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


www.arpnjournals.com

INTERNET-BASED APPLICATIONS TO HELP DESIGN SECURITY SYSTEM IN THE ORGANIZATION

Agustinus Noertjahyana, Ibnu Gunawan and David Lawrence Kusuma
Siwalankerto 121-131, Surabaya, Indonesia
E-Mail: agust@petra.ac.id

ABSTRACT

This paper presents the results of research related to the development of the design of security systems in an organization. So many functions of management is done with the help of the internet. However, there is still many IT staff in organizations that do not pay attention to an important aspect of security. So that the IT staff is still focused on the development of applications that support operations, but have not thought about the need for a security system. IT staff are just beginning to realize how important the security system for the application when it attacks both from outside and within the organization. IT staff often do not know where to start to make a security system design. For those reasons, research on how to design a security system becomes a necessity for organizational IT staff to be able to take precautions against an attack that will appear later. The purpose of this research is to help IT staff to be able to design a security system from the planning phase, implementation phase, and phase control. This study uses a framework based on the 10 CISSP domains that will be implemented in an application. By applying CISSP framework into the application, the expected results of this research are useful to assist organizations in determining security priorities, the results are in the form of an application that contains the planning, implementation, and monitoring of any design project security system in the organization.

Keyword: CISSP, internet-based applications, security design.

BACKGROUND

In the operations of organizations that use information technology based on computer networks, it is necessary to take into account the security of data in information systems. Security has become one of the important factors in the sustainability of the organization's activities. The more complex the organization using information technology, the security system will become more important [1].

Common problems associated with security systems for examples: computer or laptop thefts, theft of data due to transmission lines that are less secure, data centers are not secure because there is no access control, no security policy in the organization, the data can be easily read by unauthorized, natural disasters, the development of applications that do not use the principle of security, and operational activities of the organization are not concerned with the security aspect.

Many organizations invest heavily to protect the existing system. However, problems often arise on how to do the planning, operational until the stage of evaluation of existing security systems.

Problems that arise are the IT staff often find it difficult to make a good security system design, ranging from planning, implementation to evaluation stage. Very rarely organizational policies related to the design of security systems. For that it is necessary to develop an application that able to map CISSP framework into a system, which is useful to overcome these problems.

This system will help IT staff in the planning of the security system, so that the IT staff is able to make the design of security systems within the organization from the planning phase, the operational phase and evaluation phase.

The expected result is the existence of a system that is able to provide support at the management level to determine what steps will be taken to improve the security system in the organization.

SECURITY PRINCIPLES

The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [2].

Information security must be supported by a reliable security system, because it has the goals:

Integrity - ensuring that the data has not changed and no damage.

Confidentiality - ensuring that the data is confidential so that the information can not be seen by unauthorized.

Availability - ensuring that information is accessible whenever needed.

Each organization has different priorities in determining the security used. Government, military, corporations, financial institutions, and hospitals focus on confidential information about their customers, financial status, products, and research [3].

Companies that focus on electronic commerce, the main focus on availability, so that when the system is down, will cause a loss for the company both financially and reputation.

Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers [3].

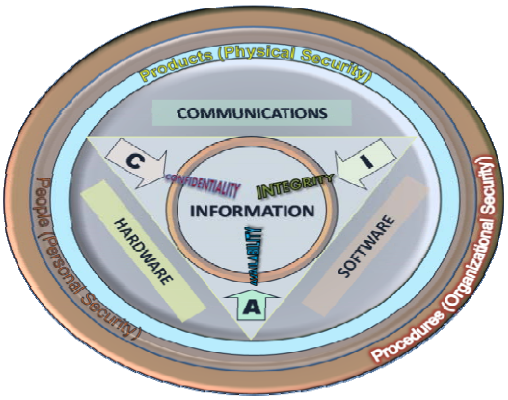

Figure-1. Relationship of Confidentiality, Integrity and availability.

SECURITY POLICY

Security policy is a plan that describes the important assets of the organization, and how to protect it [1]. The purpose of the Security policy is explain to the user what the assets are permitted and are not allowed to access. Documents must be clearly understood by the user in order to be able to understand the potential targets in the security system.

Security policy must meet the following requirements:

a) How sensitive information secured.
b) How to maintain username and password of each user.
c) How is the response to security incidents?
d) How to use a computer and internet connection securely.
e) How organizations use email correctly.

The procedure how to run a security policy is the security policy and what to do in case of violation of the security policy.

Here are some of the items included in the IT security policy:

1. Policies for the end user
   - The use of CD-ROMs and flash
   - Passwords
   - Backup Files
2. Policies for the Department
   - workplace safety procedures
   - Alarms
   - Knowledge of information systems
3. Policies for System Administrators
   - Procurement of hardware
   - Access Control
   - Computer Networks
   - Operating system (OS)
   - Software
   - Cyber crime
   - Backup Database
   - Local Area Network
   - Protection against viruses
4. Policies for Database Administrators
   - Transfer Procedure and data changes
   - Data Storage
   - Databases

INFORMATION SECURITY AWARENESS

Employees' information security awareness is an important part of an effective information security management program [4]. For the organization, the higher the level of staff awareness of the organization's security system, the security level of the organization will be higher.

CISSP

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the International Information Systems Security Certification Consortium, also known as (ISC) ².

Technological solutions alone cannot protect an organization's critical information assets. Employers demanding qualified information security staff give their organizations a leading edge by providing the highest standard of security for their customers', employees', stakeholders' and organizational information assets. (ISC)², the only not-for-profit body charged with maintaining, administering and certifying information security professionals via the compendium of industry best practices, the (ISC)² CBK®, is the premier resource for information security professionals worldwide [5].

CISSP certification helps companies to identify individuals who have the ability, knowledge, and experience necessary to implement good security practices, perform risk analysis, determine the necessary countermeasures, and helps organizations to protect facilities, networks, and information.

CISSP divides the definition of security in the 10 domains, as follows [6]:

a) Information Security Governance and Risk Management

Professional in the field of information security is capable of evaluating the risks of the organization's critical assets and use security systems to mitigate them. Many types of jobs such as firewall engineers, penetration testers and auditors have different risk and impact for any organization depends on the structure and needs of each organization.

Domain Information Security Governance and Risk Management focuses on risk analysis and mitigation of risks, which include security governance, or organizational structures needed for the success of information security programs. The difference between a successful organization and the failure is not related to

money and the number of staff, but using the right people in the right positions.

b) Access control

Domain Access Control focus on protection against unauthorized access, modification of data, and loss of confidentiality. Access Control can be achieved by applying the technique, physical, and strong administrative measure.

In Access Control, not only the term confidentiality, integrity and availability should be considered, but should consider of identification and authentication, authorization, and accountability [7].

Identification and authentication is required to prove that only the identity of the person who could legitimately have access to the system. Identity is weak because there is no evidence, and others can serve as a legitimate person to get into the system.

To prove that the only legitimate person who can get into the system, it would require an authentication process, which can be done by showing information such as a password or passport. Authorization describes the actions that can be performed by the system after passing through the phase of identification and authentication. This can be done with read, write, and execute files or programs.

Accountability keep users accountable for the actions that have been performed. This is usually done by analyzing the data logging and auditing. For some users, knowing that the data has been recorded is not enough to stated its responsibility but should be recorded and re-calibration at each specific time period.

c) Cryptography

Cryptography domain focuses on protection of confidentiality of information. Cryptography is a means to make a communication to be safe, because the information sent can only be understood by the sender and the recipient.

The purpose of cryptography is to provide protection if the information had been stolen by an unauthorized person, but can't get the information because the information is encrypted.

Encryption is a method of changing the data that can be read, called plain text, into a form that is random and can't be read, called cipher text. Plain text is a form that can be read by humans (documents) or engine (executable code), but once converted into cipher text, it can't be read by humans or machines. To be able to read the plaintext, it is necessary to process the decryption of the cipher text. This allows the transmission of confidential information over insecure channels.

d) Physical (Environmental) Security

Domain Physical (Environmental) Security focuses on the protection of the confidentiality, integrity, and availability of physical assets such as people, buildings, systems, and data. CISSP considers human safety as the most important concern in this domain. Domain Security perimeter helps prevent, detect, and correct physical access unauthorized entry. A building must use a layered defense. Important asset to be protected by physical security such as fences, doors, walls, locks, and so on.

e) Security Architecture and Design

Domain Security Architecture and Design focuses on the explanation of the logic, hardware, operating systems, and software security components and how to use it for designing and evaluating secure computer systems.

f) Business Continuity and Disaster Recovery Plan

Domain Business Continuity Planning and Disaster Recovery Planning (BCP / DRP) focuses on prevention against events such as illness, loss of life, natural disasters and the failure of the organization. Disaster is an inescapable fact of life. Referring to the threat of an event and a possible threat occurs, should be prevented / reduced by appropriate measures in the organization.

The purpose of BCP is to ensure that the business will continue to take place before, during, and after disasters, by providing long-term business strategy after the disturbing events occur.

Disaster Recovery Planning (DRP) provides short-term plan to disturbances arising, and typically relate to IT. DRP focuses on efficiency to reduce the impact of disasters and immediate response and recovery of critical IT systems. It is considered to be tactical rather than strategic because it provides a means to quickly respond to the disturbance.

g) Telecommunication and Network Security

Telecommunications and Network Security domain focus on the description of the design and architecture and secure communications network. This includes the selection of the appropriate network devices, the use of firewalls and Virtual Private Network.

h) Application Development Security

Domain Application Development Security focus on how to develop software correctly and securely. Software is everywhere, not only in computers, but in the home, car, and medical equipment. More complex the software, more errors that can occur. Developing reliable and secure software is very important. It can be started from the concept of good programming, the selection of appropriate methods of application development, testing and looking for software vulnerabilities.

i) Operations Security

Domain Security Operations focus on the threat to the production environment. Threats can come from internal or external to the organization. Internal threats often arise from employees who are not satisfied with the organization. Operations Security includes administrative security, Media Security, Continuity of Operations.

Administrative security provides ways to control access to operational data. Some aspects to consider are: Separation of Duties, Job Rotation, nondisclosure agreement, Background Checking, and Change Management.

Media Security about the process of handling the security of the media used by the organization. Some aspects to consider are: Storage and Media Sanitization or Destruction of data.

Continuity of Operations about the process of to ensure that the activities of the organization should continue under any circumstances. This can be done by a Service Level Agreement with outsiders, and fault tolerance on the design concept of each equipment.

j) Legal, Regulation, Investigation, dan Compliance

Domain Legal, Regulations, Investigation, and Compliance focus on some basic legal concepts that are important for all professionals in the field of information security, including intellectual property, and violation of privacy, but in some parts of the world, this concept is universal.

DESIGN AND IMPLEMENTATION

The design process of this research refers to the CISSP. Stages of implementation of this security system design are:

a) Choose Project

At this stage the administrator could choose an existing project or create a new project. The initial process will show 3 menu are: About, Projects, and the Choose Project. 'About Menu' featuring Team Software Developers 'Projects Menu' displays existing projects and Administrators can create new projects, and 'Choose Project' featuring a selection of existing projects. Design menu on the main page can be seen in Figure-2.

Figure-2. Home Menu.

After selecting the menu 'Project', it will display a list of projects that have been, or could choose to add the new project. An existing project can be renamed or deleted. The new project can be added by selecting the 'Add Project'. Menu 'Project' can be seen in Figure-3.

Figure-3. List of Existing Projects.

Selection of projects can be done by selecting the menu 'Choose Project', and will display the sub-menu option that can be seen in Figure-4. If the selected Project is a new project, the 'Operational', 'questionnaire', and 'Result' can't be selected before the Planning process is executed. This is an additional feature that can help the administrator to make the design process appropriate with the existing order.

Figure-4. Sub-Menu Choose Project.

b) Planning Process

This section helps administrators to plan for the needs of the system with reference to the CISSP standard. Each domain has given some standard so that the administrator can choose which suit the needs of the organization. Additional standards can be given by the Administrator if the organization requires one or more standards and yet in each domain, but still should be in the 10 CISSP domains.

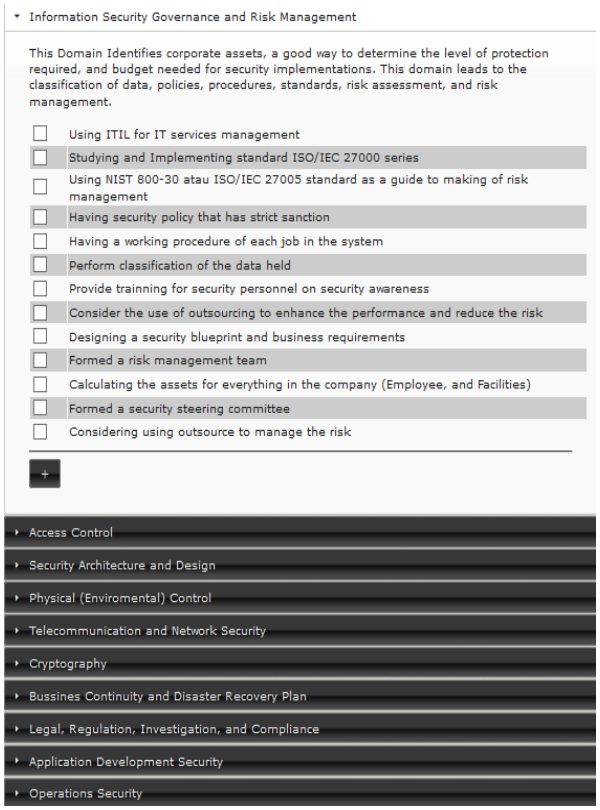

Figure-5. Display of Planning Process.

In Figure-5 displays the first domain: Information Security Governance and Risk Management. There are 13 standards in accordance with the standards of the CISSP but if the administrator wants to add another standard, can be done by pressing the '+' and the display will look like in Figure-6.

Figure-6. Adding Standard for Each Domain.

c) Operational Process

This section helps administrators by providing the risk of each chosen CISSP standards. Administrators can choose the best plan of each standard selected in accordance with the system. This section will display the risk of each item that not be chosen. After completely checking the standards needed, administrators can generate the questionnaire or print the checklist of the operations. The process can be recorded each period. Period used is monthly, so that the administrator can perform checks every month. Operational Process in the Domain Security Architecture and Design is shown in Figure-7. In the Domain Security Architecture and Design only selected 3 standards, and for standards that are not selected will be shown the risks of each standard.

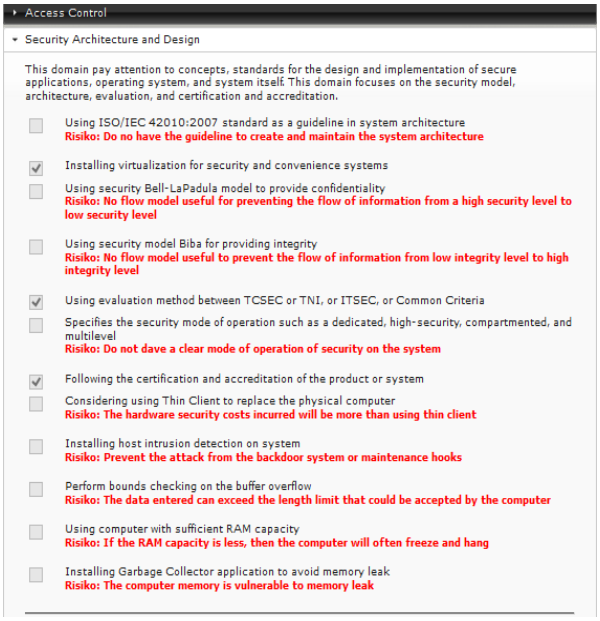

Figure-7. Domain Security Architecture and Design.

d) Create a questionnaire

Menu 'Questionnaire' can be generated after the administrators choose the standard that exists in each domain. The objective of this questionnaire is to assist the Administrator in getting feedback on any questions related to the standards that exist in each domain. Once the questionnaire is formed, then the administrator can pick the type of questions to be given to the user to get feedback based on each domain. Form questionnaire can be seen in Figure-8.

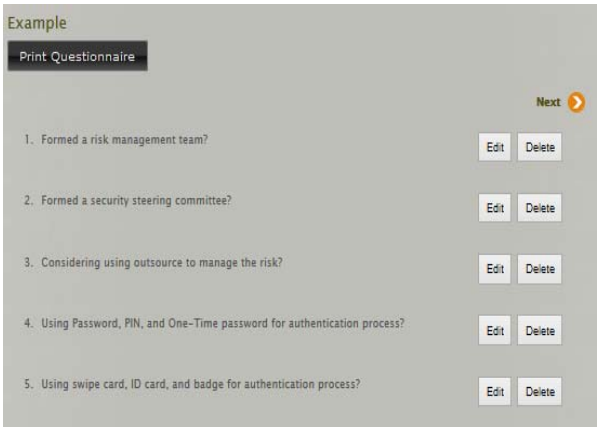

Figure-8. Sample of Questionnaire.

e) Report

This section displays the results of the Risk Assessment of the selected project. Each standard grouped in each domain and sort by priority domains. Domains that have a higher priority, which means it has a greater risk. Each standard is given a color that corresponds to the level of vulnerability. Dark green color means the risk is very low. Green means low risk. Yellow means moderate risk. Orange means a high risk. Red means the risk is very high. The results of the application can be seen in Figure-9.

Figure-9. Result of Application.

CONCLUSIONS

CISSP can help to map the inside of the security system by dividing into 10 domains. Each domain has its own standards and is flexible, so that each domain can also be customized according to the needs. By doing a good security system design, from the planning phase, the operational phase, until the evaluation stage, can help IT staff to create a security system that suits the needs of the organization, also improve staff's security awareness.

REFERENCES

[1] Ibnu Gunawan, Agustinus Noertjahyana, Hartanto Rusli. 2014. Analysis and Implementation of Operational Security Management on Computer Center at the University X. Conference, Competition and Exhibition. pp. 888-896.

[2] U.S. Code collection http://www.law.cornell.edu/uscode/44/3542.html.

[3] Sattarova Feruza Y. and Prof. Tao-hoon Kim. 2007. IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering. 2(2): 17-31.

[4] Burcu Bulgurcu, Hasan Cavusoglu, Izak Benbasat. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and information Security Awareness. Bulgurcu et al. /Information Security Policy Compliance, MIS Quarterly. 34(3): 523-548.

[5] CISSP - Why Certify https://www.isc2.org/cissp-why-certify/default.aspx.

[6] Eric Conrad. 2011. Eleventh Hour CISSP Study Guide. Amsterdam. Elsevier.

[7] Shon Harris. 2013. All-in-One CISSP Exam Guide. Sixth Edition. New York : McGraw-hill Companies.