VOL. 9, NO. 12, DECEMBER 2014 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

SECURITY RISK MANAGEMENT AT THE COMPUTER CENTER OF X UNIVERSITY

Ibnu Gunawan, Agustinus Noertjahyana and Hartanto Rusli
Department of Informatics Engineering, Faculty of Industrial Technology, Petra Christian University, Surabaya, Indonesia
E-Mail: ibnu@petra.ac.id

ABSTRACT

The process of teaching and learning in an information technology based university cannot be separated from the accompanying information technology security risks. For that purpose, we need a risk analysis based on risk management standards that have been widely accepted and commonly used, such as NIST SP 800-30. The performed risk analysis is based on 10 domains of CISSP. So, there is synergy between the two standards that we employed. Besides, the synergy also occurs between the information technology security risks and the teaching and learning process. This paper presents how to create a questionnaire-based assessment of CISSP's 10 domains mapped into NIST SP 800-30. In addition, this paper elaborates how the assessment of the questionnaires was executed and the result produced for X University. The research outputs that we generate are: a questionnaire-based assessment mapping CISSP's 10 domains into NIST SP 800-30, the ten major security risks that we discovered at the Computer Center of X University and the risk response planning to mitigate the discovered security risks.

Keywords: NIST SP 800-30, CISSP, security, risk, assessment, mapping, information technology.

INTRODUCTORY

In carrying out operations based on information technology, especially with the use of a computer network infrastructure, organizations not only need to have a good information system, but also need to consider the safety factors to assure the reliability of the information system. Secure communication network is absolutely necessary to enable the organization to provide continuous service to its members. The need for this security system must be clearly defined and may ultimately be implemented to support operations in the organization's information system. By applying the appropriate procedures for each activity, we can decide the right security needs in accordance with the organization's requirements [1].

To be able to build a security policy that provides a good foundation in the future, the first step is to create a security policy that can reduce the risk of misuse of the resources available in the organization [2].

Most of the staff involved in the creation of this security policy felt confused in the beginning; because they did not have enough experience nor did they see it necessary as no security incident ever happened before.

X University has grown in the past years and so has the various kinds of information systems running their operations. With the increasing number of systems, there is an increasing need to have the security policy in place.

This paper describes how to assess the Operational Security Management at the Computer Center of X University by applying risk management with CISSP knowledge.

RISK MANAGEMENT

The scope of risk management processes, as defined in NIST Special Publication 800-30, is very broad. Risk Management processes include: (i) Risk Mapping; (ii) Risk Assessment; (iii) Responding to Risk; and (iv) Risk Monitoring. The information and communication flow is essential to make the process effective.

The first component of risk management process deals with how the organization maps the risks or forms the context of risks that describes the environment in which risk-based decisions are made. The purpose of the risk mapping is to produce a risk management strategy that addresses how the organization intends to assess risks, respond to risks, and monitor risks. By doing this, the organization makes explicit and transparent risk perception that can be used in making investment and operational decisions.

Risk management strategies build a foundation for managing risk and describe the boundaries for risk decisions in the organization.

The second component of risk management process deals with how the organization assesses risks in the context of organizational risk framework.

The third component of risk management process addresses how the organization responds to the risks resulting from the risk assessment.

The fourth component of risk management process addresses how the organization monitors risks over time [3]. In order to monitor risks over time, we can use the technical control from Stoneburner [8] shown in Figure-1. There are four main areas defined in the technical control, i.e., identification, cryptographic key management, security administration, and system protection.

CISSP

CISSP (Certified Information System Security Professional) is a certification in the field of information security [4]. In accordance with the current global progress, the need for security and its development in the field of information technology continues to evolve. Safety first is a hot issue in the technology alone, but now

has become part of our daily lives. Information system security is essential to any organization, whether it is a government agency, a corporation, or even a military unit.

CISSP itself divides the definition of security in 10 domains. The ten domains are deemed to include all parts of computer, network, business, and security information. The CISSP's ten domains are as follows:

Domain 1: Information Security Governance and Risk Management

This domain examines enterprise asset identification, the proper way to determine the necessary level of protection required, and what kind of budget to develop for security implementation, with the goal of reducing the threat and financial loss. Some topics covered include [5]:

- Data classification
- Policies, procedures, standards, and guidelines
- Risk assessment and management
- Security personnel, training, and awareness

Domain 2: Access control

This domain discusses the mechanisms and methods used to enable administrators and managers to control what subjects can access, the extent of their abilities after authorization and authentication, and auditing and monitoring of these activities. Some of the topics covered include:

- Access control security model
- Identification and authentication technology
- Administration of access control
- Single sign-on technology
- Methods of attack

Domain 3: Cryptography

This domain discusses methods and techniques to disguise the data for the purpose of protection. This involves cryptographic techniques, approaches, and technologies. Some of the topics covered include:

- Symmetric and asymmetric algorithms and their usage
- Public Key Infrastructure (PKI) and the hashing function
- The encryption protocol and implementation
- Methods of attack

Domain 4: Physical (Environmental) Security

This domain discusses the threats, risks, and actions to protect the facilities, hardware, data, media, and personnel. It involves choosing the facility, authorized entry methods, and environmental and safety procedures. Some of the topics covered include:

- The area borders, authorization methods, and control
- Motion detectors, sensors, and alarms
- Intrusion detection
- Detection and prevention of the occurrence of fire
- Fencing, security guards, and the type of security badges

Domain 5: Security Architecture and Design

This domain discusses the concepts, principles, and standards to design and implement secure applications, operating systems, and systems. This includes the measurement of international security standards and their meanings for different types of platforms. Some of the topics covered include:

- Operating states, kernel functions, and memory mapping
- Enterprise architecture
- Security models, architectures, and evaluations
- Evaluation criteria: Trusted Computer Security
- Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), and Common Criteria
- Common flaws in applications and systems
- Certification and accreditation

Domain 6: Business Continuity and Disaster Recovery Plan

This domain examines the preservation of business activities when faced with a disruption or disaster. It involves the identification of real risks, proper risk assessment and mitigation implementation. Some of the topics covered include:

- Identification of business resources and value assignment
- Business impact analysis and predictions for possible losses
- Priority units and crisis management
- Plan development, implementation, and maintenance

Domain 7: Telecommunications and Network Security

This domain discusses internal, external, public, and private communications systems, network structures, devices, protocols, and remote access and administration. Some topics covered include:

- OSI model and the layers
- Local Area Network (LAN) technology
- Metropolitan Area Network (MAN) and Wide Area Network (WAN)
- Internet, intranet, and extranet issues
- Virtual Private Networks (VPN), firewall, routers, bridges, and repeaters
- Network topology and cabling
- Attack methods

Domain 8: Application Development Security

This domain discusses the security component of the operating system and applications and how to best develop and measure their effectiveness. It looks at the software life cycle, change control, and security applications. Some of the topics covered include:

- Data warehousing and data mining
- Various development practices and their risks
- Software components and vulnerabilities
- The malicious code

Domain 9: Operations Security

This domain discusses control over the personnel, hardware, systems, and auditing and monitoring techniques. It also includes the possibilities of misuse of the channel and how to recognize and overcome them. Some of the topics covered include:

- Administrative responsibilities related to personnel and job functions
- Maintenance concept, antivirus, training, auditing, and resource protection activities
- Preventive, detective, corrective, and recovery controls
- Standards, suitability, and the concept of precision
- Security and fault tolerance technology

Domain 10: Legal, Regulations, Investigation, and Compliance

This domain addresses computer crime, laws, and regulations. It includes techniques for investigating crimes, collecting evidence, and handling procedures. It also covers how to develop and implement an incident management program [6]. Some of the topics covered include:

- Type of the laws, regulations, and crime
- Licensing and software piracy
- Legal and export/import issue
- Type of evidence and the receipt to court
- Incident handling

REQUIREMENT ANALYSIS

X University has been growing more rapidly since it asserted its mission as an "IT-based campus", which means to use information technology more prevalently not only among faculty and staff but also among the students. For examples, the university has developed a personnel information system for managing staff matters, lecturers can enter students' grades online, students can submit their study plans through the online academic system as well, and many other support systems.

The prevalent IT uses cause a few problems. Although the above-mentioned systems are diverse, they often need to exchange data. Due to different policies among departments, a variety of data exchange protocols exist among the systems. In addition, every personnel and/or student uses the same account (i.e., username and password) for logging in. Therefore, there are needs for a security policy.

Given the problems, it is necessary to analyze the IT risks that can impact the operations of X University. Doing this risk analysis, particularly at the University's Computer Center, we may identify the risks that could happen, measure their impacts, estimate the likelihood of each risk, and finally, calculate the risk exposure.

Applying the risk analysis at the Computer Center can handle most of the problems occurring and also enforce the policies resulting from the risk calculation. Thus, the security of most systems in the University can be assured and well monitored.

The challenge is to map CISSP standards to risk management standard in order to create a questionnaire for capturing the true characteristics of the existing policies at the University's Computer Center [7].

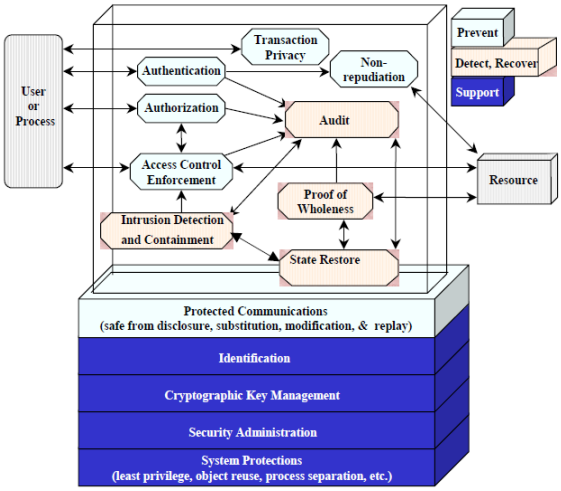

Figure-1. Technical control [8].

RISK ANALYSIS

Here is an example of a questionnaire - resulting from mapping CISSP standards to risk management standard - which we apply to some of the existing policies (i.e., some are for system users and others for system administrators) at the University's Computer Center.

User Questionnaire sample:

1. Access Control

Question 1. How often do you change your email password?

a. once a month b. 3 months c. once a year d. never

2. Security Architecture and Design

Question 11. In your opinion, how is the quality (i.e., specifications) of the computers provided by the Computer Center?

a. sufficient b. mediocre c. less worthy

3. Physical and Environmental Security

Question 15. How do you think the security and safety measures (such as placement of electrical wiring, placement of personnel, and fire safety) in the Computer Center?

a. bad b. good c. very good

4. Telecommunications and Network Security

Question 20. Do you know IP address version 6?
a. yes b. no

5. Cryptography

Question 30. Does your password consist of a combination of small and capital letters, contain numbers, and fulfill other requirements?
a. yes b. no

6. Business Continuity and Disaster Recovery Planning

Question 32. In the event of a power failure, are the lights back on immediately?
a. yes b. no

7. Legal, Regulations, Investigations, and Compliance

Question 35. Have you ever utilized the software licenses provided by the Computer Center, such as CD-Keys for Windows and other applications?
a. yes b. no

8. Software Development Security

Question 39. How is the quality of the software provided by the Computer Center?
a. excellent b. fine (errors are rare) c. poor (errors are frequent).

9. Operations Security

Question 41. How often is your removable drive (e.g., USB flash disk, portable disk) infected with viruses caused by accessing the computers in the Computer Center?
a. often b. rarely c. never

System Administrator Questionnaire sample:

1. Access Control

Question 6. How many times would be tolerated for user authentication errors?
a. 3 times b. 5 times c. 10 times d. no restrictions

2. Security Architecture and Design

Question 11. Is there a certain standard of maintenance for the computers in the Computer Center?
a. yes (please state it: .....) b. no c. do not know

3. Physical and Environmental Security

Question 16. How often are the air conditioners (AC) in the Computer Center and the server rooms being serviced?
a. once a month b. once every 3 months c. once a year d. never

4. Telecommunications and Network Security

Question 29. Had the network connection in the University ever experienced down time?
a. yes, ... times b. never c. do not know

5. Cryptography

Question 37. Is there a standard encryption method applied to the document storage?
a. yes b. no c. do not know

6. Business Continuity and Disaster Recovery Planning

Question 39. In the aftermath of a business disruption incident, are the steps of Business Impact Analysis (BIA) being carried out?
a. yes b. no c. do not know

7. Legal, Regulations, Investigations, and Compliance

Question 52. Is software used by the Computer Center protected from SQL Injection?
a. yes b. no c. do not know

8. Software Development Security

Question 62. Are confidential documents destroyed after use?
a. yes b. no c. do not know

Some of the results can be seen in Figure-2.

No.	Soal	Percentage Score	Likelihood
1	How often do you change your email password		
	A month	0	0
	3 month	2	0
	A year	21	2
	never	77	8
2	Do you log out after use email and the web service (sim.xxx.ac.id) University?		
	Yes	70	8
	Sometimes	18	2
	never	12	0
3	Is University X service that is easy you access the website?		
	easy	55	5
	sometimes	41	5
	hard	4	0
4	Is there any process other than password authentication when you login? (example: after entering the password, you will be asked to fill out a captcha or pin)		
	Yes	9	0
	no	73	8

Figure-2. Example of risk analysis questionnaire result.

RESULT

In this section, we discuss the calculation method of the Security Risk Management. The implementation of the calculation is divided into two parts, namely the implementation of risk assessment and the implementation of risk mitigation (including suggestions and explanations).

We calculate the impact using the NIST standard SP800-30 Revision 1. This standard is widely accepted as a methodology for calculating risks in Information Technology field, as we have successfully used it before for calculating RFID risks [9]. The risk level of each risk item is determined by multiplying likelihood and impact. For example, kindly refer to Table-1.

Table-1. Likelihood assessment questionnaire.

	Probability (%)	Convert (Likelihood)	Impact	Score	Risk Level
Information Security Goverment and Risk Management					
1. Is Computer Center has a Risk Management Team? His job to document the risk assessment process and procedures, mitigate risk, and so the most cost-effective manner.					
a. Yes.	0	0	0	0	*Moderate*
b. No	100	10	5	50	
2. Are assets in the Computer Center has been assessed?					
a. Yes.	20	2	0	0	*Low*
b. No	80	8	2	16	

After we assess all the risks that may happen, we continue with the risk response planning process.

The analysis of the risk assessment yields that there are ten (10) high risk items, which are most likely to have a major impact on the security of the systems. They are as follows (one of them is shown in Figure-2):

- The Computer Center has not yet had a dedicated team to deal with IT security risks facing the Computer Center (Risk Management Team).
- Access Control in the Computer Center has not been using the defense-in-depth or commonly known as double protection, as a form of protection over external penetration.
- The Computer Center has not made a permanent policy on changing passwords periodically.
- The Computer Center has not fully implemented Intrusion Detection System (IDS) to improve access control security.
- The Computer Center also has not employed Intrusion Prevention System (IPS) to the fullest.
- There is no definitive standard (like Evaluation Criteria) in selecting the products that will be used in the Computer Center.
- Network or firewall security in the Computer Center is still vulnerable to attacks such as IP fragmentation or Teardrop Attack, because penetration testing is note regularly done by the Computer Center.
- Honeypot, which is a form of IPS, is not correctly implemented in the Computer Center.
- The Computer Center has not yet had a Business Continuity Management (BCM) to respond to a significant disaster.
- Services Website at the Computer Center has not been protected from attacks such as Cross Site Scripting (XSS).

RISK RESPONSE PLANNING

Risk Response Planning is a document describing how companies should deal with these risks. Responses for the two highest risks are as follows:

a) The Computer Center has not yet had a dedicated team to deal with IT security risks facing the Computer Center (Risk Management Team).
Response: Mitigate
The impacts are slowness in responding to new risks, business disruption, no clear procedures for risk assessment.

b) Access Control in the Computer Center has not been using the defense-in-depth or commonly known as double protection, as a form of protection over external penetration.
Response: Avoid
The impacts are certainly less secure control access security, compromised business processes, data vulnerable to account privacy leakage.

CONCLUSIONS

From the work that had been done, we can make some conclusions:

a) Resulting from the interviews with the System Administrators, there are some differences in their answers, and consequently in their knowledge, about the standard security procedure in the Computer Center. The Head of System Administrators, who is also the Chief of the Computer Center, is responsible for enforcing the work force safety standards in the Computer Center.

b) The existing security system is quite safe, but it still requires some actions to improve it. There are still a lot of vulnerabilities in several aspects, which we have identified in this research work.

c) This paper is an example of successful implementation of NIST SP 800-30 standard to calculate risks that have been identified by another information technology risk assessment standard. In other words, we can use it as a guideline to asses any risk in Information Technology.

ACKNOWLEDGMENT

This paper is the result of two years (2013-2015) research funded by DIKTI on programme named PHB (Program Hibah Bersaing).

REFERENCES

[1] Danchev Dancho. 2013. Building and Implementing a Successful Information Security Policy. Internet Software Marketing. Windows Security.com.

[2] Gunawan Ibnu. 2014. Analysis and Implementation of Operational Security Management on Computer Center at the University X. CCE 2014. Penang, Malaysia.

[3] National Institute of Standards and Technology. Attn: Computer Security Division, Information Technology Laboratory. Gaithersburg (September 2012) NIST SP800-30 Revision 1.

[4] Conrad Eric. 2011. Eleventh Hour CISSP Study Guide. Syngress, 2010.

[5] Haris Shon. 2010. All-in-One CISSP Exam Guide Fifth Edition.

[6] Haris Shon. 2013. All-in-One CISSP Exam Guide Sixth Edition.

[7] Miller C Lawrence. 2012. CISSP for dummies. For Dummies.

[8] Stoneburner Gary., Alice Goguen and Alexis Feringa. 2013. Risk Management Guide for Information Technology System. NIST Special Publication 800-30 rev1.

[9] Dewi Lily Puspa, Gunawan Ibnu. 2014. Risk Assessment in Securing Radio Frequency Identification (RFID) Systems: A Case Study on Petra Christian University Library. Jurnal Teknologi, UTM, 2014. Malaysia.