IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. IV (Jan.- Feb. 2018), PP 17-21
www.iosrjournals.org

Analysis of Cyber Security Policy of Critical Infrastructure in Major Countries 0: Comparison of the Policies in the US, EU, Japan, and Korea.

Ji-Yeon Yoo*, Hyun-Ju Lee**

** Department of Intelligent Engineering Informatics for Human in Sangmyung University, Republic of Korea*
*** Master's degree holder at Department of Information and Security Management in Sangmyung University, Republic of Korea*
Corresponding Author: Ji-Yeon Yoo

Abstract : *In recent years, along with technological advances such as information and communication technology and convergence, major forms of infrastructure have different characteristics from their predecessors. As the environment surrounding them has changed, new types of risks have emerged which could pose serious security threats. In this paper, we analyze the new threats caused by environmental changes in critical infrastructure, and compare cyber security policy and systems of critical infrastructure of major countries (the US, EU, Japan, and Korea). In order to strengthen the cyber security of such infrastructure, institutional improvement, framework design, and systems sharing is being promoted. This is also required for securing international trust for international cyber security.*

Keywords – *Critical Infrastructure, Cyber Security Policy, New security threats*

Date of Submission: 16-02-2018 Date of acceptance: 01-03-2018

I. Introduction

Recently, as the use of IT assets increases in terms of both control systems and information systems directly or indirectly connected to major pieces of infrastructure, the size of the internet backbone is becoming larger and more complex[1]. As a result, the frequency and sophistication of attacks targeting this infrastructure are increasing.

In addition, since the control system in question uses a closed independent network and a private dedicated protocol, it is highly perceived that the control system has a high level of security, and thus far issues of security have not been raised. However, over time, the environment of the control system has gradually opened up for resource utilization and cost reduction, and new security threats and vulnerabilities have become apparent.

In this paper, we try to understand the characteristics of these emerging security threats according to environmental changes experience by the control system. We will compare and analyze cyber security policies, systems, and organizations found in the US, EU, Japan, and Korea that seek to respond to these security threats. We want to understand how each country reacts to newly emerging security risks, and suggest new countermeasures.

II. New Security Threats Due To Environmental Changes

Because of the efficiency of control systems and measures of cost reduction through connection with IT system, the open environment of control systems has differentiated characteristics from existing systems, and has thus led to the creation of new security threats.

Table. Comparison of the Control System

Characteristic	Previous control systems	Changed control system	New Threat Factors
Connectivity (Integrity)	Use closed network	In-house network, external network, and Internet connection	Security vulnerability due to increase in interconnections between control systems and IT service
Openness	Use private, proprietary protocols	TCP / IP, using wireless protocol	Security vulnerability caused by using an open protocol, general H/W, S/W
Purpose (Intentional)	Cyber Offensive	Cyber attack	Increase in cyber attacks aimed at control system

2.1. Security Threats due to Connectivity (Integrity)

The interconnection between control systems and the IT systems has been improved as the network which used the independent closed network and the private line changed from the internal network to the external network, and finally the Internet. In particular, remote maintenance in the is increasingly becoming a common practice, and in this situation, an external control system maintenance engineer uses an access link provided by the control system supplier to run diagnostics on the control system.

However, these access links are not well secured, and there is a very high risk of security breaches due to the use of an insecure connection between the vendor and the control system network due to insufficient establishment of authentication and encryption mechanisms.

In addition, although the company operating the control system must recognize the security problem due posed by this method of connectivity, the security of the connection device or the software used is often not properly secured. Although some structural separation of the control system is required, there are companies that do not implement the separation strategy itself.

2.2. Security threats due to openness (openness)

As connectivity within IT systems grows, control system vendors are increasingly using standard network protocols and open networks as they use other manufacturers' products for internal configuration or other compatibility.

In addition, due to cost reduction and performance improvement, standard operating systems such as MS Windows or Unix have been widely used in terms of real-time OS and embedded OS, and standard applications such as MS SQL server and MS Excel are the norm as well.

The use of such open protocols and general H / W, S / W, etc., will result in their own inherent vulnerabilities, and despite the use of general-purpose hardware or software with respect to IT systems, this poses an additional security problem because the product may not be updated or patched on a regular basis.

2.3. Security Threats Due to Intent (Purpose)

According to the ICS-CERT in the US, the number of accidents increased from 39 in 2010 to 245 in 2014, and measures of vulnerability also increased by more than 800% from 2010 to 2014.

Such attacks are taking various forms, such as malicious code insertion onto corporate and personal PCs, internal threats, organized crime, and national terrorism.

Stuxnet, which was first discovered in Belarus in June 2010, was designed to destroy major pieces of infrastructure such as power plants, railways, and airports, and is now used as a guide for developing new malicious software targeting control systems along such lines.

III. Analysis Of Major Infrastructural Policies In Major Countries

3.1 US Policy, System, and Organization Analysis

3.1.1 US Policy

The policy found in the US emphasizes the roles, functions, and responsibilities of the central agency for the protection of critical infrastructure, and requires that the federal, state, and private sectors all establish protection measures[3]. In addition, priority is given to the socio-economic impacts of the critical infrastructure in question in order to emphasize systematic infrastructure protection. This national strategy is characterized by the risk management process being key, and the existence of technical and management guidance for each sector[4].

The federal government, the state, and the private sector have specified specific cooperation procedures, and have established an effective infrastructure protection mechanism through an information sharing network to be used in case of an emergency. This emphasizes their roles and responsibilities, as well as emphasizing the phased protection of infrastructure protection facilities as outlined above. The comprehensive characteristics of these policies are bullet - type, detailed guidelines - internal policies.

3.1.2. Organization of the United States

In the US, the Department of Homeland Security plays a central role in infrastructure protection, and there is a committee under the Department of Homeland Security with the mission of advising on how to appropriately protect major pieces of infrastructure. The Department of Commerce's NIST is conducting research and technology development with the support of the Department of Homeland Security (DOE)[2]. The Department of Energy (DOE), together with the Department of Homeland Security, plays a central role in infrastructure protection.

American organizations are generally organized into a tree structure centered on the Department of Homeland Security and the Department of Energy. In the case of information sharing and accident response, federal agencies, state agencies, and local agencies have radial structures centered on the Department of Homeland Security. In other words, information is circulated through a radial network.

3.1.3. US system

The United States system provides detailed guidelines for sectoral implementation by the Department of Homeland Security (DHS) when it presents it's overall strategy at the national level. In the private sector, internal policies and systems have been established, and reports on the evaluation of critical infrastructure protection have been prepared. This will be communicated to the Department of Homeland Security through sectoral departments and the strategy will be evaluated. The evaluation results portend to indicate whether the strategy should be maintained or changed, or whether a new strategy should be developed altogether.

Strategy and policy enforcement is handled top-down, and feedback is good from the bottom up for the sake of new policy formulation. All system implementation and establishment system has a U-shaped arrow structure emphasizing actual efficiency and utilization.

3.2. Analysis of EU policies, systems and organizations

3.2.1. EU policy

The policy found in the EU is focused on the protection of the guards, taking into account the relative importance of major forms of infrastructure, and consists of various expert groups responsible for protection.

In addition, the information sharing process for the protection of critical infrastructures has also been established. Most of the policies have analyzed the interdependence of critical infrastructure[5].

It also has a certification system guide for assessing the qualifications of the control system operators and introducing them, and emphasizes partnership between control system owners, operators, and member countries. It establishes various grounds for information sharing for the benefit of the member countries and features a policy structure that emphasizes the interconnection of critical infrastructure by country. Based on the guidelines of the ENISA, member states have also established their policies and helped to shape legislation produced by the European Commission[6].

The laws of the legislated European Commission are process-oriented and are linked organically with each other in terms of policy. The guidelines of the ENISA are composed of various recommendations for the implementation of control system security, and are independent of each other.

3.2.2. Organization of the EU

The EU organization is organized for the purpose of information sharing, and each member state is gathered around the ENISA. The European Commission is supported by ENISA, but it is in the same location and has established its own information sharing process through the JRC and the ERNCIP under the committee.

Since there is a central transnational institution, there is an equal line with no coercion, and the ENISA-European Commission-member countries are organized horizontally. The relationship with the private sector in the Member States is a tree-like structure of the general state institutions, because the state can exert control over the private sector.

1.2.3. EU system

The EU system consists of the European Commission and the European Union Agency for Network and Information Security (ENISA), which are responsible for incident response and information sharing. Member States deliver relevant information to critical infrastructure operators and the public in the private sector, and submit incident results and annual reports to the European Commission and ENISA.

Compared with one country, the European Commission and ENISA play a role as government agencies, and the member countries play the role of national institutions, while the critical infrastructure operators in the respective countries are in the private sector. The European Commission and ENISA are not at the top because they are not compulsory. The EU system is in the form of a general government agency with a relational structure, content transfer down, and results up.

3.3. Analysis of Japan's policies, systems, and organizations

3.3.1. Japanese policy

Japan's policy is to strengthen the accident response system, risk management, strengthen the information sharing system, improve safety standards, and strengthen the protection base[7]. It emphasizes free circulation and mutual cooperation in terms of information, construction, and current evaluations of the security management process of private sector are also underway.

It is characterized by introducing and utilizing various strategies and guidelines related to infrastructure protection in major countries, and incorporating them into new policy formulation. Most Japanese policies are based on the above-mentioned information sharing and cooperation style. It is the recent policy trend to legislate on the basis of time-based strategy. We are building a large body of policy that encompasses government agencies and the private sector, focusing on key keywords. We are focusing on cyber security and establishing a comprehensive strategy.

3.3.2. Organization of Japan

In Japan, the National Center for Incident Readiness and Strategy for Cybersecurity (NISC), which is installed in the Cabinet Secretariat, is the center of critical infrastructure protection and the establishment and implementation of related policies in NISC begins. There are subordinate agencies that are responsible for the certification, evaluation, and the provision of technical support under each department. In addition, independent associations and agencies of the private sector conduct critical infrastructure related research.

There is a central body for the protection of critical infrastructure, but the overall organizational structure is not organized in a top-down format. The departmental departments under the government have a general tree structure, but the state and private sectors have a horizontal relationship. This is because the private sector can independently establish safety standards under the core strategy of the government and is responsible for the related certification and evaluation by the association and the organization.

3.3.3. Japanese system

Japan's system is shared by the NISC's main infrastructure related departments, Sector Scepters and Scepter Committees. In general, the NISC provides information such as early warning and accident recovery measures, and attack information and vulnerability to the NISC.

In Japan, the system at the time of the accident is different from that at the time of the accident. In the event of an accident, responding to the incident and immediate input by the disaster prevention ministries and rapid response and recovery through information sharing are noticeable characteristic of the Japanese organizational system. The overall system is a U-shaped arrow structure, and other information security departments and operators are building radial structures around the NISC and emphasizing organic cooperation.

3.4. Analysis of policy, structure and organization in Korea

3.4.1. Korea's policy

In Korea, the act on the protection of information and communications infrastructure exists as a act designed with the protection of critical infrastructures in mind. The contents of the policy are divided into critical infrastructure designation, vulnerability analysis and evaluation, establishment of protection measures[8].

Vulnerability analysis and response to critical infrastructures are specifically described, and technical support, management and countermeasures are held as key.

3.4.2. Organization of Korea

In Korea, the relevant government departments and administrative bodies are vertically present, mainly through the Information and Communication Infrastructure Protection Committee, and the technical support organizations are supporting the analysis and evaluation of the vulnerability of the administrative agencies[9].

The private sector is structured to request technical support from the management organization and for the management organization to solve it, and the organization is organized in a top-down arrow structure.

3.4.3. Korea's system

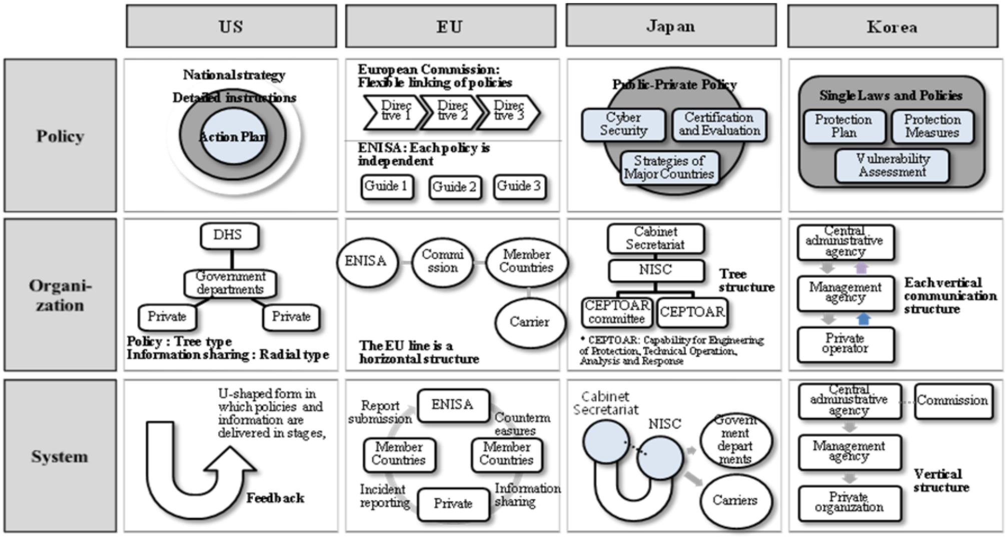
In Korea, the Information and Communication Infrastructure Protection Committee deliberates on the coordination of critical infrastructure protection policies, the coordination and promotion of protection plans, and the improvement of related systems. The Ministry of Science and ICT(MSIT) and the National Intelligence Service (NIS) serve as secretaries, and 17 central administrative agencies formulate and recommend protection guidelines, and receive periodic reports on vulnerability analysis and evaluation. The main IT infrastructure protection measures are submitted to the head of the relevant central government administration by August 31st of each year after the head of the administrative agency and local autonomous bodies are established. The major information and communication infrastructure protection plan is formed as the implementation progress of the previous year's protection plan, and the following year's protection plan must be submitted to the Board by October 31st of each year. In addition, the results of vulnerability analysis and evaluation are required to be carried out within six months after the designation of the main infrastructure in question, and shall be conducted within nine months provided any special reason. After initial implementation, evaluation is carried out annually.

There is a basic framework of setting up the next year's plan through the evaluation of the main infrastructure, and the evaluation of the result of the protection of the main infrastructure, but the actual influence of the committee is insufficient. There is a tendency to place more emphasis on carrying out roles and responsibilities than on collaboration among institutions.

IV. Conclusion

Figure 1 shows the results of the analysis of the cyber security policies and systems in major countries (the US, EU, Japan, and Korea).

Figure 1. Comparative analysis of policy, organization and system of critical infrastructure of major countries



As a result of analyzing policy against new security threats, it can be summarized as follows. First, it is confirmed that protection of main infrastructure is achieved not only through system maintenance or regulation, but also through comprehensive response while considering various aspects. It is also desirable to have a security process for proactive and reactive responses. In other words, since the management security of the infrastructure that is currently recognized worldwide is not yet applied in law or policy, and the absence of a relevant guide is the chief issue, security training for accident prevention, expansion of security manpower, and accident occurrence are most critical. After that, a process should be established to minimize damage in the event of a situation, and to return to normal conditions as rapidly as possible. If relevant information is shared based on these processes, both precautionary and reactive measures are possible. It is possible to share information with each other by constructing a consultative body for each field during the specified period of time, and to respond promptly with related information and response systems in case of an incident.

Finally, in order to strengthen the cyber security of major pieces of infrastructure, it is necessary to establish an integrated response policy, design a security process, and establish a sharing system. This is also required for securing international trust for the sake of international cyber security.

References

[1]. John D. Moteff(2015), "Critical Infrastructures: Background, Policy, and Implementation", Congressional Research Service, Pages
[2]. 3-4.
[3]. Keith Stouffer, Victoria Pillitteri, Marshall Abrams, Adam Hahn(2015), "Guide to Industrial Control Systems(ICS)
[4]. Security(Revision 2)", NIST, pages 16-20.
[5]. WHITE HOUSE(2013), "Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection", www.whitehouse.gov/news/releases/2003/12/20031217-5.html
[6]. WHITE HOUSE(2013), "Presidential Policy Directive - Critical Infrastructure Security and Resilience",
[7]. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[8]. James Stenger(2013), "The EU Cybersecurity Directive will Follow the US Framework",
[9]. http://www.tmtperspectives.com/2013/11/05/the-eu-cybersecurity-directive-will-follow-the-us-framework/
[10]. Rafal Leszczyna, Elyoenai Egozcue(2013), "ENISA Study: Challenges for Secure Industrial Control Systems", Securing Critical Infrastructures Systems: Approaches for Threat Proteciton, Information Science Reference (an imprint IGI Global), Pages 110-113
[11]. NISC(2017), "The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)."
[12]. Korea National Law Information Center, Act on the Protection of Information and Communications Infrastructure.
[13]. Hong, Jonghyun, Cho, Yong-hyuk (2014), A Study on the Improvement of the Protective Act on Information and Communication Infrastructure, Korea Legislative Research Institute (Legal Analysis Supporting Study 14-12-②), Pages 99 ~ 100, 102 ~ 103.

Ji-Yeon Yoo " Analysis of Cyber Security Policy of Critical Infrastructure in Major Countries 0: Comparison of the Policies in the US, EU, Japan, and Korea." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 17-21.