World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:2, No:2, 2008

Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)

Soon-Tai Park, Jong-Whoi Shin, Bog-Ki Min, Ik-Sub Lee, Gang-Shin Lee, and Jae-Il Lee

***Abstract*—**As the information age matures, major social infrastructures such as communication, finance, military and energy, have become ever more dependent on information communication systems. And since these infrastructures are connected to the Internet, electronic intrusions such as hacking and viruses have become a new security threat. Especially, disturbance or neutralization of a major social infrastructure can result in extensive material damage and social disorder. To address this issue, many nations around the world are researching and developing various techniques and information security policies as a government-wide effort to protect their infrastructures from newly emerging threats. This paper proposes an evaluation method for information security levels of CIIP (Critical Information Infrastructure Protection), which can enhance the security level of critical information infrastructure by checking the current security status and establish security measures accordingly to protect infrastructures effectively.

***Keywords*—**Information Security Evaluation Methodology, Critical Information Infrastructure Protection.

I. Introduction

As the information age matures, major social infrastructures such as communication, finance, military and energy, have become ever more dependent on information communication systems. And since these infrastructures are connected to the Internet, electronic intrusions such as hacking and viruses have become a new security threat. Especially, disturbance or neutralization of a major social infrastructure can cause extreme material damage and social disorder. To address this issue, many nations around the world are researching and developing various techniques and information security policies as a government-wide effort to protect their infrastructures from newly emerging threats. In the U.S., the National Information Infrastructure Protection Act was enacted in 1996, and the Presidential Decision Directive (PDD) 63 was issued on May 1998 to establish a government-wide security system for major infrastructures. In addition, the Department of Homeland Security (DHS) was founded with the issue of Executive Order-13284 on Jan 2003, and the National Strategy to Secure Cyberspace was announced on Feb 2003 [1]. Japan administered laws against illegal access acts on Feb 2000, and has established 『Information Security Measure Committee』 and 『Civilian Experts Council』 under the 『IT Strategy Center』. Korea has established Information & Telecommunication Infrastructure Security Committee under the prime minister in accordance with the Infrastructure Security Law enacted in 2001, and has been building systematic and comprehensive measures against electronic intrusions for critical information & Telecommunication infrastructures. Since the protection for operation and control of major social infrastructures requires involvement of various sectors such as communication, finance, military and energy, the committee was founded under the prime minister to direct and coordinate the establishment and execution of information & Telecommunication infrastructure security policies of various agencies. In particular, the head of a central administrative agency managing a critical information infrastructure designates critical information & Telecommunication infrastructures for each jurisdiction, establishes and executes yearly security plans, and enacts security policies and recommends them to the managing agencies of critical information infrastructures or orders actions required for security. However, such security policies have usually been established without consideration for security levels. Therefore, in order to establish a more effective security policy, methodologies must be developed to assess the security level for the managing agencies based on vulnerability analysis and result analysis. This paper intends to check the current security status and establish security measures accordingly to protect infrastructures effectively, and will propose a methodology of evaluation for the information security level for CIIP, which can enhance the security level of critical information infrastructure. The Information Security Evaluation Method will provide specific assessment schemes and methods that can be used for constant and active enhancement of security level.

Manuscript received June 30, 2006. This work was supported in part by the Korean Ministry of Information and Communication.

Soon-Tai Park (phone:+82 2 405 5313; fax: +82 2 405 5219; e-mail: cptpark@kisa.or.kr), Jong-Whoi Shin (e-mail: jshin@kisa.or.kr), Bok-Ki Min (e-mail: min@kisa.or.kr), Ik-Sub Lee (e-mail: islee@kisa.or.kr), Gang-Shin Lee (kslee@kisa.or.kr) , Jae-Il Lee (jilee@kisa.or.kr) are with the Korea Information Security Agency(KISA), 78, Garak-Dong, Songpa-Gu, Seoul, Korea.

II. Literature

There are many related standards and guidelines for effective assessment of security levels. In U.S., SP800 – 53

(Recommended Security Controls for Federal Information Systems)[2] and SP 800 – 26 (Security Self-Assessment Guide for Information Technology System)[3] were developed by the NIST. As a security guideline for protecting federal computer systems and information, SP800-53 provides roadmaps to each federal agency in accordance with FISMA (Federal Information Security Management Act) and provides security control items and guidelines for establishing procedures and policies. In addition, SP800-26 was developed as a guideline for self security assessment that can measure the current status and information security of a system or a group of connected systems. On the other hand, SSE-CMM (Systems Security Engineering-Capability Maturity Model)[4] serves as standard criteria that can be widely used by governments and businesses. SSE-CMM is intended to enhance the quality, economy and availability of products and services related to information security by developing security engineering into a well defined and mature sector.

BS7799[5] is focused on public verification of businesses ensuring the secrecy, integrity and availability of customer information. BS7799 was developed by the Treasury Dept of U.K. under the title of "A Code of Practice for Information Security Management" as a general document that can be used as a reference by managers responsible for information security of organization and has become the standard for information security of organizations.

III. Proposal Method

A. *Methodology*

The proposed assessment method includes procedures for measuring the security level of an organization and deriving the maturity of the security level by analyzing the measured data. Developed by referring to the control category of SP800-53 and the detail assessment items of SP800-26, BS7799, and ISMS[1][6], detail control items for checking the security level includes 12 control categories, 54 control items, and 89 detail control items. Also, 89 detail control items can be divided into 48 function level items and 41 function process items, respectively. The function level items are purely related to provide any function. On the other hand, the function process items can be defined as sub-process. Fig. 1 illustrates how the items were derived. Table I shows the number of detail control items. Fig. 2 illustrates the distribution of control items over 12 control categories, which include general security management items such as policies and procedures, risk assessment, incident response.

[1] Information Security Management System (ISMS) is a Korean security standard developed for administrative, physical and technical security management of an organization.

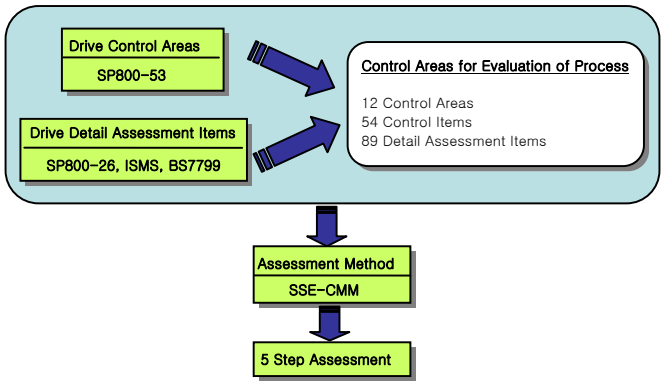


Fig. 1 Detail Control Item Selection Process

TABLE I
Number of Control and Detail Control Items for Each Category

Category	Control Item Count	Detail Control Item Count
Establishment of Security Policy and Procedure	2	2
Risk Assessment	5	11
Configuration Management	2	5
Administration & Maintenance	2	2
Media Protection	5	7
Security Awareness & Training	1	2
BCP(Business Continuity Planning)	4	6
Physical/Environmental Protection	7	10
Personnel Security	4	4
Incident Response	3	4
Audit & Accountability	5	6
Access Control & Communication Protection	16	30

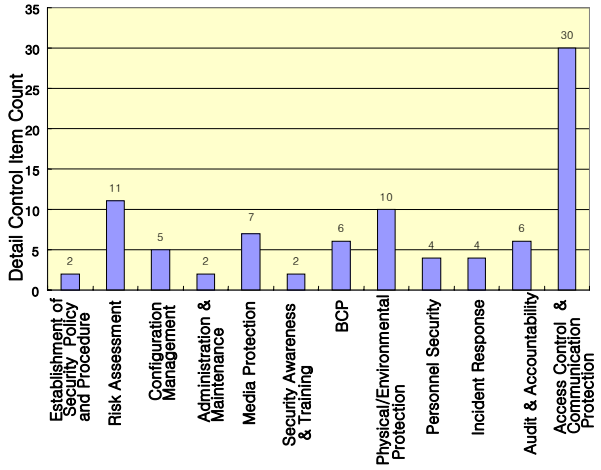


Fig. 2 Category Based Control Item Distribution

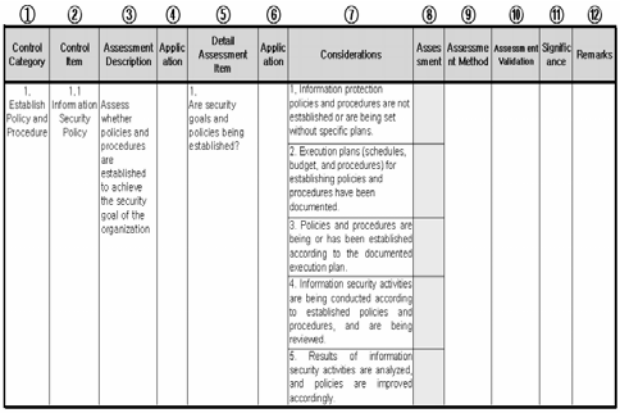
B. *Evaluation of Information Security Level*

The checklists for the 12 control categories, 54 control items and 89 detail control items presented in this paper are developed to be assessed through five levels. Based on the maturity measurement model of SSE-CMM and SP800-26, the proposed five levels were developed as a checklist that can be used for self assessment. The result of a self-assessment is certified through manager interviews, verification of related documents and on-site inspections. Table II provides definitions on the five levels of information security level assessment.

TABLE II
FIVE LEVELS OF INFORMATION SECURITY LEVEL ASSESSMENT

Level	Description
Level 1	Detail control items are not executed or are executed without specific plans.
Level 2	Execution plans (e.g. detailed procedures, schedules, and budget) for detail control items have been established and documented.
Level 3	Detail control items are being or have been executed according to documented plans.
Level 4	Results are measured for detail control items and are executed consistently for a certain period.
Level 5	Results are reviewed and improved accordingly.

Fig. 3 shows the structure of the checklist, which contains 12 fields, used for assessment.



① Control Category	② Control Item	③ Assessment Description	④ Application	⑤ Detail Assessment Item	⑥ Application	⑦ Considerations	⑧ Assessment	⑨ Assessment Method	⑩ Assessment Validation	⑪ Significance	⑫ Remarks
1. Establish Policy and Procedure	1.1 Information Security Policy	Assess whether policies and procedures are established to achieve the security goal of the organization		1. Are security goals and policies being established?		1. Information protection policies and procedures are not established or are being set without specific plans.					
						2. Execution plans (schedules, budget, and procedures) for establishing policies and procedures have been documented.					
						3. Policies and procedures are being or has been established according to the documented execution plan.					
						4. Information security activities are being conducted according to established policies and procedures, and are being reviewed.					
						5. Results of information security activities are analyzed, and policies are improved accordingly.					

Fig. 3 Assessment Template Examples

① Control Category: Names of 12 control categories

② Control Item: Names of 54 control items

③ Assessment Description: Description of assessment for 54 control items

④ Application: Whether the control item is applicable

⑤ Detail Control Item: 89 control items used for checking control items

⑥ Application: Whether the detail control item is applicable

⑦ Considerations: Facts to consider for 5-level assessment of detail control items

⑧ Assessment: Assessment of detail control items according to 5-level assessment considerations

⑨ Method: Interview and document evaluation, on-site evaluation

⑩ Verification: Note the target of assessment and the target document name

⑪ Significance: Note the significance of the detail control item as High/Middle/Low

⑫ Remarks: Note remarks on assessment

Once the assessment result is verified, the scores for each control items are calculated to grade the information security level of the organization.

$$S = \sum_{i=0}^{n} L_i \quad (1)$$

(S: Scores for control items, L_i : Score of detail control items)

$$AL = \frac{S}{N_{items}} \quad (2)$$

(S: Scores for control items, AL: Assesment Level)

The AL(Assessment Level) of organization is determined by the equation (2). For example, if the total score is 200 (when Total score of Function Process items 110, Total score of Function Level items 90) $AL = \frac{200}{89} = 2.24$, $FP = \frac{110}{48} = 2.29$, and $FL = \frac{90}{41} = 2.19$, respectively.

Fig. 4 is an example of assessing control items (e.g. establishment of information policies and procedures, risk assessment) and displaying the result in a polar graph. The graph shows that the access control & communication protection has the lowest security level.

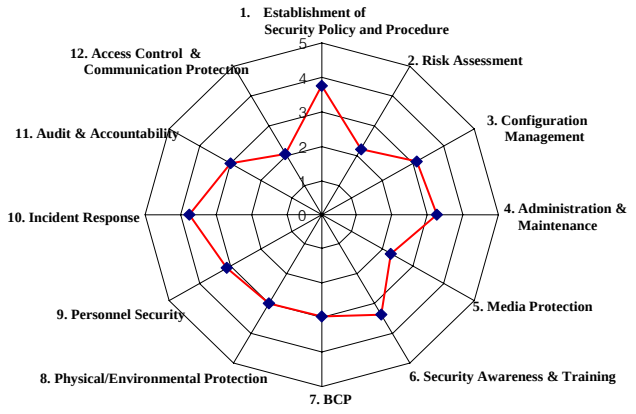


Fig. 4 Example of Level Distribution Diagram for Control Items

The level distribution diagram for control items shows which control items are strong or vulnerable to security threats, allowing managers to recognize and correct the vulnerabilities more easily. Eventually, this can used by managers of critical information infrastructure managers as a tool for conveniently measuring the information security level.

IV. Conclusion

As the information age matures, major social infrastructures such as communication, finance, military and energy, have become ever more dependent on information communication systems. And since these infrastructures are connected to the Internet, electronic intrusions such as hacking and viruses have become a new security threat. Especially, disturbance or neutralization of a major social infrastructure can result in extensive material damage and social disorder. To address this issue, many nations around the world are researching and developing various techniques and information security policies as a government-wide effort to protect their infrastructures from newly emerging threats. Korea has designated critical information & telecommunication infrastructures related to communication, finance, energy and elections, establishes and executes yearly security plans, and enacts security policies and recommends them to the managing agencies of critical information & telecommunication infrastructures or orders actions required for security. This paper has proposed a methodology of evaluation for the information security level for critical information & telecommunication infrastructures, which can enhance the security level of critical information infrastructure by checking the current security status and establish security measures accordingly to protect infrastructures effectively. This methodology will be improved into a more reliable assessment methodology by actually applying it to an organization as a test and analyzing the result.

References

[1] The White House (The Department of Homeland Security), http://www.whitehouse.gov/deptofhomeland/
[2] NIST SP800-53(Recommended Security Controls for Federal Information System) http://www.nist.gov/
[3] NIST SP800-26 (Security Self-Assessment Guide for Information Technology System) http://www.nist.gov
[4] SSE-CMM
[5] http://www.kisa.or.kr/isms/
[6] http://www.iwar.org.uk/