CHAPTER V :CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

It consists of five main components in this chapter, which are achievement of objectives, framework application, conclusion, contribution, research limitation, direction for future work and recommendation. It contains the summary of the result well explained in the report, with the outcome of the study and concept/theory relevant to the previous research. It consisted of limitations during the study for research limitations. Then, for the recommendation which are recommendation from the related parties and recommendation related to the future research. As the end of this chapter, the result of the research and implications of the research are well discussed and concluded.

5.2 Conclusion on Verification

The goal of this research was to see how effectively IT security is maintained in each organization's IT infrastructure. Then, how can suitable IT security maintenance components for IT infrastructures and services be incorporated?

The study's findings were primarily focused on defining and implementing an IT security maintenance framework for small-to-medium-sized businesses' IT infrastructure. The study aided in identifying (1) the components of the IT security maintenance framework, (2) the verification of the IT security maintenance framework, and (3) the validation of the IT security maintenance framework, all of which confirmed the hypothesis. When paired with theory and literature, the quantitative findings serve

to create statistical evidence on the strengths of the link between components and suggest directions for the relationship.

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 conventional sampling technique. The questionnaire is composed of a set of four categories. Likert scale is used to employing questionnaire for measuring components and factors of IT security maintenance framework. Whereby, in quantitative research the data were collected through questionnaire and analyze using Statistical Package for Social Sciences (SPSS) and AMOS in order to gain measurable objective. In this research, 272 questionnaires have been distributed to IT experts and the respondents answered all questionnaires. The respondents used for further analysis was 272 according to Krejcie and Morgan table based on the population of 600.

Demographic of respondents were determined by descriptive statistics and reliability test was performed and found that the IT asset identification showed Cronbach's alpha of 0.887, security breach identification is 0.928, IT security offensive protection are 0.881, IT security defensive protection are 0.923 and IT security objectives are 0.978. So, the data in this study can be classified as good and adequate for this research means.

The Skewness and kurtosis showed the result between -2 to 2. Thus, the data is normal. Frequencies and Percentages were measured for IT Asset Identification, Security Breach Identification, IT Security Offensive Protection, IT Security Defensive Protection and IT Security Objectives. The overall mean and standard deviation shown the respondents agree about IT Asset Identification, Security Breach Identification, IT

Security Offensive Protection, IT Security Defensive Protection and IT Security Objectives.

Statistical test used to investigate the relationship between the variables studied. Correlation tests used to determine the relationship between variables. The result showed IT asset identification is significant relationship with security breach identification (r=0.650, p=0.000), IT security offensive protection (r=0.580, p=0.000), IT security defensive protection (r=0.624, p=0.000) and IT security objectives. Besides security breach identification showed significant relationship with IT security offensive protection (r=0.706, p=0.00) IT security defensive protection (r=0.689, p=0.000) and IT security objectives (r=0.356, p=0.000). Next, IT security offensive protection showed significant relationship with IT security defensive protection (r=0.713, p=0.000) and IT security objectives (r=0.512, p=0.000). Lastly IT security defective protection is significant relationship with IT security objectives (r=0.580, p=0.000).

Factor analysis is a strong data reduction approach that allows academics to study ideas that are difficult to assess directly using traditional methods. It allows researchers to investigate or validate the links between survey questions and to determine the total number of parameters covered on a questionnaire by using factor analysis techniques. The factor analysis of all variables were carried out and based on the result, Bartlett's Test of Sphericity give values P< 0.05 which means all variables are statistically significant and correlated between the items.

In order to determine the dimensionality of the research scales, the items from all scales were factor analyzed using the CFA method in AMOS version 24. The degree to which the sample supports the factor structure of the scales is determined using CFA. CFA makes extensive use of statistical tests to assess the model's fit with the data that has been obtained.

The KMO Bartlett Test was used because CFA is based on theory and other standard requirements such as sufficiency of the data. The KMO test was performed by incorporating all the items of all scales to measure the sufficiency of the sample on the collected data, which scored 0.879 (> 0.5), and Bartlett's test of Sphericity of the sample was also significant (p<.001), as shown in Table 1, indicating that the study variables have been correlated It was concluded as a result of these findings that the data was appropriate for performing the CFA.

When it comes to statistics, confirmatory factor analysis (CFA) is really a unique kind of factor analysis that is most often employed in social research. It is used to determine whether or not measurements of a dimension are compatible with a researcher's knowledge of the nature of the construct under consideration (or factor). Thus, the goal of confirmatory factor analysis is to determine whether or not the data conform to a postulated measurement model in the first place. This postulated model is based on theoretical considerations and/or past analytic investigation.

An analysis of fit was carried out for each element individually (Asset Identification; Security Breach Identification; Security Offensive Protection; Security Defensive Protection; and Security Objectives), with the best possible match being determined for each factor.

Convergent Validity, discriminant Validity, constructs Reliability and model fitness was determined for each factor separately. Since all factors loadings were above excellent (>.71) criteria (Comery & Lee, 1992), so reliability of this measure was established (Hair et al., 2017).

A comprehensive CFA was conducted to assess the fitness of the five-factor model, which included Asset Identification, Security Breach Identification, Security Offensive Protection, Security Defensive Protection, and Security Objectives, and

which demonstrated the best possible fit (Chi2 = 649 / df = 138 yielded 4.71, CFI =.902, TLI =.866, RMR =.067, RMSEA =.117) between the measurement and the data collected (see Table 14).

We proposed five hypotheses as H1: IT assets significantly positive influences the IT infrastructure for IT security maintenance, H2: IT security breach significantly positive influences the IT security maintenance for IT infrastructure, H3: IT security offensive protection significantly positive influences the IT security maintenance for IT infrastructure, H4: IT security defensive protection significantly positive influences the IT security maintenance for IT infrastructure. Results of these factors as hypothesis 1) IT ASSET IDENTIFICATION intention in IT Infrastructure Security maintenance 2) SECURITY BREACH IDENTIFICATION intention in IT Infrastructure Security maintenance 3) IT SECURITY OFFENSIVE PROTECTION intention in IT Infrastructure Security maintenance 4) IT SECURITY DEFENSIVE PROTECTION intention in IT Infrastructure Security maintenance 5) IT SECURITY OBEJCTIVES PROTECTION intention in IT Infrastructure Security maintenance and table 4.33 shown that all hypothesis were accepted.

That means all variables (IT Asset Identification, Security Breach Identification, IT Security Offensive Protective, IT Security Defensive Protection and IT Security Objectives Protection) is have relationship with IT Infrastructure Security Maintenance. So we concluded factors Influencing IT Security Maintenance are IT Asset Identification, Security Breach Identification, IT Security Offensive Protective, IT Security Defensive Protection and IT Security Objectives Protection which are key elements of IT security framework.

This research proves that (Sarriegi and Santos, 2008; Turel etc al., 2017) studies were right as he stated that Information technology strategic plan should be provided to

achieve a balance between the comprehensive implementation of information technology infrastructure with business planning within the organization. Khurana & Hadley, 2010 stated that the information technology infrastructure must correctly handle the management structure of components in information technology such as information technology resources, user information systems, business information systems, and business data so our results concluded this statement right.

The research uses the qualitative approach to conduct a semi-structured interview with five respondents chosen from among the IT expert and management personnel at a public institution. A set of two categories make up the semi-structured interview. Within content analysis, the data acquired is presented in the form of numerical tables and figures, as well as statistical findings that may be used to evaluate hypotheses.

Then, for qualitative data, content analysis was used to verify the IT security maintenance framework. We came to the conclusion that all of the respondents agreed that this framework is suitable to current practice and that this framework can handle current difficulties. The respondent has said that this framework should be equipped with appropriate analysis against any information security management paradigm, particularly in ISMS (Information Security Management System). Every governance problem that has been detected during the deployment of the framework should be thoroughly examined using any information security management model that the firm employs.

5.3 Achievement of Objectives

This research successfully achieved its all objectives. It has explored new knowledge in IT security by proposing IT security maintenance framework as a new

process approach framework for IT infrastructure. Within the study methodology and research design, a framework was built through a comprehensive process. This research produced an enhanced IT security maintenance framework for IT infrastructure.

In this study, researcher had outlined first research objective, which is; **to conduct a literature review on IT Security Maintenance Framework** and second research objective, which is; **to propose a framework for IT security maintenance in IT infrastructures**. With that, the first research questions for achieving the first objective of the study was proposed, what **are the current IT security models and approaches which is important to include in the proposed of IT security maintenance conceptual framework?** Then, second research questions for achieving the second objective of the study was proposed, what **are the selected components of IT security models and approaches within the appropriate value should be include in proposed IT security maintenance conceptual framework?**

Both first and second, objective and research question was identified through the review of the literature, that there are various types of IT security concepts, theories, practices, model, framework and methodologies proposed by IT security professional body, researchers, experts and the organization to implementing into IT infrastructure. However, only few types of IT security components from all the approaches become a chosen in this research. Study have been made to see which IT security components are most frequently important used to deploy in IT infrastructure.

From the literature, the researcher identified a total of five types of IT security components which have become this research preferable choices and those are from the establish security concepts, theories, practices, model, framework and methodologies propose by IT security professional body, researchers, experts and the organization.

Then, the five components of IT security become as an IT security maintenance framework for IT infrastructure and also become the hypotheses for this study.

The third research objective, which is; **to verify the components of IT security maintenance framework in IT infrastructures.** With that, the third research questions for achieving the third objective of the study was proposed, what **are the components agreed by practitioner for proposed IT security maintenance framework?**

All the components defined from the first and second research questions were combined and made parts to develop IT security maintenance framework for IT infrastructure. IT security components is a layout of IT security maintenance framework which is organized in a way in which the components are put together to form a meaningful framework. The IT security maintenance framework was developed based on the secondary data. Therefore, a survey was conducted to strengthen and validate the framework components based on the actual IT infrastructure's situation. This study deployed a Likert style close-ended questionnaire and administrated to IT and IT security practitioners in several Malaysian public universities by using simple random sampling. The results of the findings for descriptive study and statistical analysis is discussed in Chapter 4. **The findings of this descriptive study and statistical analysis were analyzed to verify that the components were selected on the basis of a high frequency of over half the percentage of practitioners' accepted responses.**

The fourth research objective, which is; **to validate the framework of IT security maintenance in IT infrastructures.** With that, the fourth research questions for achieving the fourth objective of the study was proposed, **how to evaluate in each proposed security aspects for proposed IT security maintenance framework?**

This exploration question was satisfied by playing out the validation in two stages in the in-depth semi structured interview. Six IT experts were involved in the

validation analysis. In the first step, the interview is provided with the validation to conform to the actual practices of IT security specification consisting of necessary and adequate components. By looking at each item specified in the framework, experts evaluated the suggested framework with full attention.

All the experts accepted that the proposed framework had the following requirements, known as appropriateness, the proposed framework consists of appropriate and adequate components for the collection of IT security maintenance in the real IT infrastructure environment; objectivity, easy understanding of the process; practicality, the stage is easily understood, the way tasks are arranged and words are used; reliability, components are clearly described in the frame and the components suggested by the framework is well organized and structured. However, in order to make them suitability model, the proposed framework was reorganized and revised according to the findings of the experts. More details are available about the comments of the experts in Chapter 4 and Appendix E.

5.4 Framework Application

IT security maintenance framework for IT infrastructure was developed in this study. After that, it is very crucial to integrate this framework in current practices. Application of this framework into current practice can be carried out through the well understanding of each component that have in the framework.

After the framework development, in order to validate the developed framework, an in-depth semi-structured interview on ensuring the framework conforms to real working of IT security maintenance in IT infrastructure. In-depth semi-structured

instrument for interview on validating the framework was designed in order to gain information from the IT expert panel in public university.

The qualitative research continues by requesting experts to discuss the synthesis of IT security maintenance parameters. The list of IT security maintenance parameters can be used in ensuring the quality of IT security for IT infrastructure. As the process of integrating IT security maintenance parameters in IT infrastructure is enhanced, by listing the tasks which reflect the quality of IT security will be a stepping stone for ensuring the quality throughout the IT security maintenance process. Finally, the proposed framework's usefulness for organizations was conducted with advice from expert panels.

5.5 Contributions

The main objective of this study is to provide an IT Security Maintenance Framework that focuses on providing a layout of IT security components that is structured in a way that focuses are placed together to form a coherent framework, can be navigated at any time and can also guarantee the quality of information throughout the framework in the process of collecting meaningful data.

The main contribution of this study is the IT Security Maintenance Framework. Based on the findings of theoretical and explanatory studies, it was designed. The current method, methodology, theories and model of IT security that organizations typically use to organize all framework creation processes. The current IT security weakness strategy, methodology, hypotheses and model is that it is unable to provide evidence on any recommendations on how organizations can develop security priorities and strategies. However, all the components involved in the framework process are described in the proposed IT Security Maintenance Framework. Practitioners just need

to observe the flow of layout knowledge along with the consistency components to achieve implementation of the framework.

During the review by the experts, they concluded that the proposed framework achieved its objective of applying the IT Security Maintenance Framework by its directed practitioners. In addition, the framework can also alert practitioners by offering a holistic image of IT security maintenance in order to gather what should be planned and what needs to be gathered.

This study also provided information on the identification of IT security issues on IT infrastructure that were addressed separately by different researchers, but none of the researchers combined all methods relevant to non-technical perspectives under one framework as the taxonomy of security maintenance framework. Current methods of IT security have essential constraints in implementing a technological overview. This study identifies the importance of people and their knowledge as an IT security components of the organizations; and incomplete views of organization towards day-to-day activities where employees creating and using unofficial components are also considered as important components.

IT security practitioners are given the advantage of the framework, regardless of whether practitioners are newly entering the implementation of the IT security maintenance framework or those who have been in this area for a long time. In particular, in IT security management, this study contributes to the field of IT security maintenance by providing a process approach framework that lists all the required components to guide practitioners to the preferred IT security maintenance framework for achieving safe IT infrastructure. The proposed framework provides appropriate guidance that practitioners should use to perform IT security maintenance framework for IT infrastructure.

As a process approach-based framework for IT security maintenance, the proposed framework is able to guide practitioners in deeply gathering all the IT security components required for the framework to perform. Through doing so, practitioners will ensure that the amount of data needed for the implementation of the IT security maintenance framework is reached. This implies that the framework provides awareness at the corporate level in the context of management. Awareness of what is required to implement the IT security maintenance framework is provided by the proposed framework. The proposed framework is also able to alert practitioners to the degree to which the IT security maintenance framework required for IT infrastructure is already being conquered. This is because knowledge of high quality will help the company to make quality decisions.

Since the IT department is responsible for strategic planning, all the necessary planning needs to be done before the actual security management begins. Therefore, with the IT security maintenance framework, the method of performing the security of the IT infrastructure would be more systematic and persuasive if the organizations knew in advance what information they needed before commencement of the plan. It directs the practitioners with the general view of flow, the types of security components to be collected and the specifications to be fulfilled before conducting the framework. By deciding in advance what to do, how to do it, when to do it and how to do it, practitioners prepare, leading to achieving a consistent path to accomplish framework priorities and goals. Thus, practitioners will get to know exactly what the consequences of their decision will be and provide them with trustworthy and appropriate guidance.

In order to maintain the IT infrastructure that they support throughout the framework operations, the IT security maintenance framework will ensure that an entity has a good level of security. Decisions are only known to be as good as the data on

which they depend. Therefore, a solid foundation can be established for organizations to have faith in carrying out framework implementation by understanding the IT security components of the framework. These components of IT security will direct practitioners to do their own IT security maintenance to ensure the implementation of the IT infrastructure framework. It can therefore be inferred that the introduction of the IT security maintenance framework for IT infrastructure will facilitate the creation of a strategy leading to a specific path and eventually assist in making good decisions.

Today, the word digitization or digital transformation has become the talk of the town in the face of the Covid-19 pandemic challenge of physically limiting movement and encounter. Most companies and organizations are shifting their direction to operate almost entirely digitally or online. The government has also announced the internet line which is the driving force for all these cyber and digital activities as a third country utility after water and electricity supply.

However, one of the main constraints to the concept of cyber digitization is the threat of cyber security. Most organizations in the country are already preparing to enter the era of cyber digitization almost completely but what about the preparation to face cyber security threats?

Most organizations in the country do not have specialized units or departments in dealing with cyber security threats. Most of these tasks are assigned to the unit or department responsible for information technology matters. If abroad, the head responsible for cyber security matters is known as CISO (Chief of Information Security Officer) whose position is relatively high in an organization that shows the high commitment of an organization in facing cyber security threats.

Similarly, digital security matters for information or digital technology services and infrastructure are not included in an integrated and holistic manner. Thus, an integrated and holistic approach needs to be implemented in the cyber security strategy for an organization. Among the important components of this approach are the identification of digital assets, the identification of the type of security intrusion involved, proactive security protection, security protection and cybersecurity objectives.

The main and most important thing is the identification of digital assets owned by an organization includes all information technology services and digital infrastructure. Next, the status in terms of critical levels and priorities for all available digital services and infrastructure needs to be determined.

The second step, each digital service and infrastructure is matched to the type of security intrusion that is likely to be involved. In general, this type of intrusion consists of three types, namely vulnerability (vulnerability) which is an existing weakness in digital services and infrastructure, threat (threat) which is an agent disrupting the smooth operation or damaging the integrity of digital services and infrastructure and expected attacks or exploits that are certain techniques are used to exploit existing vulnerabilities in digital services and infrastructure.

Next to the third step, each service and digital infrastructure must be matched with proactive security protection which is the activity of analysis and testing of security of digital services and infrastructure. There are three types of proactive security protection, namely vulnerability assessment, penetration testing and digital security audit.

Then, the implementation of the fourth step which is security protection which needs to identify the security methods involved in protecting digital services and

infrastructure. Generally, it should cover three basic things namely security education and awareness, security policy and security perimeter. Security perimeter is the use of cyber security applications or technologies such as firewall software, anti-Malware software, IDS (Intrusion Detection System) software and others.

So, the implementation of these second to third steps needs to be dedicated to each specific and existing digital service and infrastructure in an organization. The last step, is to map all the above steps to the objectives of cyber security which generally includes three things or objectives of protection, namely confidentiality (confenditiality), integrity and accessibility (availability).

The implementation of this integrated and holistic cyber security maintenance approach framework is able to create a high level of cyber security awareness among all staff of an organization, especially staff in the information technology department in facing any type of cyber threat that comes. It should be noted that this humane aspect is part of a very significant cyber security vulnerability in creating cyber threats and attacks in an organization.

A major constraint in the implementation of this approach is that it requires the involvement of many competent human resources in the field of cyber security. Next also requires the involvement of comprehensive support among all staff in an organization especially strong support from top management.

The management of the organization needs to plan a sound, efficient and effective strategy in dealing with cyber security threats, especially to enable activities and operations to run better in the environment of cyber digitization.

5.6 Limitation of Study

In this research, there are several limitations faced by the researcher. One of them is time constraint to carry out the survey on the factors influencing the IT security maintenance. It occurred when the researcher was not able to commit with the time given to settle down the task due to work precedence and working commitments. In addition, the study was conducted only limited to 272 respondents which made up from various background.

Then, there are some of them do not give full commitment and cooperation during the study conducted. Moreover, this study can be extended by making comparison towards other factors which influencing IT security maintenance in different company to analyze the relationship between IT asset identification, security breach identification, IT security offensive protection, IT security defensive protection and IT security objectives towards IT security maintenance. Thus, this study can be discussed further due to the sufficient information and data. For the research which using this kind of technique, data is very important to obtain the actual output and analyze the data to examine the research is significant toward the overall research.

5.7 Direction for Future Research

There are several lines of direction for future research suggested. First, it would be worthwhile to investigate the relationships among the role of IT department in order to ensure the security system in the respective organization is secured and compare the findings with the present study which contribute to the factors which influence the IT security maintenance.

Second, it would be more valuable to study the role of certain demographic variables comprising interviewee profile in the relationship towards these five variables that influence the IT security maintenance which are IT asset identification, security breach identification, IT security offensive protection, IT security defensive protection and IT security objectives. Next, an extended study to determine the relationship between the factors influencing IT security maintenance based on the different point of view would be more interested and the researcher could do further research on the respective findings.

5.8 Recommendations

This research can be extended further by making among all the subjects to determine the factors which influence IT security maintenance. Besides that, number of sample can be increased to evaluate the factors that influence IT security maintenance. In addition, the other relationship can be study to investigate the factors influence IT security maintenance. Method of the research can be varies such as interview or observation at each of the location and respondents selected as center of the research.

Thus, it able to increase the findings and observed their relationship between those factors which influence IT security maintenance. The author of the thesis has opinion that it will cover a wider population and be able to do a proper comparison as it will incorporate a larger random sample size by questioning respondents. This would allow for further generalizability of the findings.

Based on the findings obtained, it shows that there are several factors influence IT security maintenance which are IT asset identification, security breach identification, IT security offensive protection, IT security defensive protection and IT security

objectives. Besides that, the behavioral patterns also affect IT security maintenance can be used for educational promotional purposes, as well as for the design of reminders and warning systems that could disturb IT security maintenance. In this present research, the factors of influencing IT security maintenance, it could be related to online behavior of users with IT facilities.

IT security management provides the foundation for critical infrastructure protection. The ability to effectively identify critical assets is a crucial first step to any risk management process especially in IT aspect. Ensuring that a critical infrastructure asset identification methodology is complete, reproducible, documented and defensible is essential to enabling, cross sector comparisons. The scope, approach and evaluation method are variables that can contribute to meeting these requirements. This presents an opportunity for critical infrastructure protection researchers. A multi-criteria decision making model that combines the strengths of existing methodologies is a promising approach it can provide systematic solutions that address the gaps and challenges associated with critical infrastructure asset identification efforts.

The research provides good analytical guidance on the conceptual security maintenance framework for IT infrastructure by enhancing IT security management. The research demonstrated that it is possible to create appropriate IT security model in order to enhance IT security management. Hence, through this beneficial approach, it will become an effective way to determine the factors which influence IT security maintenance.