Cybersecurity Info Structure with a Human-Technology Focus

Firkhan Ali Hamid Ali and Mohd Zalisham Jali

Fakulti Sains Komputer & Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
Fakulti Sains & Teknologi, Universiti Sains Islam Malaysia, Nilai, Malaysia

firkhan@uthm.edu.my, zali@usim.edu.my

Abstract. Web application security, infrastructure service security management, cyber security, and security technologies will revolutionize how businesses conduct business and share information in the twenty-first century. The performance of data security in web and application, scalability of infrastructure, secure mobile adaptation, secure service integration, energy efficiency, security management, and many other issues are still being researched in the area of security issues in cyberinfrastructures, information, web applications, software, and industry 4.0. On the other hand, if new requirements emerge throughout time as a result of a mix of technology and human factors, security concerns will inevitably increase in order to maintain integrity.

Keywords: Cyber security, security management, info structure.

INTRODUCTION

Some medium-sized firms are unsure about what should be done with the ICT infrastructure due to the Information Communication Technology (ICT) infrastructure's rapid growth in creating a wide range of computer products. Tragically, the organization's infrastructure purchases—particularly its ICT security infrastructure—were either underutilized or never deployed at all. This ambiguity is probably caused by a lack of control or because it does not appear to have clear advantages for organizational management and business operations.

In order to solve this challenge, it will be addressed what kind of ICT infrastructure medium-sized enterprises need. The mission and goals of the company must be taken into consideration while making plans for the ICT infrastructure, which must go beyond simply facilitating organization and commerce.

Planning for this should consider an organization's ICT requirements. Next, whether a business is for profit or provides social services, it aims to be implemented and run successfully for the prosperity of the organization.

ICT security maintenance is a crucial part of the ICT infrastructure since it allows for the early detection of any flaws that could lead to security breaches in some businesses. The preservation of security in IT services and infrastructure has also given rise to some important problems, which are currently seen as major roadblocks to their quick and widespread adoption. Security, integration, and dependable performance were among the top issues raised by CIOs in a survey conducted by IDC in 2008 and 2009 [1].

The confidentiality of their information and culpability for incidents affecting the infrastructure are important issues for SMBs transitioning to the ICT service or infrastructure, according to an ENISA (European Network and Security Administration) survey of Small and Medium Businesses (SMBs) [2]. This makes sense given that each of these elements has a significant impact on the bottom line of the company.

Similar to this, the availability of a platform for ICT services with high performance depends greatly on network quality, particularly round trip latency or delay [1]. Security is a major issue since organizations must maintain the confidentiality, integrity, authenticity, and audit ability of their data, tools, and transactions in order to remain operational, legal, and competitive. This requirement is crucial for all users, particularly for maintaining overall security in IT services and infrastructure.

LITERATURE REVIEW

A management model like the ISO network management model must be used for the management of operational security maintenance in ICT infrastructure. The International Organization for Standardization created the ISO network management model, which consists of five functional areas of network administration (ISO). It offers a design standard for implementing network management tools and technologies in the future. Performance management, configuration management, accounting management, fault management, and security management make up the five functional areas of network management.

In order to make a network run more effectively, performance management functions in the ISO network management model include monitoring, evaluating, and reviewing the available bandwidth and network consumption of resources. The ISO network management model includes performance management, which is crucial for ICT infrastructure that seeks to improve network performance in businesses.

The objective of the configuration management functions in the ISO network management model is to keep track of network and system configuration data in order to track and manage how different hardware and software versions affect network performance. Aspects of network device setup including configuration file management, inventory management, and software management will be centrally observed.

The procedure for assessing network utilization characteristics in the ISO network management model is called accounting management functions. This allows an individual or group users on the network to be suitably regulated for the purposes of accounting or chargeback. Measuring the use of all significant network resources is the first step toward effective accounting management, just like performance management. In this area of network management, clients are typically charged by Internet service providers for the resources they utilize.

The management of faults according to the ISO network management model is comparable to how most people believe the administration should manage the network. This network management function's objective is to locate, identify, and notify system administrators of issues that can impair system performance. To maintain the network functioning properly, it must then automatically resolve network issues as they arise. Fault management is likely the most extensively used kind of ISO network management since any errors might result in downtime or unacceptable network degradation.

The aim of security administration According to local regulations, the ISO network management model controls access to network resources to prevent purposeful or unintentional network sabotage. It appears that the implementation of a security management subsystem can monitor users attempting to access a network resource and deny access to those who submit improper access codes. Access to resources is managed using security measures. Then, if any resources are available, inform the appropriate authorities. Similar to a network administrator or email outsourcing, management systems can access the network to transmit notifications when certain files, routers, or servers go down.

METHODOLOGY

The experimental information technology technique will serve as the foundation for the methodology of the proposed study. The study work is examined using this methodology to illustrate the importance of proof-of-concept and proof-of-performance.

A few crucial actions were taken in order to show the proof-of-concept. Before establishing a legitimate research challenge, a thorough examination of the security maintenance research field is conducted first. The security maintenance framework is then created and analytically analyzed as a novel model. This comprises developing the system for controlling the security model, procedures, and metrics related to the application of security maintenance.

The proposed security model, processes, and metrics are integrated inside a novel conceptual framework for security maintenance in IT infrastructure to show proof of performance. It will then be evaluated using the suggested framework. The viability of the proposed solutions in comparison to other comparable baseline solutions was examined and demonstrated using a variety of parameters and workloads in the proposed framework. Additionally, a quantitative examination of a few suggested security indicators is carried out to assess their accuracy.

The major phases of the research are separated into three categories specifically:

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

IMPEMENTATION

An organization might have higher faith in the level of security it is offering for its information assets after the successful implementation and testing of a new and better security profile [3]. A significant amount of time has elapsed by the time the business has finished putting the modifications required by an improved security program into place.

Everything that is dynamic in the environment of the organization has changed throughout that period [3]. The following are some of the information security environment's factors that could change:

- 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.

It could be required to start the cycle over if the software is not responding to changes in a sufficient manner. This choice is based on the degree of change that has taken place and the adaptability of the organization's information security maintenance program [3]. The security program can probably continue to adapt successfully if a company can successfully deal with change and has developed policies and processes that can evolve with the environment.

The chief information security officer (CISO) decides whether the information security group can adjust appropriately and maintain the organization's information security profile or whether the SecSDLC (Security System Development Life Cycle) macro process must begin anew to redevelop a fundamentally new information security profile.

When an information security program is developed and put into place to deal with change, it is less expensive and more efficient [3]. Reengineering the information security profile repeatedly costs additional money.

To manage and run an ongoing security program, a management model must be adopted [4]. Models are organizational frameworks for managing a specific set of tasks or business functions [5]. A management model must be created to help the information security community manage and run the ongoing security program [6]. Management models are often frameworks that organize the duties involved in overseeing a specific range of activities or commercial operations.

A maintenance model is created to support the selected management model and concentrate organizational effort on maintenance. The maintenance discussion that follows is organized around the diagram in figure 1 that depicts an entire maintenance program.

- External monitoring
- Internal monitoring
- Planning and risk assessment
- Vulnerability assessment and remediation
- Readiness and review

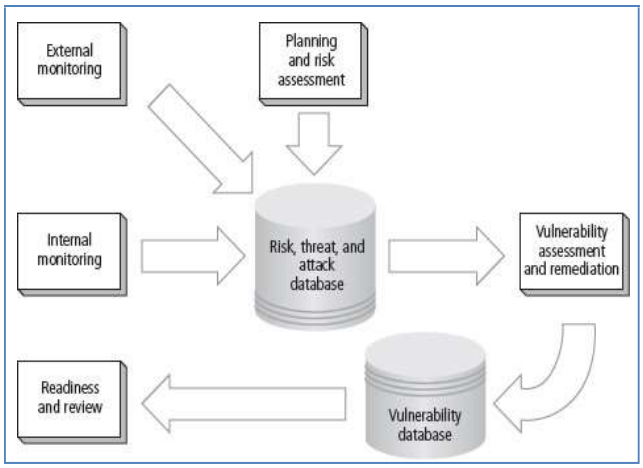

FIGURE 1. The Model of Maintenance

The proposed conceptual framework for security maintenance in mid-size IT infrastructure represents as a combination of the IT security management models and concepts spanning various areas of information security operations. The framework focuses on a number of topics, including software vulnerability, risk assessment, attack motivation, threat detection, deterrence, and security aim [7]. It has as its foundation a previous information security management approach. The framework has been improved by the incorporation of a number of constructs and modified through the recalibration of the IT security management model to ensure that potentially abnormal situations are avoided. Figure 2 illustrates the suggested framework.

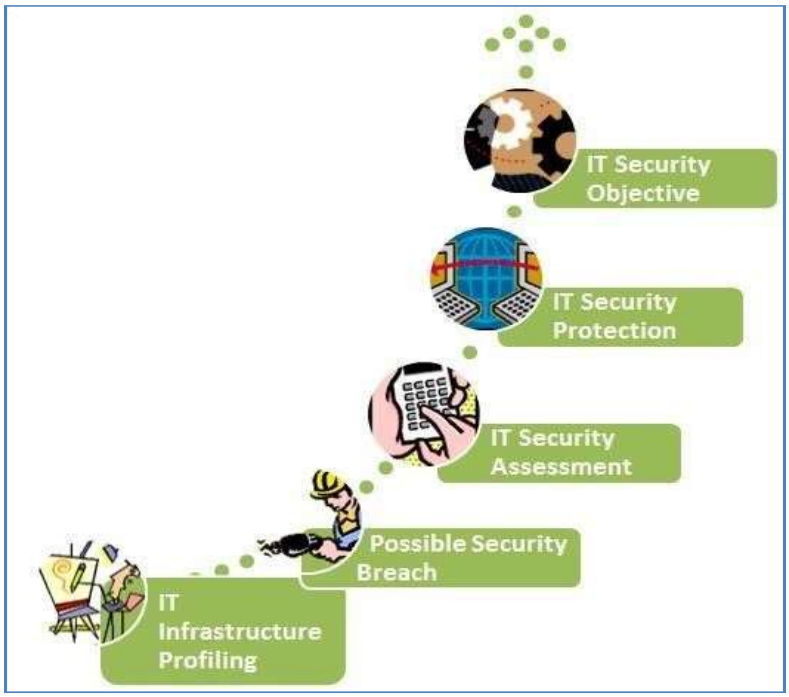

FIGURE 2. Framework for Proposed IT Security Maintenance

CONCLUSION

This gives the necessary background information and supporting data to build a security maintenance model for ICT infrastructure after reviewing information security management. Since ISO 27001 has not been widely adopted, the development of Information Security Management Systems (ISMS) has a lengthy history in all organizations [8]. Smaller businesses are undoubtedly prevented from adopting the standard by the high time and financial expenses of ISMS deployment.

In fact, a fresh conceptual framework for security maintenance has suggested making any IT infrastructures and services that adhere to those standards appropriately accessible and secure to all authorized individuals. For the upkeep of IT services and infrastructure, however, no security-related issues have been covered in detail. Next, manual access to the documents was made available, and this access must adhere to the rules.

In today's world, security concerns should be present in all IT services and infrastructures, as well as in any suggested maintenance models and procedures. Then, comprehensive coverage is required to make the rules more useful and simple to follow. For every firm using IT services and infrastructure in a safe and secure manner, security upkeep is crucial in cyberspace.

ACKNOWLEDGMENTS

Thanks to the FSKTM and Universiti Tun Hussein Onn Malaysia for supporting this paper.

REFERENCES

1. J. Fonseca, M. Vieira and H. Madeira. (2013). Evaluation of Web Security Mechanisms using Vulnerability and Attack Injection, *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1-1.
2. *Wooyun. wooyun, <http://www.wooyun.org/> [accessed 01.05.20].*
3. M.E. Whitman, H.J. Mattord. (2014). *Principles of Information Security*, fourth ed., Course Technology, Boston, MA.
4. M.A. Alnatheer. (2014). A Conceptual Model to Understand Information Security Culture, *Int. J. Soc. Sci. Hum.* 4, pp. 104–107.
5. J. May. (2008). *Analyzing the socio-organizational constructs for IS security within organizations*, in: S. Furnell, P. Dowland (Eds.), in: Proceedings of the 11th IFIP TC11. 1 Working Conference on Information Security Management, Richmond, VA, pp. 103–118.
6. K.H. Guo, Y. Yuan. (2012). The effects of multilevel sanctions on information security violations: a mediating model, *Inf. Manage*. 49, pp. 320–326.
7. S.-C. Yang, Y.-L. Wang. (2011). Insider threat analysis of case based system dynamics, *Adv. Comput*. 2, pp. 1–17.
8. A.C. Kim, S.M. Lee, D.H. Lee. (2012). Compliance risk assessment measures of financial information security using system dynamics, *Int. J. Secur. Appl.* 6, pp. 191–200.