

The Information Security Guideline for SMEs in Korea

Ho-Seong Kim	Mi-Hyun Ahn	Gang Shin Lee	Jae-il Lee
Korea Information Security Agency	Korea Information Security Agency	Korea Information Security Agency	Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul	78, Garak-Dong, Songpa-Gu, Seoul	78, Garak-Dong, Songpa-Gu, Seoul	78, Garak-Dong, Songpa-Gu, Seoul
KOREA	KOREA	KOREA	KOREA

Abstract

To address current difficulties of SMEs that are reluctant to invest in information security due to cost, this paper intends to provide an information security guideline that will allow SMEs to adopt cost efficient security measures. In particular, the information security guideline categorizes SMEs by their informatization level, presents an architecture for determining the level of security required for protecting information assets, such as PC, server, network and data, for each level, and provides cost effective information protection measures accordingly.

Keywords : *Information Security, Guideline, SMEs, Level of Informatization, Security level*

1. Introduction

The definition of SME is stated in the Enforcement Decree of the Act on Small and Medium Enterprises, but since the categorization is very complex, this paper will categorize businesses with 50~300 permanent employees as medium enterprises and those with less than 50 permanent employees as small enterprises, and the above two types of enterprises will be collectively referred to as Small and Medium Enterprises (SMEs).

Claiming 99% of Korean businesses, 50% of industry production, and 75% of employment, SMEs are an important factory in national economy and are investing massively in informatization every year to enhance business competitiveness. Such efforts

resulted in enhancements in productivity, job efficiency, and convenience.

Nevertheless, the amount of investments made by SMEs on protection of information is relatively very small. The ratio of information security investment to the total IT budget is only 2 ~ 6%, which is far behind advanced nations (8 ~ 10%) such as the U.S. and France. The number of information security experts is also very low. As a result, 74.1% (source: KrCERT, 2003) of hacking incidents reported in Korea was reported from SMEs, 46.7% of the hacking was using SMEs as an intermediate point for attacking other sites [6].

Information security breaches in SMEs not only incur serious damage to the SME, but can be abused for

criminal acts or can be used as a medium in international cyber warfare for attacking major infrastructures. Considering the proportion and scope of SMEs in Korea, poor information security of SMEs can yield catastrophic results both socially and economically.

This situation in Korea can also be seen in advanced countries such as the U.S., U.K., and Japan, where various measures are being taken to enhance the security of information, including the development of information security guidelines and studies on information security ROI for promoting investments in information security. In particular, the Ministry of Economy, Trade and Industry of Japan has developed a self-diagnostics system for information security that can be used by private businesses in order to promote the execution of information security governance.

In order to enhance the information security level of SMEs in Korea, this paper will present an information security guideline that allows SMEs to execute information security measures cost-effectively according to their business environment. While the self-diagnostics system of Japan provides upper level instructions from an overall perspective, which focuses on policies, physical security, access control and fault response, this guideline will be focusing on instructions on a lower level by presenting specific actions to be taken against vulnerabilities of information assets.

2. Current Issues in Information Security of SMEs

The type-based information security guideline for SMEs was structured according to the current situation of information security of SMEs and on their requirements. This section describes current issues in information security of SMEs in Korea, and discusses the difficulties and requests of SMEs.

2.1 Information Security State of SMEs

A survey on information security of SMEs was about information security infrastructure such as organizations, employees and budget, and state of security products, intrusions, and the difficulties and requests. It was conducted by KISA from Aug to Dec of 2004 for 1,132 SMEs through online survey and visit interviews, and the results are as follows[7]:

Among subject enterprises,
 o 71% of SMEs acknowledges the need for information security

- o Only 2% of small enterprises and 3% of medium enterprises have organizations dedicated to information security
- o Only 5% of small enterprises and 13% of medium enterprises have employees dedicated to information security
- o The ratio of information security expenses to the IT budget was 2.2% for small business and 6.1% for medium businesses
- o 5% of small enterprises and 28% of medium businesses have established information security guidelines
- o Only 26% of small enterprises and 56% of medium enterprises have firewall
- o only 6% of small enterprises and 14% of medium enterprises have Intrusion Detection System (IDS)
- o 24% of small enterprises and 28% of medium enterprises have been attacked by hacking
- o 56% of small enterprises and 30% of medium enterprises have been attacked by viruses
- o Difficulties in performing information security works are as follows:
 - 29.7% of small enterprises and 26.3% of medium enterprises said lack of expertise
 - Small enterprises say they lack in information, budget, and training, while medium enterprises say they lack in budget, training, and information

2.2 Problems in Information Security of SMEs

The ratio of investment on information security against informatization is only 2.2% ~ 6.1%, which is incredibly low compared to that of advanced nations (8~10%) such as the U.S. and France. The level of information security of SMEs is so poor that 74.1% (source: KrCERT, 2003) of all hacking incidents occur in SMEs.

According to an additional survey conducted in June 2005 for 187 SMEs in the Seoul metropolitan area on information security status, the SMEs picked the high cost of information security as the biggest reason for the low ratio of information security expenses.

The second reason was that they felt that their information assets are already well protected and that additional investment is unnecessary. However, field studies revealed that 4 out of 5 firms were exposed to various types of problems, including free access to internal networks, exposure of online certificates and malicious queries in homepages, which indicates level of awareness for potential damages is very low.

The next reason was the difficulty in managing information security products. Although over 70% of

SMEs were using basic security products, 30 ~ 56% of those companies have actually experienced virus infections, indicating that they experience difficulty in managing information security products due to lack of expertise, training and awareness.

Taking the above problems into consideration, the most effective way to enhance the information security level of Korean SMEs is to minimize the expense spent on information security and to build an environment that will allow SMEs to voluntarily enhance their information security levels.

In this perspective, the architecture and details of the information security guideline for SMEs were developed to enable SMEs to easily execute information security at low-costs.

3. Information Security Guideline for SMEs

The information security guideline for SMEs was established under the two main concepts described below:

The first main concept is to provide information security measures according to the business environment of an SME, which is implemented by providing different levels of security for different types of informatization category.

The second main concept is to provide information security measures that can minimize related expenses, which is realized by differentiating the type of measures required for a business environment and utilizing to the utmost the information security functions embedded in legacy systems.

This chapter details the architecture of the guideline and explains the detail instructions of the guideline.

3.1 Guideline Architecture

The architecture of the information security guideline for SMEs first describes how to categorize SMEs by the level of informatization, how to determine the level of security for information assets (e.g. PC, server, network, data), and finally how to define the security level required for each information asset according to the business environment of each SME, which is represented by the level of informatization.

3.1.1 Informatization Level

While there may be many ways to categorize the environments of SMEs, this paper used the informatization level for classifying the type of environments. This is to reflect the fact that businesses usually determine the level of information security based on the type of jobs using information systems and on the significance of an information asset.

The level of informatization can be divided into many stages, and the criteria for such classification have been presented by many institutes.

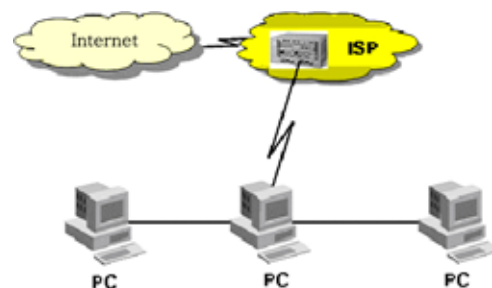
The IT Research and Consulting (ITR) has categorized the level of informatization into four levels - functional informatization, job informatization, internal informatization, inter-business informatization, and knowledge informatization - based on overall informatization environment (e.g. informatization objective, facility, application, utilization) [1].

The Korea Information Management Institute (KIMI) also categorized the level of informatization into four similar levels - foundation building, job efficiency, organizational strategy, and knowledge informatization - based on the phase of execution [8].

While this paper adopted the informatization level categorization of ITR, the levels have been simplified into the four categories described below since SMEs by nature are not applicable to numerous informatization levels and some levels represent security levels that are too high for SMEs, and to prevent unnecessary complexities.

1) SM1

PCs are mostly used for managing customers or performing jobs, as can be seen in clothing or catering businesses.

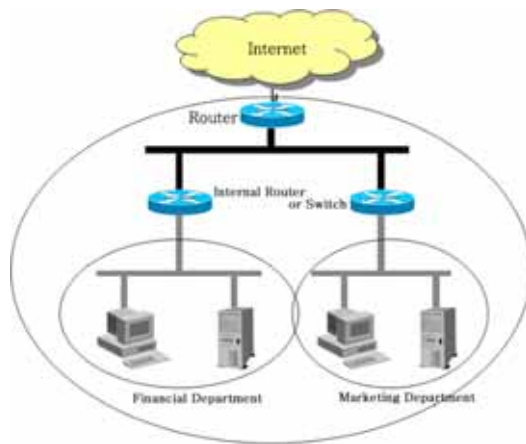


<Fig. 1 SM1 IT Environment>

2) SM2

As can be seen in common small & medium manufacturers, individual operations such as HR, finance and process management are processed using

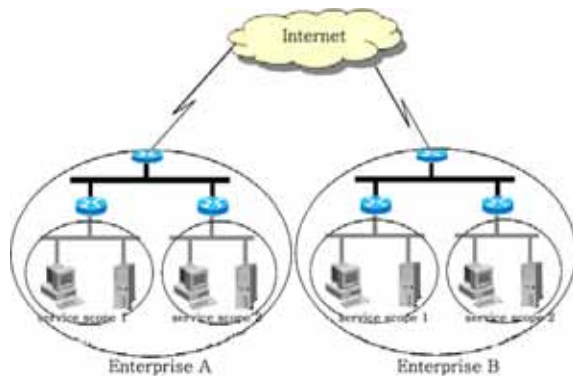
groupware or collaborated using ERP based on internal network.



<Fig. 2 SM2 IT Environment>

3) SM3

Electronic trading or works such as SCM and EDI are performed via external networks for B2B and B2C, as can be seen in online shopping and financing businesses.



<Fig. 3 SM3 IT Environment>

3.1.2 Information Security Level

This paper defines the target of protection as tangible and non-tangible information assets, which includes PC, data, server and network.

The security level for information assets is divided into four levels, from S1 to S4, based on the level of response against attacks and the relevant cost. Higher security levels require more aggressive countermeasures, increasing the cost of protection accordingly.

The basic concepts for each security level are described below. Concept of a higher level includes that of a lower level.

1) S1 (Basic Security)

Utilizes basic security features of the OS of PC or server without cost investment

2) S2 (Medium Security)

Prevents attacks by adding individual security tools such as vaccines and firewalls, and utilizes advanced security features of the OS without cost investment

3) S3 (High Security)

Detects attacks by integrating or automating individual security tools

4) S4 (Highest Security)

Monitors and responds to attacks by utilizing an integrated security tool at a corporate level, and recovers damages incurred by intrusions.

The following security actions should be taken to protect information assets according to the security level defined above:

1) S1

PC : Use basic security functions by setting ID/password and screen saver.

Server : Use basic security functions by setting ID/password and file system authority.

Network : Hide network configuration by configuring a private network using an IP sharer.

Data : Use the copy function of the OS for work, and perform user data backup.

2) S2

PC : Install individual security products such as vaccines and use advanced security functions of the OS such as deleting unnecessary service.

Server : Use advanced security functions of the OS such as user authority and set application security function.

Network : Set security function of network device and use security products such as firewalls.

Data : Backup OS and applications by using self or individual backup tools.

3) S3

PC : Apply integrated PC security by using centralized patch and ISP security service.

Server : Apply integrated security management for server and perform regular vulnerability checks.

Network : Detect network attacks by using intrusion detection/prevention systems.

Data : Backup/Recover entire system and data by operating dual system and equipment.

4) S4

PC : Same as S3

Server : Same as S3

Network : Monitor and respond to network attacks through monitoring and Enterprise Security Management (ESM).

Data : Backup/Recover entire system and data through line replication and remote backup.

3.1.3 Security Requirements for Each Informatization Level

In order to define the level of security required for each informatization level, the minimum information security requirement is defined for each informatization level as follows:

1) Minimum Security Requirements for SM1

At SM1 level, individual jobs are processed mainly by PCs and loss of data does not cause critical damage. Thus, the target of protection is individual PCs, servers and individual work data saved in those devices. This level requires minimum cost investment for responding to routine level of intrusions, which are defined as follows:

[Security Requirements]:

- o Prevent worm/virus and spam for each PC, and protect customer and user data
- o Blind external network of internal PCs

2) Minimum Security Requirements for SM2

At SM2 level, individual jobs are processed using groupware or ERP systems that operate on a somewhat complex information system and networks. The dependency on informatization is high, and system damage or loss of data can interrupt work for a certain period of time and incur significant costs. Thus, the main target of protection is servers, network devices, individual work data and shared work data. This level requires a certain amount of investment in order to prevent attacks by an experienced attacker, which are defined as follows:

[Security Requirements]:

- o SM1 requirements
- o Corporate level PC management for maintaining certain level of information security
- o Protect user and application support server
- o Prevent hacking and worm/virus attacks from external networks

3) Minimum Security Requirements for SM3

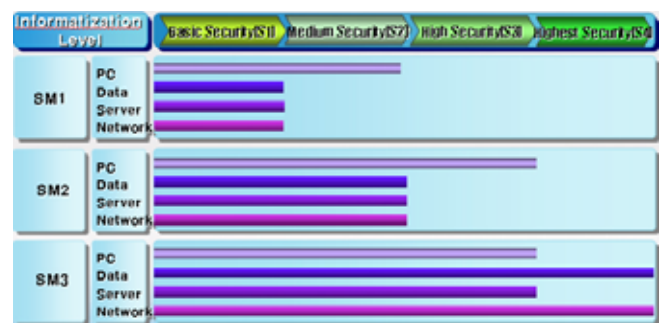
At SM3 level, e-transactions such as B2B and B2C, and works such as SCM and EDI are processed by connecting to external networks. The dependency on informatization is very high, and system damage or loss of data not only causes internal work interruption and

cost, but also incurs damage to customers and can have negative impact on society. Accordingly, very high level of reliability and security is required. Thus, the main target of protection is servers, network devices, internal work data and customer data. This level requires a certain amount of investment in order to prevent attacks by an expert attacker, which are defined as follows:

[Security Requirements]:

- o SM2 requirements
- o Protection for internal/external networks and for servers used for B2B or SCM
- o Monitors and responds to hacking and worm/virus attacks
- o Replication of data, servers and lines used for providing service

As informatization advances, the dependency of jobs on information system increases, demanding higher level of information security and incurring more costs. The requirements described earlier can be summarized as shown below:



<Fig. 4 Information Security Level for Each Informatization Level >

Once the informatization level of an SME is identified, the protection level is determined by the above table, but further security can be added for each asset depending on the job feature. For instance, a company that falls into the SM2 level may require further security measures if it handles sensitive customer data.

3.2 Guideline Content

The content of information security guideline is based on the guideline architecture described earlier, and is intended to provide the most cost effective security measure for the corresponding informatization level.

3.2.1 Information Security for SM1

In this level of informatization where individual jobs are processed by PCs, measures for protecting each PC from worms/viruses and spams, measures for protecting customer and user data, and measures for hiding the network are required as follows:

- 1) PC
 - OS update and service pack installation
 - Account and password management
 - Shared folder management
 - Security setup for screen saver
 - Security setup for web browser and email
 - Security setup for email
 - Personal firewall and pop-up block setting
 - Remove unnecessary service
 - Event and log management
 - Use virus vaccines, spyware removers and personal firewalls
- 2) Server
 - Server OS security patch
 - Account and password management
 - Shared folder management
 - Set file system security
- 3) Network
 - Construct private network using basic functions of windows OS and IP sharing devices
- 4) Data
 - Backup user and job data using OS or file server

The instructions for the above items are provided in detail in the guideline so that administrators or users of SMEs can easily follow the instructions free of charge.

3.2.2 Information Security for SM2

In this level of informatization where individual jobs in HR, finance and process management are processed over an internal network, measures for managing PCs at a corporate level, measures for protecting servers that support users and applications, and measures for preventing attacks such as hacking and worms/viruses are required as follows:

- 1) PC
 - All items in SM1
 - Operate/Manage patch management system
 - Operate/Manage integrated security management system
- 2) Server
 - All items in SM1
 - Access control
 - User authority setting

- Delete unnecessary service
- Use security option and TCP/IP setting
- Operate web/mail/DB/DNS server security and security OS

- 3) Network
 - All items in SM1
 - Security setting for routers and switches
 - Install and operate F/W, virus wall, and spam prevention products

- 4) Data
 - All items in SM1
 - Windows, Unix and Linux OS backup
 - DB/web/mail/DNS server backup

Security measures recommended to SM2 level enterprises can be summarized as enhancing the readiness against experienced attackers at lower costs by using advanced security functions of the OS and operating individual information security products.

3.2.3 Information Security for SM3

In this level of informatization where e-transactions such as B2B and B2C, and works such as SCM and EDI are processed by connecting to external networks, measures for protecting the job processing server and internal/external network, measures for monitoring and responding to attacks such as hacking and worms/viruses, and measures for replicating data, servers and lines are required as follows:

- 1) PC
 - All items in SM2
- 2) Server
 - All items in SM2
 - Install and operate patch management system
 - Vulnerability check
- 3) Network
 - All items in SM2
 - Install and operate IDS, IPS and VPN
 - Operate NMS and ESM
 - Security operation service
- 4) Data
 - System replication and operation of backup site

Security measures recommended SM3 level enterprises can be summarized as enhancing the readiness against expert attackers by facilitating the management of security at a corporate level.

3.2.4 Miscellaneous

The guideline architecture provides information security instructions according to the security level required for each informatization level and may lack instructions on a managerial level. Management instructions are also required to guarantee the effectiveness of the guideline and instructions for security management are provided additionally. Information on free education and training is also provided in order to help SMEs enhance their working-level capabilities to respond to intrusions.

4. Conclusion

To address current difficulties of SMEs that are reluctant to invest in information security due to cost, this paper provided an information security guideline that will allow SMEs to adopt cost efficient security measures.

This guideline is significant in that it allows SMEs to take necessary security measures and to realize what security products are required and what actions must be taken for additional information security. This will help SMEs protect their information assets, and will ultimately promote nationwide informatization.

It is also significant in that this is a new approach presenting an information security framework for SMEs that reflect the environment, investment costs and voluntary participation of SMEs. Still, further studies are required in order to define a more practical method for determining the security level according to the informatization level.

Since the guideline based on directions given in this paper has not been tested for long time in real working environments of SMEs, further analysis on the cost effectiveness of the guideline is required, and the result should be used for identifying problems and solutions to be reflected on future guidelines.

References

- [1] IT Research & Consulting, White Paper on Information-Oriented Operation of Enterprises in 2005, IT Research & Consulting, 2005
- [2] Korea Information Security Agency, Development of Information System Security Policy and Management Guideline, Korea Information Security Agency, 2002
- [3] National Cyber Security Center, National Cyber Security Manual, National Cyber Security Center, 2004
- [4] Korea Information Security Agency, Cyber Security Manual of Civil Sector, Korea Information Security Agency, 2004

- [5] IT Research & Consulting, Report on Results of Assessment of Level for Information-Oriented Operation of Enterprises, 2003, IT Research & Consulting, 2004
- [6] Korea Information Management Institute for Small and Medium Enterprises, 2003 Survey of Status on Adverse Effects from Information-Oriented Operation at Small and Medium Businesses, 2003
- [7] Korea Information Security Agency, 2004 Report on Survey of Current Status for Information Protection at Small Businesses, Korea Information Security Agency, 2005
- [8] Korea Information Management Institute for Small and Medium Enterprises, 2004 Information Management Level Test for SMEs, 2004
- [9] Korea IT Industry Promotion Agency, Report of Study on Survey of IT Demands at Small Businesses, Korea IT Industry Promotion Agency, 2005