International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.5 (2014), pp.301-306
http://dx.doi.org/10.14257/ijmue.2014.9.5.30

A Study on Efficiency of ISMS for ICS with Compliance

[
JunSeok Seo, Misun Song and Kyungho Lee

Center for Information Security Technologies, Korea University, Seoul, Korea
nababora@naver.com, { misun1535, kevinlee}@korea.ac.kr

Abstract

A policy is a set of ideas or plans that is used as a basis for making decisions, especially in politics, economics, or business, and it serves as a reference for the organization's activities or specific individual. In this sense, it is important to strengthen the capability of security performance. When it comes to Industrial Control Systems (ICS) which considerably affect the national security, policy compliance with consideration of ICS's characteristic is crucial. This paper is based on data from evaluating the degree of compliance of specific country's infrastructure with survey. Method used in this paper consists of four steps. First, an employee of specific company participates as a subject and evaluates the compliance of his/her organization with personal discretion. Second, determine criteria for further analysis. Third, analyze data for existence and compliance of policy. Fourth, calculate 'Policy-Domain-System (P-D-S)' index from data processed in the previous step. PDS and ISMS data can be used at the same time. This paper will contribute the efficiency of existing ISMS standard.

Keywords: *ICS, SCADA system, policy domain, compliance*

1. Introduction

Information technology has been applied to national Infrastructure like power generation, aviation transportation field by virtue of efficiency of operation and advanced IT system. The advantages of introducing ICS give the efficiency of operation and reliability of control. However, dangerousness and impact of hacking has increased either. In an effort to identify and prevent these types of security threats, International Organization for Standardization (ISO) had developed Information Security Management System (ISMS). Nevertheless, unique characteristic and impact of ICS have not been effectively considered for now.

The limitation of existing ISMS is that it only counts on one-dimensional evaluation for security policy which is fundamental to the ability of information security performance. With regard to efficiency, it is pointless to revise basic idea of existing ISMS or apply different criteria for different field. This paper suggests promising way of improving efficiency by analyzing policy compliance.

2. Data Collecting

To collect data for analyzing, specialized control item questionnaire was built with reference to 'NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations of the Industrial Control Systems Guidance'. The questionnaire consists of 17 domains and 88 sub-domains. Process to improve reliability was conducted in accordance with the evidence and its paper that is written by subjects for each control items in questionnaire. To increase understanding about the purpose of questionnaire, education was

ISSN: 1975-0080 IJMUE
Copyright ⓒ 2014 SERSC

conducted at each company. After that, distribute questionnaires to each operational center and take back when it is done.

3. Methods of analysis

This paper was written with the result of analyzing power generation specific data which is the most influential entity for power production in subject country. Besides, eight operational centers were selected to do a sample survey. Following flowchart shows the whole analysis process.

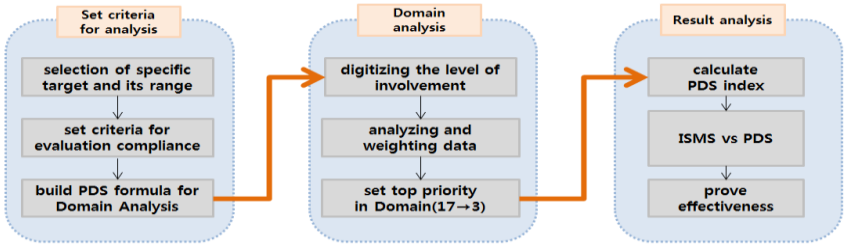

Figure 3.1. Flowchart of analysis

3.1. Set criteria for analysis

- **Select specific target and its range:** In the previous step, survey was conducted for different types of infrastructure field such as thermal, hydraulic, nuclear energy. Among them, the author selected 8 operational center of thermal power generation field which were considered as the biggest population after sorting questionnaires[1].
- **Set criteria for evaluation compliance**: Main variables in questionnaire are the control status, answer basis, evidence (paper). In case of control status, it is considered that 'Yes/No/Partial' as the group, and exclude 'N/A' items. Performing evaluation according to the presence of policy (paper).
- **Build PDS formula for domain analysis**: PDS index is an all-in-one factor with composition of policy existence, domain priority, and tailored policy existence. It ranges from 0 to 1(1 is the maximum score). The closer the PDS index to 1, the higher the level of compliance can be expected. Following flowchart shows formula deduction process and other details of PDS index.

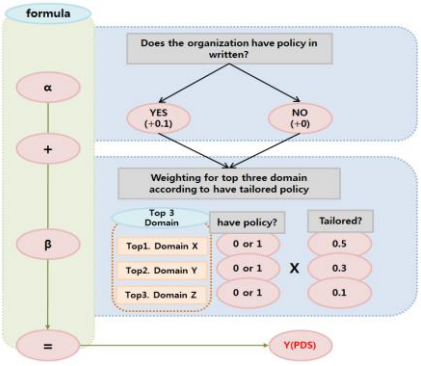

Figure 3.2. Flowchart and Formula of PDS Index

[1] Since the purpose of this paper is not on deducting correlation or common factor from analyzing as many number of cases as possible but to find out the level of compliance, the number of subject merely affect the result.

Copyright ⓒ 2014 SERSC

As Figure 3.2 suggested, set a score depending on the presence of policy[2] as to 17 domains in subject operational center. Here, a score '0.1' can be adjusted. Since the purpose of this paper is on evaluation of ICS specific policy compliance, '0.1' was chosen for the clarity[3]. Next, re-evaluating(0 or 1)[4] on the presence of policy for top three domains from analysis and deduction is conducted, and then multiply this factor(0 or 1) and tailored weight(0.1~0.5). 'Tailored weight' is a value for checking policy suitability (papers) whether it is related to characteristic of ICS. A following formula explains the way of deducing PDS index.

α = has policy(+0.1) or doesn't have policy(+0.0)
β = has policy for specific domain(1) * has tailored policy for ICS(weight)

$$\mathbf{y = \alpha + \beta}$$

PDS index = policy existence + $\sum_{n=1}^{3} Dn(policy\ existence * tailored\ policy\ existence)$

3.2. Domain Analysis

- **Analyze the level of involvement in a domain**: In questionnaire, the level of involvement is divided into 5 levels (very low ~ very high). Weighting on answers (very low:1 ~ very high:5) as to the level of involvement for all 17 domains, scoring and digitizing the degree of involvement for each operational center
- **Analyze the level of involvement in a domain**: In questionnaire, the level of involvement is divided into 5 levels (very low ~ very high). Weighting on answers (very low:1 ~ very high:5) as to the level of involvement for all 17 domains, scoring and digitizing the degree of involvement for each operational center.
- **Set the top three domains**: Based on the digitized data from previous analysis, arranging the degree of involvement descending order, and select the top three domains of them. The author made a decision that no one could know which policy the company has, and what policy they have to apply for each domain. In this sense, the author made a premise that employee has to know what they need at least in top three domains (the highest degree of involvement). Clearly separated domain[5] uses three domains from its own priority. Domain that separated ambiguously (ex) in the case of score - 1,2,3,3,3,3,3) uses the top three standard domain deducted based on the average score of domain involvement).

3.3. Result Analysis

- **Calculate PDS index**: Calculate the PDS index based on the formula that is defined in the previous step. As mentioned before, 'policy presence' score is determined according to exceed/not exceed of average score. Domain evaluation score (top 3) corresponding 'β' is determined by the 'evidence paper' which is written by subject. The presence of 'tailored policy' is determined depending on the keyword in paper title. If keywords in paper title do not have the relation with specific ICS, it is considered as 'this organization does not have tailored policy'.

[2] This step verifies the reason subject's answer is based on policy paper. To ensure objectivity in judging the presence of policy, it uses the same algorithm used in evaluating the level of domain involvement. For instance, digitizing (0~1) the number of existing 'policy paper' for each 10 items except 2 NA among 12 questions in domain one, and then calculate average score of all 17 domains. If result score exceeds the average score, it is considered that 'subject has policies(get score 0.1)

[3] The reason why 0.1 was chosen will not be handled in this paper. In short, '0.1' is clearer for analysis than other rate.

[4] The first step of checking the presence of policy is focused on the whole 17 domains. In Second step, the range of 'checking' varies from first step. It evaluates only for top 3 domains

[5] For example, in the case of extracting 2 domains from 6 domains and total score is [1,2,3,4,5,6], it is not difficult to identify top 2 domain(5,6).

Copyright ⓒ 2014 SERSC

- **Correlation analysis between ISMS and PDS index**: To prove the effectiveness of PDS index, correlation analysis was carried out between two factors. Although ISMS score does not affect the success of certification audit in reality, control status (Yes/No/Partial/NA[6]) is used to digitize ISMS score. Since this is for only comparison, calculating ISMS score exact same domain from PDS analysis
- **Result analysis**: Based on the PDS index and graph, make a conclusion or new assumption for further analysis.

4. Result

ISMS score was calculated by following rules. First, same domain was chosen from PDS index to even the variance of PDS index. Second, score ranges from 0 to 1. 1 means all control status (answers) were marked with 'Yes'.

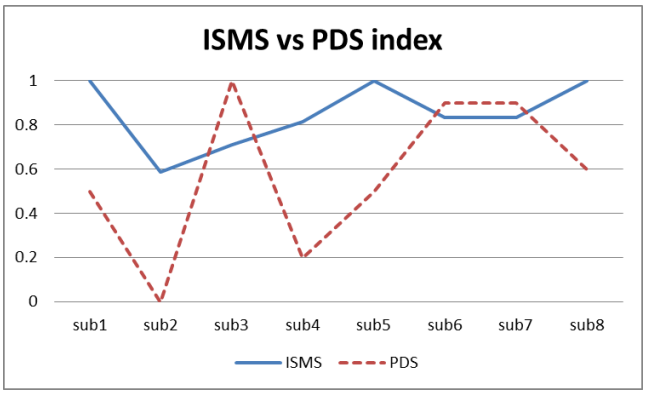

Figure 4.1. ISMS versus PDS Index

Figure 4.1 suggests that only sub3,6,7 of PDS index scores are higher than ISMS score, and sub1,2,4,5,8(0.63% of total) of PDS index scores are lower than ISMS score. In other words, 60% of subject are not compliance with the policy they have. It is definitely true that effectiveness of PDS index is valid.

5. Conclusion

The purpose of this paper is to find out subsidiary security index that can help enhancing the efficiency of existing ISMS, especially for ICS-ISMS. All data and assumptions were rest on questionnaire collected from national infrastructure. Specifically, this paper focuses on 8 operational centers of thermal power generation. Through the analysis, the effectiveness of PDS index was proved successfully. Nevertheless, there are hidden variables the author could not catch, and it restricts only on thermal system. With efforts on eliminating errors and exceptions, PDS index can be applied to any field that has unique characteristic (organizational and technical) such as ICS.

Acknowledgements

The work was supported by a Korea University Grant.

[6] Yes=1 / Partial=0.5 / No=0

 Copyright ⓒ 2014 SERSC

References

[1] Policy, http://en.wikipedia.org/wiki/Policy
[2] NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations of the Industrial Control Systems Guidance.
[3] NIST 800-55 Performance Measurement Guide for Information Security.
[4] NIST 800-82 Guide to Industrial Control Systems (ICS) Security.

Authors

JunSeok Seo, he is now a Master Course in Graduate School of Information Management and Security(Samsung Track) at Korea University since 2014.

Misun Song, she is now a Master Course in Graduate School of Information Management and Security at Korea University since 2013.

Kyungho Lee, he received his Ph.D. degree from Korea University. He is now a Professor in Graduate School of Information Security and Security at Korea University, and leading the Risk management Laboratory in Korea University since 2012. He has a high level of theoretical principles as well as on-site experience. He was a former CISO in NAVER Corporation, and now he takes as the CEO of SecuBase Corporation. His research interests include information security management system (ISMS), risk management, information security consulting, privacy policy, and privacy impact assessment(PIA).

Copyright ⓒ 2014 SERSC

Copyright ⓒ 2014 SERSC