A Study on Threat Containment through VDI for Security Management of Partner Companies Operating at Industrial Control System Facility

Sangdo Lee*, Jun-Ho Huh**
*Security and ICT Department, Cyber Security Control Team, Korea Hydro and Nuclear Power (KHNP) Co. LTD, Gyeongju, Republic of Korea
**Assistant Professor of Department of Data Informatics, Korea Maritime and Ocean University, Republic of Korea
**Corresponding author e-mail : 72networks@kmou.ac.kr

Abstract

The results from the analysis of recent security breach cases of industrial control systems revealed that most of them were caused by the employees of a partner company who had been managing the control system. For this reason, the majority of the current company security management systems have been developed focusing on their performances. Despite such effort, many hacking attempts against a major company, public institution or financial institution are still attempted by the partner company or outsourced employees. Thus, the institutions or organizations that manage Industrial Control Systems (ICSs) associated with major national infrastructures involving traffic, water resources, energy, etc. are putting emphasis on their security management as the role of those partners is increasingly becoming important as outsourcing security task has become a common practice. However, in reality, it is also a fact that this is the point where security is most vulnerable and various security management plans have been continuously studied and proposed. A system that enhances the security level of a partner company with a Virtual Desktop Infrastructure (VDI) has been developed in this study through research on the past performances of partner companies stationed at various types of industrial control infrastructures and its performance outcomes were statistically compiled to propose an appropriate model for the current ICSs by comparing vulnerabilities, measures taken and their results before and after adopting the VDI.

1. Introduction

It was reported in the 2017 ICS-CERT that the number of cases involving infringement on national infrastructure ICSs is rapidly increasing due to active cyberattacks which could not only result in simple financial loss but also devastating social damage or chaos often caused by their malfunction or unexpected interruption. Some of the typical examples include the blackout incident in Ukrain (Dec. 2015), power facility shutdown caused by the USB-embedded malignant code at a German nuclear power plant (Bavarian State, Apr. 2016), and the cyber threat against Korea Hydro & Nuclear Power (Dec. 2014) [1-2].

This study has attempted to induce a voluntary effort and investment for enhancing partner companies' information protection capability and developed a security index for special circumstances in terms of management, technical, and physical aspects. For the partner companies, security inspections were conducted periodically for each company according to their respective 'Class'. However, as their vulnerabilities in security had appeared repeatedly every year, this study proposes an innovative technological method which will be able to deal with cyberattacks by establishing a virtual environment.

2. Related Studies

Both domestic and foreign information protection/management systems were studied to investigate whether there are any control regulations for the management of partner companies and their contents were observed once they had been identified. For example, an information security certification ISO27001 evaluates security regulations for certification by each relevant area whereas ISO/IEC27001 originates from British BS7799 [3-5]. Being a typical standard for implementing an Information Security Management System (ISMS), this is being adopted widely by global companies as a procedure to assess their adequacy/capability in security policy and its execution as well as the ability in dealing with security threats [6-9]. This certification standard also assists an organization or firm in constructing a framework for adopting and implementing a Plan – Do – Check –Action (PDCA) model when establishing and executing an ISMS to perform monitoring, reviewing, maintaining, and improving security measures.

3. Establishment of Partner Company Security Management System Model

The partner company security management system should have professional and objective aspects as it is the standard index for security control, process planning, and security inspection tasks.

This study has proposed a partner company security management system model after establishing a security standard for designing and studying some of the actual application examples and based on this, the system was designed for application to increase effectiveness.

Approx. 1,000 companies were selected from a list of ICS companies who were in the contract period from 2014 to 2017 to establish a partner company security management

system model and based on each partner's characteristics, they were largely classified initially into four areas as service & construction, manufacturing & wholesale/retail, equipment repair, and auxiliary equipment companies <Table. 1> while analyzing their task- performing environment as well as the possibility and the impact of information leaks on the basis of the value of the information provided to them <Table. 2>.

<Table. 1> Classification of partner companies

	Company Type
1	Service & Construction
2	Manufacturing & Wholesale/Retail
3	Equipment Repair
4	Auxiliary Equipment

Depending on the significance of the value of information provided to the partner by the company, the impact of information leaks on the company can vary so that the risk of information leaks was considered along with the type of contract when classifying the partners <Table. 2>.

<Table. 2> The criteria for risk analysis

Criteria	Risk Analysis
Impact of information leaks	Value of information provided.
Possibility of information leaks	Task-performing environment of the partner

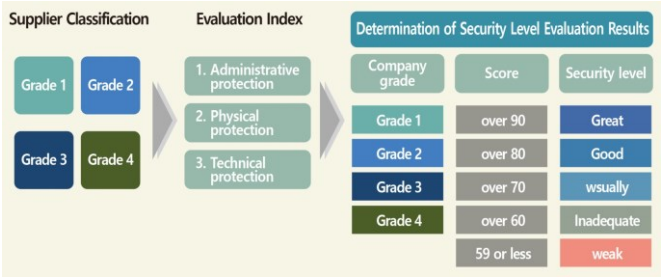
<Table. 3> is showing the criteria for classifying task-performing environment, where it is necessary to set criteria for requirements when distinguishing them by class. The criteria consisted of four situational categories: Whether they 'stay within the company at all times', 'perform their tasks by accessing the internal network or intranet of the company', 'share important information with the company by accessing the internal network', and 'are connecting with a separate internet internally'. Various aspects of their internal and external environments were analyzed for classification.

<Table. 3> The criteria for analysis of the security environment of partner companies

No.	Criteria
1	Stationed within the company or otherwise.
2	Accessing the company's internal network or otherwise.
3	Handling the technical/technological information of the company or otherwise.
4	Using separate internet while stationed within the company or otherwise.

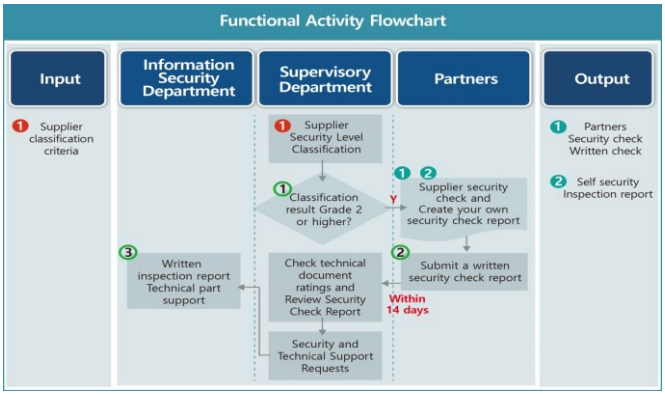
The level of documents handled by the company should be considered when establishing the criteria for classifying partners. First, the security levels should be set for each drawing, document, etc. to apply higher security to those which require confidentiality or allow sharing of lower-level documents to benefit both parties. Table 5 is showing a reference standard for determining which document or drawing corresponds to a particular grade or level. Grade A includes the key company information requiring special attention/management so that the company's fate may depend on it whereas Grade D is the lowest security grade and can be disclosed to the public or published, bringing no harm to the company.

Meanwhile, as in (Figure 1), the security level of each partner can be determined based on the classification procedure where each company is graded according to the index pertaining to management, physical, or technical/technological protection measures, identifying them as Excellent, Good, Normal, Poor, or Vulnerable. The companies belonging to the 1stClass will be inspected regularly to maintain their current excellent security level whereas those who fall short of the standard will be given a penalty.



(Figure 1) The evaluation standard based on the class of a partner.

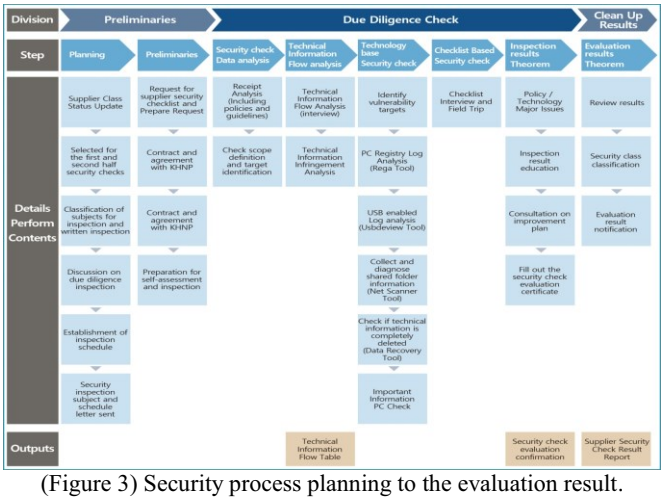
After classifying the partners based on the reference standard, security inspection should be performed next. (Figure 2) is showing the sample inspection procedure flowchart of company's supervising department when the partner belongs to the 2nd Class or above, where. self-inspection is performed by the partner first and the documented result will be reviewed by the company next. In this case, the information security department support is to support inspection or provide technical/technological support.



(Figure 2) Inspection flowchart for each partner.class.

The company's security dept. conduct inspections by splitting them into a spot or regular inspection. For the new contracts, an initial (new) inspection will be conducted and for the existing ones, regular inspections will be applied. In such cases, the partner submits the security report after conducting and diagnosing their own security activities and the company's security dept. reviews the written report and carry out an on-site inspection when it is deemed insufficient (Figure 3). However, if the partner has acquired the information security certification (e.g., ISO27001, CoBit, etc.) or complied with the required security process, the on-site inspection can be replaced with other means. Figure 3 is a detailed security inspection flowchart starting from the

security process planning to the evaluation result, where the partner's security level is determined based on the on-site evaluation result.



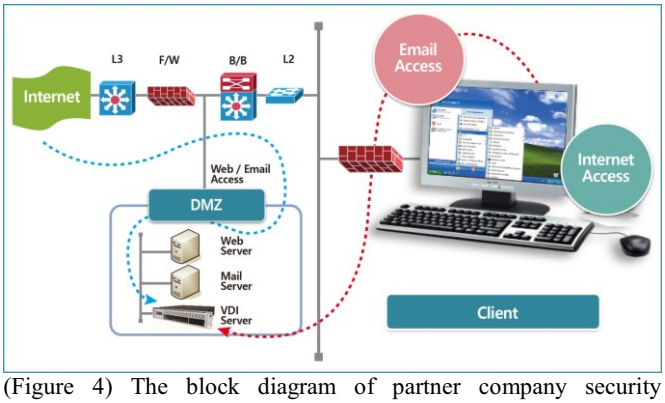
(Figure 3) Security process planning to the evaluation result.

4. Construction of Partner VDI System: Status of System and Network

The similar security incidents continuously occurred in the following year even the partners had been classified by developing an evaluation index and security inspections were carried out: the number of malicious code-based infections through the internet never decreased despite of constant education or guidance. At the same time, a new contract was awarded to other companies and the regulation violations by their employees did not stop so that a more systematic approach was necessary. Thus, a fundamental system that could reduce such a problem was designed by constructing a virtualization system to minimize internet access and strengthen data access control.

After evaluating and inspecting partner companies, there is an indispensable preliminary process when applying the virtualization system to all the partners stationed within the company – 'integrity check'. It has to be proven that there are not any malicious code (e.g., warm, virus, etc.) in the internal PCs as of 'now'. That is, the integrity level should be maintained at a 100% level so that the origins of future infections can be tracked while securing reliability. In this case, all the information systems including partner's PCs are checked with a vaccine program for their integrity as well as all other equipment/devices entering the control system even if they are to be used for testbed experiments or inspections. Those PCs cleared are called a Clean-Zone PC which is an independent PC and they are subjected to a vaccine test before accessing the control network and allowed to be brought in only after they have been cleared of any abnormalities.

When designing the partner security management system model, the focus was laid on controlling outside access from the company itself and the users to go through the approval process at the point of internet access. Also, a separate (exclusive) network for the partner company was constructed in a way to have the same security level with the company (Figure 4).



(Figure 4) The block diagram of partner company security management system.

This is the network configuration where all the partners stationed at individual branches are being connected. The networks connected from each area make outside access only after passing through the central security system where all the data exchanged by the partners will be checked by the spam mail server, APT detection system, etc, Meanwhile, each user is able to protect him/herself from malicious code or information leaks by establishing access through internet browser with his/her own designated account. For network security, the security system for network control consists of a firewall, IPS, NAC security equipment, etc. and a new mail server is provided to the partners. It is possible to use their own mail server but those who are stationed within the company must use the server provided by the company only as it is essential that the important materials leaving from the company have to be monitored and approved. Such a system is quite important when designing the system as it is necessary for inspecting the high-level security documents corresponding to A, B, or C level.

5. Conclusion and Future Work

A security management system for the partner companies working together at the industrial sites operating an ICS facility was designed in this study to propose an appropriate model along with an adequate technical/technological plan. The model worked flexibly during its full implementation. The necessity of strengthening the security management capability is often emphasized when developing an industrial control system in addition to constructing a technologically error-free security system such that this study presented a method of classifying the partner companies who are often remaining in a blind spot of security management based on the major security elements along with the management system appropriate for individual security levels. Also, a virtualization solution VDI was applied to allow the partners to use internet securely by preventing information leaks or protecting their system from any infections or attacks originating from the hackers using malicious code.

Acknowledgements

This work was supported by the this research was supported by the MSIT Ministry of Science and ICT), Korea, under the ITRC Information Technology Research Center) support program IITP-2019-2014-1-00743) supervised by the IITP Institute for Information & communications Technology

Planning & Evaluation). Also, this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2017R1C1B5077157).

References

[1] Diederik P. Kingma, Jimmy Lei Ba, “Adam: A Method for Stochastic Optimization,” ICLR Conference, 2015.
[2] Y. LeCun, Y. Bengio, G. Hinton, “Deep learning”, Nature, 521, pp. 436-444, 2015.
[3] P. Sermanet, D. Eigen, X. Zhang, M. Mathieu, R. Fergus, Y. LeCun. “Overfeat: Integrated recognition, localization and detection using convolutional networks,” CoRR, 2013.
[4] S. Chintala. convnet-benchmarks. https://github.com/soumith/ (accessed on 26 September 2019).
[5] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, M. Riedmiller. “Playing atari with deep reinforcement learning,” NIPS Deep Learning Workshop, 2013.
[6] Linux KVM. Available online: http://www.linux-kvm.org (accessed on 31 May 2019).
[7] VMware. Available online: http://www.vmware.com (accessed on 15 May 2019).
[8] Oracle VM Virtualbox. Available online: http://www.virtualbox.org (accessed on 15 May 2019).
[9] Lee Myanghee, Lee KyeongHo, “Study of collaborative company’s security management model for the nuclear safety operaion,” Proceedings of the ITFE Summer Conference, September 1-3, 2016.