on the existing drawbacks and experience from research and analysis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

ISF	Information Security Framework
CI	Critical Infrastructure
CII	Critical Information Infrastructure
SMEs	Small and Midsized Enterprises
NIST	Nation Institute of Standards and Technology
LR	Literature Review
SOP	Standard Operating Procedure
ISO	International Organization for Standardization

CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

The information security framework is one of the management tools that helps to provide scientific and significant methods and references. The framework will follow three security principles: confidentiality, integrity and availability (CIA). When properly implemented, an information security framework will enable any security executive to effectively manage the cyber risk within their firm. The framework comprises several documents in detail defining the adopted rules, procedures, and processes your organization must follow. It efficiently communicates how information, systems, and services are managed within your organization to all parties (internal, indirect, and external). The framework specifies daily practices intended to lessen the risk exposure, and guide in an emergency.

This chapter discusses the definition and function of information security framework for critical information. This chapter discusses the research background, problem statement, research aim and objectives, research questions, significance of research, research scope and project organization as well. This chapter designs the structure of this research study. The research value is explained, and it indicates it is necessary to launch the study.

1.2 RESEARCH BACKGROUND

An asset or system that is crucial for the upkeep of fundamental societal functions is known as critical infrastructure. Critical infrastructure damage, destruction, or interruption caused by terrorism, criminal activity, or other nefarious behaviours may

seriously harm security of the life and business running. Assets (real or virtual), networks, systems, processes, information, and functions that are crucial to the country and whose loss would have a disastrous effect on both national security and the economic and social well-being of its citizens are collectively referred to as critical information infrastructure (CII). CII may consist of various distinct infrastructures with crucial information flows and interdependencies between them (Mrs Ursula Owusu-Ekuful (MP), 2020). Based on current situation of the market, CII is the core in most companies especially in some technology organizations. IoT and big data are popular now, more people are using intellectual products during life and work. CII will be the root to support the society fulling intellectual products to run smoothly. CII will help companies to run business and extend smoothly. Most companies and organisations have one or more alternate power equipment to support work and life devices. However, companies or organizations do not have enough alternate network, systems and communication platforms. It is necessary to create a suitable information security framework for critical infrastructure especially for CII. More companies and organizations are paying more attention on CI and CII protection.

Small midsize enterprises and organizations are the huge market. Due to lack of powerful finance support and security awareness, they tend not to have relevant security framework to implement. Therefore, some threats always happened in these companies and organizations. These companies and organizations need relevant security framework to provide basic guideline and standards to help proceed with business running smoothly. SME is the target to collect practice data and analyse.

Information security framework for critical infrastructure provides the guideline about relevant management and protection. Example of CII sectors are energy financial institutions, telecommunications, health, and education. The loss of companies is huge when the critical infrastructure or critical information infrastructure is encountering destroy.

The main reason to develop the valuable information security framework is that the critical infrastructure and critical information infrastructure have a lot of threats or risks. Most common threats or risks of CI and CII are nature disasters,

cyber-attacks, human errors, and dependencies between each sector of CI and CII. A vulnerability is a property of an installation, system, asset, program, or any of its dependencies that, if it is exposed to a specific level of threat or risk, could result in its degradation or loss (inability to carry out its intended purpose) (Robles1, 2008). The descriptions of the Common Vulnerabilities and Exposures (CVE/CAN) are used to create the vulnerability specifications for the formal model of the sample scenario (Rieke, 2008). Some CVE and patches are given by products manufactures, but small-midsize enterprises do not upgrade timely. Therefore, more and more attacks will occur. Since these companies do not establish professional team to handle these issues such as check and test vulnerable products or network. These threats or risks influence the normal business running for relevant enterprises. If small and midsized enterprises cannot recognize these threats or risks, they will encounter more incidents and suffering from the lost. Therefore, the new ISF for CII will help relevant enterprises to solve these problems.

There are a lot of information security frameworks implemented in many companies or organization. Many information security frameworks involve machine learning, and many monitoring tools and applications need to support and proceed information security framework for CI and CII running. Latest technology and tools will upgrade the business environment, and existed information security frameworks will be old version. Therefore, old version tends to make risk and even incidents when companies are implementing relevant information security frameworks. Current versions need to take a high cost, and small and midsized enterprises cannot afford on it. Since they will not take huge cost like tools and devices implementation, the framework is required to allow SMEs to evaluate IT security measures at minimal cost due to the constrained IT budgets for SMEs (Kimwele, 2011). Existed information security frameworks for CI and CII can help accumulate abundant experience and avoid some risks while developing the new information security framework.

There are some challenges while developing and implementing information security framework. Owners of SMEs do not have enough security awareness to implement framework for CII. Moreover, they do not have enough budget to implement information security framework in SMEs. Employees do not have enough

knowledge about information security in SMEs. Most employee will not be enough professional in the aspect of information security. Excellent employees tend to join bigger enterprises and platform to develop and make efforts. That is one reason that SMEs do not have a stable cyber environment for work, and a lot of human errors will happen. Employee will impact the progress of implementing relevant information security framework. Employee of SMEs do not have enough relevant knowledge and technical skills to solve issues and make information security framework for CI and CII run smoothly. It will increase the time and finance cost. Therefore, the gap of employee is one challenge of implementing information security framework for CI and CII in SMEs. For this reason, it is necessary for SMEs use suitable information security framework to increase the security of CI and CII.

Therefore, most employee need to get relevant training and education about basic knowledge of cyber security. SME owners are unaware of how crucial information security is to the success of their business strategies. SME owners are more likely to take a reactive than a proactive approach to information security. According to the survey 2021, convincing SME owners to engage in a structured scenario-based process for risk analysis/information asset protection is one approach to solving this issue. SMEs cannot go through huge incidents or cyber-attacks. SMEs do not have enough assets to loss, and some incidents and cyber-attacks will destroy the whole company. Owners of SMEs need to consider more and some cost for information security framework is necessary. The new information security framework for CII will not occupy a huge cost in SMEs, and it will help reduce loss and risks.

There are many factors are influencing the development of management and protection of critical infrastructure in companies. The background of study of information security framework for critical infrastructure is very complex, and a lot of factors are impacting the development of information security framework for CI and CII. These factors are necessary of current society and SMEs, development trend in the future, nature disasters, human errors and cyber-attacks.

When the need of current society appearing, more supplement and discovery will be launched. It is necessary to study and develop information security framework for critical infrastructure. Companies and organizations may have many employees and equipment to support business running. The clear and scientific framework will lead the company and organization to proceed with business running. Current society need relevant framework to supply clear guideline to develop. As the development of technologies, companies prefer to implement IoT things and intelligent products in work and life. Therefore, more tools and platform need to manage, and more mistakes may happen during the business running. Holistic framework can help reduce mistakes and optimize management. Once some parts of CI are destroyed, the holistic framework will help reduce the lost and recover the business ruing and normal life. Companies and society need better framework to maintain and management so that better development will be proceeded.

As the incidents of cyber-attacks increased, more companies are suffering from cyber-attacks. Systems and online platform are some sectors of critical infrastructure, it is necessary for companies to create necessary information security framework to provide guideline so that companies can reduce lost after encountering cyber-attacks. The frequency cyber-attacks happened is high and it will cause huge damage to SMEs. This study focusses more on research of cyber-attacks/incidents.

1.3 PROBLEM STATEMENT

Many companies are in the progress to enhance the security level for CII, and they tend to identify relevant threats and risks so that they can create relevant solutions based on these threats. Companies analyze existing information security frameworks and compare current business environments to identify drawbacks of existing frameworks, and companies can optimize or propose the new framework to protect critical information infrastructure.

However, the number of incidents caused by critical information infrastructure failure are increasing and those threats or risks are impacting the normal business running deeply. Some businesses cannot run normally because of existing threats and new threats. Since the working environment changes such as working on

the cloud, the new threats related to critical information infrastructure are coming. SMEs cannot identify all threats or risks well. Past research (Begishev, 2019) has identified threats to CII, but not all the threats are fit with the SMEs in Asian countries. For big country like China, identifying the right threats have become crucial to CII due to the political landscape and competitiveness among companies to grow.

There are many existing information security frameworks as NIST, ISO 27001, COBIT and so on. However, the frameworks are generic in nature, and do not specifically customize for specific sectors. Moreover, most of the frameworks developed by consultants from western countries, which may have different culture, knowledge, skill, practice, or expertise than Asian countries. Because of this differentiation, it may cause unsuitability to adapt the framework without considering contextual factors. Many SMEs do not have their own frameworks or SOP to manage CII due to finance burden. Some current frameworks consist of a lot of tools and machine learning, and the cost is very high. Most SMEs cannot afford these frameworks. Companies avoid spending money and effort on specialists and tools for risk assessments. Consequently, there are more information security issues (Turskis, 2019). Therefore, this study analyses the existing well-established information security frameworks and considers the contextual factors from CII in current market to propose a framework that suitable for the SMEs.

1.4 RESEARCH AIM AND OBJECTIVES

The aim of this research is to propose the information security framework for critical information infrastructure which will be suitable for small and midsize enterprise (SME). Below are some research objectives:

1. To identify threats and risks of critical infrastructure (CI) especially for critical information infrastructure (CII).
2. To identify the existing process of information security framework (ISF) of critical infrastructure especially for critical information infrastructure.
3. To develop information security framework for critical information infrastructure.

1.5 RESEARCH QUESTIONS

1. What are the threats and risks for critical infrastructure especially for critical information infrastructure.
2. What are the processes obtained from existing security framework for critical infrastructure and critical information infrastructure?
3. How the information security framework for critical information infrastructure to SMEs be developed?

Above questions will be researched in this paper. These questions will find detailed explanation about the challenges and limitations while some companies or organization are implementing relevant information security framework for their critical infrastructure and critical information infrastructure.

1.6 SIGNIFICANCE OF RESEARCH

The study is necessary for researchers to study, the be information security framework of critical will be proposed based on those experience obtained from study. Some threats and vulnerabilities of CI and CII will be discovered and analysed. Some existed ISF for CI and CII will be analysed, and the aim is to propose the more suitable ISF for CII based on experience and analysis result. Small midsize enterprises and organizations need this security framework to optimize the management, defence, business running and future development. This study will satisfy the need of market and lead the development trend to better and safer environment. It will increase the success of defence and protection on cyber-attacks and threats. The study will reduce and optimize the dependencies between each sector of critical infrastructure. The cost will be reduced while some irresistible disasters happened such as earthquake, flood and blackout so on.

1.7 RESEARCH SCOPE

The research scope focus on investigating the factors related to information security framework for critical information infrastructure. Some papers discussing relevant

factors will be reviewed as reference. Past research helps find guidelines to launch necessary investigation to specific target.

Small and midsize enterprises (SMEs) is selected as the study target to analyse. The new information security framework for critical information infrastructure will be developed based on analysis results of SMEs. Small and midsize companies or organizations always encounter a lot of incidents and risk of critical infrastructure. Normally, they do not have enough finance support to establish or optimize holistic information security framework for critical infrastructure especially for critical information infrastructure. SMEs may lack the knowledge and resources necessary to effectively manage information security. Small businesses lack the specialized information security knowledge necessary to effectively comprehend information security risks and controls, conduct risk assessments, or create information security policies. Another factor is that these companies do not pay attention on framework establishment and application. Therefore, this project will propose the suitable framework for such companies and organizations to apply.

This research period will be two months and it selects three SMEs to launch investigation, and three people will be selected from IT department, financial department and the owner or leader of SMEs to participant in interview. These SMEs have different type of industry but all of them are not professional in information security industry such as food, education and real estate industry. The investigation focus on SMEs locating in China and Malaysia, and some SMEs in Shanghai city and Kuala Lumper. These SMEs has clear need for critical information infrastructure protection.

The analysis data collecting method will be go through interview. These data will be filter and analysis by relevant tools such as google form and excel so on. The research study select the content analysis method to extract valuable data from interview. These data will help the study on the background of SMEs better so that some limitations, drawbacks and threats can be discovered well. It will enhance the SMEs' performance after implementing suitable information security framework for critical information infrastructure.

The challenge is to have approval to launch interview to staffs in relevant SMEs since companies have some privacy and limited time to accept interview and share the work and development situation in the company. Moreover, some Chinese staffs may have poor English to discuss relevant topics. This research will send many invitations to SMEs and increase the approval rate. Moreover, only some staffs with fluent English speaking will be selected in the interview.

1.8 PROJECT ORGANIZATION

This dissertation is divided into five chapters and include research part and innovation part. Brief introduction as following:

Chapter one discusses some components and introduce ISF, CI, CII and necessary sectors of CI and CII. The research background and research problem statement are discussed in this chapter. Some statistics is used to prove the problem background and statement. Some issues and threats among CI, CII and existed ISF are discussed. Based on the analysis of current cyber landscape for CI and CII, the research question, aim, objectives and scope of the study is defined. The significance of study discusses the effort and the importance of this research, so that the ISF for CII will be better in the future.

Chapter two focus on discussing a literature review based on research questions listed in last chapter. Many articles are reviewed and some of them are selected to define key points among research questions. A lot of risk and threats of CI and CII are researched from those articles published. It will provide the background and reason to propose more suitable ISF for CI and CII. There are a lot of existed ISF for CI and CII, and these ISF have some drawbacks and vulnerabilities for current CI and CII. It provides abundant experience and basic structure to develop a better ISF for CII implemented to SMEs. Some challenges are researched while implement ISF for CII into current SMEs. It will help to avoid when develop a new and more suitable ISF for CII. The conceptual framework will be designed based on paper review and analysis. Some investigations are proceeded, and a lot of evidence are found to prove in this chapter.

Chapter three explains the methodology and methods included when conducting the research in this project. The process from start to finish is discussed, and the data acquisition method is discussed as well. The framework of research study is proposed, and each step is explained. The research details of literature review are discussed. Some tools, resources selected and review processes are explained. This chapter will design all protocols such as paper search processes, paper selection criteria and interview protocol and so on.

Chapter four focus on presenting and analysing data collected. Some analysis methods such as content analysis, thematic analysis and so on will be used. The research will identify threats and vulnerabilities of critical information infrastructure among selected SMEs, and some drawbacks and limitation of information security management will be discussed as well. The analysis result helps the study propose the suitable information security frameworks for critical information infrastructure in SMEs.

Chapter five discusses the new ISF for CII. It explains the content and some processes of ISF for SMEs. Some extend points of the new ISF for CII will be discussed and analysed such as security policies and CII protection so on. Benefits of the ISF for CII will be discussed and the aim of the new ISF for CII is to solves issues, threats and vulnerabilities of CII and ISF with old versions.

Chapter six concludes the research finds and opinions. It will discuss the drawbacks and benefits of the study as well. Some general recommendations and improvements for future development of ISF for CII will be provided as well.

1.9 SUMMARY

This research findings will devote to development of ISF for CII for SMEs, and it will help SMEs to increase the cybersecurity environment and security level for CII. This chapter help to introduce some components and relevant topics of ISF for CI and CII. Some threats and vulnerabilities of CI, CII and existed ISF are found and analyzed. It will help to provide basic insight and experience about the development of ISF for CII in SMEs. Some statistics and factors of incidents related to cyber environment and CII

are presented. It indicates that the development trend of ISF for CII is brilliant and all enterprises need it to defend threats and risk especially for SMEs. This chapter also ensure the research objectives and questions which will help further study and scope for this topic. Moreover, the further study plan and research organization are confirmed. The significance of this research findings explains the importance of ISF for CI and CII and benefits for SMEs. Based on this research findings, the research study for ISF for CII is necessary, and it will optimize the cyber environment and management of CI and CII.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter designs the structure of literature review such as search process, criteria of selecting journals, conduct review and analyse review results. Abundant journals related to information security framework for critical information infrastructure will be reviewed. The first part is to review relevant journals and define all concepts such as critical infrastructure, critical information infrastructure, information security framework, SMEs and so on. To make people understand information security framework, critical infrastructure and critical information infrastructure better. The second part is to review relevant journals and address relevant threats and risks of critical infrastructure and critical information infrastructure. The third part is to review relevant journals and identify drawbacks of existing ISF for CI and CII. The fourth part is to review relevant journals and define limitation and challenges of SMEs.

2.2 DEFINITION OF CONCEPTS

This section discusses the concepts that related to this study such as information security framework, critical infrastructure, critical information infrastructure and SMEs. These concepts influence the development of suitable information security framework for critical information infrastructure. Each concept has its own vulnerabilities and impact the business continuity and work environment in companies.

2.2.1 Information Security Framework

Information security framework is the enhancement management or stand operation guideline to help companies or organizations protect their assets. The frameworks allow these agents to comprehend how companies will safeguard their data or offerings. Companies can fulfil that requirement with the aid of this Information Security Framework (ISF). From the standpoint of their employees, clients, and suppliers, it's crucial that the company is perceived as adhering to basic security practices in terms of how companies manage their personal and confidential data (International Association of Accountants Innovation and Technology consultants (IAAITC) , 2011).

A lot of firms might align with one of the best practice frameworks for information security. This necessitates that the national institute of standards and technology cyber security framework (NIST CSF) be in line with such frameworks. Industry best practices and standards are included in the NIST CSF. The NIST CSF framework makes it abundantly apparent that companies planning to use it can use their current procedures and layer them on top of the framework to find any gaps. The enterprise risk management method is used to manage the risk of cyber security, which is one of the three key components of the NIST CSF. The framework core, risk tiers, and framework profile are the three components. As a framework, the NIST CSF must adhere to a number of standards, such as the high-level requirements for information security. It must adhere to regulations and standards such NIST SP 800-53, ISO-27001 Annex, and ISF SoGP (Almuhammadi, 2017).

2.2.2 Critical Infrastructure and Critical Information Infrastructure

A critical infrastructure (CI) is a collection of physical or virtual systems and assets that are so crucial to the country that any interruption of their operations could have a negative impact on public safety, health, or economic well-being, or any combination of these (Alcaraz, 2015). A vital information infrastructure is a computer system or computer network that is necessary for either national security or the economic and social well-being of residents, according to the Cybersecurity Act, 2020 (Act 1038). Critical information infrastructure (CII) and critical infrastructure are distinct but

connected. The connection is mainly being ignored, though. It is crucial to make a distinction between the two for the purposes of this article, which discusses critical infrastructures in general.

CII is a crucial infrastructure, which means that critical infrastructures often include but are not limited to CII; however, not all critical infrastructures are CII. Critical infrastructure may fail because of CII failure, however critical infrastructure may also collapse for a variety of unrelated reasons. For instance, a natural disaster like an earthquake or flood could cause critical infrastructure to fail, but cyber-related threats (i.e., cyber-attacks) or the failure of a critical infrastructure are the main causes of CII failure. This suggests that compared to CII, critical infrastructure is more vulnerable to a wider range of risks (Zaballos, 2016).

2.2.3 Small Midsize Enterprises (SMEs)

SMEs are playing more and more important role in current market, and they are occupying more and more market. It states that a company is considered to be small or medium-sized if the sum of all of its employees is less than 250. According to the European Commission, a business can be classified as medium-sized if it concurrently fits the following criteria: greater than 49 but fewer than 250 people work there (Savlovschi, 2011). It is the scale of SMEs, and it indicates SMEs do not have a lot of staffs to run business. Considering another side of SMEs, the capability is another factor to define SMEs. SMEs do not have abundant capabilities such as finance support, abundant critical infrastructure, and stable working environment. In the overall operations of SMEs, IT infrastructure has emerged as a highly important asset. The rise in cyberthreats against SMEs has made management boards more aware of the necessity and significance of addressing the risk associated with the general reliance of company on information technology.

2.3 THREATS AND RISKS FOR CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE

In this part, some articles related to threats or risks for critical infrastructure especially for critical infrastructure will be searched and reviewed. These threats and risks will

be filter out and discuss. Some factors and vulnerabilities of critical infrastructure and security framework will be researched in this chapter. It will provide a lot of experience for author to learn and launch the establishment of information security framework for critical infrastructure.

According to the article “Vulnerability of Critical Infrastructure by Nature Disasters” (Saša Mijalković, 2013), Understanding the physical characteristics of natural disasters—namely, their destructiveness, which is determined by destructive force and probability of propagation in the territory—allows one to grasp how they affect essential infrastructure. Disaster severity and community vulnerability are strongly correlated; for instance, an earthquake of a given magnitude will not inflict the same damage on a town with contemporary concrete multi-story structures as it will on a village with disintegrating clay cottages. This journal analyzed the different consequences of nature disasters on critical infrastructure such as geophysical disasters, hydrological consequences and meteorological disasters and so on. This analysis will help the framework will be proposed optimize content about nature impact of critical infrastructure. Below are some data of nature disasters.

Primary hazard	Secondary hazard
Earthquakes	Landslides, tsunamis, fires, floods
Storm surges	Coastal floods
Volcanic eruptions	Earthquakes, wildfires, floods
Wildfires	Landslides
Severe storms	Tornadoes, flash floods
Landslides	Tsunami
Extreme summer weather	Wildfires
Floods	Fires
Hurricanes/cyclones	Storm surges

Figure 2.1 Primary and secondary risk of nature disaster (Bimal, 2012).

Type of disaster	Frequency (time)/%	Deaths (persons)/%	Population affected (ten thousand)/%	Direct economic losses (USD 0.1 billion)/%
Flood	206/56.13	4393/41.87	2919.81/28.03	746.07/29.59
Storm	82/22.34	1876/17.88	1761.45/16.91	1376.76/54.60
Earthquake	25/6.81	2742/26.13	109.13/1.05	113.06/4.48
Wildfire	19/5.18	128/1.22	71.77/0.69	92.54/3.67
Drought	13/3.54	0/0	5504.67/52.84	121.00/4.80
Landslide	11/3.00	224/2.13	0.56/0.01	2.50/0.10
Volcanic eruption	8/2.18	85/0.81	49.37/0.47	13.45/0.53
Extreme temperature	3/0.82	1044/9.95	0/0	56.00/2.22
Total	367/100	10492/100	10416.76/100	2521.38/100

Figure 2.2 The incidents details about disasters worldwide in 2021 (Govt.China, 2022).

Both individuals and organizations, from huge multinationals to medium-sized, small, and micro enterprises, were impacted by these calamities throughout Asia. As an illustration, the 2011 floods in Thailand affected at least 557,637 firms, 90% of which were small and medium-sized organizations (SMEs). Additionally, this catastrophe resulted in the loss of jobs for nearly 2.3 million workers [2]. Economic losses were estimated to be USD45.7 billion by [3], with SMEs bearing the majority of the losses (Auzzir, 2018).

Period	1985 - 1999	2000 - 2014	Percentage (%)
Occurrence	3 981	6 506	63.43 (increased)
Death	687 633	1 272 868	85.11 (increased)
Economic damages ($'000)	800 368 660	1 777 383 206	122.07 (increased)

Figure 2.3 Impacts of natural disaster in Malaysia. Source from: (Auzzir, 2018).

According to the article "Impact of Cyber-attacks on Critical Infrastructure" (Kutub Thakur, 2016), hospitals, critical facility management systems, and electronic national defense systems are the main targets of cyberattacks and the resulting damages. Additionally, water supply, power and grid systems, financial platforms and banking systems, automated transportation control systems, and military and civil air traffic controllers. A gadget or a set of computer instructions intended to illegally

harm a computer or telecommunications system is referred to as a "cyber weapon." Additionally, the nature of vital infrastructure, its programs, or its data makes it easier for its operation to be completely, partially, or differently interrupted. Critical infrastructure is the first target to launch cyber-attacks, this author needs to use proper method to improve the protection in this aspect. Now, cyberattacks on networks, hardware, software, processed data, or data that has been stored or processed are the most common (Požár, 2019). There are a lot of different methods to destroy the critical information infrastructure such as hacking, phishing, sniffing, ransomware, denial of services and encryption and so on.

Only 10% of computer crimes reported to the police by small and medium-sized businesses result in the conviction of criminals, despite the fact that 77% of cybercrime targets SMEs, 58% of SME managers do not view cyber-attacks as a significant concern, and 65% of SMEs lack a security policy (Ključnikov, 2019).

One of the attacker's most well-organized cybercrimes in the twenty-first century. Phishing is described as "Criminals' creation and use of e-mails and websites - designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies - in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords," by the United States Department of Justice (Sangani, 2012). Based on the journal “Cyber Security Scenarios and Control for Small and Medium Enterprises”, many types of cyber-attacks to SMEs are identified such as phishing, web application attacks, SQL injection, Cross Site Scripting (XSS), insider attacks, wireless network breaches, Wi-Fi hotspots and so on. Malware attacks rose 358% in 2020 compared to 2019. Through 2021, the number of cyberattacks climbed by 125% globally, and in 2022, more and more cyberattacks threatened both enterprises and individuals. 323 972 online users reportedly fell for phishing scams in 2021. This indicates that 50 percent of the users whose data was compromised fell victim to a phishing scam (AAG, 2023).

The incident of cyber-attack is growing more during these decade. A lot of crimes switch the attack methods to emails. Criminals can steal the data and other

assets from the email, and email threats are existing among a lot of people. People are suffering from these email threats and attacks. A lot of enterprises and institutes lost lots of assets from the email attack. In 2021, phishing campaigns and credential phishing both grew. In 2021, almost 6.3 million credential phishing attempts were detected and stopped by Cloud App Security, a 15.4% increase. Similar to 2020, there were more known phishing attacks discovered than undiscovered ones, but the difference increased by an astounding 72.8% (Trend Micro, 2022). These data indicate that people are facing terrible email environment. Based on the trend, more and more incidents will be appeared in the future.

Phishing attacks is keeping increasing in 2021. People are suffering from this email threat deeply. Due to the huge number of statistics about phishing attacks below, it is necessary for people to seek more useful prevention methods. Below is the statistics in phishing activity trends report 4th Quarter 2021.

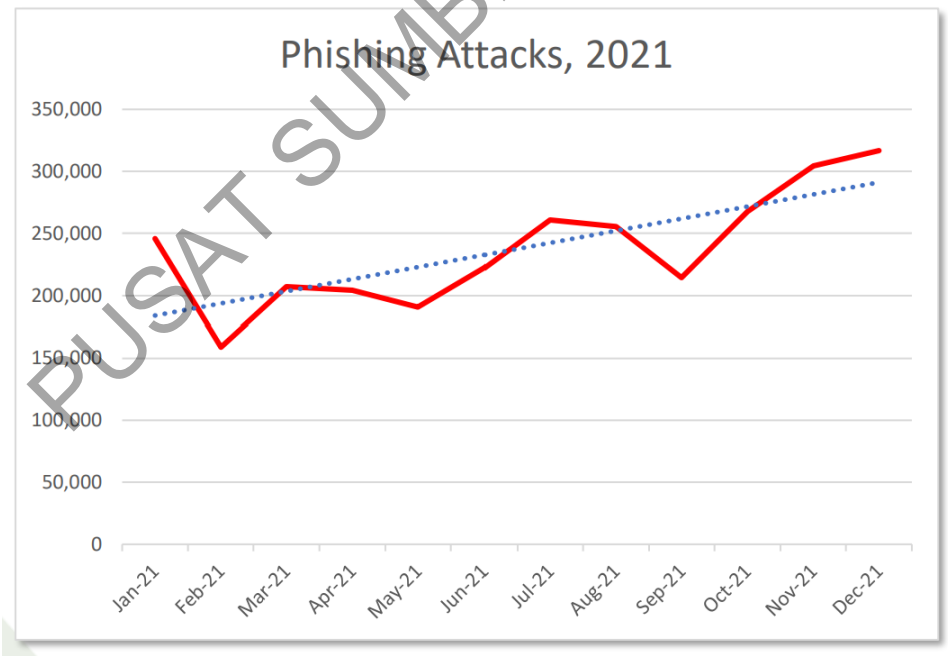

Figure 2.4 Phishing attacks statistics, source from: (APWG, 2022)

Since early 2020, when APWG (Anti-Phishing Working Group) was tracking between 68,000 and 94,000 attacks per month, the number of recent phishing attacks has more than tripled.

	October	November	December
Number of unique phishing Web sites (attacks) detected	267,530	304,308	316,747
Unique phishing email subjects	12,350	13,937	16,461
Number of brands targeted by phishing campaigns	624	682	521

Figure 2.5 Number of attacks. Source from: 4 (FEDERAL REGISTER , 2013)

The impact of cyber-attacks is huge for companies and organizations. Comparing to nature disasters, companies can choose to avoid this problem and lost for critical infrastructure. Since the outstanding management and defence can help SMEs to avoid cyber-attacks. Phishing attack is becoming more and more popular, and above data are indicating the situation of current cyber environment. In this paper, information security framework will provide excellent guideline about protection, response and recovery of critical information infrastructure. It will help reduce the risk and lost after encountering relevant issues for companies and organizations.

"Hyper Threats to Critical Information Infrastructure: Bringing the AI in the Game" discusses the dependencies is another threat to critical infrastructure and critical information infrastructure (HADJI-JANEV, 2021). As the first line of defence against failures and attacks, critical information infrastructure security and resilience must be addressed from a systemic perspective due to the high reliance on them, their cross-border interconnectedness and dependence with other infrastructures, as well as the vulnerabilities and threats they face. The dispersed, redundant design of the Internet has made it a remarkably reliable infrastructure. As a result, various policy drivers are responsible for CII protection (CIIP). These forces cut across the lines of globalization, convergence, and reliance, as well as those of conflict, terrorism, cyberattacks, and natural catastrophes, and extend all the way up to laws, rules, instructions, and reaction strategies. Each sector of critical information infrastructure will impact the whole business running. As an example, if the router is broken, and all business online cannot work normally. It is one of examples to prove that the dependency is one threat of CI and CII. Other sectors will be influenced by some sectors deeply. In addition, if some sectors are encountering cyber-attacks, other

sectors will be affected soon. As another example, if the printer is encountering the ransomware attack, other devices connected to this printer will be affected by ransomware soon. Therefore, low interdependencies between each sector of CI and CII will reduce the threats and risks.

The kind and extent of dependencies have a significant impact on how the impacted infrastructures operate. A vulnerability in linked infrastructures can result in failures among the impacted infrastructures that have a common source, cascade, or even escalate. As a result, understanding dependencies is crucial for reducing the risks brought on by an infrastructure's weaknesses. (Eronen, 2006)

According to the article “Security threats to critical infrastructure: the human factor”, the human factor is one threat to critical infrastructure and critical information infrastructure. Although monitoring tools and intrusion detection systems are important for network security, the human element should also be taken into account. To prevent people from unintentionally introducing malware to the organization, it is essential that proper care and caution be exercised at all levels during technological contact. Although security awareness training programs have a reputation for offering efficient means of spreading information about security precautions, they have a few drawbacks (Ghafir, 2018). Human errors can bring direct and indirect influence on business running in companies. It will impact the CI and CII as well. Human errors will impact the maintenance of CI and CII, and it even break CI and CII as well. Some employees may leak some sensitive data such as account information and so on. Some hackers will launch relevant attacks and destroy some critical information infrastructure such as server and memory devices based on account information of companies. Thus, it brings indirect influence and causes the company suffering from different attacks. Phishing is an attack method which takes advantage of human factors. Some employees may not have enough security awareness or knowledge, they tend to click some suspicious links so that some phishing and ransomware attacks can be launched successfully. Below table are some case studies about consequences of human errors.

Table 2.1 Case Studies About Human Errors.

Case study	Human errors	Description
Southwest 2011 blackout	Operator error that results in non-compliance with NERC-CIP N-1 contingency standards.	The system "was not in a NERC-CIP N-1 compliant state," according to reports from the Federal Energy Regulatory Commission (FERC). The system must be operated with utilities in order to prevent instability, separation, or cascading caused by the failure of a single component.
Florida 2008 grid blackout	Due to operator error, internal redundancy safeguards were disabled, which prevented the grid from operating in real-time.	Human errors always cause the damage make companies and organizations to lose a lot. It is similar to nature disasters.
Colombia 2008 total blackout	Employee did not follow substation interlocking procedures correctly.	Due to human mistake made at the 230 KV Torca substation, 25 million people in Colombia experienced a complete blackout.

Unintentional human mistake now accounts for 50% of the worst breaches in the past year, up from 31% the year before, which may come as a surprise to people outside the security community. As a result, a single factor that has not changed since the inception of information security management is to blame for 50% of significant security events. People and the accidental faults and blunder they commit make up this part. Additionally, according to Dunn, 93% of breaches were caused by human mistake, and 95% of data loss in the UK was brought on by social and cultural issues (Mark Evans, 2016).

This research study has reviewed many journals based on keywords and string searching. Only a few journals are selected based on selection criteria, and the valuable data were extracted and presented on the study. Regarding threats and vulnerabilities of CII in SMEs can be analyzed from three aspects which are Physical,

cyber-attacks and human errors. Some statistics are extracted to support the opinions. Below table are analysis details.

Table 2.2 Summarized findings of threats and vulnerabilities of CII in SMEs

	Threats or Incidents	**Analysis Type**	**Business Impact**	**Solutions**
Physical Threats	Nature disasters, dependencies	Content analysis and statistics.	It can destroy all assets and business completely, but it will not happen frequently.	Backup and great recovery strategies.
Cyber-attackers	Phishing, web application attacks, SQL injection, Cross Site Scripting (XSS), insider attacks, wireless network breaches, Wi-Fi hotspots etc.	Content analysis and statistics.	It will cause huge damage, and SMEs will lose a lot of money. It can happen frequently.	Security awareness of employees, defense tools and service such as firewall, WAF and so on.
Human Errors	Data breaches data leakage, indirect cause cyber-attacks such as phishing, indirect to cause devices broken.	Content analysis and statistics.	It can cause huge damage and little damage depending on the level of human errors. It can happen frequently.	Security awareness training, security polices, access control.

Threats and vulnerabilities of CI and CII can impact the business running in companies. It finds these threats and vulnerabilities of CII existing in SMEs, some statistics are extracted to indicate the numbers of incidents. These threats and vulnerabilities are keep existed in CI and CII. We cannot remove or avoid these threats and vulnerabilities absolutely. The solution can reduce the influence and loss

caused by these threats and vulnerabilities. Threats and vulnerabilities identified to CI and CII are nature disasters, cyber-attacks, dependencies and human factors after reviewing articles. Most opinions are agreed for the study, and the solution is to develop the new information security framework for critical information infrastructure. The information security framework will help reduce the influence and risks caused by these threats and vulnerabilities through suitable guidelines and management.

2.4 EXISTING INFORMATION SECURITY FRAMEWORK

There are some existed security frameworks for critical infrastructure. Mostly, those frameworks will only focus on one part of sector of critical infrastructure. Below are some existed security frameworks and management structure which will help the study to propose the information security framework for critical information infrastructure.

2.4.1 Cross-Layered Framework (Agnew, 2022)

The figure 2.2 indicates the security framework for one part of critical infrastructure which are power grid and communication network. The source is from article "Implementation Aspects of Smart Grids Cyber-Security Cross-Layered Framework for Critical Infrastructure Operation" (Dennis Agnew, 2022). the framework is divided into three phases which are detection, identification and correction about cyber-attacks based on machine learning. The applied targets are power grid and communication network. The logistic of this framework is to collect data from power grid and communication network, then save those data in the "CSV" file after cyber-attacks tool place and their effects happened. The framework will launch each process to analyse these data and find attack evidence.

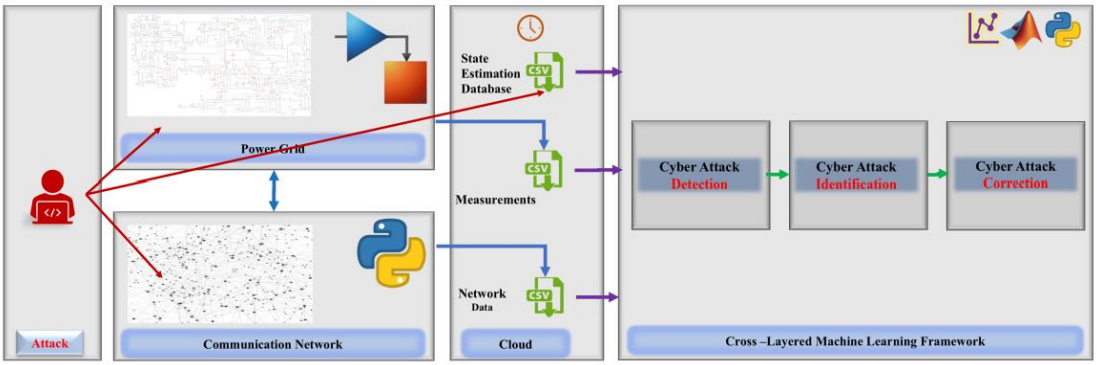

Figure 2.6 Proposed framework for cross-layer.

2.4.2 Detection Framework (ICRC, 2017)

Figure 2.5 is the detailed framework of detection for cyber-attacks. Based on the data from "CSV" file, the machine learning will help to filter and identify if those attacks are true positive sign. (ICRC, 2017)

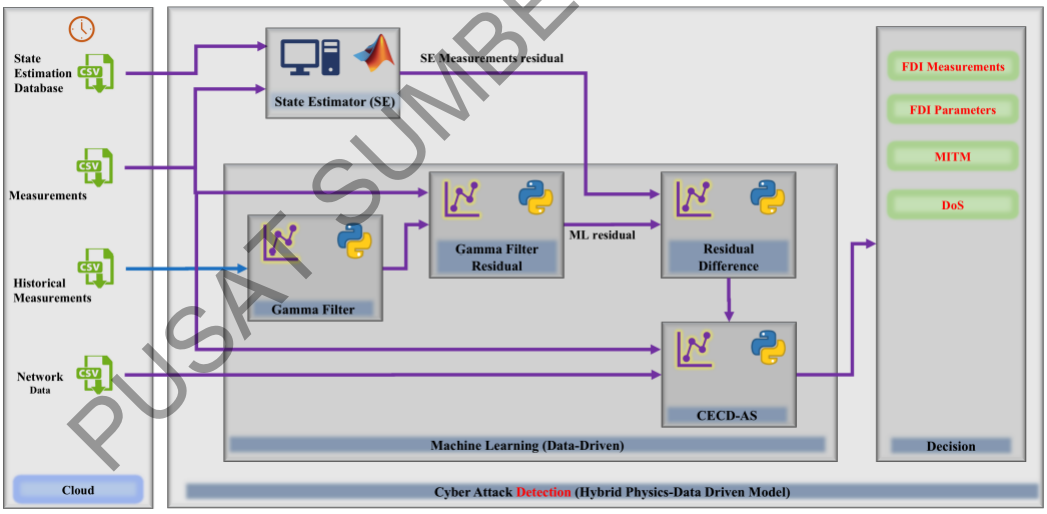

Figure 2.7 Detection framework

2.4.3 NIST Information Security Framework

Based on the article "Information Security Framework", the Information Security Framework shall serve as the basis for all technological, organizational, and regulatory regulations and procedures intended to ensure the security of information and information systems (ICRC, 2017).

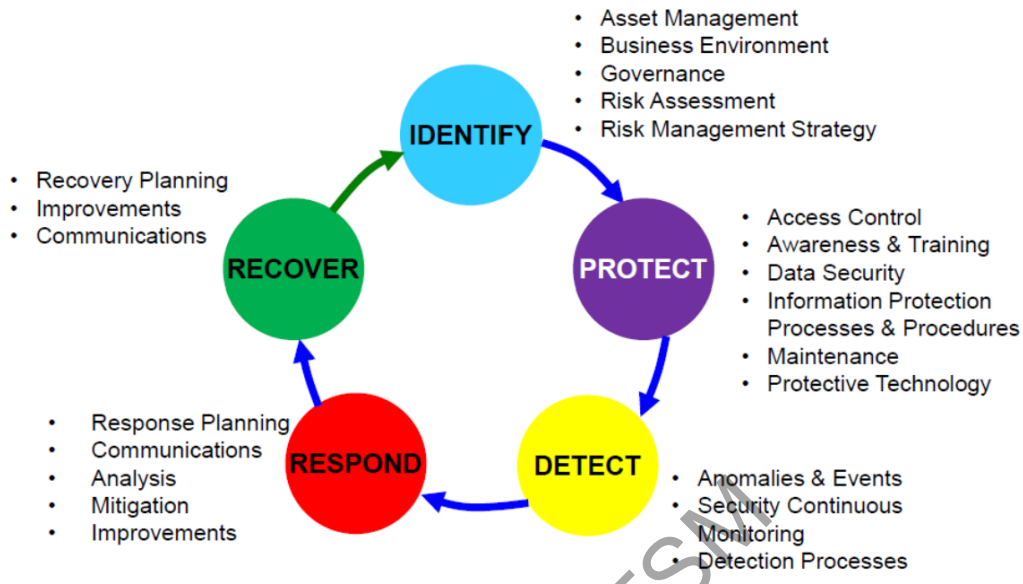

Figure 2.8 Information system management framework.

There are five main processes in this framework which are necessary proceed with the better management for relevant information system. For critical infrastructure, these processes also provide with scientific guideline in the management cycle. The National Institute of Standards and Technology (NIST) also recommend these processes to manage and guide organizations or companies to protect relevant targets. Below figure is indicating the cybersecurity framework core structure (NIST, 2018).

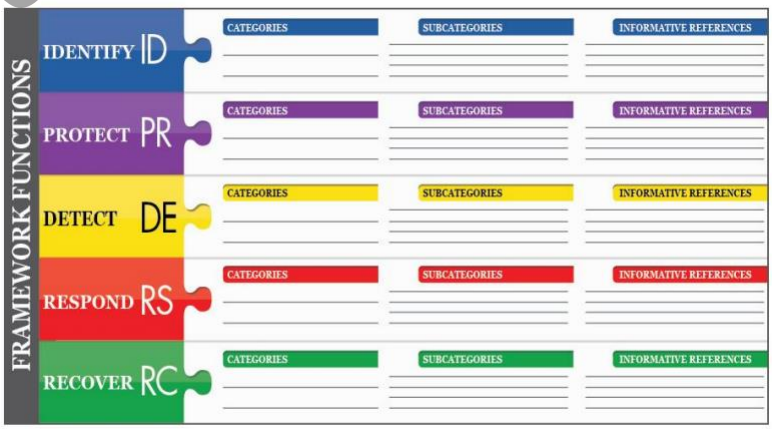

Figure 2.9 Cybersecurity framework core structure.

Identify, Protect, Detect, Respond, and Recover are the names of these functions. By organizing information, facilitating risk management decisions, mitigating threats, and improving by drawing lessons from past actions, they help a company communicate its management of cybersecurity risk. A Function is divided up into categories, which are collections of cybersecurity outcomes tightly related to specific programming requirements and activities. Subcategories further categorize a Category into particular managerial and/or technical activities' results. Specific sections of industry-wide norms, policies, and procedures that provide examples of how to accomplish each Subcategory's objectives are considered Informative References.

2.4.4 Security Framework Algorithm

Based on the article " PolyOrBAC: a security framework for critical infrastructures" (Anas Abou El Kalam, 2009), A security policy is defined, implemented, and audited by PolyOrBAC in intra- and inter-organizational workflows. The security framework is a set of rules expressed by algorithms. Below figure shows detailed framework processes of algorithms:

$$
\begin{aligned}
&\forall \text{ org} \in \text{Organizations}, \forall \text{s} \in \text{Subjects}, \forall\, \alpha \in \text{Actions}, \forall \text{ o} \in \text{Objects},\\
&\forall \text{ r} \in \text{Roles}, \forall \text{a} \in \text{Activities}, \forall \text{ v} \in \text{Views}, \forall \text{ c} \in \text{Contexts}\\
&\boldsymbol{Permission}\ \mathbf{(org, r, v, a, c)} \wedge\\
&\textit{Empower}\ (\text{org, s, r}) \wedge\\
&\textit{Consider}\ (\text{org}, \alpha, \text{a}) \wedge\\
&\textit{Use}\ (\text{org, o, v}) \wedge\\
&\textit{Hold}\ (\text{org, s, a, o, c})\\
&\rightarrow \boldsymbol{Is\ permitted}(\mathbf{s}, \alpha, \mathbf{o})
\end{aligned}
$$

Figure 2.10 Security framework: rules algorithms.

This rule states that if a security rule in a particular organization allows role r to perform activity a on view v when context c is true, and if r is assigned to subject s, if action is a part of a, if object o is a part of v, and if c is true, then s is permitted to perform (for example, WRITE) on o. (e.g., f1.txt). The definitions of responsibilities and prohibitions are equivalent. This framework is paying more attention about security policies to limit each processes running. For businesses taking part in a CII,

OrBAC offers a number of advantages and solves a number of security needs, including rules expressiveness, abstraction of the security policy, scalability, heterogeneity, and evolvability.

2.4.5 LCCI

The implementation of the least cybersecurity controls with regard to DiD and the least cybersecurity controls for mission-critical assets with regard to CIA Triad priorities will serve as the foundation for the least cybersecurity control implementation (LCCI). In order to be implemented effectively, it has three stages. The framework includes seven steps make up the LCCI, as indicated below and explained in more detail in subsequent parts (Pawar, 2022).

Figure 2.11 Seven steps of least cybersecurity control implementation (LCCI)

2.4.6 SME Security Guidance

The study offers a high-level structure for these principles below and advises that SMEs information security rules be given a consistent format. SMEs can conclude that prioritization and structuring of guidelines will be a driver to more effective communication and a better understanding among the enterprises given that analysis of the major information security advice sources for SME shows a large number of gaps and overlaps (Lacey, 2010).

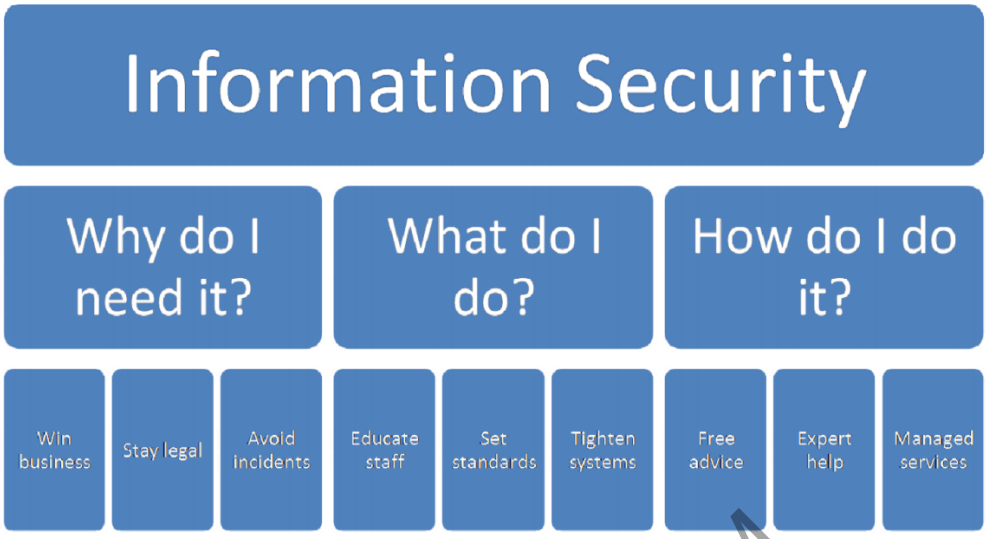

Figure 2.12 An efficient structure for SME security guidance, source from: (Lacey, 2010)

2.4.7 Framework for Establishing an Information Security Culture

SMEs should periodically review and assess the actions taken to advance forward. This conclusion has previously been reached for information security management programs. Responsibility, integrity, trustworthiness, and ethics are desirable behavioural attributes that can be developed through a variety of internal and external activities. For large organizations, internal management initiatives are required to bring about this transformation, according to Dhillon and Backhouse (2001), but the framework created for the study also assigns duties to external organizations like the government and vendors and recognizes the importance of national and societal/ethical culture, as shown in the figure below (Dojkovski S. L., 2007).

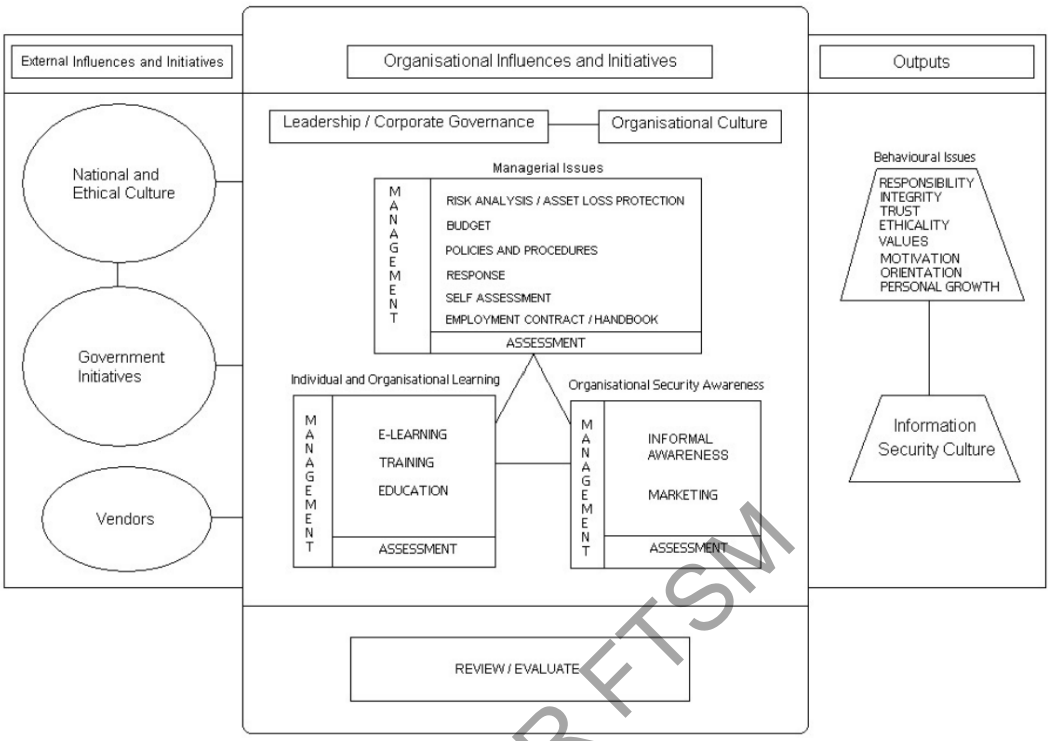

Figure 2.13 Framework for Establishing an Information Security Culture in Australian Small and Medium Size Enterprise. Source from: (Dojkovski S. L., 2007).

2.4.8 Analysis of Existing Frameworks and Information Security Guidelines

Above review results show the sample security framework for single sector of critical infrastructure and whole critical infrastructure. People can understand that the type of framework can be different such as machine leaning processes, cycle processes and rule algorithms. In this paper, the security framework will use cycle processes to provide general guideline, some sectors will use other types of frameworks especially for sectors of critical information infrastructure. Below table shows the analysis of three framework above:

Table 2.3 Compilation of reviewed information security framework for critical infrastructure.

Article Reviewed	Framework Types	Benefits for Proposing New Framework	Challenges
Implementation Aspects of Smart Grids Cyber-Security Cross-Layered Framework for Critical Infrastructure Operation	Machine learning process	Use technical logistics to propose the security framework, the machine learning will help establish the framework for critical information infrastructure protection	Machine learning will ignore factors, High cost.
Information Security Framework, Framework for Improving Critical Infrastructure Cybersecurity	Cycle process	It will help establish the general framework to manage all sectors of infrastructure	Lacking detailed processes in specific sector such as power and water
PolyOrBAC: a security framework for critical infrastructures	Rules algorithms	It is benefited to establish security policy, especially for employee management	The algorithm is not flexible, there are a lot of human factors

There are three typical information security frameworks and management structure for SMEs extracted from LR. These existing frameworks and management structures focus on SMEs and they are still having some drawbacks based on analysis below.

Table 2.4 Analysis of drawbacks of existing frameworks and management structures in SMEs

	Drawbacks	Analysis Type	Solutions
LCCI	Lack of backup, security awareness training and recovery part.	Processes analysis and content analysis.	Based on real situation of SMEs, fulfill relevant parts and process.
SME Security Guidance	Lack of tools and services selection and implementation such as cloud service and relevant defense service.	Processes analysis and content analysis.	Although SMEs have finance burden, they still need to purchase necessary service and tools to optimize the defense level.
Information Security Culture Framework	Vendors service may cause high cost and reduce the security level and flexibility.	Processes analysis and content analysis.	Reduce some redundant parts and consider the cost of the framework.

2.5 SMALL, MEDIUM, ENTERPRISE

The role of SMEs is critical challenge encountered while implementing information security framework for critical information infrastructure. There are many critical challenges such as budget limitations, low capability, lack of security experts, lack of security awareness, SME's owner attitudes and behaviour and so on.

2.5.1 Budget Limitations

Cost is the first consideration for SMEs. SMEs do not have enough budget to support, and most of them cannot afford on adequate resources such as tools and services so on. Some aims of information security framework is to reduce the cost among the cybersecurity. Based on the article "Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs)", this farmwork aim to make SMEs proceed security processes at low costs.

The framework is required to allow SMEs to evaluate IT security measures at minimal cost due to the constrained IT budgets for SMEs. This work provides an IT security implementation framework that will enable SMEs to adopt cost-effective security measures whose efficacy can be evaluated using relevant metrics, addressing the current challenges of enterprises reluctant to invest in IT security owing to cost (Michael Kimwele, 2011). Cost of SMEs is becoming the critical factor, and all work arrangement and solutions deployment will be proceeded based on limited budget. Most SMEs cannot afford on better platform, tools and services. Therefore, it is the challenge to implement ISF for CII in SMEs.

2.5.2 Low Capability

Low capability includes two main parts which are resources and staffs. SMEs do not have enough finance support and they cannot afford on great security products and relevant solutions so on. From another side, SMEs do not have powerful team to support the business running. SMEs cannot provide professional training with great quality. According to An Investigation of Information security in Small and Medium Enterprises (SME's) in the Eastern Cape, lack of staff training is another vulnerability

that many SMEs are encountering. Employees are frequently required to pitch in and do whatever is necessary to complete their tasks. People tend to know and trust one another more readily in a SME due to its size. Although informal relationships and procedures may characterize how small organizations operate, this may eventually have a negative influence on their information security (Upfold, 2005).

2.5.3 Lacking Professional Employee and Security Awareness

Other significant obstacles with the use of cybersecurity best practices include the challenges with obtaining funding for cybersecurity projects, the degree of cyber awareness among collaborators, and the eventual shortage of resident Information Technology (IT) workers. Frameworks and standards for information security are essential for enhancing cybersecurity and reducing risk in businesses (Mário Antunes, 2021).

The article “Information security and Cybersecurity Management: A Case Study with SMEs in Portugal” also prove that lack of professional staffs with enough knowledge will cause a huge risk of SMEs. When implementing ISF for CII in SMEs, they need to have some professional staffs who can understand the processes and structure of the ISF. If there are no relevant staffs to understand ISF, it will be difficult for SMEs to launch and implement this ISF. SMEs cannot afford on cybersecurity experts, and they cannot provide relevant training to other staffs. SMEs may lack the knowledge and resources necessary to effectively manage information security. Small businesses lack the specialized information security knowledge necessary to effectively comprehend information security risks and controls, conduct risk assessments, or create information security policies.

2.5.4 SME’s Owner Attitudes and Behaviour

Owners of SMEs are leaders, and they have direct right to lead the company. Therefore, the development quality of the company depends on owners and their decision and strategies so on. Owners can decide if their companies need to implement ISF for CII. Owners will take full consideration such as cost, value and profits so on. However, the security awareness and relevant professional knowledge

will influence owners to make decisions. The journal “Enabling Information security Culture: Influences and Challenges for Australian SMEs” states that before choosing to adopt security software, several SME owners consider the accessibility of outside IT help. Even some owners are sceptical about the value of security systems. SME owners rarely examine their information security requirements. Additionally, since there will be fewer information security breaches than in large organizations, fewer incident reports will be written and read. As a result, information security may seem even less significant and garner less support and attention from SME owners (Dojkovski, 2010). Therefore, the challenge is to persuade SEMs owners to invest on ISF for CII. It is necessary for SMEs purchase some tools and services to protect their critical infrastructure.

2.5.5 Other Challenges

It is not possible to "cut and paste" big scale solutions into small business cyber security. Consideration must be given to the availability of resources, the technological environment, and small business operational procedures. Since cybercriminals are aiming for smaller targets, small firms have several common challenges that must be taken into account in cyber-security strategies such as technical challenge, human challenge, organisational or process maturity, industry standards cyber insurance, legal remediation and cost of a data breach (Tam, 2021). It is the challenge or vulnerability of its role.

SMEs are currently not sufficiently tackling information security. Although SME leadership is aware of the necessity of information security, this understanding is sometimes only fleeting. SME leadership must become involved with, comprehend, and implement formal information security procedures; otherwise, their organizations may suffer greatly from unintentional dangers or malicious attacks on their information systems, which could ultimately result in company collapse (Upfold C. T., 2005).

According to SMEs in this study, cybersecurity implementation presents unique difficulties. Budget restrictions, management, and staff support and dedication toward IT system security issues were the key organizational problems. The study

expressed opinions about the shortage of financial resources, particularly the budget for IT-related resources and cybersecurity. In the absence of this resource, management started to participate in IT choices and execution, despite the fact that they lacked the necessary competence. The results demonstrate that funding, management support, and attitudes are internal organizational constraints that limit how SMEs perceive cybersecurity. These elements are thought to have a detrimental effect on cybersecurity implementation and impose restrictions on it. Since SMEs do not typically have complicated systems, adopting strict cybersecurity precautions may prove challenging. The absence of complicated corporate procedures and antiquated systems is seen favourably (Kabanda, 2018).

2.5.6 Critical Challenges

There are a lot of challenges while implementing information security framework for critical information infrastructure. These challenges are divided into three parts which are limited budget, low capability and owners' attitudes and behaviours of SMEs. These challenges are influenced by a lot of factors. Below table indicating the analysis result:

Table 2.5 Analysis result for challenges in SMEs.

Challenges	Influence factors	Analysis and evaluation
Low Budget	Cash flow difficulty, occupy the high percentage of total cost, small business	Agree these opinions. Finance support is the core factor, and most SMEs are encountering this issue.
Low capability	Less tools and services deployment, Staffs do not have enough information security knowledge, Inadequate training and management.	Agree with these opinions, the quality of staffs are root and basic energy to support business running. HR department can hire more accurate staffs with abundant information security knowledge

to be continued…

…continuation

Owners' attitude and behaviour of SMEs	Less security awareness, business and resources limitation, less relevant knowledge	Agree with these opinions, as owners of SMEs, they need to accumulate a lot of different knowledge and make accurate decision
Lack of professional employee and security awareness	It is difficult to hire security expertise by limited budget and work environment. There is no clear security framework to guide and provide security awareness training.	Most SMEs have same challenges and limitations, most journal state accurate challenges about SMEs

Although the information security framework for critical information infrastructure have a lot of benefits and it will help create more value. There are still many challenges when implementing it in SMEs. It is because the role of SMEs has a lot of drawbacks and vulnerabilities by itself. Through the review, these challenges are still existed in SMEs. The new ISF for CII will help to overcome these challenges and mitigate the influence.

2.6 SUMMARIZING FINDINGS OF LR

Based on content analysis and statistics analysis, cyber-attack is the popular type of threats and phishing is the most popular and common attack ways in SMEs. Cyber-attacks happen in high frequency, but nature disasters cause the most serious consequences, and it can destroy all assets. However, human errors are the root cause of huge damage and indirect to cause different cyber-attacks. The security frameworks should pay more attention on human factors and provide relevant security awareness training with employees.

Existing security frameworks and management structures have some gaps and drawbacks related to the current work environment of SMEs. The security

frameworks should consider more about cost and security awareness training for employees. Some frameworks are old versions, and it is not suitable for the current work environment. Some frameworks are causing high costs and the performance is not great. Moreover, some frameworks are too complex, and it is not suitable for SMEs.

The budget limitation is the most challenge for current SMEs. There are a lot of services and tools sold by tech giants such as Microsoft, Google, Alibaba and so on. But the price is very high, SMEs cannot solve the challenges of budget limitation, but they can optimize their management to reduce relevant terrible consequences. The suitable information security framework for CII is necessary for them to reduce the cost and increase the profit.

2.7 CONCEPTUAL FRAMEWORK

The explanation for why a certain study should be done is provided in the conceptual framework. The conceptual framework specifies the methodological foundations of the research endeavor and describes the state of existing information, typically through a literature study. It also reveals gaps in the understanding of a phenomenon or problem. Typically, a conceptual framework includes a summary of pertinent literature, a synopsis of the pertinent theory, an explanation of why this theory might be instructive in this context, a specific research question that probably contains a hypothesis, a justification for the research methodology chosen, and a number of outcomes or variables of interest. Before the study begins, a conceptual framework is decided upon, and once data collecting has begun, it is rarely changed (Varpio, 2020). The conceptual framework provides the general structure of new security framework for critical information infrastructure. It extracts a lot of experience from the literature review such as threats of CI and CII and so on.

Based on LR, the research study identified three main aspects that influence the information security framework for critical information infrastructure. Moreover, another aspect needs to fulfill as well, it is the criterion and requirement. These aspects are:

1 Threats and vulnerabilities existing in CI and CII: The information security framework aims to solve these threats and vulnerabilities, and it will be optimized based on these threats and vulnerabilities. Through the LR, these threats and vulnerabilities identified are cyber-attacks, human errors, nature disasters and dependencies. The conceptual framework will consider these threats and vulnerabilities and avoid or solve them in relevant section.

2 Drawbacks of existing information security framework: The existing security frameworks are not suitable for current society. Some companies have implemented some work on cloud. They tend to save data into cloud, and it is more convenient and safer. The existing framework is too complex, and they have many gaps with current working environment. Some existing frameworks are taking high cost.

3 Challenges and Limitations of SMEs: The conceptual framework is designed for SMEs, and it need to consider the background and real scenario of SMEs. Most SMEs are having finance burden and they cannot afford on expensive tools and services. Most of them have low capabilities, and they cannot deploy many devices and services. Most employees of SMEs do not have enough professional knowledge and security awareness.

4 Confidentiality, Integrity, Availability (CIA): The conceptual framework must follow CIA rules, and it needs to protect SMEs' data and privacy fulfill the requirements of CIA.

The conceptual framework provides the general structure and relevant management method with all companies especially SMEs. A lot of existing framework and information security management method inspire the development of conceptual framework. The NIST information security framework, security guidance and the framework of establishing information security culture provides the basic structure. The information security performance is the core and the output. LR provides relevant factors and methods relate to information security management. Microsoft issued some structure and framework for critical infrastructure protection, and the guidance provides the design of necessary structure and steps such as prevent, detect, respond and recover (Microsoft, 2014). The conceptual framework develops

based on CIA and business situation in companies. Below is the detail of the information security framework for critical information infrastructure:

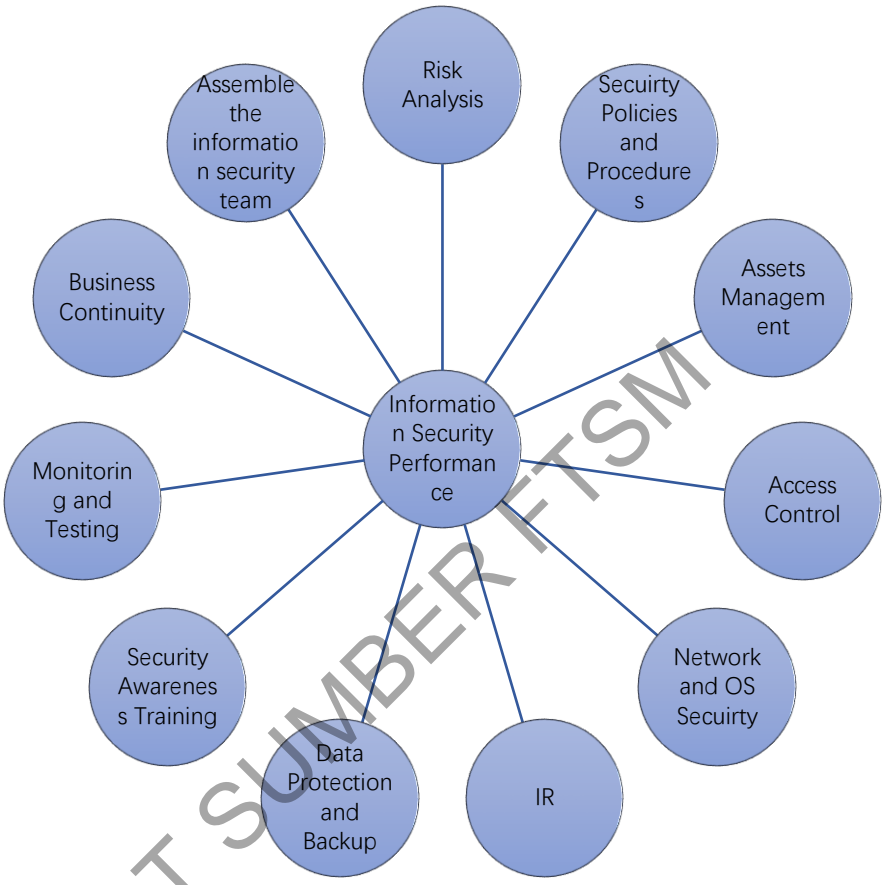

Figure 2.14 Conceptual Information Security framework for CII.

1. Assemble the Information Security Team

The professional job needs to be carried out by professional employees. Companies need to have the leader with professional knowledge to lead the team optimize the whole framework and structure in information security aspect of companies. Creating a governance framework for information security within the organization that outlines roles, responsibilities, and decision-making authority.

2. Risk Analysis

Team members need to conduct the risk analysis for all aspects of critical information infrastructure. Relevant risk assessment and criteria need to be designed as well. To identify and evaluate potential threats, vulnerabilities, and dangers to the key information infrastructure, conduct a complete risk assessment. Put risks in order of importance based on likelihood and potential impact. Creating risk mitigation plans and controls to handle the hazards that have been identified. The team needs to discover and excavate relevant threats and risks of CII in companies by professional test such as penetration testing and so on.

3. Design Suitable Security Policies and Procedures

The team need to design security policies and standard operation procedure (SOP) to limit all employees. It can help to reduce threats and potential risks from behaviours of employees. Create thorough security rules and processes that comply with legal standards and industry best practices. Including policies for business continuity, incident response, data classification and handling, access control, change management, and other pertinent areas. Making that all pertinent stakeholders are informed of regular policy reviews and updates.

4. Assets Management

Proper assets management helps reduce the rate of incidents. Many attacks or services broken are caused by these devices related to CII such as printer and so on. All equipment can be the entry for hackers to attack the cyber structure of companies. Keeping track of all essential components of the critical information infrastructure, such as networks, data, hardware, and software. Based on the value and criticality of the asset, apply the appropriate security controls. Implementing asset lifecycle management procedures, such as those for purchasing, deploying, maintaining, and disposing of assets.

5. Access Control

Access control is one part of implementing security policy. It needs to control all access about employees and activities such as entry to company, entry to devices of company, entry network environment of company and so on. Put in place reliable access control measures to guarantee that only people with permission can access vital information infrastructure. Enforcing the least privilege principle by only allowing users the rights they require to carry out their responsibilities. Making use of multifactor authentication, secure passwords, and routine access permissions reviews and revocation.

6. Network and Operating System Security

Putting in place strong network security measures including firewalls, an identity provider (IDP) system, and secure network architecture. Establishing procedures for network segmentation and isolation, and routinely keep an eye out for unusual activity. Protecting sensitive data in transit by encrypting network communications. OS security needs to be pay attention as well, the administration security needs to be tracked. Team members can review and check relevant logs timely. Based on industry standards and vendor recommendations, implement secure settings for operating systems, servers, and applications. Applying security updates and fixes on a regular basis to reduce known vulnerabilities. To find and fix problems, conduct regular vulnerability assessments and penetration tests.

7. Incident Response

Creating a plan for responding to security issues that describes how to prevent them from happening in the first place. Creating an incident response team and outline each member's duties. To evaluate and enhance response capabilities, conduct frequent incident response drills and exercises. The incident response team can select from the whole information security team and focus on the job of incidents response. Team members can conduct the response by following the SOP designed.

8. Data Protection and Backup

Use procedures for data loss prevention, data masking, and encryption to protect sensitive and important data. Creating policies for data retention and destruction that are compliant with legal obligations. Following all relevant privacy laws and rules and put privacy controls in place to safeguard personally identifiable information. All data need to be stored in particular place, and all authorization need to be managed and monitored. It needs to follow the rules and requirements of confidentiality, integrity and availability. The team needs to back up relevant important data such as business, customers, employees and so on. These back up data needs to be checked and tracked timely, and it is responsible for providing business resilience and continuously.

9. Security Awareness Training

It is necessary to provide relevant security awareness training with all employees in the company. Human always be the vulnerability of security, and it helps to reduce potential risks. To foster a culture of security, offer continual security awareness and training programs for employees and contractors. Users should be made aware of typical security dangers, social engineering techniques, phishing scams, and safe computing procedures. Reenforcing security policies and procedures and conduct regular security awareness initiatives.

10. Monitoring and Testing

Installing a reliable security monitoring and tracking system to quickly identify and address security events. Conducting routine security assessments and audits to find holes and confirm adherence to the security framework. Checking logs, network activity, and system behaviour for any unusual or suspicious activity. Team members needs to conduct necessary test to systems, services and devices timely. To check current work situation and excavate potential threats.

11. Business Continuity

This part includes business impact analysis and business recovery. It needs to identify Business Influence, Expected Loss, Maximum Tolerable Downtime (MTD), Maximum Acceptable Outage (MAO), Minimum Business Continuity Objective (MBCO), Recovery Point Object, Recovery Time Objective, Work Recovery Time (WRT), Recovery Plan and so on. Constantly evaluate and improve the information security architecture in light of new threats, technological developments, and incident-related lessons. Regularly evaluate the efficiency of security safeguards and address any flaws or vulnerabilities found. Keeping abreast of market developments, recommended procedures, and legislative updates to make sure the framework is current.

The important information infrastructure of the organization should be taken into account when designing this framework for its needs and hazards. To guarantee a comprehensive and successful implementation, it is crucial to include pertinent stakeholders, such as the legal, compliance, and IT teams. It depends on companies' investment. For SMEs, they do not have enough finance support, they can reduce the team scale, service and tools purchasing and so on. It helps SMEs to save the budget. Moreover, SMEs, do not need whole function and services since they do not have a lot of sectors of CII to protect. The business impact analysis result is low than investment.

2.8 SUMMARY

This LR launched a full review about relevant factors and challenges related to information security framework for critical information infrastructure. The study defined some key words and strings, and relevant articles will be filtered by searching for these key words and strings. The research and review are launched based on research questions. These factors and challenges related to research questions are defined and analyzed. This study analyzed and evaluated these factors after reviewing those articles.

The LR results are analyzed based on relevant factors of research problem, research objectives and research questions. The final aim is to develop the ISF for CII and implement it in SMEs. Therefore, the first review part was conducted based on definition of each topic such as ISF, CI, CII and SMEs. It makes people have full understanding about these topics. The second part was to review threats and vulnerabilities of critical infrastructure and critical information infrastructure. Through review, some threats and vulnerabilities are found and analyzed which are nature disasters, cyber-attacks, human factors, and dependencies. These threats provide the reason to develop the new ISF, and the ISF aims to overcome these threats and reduce the influence so that it can provide relevant service with critical information infrastructure.

The third part was to review relevant articles which describe existing information security framework. Through the review, some drawbacks and vulnerabilities of existing ISF are defined and discussed. These factors are old version, high cost, not flexible, and ignoring human factors so on. These factors provide the experience with this study, and it will help to consider and avoid these factors when developing the new ISF for CII.

The last part focuses on the challenges and limitations of SMEs. Some challenges while implementing the information security framework for critical information infrastructure in SMEs are discovered as well. The LR analyzed and discussed the background of SMEs, and made people understand the role of SMEs. These challenges are limited budget, low capability and owners' attitude and behavior of SMEs. These challenges will influence the value and significance of developing the ISF for CII. The background and the business of SMEs cannot be changed, the study can change the owners' attitude and behaviors. The ISF for CII will create more value rather than drawbacks and limitations.

The conceptual information security framework for critical information infrastructure is designed in this chapter. It indicates the optimized management from necessary aspects such as human, policies, CII and so on. It can provide better management and protection with companies. Relevant companies can select necessary services and rules which are suitable for their business and work environment. Some services and tools are optional, and necessary services and tools can support particular needs and requirements of different companies.

The LR creates a lot of value and provides clear guidelines and experience, the study can analyze these factors and experience so that these factors and drawbacks can be avoided or reduced during developing the new ISF for CII. Finally, this chapter highlights the threats and risks existing in critical infrastructure, drawbacks of existing ISF and challenges while implementing the ISF to target users through systematic literature review. Moreover, the conceptual framework was designed based on LR result. It will provide the experience and reasons for the next study and research.

CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

The research methodology describes and discusses the method of data gathering and analysis used in the study. It explains the type of research which will be conducted in this study. Some reasons and benefits of the research methodology selected will be discussed as well. In the study, some tools and materials will be introduced during the data collection and analysis phase. The research methodology focusses on providing the guideline and framework to launch the discovery and analysis about the topic selected.

In this study, the qualitative method will be used as the methodology. Utilizing a methodical approach known as research methodology, problems in research are solved by choosing the best and most efficient ways to carry out the study while adhering to its intended purpose and objectives. The qualitative method is used to comprehend people's attitudes, interactions, behaviours, and beliefs. It produces data that is not numerical. Researchers from several disciplines are paying more attention to the integration of qualitative research into intervention studies. The study will use interview to collect necessary data and analyse them to identify those factors influenced to ISF for CII.

3.2 RESEARCH DESIGN

This study will use qualitative method to extend the research by interview solution that will collect data and analyze these factors from SMEs in best practices. These methods will help address research objectives and questions. Factors and challenges related to research objectives and questions will be identified from two sides which are papers and practices from SMEs. The study will carry out four phases which are initial phase, development phase, practice phase, creation phase and summary phase as shown figure below.

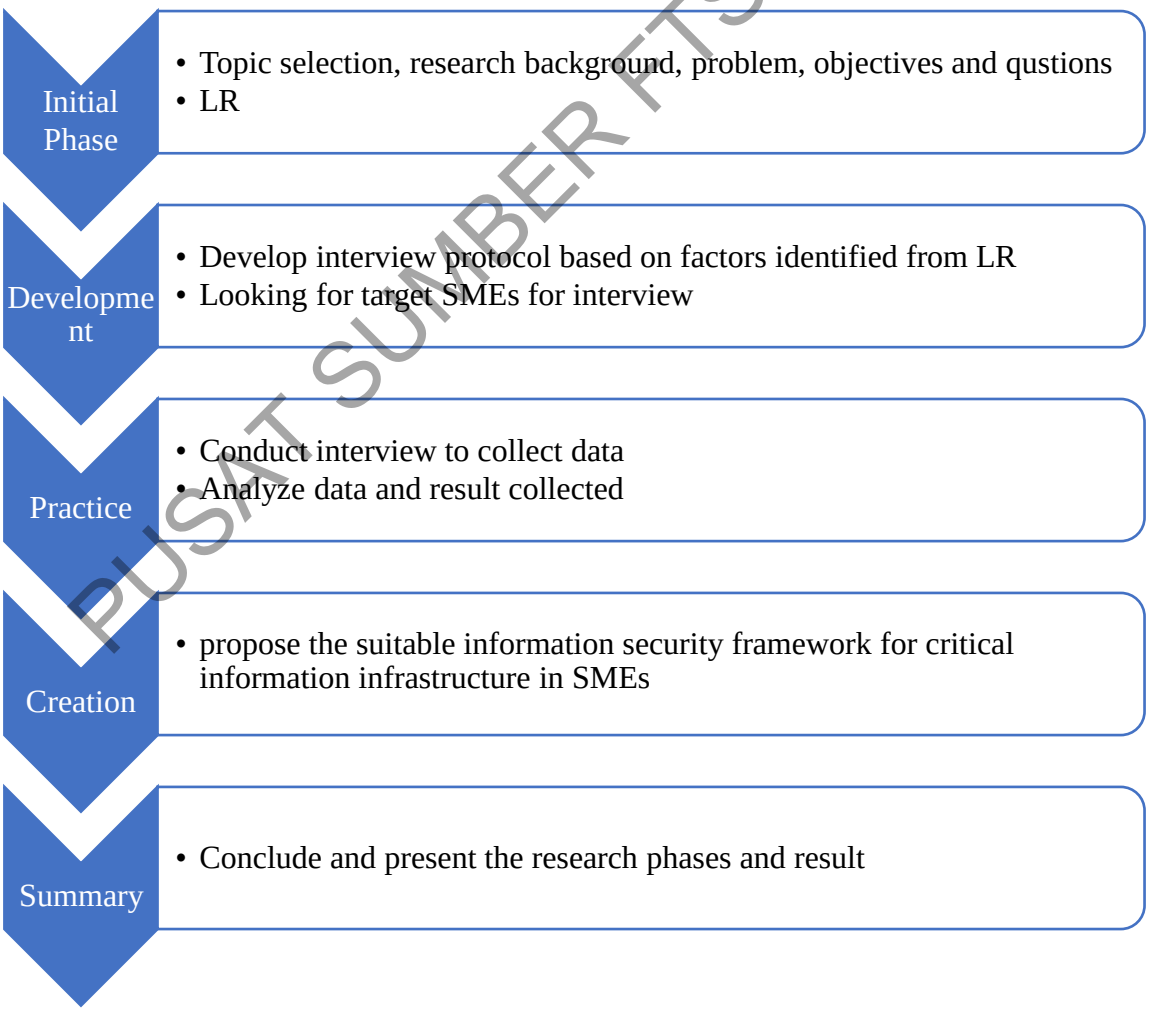

Figure 3.1 Research design phases.

The initial phase addresses the basic structure and trend for this study. Topic, research background, problem, objectives and questions are identified. LR launch the research from articles published, and it helps to identify factors and experience from papers. The development phase is to develop the further research based on factors and experience identified from papers. It will help develop the interview protocol and look for target SMEs so that the practice study can be proceeded successfully and smoothly. The practice phase will conduct interviews to selected SMEs. The data analysis will be preceded based on content and communication. This phase will help to identify factors and experience from actual practice. The creation phase is to develop the new ISF for CII in SMEs based on factors and experience identified from papers and practice. The last phase is summary. This phase will conclude and evaluate each phase and result, and it will forecast the future development based on the trend.

3.3 RESEARCH FROM PAPERS

Research from papers is the process to proceed with the study from articles published. Based on current cybersecurity environment, some hot topics are filtered and considered. Therefore, the topic of information security framework for critical infrastructure is selected. It is because the critical infrastructure is the root to support the work and business running in each company. As the development of technology, more and more enterprises tend to work and run business online. It means critical information infrastructure is playing the most significant role. Therefore, it is valuable and necessary to launch the further study in this aspect. A lot of articles related to the topic selected will be reviewed and analyzed. Some key structure and trend are addressed by first research from papers such as research background, problem, questions and objectives.

3.3.1 Search and Review Process

This paper will catch some key words to research and analyse, and only open source will be paid more attention. Google is the main search engine for this paper to do research. The search process is divided into five steps which are preparation, search, discuss and optimize and summarize. Each step will have different procedures to proceed with data collection and analyze. The search process implements to all research study in this paper including LR and other reference.

Figure 3.2 Steps of search and review process

1. Preparation

First step is preparation, some tools and devices will be prepared in this step. Based on the title, some keyworks or string will be prepared. Below keywords need to be searched:

a) Information Security Framework
b) Critical Infrastructure
c) Critical Information Infrastructure
d) Security Policies
e) Critical Infrastructure Protection

f) Challenges and Vulnerabilities of Critical Infrastructure/ Critical Information Infrastructure
g) Benefits of Information Security Framework for Critical Infrastructure
h) Cyber Attacks
i) Cybersecurity
j) SMEs
k) Security Awareness

Research resources will be from Google Scholar and UKM resources portal (eResources@ptsl). This paper will only focus on open-source due to limitation of finance.

2. Search

In this step, the search processes will be based on keywords or strings. The search engine is Google. The resource platform is Google Scholar and UKM resources portal. Regarding the search result, this paper will have some selections. Books, Journals, Report, and conference paper will be checked and reviewed. The year of published will be from 2005 to now. The reason is that old versions of reference will provide some experience. As an example, there are still a lot of vulnerabilities of critical infrastructure pending for fixing and optimizing. The latest reference will only focus on cyber issues. Based on the search result, the author will only focus on first ten pages. It is because the result of first 10 pages will be more accurate. These resources are from ScienceDirect, IEEE and university journals so on. There are not a lot of limitations on this part. It is because the author wants more result so that proceed with comparison to achieve more accurate result.

3. Review and Analyse

The author will use systematic review methodology to review those papers searched based on keywords. Some case study and statistics will be analyzed. The author will proceed with investigations based on the research issues and problems. The result will be applied to support the establishment of information security framework for critical infrastructure. Some factors influenced critical infrastructure such as nature disasters, human errors, cyber-attacks and dependencies will be analysed based on case study and statistics.

4. Discuss and Evaluation

In this step, some analyse results will be discuss and evaluate. Some opinions of those papers may not be suitable for current situation of companies and organizations, especially after IoT things and intelligent products are applied. As an example, the dependencies of critical infrastructure can be enhanced a lot. Companies can use IoT devices to monitor data of each sector of critical infrastructure, once some failure from single sector happened, the IoT devices can switch to alternate equipment. If the blackout happened, IoT will help switch to alternate electric generator. It will reduce the lost after some disasters happened. Moreover, as the technology development and trend, the author will give own opinions based on latest situation.

5. Summarize

The last step is to summarize discussion and optimization result. It is also the process of filtering. Some accurate and valuable points and content will be recorded and indicated on this paper. Moreover, the citation will be created based on the research result. Therefore, the final content may have similar opinions with journal searched. But the opinions optimized will be more suitable for companies and organizations, and it will create more benefits.

3.3.2 Criteria of Literature Selection

Not all literature will be reviewed, and the search results will be filtered. There are a lot of search results by keywords and strings. The author will check the and title and abstract to address the topic and direction of each literature. The author uses “find” function to review some content roughly by some keywords such as threats, vulnerability and challenges so on. It will be completed by “Ctrl and F” of keyboard from computer. This filtering progress will take around 3 minutes. Below are necessary criteria need to consider in literature selection:

1. Open source.
2. Contend related to the study.
3. Publish year between 2000 and 2022.
4. Writing in English.
5. Topics and study related to research questions of this paper.
6. Articles are published in professional academy platform not from website and blog so on.
7. Academic opinions are correct and clear.

Those literature need to satisfy these necessary criteria, and they are qualified to be selected and proceeded with detailed review and referred.

3.4 SEARCH RESULTS OF THE LR

Through the professional review processes, a lot of results are achieved. The study has reviewed papers and it focused on search results with Open Access and the PDF download option available. Keywords/strings search results are tabulated in the table below. For searching results, the study focuses on the first 10 search results’ pages because it will contain the most relevant search keywords/strings.

The research study obtains the results according to the key words listed in the preparation phase. The filter process includes two main parts which are filter function of the browser and manual filter. Some filter functions are used in the browser such as year and open access which are listing the criteria of the LR. The appendix B indicates the filter functions of search in the browser and databases.

The manual filter is to review all open access journals list in the first 10 pages of search pages simply. Since these journals will match to the research topics highly. The simple review is to review the abstract of papers and review specific paragraph according to keywords by "finding" function of searching. If the abstract and specific paragraph have enough content to match the topic searched, the journal will be selected to review detailly and extract valuable opinions and content. The table 3.1 shows the search results filtered by advanced search function of browsers and manual filter.

Table 3.1 Search result by keywords/strings.

Repository	Year	Search strings	Result	Category
IEEE	2000-2022	Threats/Vulnerabilities of critical infrastructure and critical information infrastructure, Information security framework for critical infrastructure or critical information infrastructure, ISF, critical information infrastructure protection, SMEs, challenges of implementing ISF for CII in SMEs.	56	Conferences, Journals, Magazines

to be continued…

… continuation

ScienceDirect	2000-2022	Threats/Vulnerabilities of critical infrastructure and critical information infrastructure, Information security framework for critical infrastructure or critical information infrastructure, ISF, critical information infrastructure protection, SMEs, challenges of implementing ISF for CII in SMEs.	32	Review articles, research articles, book chapters
Google Scholar	2000-2022	Threats/Vulnerabilities of critical infrastructure and critical information infrastructure, Information security framework for critical infrastructure or critical information infrastructure, ISF, critical information infrastructure protection, SMEs, challenges of implementing ISF for CII in SMEs.	12 6	Conferences, Journals, Magazines, review articles, book chapters, research articles

The result is filtered, and some open resource will be selected only. Filling in the gaps found in the literature and deepening our understanding of the subject are possible goals of future research. Implementing the findings into policy and practise: By emphasising best practises and evidence-based suggestions, the findings of the literature study could be utilised to guide policy and practise in the area of ISF for CII and implementation in SMEs. Continuously reviewing and updating the literature will be necessary to keep up with the most recent advancements in the area because the literature on ISF for CII is constantly changing. findings of a thorough literature study

on ISF for CII and implementation in SMEs can help to shape and direct future work in the subject.

3.5 INTERVIEW

The study selects the qualitative approach and uses interview to extend study and collect data. The interviews provided researchers with rich and detailed qualitative data on the participants' experiences, how they described them, and their understanding of them. Given the centrality of interviews in qualitative research, books and articles on conducting research interviews abound. These existing resources typically focus on fostering the conditions for quality interviews, such as access and participant selection (Castillo-Montoya, 2016). The interview will conduct on employee of SMEs. The study plans to select three or four SMEs and select three staffs from each SME to conduct interview. Some interview protocol and plans will be designed in further research.

The research study will select SMEs with non-technological industry such as food, education and so on. These companies have different drawbacks and vulnerabilities among information security, and they have more need on this aspect. Interviewee will be select from IT department, financial department and the leader or owner of SMEs. These interviewees have a lot of links with information security performance. The owner or leader of SMEs can decide all development trend and services deployment. It influences the enhancement of information security management directly. Staffs from financial department have clear and professional analysis about cost of information security management optimization. Leaders or owners will make decision based on these cost report from financial department. Staffs from IT department have clear and professional about information security management and services. These solutions will influence the business and work environment directly. Leaders or owners will refer to development strategy from IT

department and decide to invest to the enhancement of information security framework for critical infrastructure. SMEs have the owner or stakeholder as the core and decide all development and services deployment. Therefore, it is valuable to conduct the interview to these groups.

3.5.1 Design Interview Protocol

A protocol for an interview goes beyond a list of questions; it also covers the procedural aspects of interviewing and includes a script for what you will say prior to the interview, a script for what you will say after the interview, prompts for the interviewer to obtain informed consent, and prompts to remind the interviewer of the information they are hoping to gather. Interview protocols serve as a procedural manual for guiding a novice qualitative researcher through the interview process in addition to serving as a set of questions (Stacy A. Jacob, 2012).

The interview protocol of this study will include many phases which are preparation, design the script to open and close the interview, design informed consent collection, create interview questions, manage interview process and pilot test. Some phases will include some forms which will be designed by the author. These forms are using to collect relevant consent and answers.

3.5.2 Preparation

Preparation phase includes many parts which are company selection, design invitation mail, tools selection and so on. The first part is to select SMEs. These SMEs need to have relevant critical information infrastructure. They have capability to work and run business online. The study can search relevant and filter some companies online and record their contact information such as telephone number and email address so on. It is better to find some familiar companies and it will increase the rate of success to

conduct the interview. These companies will be some targets that friends or classmates who work or conduct internship before. After selecting relevant SMEs, the study will design the invitation mail to have their consent and join the interview.

1. SMEs and Interviewees Selection

The SME selection needs to follow the four main principles. The company is the small and midsized enterprise and its employees do not exceed 250. The industry the company running needs to satisfy the critical information infrastructure such as education, real estate, food, health and so on. The company agrees to join the interview and allow the study to publish the interview result and some private information. The company do not have adequate information security framework and management. These parts and situation can be obtained from the early call or emails of invitation.

The SMEs will be searched and invited from two methods. The first method is to search small and midsized enterprises related to education, real estate and food on the website. Some contact information are existing on the website of “contact us”. The second method is to contact to those companies which known people has worked or cooperated. The research study can be recommended by known people to these companies and the interview can be accepted highly.

The interview has three parts to three different roles in SMEs which are staffs from IT department, finance department and the owner of the company. Based on the plan, the interview will conduct to three employees of each company. The interview will conduct to three SMEs, and the total interviewees will be nine. The interviewee selection will be discussed with their companies. The selection needs to consider their working shift, availability, satisfying the research topic and consent of interviewee.

2. Design Invitation Mail

This mail will use to invite selected SMEs and achieve their consent to participant in the interview. Below is the mail content:

Subject: Interview invitation about the research study of information security framework for critical information infrastructure.

Greetings

Dear (relevant SMEs with specific contact person)

My name is ZHANG LULU, the student from the national university of Malaysia. I am preparing the final project for my master of cybersecurity. There is academic research about information security framework for critical information infrastructure in small and midsize enterprises. I would like to invite you to join the interview and discuss security issues and threats of your critical infrastructure and critical information infrastructure, current security framework implemented and challenges encountered.

This interview can help me to acquire the practice data about information security framework for critical information infrastructure. Meanwhile, we can exchange opinions to find solutions about threats and risks of critical information infrastructure and current security framework implemented in your company. This interview can conduct as online and offline. I am looking forward to having your response.

You can contact me by replying to this mail and my telephone number is +86 15952363793. If you have any questions, please do not hesitate to contact me.

Sincerely

Thank you.

Best Regards,

ZHANG LULU

3. Tools Selection

Some companies or employee may prefer to conduct this interview online. Thus, the interview will be conducted by Teams or Zoom meeting which are carry out remote conservation. The interview questions will be created by Google Form, and it can transfer to link and send to interviewee. They can review these questions and give basic answers. The pop out questions or opinions can be discussed based on these answers during the interview.

3.5.3 Script to Open and Close the Interview

Before starting the interview, the script will let people communicate all of the pertinent material regarding research study and the essentials of informed consent. Additionally, it will provide a place to wrap up the interview and provide the participant a chance to add any final views that haven't been covered. The participant's understanding of their rights as a participant in the study is aided by the information provided in the script, which also guarantees that our research will be conducted ethically.

1. Script to Open the Interview

Hello [interviewee name], My name is ZHANG LULU, the master student from The National University of Malaysia. Thank you for participating in this

interview. There is a research study in my project and the interview will help to identify threats and challenges from practice side. It will help to find solutions about those threats and challenges as well. The research title is Information security framework for critical infrastructure. It will discover and discuss more about critical information infrastructure. It will include the threats and risks of your critical infrastructure and critical information infrastructure. Challenges your company is encountering so on. You need to sign for the consent collection form since our interview will contain some information related to you and the company. Our interview will conduct for around 30 minutes and all questions are open-end questions, we can discuss and discover more. Let's start our interview.

2. Consent Collection Form

The consent collection form is designed to collect the consent of interviewee. It contains some rules and requirements which need interviewee and interviewer to sign. It means the interviewee agrees all rules and requirements and they will follow all rules. Below is the content of the consent collection form for each interviewee:

Consent Collection Form

I _____ voluntarily agree to participate in this interview and agree and follow these rules and requirements below:

- If you agree to join now, you can withdraw at any time or refuse to answer any questions without any consequences of any kind.
- You can withdraw permission to use data from the interview within one months after the interview, in which case the material will be deleted.
- You have had the purpose and nature of the study explained to you in writing and you have opportunity to ask questions about the study.
- Participation involves IT department, Finance department and leader or owner of the company.
- You will not benefit directly from participating in this interview.
- You agree to the interview being audio-recorded.
- All information You provided for this interview will be treated confidentially.
- In any report on the results of this interview your identity will remain anonymous. This will be done by changing your name and disguising any details of the interview which may reveal your identity or the identity of people I speak about.
- The disguised extracts from your interview may be quoted in dissertation and presentation.
- If you inform the researcher that yourself or someone else is at risk of harm they may have to report this to relevant authorities- they will discuss this with you first but may be required to report with or without your permission.
- You understand that signed consent forms and original audio recording will be retained in dissertation file stored in the interviewer and The National University of Malaysia.

to be continued...

...continuation

- You understand that under freedom of information legalization you are entitled to access the information you have provided at any time while it is in storage as specified above.
- You are free to contact any of the people involved in the interview to seek further clarification and information.

Interviewer Name: ZHANG LULU

Supervisor: Dr Umi Asma' Binti Mokhtar

Interviewer mail address: P117754@siswa.ukm.edu.my

Signature of research participant

---------- ----------

Signature of interviewee Date

Signature of Interviewer

I believe that interviewee is giving informed consent to participate in this interview.

---------- ----------

Signature of interviewer Date

Figure 3.3 Consent Collection Form

3. Script to Close the Interview

This interview is coming to the end. Thank you for making time to participant in this interview. I am grateful to discuss and discover these questions related to the research study. Your answers and opinions are valuable for the study to analyse and refer. I believe that your answers will help a lot in further study in information security framework for critical information infrastructure. If you have any questions, please do not hesitate to contact me. I wish all the best in your work and life. Have a nice day!

3.5.4 Create Interview Questions

Interview questions are designed based on research questions of this study. These questions are open-ended questions, and interviewee can give answers in different aspect. The study will use google form to create questions and these questions will be sent to interviewee. They can answer these questions before interview, and some other questions based on answers will be popped out. The study will discuss the answers and other questions to seek for solutions and correct opinions. Interview questions will be divided into three parts which are designing for staff in IT department, staff in Finance department and the owner or leader of the company.

The interview questions are extending from the three research questions of this research study. The answers and scope will satisfy the research objectives and the answers can provide the inspiration for the new information security framework development. The ideas and topics of interview questions are extracted from “threats and vulnerabilities of critical information infrastructure”, “drawbacks of current information security frameworks and management”, “limitations among their companies”. The interview to these departments can bring full understanding and insights about the information security issues of SMEs. This study launches this

research study and practice to collect abundant data and opinions from full aspects related to information security framework for critical information infrastructure. Below are interview questions designed:

1. Interview Questions – IT Department

a) What you are responsible for working in your company?

b) What threats and risks your critical infrastructure especially critical information infrastructure are encountering in your company?

c) What kind of danger or lost these threats and risk brought before in your company?

d) What will you do when these threats influence the security or business running in your company?

e) Do you have any specific cybersecurity team?

f) Does your company implement any information security framework to manage and maintain your critical infrastructure and critical information infrastructure?

g) Does your company purchase any services or tools to protect your critical information infrastructure?

h) Did your company have any incidents about critical infrastructure security?

i) In your opinion, is it necessary to develop an information framework for critical information infrastructure?

j) Based on your working experience and current situation of your company, what solutions need to develop to solve or reduce threats and risks to critical information infrastructure?

2. Interview Questions for Owners or Leaders of SMEs

a) What kind of business your company are conducting?

b) Do you understand any security issues for critical information infrastructure in your company?

c) How do you think about current critical information infrastructure protection and management in your company?

d) What kind of challenges your company is encountering in enhancing the critical information infrastructure protection and management?

e) Do you want to implement any new information security framework for critical information infrastructure?

f) What kind of factors you will consider if you want to implement any information security framework for critical information infrastructure in your company?

g) Do you have any deployment plan or arrangement for your IT or cybersecurity team?

h) What is your vision for the development of the business in your company?

i) How do you think about this interview conducting for discussing and discovering information security framework for critical information infrastructure?

j) After this interview, Will you pay more attention about security condition of critical information infrastructure in your company?

3. Interview Questions for Finance Department

a) What you are responsible for working in your company?

b) Do you understand critical infrastructure and critical information infrastructure in your company?

c) Do you provide powerful finance support with critical information infrastructure in your company?

d) Did your company encountered any security incidents related to critical information infrastructure, how much lost has your company suffered?

e) Do you think it takes a huge cost to implement some critical information infrastructure protection?

f) Do you think it is valuable to take some cost about critical information infrastructure protection?

g) Based on your working experience and current situation of your company, what kind of protection for critical information infrastructure is valuable to implement?

h) Does your company often provide you with relevant information security training?

i) Do you think you have relevant cyber security awareness?

j) In your position, what kind of security protection do you need?

Each interviewee will have ten questions to answer. They can give short answers for each question. The google form will collect their name, work content and email as well. It will be convenient to contact them and record their personal information. These questions will help the research study to collect practice experience in SMEs.

3.5.5 Manage Interview Process

The most important thing is to arrange this interview to certain that both interviewer and the interviewee block off plenty of uninterrupted time. With time blocked off, there will be no snafus. Make sure us allow more time than anticipate being required, clear our schedule, and turn off or set airplane mode for our mobile devices. I will use relevant devices to record the interview if necessary. Moreover, I will make this interview to be interesting by using some funny samples. The aim is to keep us focusing on discussing these questions and topic. I will also have genuine care, concern, and interest for the interviewee. It will help us to feel comfortable, and the interview will not be cabined. I will also use basic counselling skills to help interviewees feel heard. Many of the approaches used by the counselling profession are very helpful to qualitative researchers when they interact with their respondents. The counselling profession is continuously thinking about how to become better listeners who can assist clients express their stories.

When you pose open-ended questions, your hope is that the respondent will take advantage of the chance to share in-depth qualitative information about their experiences and viewpoints with you. Participants, however, occasionally require instructions to get them moving. Consider what cues you might use to assist someone in responding to each of your open-ended questions (Jacob, 2012). In this interview, I will use proper prompts to guide interviewee to find correct answers. It is because some interviewees are from finance department, and they may not understand relevant knowledge about information security and critical information infrastructure so on.

3.5.6 Pilot Test

The study will determine whether the interview questions make sense by pilot testing the interview protocol. I will familiarize myself with the questions' sequence and flow during the pilot testing process, which will make me feel more at ease when I start conducting interviews for the data gathering. I will test this interview protocol and process with classmates or friends to collect experience and drawbacks. Pilot testing phase will test all questions and forecast the things happened during the interview.

3.6 INTERVIEW RESULT ANALYSIS METHOD

The data analysis approach of interview result is content analysis. This research study counts the number of times concepts or keywords appear to deduce meaning. The content analysis will use some themes to filter the interview result from the original transcript. The answers and interview questions will be classified according to research objectives and questions.

The theme is the first phase to filter the analysis result, and the count of keywords will determine the next analysis output. The second phase to filter the analysis result is according to numbers of keywords among the answers. If answers

from different interviewees cover the same result, this result will be the final conclusion of the interview output. The interview questions ask about the threats and vulnerabilities of critical information infrastructure encountering in their companies. If most interviewees agree and answer cyberattacks, the popular and critical threat will be cyberattacks.

3.7 SUMMARY

In this chapter, the methodology of research study on papers and practice are introduced. Some search process and literature selection criteria are discussed, and LR was used to review papers and find relevant factors related to research questions. Regarding practice data collection, the interview is selected as the methodology. The interview targets are staffs from SMEs, and the interview protocol is designed. The consent collection form needs both interviewer and interviewees to sign and agree to all rules. The interview data will be used for this research study, and they will be used by the interviewer and UKM. The interview result analysis method is content analysis, and it follows themes and count of keywords among answers. The interview data will be stored in the interviewer and UKM as well. The interview aims to fulfil the research factors and requirements discussed in chapter two, and it will define those opinions from real practice. It indicates the real situation and challenges from SMEs. It is valuable to push this research study forward to the correct future.

CHAPTER IV

RESULTS AND DISCUSSION

4.1 INTRODUCTION

In this chapter, The result of interview to SMEs will be presented as well. Three main parts will be extended which are presenting data, analysing data collected from SMEs by interview and concluding analysis result. In the part of presenting data, some screenshot and document scanned will be indicated such as interview progress, consent collection form feedback, feedback of interview questions and so on. In the part of discussing data, some analysis methods will be used to analyse those data collected. Since the interview will collect more accurate data with high quality, rather than questionnaire so on, it pays more attention on the quality of data rather than quantity. Therefore, the study is using inductive methods to analyse data and the thematic content analysis will be the approach to find out significant factors related to research questions and research objectives.

An organized process for examining qualitative data, the inductive approach is likely to be directed by specified evaluation goals. Inductive analysis refers to methods where concepts, themes, or models are derived from extensive readings of the raw data by an analyst or researcher (Thomas, 2006). In order to reveal key study topics, thematic content analysis was used to determine the diverse intellectual viewpoints that underlie consumer experience. Unlike earlier work, which employed quantitative methods to bibliometric analysis (García-Lillo, 2016). This chapter will

analyse and find factors based on the interview content and answers from interview questions.

4.2 PRESENTING DATA OF INTERVIEW

The data of interview are divided into three parts which are interview for owners of SMEs, finance department and IT department. This research study has conducted interviews for three companies, and they are doing different business. These data are collecting from google form and note of interview. Based on answers of interviews, some other questions popped out during the interview. Appendix C are consent forms signed by all interviewees and allow this research study to publish interview answers. Tables in appendix D indicate the interview transcript extracted from the interview note, and all data are not changed. These data are expressed by interviewee directly.

If interviewees do not undertand relevant topics and knowledge of information secuirty, the interviewer explained critical inforamtion infrastructure and relevant topics to interviewee. The SMEs interviewed have diffreent industry which are real estate, education, and education. These industry belong to sectors of criticla information infrastructure. The interviews aim to collect accurate data from different perspectives and insights. There are total nine interviewees joined the interview. Theses interviewees satisfy the research topic, they are available and free to join, their managers agree their attendance.

4.3 DISCUSSING AND ANALYZING THE INTERVIEW RESULT

The analysis methodology of analysing the interview result is content analysis. Based on the interview content, this study analyses the content during the communication and extract valuable data from these content. All content is divided into three main themes to discuss and analyse based on research objectives and questions. All

interview data from different departments and companies have specific opinions and consequences related to research questions. The themes are threats and vulnerabilities of critical information infrastructure among SMEs, drawbacks of current information security framework or management existing in these SMEs and challenges and limitations in theses SMEs interviewed. There are some sub-themes including in these main themes which are factors affecting information security.

4.3.1 Characteristics of Interviewees

This interview conducts to different staffs in different companies, and the aim is to collect accurate data. However, the interviewees have many different characteristics. In total, nine participants joined the interview, and 67% interviewees do not have relevant information security knowledge and security awareness. There is no information security expertise join the interview. The analysis result is extracted from the interview answers of interviewees.

Interview Questions: Do you understand any security issues for critical information infrastructure in your company?

Answers: “Maybe our PCs, printers, systems.”, “Understanding few of them, attacks by hackers, and some devices are broken by relevant activities.”, “ I do not understand, this part is responsible for IT department.”

Interview Questions: Do you understand critical infrastructure and critical information infrastructure in your company?

Answers: “I do not understand, maybe PS and so on.” , “Not very clear.”, “No, my working experience and education background are related to finance.”.

4.3.2 Current Security Situations in SMEs Interviewed

Currently, most SMEs are having some incidents about cybersecurity, and these incidents have brought the damage and loss to companies. Different companies have different incidents, and these incidents are caused by human errors and cyber-attacks.

Interview question: Did your company encounter any security incidents related to critical information infrastructure, how about your loss?

Answers: “We had relevant incidents before, we spent some money fixing the devices.”. “We lost some information of customers.”. “Yep, we lost some money, and we have to buy new devices.”

Interview question: What kind of danger or loss threats and risk brought in your company?

Answers: “Lose customers’ data, money, reputation value.”. “Finally, it will direct and indirect to cause finance issues, the reputation of company will be influenced as well.”. “Financial loss, business disruption.”.

4.3.3 Threats and Vulnerabilities of Critical Information Infrastructure

During the interview, the research study has full understanding about the work environment and background. Some factors and limitations existing in SMEs discussed during the interview. The analysis approach is content analysis, and all analysis results are summarized according to interview content. Cyber-attack is one threat existing in the critical information infrastructure, and a lot of companies are suffering from this threat. This threat is proved by interviewees’ answers.

What threats and risks your critical infrastructure, especially critical information infrastructure is encountering in your company?

Answers: “Phishing, data leakage, human errors.” “Cyberattacks, Insider threats, data breaches, and so on.” Cyberattacks, data breaches, nature disasters”.

“But we encountered phishing before. The company does not buy any specific security products to defend against phishing.”

“Human error always be popular threat which influences different industries. Human errors always cause damage of these devices, and these data may be lost or break. Humans are the core of the company. Some phishing and virus influence are indirect caused by human errors as well.”

Those answers have mentioned relevant threats and vulnerabilities in companies. All interviewees from three departments and companies have discussed the threats and vulnerabilities in their company during the interview. Below table is the analysis details based on the interview content of three departments.

Table 4.1 Analysis of interview result about threats and vulnerabilities of critical information infrastructure.

Source	Threats and vulnerabilities	Remark	Factors Considered in Development of Cybersecurity
Owners or leaders of SMEs	Cyber-attacks, human factors	The owner cannot understand and analyse full threats and vulnerabilities due to limited knowledge in information security and lack of security awareness. But they want to implement necessary services to reduce threats and incidents.	Business need, cost, rate of return, development trend.
Finance Department	Human factors	Due to limited security knowledge and awareness, staffs cannot recognize the consequences and urgency.	Business need, budget limitation, attitude of owners or leaders.
IT Department	Cyber-attacks, phishing, human errors, insider threats, data breaches, nature disasters	Have abundant knowledge of cybersecurity and security awareness, they need expertise and guidance to create the holistic solutions.	Business need, security function, vulnerabilities existing, urgency of threats.

4.3.4 Drawbacks of Current Information Security Framework or Management

During the interview, some drawbacks and weaknesses of current information security management were discussed. These issues will cause relevant incidents, and these companies interviewed are keeping enhancing and optimizing the information security management from full perspectives. There are a lot of answers from interviewees identifying these drawbacks.

1. Lack of Professional Team

Do you have any specific cybersecurity team?

"We have some staffs to solve issues, but the team is not strong", "Yes, we have the team, but our cybersecurity team only have few members.", We do not have specific cybersecurity team.".

2. High Cost

"We do reject some projects, although these projects will bring better result. But the cost is very high. After discussion, we may reject those projects that may cause some finance risks. We are growing solwly.".

3. Inadquate Management

"The management and investment on security protection are inadequate. The management include some security policies and training are not enough. The company is developing, and some weaknesses are optimizing. The investment includes security products, services and employees. The company has budget limitation, and we cannot buy enough security products and services and establish the powerful platform to detect, identify, respond, recover and monitor. Moreover, the company does not hire

enough IT staffs and establish specific team do be responsible for each branch of cybersecurity. Normally, one staff has to be responsible for serval duties and most staffs are not experts and many IT staffs are growing slowly due to lack of relevant training and guideline.".

The above answers indicate relevant drawbacks of current information security framework and management among companies. It is because the cost is very high, the finance department has rejected some projects about optimizing information security framework. Table 4.14 summarizes the analysis result.

Table 4.2 Analysis of interview result about drawbacks of current information security framework or management.

	Drawbacks of current information security management	**Root causes of weakness**	**Attitude to Security Deployment**
Owners or leaders of SMEs	Lack of expertise and professional staffs. Have many gaps existing current working environment	Lack of security knowledge and awareness	Agree to pay more attention on better security services deployment and accept more security awareness training.
Finance Department	High cost	Limited budget	Accept more security knowledge and training, detailed security services deployment needs to be decided by leaders and stakeholders.

to be continued…

…continuation

IT Department	Lack of professional guidance, the management is not holistic. Lack of useful tools and security products due to limited budget.	Limited security knowledge and awareness. The security team is not very powerful. Limited budget	Hiring more professional staffs and purchase necessary tools and security products. Implement relevant security framework guidance.

4.3.5 Challenges and Limitations of SMEs

According to the interview content, a lot of challenges and limitations are mentioned in these companies. Most SMEs have same challenges, and these challenges bring lots of trouble and limit the business development.

1. Limited Budget

Do you provide powerful finance support with critical information infrastructure protection in your company?

Answers: “No we do not provide a loft of finance support”. “No, we have very limited budget for this part”. “Based on our need and decisions from boss, it is not powerful enough.”.

2. Low Security Awareness

Does your company often provide you with relevant information security training?

Answers: “No, we signed some agreement about devices and internet usage before, but the company did not explain them detailly.”. No, that is why we had some incidents, most staffs do not have security knowledge and awareness.”. Not often, most staffs will ignore these training.”.

Do you think you have relevant cyber security awareness?

Answers: “I do not have, some of my colleagues do not have these as well.”. “No, I do not have, but I am willing to learn some.”. Nope, I will learn some knowledge from our IT department when they provide training.”.

3. Low Capability

“We are optimizing security protection, and we are implementing some services and tools, but we do not have adequate capabilities to satisfy relevant deployment and we have limited budget.”. “We do not have employees with great practices and knowledge in this aspect, we do not have enough finance support to buy services and tools.”

4. Weak Security Team

“My employee does not have enough skill and knowledge to guide the protection, economics burden and so on.”.

Above interviewee answers indicate some challenges of SMEs, and these challenges will limit the security development. Below table is the analysis about the interview data.

Table 4.3 Analysis of interview result about challenges of SMEs

	Challenges and limitations identified	**Attitude to ISF for CII Deployment**	**Factors Considered in Security Service Deployment**
Owners or leaders of SMEs	Budget limitation, security team is not strong, staffs do not have enough security awareness.	Agree to optimize and implement suitable ISF for CII in the company.	Business need, cost, decision of top managers and leaders.
Finance Department	Limited budget, non-technology staffs do not have enough security awareness	Agree to implement relevant services and security products to optimize and customize the ISF for CII in the company.	Business need, budget limitation, development trend, decision of leaders and stakeholders.
IT Department	Budget limitation, low capability, Limited support of top leaders, other staffs have limited security awareness.	Accept to implement better ISF for CII and enhance the security governance by applying necessary products and services.	Business need, cost, capabilities of current infrastructure.

4.4 SUMMARIZING ANALYSIS RESULT OF INTERVIEW

The interview analysis result has high similarities with literature review result. Based on the interview, these companies have the owner or leader as the core. All decisions and development plans need to be approved by owners or shareholders. Moreover, three owners answer that they do not have relevant cybersecurity knowledge and awareness. Therefore, most owners do not have enough cybersecurity knowledge and awareness, and their decisions about security services deployment may be influenced by these factors. All staffs from finance departments and owners of the companies mentioned that their companies have budget limitations and low capabilities, and their existing equipment and services cannot support the better security products to apply. These companies do not have powerful and specific cybersecurity teams to handle relevant security issues as well. Most employees in these companies do not have enough security awareness training.

These companies have some threats such as cybersecurity, human errors, nature disasters and so on. Phishing, virus, malware, and data leakage are some main cybersecurity threats existing in the company. Three staffs from IT department of each company answer that cyberattack is the popular threat among their company. These SMEs consider the cyber-attack is the critical threat. Most IT staffs agree that human factors are the main root cause for incidents happened in their companies. These companies are keep optimizing their information security management to resolve security issues, and they are willing to have better information security framework for critical information infrastructure to help to establish the better management, monitoring, identification, response and recovery system and framework.

These SMEs interviewed have similar weakness of current information security framework and management. Based on the result from nine interviewees, all of them agree that they do not have powerful team and they do not have clear

guidance and SOP to follow. Some frameworks and method methods are taking the high cost. These SMEs have similar challenges and limitations. All of them are having limited budget and low capabilities. Most staffs from different departments do not have enough security awareness such as finance department. It will increase the human errors.

4.5 SUMMARY

In this chapter, the data presenting and analysis are carried out from LR and interview. A lot of journals related to the study are reviewed and some valuable data are extracted from papers. These data are analysed and evaluate critically. Some threats and vulnerabilities, drawbacks of existing security frameworks, limitations of SMEs are identified from journals. This study conducts the interviews to three SMEs with different industry. Three staffs from each company are selected to join the interview and answer questions. All questions and answers popped out are presenting through reorganization and optimization based on note of interview. During the interview, the study understand more about the background, work process, development opinions and so on. It helps the study to accumulate experience. Both SLA and interview helps the study find relevant factors related to development trend of ISF for CII in SMEs.

CHAPTER V

INFORMATION SECURITY FRAMEWORK FOR CRITICAL INFORMATION INFRASTRUCTURE IN SME

5.1 INTRODUCTION

This chapter focuses on proposing the new information security framework for critical information infrastructure in SMEs. It is suitable to all SMES especially for companies with non-technology industry such as food, education, real estate and so on. This chapter is the extension and final objective of chapter II and chapter IV. Chapter II and chapter IV collected a lot of factors related to development of the new framework and provided the clear guideline from papers and practice. When developing the new framework, the research study considers these factors and solves those issues identified. Literature review and interview provide the current background and limitations of SMEs, the new framework will overcome the limitations and challenges of SMEs.

In this chapter, several sections will be discussed including the aim and objectives of this framework, framework presenting, sectors discussion and so on. The new framework is inspired by conceptual framework and existing information security framework and management. It will follow the principles of CIA and business continuity, and it will discuss more details about critical sectors such as risk assessment, data recovery and so on.

5.2 FRAMEWORK DEVELOPMENT AND DESIGN

This framework will consider more factors influenced to SMEs and it provides some optional service deployment based on business need and development trend of companies. The framework provides the general guidelines and necessary critical information infrastructure protection, each SME needs to customize the framework to fit the specific needs and resources or current capabilities in the company. Review and update the framework as necessary as new threats and technologies appear.

5.2.1 Framework Development Aim

The aim of this information security framework is to guide SMEs to customize own suitable information security framework according to this framework proposed.

5.2.2 Framework Development Objectives

1. Guiding SMEs to develop their own processes about identifying threats and vulnerabilities among the company.
2. Guiding SMEs to implement suitable sources and services by their own conditions.
3. Guiding SMEs to develop relevant acceptance of security criteria.

5.2.3 Factors Considered About Framework Development

The first part needs to consider is critical threat existing SMEs. The threats identified from literature review and interview are nature disasters, cyber-attacks, human errors, dependencies and so on. The security framework will reduce these threats. According to the final result of literature review and interview, cyber-attack is the critical threat and phishing is most popular attack method. This framework will focus on solve these critical threats.

The second part needs to consider is the drawback or weakness of current information security framework and management in companies. The drawback identified from literature review and interview are high cost, unsatisfied current work environment, unsatisfied security controls and so on. The third part needs to consider is the challenge of SMEs. The critical challenges and limitations of SMEs identified from literature review and interview are budget limitations, low capabilities, lack of information security expertise, lack of security awareness, Owners or leaders lack of professional vision about security service deployment and so on. The framework will implement optional service or tools to solve and reduce these drawbacks. The core limitation is budget limitation; therefore, the framework will be implemented with low cost.

5.3 INFORMATION SECURITY FRAMEWORK FOR CRITICAL INFORMATION INFRASTRUCTURE

This security framework is intended to help SMEs safeguard their critical information infrastructure against risks and threats. It should be tailored to the unique requirements and operating scope of each SME and adhere to the necessary information security standards and laws. Below figure is a flexible framework which can be implemented to different SMEs with different industry.

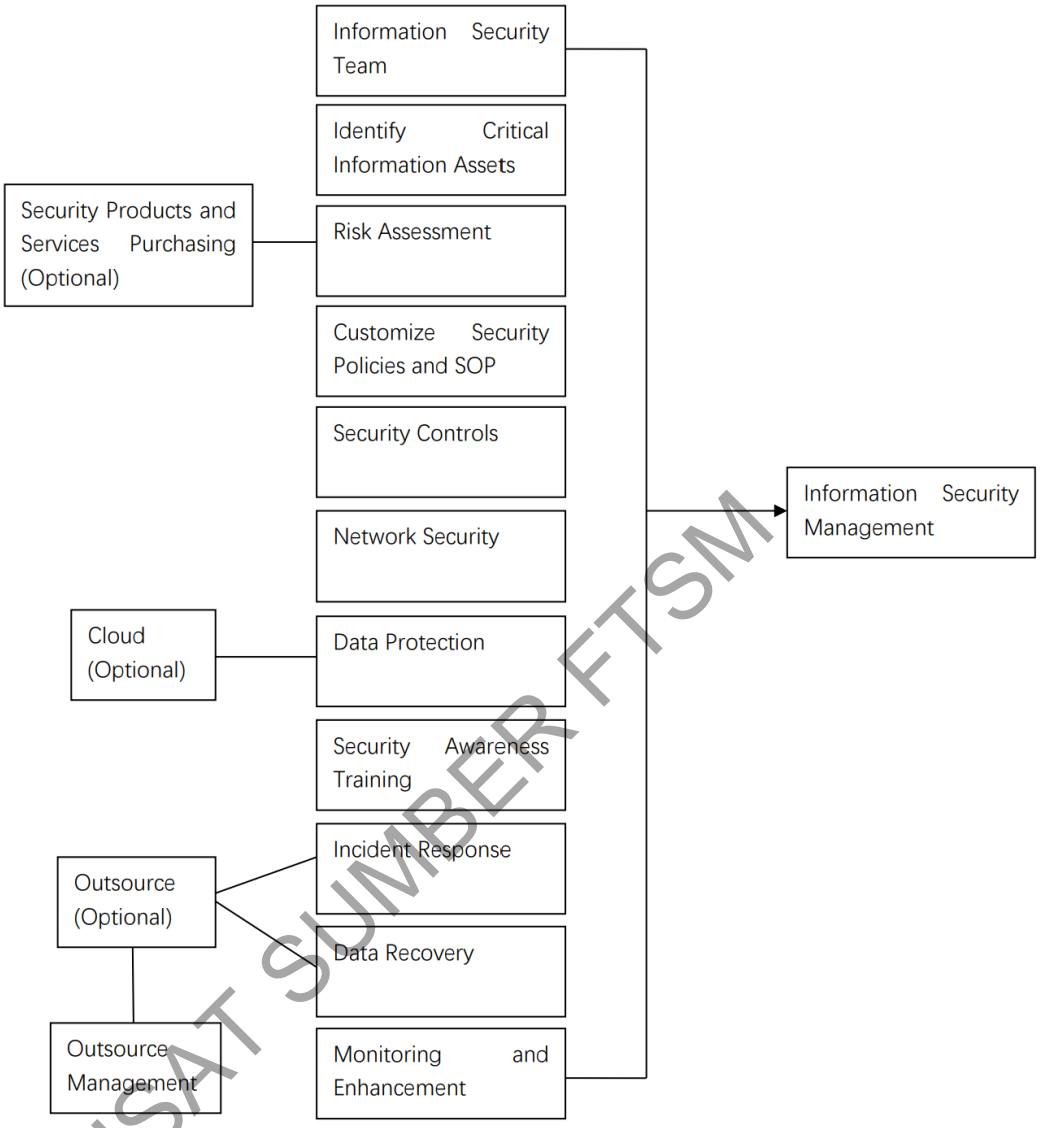

Figure 5.1 Information security framework for critical information infrastructure in SMEs

This framework allows SMEs to outsource relevant services to increase the information security management. Some SMEs may have limited budget and low capabilities, and these limitations cannot satisfy specific security services and products deployment. Outsourcing is one selection. Cost control, financial considerations (such as a lack of funding for internal development), improved management information systems (MIS) control, access to technology, and strategic focus (i.e., the ability of the organization to concentrate on its plan) are all advantages.

Cost management is a crucial benefit for SMEs because it would enable them to better balance their budgets and avoid making a significant investment in an IT department. However, the study also discovered a drawback to outsourcing. Coordination costs (i.e., coordinating internal IT with the outsourced vendor), a lack of flexibility and control, and staff upheaval are the identified disadvantages. Coordination expenses can be a trap for SMEs since, if they become too high, they may endanger their very existence (Velinov, 2021). Since most SMEs has budget limitations and low capabilities, companies can customize suitable solutions between outsourcing and insourcing.

5.3.1 Assemble the Information Security Team

The company needs to assemble the specific information security team to handle all issues. It is necessary to hire one expertise or professional staff to guide and lead the team. Although, it will take some cost due high salary, but the expertise can make effort and provide training and guideline with other staffs. The team leader needs to analyse each team member and offer members with specific role and responsibilities. The clear structure and authorization of the information security team need to present to owner of the company. A powerful and scientific team can make all processes to be visible and scientific.

5.3.2 Identify Critical Information Assets

Start by determining which SMEs have the most important information assets. This includes confidential client information, proprietary information, financial data, and any other data that is essential to the running of the business. The specific information security team member needs to manage these assets and define the capability of the security infrastructure. It helps the company determine the further service and defence deployment and necessary security products purchasing. Moreover, it is critical to

manage and monitor the status of these critical information assets, once any assets are out of service, it must follow SOP to recover the service soon.

5.3.3 Risk Assessment

After Identifying the organization's crucial resources and infrastructure, the team needs to analyse potential risks, weaknesses, and threats related to each asset. Moreover, the team needs to prioritize the risk based on their likelihood and potential impact. To find potential threats and weaknesses that could jeopardize the security of the important information assets, do a thorough risk assessment. Prioritize security measures by assessing the likelihood and potential effect of these hazards. Information security risk can be expressed as the impact of uncertainty on information security objectives. In the context of information risk management, risk assessment helps organizations assess and manage events that may harm your sensitive data. Risk assessment includes risk identification, risk analysis and risk evaluation. Each phase will have relevant value of potential risk, and all value will be calculated to indicate the accurate result which the organization can accept or reject.

A lot of different risk assessment methodologies we can applied in our assessment, and it depends on the different organizations based on different situations and background. There are many attributes we need to consider when the organization select suitable methodology. Some significant attributes such as background of organization, scope of business, scale of organization and cost etc. A risk assessment methodology needs to contain following:

1. Criteria for determining risks and accepting risks.
2. Repeated risk assessments produce consistent, valid, and comparable results.
3. Activities for identifying risks.
4. Activities for analyzing risks.

5. Activities for evaluating risks.

Many pertinent aspects and assets will take into account criteria for calculating risks. Confidentiality, integrity, availability, likelihood, and business impact should all be added up to determine risk level. Each company can customize own criteria for accepting risks. Below table is the sample of criteria.

Table 5.1 Criteria of accepting risks for SMEs.

Value	**Risk level**	**Decision**
1-5	Low risk	Accept
6-9	Medium risk	Treat
10-15	High risk	Treat risk

Total value of this criteria is 15, and this criterion is separated as three phases which are 1 to 5, 6 to 9, and 10 to 15. The total value will be calculated by confidentiality plus integrity and plus availability and plus likelihood and plus business impact. The formula is following:

Risk level = C+I+A+L+BI.

The company need to make the standard about their acceptance of confidentiality, integrity, availability, likelihood and business impact. Below table is the sample for SMEs to follow. The company can customize the acceptance content for confidentiality, integrity, availability, likelihood and business impact. In the table, x means customization content by each SME.

Table 5.2 Value of C.I.A.L.BI.

Value	Description	Confidentiality(C)	Integrity(I)	Availability (A)	Likelihood (L)	Business Impact (BI)
1	Low	x	x	x	x	x
2	Medium	x	x	x	x	x
3	High	x	x	x	x	x

Risk identification is the process of seeking, recognizing, and recording risks. Risk identification will help to obtain the condition and factors affecting to SME's security objectives. It is the process of identifying positive or negative consequence to the applications objective in a methodical way. (Arun, 2017). The company can create their risk identification standard, and the criteria need to include relevant sectors such as asset identified, location, belongings, purpose and business function and so on. The analyse method can be complete by scores calculation as well, each asset can be given specific score based on confidentiality, integrity, availability, likelihood and business impact. The risk identification result can be justified by total value or scores.

Risk evaluation is the process of comparing an estimated risk with a given risk criterion to determine the significance of the risk. Risk evaluations need to compare the value of risk analysis with the risk assessment methodology so that each SME can achieve the final result which part is high risk.

The foundation of risk management and cybersecurity are information security measures. The business requirements and related security requirements should be taken into consideration while choosing the security measures. Each SME will give security measures for each asset indicated a priority based on risk identification,

analysis, and evaluation. Therefore, relevant information security controls can be taken by the result of risk assessment.

In the phase of risk assessment, the company can purchase necessary security products or services based on business need and top risk. Security products and services are one security control or solution. However, some SMEs may have budget limitation, and these companies may outsource or use management and policies measure to reduce the risks. This phase provides many optional measures for SMEs to choose according to different business need and budget.

5.3.4 Customize Security Policies and SOP

Create a comprehensive set of security rules and procedures that set out standards and best practices for securing the vital information infrastructure. Access restrictions, data classification, incident response, and encryption standards should all be covered. The company need to customize the security policies to limit and manage the behaviours of employee, business extension, security management and so on. Each SME can keep optimizing policies based on risk identified and vulnerabilities. In addition, standard operation procedure (SOP) needs to be designed based on risk and threats. Once any incidents happened, the company can follow the SOP to solve issues and resume relevant business function.

5.3.5 Security Controls

Based on the identified risks and security policies, SMEs need to implement the necessary security controls. This could include secure authentication techniques, firewall setups, and intrusion detection systems. The company needs to enforce the least privilege principle by allowing users only the access necessary to perform their job duties. Review and update user access rights and permissions on a regular basis.

This part needs to follow all principles of confidentiality. SMEs can purchase suitable security products and service to implement security controls based on budget, business need and development trend.

5.3.6 Network Security

SMEs need to protect the network perimeter by putting in place firewalls, intrusion detection systems, and intrusion prevention systems. To safeguard data while it is in transit, use secure network protocols (such HTTPS and VPN). To fix vulnerabilities, patch and update network hardware and software frequently. This part may need to purchase many security products and services such as proxy, WAF and so on. SMEs need to manage network security based on self-situation.

5.3.7 Data Protection

SMES need to secure sensitive data both in transit and at rest. For company continuity, implement data backup and recovery strategies. The company needs to create policies for data retention and enforce them to meet statutory and regulatory requirements. For some SMEs with education and media industry, data is the most valuable, and these companies make business based on data. Therefore, data protection is very critical for these SMEs. Data protection include data storage and back-up. As the development of cloud services, more companies are willing to save data into cloud. In this framework, the research study advises to save data into cloud and back-up in physic devices such as mobile hard disk as well. Once any incidents happened, these companies can find data resume business from full platforms both cloud and physic devices. Especially for nature disasters, it helps to find data and recover business better.

5.3.8 Security Awareness Training

By providing training, instructional materials, and emphasis on security procedures in daily activities, SMEs can increase the understanding of information security among their personnel. To increase information security vigilance, this also includes incident reporting, spotting phishing attempts, and other preventive actions. By offering frequent training sessions and awareness initiatives, you may help your staff develop a culture of security awareness. Inform them of typical dangers, social engineering strategies, and the significance of following security policies and procedures.

According to literature review and interview, phishing is becoming more popular and it brought a lot of damage and incidents as well. The economic core of the solution to reduce phishing is human. Human is the trusted protection and human will connect to all information transmission. Human is very important among email security. If people have enough email security awareness, the email environment will be safer. Security awareness include a lot of different aspects, and enterprises and people need to pay more attention. Security awareness will help avoid more and more future attacks, and people will manage their behaviours better. Moreover, the security awareness training needs to provide basic security knowledge with employee. Employee need to understand the some causes of cyber-attacks and employee will be sensitive when cause potential data leakage. In SMEs, the information security team can schedule specific online training and prepare necessary documents as well. The company can set reward and punishment policy, and human will impress some mistakes by punishment, and it helps increase the security awareness.

5.3.9 Incident Response

SMEs need to create a security incident response strategy that outlines the actions to be taken, and companies need to create an incident response team with specific duties

for containment, investigation, and recovery. The company needs to test and revise the incident response strategy frequently in light of lessons learnt. Organizations use many setups to carry out their IR role. In small to medium-sized businesses, IR may be carried out by the IT manager, a small group of people selected from the IT unit, or even by outside contractors. event response teams (IRTs) in small to medium sized enterprises typically develop ad hoc and reactively as soon as the event is discovered, mostly due to resource limitations (Ahmad, 2021).

The company needs to assemble one IR team from IT department or information security team. IR team is responsible for handle incidents and find root cause. There are many objectives of IR such as protect life and prevent injuries, protect the environment, mitigate the damages. Contain and control the crisis and so on. The IR team need to define level of crisis and proceed with specific processes based on minor and major crisis. The IR team needs to take relevant actions in three phases of incident response which are pre-strike phase(before), strike phase(during) and post-strike phase(after). Each SME can customize own incident response processes according to different crisis and business requirements. Below five steps are sample of incident response. In preparation step, IR team needs to make the plan, get commitment from senior management, prepare detailed incident management scheme, prepare necessary tools and so on. IR team analyses the events and determine the type, nature, and scope of an incident once it has been recognized. The next step is to stop the incident from harming the company anymore. When a high severity incident occurs, this phase can entail shutting down mission-critical systems. The IR team must locate and eliminate the incident's primary cause (such as malware in corporate networks and systems) in order to eradicate it. During the monitoring step, IR team needs to monitor the status of business running. The last step is report and enhancement. IR team needs to report the vulnerability and root cause. Some solutions or patches need to be justified by IR team.

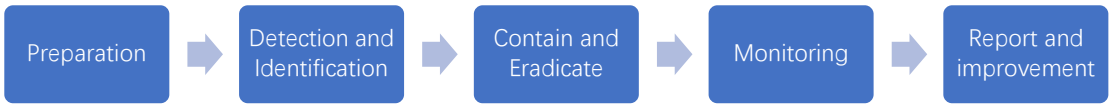

Figure 5.2 Incident Response Steps.

Due to budget limitation, some SMEs may not have specific IR team and platform to proceed with incidents handling and response. These SMEs can outsource this part to other specific company. It helps SMEs to save cost and increase the security since SMEs are seldom attacked due to less value.

5.3.10 Data Recovery

Normally, data recovery is linked with incident response. However, it is different to proceed with SMEs. Some data may not be valuable for companies. For SMEs in real estate or property industry, the incidents will cause the data loss or damage about properties. The company will not recover these data due high cost, and the company can remeasure the parameters of properties. It will reduce the cost about data recovery, and the recovery can proceed with relevant business need and requirement.

During the recovery phase, SMEs need to define interdependencies, recovery point objective (RPO), recovery time objective (RTO) and minimum operations resources (MOR). Interdependence is the identification of any interdependent activities, assets, support infrastructure, or resources that require ongoing maintenance or recovery time. Specific interdependencies that exist in business networks influence the outcomes of business relationships (Per Vagn Freytag, 2017) Dependencies is one vulnerability of critical information infrastructure. If one sector is damaged, it will influence other sectors and cause huge damage. The recovery phase needs to define the independencies between each sector and finds best solutions.

Recovery point objective (RPO) defines the maximum acceptable loss of data that a business process can withstand in a single application before being severely impacted (Josef Krahulec, Business impact analysis in the process of business continuity management, 2015). Recovery time objective (RTO) is the time in which a business process and its associated applications must be functional again after an outage event. Minimum Operating Resources (MOR) are the minimum resources (people, facilities, systems and data) required for the resumption of the business functions at the recovery centre (MS 1970:2007 , 2018). Below table is the sample for RPO and RTO, SMEs can customize own criteria based on business need.

Table 5.3 RTO & RPO criteria matrix for SMEs.

Critical Level	**RPO**	**RTO**
Very high	Immediately	Within 1 hour
High	4 hours	Within 2 hours
Medium	24 hours	Within 24 hours
Low	5 days	Within 120 hours

MOR requires SMEs to define the existing resources and business function, and certain the company can use these resources and recover necessary business function. However, data recovery also can outsource depending on business requirements and budget.

5.3.11 Monitoring and Enhancement

The information security team needs to monitor all status of critical information infrastructure, some solutions and actions can be taken based on relevant risks and threats. During the monitoring, all services must be ensured to fulfil the compliance and regulations. Ensuring adherence to applicable data protection laws, industry norms, and privacy standards. Keep abreast of any legislative or regulatory changes that may have an effect on how secure SMEs' critical information infrastructure is.

5.3.12 Outsourcing Management

Some SMEs can outsource a lot of services due to budget limitations and low capabilities. SMEs need to analyse the security posture of service providers and third-party vendors and implement agreements and contracts with security clauses. The companies need to check and verify vendor adherence to security standards on a regular basis.

5.4 DISCUSSING OF INFORMATION SECURITY FRAMEWORK PROPOSED

This framework is developed by referring to the results of literature review, conceptual framework, and analysis result of interview. Information security management is the output, and it will be influenced by all concepts which are assembling the information security team, identify critical information assets, risk assessment, customize security policies and SOP, security controls, network security, data protection, security awareness training, incident response, data recovery, and

monitoring and enhancement. The source SMEs can used are relevant platforms such as cloud. SMEs can save or backup data on the cloud based on specific budget. Moreover, outsource is the choice for SMEs to implement based on current conditions.

Some companies may not have enough capabilities and platforms to conduct IR and recovery services. These companies can outsource the professional team to handle these issues according to limited budget. It helps to save costs and achieve better security governance.

5.5 SUMMARY

This chapter proposes the new information security framework for critical information infrastructure in SMEs according to threats or vulnerabilities, gaps of existing information security management of SMEs, and limitations of SMEs defined by literature review and interview. This framework does not have any test and implementation. SMEs can customize their own framework and management methods based on this guideline. Information security management is the output, and it is influenced by information security team, risk assessment accuracy, security policies and SOP, security controls, network security, data protection, quality of security awareness training, incident response, data recovery, monitoring and enhancement of critical information infrastructure and outsourcing management.

This chapter extends the discussion of specific processes such as risk assessment, data recovery and so on. These processes can be controlled by SMEs better and accuracy is most important. The information security team cannot make any mistakes among these processes. The security framework will be optimized during the development of relevant security products and services in the future, and it will satisfy all the business requirements for the SMEs better.

CHAPTER VI

CONCLUSION AND FUTURE WORKS

6.1 INTRODUCTION

This research study's main aim is to propose a new information security framework for critical information infrastructure in SMEs. The research target focus on SMEs, and the security framework is developed based on the role of SMEs. The study researches the threats and vulnerabilities of critical infrastructure and critical information infrastructure, gaps and weakness of existing information security frameworks and management and limitations for the role of SMEs. The research objectives are completed and identified according to many methodologies and measures.

This chapter discusses the summary of this project, and each research objective will be defined based on specific research content. This chapter discusses the limitations of research study and future works. The development trend will be forecasted based on the current research result.

6.2 ACHIEVEMENT OF RESEARCH OBJECTIVES

The research objectives are designed according to the topic and popular research among current markets. SMEs often become popular research and discussion target in the market. As relevant technology has developed rapidly in recent years,