Security Assessment Ensuring "Secure Practice" Against Escalating Cyberattacks

KURIBAYASHI Toshimitsu, TANAKA Hiroshi, KOMAGOME Daisuke, KUSUDA Toru

Abstract

Enhancement of security measures has become a serious issue in the management of enterprises and organizations. On the other hand, sophisticated attacks, expansion of IT usage and the increasing complexity of countermeasures have made it extremely difficult to decide on the "level of security measures to be taken now". The security assessment proposed in this paper envisages current status from the three viewpoints of; the policy & control level, the communications status and the operational system. Based on results, a plan is proposed for security measure investments. This strategy provides enterprises and organizations with the source data for management decisions on the "timing and the amount of management resources (human, things and money) to be spent on security measures.

Keywords

security consulting, security diagnosis, cyberattack countermeasure, inside job countermeasures, security enhancement planning

1. Introduction

Information leaks due to cyberattacks and in-house security failures are increasing continually. These leaks are becoming a serious management issue affecting the business continuity for many of our customers' enterprises and organizations. The techniques of attacks are becoming more sophisticated and malicious and the countermeasures are accordingly becoming more diversified and complicated. The dissemination of the utilization of IT scenarios such as cloud environments, smart devices and corporate SNS is tending ironically to increase the range of the measures to be taken.

Consequently, it has become extremely difficult for many of our customers' enterprises and organizations to decide on the "level of security measures to be taken now."

This paper introduces security assessment, which is a tool for responding to the problems outlined above by deriving optimum solutions for protecting information assets against the threats of cyberattacks and in-house security failures.

2. Outline of Security Assessment

Security assessment is a consultation service that assesses the security control status of each customer enterprise or organization and draws up a plan for the arrangement and execution of projected security measures based on the results. **Fig. 1** indicates perspectives used in such assessments. Three viewpoints are used, which are; the policy & control level, communication status and the operational system. Based on the results, a plan is drawn up to define the proposed security measures investment. This provides enterprises and organizations with source data for management decisions on the "timing

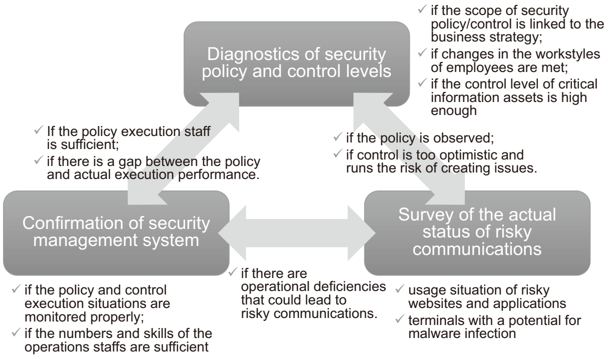
Diagnostics of security policy and control levels
✓ if the scope of security policy/control is linked to the business strategy;
✓ if changes in the workstyles of employees are met;
✓ if the control level of critical information assets is high enough
✓ If the policy execution staff is sufficient;
✓ if there is a gap between the policy and actual execution performance.
✓ if the policy is observed;
✓ if control is too optimistic and runs the risk of creating issues.
Confirmation of security management system
Survey of the actual status of risky communications
✓ if there are operational deficiencies that could lead to risky communications.
✓ if the policy and control execution situations are monitored properly;
✓ if the numbers and skills of the operations staffs are sufficient
✓ usage situation of risky websites and applications
✓ terminals with a potential for malware infection

Fig. 1 Viewpoints of security assessments.

and the requisite amount of management resources (human, things and money) to be spent on security control measures."

3. Security Assessment Issues

In the development of security assessment, we take special care to "let the customer recognize the actual status of threats correctly and to implement sure arrangements and control measures in a short time period." In the following subsections, we will describe the assessment points introduced for each of the three viewpoints described above together with the differences compared to ordinary simplified assessments.

3.1 Policy & Control Level Assessment

This procedure consists of checking if the security control is inadequate by security policy evaluations and trials. Most of the ordinary simplified assessments conduct "wide but limited" diagnostics of the measures taken by the whole enterprise using a technique called the baseline approach. In this context, however, it is hard to determine the control target range and to decide on the measures to be taken.

The present assessment adopts the technique of adding partial detailed risk analyses to the baseline approach. The differences between the two kinds of approach and details of the approach taken by the present assessment are shown in **Table 1** and **Fig. 2** respectively. The key targets of the invested security control measures can be set by adding a deep assessment targeting the IT environments related to important information assets (Fig. 2-(1),) and to an assessment targeting all of the IT systems and devices in the enterprise (Fig. 2-(2)).

Table 1 Representative analysis techniques.

Risk analysis techniques	Outline of technique
Baseline approach (simplified risk analysis)	Technique performing simplified risk analysis using standards and guidelines open to the public. It does not clarify the information assets, threats and vulnerabilities.
Detailed risk analysis	Technique clarifying the information assets, threats and vulnerability before evaluating the degree of risk. This technique takes more time and labor than the baseline approach.

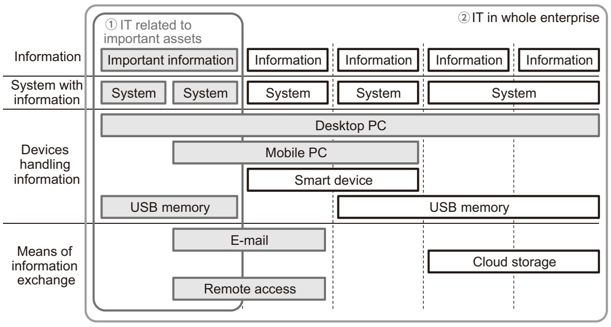

Fig. 2 Approach taken by the assessment.

3.2 Communication Status Assessment

This procedure checks illegal communications by connecting the next-generation firewall to the mirror port. The illegal communications include those with suspicious behaviors against the in-house network, the use of non-permitted free mails or file sharing with external persons, and behaviors breaching the security policy. In many cases, these threats are often unnoticed until actual damage is detected and it is therefore difficult for the baseline assessment to obtain an accurate solution. The present assessment lets the customer recognize the fact of a thread occurrence situation based on the log detected from the next-generation firewall.

3.3 Organization/Institution Assessment

After the arrangement of the security measures, this assessment evaluates whether they can be executed or not, by judging adequacy of human resources and their current allotment for the security control. However, various issues have been seen in actual cases in the past; the team in charge of the security control execution was not organized in the IT department (or subsidiary), enough number of skilled staffers to manage and execute the security measures were not allocated, etc. In order to solve such issues, NEC will collaborate with enterprises to examine building the system enabling smooth execution of extracted measures.

4. Security Assessment Flow

Fig. 3 shows how the security assessment is advanced.

The standard period is set at two months. Seven work sessions are held on a weekly basis and each work session lasts for about two to two and half hours.

The first step of the process, "Basic information identifica-

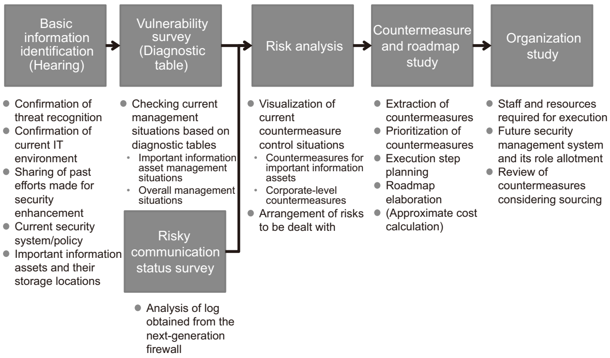
Basic information identification (Hearing)
Vulnerability survey (Diagnostic table)
Risky communication status survey
Risk analysis
Countermeasure and roadmap study
Organization study
● Confirmation of threat recognition
● Confirmation of current IT environment
● Sharing of past efforts made for security enhancement
● Current security system/policy
● Important information assets and their storage locations
● Checking current management situations based on diagnostic tables
• Important information asset management situations
• Overall management situations
● Analysis of log obtained from the next-generation firewall
● Visualization of current countermeasure control situations
• Countermeasures for important information assets
• Corporate-level countermeasures
● Arrangement of risks to be dealt with
● Extraction of countermeasures
● Prioritization of countermeasures
● Execution step planning
● Roadmap elaboration
● (Approximate cost calculation)
● Staff and resources required for execution
● Future security management system and its role allotment
● Review of countermeasures considering sourcing

Fig. 3 Flow of security assessment.

tion” checks the current IT environment and the IT environment related to important information assets.

Next the “Vulnerability survey” checks the policy and control measure situations by hearings based on the assessment sheet, which is structured as shown in **Table 2**. It consists of 42 main items and 256 sub items in eight fields.

Concurrently, the “Risky communication status survey” assesses the actual status of communications using the next-generation firewall.

Based on the above results, “Risk analysis” is conducted in order to clarify the domains in which the security measures are inadequate by means of per-item result analyses as well as by comparison with other enterprises. This is based on the benchmark data of the Information technology Promotion Agency, Japan (IPA) and data obtained from enterprises assessed in the past.

Then, a “Countermeasures and roadmap study” is performed based on the analyses results. Countermeasures are studied in discussions based on the current IT environment and by using the TOBE model prepared by NEC. The TOBE model of a cyberattack is shown in **Fig. 4**.

Table 2 Configuration of assessment sheet.

Field	Contents
I. Management system	Security policy & system, contracting with outsourcing destinations.
II. Human/physical measures	Office countermeasures, server room countermeasures
III. Information management	Management of external storage media including the PC, smart devices and USB memories, usage rules of E-mail and Internet.
IV. Access management	User ID/password management, system administrator’s access management
V. Hacking countermeasures	Virus countermeasures, vulnerability countermeasures
VI. System network configuration/ operation management	Server/system/network modification/operation rules, anti-fault backup, network segmentation
VII. System/network management	Server/system/network monitoring & log management
VIII. Incident response	Process and system for countermeasures against security breach/ incidents

The extracted countermeasures are not only ones of a technical nature but also include management-related ones such as user training.

The execution roadmap of the countermeasures is defined. The roadmap covers the coming three years based on the priority of countermeasures set in the risk analysis and in the technical relationships between the countermeasures and the mid-term IT program. The approximate cost of each countermeasure is calculated or set with preconditions in collaboration with the SE members.

Finally, the standard assessment completes with the “System study” for the execution of the countermeasures.

5. Actual Cases of Security Assessment

5.1 Housing Manufacturer A

Considering that information leak incidents due to in-house security failures are occurring as social problem, company A decided to shift the conventional security control that is built based on the optimistic orientation and to share this idea in the entire corporate. It therefore adopted the current assessment in compiling the report submitted to promote the security investment plan.

After an assessment period of about two months, the report was submitted and the company is currently executing the preparatory measures, including enhancement of the authorization platform environment.

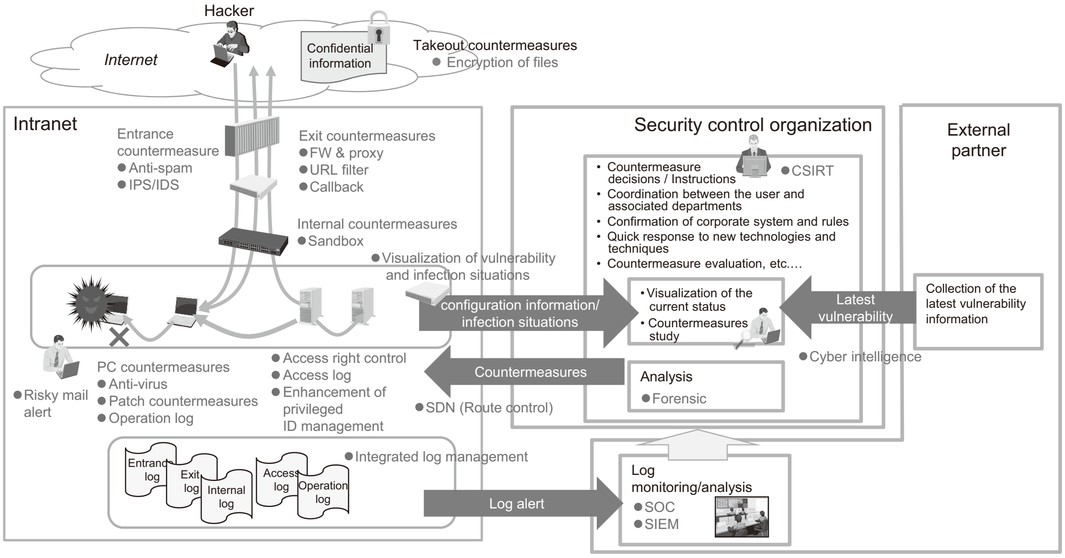

Fig. 4 TOBE model of cyberattack countermeasure.

5.2 Railroad Company B

Company B decided that enhancement of the risk resistance of group subsidiaries is necessary for enhancing the management of its group subsidiaries. It therefore adopted the current assessment, aiming at fostering security consciousness in the group subsidiaries and the visualization of security-related IT environments. The assessment period extends over half a year, during which time the security enhancement plans of the IT department of the head office and management of the group subsidiaries are coordinated. Meanwhile the specific study for turning security into a shared service is being advanced by the IT subsidiary.

5.3 Chemical Material Manufacturer C

Company C has forged an IT strategy and conducted the security enhancement at the group level, however, the inadequacy of the security staff in the IT subsidiary was becoming a serious issue. In order to solve this issue, it was necessary to tune the system including collaborations with external enterprises, and eventually the company decided to adopt the current assessment. In the assessment period of about a month, the company reviewed the role allotment between the IT department of the head office and the IT subsidiary, and also examined the security management system of the IT subsidiary that included the collaboration with NEC as their choices.

6. Conclusion

In the above, we introduced an outline of the issues and actual cases of our security assessment proposals. Security is one of the critical strategy topics comprising the social solutions of NEC and the assessment described here is a supporting tool to open the door for the expansion of business discussions. In the future, we intend to further enhance such solutions by continually identifying changes in customers' perspectives.

Authors' Profiles

KURIBAYASHI Toshimitsu
Senior Expert
Consulting Business Division

TANAKA Hiroshi
Unit Manager
Security Consulting Unit
Infosec Corporation

KOMAGOME Daisuke
Assistant Manager
Consulting Business Division

KUSUDA Toru
Assistant Manager
Global Products and Services Development Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese | English

Vol.10 No.1 Special Issue on Enterprise Solutions to Support a Safe, Secure and Comfortable Life - Value Chain Innovation Linking "MAKE," "CARRY" and "SELL" -

Orchestrating a brighter world NEC
NEC Technical Journal
Special Issue on Enterprise Solutions to Support a Safe, Secure and Comfortable Life
Value Chain Innovation Linking "MAKE," "CARRY" and "SELL"
Vol.10 No.1

Vol.10 No.1

December, 2015

Special Issue TOP