International Journal of Information Technology and Education (IJITE)
Volume 1, Number 1, December 2021

Analysis of Information Security Management Systems at University

Bierhoff Parengkuan, Kenny Tatauhe , Fanny Worotijan
Department of Information Technology and Communication Education, Universitas Negeri Manado, Tondano, 95618

Corresponding author: bierparengkuan@gmail.com

Abstract

One of the keys to the success of securing information systems is the vision and commitment of top management leaders. Security efforts or initiatives would be meaningless without them. In the absence of commitment from top management, the impact on data security investment. In addition, success is also determined such as the process of design, implementation, configuration, and use. For this reason, adequate standards and management are needed so that security can be carried out adequately. Competency standards can be carried out in accordance with TKTI if using National standards. Competency standards do not mean only the ability to complete a task, but are also based on how and why the task is done. In addition, the ISO standard which is an international standard can be applied using ISO 17799. Security operations management must fulfill several important things, namely control and protection, monitoring and auditing, as well as an understanding of threats and vulnerabilities.

Keywords: SKMI, SOP, ISO 17799, Information Security, UNIMA

Introduction

Computer security issues are always interesting to discuss, this is because of the development of increasingly sophisticated and widespread information technology. Increasingly sophisticated information technology is sometimes not followed by the application of adequate security, so that security threats are always a scourge for the implementation of computer systems in an organization or company. One of the keys to the success of securing information systems is the vision and commitment of top management leaders. Security efforts or initiatives would be meaningless without them. In the absence of commitment from top management, the impact on data security investment. Data security cannot just grow without effort and expense. Electronic data security requires investment, without investment data security efforts will be in vain. Unfortunately this is often overlooked due to the lack of commitment from the management for security solutions.

Method

This study uses a qualitative research model. Qualitative research aims to obtain a complete picture of a matter according to human perspective under study. Qualitative research deals with ideas,

perceptions, opinions, or beliefs of the person being studied; everyone cannot be measured by numbers.

Results and Discussion

Design errors occur at the design stage where security is often overlooked or after thought. For example, there is an information system that assumes that the operating system will be safe and the network will be safe so that there is no design for data security, for example by using encryption.

Implementation errors occur when the design is implemented into an application or system. The information system is implemented using software. Unfortunately software developers often do not have knowledge about security so that the applications developed have many security holes that can be exploited.

A configuration error occurred at the operational stage. The system used should usually be configured according to company policy. In addition to misconfiguration, there are also problems caused by the absence of procedural policies from the system owner, making it difficult for managers to make restrictions. Usage errors occur at the operational stage as well. Sometimes because the system is too complex while the available resources are very limited, there may be errors in usage.

The errors above can lead to security holes. This loophole does not necessarily cause problems, because there may be a gap but no exploitation occurs. However, this loophole is a risk that must be controlled in a security management.

Computer Security Standard

1. Security Competency Standards according to TKTI.

Competency standards are defined as a measure or benchmark of knowledge, skills, and work attitudes that must be possessed by someone to do a job or task in accordance with the performance required by the Indonesian Telematics Coordination Team (TKTI, 2004). Competency standards do not mean only the ability to complete a task, but are also based on how and why the task is done. Based on the type of group of Human Resources (HR) in information and communication technology (ICT) and their competencies, which relate to computer security and maintenance, are :

a. Competency unit no. 16.
   Unit Title : Describing Precautions Against Information Security
   Unit Description: This unit of competence deals with understanding the principles of information security in order to increase awareness of information security. in the form of :
   - o General Information Security Rules
   - o Password Selection and Use
   - o Identification of Security Risks Over Internet Use
   - o Safe Management of Data/Information

b. Competency unit no. 17
Unit Title : Using Anti Virus Software
Unit Description : This unit of competence deals with the use of anti-virus software that is commonly used with the aim of protecting computers from various types of standard viruses that can spread on our computers. in the form of :
- o Identify the type of virus
- o Preparing Anti Virus Software to run.
- o Operate anti-virus software
- o Take precautions

c. Competency unit no. 20
Unit Title : Perform initial handling (Troubleshooting) for problems on the PC
Unit Description: This unit of competency relates to an understanding of how a computer (PC) works and how to handle it if the computer cannot work. in the form of :
- o How Computers Work
- o Computer Component Installation
- o Use of Problem Detection Tools
- o Troubleshooting and Troubleshooting

d. Competency unit no. 21
Unit Title : Operate basic utilities for Backup, Restore, Data Recovery
Unit Description: This unit of competence deals with the basic steps in securing electronic data in the computer owned. in the form of :
- o Identify and describe aspects of data security
- o Protect data on computer from distraction
- o Performing Data Reovery

e. Competency unit no. 24
Unit Title : Implementing a security and safety system in computer operation
Unit Description: This unit of competency relates to the mastery of the basic concepts of computer system security that must be made to ensure the security of the computer system used. in the form of :
- o Identifying Security Threats
- o Basic Computer Security Standards

2. Security Management according to ISO 17799
ISO (International Standards Organization) is an international standard-setting body consisting of representatives from the national standards bodies of each country. ISO sets the world's industrial and commercial standards. The ISO 17799 standard is an information security management system standard that has been refined and implemented for use by companies in securing their data or information. With the ISO 17799 standard, we will be able to measure whether the information security system that we have implemented is effective and provides security guarantees to consumers.

Prior to the introduction of ISO 17799, in 1995, the British Standards Institute (BSI) launched the first standard on information management worldwide, namely "B 7799", Part One: Code of Practice for Security Management Information, which is based on Basic infrastructure B 7799. Then on December 1, 2000, a new ISO 17799 standard on information management was published.

The use of the ISO 17799 standard includes the need for the following :

- Information security policy documents
- Responsible for information security
- Information security education and training programs exist for all users
- Develop a system for reporting security events
- Introducing virus control techniques
- Develop a business continuity plan
- Controlling copying of proprietary software
- Cover letter of organizational archives to follow data protection needs,
- Establish procedures for complying with security policies.

Meanwhile, the control or control policies according to the ISO 17799 standard include: security policies, security organization, asset classification and control, personnel security, physical security and environmental control, computer network development and management, access control systems, system maintenance, business continuity planning, and compliance. . In order to minimize the risk of security threats that harm the business, these problems must be handled using a preventive action without having to wait in an emergency to take security actions. In order to be proactive towards security needs, the security architecture includes three main elements :

The company's policy is management involvement in resource allocation and a strategic vision and global issues in security, individual behavior (employee training, and the existence of a communication process).

In the ISO 17799 standard, an effective and efficient information security management system will provide guidance for companies or organizations to :

- Constantly update (update) on new threats and take action with systematic consideration.
- Handling accidents and losses with preventive measures and continuous improvement of system security.
- Knowing when policies and procedures are not adequately implemented in an effort to prevent security threats.
- Implement policies and procedures regarding the importance of security management, following "best practice procedures" and good risk management.

By recognizing the strategic value of information security management, a certification innovation plan can be offered, based on the BS7799-2:1999 certification plan and ISO17799 guidelines. Where the contents of ISO-17799 include: 10 control clauses, 36 control objectives, and 127 controls. These controls are described at a high level, without including technological issues in detail, in order to leave each company/organization totally free to choose those controls that are closest to their own cultural/technological situation and needs.

Security Functions in Organizations

Every IT security personnel (staff) must understand and implement management, operational and technical controls. Full implementation of all types of controls requires IT security staff with various skills. At one time the security team can act as a procurement specialist who reviews a specification of a system upgrade or then act as a teacher in an IT security awareness class.
In fact, in organizations with various tasks, the IT security team is often faced with a lack of resources or priority workloads to complete only the essential tasks. The functions discussed below contain the minimum number of staff required to complete these functions. This rate is calculated as a percentage of 1 staff a year.

a. audits.

Auditors are responsible for checking the system to see if it meets IT security requirements. Including organizational systems and policies, and whether IT security controls are in place.

b. Physical Security

In many organizations, this physical security section is generally a security staff in the form of a security unit (security guard). The physical security department is usually responsible for developing and maintaining sound physical security controls, in consultation with computer security management. program and functional managers, and others as needed.

c. Disaster Recovery/Contingency Planning

IT security staff must have a disaster recovery/contingency planning team. This team is responsible for the organization's contingency planning activities and works closely with the physical security, telecommunications, IRM, procurement and other employees.

d. Procurement

The procurement department is responsible for ensuring that the procurement of goods within the organization has been reviewed by authorized personnel.

e. Training

IT security training is included in IT security requirements. IT security staff has one of the main responsibilities to provide training to users, operators, and managers on computer security.

f. Human Resources (Personal)

Personnel and IT security staff must cooperate in conducting an investigation into the background and, termination procedures of an employee who wishes to resign.

g. Risk Management/Planning

Some organizations have staff tasked with studying the various types of risks that may be faced by the organization. IT security staff must develop processes to identify risks that exist in the life cycle of the organization. When a vulnerability is detected, the security team must analyze the risk and the amount of resources needed to mitigate the risk.

h. Building Operations

The building maintenance department is responsible for ensuring that every building security facility, electrical power and building environmental control, is safe to use during the organization's operational period.

i. System Management/System Administrators

These employees are managers and technicians who design and operate a system, computer network and LAN of the organization. They are responsible for implementing technical security and must be familiar with IT security technologies associated with their systems. They also need to ensure the continuity of their services in meeting the needs of functional managers, as well as analyze the weaknesses in the system.

j. Telecommunication

The telecommunications department is responsible for providing telecommunications services including voice telecommunications, data, video and fax services.

k. Help Desk

Whether or not the Help Desk handles each incident, it must be able to identify a security breach and forward the call to the appropriate authorities within the organization for a response. The IT security team must work closely with the help desk management to ensure that procedures are in place to deal with incidents related to IT security.

l. Maintenance of Security Program

The security program requires some additional activities that are not listed in the above functions. For each function area there should be a guide document for IT security staff and team. The document should be researched, written, reviewed and monitored on a regular basis.

Security Operations Management

In the use of information technology in every institution, especially those that prioritize information technology in its business processes, it requires an optimal operation to be able to support the ongoing business. When talking about operations, there are many things that can be involved, starting from hardware, software, procedures and human resources themselves to be able to carry out these operations. The dependence of each of the components above will determine the success of the operations carried out, but even with the success of operations with sophisticated technology without involving the security factor, everything becomes meaningless because any information or data produced from technology without security can be a disaster if you do not pay attention to confidentiality, integrity. and availability in general and security in particular so that any information held is truly treated as a valuable asset for the institution.

To ensure operational security, it is not only about protective technology, but also clear policies in carrying out operational security which is very important to be carried out properly because the highest threat in practice is from internal resources themselves. This is a threat that is actually very threatening and difficult to predict, because internal resources already exist in the system itself. In order to minimize this threat, a policy for operational security must be made in as much detail as possible, predicting things that can become threats, and carrying out security procedures consistently. So without good policies and procedures, it is not only threats from outside that are

scary but also threats from within. For this reason, each information technology division must have a policy for corporate users to use their information technology resources.

In this discussion, we will explain at least 3 big things that must be understood :

1. Control and Protection. Contains an understanding of regulation and protection in operational activities in order to achieve an optimal level of operational security, there are several things that must be considered, including preventive control, corrective control detective control, deterrent control, application control, transaction control and separation and rotation of duties which emphasizes more on confidentiality (confidentiality) and integrity or data integrity. All of the above also focuses more on optimal supervisory procedures in carrying out various things from prevention to good job rotation and if not done properly it will become a threat and open the door to security.

2. Monitoring and Auditing. After proper regulation and protection is carried out, it cannot only stop to be able to carry out protection, but monitoring and auditing is still needed to be able to find out and ensure the extent of security that has been achieved, the factors that must be considered are Change management, Escalation management, Record retention, Due diligence , and Logging monitoring. By doing the things above which are more procedural in nature, security supervision can be further improved.

3. Threats and Vulnerabilities. Contains an understanding of the types of threats and weaknesses that can threaten the security operations that have been carried out. For threats and vulnerabilities, several things that will be discussed are Accidental Loss, Inappropriate Activities, Illegal computer operations, Account maintenance, Data Scavenging Attacks, IPL/rebooting, and Network highjacking.

Conlusion

The implementation of a security system in an ideal organization must of course meet the standardization requirements in accordance with the provisions applicable to security system standards, both TKTI and ISO. However, given the limited resources in several small and medium-sized organizations or companies, some of the standards can be combined. However, the security principle must still fulfill the aspects that become security requirements, namely confidentiality, integrity and availability. To achieve this aspect, it is necessary to pay attention to several important things, namely the existence of control and protection, monitoring and auditing, as well as an understanding of threats and vulnerabilities.

References

Depkominfo, 2006, "*Pedoman Praktis manajemen Keamanan Informasi untuk Pimpinan Organisasi, 10 Rekomendasi Terbaik Manajemen Keamanan Informasi* ", Direktorat Sistem Informasi, Perangkat Lunak Dan Konten Direktorat Jenderal Aplikasi Telematika Departemen Komunikasi Dan Informatika

Budi Raharjo, 2005, "*Keamanan Sistem Informasi Berbasis Internet*", PT Insan Infonesia - Bandung & PT INDOCISC – Jakarta Internet

Gary Stoneburner, dkk, 2004, "*Computer Security:Engineering Principles For Information Technology Security (Baseline for Achieving Security), Revisian A*", NIST. 4. http://www.wikipedia.org

http://amutiara.files.wordpress.com/2007/01 /sp800-86.pdf

IEEE 802.11Working Group. http://grouper.ieee.org/groups/802/11/index. html.

NIST Special Pub. 800-86:, 2005, "*Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident*

Response (Draft) ", http://csrc.nist.gov/publications/drafts/DraftSP800-86.pdf.

J. R. Batmetan Suyoto, J. D. C. L. Suares, "An Empirical Investigation on Customer Behavior to Adopt Mobile Commerce among the Y Generation in Indonesia", Sriwijaya International Conference On Engineering, Science & Technology [SICEST 2016], 2016

J.R. Batmetan, "Algoritma Ant Colony Optimization (ACO) untuk Pemilihan Jalur Tercepat Evakuasi Bencana Gunung Lokon Sulawesi Utara", Jurnal Teknologi Informasi-AITI, 2016, vol.13, no.2, pp 31-48

L. Madeso, D. R. Kabo, J. R. Batmetan, " Rancang Bangun Sistem Pakar Penentuan Status Gizi Pada Balita Menggunakan Metode Forward Chainning", E-Jurnal UNSRIT, vol.2

J. R. Batmetan, V. R. Palilingan, " Higher Education Students' Behaviour to Adopt Mobile Learning", IOP Conference Series: Materials Science and Engineering, 2018, vol. 306, Issue 1, pp. 012110 (2018)

V. R. Palilingan, J. R. Batmetan, " Incident Management in Academic Information System using ITIL Framework", IOP Conference Series: Materials Science and Engineering, 2018, vol. 306, Issue 1, pp. 012110 (2018)

J. R. Batmetan, A. J. Santoso, Pranowo, " A Multiple-Objective Ant Colony Algorithm for Optimizing Disaster Relief Logistics", Advanced Science Letters, 2017, vol.23, no.3, pp. 2344-2347

M. L. Tompodung, F. Supit, J. R. Batmetan, " Rancang Bangun Aplikasi Sensus Penduduk Berbasis Android", Buletin Sariputra, 2017, vol.7, pp. 57-61

J. R. Batmetan, " Optimasi Strategi Smart Environment Dalam Mitigasi Bencana Menggunakan Multi-Objective Aco (Mo-Aco) Algorithm", Pasca Sarjana Magister Teknik Informatika Universitas Atma Jaya Yogyakarta, 2016