CHAPTER I : INTRODUCTION

1.1 Introduction

An overview of the background study, scope, objectives and potential contribution along with the significance of the research study are provided in this chapter. The organization of thesis including chapter outlines and definitions of the key terms are also explained in this chapter.

Information technology infrastructure refers to the components required to operate and administer enterprise IT environments. This study is to segment Information Technology (IT) infrastructures according the types of IT infrastructure profiling, the result of the segmentation will be classified based on the IT security maintenance framework to determine the maturity secure of the IT infrastructures. This is important to do due to the specific type of IT infrastructure or asset to control security issues for overall IT infrastructure. Currently, the process of IT security maintenance is done separately or manually by using any IT security model or method with a different location, department, or IT services.

Other misconceptions concerning IT infrastructure might also cause issues. For example, an IT security issue may perform in one environment but not in another, especially if they are collaborating with a partner organization in another department that has a different type of IT infrastructure. As a result, if a corporation changes its IT infrastructure, adds a new cluster, or migrates to new IT Infrastructure profiling or type of IT asset, its assumptions may no longer be valid. As a result, it's critical to keep an

eye on IT infrastructure and services and profile them on a regular basis to avoid falling into any of these pitfalls.

Due to the challenges posed by digital technology, the year 2020 marked a turning point for digitalization initiatives in all sectors of the business and society. Unfortunately, the rapid adoption of digital technology may have resulted in some risks being taken, and threat actors are taking advantage of this. To keep ourselves safe in cyberspace, the government, organizations, and individual users must collaborate.

The increase in cyber-attacks that businesses and governments have seen as a result of each year is a direct result of the additional opportunities and vulnerabilities that digital world has created. Despite the general battle to keep secure during the digital transformation era, most CISOs are optimistic about their prospects for cyber security, as they seek to prevent targeted threats, safeguard data, and make their users more resilient to cyber-attacks.

The road to full digitalization, or the 4th Industrial Revolution era, is fraught with problems and perils. The most common is cybersecurity, as well as the hazards that it brings. Cybersecurity is ingrained in today's society, but many people are unaware of its presence or practical applications within organizations and countries. Following that, CyberSecurity Malaysia is also had number of 10,790 cyber security incident reports during the year of 2020 as state on following Figure 1.1. These statistics are released based on a number of categories such as intrusion, intrusion attempts, content related, and vulnerabilities report, denial of service, cyber harassment, fraud, malicious code and spam.

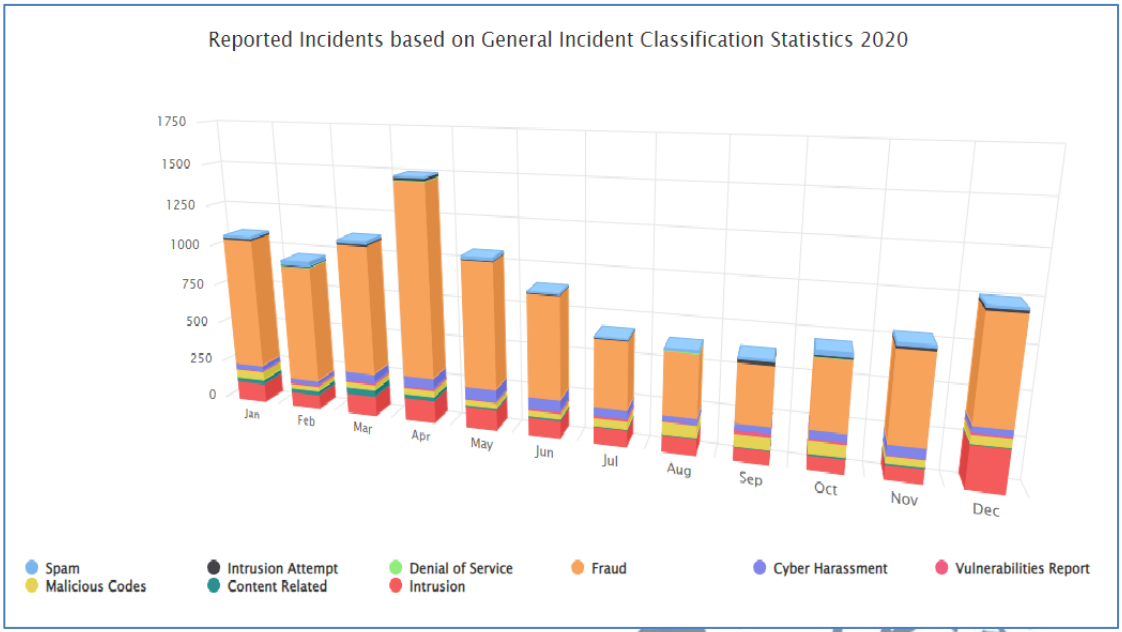

Figure 1.1: Cybersecurity Incident Report 2020

Malaysia is the sixth most vulnerable to cybercrime which is reported by Sophos Security Threat Report, 2013. Complacency of the IT services usage is the foremost reason on Malaysian organizations are easily becoming target to cybercrime (Norton, 2016).

The main objective of the research is to use and combine the appropriate components of IT security into an integrated and focused of IT infrastructure security maintenance framework.

1.2 Background Study

Modern information technology infrastructures hold a great promise to offer computing and IT as a cheaper yet convenient service to the mid-size organization, the Enterprise and Small Medium Businesses (SMBs) (Chang S.L. et al., 2010; UNCTAD, 2019). The many advantages of IT usage such as economy of scale, consolidation, efficiency in configuration and management, high availability and energy savings are

well documented (Gary and Alice, 2002; UNCTAD, 2019). Within that, many top industry analysts such as the International Data Corporation (IDC) predict that secure information technology infrastructures will lead to major, transformational changes across the industry (Spiezia, V., 2013; UNCTAD, 2019). Several industry analysts and IT leaders are also in aligned agreement that secure information technology infrastructures are poised to be a significant growth area (Verizon, 2014; Verizon, 2016).

IT security maintenance in information technology infrastructure is expected to help IT usage achieve better utilization and help the enterprise avoid the costs of resource overprovisioning. It would also allow the enterprises, especially the medium organizations and SMBs to maintain IT setup and management, which typically are not their core expertise and focus more on their business area (Stoneburner and Goguen, 2002; Craig et al., 2011).

Nowadays, within the growth of technology such as internet access and mobile devices had put many digital security issues in IT infrastructure such as hacking activity, malware attack and others (Jun, Punit & Kai, 2011). Most of the IT infrastructure's components had been exposed to the outsider by using the internet access and web-based application (Shahibi & Fakeh, 2011). More than 60 websites of Malaysian government agencies had been compromised in 2015 including public universities (Berita Harian, 2015). Hence, IT security maintenance in information technology infrastructure should be implemented as soon as possible to improve the digital security of the organizations. Then, with the full coverage access of IT infrastructure and services usage, the focus of IT security maintenance in information technology infrastructure should be done as completely as feasible. (Alnatheer, 2014).

Digital security of information technology infrastructure is required with a variety of functions including security planning, policy formation, staffing, risk management, security technology selection, threat assessment, countermeasure implementation, performance monitoring and maintenance (Whitman & Mattord, 2012). Choosing the right countermeasures to security threats had become one of the more pressing issues that continual require attention (Verizon, 2016).

Detection, deterrent, vulnerability reduction, education, and training are some of the tactics that can be used to combat a wide range of digital security risks that now exist (Kozlovszky, 2013). However, adopting an overall coverage within importance priority solution within an IT security maintenance framework is preferable to a superior method. Each IT security maintenance model or framework required different costs, effectiveness and potential benefits. In reality, many of these are difficult to quantify, reporting by Verizon Data Breach Investigations Report 2015.

The business value derived from information security investment may be difficult to estimate or undeniable (Kim et al., 2011). This difficulty happens because of the unexpected of threat manipulation, the duration of damage incurred, the duration of recovery, and any ripple effects to other parts and a loss of reputation (Verizon, 2015). Many successful factors engage with these IT security maintenance framework including innate vulnerabilities, the perceived attractiveness of targets, the engagement of attackers, the attack tools and vectors, and the extent and nature of backup facilities (Verizon, 2016).

Before that, most of the information security matters were treated in form of technical issue (Singh, Picot, Kranz, Gupta, & Ojha, 2013). Then, majority of the

attention was given to technological solutions as an isolation situation and these did not prove to be sufficient. Information security challenges should be considered in a structured and managed to do digital security maintenance in IT infrastructure, according to certain studies (Ernst & Young, 2012; Phillips, 2013; Singh et al., 2013; Siponen, Mahmood, & Pahnila, 2014).

IT staff must never overlook the importance of IT security maintenance in any IT infrastructure that needs to be protected. The IT security maintenance entails the numerous forms of existing IT assets in maintenance, such as corrective and preventative in any security issues, as well as the contrasts between them. These suggestions have raised the interest of the study to review extant literature regarding the reported role of IT security maintenance framework in information technology infrastructure.

1.3 Problem Statement

IT security maintenance is very important aspect in information technology infrastructure to identify any weaknesses which involved security breach in some organizations at early time. At the same time, some key concerns have also emerged about IT security maintenance in information technology infrastructure, which currently are viewed as significant barriers to its fast and wide-spread adoption. According to an International Data Corporation (IDC) survey of Chief Information Officer (CIOs) consecutively in 2008 and 2009, security, integration and reliable performance ranked among the top concerns expressed (Fonseca & Vieira, 2013).

An ENISA (European Network and Security Administration) survey of SMBs also confirms that major concerns for SMBs migrating to the IT service or infrastructure

include the confidentiality of their information and liability for incidents involving the infrastructure (Wooyun, 2015). This is understandable, because each of these factors have a major influence on the enterprises bottom-line.

Similarly, availability of the IT services platform with good performance and depends heavily on the quality of network characteristics, especially the round trip delay or latency (Fonseca and Vieira, 2013). Security is a key concern, because confidentiality, integrity, authenticity and auditability of business data, tools and transactions are critical requirements for businesses to stay functional, legal and competitive. This need is critical for all users especially for overall IT security maintenance in information technology infrastructure.

The implementation of IT security framework on the information technology infrastructure emphasizes on the controls needed. Only a little information is given about security objectives and on the potential strategies to implement these objectives (Wooyun, 2015). Therefore, the most existing framework is unable to provide information on any recommendations on how organizations should develop security objectives and strategies (Tan et al., 2014).

Many of the security framework are all documents ranging from detailed technical guidelines to high-level principles (Conner et al., 2003; Smith & Brooks, 2013). Most of the security framework focus primarily on general principles and guidelines and leave users without sufficient detail for implementation (Sendi et al., 2010; Smith & Brooks, 2013). Standards had been provided only for a set of general and generic guidelines (Franceschini et al., 2006; Smith & Brooks, 2013).

However, there is no open, comprehensive, and publicly accessible IT security maintenance framework that an organization may utilize to close the security gap that is relevant to their needs (Bartock et al., 2016).

Many organizations undertake digital security maintenance on each specific IT service or infrastructure, such as operating systems, network, servers, and others (Bhilare and Ramani, 2010; Bourgeois, 2014). However, it only focuses on the accessibility and availability aspects for certain IT service or infrastructure in conveniently. Then, there is not much security aspect had been proposed in detail and as a main goal especially for IT security maintenance in IT infrastructure. IT security maintenance is very important for authorized peoples can access any IT service or infrastructure in more secure and safe manner.

These limitation factors are related to issues and challenges to be addressed in IT security for IT infrastructure. Which is, IT security maintenance framework is designed to focus organizational effort on maintaining system rather than management model which is method to manage and operate system.

The momentum is one of the most important aspects of IT security. The term "momentum" refers to how to execute IT security in a systematic and consistent manner. What is a basic action that could be taken now to create momentum toward effective IT security transformation? When you ponder too much, you can lose your momentum. Many organizations struggle to comprehend their existing level of progress and effectiveness when it comes to launching new digital initiatives. Where should they concentrate their efforts in order to convince senior stakeholders of the value of the IT security implementation?

How did you remove as much friction from the user's digital experience as possible? Leadership, product, development, architecture, and operations are just a few of the primary areas of transformation failure that many organizations have experienced. What began as a conversational explanation of these failure patterns has grown into a guidance framework focusing on IT infrastructure components to explore organizational capabilities, risk, and remediation. On beyond that, it required speed and simplicity IT security maintenance framework to fuels the successful of digital transformation.

The issues and challenges are related to IT security maintenance because there is limitation structure of existing IT security framework for a visibility solution implementation across overall the IT infrastructure, as well as address the challenges.

1.4 Research Questions

Based on the problem statement, the main research question is about **(1) how the IT security is well maintained to serve IT infrastructure in any organization?** Then, **(2) How may appropriate IT security maintenance components for IT infrastructures be incorporated?** With that, the following research questions are being evolved to address this question.

1. Why are the current IT security components which is important to include in the proposed of IT security maintenance conceptual framework?
2. How are the selected components of IT security models and approaches within the appropriate value should be include in proposed IT security maintenance conceptual framework?

3. How are the components agreed by practitioner for proposed IT security maintenance framework?
4. How to evaluate in each proposed security aspects for proposed IT security maintenance framework?

1.5 Objectives

Based on the research questions, four (4) research objectives have been developed which are:

1. To identify components/factors on IT Security Maintenance Framework.
2. To propose a framework for IT security maintenance in IT infrastructures.
3. To verify the components of IT security maintenance framework in IT infrastructures.
4. To validate the framework of IT security maintenance in IT infrastructures.

1.6 Research Scope

From the proposed study, this research only focuses and expected to have a concrete and holistic of IT security components only for a conceptual IT security maintenance framework in IT infrastructures. The scope of the study is limited to existing IT infrastructures at a few Malaysian public universities, and it does not go into detail about any forms of attacks that might occur. Because the notion of basic usage of IT, IT infrastructure, and IT security is almost the same across areas, types of businesses, and types of organizations, the selected Malaysian public university can represent IT usage in a campus-based network.

With that, the area of study in this research covers the perception of the management personnel as technical and experienced personnel who are involved in IT

infrastructures and security. The survey questionnaire's respondents are from Malaysia's public universities, which were chosen as an organization or unit of analysis for the study. The proposed framework's components significantly chosen based on response by selected IT practitioners and validated by selected IT experts to ensure the framework achieves the IT security maintenance requirements. The proposed framework is a generic framework for IT security maintenance which only considers on IT infrastructures perspective.

This research aims to establish an IT security maintenance framework since a framework demonstrates related concepts and how they relate to each other in a descriptive way. The framework prescriptive, a type of lower-level research guidelines and more highly formalized representations of phenomena and their interactions, and is generated in most cases to predict or regulate phenomena (Antonio & Labuschangne, 2012). The framework, however, is a way of defining the empirical relationship between each element necessary for research consideration. Framework can be seen from multiple viewpoints, such as organized thoughts, principles, and other things that are cohesive and simple to convey to others (Sensuse et al., 2014). This study decided, with those reasons, to mark the result as a framework.

In this study, selected public university had been chosen because in public university, research work is done at higher level due to presence of expensive instruments. Public university is also collect funds from federal. So, a huge number of students involved in the university and they also manage do research work. With this reason, public university had become main selection to this study.

Then, the use of IT security maintenance framework had been selected in this study rather than IT security management model because of the framework is designed to focus organizational effort on maintaining the system. Hereby, the IT security management model is methods to manage and operate system.

1.7 Research Significant

The innovative and enhanced conceptual framework for IT security maintenance in IT infrastructures should be able to improve IT security practices on the accessibility of IT infrastructures and services in a campus-based network. There is a structural method and approach to perform IT security maintenance for overall IT infrastructure in the organization.

By achieving the research objectives, this framework can be beneficial to the information security practitioners, regardless of whether practitioners are newly approaching to apply any model of information security management or those that have been long in this field. These are discussed further subsequently.

1.7.1 Significance to Academic

In this study, a novel conceptual IT security maintenance framework for IT infrastructure had been proposed and open for discussion for the framework improvement in academic and practices purpose. Then, it involves in increased the number of study for IT security field. With that, it will make more references for the future researchers.

In addition to these, this study also offers awareness on the identification of components of IT security maintenance that have been addressed separately by different researchers, but none of the researchers have integrated all the IT security maintenance

system relevant to technical and non-technical perspectives under one framework as the information security management taxonomy. In adopting a technological viewpoint, current IT security concepts, theories, models and frameworks have essential limitations. The research brings both technological and non-technical viewpoints relevant to IT security together under one framework.

1.7.2 Significance to Practice

First, this study sets out the literature study of IT security maintenance. This is very important for IT or information security department or unit for doing strategic planning that required before starting the actual IT security maintenance. It will guide the practitioners with the general view of flow and types of IT security maintenance to be gathered and the requirements to be met before the framework is conducted. Thus, IT security practitioners will get to know exactly what the outcome of their decision will be and provide trustable and applicable guideline to them.

Second, this study set out the components of IT security maintenance framework. IT security maintenance can ensure that an organization has a good level of security to support the IT infrastructure they gathered throughout the components of IT security maintenance (Chen and Nazareth, 2010). These components can guide information security practitioners to do their own IT security maintenance for ensuring the security of IT infrastructure support in a well manner. Thus, it can be concluded that the process of gathering quality components of IT security maintenance would encourage in making an IT infrastructure security support that leads to a clear direction, and ultimately help to make decisions that lead to success.

The proposed framework is able to guide IT security practitioners on maintain and support any IT security on IT infrastructure of any organization. This means, the conceptual framework propose will gives corporate level awareness in the management context. The proposed framework provides awareness of what is needed to secure maintain the IT infrastructure. The proposed framework is able to alert the practitioners whether they are already conquering the IT security maintenance needed for IT infrastructure. This is because the better maintain of IT security in IT infrastructure can enable the organization in a well manage and can have a better productivity.

1.8 Research Methodology

The research used mix-method approach to answer the research questions. In the quantitative method, the study distributes self-administrated survey questionnaire to specified respondents using simple random sampling technique. The questionnaire is composed of a set of four categories. The Likert Scale is a questionnaire that is used to measure the components/factors of an IT security maintenance framework. The data obtained are in the form of numerical tables and figures together with the statistical results that will be helpful for hypothesis testing.

In the qualitative method, the study conducts an in-depth semi-structure interview with six specified respondents which among the expert and management staff of IT in selected public university. The in-depth semi-structure interview is composed of a set of two categories. Within that, content analysis the data obtained are in the form of numerical tables and figures together with the statistical results that will be helpful for validate components/factors of an IT security maintenance framework. Then, content analysis was employed for qualitative data to validate IT security maintenance

framework. In Table 1.1, it shows the relationship between research problem, research questions, research objectives, research activities and research outcomes in this study.

Table 1.1: Research Problem, Questions, Activities and Outcome

Research Problem	**Research Questions**	**Research Objectives**	**Research Activities**	**Research Outcomes**
Limitation structure of IT security framework for a visibility solution implementation across overall the IT infrastructure	1. How are the current IT security in the IT infrastructure.?	To conduct a literature review on IT Security Maintenance Framework.	Literature Review Analysis	Descriptive study on IT security
	2. How are the selected components of proposed IT security maintenance conceptual framework?	To propose a framework for IT security maintenance in IT infrastructures.	Literature Review Analysis	Develop a framework
	3. How are the components agreed by practitioner for proposed IT security maintenance framework?	To verify the components of IT security maintenance framework in IT infrastructures.	Quantitative-Likert Scale Survey Questionnaire Quantitative Analysis	Verify the framework
	4. How to evaluate proposed IT security maintenance conceptual framework?	To validate the framework of IT security maintenance in IT infrastructures.	Qualitative In-depth Semi-Structured Interview Content and Quantitative Analysis	Validate the framework

1.9 Organization of the Thesis

This thesis is arranged and divided into five (5) chapters. Chapter 1 discussed the introduction and background of the study. Besides that, the issues and research problems have been explained deeply. Resulting to this, several scopes of this research

have been formulated to ensure this study is following the right track and the objectives that have been set up are achievable.

Chapter 2 has included the literature review of the study. It explores several concepts related to this study as the concept of information technology, information security, information security management, information security models any relevant matter to the IT security. These concepts are discussed deeply to understand the issues related to this study. Moreover, this study emphasizes information technology security practices in the information technology security maintenance. Therefore, this chapter highlighted to answer the Research Question. With that, findings in this chapter are to fulfill the requirement of Research Objective. Then, theoretical framework that was developed based on the information technology security practices and model to understand the issues and fill the gap of poor information technology security maintenance implementation.

Chapter 3 describes the detail of the study area profile and justification of study area selection. This chapter discusses the research methodology that was used to achieve the Research Objective number three of this study and fulfill the answer of the Research Question number three. This chapter aims to provide a review of the relevant principles of research design and methodology adapted in this research. It discusses the four phases, known as background research, framework development and verifications, framework validation and report the finding. It also justifies the use of quantitative and qualitative methods, designing the instrument to collect data, justifies the reasons of using analysis techniques, discusses the validity and reliability of the instruments and finally sample and population in this research.

Chapter 4 discuss the result of this study. This chapter states the quantitative and qualitative data collection analysis results in order to develop the IT security maintenance framework. This chapter presents statistical analysis in order to verify the development the research framework. The findings from the quantitative analysis will be further confirmed with experts by obtaining their opinion on validating the components in the IT security maintenance framework and its usefulness for IT security practitioners. The qualitative study will further provide a synthesis of IT security maintenance parameters. Qualitative data is achieved from semi-structured interview with six expert panels.

Chapter 5 concludes the research by recapitulating the study. Then, the contributions of this research are highlighted. Finally, the limitations of the research are addressed followed by the future directions in the related field.