NEC's Efforts for Security

NEC's Security Business Strategy

By Michihiro KIMURA*

ABSTRACT For any organization, security is indispensable. New issues on security become obvious as a result of technical innovation, fluidization of social structures and diversification of values. Therefore, it is becoming difficult to maintain security in the current manner. In this paper, after first surveying the issues resulting from changes to the latest business environment, I go on to introduce the security business strategy of NEC and then to outline security solutions and services.

KEYWORDS **Information security, Security management, Management cycle, Cyber attack, ID management, Information disclosure, Social responsibility, Privacy, Long term preservation**

1. INTRODUCTION

Recently, the business environment related to security is changing drastically in terms of technology, social structure and sense of values.

Regarding technology, a small light-weight PC with a large capacity is becoming popular, so that office environment can be carried anywhere and at anytime. DSL (Digital Subscriber Line), mobile, and wireless LAN have also become popular. As to social structure, fluidization of employment is progressing with a collapse of the lifetime employment system. It is now not at all unusual that the key operations of a company are entrusted to personnel dispatched from an outside service company.

With regard to the sense of values the trend is increasing rapidly to demand private corporations to assume their social responsibilities. The "import beef disguise" and "defective car cover-up" scandals in Japan are only a couple of the large number of cases showing this trend. Moreover, a new consciousness that every individual should be capable of controlling data on oneself by oneself is currently underway.

Security-related accidents and incidents are occurring frequently as a result of the above changes.

Accidents in which a worm spreads from a PC carried into the office are frequent occurrences. As also are Leakages of customer information and personal information due to the theft or loss of a PC. Since information is one of the fundamental assets of business management, positive measures for prevention of information leakage is essential for building trustful relationships with the customers and investors as well as for the business management. Security is also important as an IR activity. A security accident causes major damage to corporate management and it may result in a loss of indemnity, a collapse of credit, or a loss of reputation, etc.

In this paper, after first surveying the security issues resulting from changes to the latest business environment, I go on to introduce the security business strategy of NEC and outline the latest security solutions and services. Issues resulting from changes are discussed in Section 2. NEC's security business strategy is introduced in Section 3. Related security solutions and services are summarized in Section 4 and Section 5 respectively.

2. SECURITY ISSUES

As a matter of fact due to the recent changes in social structures, it is difficult to maintain security if we continue to use traditional methods. Security can no longer be assured by simply introducing some tools, because accidents tend to occur more easily than under the previous management and employment systems. This renders it necessary in addition to ensuring open management, for every private corporation to draw up corporate measures on the assumption that accidents do occur. The effects of accidents should be minimized so that they do not lead to fatal results. Since threats are increasing every day a continuous strengthening of security is essential.

In the current IT society, private corporations face a large number of human or organization-related issues, which need to be solved in addition to technical

* IT Platform Systems Development Division

issues. Some of the issues that are being encountered by many organizations are as follows:

(1) Objective Evaluation

Security is not a matter that can always be confined within a private corporation or organization. Today, every corporation needs to demonstrate to the customers and investors how its security is maintained. This responsibility is called the accountability. The establishment of a means of objective evaluation that can convince the stakeholders is a critical issue for most organizations when they wish to demonstrate the sufficiency of their security measures.

(2) Governance Thoroughness

Security is positioned as a core issue of IT governance for the effective enforcement of the IT strategy. Nevertheless, many organizations often do not identify even the number of PCs to be patched or of the patching process. It is not unusual that a worm infects the whole company at the moment when a PC carried from outside is connected to the LAN. The current problem lies in the fact that what should be done is not being done perfectly. The limits of traditional management techniques have also been exceeded and this is the reason why thorough governance that makes full use of IT technology is urgently required.

(3) ID and Privacy Protection

Since individuals and their properties to be guarded can be identified with ID numbers, it is indispensable to protect the IDs. But it is quite difficult to administer the IDs safely and without spoiling their convenience. User authentication and personal information are in a close relationship, for stricter authentication necessitates a larger amount of personal information. Consequently, a new method of concealing personal information is sought.

(4) Prevention of Illegal Actions

The security protection measures are more difficult to be taken when they are applied to insider personnel having access authorization than for outside intruders and insider personnel without access authorization. The prevention of illegal actions by insider personnel is a deep-rooted issue.

(5) Traceability and Preservation of Evidence

Proper measures to counter an event are possible when the event is identified correctly and the path and method of invasion are determined. In this context, the audit trail occupies a key position. The main issue for the audit trail is how to protect privacy and anonymity in the alteration prevention measures.

(6) Long Term Preservation

In order to save an electronic document for a long period of time and to be able to refer to it as proof at a late dater, it is necessary to prove that the electronic document is the original one and that it must have actually existed at the time. In addition, considering the reality in which operating systems and applications are subjected to constant upgrading and media are being degrading continuously, the long-term preservation of electronic documents has become an important issue.

3. SECURITY BUSINESS STRATEGY

The basic security strategy of NEC is to carry out support for solving the issues that concern customers. These have two aspects as shown in **Fig. 1**: a solution aspect and a service aspect.

The solution aspect consists of four tiers: a security management, integrated ID management, cyber attack protection and secret protection (information disclosure measurement). On the other hand, the service aspect has five categories: consulting, design and integration, operation support, outsourcing and training. Taking advantage of technical competence services and products are offered consistently for each solution based on the notion of the management cycle.

The technical competence of NEC in the security field are various from component engineering (such as signature, cipher, and biometrics) to system technology (such as PKI, filtering, and anomalous behavior detection). NEC is also advancing the new research and development which is adapted for the further progress of the IT environment, such as GRID security and quantum encryption.

4. SECURITY SOLUTIONS

NEC's security solutions are provided on the basis of the concept "the first step of management begins from visualizing, and perfect counting is possible only by incorporating a mechanism for counting." Each solution is designed to be capable of the following operations.

(1) Security Management

In order to maintain security, systematic management is required. Against a new threat, repetition and the continuation of strengthening is also required. The security management solution responds

to this requirement by building a mechanism for the management cycle of the organization. It will enable a highly reliable management cycle by introducing evaluation standards such as ISO17799 and ISO15408.

(2) Integrated ID Management

It is the basis of any secure system to be capable of matching the IDs of users, permitting each user to access exclusively the resources the user is permitted to access, and recording the accesses made by the user.

Dynamic reorganization needs to the continuity of ID or of access control take into consideration in advance. The integrated ID management solution builds the foundations for user authentication and access control taking the protection of privacy into consideration based on the directories and PKI. VPN and secure wireless LAN can also be brought under the control of the integrated ID management.

(3) Cyber Attack Protection

Shifting from "symptomatic therapy" to improvements in protection becomes important against cyber-attacks. Measures that conform with this trend are essential with regard to a server, content and networks.

The foundation for these protection improvements is in the application of the latest patches, and vaccines. However, it is a fact that they cannot be put into practice easily as has been mentioned above.

Cyber-attack protection solutions enable thoroughness of governance by the construction of new security infrastructures which utilize IT. They permanently identify the status of all PCs and apply the latest patching automatically. In addition, when a PC is newly connected to the network, it applies appropriate measures, including quarantining, automatically. The concept of cyber-attack defense is shown in **Fig. 2**.

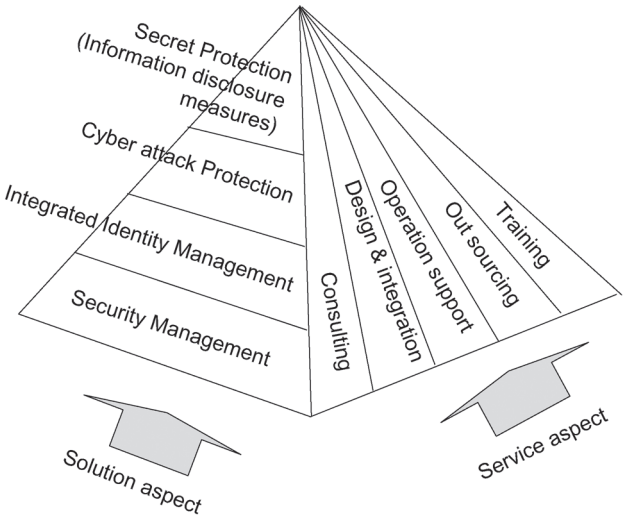

Fig. 1 Overview of security solutions and services (iBestSolutions/Security).

(4) Secret Protection (Information Disclosure Measurements)

The secret protection solution builds the foundations of information leak prevention by restricting unnecessary referencing, copying and printing, and collecting and analyzing operation logs according to the need-to-know principle.

Figure 3 shows the concept of secret protection.

This solution has extended its scope to a solution targeting the protection of general data that has now begun to provide a basis for enabling the long-term preservation of electronic documents with signatures to ensure an equivalent evidential capacity the traditional paper documents.

5. SECURITY SERVICES

Security services support security measures comprehensively and in depth from the planning to operations stages. The employment of professionals with adequate experience equipped with the latest technologies can sharply reduce the operation loads.

(1) Consulting

This service helps to build the processes of the security management cycle by functioning as a bridge across the gap between the management strategy and IT strategy. This includes for example, the establishment of a security policy according to the assets of each organization, implementation of information security audits and the acquisition of various security-related certifications.

(2) Design and Integration

While selecting suitable tools according to the concept of "visualization and checking," design and integration of secure systems are supported across network boundaries, servers, applications and physical environments.

(3) Operation Support

This service consists of the handling of the security administration by a specialist organization, freeing its users from the problems of lack of specialists or of

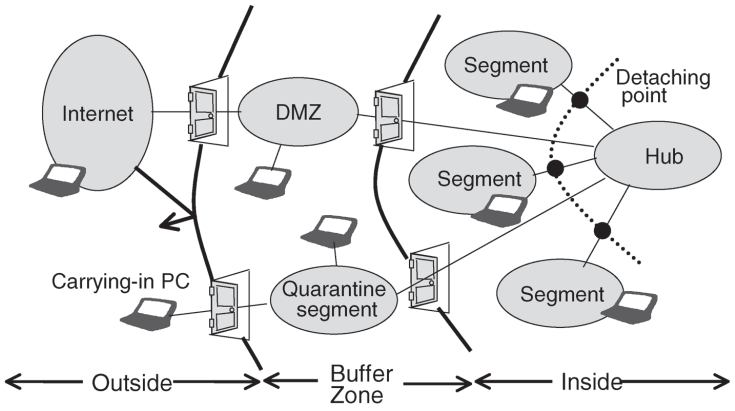

Fig. 2 Conceptual model for cyber attack protection.

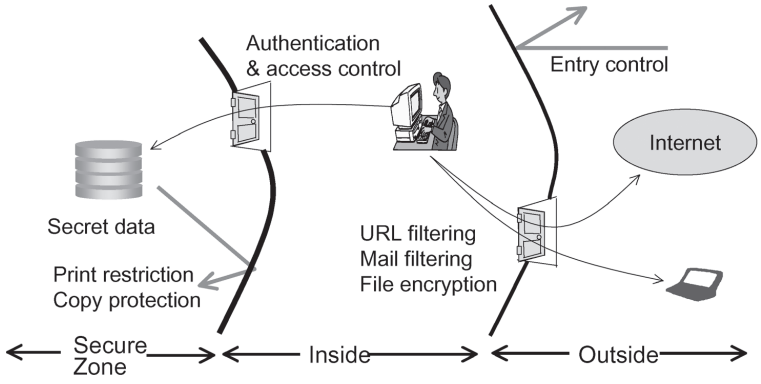

Fig. 3 Conceptual model for secret protection.

a heavy burden of auditing operations.

(4) Outsourcing

With this service, general management operations related to system security are handled by a highly reliable outside data center, 24 hours per day and 365 days per year. This policy allows the users of the service to concentrate on their original jobs.

(5) Training

Security courses for both users and engineers are prepared, respectively. Systematized curricula that can be chosen freely help participants' skills to be improved.

6. CONCLUSION

This paper has introduced security issues, NEC's security business strategy, solutions and services. The importance of security is increasing in a business environment that changes every day. For all solutions, services and products, the continuation of strengthening is an important issue that promises a safe and secure system for the future.

Received January 21, 2005

* * * * * * * * * * * * * * * * *

Michihiro KIMURA joined NEC Corporation in 1973, and is currently Chief of Architecture Strategies, IT Platform Systems Development Division, and Chief systems architect.