Research Article

A Study on Industrial Security Experts Demanding Forecasting in Intelligent Sensor Network

Hyungwook Yang,1 Hyeri Kim,1 and Hangbae Chang2

1Department of Information Security Management, Sangmyung University, Seoul 110-743, Republic of Korea
2Department of Industrial Security, College of Business & Economics, Chung-Ang University, Seoul 156-756, Republic of Korea

Correspondence should be addressed to Hangbae Chang; hbchang@cau.ac.kr

Received 30 September 2014; Accepted 17 November 2014

Academic Editor: Naveen Chilamkurti

Copyright © 2015 Hyungwook Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

There have been efforts made to come up with a solution through advancement based on developing technological solution. However, it has come to the point where various forms of the leakage centering on people that are the subject of core asset leakage cannot be solved through technological method. At present time in which the limitation of information security that seeks technological solution has been clearly revealed, there is an increasing interest in industrial security for establishing convergence security system upon understanding technological/physical/managerial security measures and establishing security strategies. Accordingly, this paper conducted an analysis on the characteristics of industrial security manpower to present a vision and systematically cultivate industrial security experts manpower for protecting core technologies of companies in intelligent sensor network. In particular, occupational cluster of industrial security experts manpower was classified, which was verified by conducting case analysis. In addition, it estimated the demand for industrial security experts manpower by substituting it to the present condition of manpower of Korea. It is expected that the result of this study will be able to be used as basic information for cultivating industrial security experts manpower in intelligent sensor network.

1. Study Background

In recent years, computing environment is rapidly changing into ICT convergence environment using intelligent sensor network that is a form of convergence of ICT-traditional industry upon converging with various existing industries. For the purpose of gaining competitive advantage in the midst of such environment, companies are seeking corporate informatization innovation [1, 2]. Such innovation is becoming a means of ensuring corporate competitiveness through productivity enhancement and transaction cost reduction by advancing computing environment instead of simple changes in corporate management environment.

In recent years, the change into computing environment that is a means of informatization innovation of companies has become an essential element [3]. In computing environment, a company’s core assets need to be safely protected by converting them into information for storage in an intangible state [4, 5]. However, such core assets are being easily leaked outside or to competitors. Such leakage of core asset is not only causing enormous damage to respective company but also affecting industry, society, and nation.

For the purpose of preventing the leakage of core assets that impedes the continuous growth of organization, there have been efforts made to come up with a solution through advancement based on developing technological solution. However, it has come to the point where various forms of the leakage centering on people that are the subject of core asset leakage cannot be solved through technological method. In the case of Korea, particularly, the main causes of technology leakage involve internal leakage by former/current employees that occupies about 80% in addition to external cyber-attack such as hacking and malware. It is also followed by technology leakage by partner companies with a continuous increasing trend of technology leakage resulting from financial allurement and personal profit.

In the midst of the current situation in which the limitation of information security that pursues technological
security has been clearly revealed, there is an increasing interest in industrial security for developing convergence security system by establishing security strategy upon understanding technological/physical/managerial security measures. However, definition and job form of manpower in particular areas vary according to society, company, and national environment and system. In the case of Korea, the present condition is that analysis of job skills of manpower that will be responsible for industrial security area is lacking compared to that of information security manpower that has already been systemized.

Accordingly, the purpose of this study is to perform analysis on the characteristics of industrial security manpower and analyze according manpower demand research to present vision and systematically cultivate industrial security experts manpower to protect corporate core technologies in intelligent sensor network environment.

2. Previous Studies

2.1. Information and Industrial Security Comparison in Intelligent Sensor Network Environment. Li and Tang [6] have proposed a conceptual framework of information security engineering. This framework explicitly illustrates the methodological system, content system, procedures, and strategies for information security engineering research and practices.

Siponen and Willison [7] have analyzed BS7799, BS ISO/IEC17799: 2000, GASPP/GAISP, and SSE-CMM to determine and compare how these guidelines are validated and how widely they can be applied.

Gillies [8] has proposed a step-by-step framework designed to simplify the process for organizations working towards ISO27001 and offer significant benefits at milestones before systems are mature enough to achieve certification.

Vaughn Jr. et al. [9] have presented lessons learned and observations noted about the state of security-engineering practices by three information security practitioners with different perspectives.

Naedele [10] has examined the interests of the various stakeholders in the industrial security field (e.g., society, plant owners, service providers, automation vendors, and consultants) and evaluated some of the more visible industrial security initiatives (ISA, NERC, and IEC) with regard to stakeholder benefits and requirements. The paper then proceeds to give some details on the approach and current draft of the industrial control system security working group within IEC TC65.

Li [11] has discussed three tiers of the concept of industry as required by the study.

2.2. Manpower Skills Framework Study. Baraglia et al. [12] have proposed a new multicriteria job scheduler for scheduling a continuous stream of batch jobs on large-scale computing farms. Our solution, called convergent scheduler, exploits a set of heuristics that drives the scheduler in taking decisions. In order to validate the scheduler we proposed, it has been compared versus two common job scheduling algorithms.

Gould et al. [13] have considered the implications for nurses and their managers and the impact on university departments delivering continuing professional development for nurses. The new system has the potential to increase the human resources management aspect of the clinical nurse managers’ role and could have legal implications, for example, if practitioners perceive that their needs for continuing professional development have been overlooked to the detriment of their pay and career aspirations. The new system also has implications for providers of continuing professional development in the universities and is likely to demand closer liaison between education providers and trust staff who commission education and training. The knowledge and skills framework is of interest to nurses and nurse educators internationally because the system, if effective, could be introduced elsewhere.

Walsh et al. [14] have presented the development of an interprofessional capability framework that articulates the learning outcomes that students need to achieve and continue to develop in order to become capable interprofessional workers. Although there tends to be a general agreement on the subject matter to be included under the rubric of interprofessional learning, little information is available regarding the learning outcomes students need to achieve in order to become effective interprofessional workers.

3. Industrial Security Experts Analysis in Intelligent Sensor Network Environment

3.1. Industrial Security Experts Structure Analysis (the Korean Case). Industrial security experts manpower refers to experts manpower that has expert knowledge (capabilities) in managerial, physical, and technological security methods for industrial security based on extensive understanding on industrial security studies to protect industry technologies from encroachment elements and perform the duties of preventing illegal leakage and damage from disasters. It can also be understood through an extended scope including the protection of intangible assets from disasters such as fire, quake, and calamity, in addition to man-made disaster such as illegal leakage of industry technology.

For the purpose of analyzing the job skills of industrial security experts manpower, the literature research on industrial security occupational cluster and expert interviews were performed.

Occupational cluster of industrial security experts manpower can be mainly classified into industrial security planning and operation and industrial security method (measure). Industrial security planning and operation occupational cluster can be segmented into industrial security consulting (diagnosis), industrial security compliance (law), industrial security education, industrial security management (policy design and operation), and industrial security certification evaluation (inspection). The segmented occupational cluster can be defined as follows.

First off, industrial security consulting (diagnosis) occupational cluster refers to an expert occupational cluster
that diagnoses the present condition of industrial security of organization to effectively (efficiently) respond against acts of industry technology leakage and present according countermeasures. Next, industrial security compliance (law) occupational cluster refers to experts that instruct and manage specific regulations and guidelines related to industrial security laws. In addition, industrial security education occupational cluster refers to experts that plan and perform education for organizational constituents to increase their awareness of industrial security and increase knowledge (capability). Industrial security management (policy design and operation) occupational cluster refers to experts that design policies from the perspective of organizational management for industrial security activities and implement (visualize) and operate industrial security activities. Lastly, industrial security certification evaluation (inspection) occupational cluster refers to experts that certify and evaluate organization on its status of establishing and operating management system to protect industry technologies.

The industrial security method (measure) occupational cluster can be segmented into industrial security system development and establishment, industrial security guard and surveillance, and industrial security encroachment accident response (investigation). The segmented occupational cluster is defined as follows.

First off, industrial security system development and establishment occupational cluster refers to experts that develop, establish, and operate IT security system (document security system, database security system, network security system, etc.) to protect industry technology within organization. In addition, industrial security guard and surveillance occupational cluster refers to a group of experts that develop, establish, and operate physical security system (guard system, surveillance system, etc.) to protect industry technologies within organization. Lastly, industrial security encroachment accident response (investigation) occupational cluster refers to experts that perform activities of encroachment accident detection, early response, research (investigation), security measures, and follow-up measures.

These industrial security experts manpower occupational clusters can be displayed as shown in Figure 1.

### 3.2. Industrial Security Experts Manpower Skills Analysis

In regard to the industrial security experts manpower occupational clusters classified based on previous literature research and expert meeting, their types and percentages will be analyzed in addition to the main duties. Accordingly, survey research was conducted with 63 demand organizations that need industrial security experts manpower.

First off, current status on the retention of industrial security product/service experts manpower was examined. For the purpose of researching the percentages (%) of industrial security product/service experts manpower, they were classified into security consulting, security system, security guard, security control, security education, security inspection/certification evaluation, and others based on a pilot test of previously classified industrial security experts occupational clusters.

In regard to industrial security experts manpower, security guard manpower occupied 57.4% in terms of simple number of manpower, thereby revealing the highest in number. It can be recalculated as shown in Figure 2 (the circle in the right side) as you look in detail the part excluding security guard manpower for physical security measures, and general administrative manpower and remaining classification of industrial security other occupational clusters. As for the percentages of manpower that comes up with technological security and managerial security measures, they were found to be in the order of 34.9% for industrial security system development manpower, 33.1% for industrial security control experts manpower, and 30.3% for security consulting experts manpower (see Figure 2). In addition, the percentage
of security education and security inspection/certification evaluation manpower was found to be at a very low level.

Status on the availability of organization (staff) exclusively in charge of industrial security at target organization is as follows.

In the case of companies that have an exclusive organization consisting of more than two staffs, it was found that merely 6.3% and about 25.4% had only one dedicated staff. In particular, more than majority of the research targets were found to have no dedicated staff or staff that have additional duties (over 68.2%). Considering the seriousness of recent security accidents, establishing measures to supply manpower is urgently needed (see Figure 3).

The reason for not having such dedicated organization or staff in charge of industrial security was researched. The results were found to be in the order of high labor cost for industrial security experts manpower (37.3%), followed by cost and time required for internal education and training (22.4%). Accordingly, it would be necessary to supply well-qualified manpower that can meet the demand, along with education course for systematically reeducating existing business manpower (see Figure 4).
In addition, relatively organizational structure of industrial security staff (in charge) and information security (IT security) staff in charge was examined. In terms of industrial security staff (in charge) and information security (IT security) staff (in charge) within organization existing separately as equal status, as shown in Figure 5, the percentage was found to be the highest with 42.9%, followed by the case of having additional duties with 33.3%.

Meanwhile, main duties of industrial security experts manpower were analyzed and the result showed that they deal with multidimensional studies of law/policy, management, crime, and technology. As shown in Figure 5, academic system was classified and the most preferred major was engineering, followed by business and economics and law (see Figure 6).

In addition, the result showed that companies want certification education to quickly cultivate and supply industrial security experts manpower according to company scale, and, in the case of wanting multidimensional knowledge, the result showed that they preferred university curriculum.

3.3. Industrial Security Experts Manpower Demand Analysis. Based on the result of industrial security experts manpower job skills analysis, analysis was conducted to forecast the demand for industrial security experts manpower for the next five years for the advancement of industrial security and cultivation of manpower. For the demand forecasting of industrial security experts manpower, increase in the demand for industrial security manpower was forecasted by dividing the demand into new demand and alternative demand. The new demand refers to demand for manpower by organizations resulting from establishing industrial security dedicated organization. The alternative demand refers to demand for manpower resulting from retirement and job change of existing industrial security manpower.

Formula 1 (new demand formula). Consider

\[ (\text{New Demand}) = (\text{Number of Mean Manpower of Organization}) \times (\text{Industrial Security Experts Manpower New Hiring Percentage}) + (\text{Number of New Companies Created}) \times (\text{Number of Industrial Security Experts Manpower for Stable Security Management}). \]  

(1)
Formulas (alternative demand formula). Consider

\[
\text{Alternative Demand} = \left( \frac{\text{Number of Mean Manpower of Organization}}{1.0\%} \right) 
\times \left( \frac{\text{Retirement and Job Change Percentage}}{0.6\%} \right) 
\times \left( \frac{\text{Total Industrial Security Experts}}{1.0\%} \right)
\]

Based on the above formulas, major figures for forecasting industrial security experts manpower are as shown in Table 1.

These major figures were entered into the present condition of Korea to forecast the demand for industrial security experts manpower. The results are as shown in Table 2 showing that manpower demand of about 150,000 workers will occur in the next five years.

4. Conclusion and Future Study

In recent years, the change into computing environment that is a means of informatization innovation of companies has become an essential element. However, a company's core assets that need to be safely protected by converting them into

Table 1: Major figures for forecasting industrial security experts manpower demand.

| Description                                      | Percentage |
|--------------------------------------------------|------------|
| (i) Growth rate of number of workers             | 1.0%       |
| (ii) Growth rate of number of companies          | 0.6%       |
| (iii) Percentage of retirement and job change    | 1%         |
| (iv) Percentage of industrial security experts manpower retention | 31.7% |
| (v) Percentage of industrial security experts manpower new recruitment | 8%        |

information for storage in an intangible state are being easily leaked outside or to competitors. Such leakage of core asset is not only causing enormous damage to respective company but also affecting industry, society, and nation.

For the purpose of preventing the leakage of core assets that impedes the continuous growth of organization, there have been efforts made to come up with a solution through advancement based on developing technological solution. However, it has come to the point where various forms of the leakage centering on people that are the subject of core asset leakage cannot be solved through technological method.

At present time in which the limitation of information security that seeks technological security has been clearly
Table 2: Industrial security experts manpower demand forecast (the Korean case).

| Classification               | 2015 (Y) | 2016 (Y) | 2017 (Y) | 2018 (Y) | 2019 (Y) |
|-----------------------------|----------|----------|----------|----------|----------|
| New demand                  | 27,376   | 27,540   | 27,706   | 27,872   | 28,039   |
| Alternative demand          | 2,190    | 2,203    | 2,216    | 2,229    | 2,243    |
| Total demand                | 29,566   | 29,743   | 29,922   | 30,101   | 30,282   |

(revealed, there is an increasing interest in industrial security for establishing convergence security system upon understanding technological/physical/managerial security measures and establishing security strategies.

Accordingly, this paper conducted an analysis on the characteristics of industrial security manpower to present a vision and systematically cultivate industrial security experts manpower for protecting core technologies of companies. The result can be summarized as follows.

(i) Occupational cluster of industrial security experts can be mainly classified into industrial security planning and operation and industrial security method (measure). Industrial security planning and operation occupational cluster can be segmented into industrial security consulting (diagnosis), industrial security compliance (law), industrial security education, industrial security management (policy design and operation), and industrial security certification evaluation (inspection). Industrial security method (measure) occupational cluster can be segmented into industrial security system development and establishment, industrial security guard and surveillance, and industrial security encroachment accident response (investigation).

(ii) Among the classified industrial security experts manpower occupations, security consulting, security system, security guard, security control, and security investigation/certification evaluation manpower occupied about 80% of the entire industrial security manpower.

(iii) Industrial security staff (in charge) and information security staff, security system, security guard, control), and security investigation/certification evaluation manpower were mostly highly distributed with equal structure of relative status within organization.

(iv) It was found that convergence knowledge in various aspects consisting of engineering, business and economics, law, and humanities and society was needed as job skills of industrial security experts manpower.

(v) It is expected that the result of this study will be able to be used as basic information for cultivating industrial security experts manpower in intelligent sensor network. As for future study, a study on the present condition of industrial security experts manpower demand and job transfer path will be conducted.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1018) supervised by the IITP (Institute for Information & Communications Technology Promotion). This work was also supported by the Human Resources Development (no. 20154030200860) of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea Government Ministry of Trade, Industry and Energy.

References

[1] M. Kim, S. O. Park, W.-K. Joo, K. Choi, Y.-S. Jeong, and Y.-K. Kim, “Tag based collaborative knowledge management system with crowdsourcing,” Journal of Internet Technology, vol. 14, no. 5, pp. 859–866, 2013.

[2] C. Pearce and J. Marshman, “A framework for specialist nurses,” Nursing Management, vol. 15, no. 3, pp. 18–21, 2008.

[3] I. Choi, S. Rho, and M. Kim, “Semi-automatic construction of domain ontology for agent reasoning,” Personal and Ubiquitous Computing, vol. 17, no. 8, pp. 1721–1729, 2013.

[4] C. Ichniosvski, K. Shaw, and G. Prentushi, “The effect on human resource management practices on productivity: a study of steel finishing industry,” American Economic Review, vol. 87, no. 3, pp. 291–313, 1997.
[5] H. Cornor, J. Hillage, J. Millar, and R. Willison, *An Assessment of Skill Needs in Information and Communication Technology*, NTO (National Training Organizations), New South Wales, Australia, 2002.

[6] M. Li and M. Tang, “Information security engineering: a framework for research and practices,” *International Journal of Computers Communications & Control*, vol. 8, no. 4, pp. 578–587, 2013.

[7] M. Siponen and R. Willison, “Information security management standards: problems and solutions,” *Information and Management*, vol. 46, no. 5, pp. 267–270, 2009.

[8] A. Gillies, "Improving the quality of information security management systems with ISO27000," *The TQM Journal*, vol. 23, no. 4, pp. 367–376, 2011.

[9] R. B. Vaughn Jr., R. Henning, and K. Fox, "An empirical study of industrial security-engineering practices," *Journal of Systems and Software*, vol. 61, no. 3, pp. 225–232, 2002.

[10] M. Naedele, "Standardizing industrial IT security—a first look at the IEC approach," *Emerging Technologies and Factory Automation*, vol. 2, pp. 857–863, 2005.

[11] M. Li, *Research on Industrial Security Theory*, Springer, Berlin, Germany, 2013.

[12] R. Baraglia, G. Capannini, P. Dazzi, and G. Pagano, "A multi-criteria job scheduling framework for large computing farms," *Journal of Computer and System Sciences*, vol. 79, no. 2, pp. 230–244, 2013.

[13] D. Gould, E.-J. Berridge, and D. Kelly, "The national health service knowledge and skills framework and its implications for continuing professional development in nursing," *Nurse Education Today*, vol. 27, no. 1, pp. 26–34, 2007.

[14] C. L. Walsh, M. F. Gordon, M. Marshall, F. Wilson, and T. Hunt, "Interprofessional capability: a developing framework for interprofessional education," *Nurse Education in Practice*, vol. 5, no. 4, pp. 230–237, 2005.
