Information Security Solutions

● Kiyotaka Uchida ● Noriaki Sugano ● Syouichi Andou

(Manuscript received December 20, 2006)

Now that regulations such as the Japanese Sarbanes-Oxley (J-SOX) act have been enacted, organizations that hold personal information and/or provide important services are expected to promote various approaches towards information security governance. To establish such governance, these organizations have been requested to develop management systems and regularly explain their information security measures to stakeholders such as customers, investors, and business partners. The Japanese government also advocates an information security report model to help companies promote efforts toward security measures. Against this background, Fujitsu has proposed the Enterprise Security Architecture (ESA) concept for supporting effective and efficient corporate investment in information security. Fujitsu also provides the security solutions incorporated in the foundations of its products and services. This paper describes the government's information security report model, Fujitsu's ESA concept, and some ESA-based security solutions.

1. Introduction

In the last several years, there have been frequent instances of serious security problems with information systems. For example, there have been attacks by computer viruses, worms, and illegal access and also business suspensions caused by computer system shutdowns. Furthermore, there have been leakages of security information and private information that have had non-negligible influences on corporate management, lowered the credibility of organizations, and cost customers money.

Recently, the speed of business information system development has been accelerated, and total society networks have been improved. Therefore, there is concern that information system troubles may influence the whole of society and not just individual organizations.

The need for information security measures in organizations is already recognized, and technical measures such as the use of firewalls and computer antivirus products have been adopted. However, management measures such as defining a security policy, security audits, and access log collections and analyses are not adequately being implemented.

Under these circumstances, security regulations such as the Japanese Sarbanes-Oxley (J-SOX) act have been enacted, and organizations have been asked to enforce internal controls. These days, organizations greatly depend on information systems to conduct their operations. Therefore, to enforce internal controls, they must improve their information systems and also their information security governance — which is an important part of information system improvement.

This paper describes the responsibilities of organizations toward information security and the structure of the government-advocated information security reports that should support their information activities. It then describes the information required to create information

security reports and Fujitsu's Enterprise Security Architecture (ESA) and security solutions.

2. Taking information security measures

2.1 Necessary conditions for information systems

As described in the Introduction, information system troubles can seriously threaten the existence of organizations and also influence the whole of society.

Therefore, organizations are responsible to stakeholders such as customers, investors, and business partners and to society as a whole to protect their information systems.

2.2 Difficulty of taking information security measures

Organizations recognize the need for information security measures to protect their existence and comply with legal requirements.

However, information security measures can be costly. The persons in charge of the information systems of organizations ask their business managers to allocate sufficient funds for information security measures. However, it is difficult to quantitatively show how much such measures will reduce risk. Therefore, managers often do not understand budgetary requests and do not allocate the necessary funds.

In addition, there is no system that enables stakeholders to accurately evaluate the effectiveness of information security measures that organizations have taken. This is another reason why it is difficult for business managers to take positive information security measures.

Therefore, organizations recognize the need for information security measures but find them difficult to implement.

2.3 Promotion of activities for information security

The information systems of organizations are constantly threatened by attacks. Even if measures are taken when an attack occurs, different types of attack will soon arise. Therefore, instead of responding to individual attacks, organizations must employ a system to establish information security governance that is self-sustainable and continuously improved.

For this purpose, stakeholders such as customers, investors, and business partners must be able to evaluate whether organizations are taking the necessary information security measures.

To help in this area, the government has announced environmental arrangements for promoting independent information security activities by companies and has advocated the use of an information security report model.

3. Creating information security reports

3.1 Information security report model

Organizations supply stakeholders such as customers, investors, and business partners the information required for investment activities via investor relations (IR) and write information security reports so their stakeholders can understand the execution status of their information security measures.

The contents of the information security reports can be selected according to the organizations' status, and the reports can be created as Corporate Social Responsibility (CSR) reports or as independent reports.

The Ministry of Economy, Trade and Industry advocates a model for information security reports that shows the information required to enable correct evaluations by stakeholders. Specifically, the model shows that reports should describe the information security policy, internal mechanism for executing the policy, and items to be evaluated by third parties.

3.2 Information security reports

An information security report describes a security activity policy, its target scope, and management system. It also describes a mid-term

or long-term information security strategy and the information security risks.

To create such a report, action plans and numerical targets must be determined, the results must be evaluated and analyzed by companies or other organizations, and the results must be evaluated and authenticated by third parties.

There are seven categories of information to be provided in a report. Some examples of the information in each category are as follows.

1) Basic information

Report issuance purpose, notes on use, target period, responsible section

2) Business managers' thoughts about information security

Policy, target scope, stakeholder position, messages

3) Information security governance

Management system, risks, information security strategy

4) Plan and targets of information security measures

Action plan, numerical targets

5) Results and evaluation of information security measures

Results, evaluation, trouble reporting

6) Main themes of information security

Themes to be promoted

7) Evaluation and authentication by third parties

Objective evaluations

3.3 Information required to create information security reports

Creating an information security report requires audit trails, the work of which can be broadly classified into the following.

1) Establishment of management system

A management system must be established, a security policy decided, and numerical targets and an information strategy determined. Each information asset should be analyzed using the Confidentiality, Integrity, and Availability (CIA) analysis method. Then, the analysis results must be recorded and evaluated. Establishing a management system therefore requires cooperation throughout an entire organization.

2) Log collection and management

An audit trail indicating which data has been accessed and who accessed it must be prepared, managed, and analyzed (**Table 1**).

3) Evaluation and audit trails by third parties

An Information Security Management System (ISMS) conformity evaluation system, information security audit system, and privacy mark system that personal information is suit-

Table 1
Information security measures and some practical examples.

Security information protection	Access control	• Installation of firewall • Installation of intrusion detection system (IDS) • Others
	User authentication	Individual authentication
	Information leakage prevention measures	Encryption, etc.
	Antivirus measures	Installation of antivirus software, etc.
Legal measures	Log management/analysis	Unified management of collected logs (management of audit trails), etc.
Others		Outsourcing of: • Security vulnerability diagnosis • Intrusion detection system operation • Information leakage prevention others

ably handled and managed in the business operation must be established to make objective evaluations of information security handling.

However, it is sometimes difficult to obtain the security techniques and labor needed to operate these systems.

4. Fujitsu's security solutions

4.1 Appropriate investment for information security

To start information security activities, it is important that business managers take optimal measures with high investment effects and recognize the remaining risks.

Fujitsu has proposed the Enterprise Security Architecture (ESA) concept for supporting effective and efficient investment for information security (**Figure 1**).

4.2 ESA

In the processes from information security policy determination to system installation, it is necessary to select the technologies (e.g., password authentication and biometric authentication) and security function implementation method (e.g., password length and expiration date for password authentication) that will be used. However, conventional security measures do not provide the security standards needed to make these selections, and this shortcoming has greatly reduced the effectiveness and efficiency of business and investment in security measures.

ESA clearly specifies the details of authentication and identity management, access control, audit trail management, and centralized management. For example, it specifies that passwords and biometrics should be used for authentication and identity management (**Figure 2**).

As described above, Fujitsu has defined the basic concepts of security in ESA. Also, Fujitsu defines the IT-infrastructure model patterns as TRIOLE templates and supplies categorized products and services as security solutions.

4.3 Security control solutions

The above four functions for security control are arranged, as products and services, based on ESA. **Figure 3** shows an example of a security control solution comprised of these products and services.

The main security products and services are as follows:

1) Authentication and identity management
   • SMARTACCESS/Premium

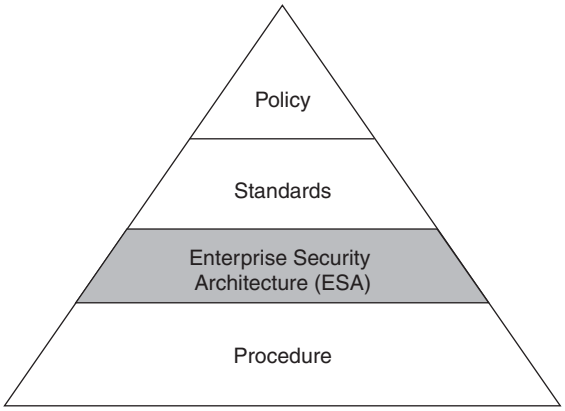

Figure 1
Positioning of ESA.

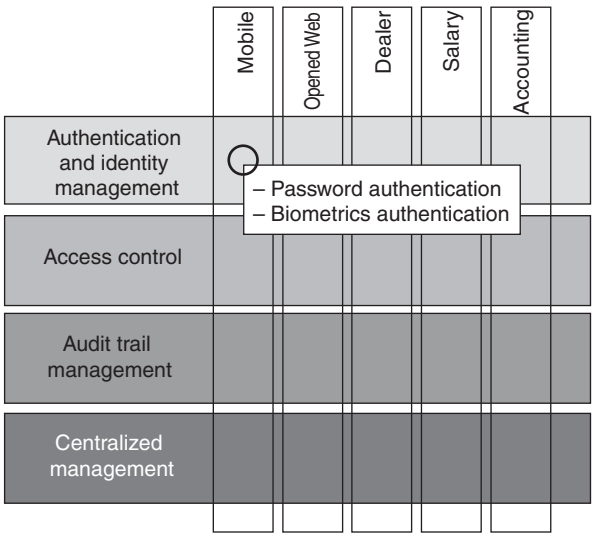

Figure 2
Basic functions and implementation method.

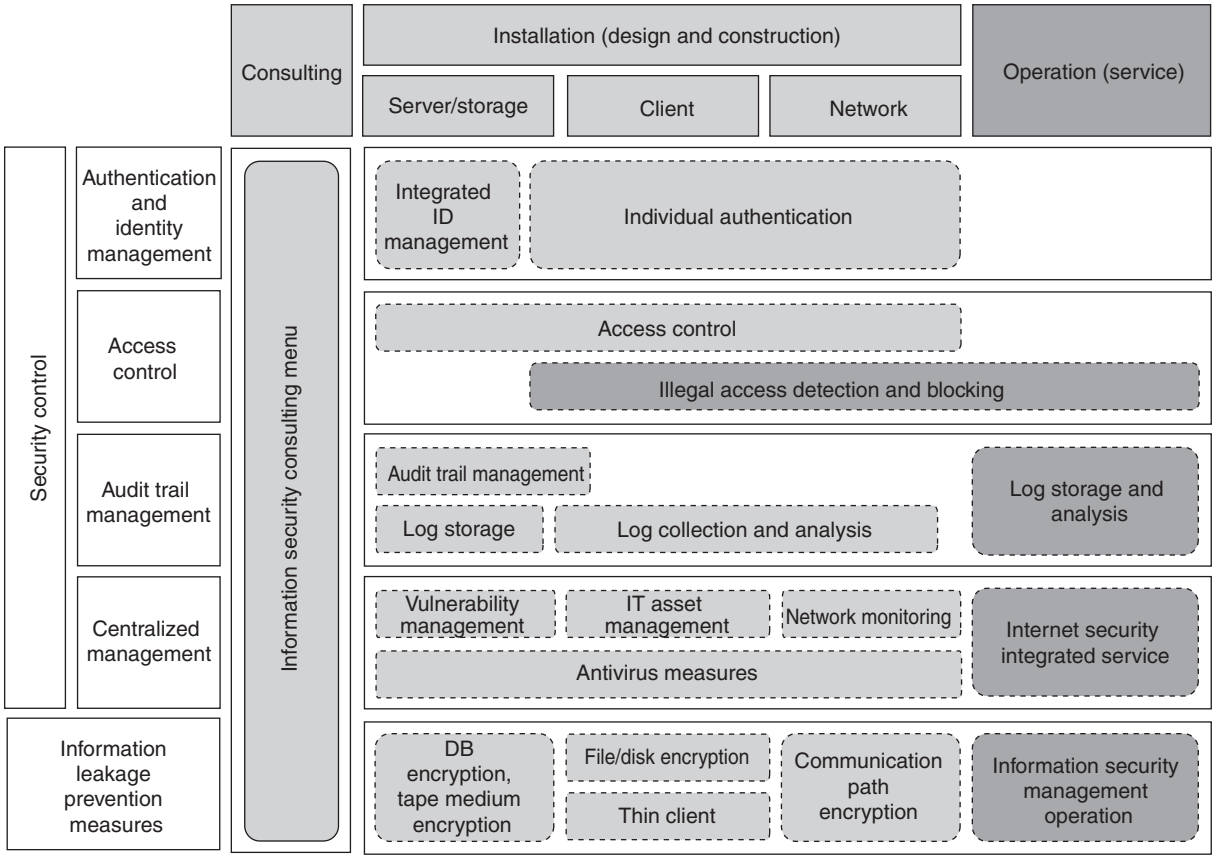

Figure 3
Example security control solution.

- Biometric authentication unit
- Palm vein pattern authentication unit
- Secure Login Box
- Sun Java System Identity Manager

2) Access control
- Systemwalker Desktop Rights Master
- eTrust Access Control
- End-point security solution

3) Audit trail management
- Systemwalker Centric Manager
- Systemwalker Desktop Keeper
- Systemwalker Desktop Log Analyzer
- Performance Insight for Security for Oracle (PISO)
- ETERNUS3000 storage system
- NR1000 network disk array
- Personal information protection/information leakage protection service

4) Centralized management
- Systemwalker Desktop Patrol
- Systemwalker Centric Manager
- Systemwalker Process Management (tentative name)
- Internet security integrated service
- Attack Test Service Express
- Web application security diagnostic service
- Security monitoring service
- Entrance/exit and dynamic state monitoring
- Image monitoring

With these products and services, Fujitsu provides customers with powerful security measures and total system support from consulting to installation and operation.

5. Conclusion

Fujitsu's ESA enables organizations to create information security reports that are appropriate for their needs, thereby ensuring the correct establishment and improvement of information security governance. When organizations use ESA, they can build a healthy business environment because stakeholders such as customers, investors, and business partners can accurately evaluate them. Fujitsu will continuously supply products and services for establishing and improving the information security governance of organizations.

Kiyotaka Uchida, *Fujitsu Ltd.*
Mr. Uchida completed an information technology program at Tokyo Technical College in 1991. He joined Fujitsu Ltd. in 1991, where he has been engaged in research and development of security infrastructure services and solutions. He is currently engaged in an information security audit project.

Noriaki Sugano, *Fujitsu Ltd.*
Mr. Sugano received the B.S. degree in Information Technology from Niigata University in 1996. He joined Fujitsu Ltd. in 1996, where he has been engaged in research and development of security systems for governmental and public institutions. He serves as a security architect and is currently engaged in the design and implementation of security systems. He is a CAIS-Assistant of the Japan Information Security Audit Association (JASA).

Syouichi Andou, *Fujitsu Ltd.*
Mr. Andou received the M.S. degree in Information Systems from Ritsumeikan University in 1998. He joined Fujitsu Ltd. in 1998, where he has been engaged in outsourcing business. He serves as an IT architect and is currently engaged in the implementation and operation of information systems.