Contemporary Engineering Sciences, Vol. 7, 2014, no. 32, 1755 - 1761
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.411235

National Cyber Threat Information Sharing System Strengthening Study

Chulki Jeong*

Sungkyunkwan University of Korea
*Corresponding author

Sungjin Ahn

Sungkyunkwan University of Korea

Abstract

As the global crisis is escalating on cyber safety, including the US, Europe, Japan governments to strengthen information sharing system for cyber attacks, especially civil and pipe stresses the need for sharing information and cooperation. Korea seeks to establish an effective response measures through improved protection system for geopolitical as always in aggressive competition with China, North Korea, Russia, Japan, USA, etc. as much as their neighbors in adjacent major information and communication infrastructure of the country.

Keywords: Critical Information and infrastructure Protection, Cyber Attack, Threat, Incident Response, Based

1 Introduction

Domestic corporations, financial institutions, media and government are constantly led cyber attacks targeting institutions, corporations and financial institutions in several large privacy breaches are occurring not far from the day. As the global crisis is escalating on cyber safety, including the US, Europe, Japan governments to strengthen information sharing system for cyber attacks, especially

civil and pipe stresses the need for sharing information and cooperation. Korea is located on the aggressive enemy is always competition between China, North Korea, Russia, Japan, and the United States in these neighboring countries such as neighboring countries equally vulnerable position of critical infrastructure and cyber attacks against corporate and industrial espionage targeting the Industrial Technology in the midst of. Recent cyber attacks are called APT (advanced persistent threat) attack the most various cyber attacks and then when you take advantage of the information collection and analysis techniques to prevent cyber attacks by hackers, and create a family tree for a hacker group, to defend and rapid recovery has become an important policy tool. In order to establish the hacker and countermeasures to support the technology developed by analyzing the behavior pattern of the hacker group must be introduced into the analysis system of shared public and private cyber attack information.

2 Recent Trends

The US telecommunications sector, IT sector, banking sector establishment, number and power sector of Information Sharing Analysis Center (ISAC) is operating, has, since September 11, the 17 pieces of information in the field of 18 is now expanded in 2013, the number gradually shared analysis Center (ISAC) has been identified as being founded, and operated. Information Sharing Analysis Center was established as gatgiro Committee will meet monthly to share information gathered representatives from each area analysis centers are voluntarily strengthen the trust relationship between information sharing and analysis centers dealing with common issues and concerns. There is also cooperation within the federal government system for enhancing information sharing through a public-private partnership. Critical infrastructure protection (CIP) as an initiative of the department of Homeland Security (DHS) is a kind of cyber threat information to the control center 'National Cyber Security and Communications Integration Center' (National Cybersecurity and Communications Integration Center, NCCIC) to leave, and that only and operates a number of organizations to strengthen public-private partnerships. The Homeland Security organization to respond quickly to the incident and provide technical assistance to an information processing system operators. CCIC is especially DHS and critical infrastructure partners to 24 hours a day, 365 days a common integrated response system for both the public and private sectors as the hub of a public-private partnership organization that is dedicated to the critical infrastructure protection in the United States by providing support in order to prepare the (common operating picture) to adjust the information gathered from a number of sources. The European Union is also especially critical information infrastructure cyber security, information network, the Member State level early in order to obscure the information system, etc. Of course, to expand the range of policies at Community level. However, EU member states have traditionally been

the need for monitoring a person's privacy online activities due to strong cyber safety or collect personal Internet traces, to hold a very negative. Japan May 21, 2013, organized the country's cyber security plan in 2015, which was published a draft of a "cyber security strategy. Because it is based on the recent Open Data and Big Data Intellgent Transport System (ITS) or smart grid, such as the national economy of IT systems that comprise them are used as growth factors and communication networks targeted cyber threats are increasing and the situation. The Japanese government has pointed out that the threat surrounding the cyber space increases, the threat of cyber-space have also been expanding influence in the real world will be established and existing under the judgment that the same strategies require different strategic approaches.

3 Status of Threat Information Sharing Infrastructure

Information Infrastructure Protection Act has been infringed by the accident analysis system for cyber attacks, information sharing and recovery scheme introduced a reporting and information sharing and analysis center system. The head of a major information and communications infrastructure management agency jurisdiction for infringement when the accident occurred shall promptly take necessary measures for the recovery and protection of your information and communication infrastructure, by notifying the incident to the management agencies contributed to the prevention of damage spreading government can financially support such a restoration expense within the budget Information Infrastructure Protection Act will establish information sharing and analysis center in order to protect the financial and telecommunications sector, including information and communication infrastructure, and regulations to operate. The government encourages the establishment of information sharing and analysis center and can provide technical support for it. Information Sharing and Analysis Center are: 1) the vulnerability and Infringement factors and provide information about the response measures, 2) When an incident occurs, it is to perform tasks such as real-time information and analysis of operating systems.

4 Issue of Cyber Threat Information Sharing System

South Korea is introducing a system of reporting and analysis on cyber threat information from various law-operated, but there is no institution that collects, analyzes in this comprehensive national information system owned by monitoring the cyber threat, information about the agency or organization that operates and investigation and shall not be authorized to be analyzed, the provision of cyber threat information with respect to the private sector, are not equipped with a device capable of incentives to encourage sharing. Information owned by the communication information-based protection system, which operates or information to share cyber threat information analysis center to monitor and

follow many legal risks directly to the cause and origin investigation and analysis.

Information system owner, operator provides the basis for the cyber threat information sharing and analysis center for information is unclear, and it is not even clear evidence of the collection. Exchange of cyber threat information, do not leave no provision for sharing. Therefore, information sharing and analysis center, even if the installation activities that can be done to the analysis of cyber threat information sharing, there are limits. Information Infrastructure Protection Act is to encourage the establishment of information sharing and analysis center, and shall not require to be able to provide technical support, but mandated the establishment of the Information Sharing and Analysis Centers for him, chapter of relevant central administrative agencies have a responsibility information There is also a device is not shared, it is not to be encouraged to build analytical center. Provide evidence of cyber threat information, and refine the criteria, scope, etc., for the parties to avoid reporting or provision of cyber threat information should be established penalties or sanctions regulations, incident report faithfully the facts and information or cyber threat information for the person who provides the faithful unless there is intention or gross negligence and for reduction of criminal liability and administrative responsibility should be to reduce the psychological burden from the punishment in accordance with the information-sharing concerns. Provide evidence of cyber threat information, and refine the criteria, scope, etc., for the parties to avoid reporting or provision of cyber threat information should be established penalties or sanctions regulations, incident report faithfully the facts and information or cyber threat information for the person who provides the faithful unless there is intention or gross negligence and for reduction of criminal liability and administrative responsibility should be to reduce the psychological burden from the punishment in accordance with the information-sharing concerns.

5 Cyber Security Threat Information Sharing System Improvements

First and foremost cyber threat information sharing in order to strengthen the system, shall be provided with a legal legal basis to share threat information without risk, and secondly, the vertical, horizontal integration, integration and sharing cyber threat information that can be analyzed center is required, and, third, collecting integrated cyber threat information in real time, analysis, a safe system can be propagated must be established. Incident reporting, recovery and information sharing, amending the Telecommunications Act that only regulations based installation based on the analysis of the incident, including information centers provide a basis for the overall cyber threat information sharing, and information sharing in the cyber-threat information system share, should strengthen the role of information sharing and analysis center so that the center can be a substantial role analysis. Information and communication based area communications, IT, finance, energy, transportation, health, healthcare, e-commerce,

education, research, water resources, chemical facilities, nuclear power, dam, defense, electronics, etc. separate and divided government, the central government of the jurisdiction at least one chapter in each area to share information analysis center installation or to specify. The main information and communication management agency designated as mandatory for all infrastructure should join the information sharing and analysis center of the field of jurisdiction, the system owner, operator or other information shall also support participation through a variety of incentives to join the Information Sharing Analysis Center. Information system owner, operator and specify the basis to analyze and collect information related to cyber threat to law, order this collection, use and type of information that can be provided with a range of information-gathering, use and method of providing should clarify.

Table 1. Type and timing of information sharing

Topics	Related Information	Time
Informative in terms of relapse prevention	■ disability cases: Content, causes, caused emergency measures and long-term measures, such as correlation	Usual
Informative in terms of prevention	■ laws and institutions, and information regarding climate change: international trends (criminal cases, disability cases, technology trends, etc.), the relevant instructions, Regulatory information, including statistical information into cyber attacks occur, information security policy Implementation Status information, measures, practices attack, attack, etc.), information security policy information (critical infrastructure management agency analysis reports, industry trends, best practices)	Usual
Information needed for disability prevention, recovery enlarge	■ attack warning signs · Related information: vulnerability-related information (information vulnerabilities, countermeasures), alert for signs of attack (attack symptom information, traffic information, observation, analysis, opinion), critical infrastructure, such as cyber attacks targeted ■ Information about individual threats (large cyber attack): Attack contents, attack techniques, Measures, Analysis views ■ IT failure information: disability information, causes, and corresponding measures, recovery expected, the correlation	Boundary requesting, in the event of a failure (Real-time required)

Information should be provided to collect and analyze cyber threat analysis centers to share information from national sources, future creation and Science, Department of Defense, and sword, police, etc., shall provide cyber threat information held on their 'ISAC Council.

6 Conclusion

First and foremost cyber threat information sharing in order to strengthen the system, shall be provided with a legal basis to share threat information without risk, and secondly, the vertical, horizontal integration, integration and sharing cyber threat information that can be analyzed center is required, and, third, collecting integrated cyber threat information in real time, analysis, a safe system can be propagated must be established.

Domestic and foreign cases of cyber attacks exploit the vulnerability of Internet connection, including a look at the rapidly increasing. Recently, broadcasting, financial and other countries have been increasing cyber attacks by hostile forces in the North, such as in the case of critical facilities of state government information security system has been strengthened measures are emerging as an important issue.

However, you can now specify criteria for major information and communication infrastructure vague designation of new enlarged to cause controversy on the nature of the critical facilities if there is not, or not systematically reflect changes in the underlying protection and regulatory work autonomously oriented activities and support improvement of the to exert a more effective system for the introduction of an incentive suggested in the study.

In the future, this designation is expanding infrastructure and facilities as specified in the various sectors support the promotion and regulation system in order to properly reflect the reliable protection system established by management than the measures that can be performed based on the secure protection and social services in the country continuously, it is necessary to research and development.

References

[1] State of Information Security White Paper (2013).

[2] Information Infrastructure Protection Act (2009).

[3] Korea Internet Security Agency (KISA), "Information Infrastructure Protection Guide"(2009).

[4] The White House, "Executive Order - Improving Critical Infrastructure Cybersecurity" (2013).

[5] Computerworld, "Obama to issue cybersecurity executive order this month" (2013).

[6] Computerworld, "Obama signs cybersecurity order" (2012).

[7] Department of Homeland Security, "ICS-CERT Incident Response Summary Report 2009-2011"(2012).

[8] Fierce, "Civil liberties watchdogs oppose Senate cybersecurity bill" (2012).

[9] Forbes, "President Obama's Cybersecurity Executive Order Scores Much Better Than CISPA On Privacy" (2012).

[10] Nextgov, "OBAMA’S CYBER EXECUTIVE ORDER LAYS FOUNDATION 10. FOR MANDATORY REGULATIONS"(2012).

Received: October 1, 2014; Published: December 2, 2014