American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-7, Issue-8, pp-210-216
www.ajer.org
Research Paper Open Access

# A Case Study On Major Security Management Measures In Computing Centers

Jinseop Choi
*Researcher, Korea Institute of Civil Engineering and Building Technology, Korea*
*[*]Corresponding Author: Jinseop Choi*

***ABSTRACT:*** *Intelligent transportation systems are currently being developed for the elemental technology development of cooperative intelligent transport systems, which enable vehicles to communicate with each other or reduce the risk of traffic accidents. Services have been defined and standardized by country for the purpose of solving traffic safety problems. Therefore, in this study, in the developed countries that are using the V2X (vehicle-to-everything) technology (USA, European countries, Japan, etc.), the service cases selected in the field demonstration stage after the completion of the element technology development were analyzed to suggest the direction of future development.*

***KEYWORDS –*** *Security Management in Computing Centers, A case study on security, Cyber-attack incident, Cyber-safety service*

---------------------------------------------------------------------------------------------------------------------------------------

Date of Submission: 31-07-2018 Date of acceptance: 15-08-2018

---------------------------------------------------------------------------------------------------------------------------------------

## I. INTRODUCTION

In recent years, the information technology environment evolved into the Internet of Things (IoT) environment, and the Internet and Web-based information technologies have since been gradually converging and being fused with WiFi, RFID, and other wired/wireless communication and broadcasting technologies, thus developing into the "Always Connected" environment. The national and public administration environment is also gradually shifting to Internet-based public services [1]. Such IT convergence technologies have been developed and commercialized so that they could be introduced into and utilized in areas closely related to people's daily lives. One typical example of such IT convergence technologies is the ITS (intelligent transport system) technology. The ITS technology has been adopted at a faster rate in South Korea due to the domestic geographic features, resulting in the operation of a large number of traffic information centers ("TICs") across the country.

Such technological development has made it possible to provide users with more convenient and precise services, but because a vast number of diverse systems have security vulnerabilities, the operation of intrusion detection and blocking and other information protection systems alone cannot thoroughly cope with cyberattacks or vulnerable factors.

Kaspersky Lab, a world-class cybersecurity solution company, recently conducted an onsite survey of the smart-city infrastructure in Moscow. Kaspersky Lab Global Research & Analysis Team (GReAT) proved that road-traffic-information-gathering sensors can be easily threatened by external attacks, and that if data damage (revision, falsification, and deletion) occurs due to unauthorized access, etc., and if the system is out of control, the consequential potential danger (the destruction of high-price equipment, sabotage, etc.) can have huge adverse effects not only on the road traffic infrastructure but also on the entire city [2].

In preparation against such incidents, not only the non-governmental sector but also the national and public sector have established cybersecurity control centers and are operating these, and such efforts have made it possible to tackle the physical and technical security vulnerabilities of computing centers with real-time security control, enabling the detection and blocking of cyberattack incidents.

Despite such security control efforts, however, some of the recent cyberattack incidents occurred due to the mismanagement of security vulnerabilities that could actually be sufficiently tackled. Thus, this paper examines such cases of cyberattacks and the measures that were taken to tackle them, with focus on the importance of security as well as the features of TICs' security work system, so as to propose major security management measures aimed at systematically performing security management of general computing centers.

## II. FEATURES OF DOMESTIC TICS' SECURITY SYSTEMS

### 2.1 Security Control

Most of the domestic security control centers ("SCCs") have a centralized security system by which they commonly extract the features of cyberattacks and produce the patterns of such cyberattacks to utilize them for security detection, and by which they monitor multiple relevant institutes from one SCC to tackle cyberattacks [2].

Likewise, TICs and other related institutes receive security control by the SCC of a higher institute. This method has the merit of relatively ensuring the safety of the resources of internal systems and networks from simple standard attack patterns predefined by attack rules aimed at detecting and blocking intruders' attacks [3].

The aforementioned method, however, cannot accurately identify the network structure of TICs and the features and importance of the handled information for the establishment of a security system and the preparation of security reinforcement plans against the rapidly changing security issues.

### 2.2 Construction of Information Protection Systems

Generally, the information protection system of TICs is constructed by configuring the security system using the firewall, IPS, TMS, and Anti-DDoS equipment to tackle individual attack patterns. The SCC links with the diverse security devices and diverse solutions of the TIC so that the EMS is configured to monitor the attack-threatening traffic in real time [4], and through the EMS, it analyzes the connectivity between the generated security events so as to continue to detect zero-day attacks and massive cyberattacks early on [5].

### 2.3 System of Security Management Organization

The SCC, which aims at security control, normally forms an organization or group of security specialists to ensure systematic security management. TICs, however, which aim mainly at offering services to the people, make it difficult to deploy security specialists thereto. Thus, generally, TICs have a computing system staffer who conducts system operation, maintenance work, and security work all together.

Most of the computing system staffers, however, who are usually neither security specialists nor experienced in security work, have little knowledge and capability in security work. Thus, the security work cannot be thoroughly be managed.

## III. CASES OF MAJOR DOMESTIC CYBERATTACK INCIDENTS

### 3.1 Hacking of the Ministry of National Defense Internal Network

In September 2016, the vaccine relay server of the National Defense Integrated Data Center, which manages some 20,000 personal computers connected to the external Internet network of the Korean Army, Navy, and Air Force, was hit by a malicious code. The virus spread, and multiple computers were affected. The National Defense Ministry, together with several agencies, including National Intelligence Service, conducted a two-month survey and discovered that some 3,200 computers were infected with the malicious code, and that such computers contained secret information.

The Republic of Korea (ROK) Armed Forces separates its Internet network and Intranet (national defense network) so as to configure a computing network that would prevent its secret data from leaking. The survey revealed that a vaccine relay server used by a unit was connected both to the Internet and the Intranet [6]. This failed to serve the purpose of the principle of network separation, which is the standard of configuring computing networks, and as such, a vaccine relay server should be constructed in each of the individual networks, and should be operated as a closed network. Further, it is desirable for the engineers in charge to manually and regularly update the vaccine files via CD-ROMs and other verified media. The cited case could have been avoided if the unit had stuck to the principle of security system configuration.

### 3.2 Hacking of Bus Information Systems

In April 2016, a terminal monitor of the bus information system (BIS) at an intra-bus stop in a certain area happened to display a porn video, causing confusion. The police announced that the BIS was highly likely to have been attacked by a leased line that was vulnerable to security attacks, and indicated that the remote control function was turned off at the time of the accident, leading to the accident. Further, given that only one terminal was hacked, the police announced that the possibility that the terminal was directly attacked could not be excluded [7].

The problems surrounding this and similar accidents are attributed to the use of general leased lines, which are relatively cheap but share TVs, the Internet connection, and the like, and to the mismanagement of the field terminals' security.

To prevent these accidents, the relevant agencies should use either their own lines or dedicated lines, or should use VPN lines, which use encrypted communication, and should change the basically set access information of each terminal so that the information cannot be acquired by guessing, in a bid to take security measures for each terminal.

## IV. CASES OF CYBERATTACKS AND MEASURES OF TACKLING THEM

### 4.2 TICs' Cyberattack Incidents

In July 2015, a certain TIC suffered cyberattacks when a software service firm gained unauthorized remote access to it. The TIC was configured to be accessible to its internal band (server) from the external source because the network band was not separated.

Remote access required the security staff's approval, but the software service firm violated the procedure and gained unauthorized access to the TIC — i.e., without the approval of the security staff — so a hacking program was installed in the TIC system via the pre-infected service firm's computer, causing a cyberattack incident occurrence.

The higher-level agency's cyber safety center detected the cyber intrusion early on and thus surveyed the accident and took follow-up corrective action, imposing a punishment on the service firm's security staff.

The ITS Center established a certain level of network security infrastructure and was monitoring possible cyber intrusions, but the importance of the information handled was not high, and there was no storage of important personal information; thus, the incident was not significantly raised as an issue, but the intrusion onto the public ITS Center itself cannot be taken lightly.

### 4.3 Tackling Measures Employed

After the intrusion incident, the TIC reinforced its security management by disabling the remote connection to it from the external source, securing an additional budget for consultation on the overall security by category, and planning and implementing corrective measures based on the consulting results. The details are listed in Table 1.

**Table 1. Security Reinforcement Measures**

| | **Category** | **Description** |
|---|---|---|
| Managerial security | Protection of personal information | A manual for tackling the personal information intrusion incidents |
| | Improving the policy on information protection | Establishment of guidelines for the information protection policy |
| | Applying the development security guide | Performing software development service according to the development security guide |
| Technical improvement | Removing vulnerabilities | Removing vulnerabilities in servers, DBMS, etc. |
| | Introduction of security equipment | Intrusion prevention system |
| | | Solutions designed to control network access |
| | | Patch management system |
| | | Server access control solutions |
| | | Integrated log management solutions |
| Physical improvement | Improvement of internal facilities and data | Expansion of networks subject to band separation |
| | | Adoption of media control solutions |
| | | Installation of CCTVs in control areas |

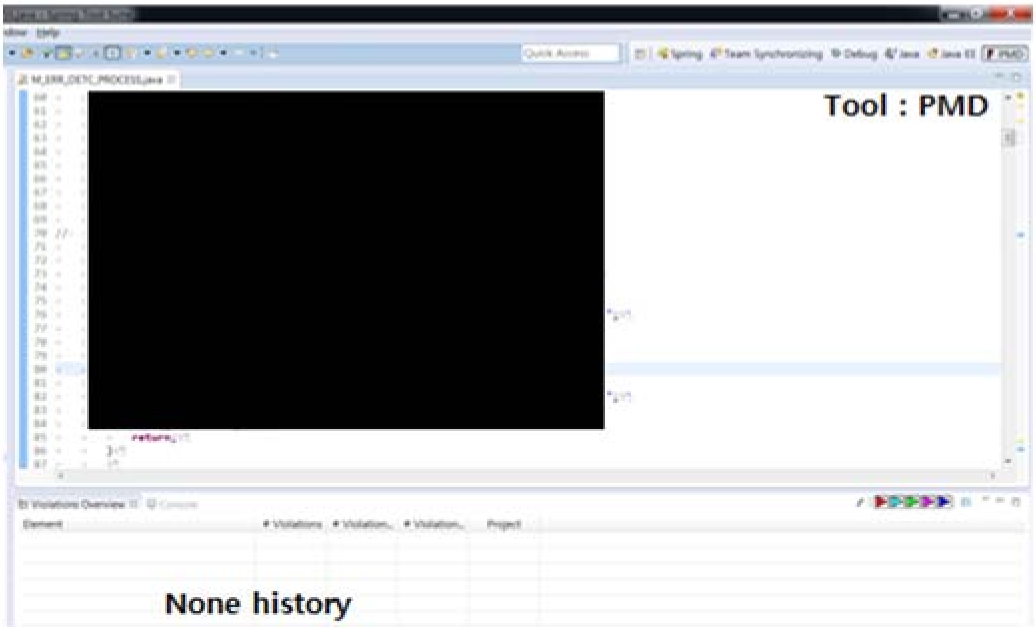
### 4.3.1 Managerial Security

The ITS Center established the following corrective measures and plans in preparation for a change in the operation policy and a revision of the guidelines.

− Protection of personal information: The center currently does not store the videos for traffic information gathering but will establish a policy mandating the writing and implementation of manuals for coping with incidents of personal information intrusion.

− Improvement of the information protection policy: The center overhauled the security guideline, which included the upper-level agency's documentation asset management, personal security, and information protection training, so as to establish an applicable action plan.

Application of the development security guide: After the intrusion incident, to prevent security vulnerabilities caused in the software development stage, the center reinforced its supervisory management so that it could apply the development security guide to new software development service projects.



[redacted]

**Figure 1. Results of checking software development security tools**

### 4.3.2 Technical Improvement

Regarding the existing settings of reinforced security equipment, the ITS Center reviewed the priority levels of the security equipment necessary for tackling security vulnerabilities and ensuring network security, and took necessary action to make the necessary adjustments.

− Removal of vulnerabilities: Regarding the settings of the existing servers, DBMS, and network security equipment, the center derived security vulnerabilities through consulting, and changed the settings of equipment so as to remove the vulnerabilities.

− Introduction of security equipment: The center reviewed the introduction of security equipment to improve the tackling of the security vulnerabilities of network configuration, and changed the network configuration as in Fig. 2 by adopting intrusion prevention, network access control, and patch management systems.

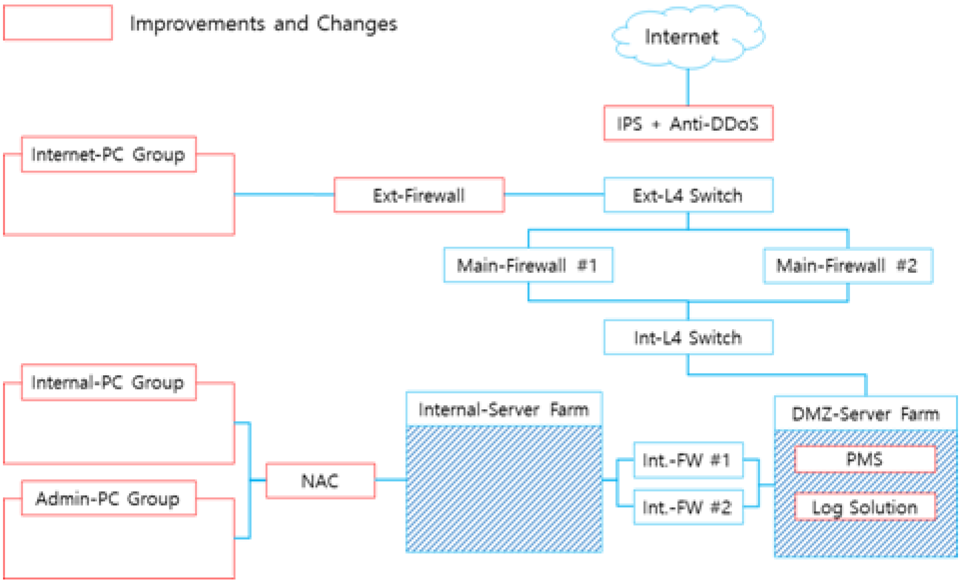


**Figure 2. Network diagram**

### 4.3.3 Physical Security

To improve the internal facilities and work data, the center is planning to take the following improvement actions:

− Expansion of networks subject to band separation: Applying the policy on physical network band separation to all the employees within the center, including the operators and manager, with regard to the network band separation

− Adoption of media control systems: Adoption of security USB aimed at delivering data between network bands, and of media control solutions aimed at data delivery, according to the application of network band separation

Installation of CCTVs in the control areas: Installation of CCTVs for monitoring those who have gained access to the server room, which is a control area

## V. MAJOR SECURITY MANAGEMENT MEASURES IN COMPUTING CENTERS

The aforementioned cyber intrusion incidents were not caused by the agency's lack of information protection systems or its failure to tackle new attacks. They were caused by failure to observe the safety rules, thus allowing exceptional situations, which in turn invited hackers' intrusions. Thus, the agency's security staff must be held accountable for neglecting security management, but the reality is that it would be difficult to take measures like the deployment of security specialists.

As such, in security management work, the role of the security staff is more important than any other. Even with the construction of a large number of information protection systems and preparation against possible attacks, if the security staff neglects security management, intrusion incidents will occur.

The security staff at computing centers should thoroughly understand the importance of security management, and should be keen on safety to conduct thorough security management.

### 5.1 Education of Security Staff to Foster Their Basic Security Ability

Most computing centers lack security staff, so they mostly assign a staffer to conduct security work concurrently. Thus, the training of security staff to foster their basic security capabilities is the first priority in reinforcing security management. Security staff need to be trained in managerial, technical, and physical security areas to conduct security management of computing centers, and the training details are described in Table 2.

**Table 2. Training Details**

| Category | Detailed items | Description |
|---|---|---|
| Managerial security | Guidelines for security work | − Security work organization<br>− Role of security staff |
| | Information to be handled | − Importance of the information handled<br>− Encryption to transmit or not |
| | Manuals | − Manuals for responding to warnings of cyber crisis<br>− Manuals for responding to intrusion incidents |
| Technical security | Configuration of computing networks | − Configuration of the network equipment<br>− Overview of the construction of information protection systems |
| | Information protection systems | − Function and role of information protection systems<br>− Establishment of a policy for information protection systems |
| Physical security | Access control | − Determination of the access control system to be implemented, and of the access control areas<br>− Management of access books |
| | Facility security | − Locking of access limitation and control areas<br>− Anti-crime systems |

In terms of the managerial aspects, the security staff should basically be made familiar with the computing center's security work guideline, the information to be handled, the manuals, etc. They thus should be trained so that they would become familiar with their role, the importance of the information to be handled, and the procedure they should carry out for tackling intrusion incidents so as to control systems and manpower when accidents occur.

In terms of the technical aspects, the security staff should be trained so that they would be able to identify the computing network configuration and information protection system situations and regularly inspect the policy establishment situations of network equipment configuration and information protection systems and thus recognize vulnerabilities before accidents take place.

In terms of the physical aspects, the security staff should be trained so that they would become familiar with access control and facility security situations and would be able to manage access control and control area access books and regularly check if the locking devices and anti-crime systems are normally operated.

### 5.2 Preparation of Checklist for Security Management

The preparation of a security management checklist is essential for the security management of computing centers, along with the training of the security staff to boost their capabilities. Even with the security staff thoroughly trained, if the security management work system is not properly established, the work will create defects, which in turn may lead to cyber intrusion incidents.

To prevent such incidents, the security management checklist should be written. If a checklist for security management is written according to the characteristics of the computing center that is to conduct security management work, systematic, efficient security management will be ensured.

**Table 3. Checklist main items**

| Category | Description |
|---|---|
| System construction | − Review the merits<br>− Check security acquisition status<br>− Consideration of security compatibility |
| System management | − Information protection system policy check<br>− Check security vulnerabilities and complement |
| Maintenance | − Latest security update<br>− SLA(Service Level Agreement) |
| Software development management | − Security check of development environment<br>− Check whether to comply with development security guide<br>− Source code archiving and configuration management |

The proposed essential items to be listed in the security checklist are shown in Table 3. The listed items are the minimum items for basic security management, so a checklist should be written by adding more items to it according to the situations encountered by the computing center that is to conduct security management.

The major items of the security management checklist are divided into system construction, operation management, maintenance, and software development management.

The system construction area lists the things to be reviewed for the introduction of new systems. It begins with the review of the justification of the introduction of the system, and a string of reviews is required, including the review of the security suitability for the network configuration change caused by the introduction of the system.

The system operation area lists the things to be inspected for the system operation and management. The security staffer checks if the policy for the information protection system is properly established, and if there are security vulnerabilities, so as to take improvement action if necessary.

The maintenance area checks if the security of the system equipment is updated, in line with the system operation and management. Further, through the definition of the SLA, it prioritizes the impacts on the equipment service operation to manage such points.

Lastly, the software development management area lists the things to be checked for the development of software. In providing the development environment to the developers, the review begins with checking the possible violation of the security policy, and it needs to be determined if the security policy is proper for the storage of source codes and for the management of the configuration.

### 5.3 Cyclic Inspection of the Information Security Condition

Generally, the protection of the various information handled at computing centers aims to prevent accidents via the logical and physical devices used between the information provider and the user. To conduct such information protection activities for a long period of time, security staff training aimed at fostering their capabilities, and the preparation of a checklist for security management, as the aforementioned major security management plan of computing centers, as well as the cyclic inspection of information security items, should be conducted.

It is important that, under the leadership of the security staffer at the computing center, the information security inspection cycle be appropriately set up by dividing it into day, week, month, quarter, etc. to establish a management schedule.

## VI. CONCLUSION

This paper examines the several recent cases of cyber intrusion incidents, with focus on the importance of security management, and proposes the major security management measures that can be taken by general computing centers by referring to the security system features of traffic information centers (TICs).

The proposed security management measures are the methodology by which the security staffer can conduct security management work more systematically and efficiently given the reality that in most of the South Korean computer centers, the system staffer should conduct security management work concurrently with his or her other work tasks. The major security management measures include the training of the security staff aimed at fostering their capabilities, and the preparation of a checklist for security management.

The presented importance of security training is that of enabling the security staff to clearly recognize their role and helping upgrade their work capabilities so that they could thoroughly conduct managerial, technical, and physical security management of computing centers. In addition, the proposed preparation of a checklist for security management involves listing the important items to be checked so as to conduct security management work more systematically.

If the security staff conducts their work according to these major security management measures, it will increase their work efficiency and the computing center’s security management levels. If security training and the updating of the security management checklist through the cyclic field inspection of information security are not conducted, however, exposure to cyber intrusion incidents will not be avoided. Thus, there is a need to spread and institutionalize such security measures so as to make security management mandatory.

## REFERENCES

[1]. Kim Yeong-jin, et al. "A Study on Efficient Implementation Measures for National Computing Network Security Control Work.” The Korea Institute of Intelligent Transport Systems Dissertations Journal 19.1 (2009): 103-111.

[2]. Ministry of Land, Infrastructure and Transport, Annual Report of ’Development of Intelligent Security Technology based on Spatial Information for Safe Life’ (2016)

[3]. T. Nam, et, al. “Reliable Next Generation Network Security System.”, Korea Information Protection Academic Association J. 6. (2003): 1-12.

[4]. W. Seo and M. Jun, “A Study on the Realization of Diskless and Stateless Security Policy Based High-speed Synchronous Network Infrastructure.” J. of the Korea Institute of Electronic Communication Sciences. 6.5 (2011): 676-679.

[5]. W. Seok and M. Jun, “A Study on the 3D-Puzzle Security Policy in Integrated Security System Network.” J. of the Korea Institute of Electronic Communication Sciences, 5.4 (2010): 425-434.

[6]. J. Song, et, al. “A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts,” The 2008 Int. Symp. on Applications and the Internet(SAINT2008), The IEEE CS Press, Aug. (2008): 51-56.

[7]. Hwang Byeong-jun. “Leak of Military Secret due to the Incompetence of the National Defense Ministry and Hacking of Intranet [an analysis],” Special Economy (December 13, 2016)

[8]. Digital News Team, “Yeosu Bus Stop Information Device that Caused the Showing of Porn Video, Leased Network Vulnerable to Hacking…Hackers, Remote Control Are Blocked?,” The Dong-A Ilbo (April 26, 2016)

[9]. AhnSeong-chae, et, al. “Security Control of Smart City Data Center,” KICT Smart City (2016). 176-179.

Jinseop Choi"A Case Study On Major Security Management Measures In Computing Centers.” American Journal of Engineering Research (AJER), vol. 7, no. 08, 2018, pp. 210-216