CYBER SECURITY MAINTENANCE BASED ON HUMAN-TECHNOLOGY ASPECTS IN DIGITAL TRANSFORMATION ERA

Firkhan Ali Bin Hamid Ali
Mohd Zalisham Jali

ABSTRACT

The development of Information Communication Technology (ICT) or cyber infrastructure had growth which is very fast in producing a wide range of computer products cause some medium sized organizations are confused and ambiguous as to what should be done to the ICT infrastructure. This resulted in tragedy 'white elephant' where cyber infrastructure is purchased by the organization were not fully utilized or not used at all especially for ICT security infrastructure. While digital transformation has led manufacturers to incorporate sensors and software analytics into their offerings, the same innovation has also brought pressure to offer clients more accommodating appliance deployment options. So, their needs a well plan to implement the cyber infrastructures and equipment. The cyber security play important role to ensure that the ICT components or infrastructures execute well along the organization's business successful. This paper will present a study of security management models to guideline the security maintenance on existing cyber infrastructures. In order to perform security model for the currently existing cyber infrastructures, combination of the some security workforces and security process of extracting the security maintenance in cyber infrastructures. The implemented cyber security maintenance within security management model in a prototype and evaluated it for practical and theoretical scenarios. Furthermore, a framework model is presented which allows the evaluation of configuration changes in the agile and dynamic cyber infrastructure environments with regard to properties like vulnerabilities or expected availability. In case of a security perspective, this evaluation can be used to monitor the security levels of the configuration over its lifetime and to indicate degradations. The focused on the cyber security maintenance within security models in cyber infrastructures and presented a way for the theoretical and practical analysis based on the selected security management models. Then, the proposed model does evaluation for the analysis which can be used to obtain insights into the configuration and to specify desired and undesired configurations.

Keywords: Cyber, cyber security, ICT infrastructure, security maintenance, digital transformation, information security.

INTRODUCTION

In Malaysia, ICT infrastructure had been use in many organizations for doing their activities in efficiently and effective to support a quality of production. The study will discuss about more issues of digital security in the usage of ICT services. Security issues of the digital environment are not too become priority things in many organizations in the Malaysia especially for small medium enterprises. This subject is happen in the digital environment because it has a lot of ICT facilities and ICT knowledge had become more familiar with the Malaysian peoples.

The governments and the private sectors had promoted the ICT technology usage very hardly whether in the advertisement, party, contest or others incentive. Beside the ICT technology itself, it also cover sub-contents of the ICT such as multimedia technology, web applications, networking technology, programming and others. However, it not much concern on how to secure for those kinds of ICT technology and digital environment itself.

ICT is a short form of the Information and Communication Technology, which is about all the infrastructures, devices and components of the digital environment and communication such as software, hardware, system, database, and network, Internet and others related. Digital security is the method that we use to prevent and protect our digital environment using IT facilities and communications from the threats like disasters, systems failure or unauthorized access that can result in damage or loss.

THREATS ON THE ICT INFRASTRUCTURE

The usage of ICT services and infrastructures can be disabled or become poorly usage by many factors. It will be down the productivity of businesses in the organizations. All this factors may be become from one of these agents which it is the components of the ICT itself whether it is in indirectly or not indirectly such as peoples, procedural, software errors, applications, electromechanical problems, dirty data, and hardware and communication parts.

Digital environment is also can be threatened by natural hazards, by civil strife or terrorism. All these threaten can be done in indirectly or not indirectly situations. So, all the organization must know of all this threats first that make us easy to control and overcome any ICT security problems. Then, easy to ensure sure the digital security in the organizations are in safely manner.

Types of threat in ICT can be discussed as following matters.

1. ***Errors and accident - These threats are happen from by many agents like people errors, procedural errors, software errors, electromechanical problems and dirty data problems.***
2. Natural and other hazards - Some of these threats can causes all the systems or applications will be down overall and permanently.
3. ***Crimes against the ICT infrastructures -This kind of the threat is about illegal act perpetrated against the ICT infrastructures.***
4. ***Crimes using the ICT infrastructures - Before that, it had discussed about how the crimes act to the ICT infrastructures but now how the crimes happen by using ICT infrastructures.***
5. ***Malware - It is a computer programs or software that can causes destruction or make slowly the operations of the computers, systems or other ICT services and infrastructures.***
6. ***Computer criminals. - This is about types of the people who's involved in this ICT threats. People in the organization such as the employees and the people outside the organizations such as suppliers, customers, hackers, crackers and professional criminals can be categorizing as that types.***

In the many cases of the computer criminals, the organizational employees do it itself. This is happen because they can access the ICT infrastructure own by the organizational from the inside of the organizational. They may be use the ICT facilities in the organization in the dishonesty purpose for his personal profit, sell the information or steal the hardware.

Outside users such as suppliers and customers may be having a link or certain access to the ICT infrastructure of that organizational. So, they can use this ability to make a threat to the ICT facilities of that company.

But in the cases of the hackers and crackers, which are usually categorized as the outside people, are the peoples that are can get the unauthorized access to the ICT infrastructure of the company. The different between these two kinds of users are the hacker does it for challenging but the cracker does it for malicious purpose.

Professional criminals are members of the crime are organizational. They didn't only using ICT but also does the illegally business or process like selling the drugs or gambling. All this threat to the ICT infrastructure had become more seriously to the any organizations because of the increments of the more sophisticated user which is using its ability to make an unauthorized access and make several software that can break the any organization's digital security. By this problem any organization must have its control and safeguarding on their ICT infrastructures that will be in details on the next part.

ICT SECURITY MANAGEMENT

The definition of Information Security based on ISO/IEC 17799:2005 is "preservation of confidentiality, integrity and availability of information, in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved".

Information has many definitions as follows:

i) Information is about someone or something consists of facts about them.

ii) Important or useful facts can be obtained as output from a computer by means of processing input data with a program.
iii) Information is an asset which is like other important business assets which is has value to an organization and consequently needs to be suitably protected.
iv) Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films or spoken in conversation.

The core elements of information security management are to ensure the information assets, namely the following aspects.

i) Confidentiality
ii) Integrity
iii) Availability

Upon the successful implementation and testing of a new and improved security profile, an organization might feel more confident of the level of protection it is providing for its information assets (A. Vance, 2012). By the time the organization has completed implementing the changes mandated by an upgraded security program, a good deal of time has passed.

In that time, everything that is dynamic in the organization's environment has changed (A.C. Kim, 2012). Some of the factors that are likely to shift in the information security environment are:

- New assets are acquired.
- New vulnerabilities associated with the new or existing assets emerge.
- Business priorities shift.
- New partnerships are formed.
- Old partnerships dissolve.
- Organizational divestiture and acquisition occur.
- Employees who are trained, educated, and made aware of the new policies, procedures, and technologies leave.
- New personnel are hired possibly creating new vulnerabilities.

If the program is not adjusting adequately to change, it may be necessary to begin the cycle again. That decision depends on how much change has occurred and how well the organization and its program for information security maintenance can accommodate change (C. Melara, 2003). If an organization deals successfully with change and has created procedures and systems that can flex with the environment, the security program can probably continue to adapt successfully.

The CISO determines whether the information security group can adapt adequately and maintain the information security profile of the organization or whether the macroscopic process of the SecSDLC (Security System Development Life Cycle) must start a new to redevelop a fundamentally new information security profile. It is less expensive and more effective when an information security program is designed and implemented to deal with change (J.Fonseca, 2013). It is more expensive to reengineer the information security profile again and again.

Management model must be adopted to manage and operate ongoing security program (K.H.Guo, 2012). Models are frameworks that structure tasks of managing particular set of activities or business functions. With that, by assist the information security community to manage and operate the ongoing security program, a management model must be adopted (Tripathi A. Singh, 2011). In general, management models are frameworks that structure the tasks of managing a particular set of activities or business functions.

METHOD AND PROPOSED MODEL

The usage of ICT services and infrastructures can be disabled or become poorly usage by many factors. It will be down the productivity of businesses in the organizations. All this factors may be become from one of these agents which it is the components of the IT itself whether it is in indirectly or not indirectly such as peoples, procedural, software errors, applications, electromechanical problems, dirty data, and hardware and communication parts.

The methodology of the proposed research will be carried out based on the fundamental of the experimental information technology method. This method examines the research work to demonstrate two important concepts: proof-of-concept and proof-of-performance. To demonstrate the proof-of-concept, some important steps were performed. First, the research area within security maintenance is critically reviewed to provide the overview that leads to the justification of a valid research problem. Then, a novel model of the security maintenance framework is designed and analytically analyzed. This includes the creation of the mechanism for managing security model, processes and metrics in relation to use of security maintenance.

Proof-of-performance is demonstrated by integrating the proposed security model, processes and metrics within a novel conceptual framework of the security maintenance in ICT infrastructure. Then, it will be assessed using proposed framework. In those proposed framework, various parameters and workloads were used to examine and demonstrate the viability of the proposed solutions compared to other similar baseline solutions. Also, analytical analysis of some proposed security metrics is performed to evaluate the correctness.

Specifically, the main stages involved in the research are divided into three:

- Data Acquisition Stage
- Investigation and Modeling Stage
- Analysis and Evaluation Stage

The proposed conceptual framework for security maintenance in mid-size ICT infrastructure represents as an integration of ICT security management model and concepts covering several facets of information security aspects and processes. The framework draws from multiple areas including software vulnerability, risk assessment, attack motivation, threat detection, deterrence and security objective. It is based on an earlier model for information security management model. The framework has been enhanced with the inclusion of combination of constructs and refined through the recalibration of cyber or ICT security management model to ensure that potentially anomalous situations are prevented. The proposed framework is depicted as in Figure 1.

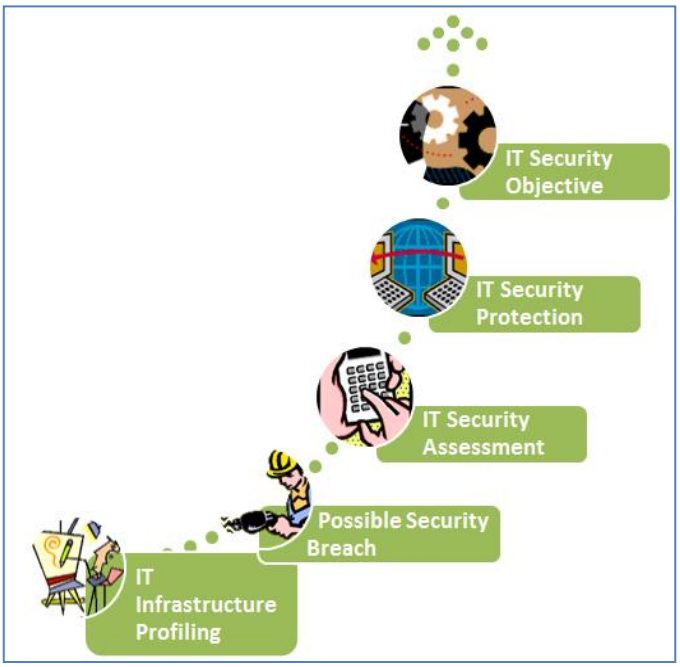

Figure 1. Proposed Cyber Security Maintenance Framework

CONCLUSION

Actually, a novel conceptual framework of the security maintenance had proposed to make any ICT infrastructures and services that follow those guidelines will accessible properly and secure by any authorized peoples. However, there are no security aspects had been discuss in details for ICT services and infrastructure's maintenance. Then, the documentation had been provided as a manual access which is needs to follow the guidelines.

Now days, security should be concern in any ICT services and infrastructures including in any proposed maintenance model and guidelines. Then, its need overall coverage to make the guidelines become more effective and easy to use. Security maintenance is more important in cyber space for any organizations especially for ICT services and infrastructure usage in safe and secure manner.

REFERENCES

A. Vance, M. Siponen, S. Pahnila, Motivating IS security compliance: insights from habit and protection motivation theory, Inf. Manage. 49, 2012, pp. 190–198.

A.C. Kim, S.M. Lee, D.H. Lee, Compliance risk assessment measures of financial information security using system dynamics, Int. J. Secur. Appl. 6, 2012, pp. 191–200.

C. Melara, J.M. Sarriegui, J.J. Gonzalez, A. Sawicka, D.L. Cooke, A system dynamics model of an insider attack on an information system, in: J.J. Gonzalez (Ed.), From Modeling to Managing Security: a System Dynamics Approach, Norwegian Academic Press, Kristiansand, Norway, 2003, pp. 9–36.

J. Fonseca, M. Vieira and H. Madeira, "Evaluation of Web Security Mechanisms using Vulnerability and Attack Injection," IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1-1, 2013.

K.H. Guo, Y. Yuan, The effects of multilevel sanctions on information security violations: a mediating model, Inf. Manage. 49, 2012, pp. 320–326.

Tripathi A, Singh UK. Taxonomic analysis of classification schemes in vulnerability databases. In: Computer sciences and convergence information technology (ICCIT), 2011 6th international conference on. IEEE; 2011. p. 686–91.

Firkhan Ali Bin Hamid Ali
JTW,FSKTM
Universiti Tun Hussein Onn Malaysia, 8640000 Batu Pahat, Malaysia
Email: firkhan1977@yahoo.com

Mohd Zalisham Jali
Faculty of Science & Technology
Universiti Sains Islam Malaysia, 54000 Nilai, Malaysia
Email: zali@usim.edu.my