Definition of Security Practices in Security Management Part of Security Level Management Model

Tai-Hoon Kim
Dept. of Multimedia, Hannam University, Daejeon, Korea
taihoonn@hnu.ac.kr

Kouichi Sakurai
Dept. of Computer Science & Communication Engineering, Kyushu University, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract

To manage security level of IS, the first, organizations must be able to decide security level, the second, organizations must have procedures for building security countermeasures according to security level. For next step, organizations must be able to select areas where security countermeasures should be applied, and the last, organizations must be able to evaluate and improve the effect of security countermeasures. In this paper, we propose some essential elements for security level management of IS. These essential elements are expressed like as security practices, and in this paper, we propose some security practices related to security management area.

1. Security Level Management and Security Practices

Security level management is the activity to sustain the security level which defined as an essential one by considering operational environments of information systems. So security level management is not the check of temporary status in short time but the continuous observation to the variable environment.

To perform the security level management, all factors related to the operation of information system should be considered, and by doing so, security of whole information systems can be managed. But because of the limitation occurred by some reasons, all factors can not be managed by same level. To overcome this problem, selection of important factors should be done first [1].

In this paper, we propose 16 security practices, organized in 3 areas for the SMP (Security Management Part) in SLMM (Security Level Management Model). These security practices cover major areas of security countermeasures in management aspect. Additionally, more security practices organized in additional areas can be appended, and these additional practices can be drawn from the other systems engineering or security engineering areas.

The security practices were gathered from a wide range of existing materials, practices, and expertises. The practices selected represent the best existing practice of the security community, but these practices are not static and can be modified by considering characteristics and environments of information system.

Identifying security practices is complicated by the many different names for activities that are essentially the same. These activities occur anytime in the life cycle, at a different level of abstraction, or are typically performed by individuals in different roles.

An organization cannot be considered to have achieved a security practice if it is only performed during the design phase or at a single level of abstraction. SLMM does not ignore these distinctions because these can be a candidate practice organizations can select. But SLMM does not contain these practices, so security level manager should decide if they want to include these practices.

It is recommended that each security practice has some characteristics like as:

- Practice should be able to be applied across the lifecycle of the organization.
- Practice does not overlap with other practices.
- Practice represents a "best practice" of the security community.
- Practice does not simply reflect a state-of-the-art technique.
- Practice is applicable using multiple methods in multiple business contexts.
- Practice does not specify a particular method or tool.

The security practices have been organized into security areas in a way that meets a broad spectrum of security organizations. There are many ways to divide the security domain into areas.

Each security area has a set of goals that represent the expected state of an organization that is successfully implementing the security area. An organization that performs the security practices of the security area should also achieve its goals.

It is recommended that each security area has some characteristics like as:

- Security area assembles related activities in one area for ease of use
- Security area relates to valuable security services
- Security area applies across the life cycle
- Security area includes all security practices that are required to meet the goals of the security area

The 8 security areas are listed below. Note that they are listed in alphabetical order to discourage the notion that there the security areas are ordered by lifecycle phase. But in this paper, we propose the security practices related to security management part (SMP)

Part 1: Security Management Part (SMP)

- SA01 Human Resource
- SA02 Operation and Administration
- SA03 Physical Protection

Part 2: Security Technology Part (STP)

- SA04 Access Control Technology
- SA05 Cryptography Technology
- SA06 Identification and Authentication Technology
- SA07 Service Assurance Technology
- SA08 Shielding Technology

2. Security Practices in Security Management Part

In this paper, security areas in security management part are divided into 3 groups such as human resource, operation and administration, and physical protection.

Part 1: Security Management Part (SMP)

- SA01 Human Resource
- SA02 Operation and Administration
- SA03 Physical Protection

2.1. SA01 Human Resource

Many practices are needed to do security level management. But some practices related to people are very important. Even though some technologies developed very carefully, these will not be operated in best conditions if operators may not generate or operate them. And even though an organization established good security process, these will not kept properly if employees may not follow or stick to them.

Because hiring, training and education, disposition, and retirement of human resource are being rotated continuously, the level of individual resource can be changed variously. And therefore, the security level of each organization can not be fixed and has the possibility of changing.

By hiring the people of proper level, sustaining their level before retirement, and replacing them with other new employees of same capability, organization can manage its security level. And this is the objective of this security area.

In SA01 Human Resource, there are 4 security practices

- SP.01.01 Personnel Management
- SP.01.02 Clearance Level
- SP.01.03 Monitoring of Suspicious Action
- SP.01.04 Training and Education

2.1.1. SP.01.01 Personnel Management

Personnel are managed in accordance with the personnel management plan and operational requirements.

Related Work Products

- personnel management plan

- operational requirements specification
- hired personnel
- record of hire and retirement

2.1.2. SP.01.02 Clearance level

Organization should assign proper clearance level to each position or person. Clearance level is not same with the skill level of employee, and furthermore, has no relationship with position level.

Related Work Products
- personnel management plan
- operational requirements specification
- record of hire and retirement
- clearance level assignment record

2.1.3. SP.01.03 Monitoring of Suspicious Action

Monitor all suspicious or abnormal actions made by personnel. Sometimes a small violation can be connected to harmful situation, even though personnel break the regulation by mistake.

Related Work Products
- record of hire and retirement
- clearance level assignment record
- monitoring report
- sample list of suspicious actions

2.1.4. SP.01.04 Training and Education

Personnel are educated and trained in accordance with the education and training plan in personnel management plan.

Related Work Products
- trained personnel
- education and training plan
- personnel management plan
- operational requirements specification

2.2. SA02 Operation and Administration

Small organization can make decision by simple discussion or intuitive estimation. But the bigger organization is, the more important operation or administration by using proper procedure is. Especially, in the case that security related incidents are happen or the possibility of incidents are very high, it is possible to reduce the damage by confronting efficiently and actively.

It is very difficult to predict when or how security incidents may occur. Therefore, organization should prepare rules and procedures to encounter with incidents, and force employees to follow these. Most incidents may be not solved by physical system only, so organization should consider management system together.

In SA02 Operation and Administration, there are 9 security practices

- SP.02.01 Establishment of Security Role
- SP.02.02 Configuration Management of Security Controls
- SP.02.03 Incident Identification
- SP.02.04 Incident Management
- SP.02.05 Monitoring of Change
- SP.02.06 Security Control Management
- SP.02.07 Common Use of Security Constrains and Considerations
- SP.02.08 Guidance
- SP.02.09 Identification of Laws, Policies, Standards, and External Influences

2.2.1. SP.02.01 Establishment of Security Role

Responsibilities and accountability will be imposed to each security role.

Some aspects of security can be managed within the normal management structure, while others require more specialized management.

The procedures should ensure that those charged with responsibility are made accountable and empowered to act. It should also ensure that whatever security controls are adopted are clear and consistently applied.

Related Work Products

- personnel management plan
- role of position
- education and training plan
- definition and description of security role
- requirements of each security role
- security policy
- incident response procedure

2.2.2. SP.02.02 Configuration Management of Security Controls

Security controls are managed by proper procedure, and organization can check the change of controls.

Related Work Products

- security control configuration list
- security control configuration management procedure
- security control implementation
- role of position
- definition and description of security role

2.2.3. SP.02.03 Incident Identification

Determine if a security relevant incident has occurred, identify the details, and make a report if necessary. Security relevant incidents may be detected using not only system information such as historical event data, configuration data, or other system

information but also changed environment such as rapid drop of stock value, sudden similar product development of competitor.

Related Work Products
- definition and description of incidents
- history of incident and response
- incident reports
- periodic incident summaries
- security control configuration list
- security control configuration management procedure
- security control implementation
- role of position

2.2.4. SP.02.04 Incident Management

Many events can not be prevented, thus the ability to respond to disruption is essential. A contingency plan requires the identification of the maximum period of non-functionality of the system; the identification of the essential elements of the system for functionality; the identification and development of a recovery strategy and plan; testing of the plan; the maintenance of the plan.

Related Work Products
- periodic evaluation schedule and procedure
- recovery strategy and plan
- definition and description of incidents
- history of incident and response

2.2.5. SP.02.05 Monitoring of Change

Monitor changes that may give any impact to the current security status, regardless of positive or negative.

Security controls should be in relation to the threats, vulnerabilities, impacts and risks as they relate to its environment both internal and external. None of these are static and changes influence both the effectiveness and appropriateness of the security controls.

All must be monitored for change, and the changes analyzed to assess their significance with regard to the effectiveness of the security controls.

Related Work Products
- report of changes
- history of change and countermeasure
- periodic assessment of changes and their impact
- security control configuration list

2.2.6. SP.02.06 Security Control Management

The security status of a organization is subject to change based on the threat environment, operational requirements, and system configuration. Changes are occurred as a necessity, with the consequence that the environment considered is changed, too. Therefore, security controls should be changed to cover necessary changes to sustain security level.

Related Work Products
- history of change and countermeasure
- security control configuration list
- security control configuration management procedure
- security control implementation

2.2.7. SP.02.07 Common Use of Security Constrains and Considerations

The purpose of this practice is to search, analyze, identify, and share all the security constraints and considerations needed to make informed choices. The security engineering group performs analysis to determine any security constraints and considerations on the requirements, design, implementation, configuration, operation, management, and documentation. Constraints may be identified at all times during organization's life. They may be identified at many different levels of abstraction, and can be either positive or negative.

Related Work Products
- list of security constrains and considerations
- analysis report of constrains and considerations

2.2.8. SP.02.08 Guidance

The purpose of this practice is to develop security related guidance and provide it to the employees. Guidance can be divided into many small ones.

Related Work Products
- administrator manual
- user manual

2.2.9. SP.02.09 Identification of Laws, Policies, Standards, and External Influences

The purpose of this practice is to gather all external influences which affect the security of the organization. A determination of applicability should identify the laws, regulations, policies and standards which govern the target environment of the organization. A determination of precedence between global and local policies should be performed. Requirements for security placed on the organization must be identified and the security implications extracted.

Related Work Products
- list of security constrains and considerations
- analysis report of constrains and considerations

2.3. SA03 Physical Protection

This security area, physical protection, contains security practices related to not only the protection of physical space but also the protection by using physical resource.

Space used by organization may be divided into several sub-spaces, and each sub-space may be assigned by different security level. And only the person who has the permission can enter the space.

Physical resource does not mean only digital device or equipments should be used. But the history of entrance and exit should be recorded.

In SA03 Physical Protection, there are 3 security practices

- SP.03.01 Secure Zone
- SP.03.02 Physical Security Perimeter Management
- SP.03.03 Classified Materials Storing

2.3.1. SP.03.01 Secure Zone

Establish a secure zone, and allow entrance and exit to whom has permission only.

Related Work Products
- secure zone list and map
- entrance and exit procedure
- security level of secure zones
- role of position
- clearance level assignment record

2.3.2. SP.03.02 Physical Security Perimeter Management

To check the entrance and exit status, physical security perimeters are prepared and managed.

Related Work Products
- secure zone list and map
- entrance and exit procedure
- security level of secure zones
- role of position
- record of clearance level assignment
- physical security perimeter
- security perimeter passage record

2.3.3. SP.03.03 Classified Materials Storing

Classified materials should be protected by securing facilities. Organization can select facilities by considering the importance of materials and change of environment.

Related Work Products
- securing facilities
- list of facilities and equipments
- security level of each space
- secure zone list and map
- security level of secure zones
- record of clearance level assignment
- physical security perimeter

3. Future Work

As we mentioned in chapter 1, SLMM can be divided into 2 groups, SMP and STP. By considering these 2 parts together, we can complete security level management activities.

But in this paper, we propose only 16 security practices, organized in 3 areas for the SMP (Security Management Part) in SLMM (Security Level Management Model). These security practices can cover major areas of security countermeasures in management area, but not technology area. Therefore, security practices related to STP should be defined and listed in near future.

4. References

[1] Tai-hoon Kim, Gil-cheol Park and Kouichi Sakurai, A study on Security Level Management Model Description, International Journal of Multimedia and Ubiquitous Engineering, Vol.3 No.1, January 2008, pp.87-94

[2] ISO 14001, "Environmental Management Systems - Specification with Guidance for Use", 1996

[3] ISO/IEC 17799, "Information Technology - Code of Practice for Information Security Management", 2000

[4] BS7799-2, "Information Security Management Systems - Specification with Guidance for Use", 2002

[5] ISO/IEC TR 19791, "Information Technology - Security Techniques - Security Assessment of Operational Systems", 2005

[6] ISO/IEC 21827 SSE-CMM, http://www.sse-cmm.org/index.html