ICIC Express Letters
Part B: Applications
Volume **11**, Number **9**, September **2020**

ICIC International ©2020 ISSN 2185-2766
pp. **881–887**

A STUDY ON THE COMPETENCY SYSTEM DESIGNING FOR THE PROFESSIONAL TRAINING IN INDUSTRIAL TECHNOLOGY OUTFLOW INVESTIGATION

Juyeon Ji[1], Jongwan Kim[2] and Hangbae Chang[3]

[1]Douzone
130, Beodeul 1-gil, Namsan-myeon, Chuncheon-si, Gangwon-do 24465, Korea
juyeonji@douzone.com

[2]Security Convergence
[3]Industrial Security
College of Business and Economics
Chung-Ang University
84, Heukseok-ro, Dongjak-gu, Seoul 06974, Korea
{ winstreet; hbchang }@cau.ac.kr

Received March 2020; accepted June 2020

Abstract. *With the advent of the 4th industrial revolution recently, it is changing into a future industrial convergence environment. The number of attacks on the outside and cybercrimes (crime using information technology) based on unspecified majority is increasing every year because of the changing environment. As the risk of industrial technology outflow increases and the damage size increases, the demand for industrial technology outflow investigation personnel is increasing, and crime of industrial technology outflow is becoming more intelligent. Accordingly, it is urgent to introduce state-of-the-art investigative equipment and foster experts in industrial technology outflow investigations that can be utilized. The final goal of this study is to design a "preemptive degree curriculum" as the future convergence environment progresses. Through this, the government intends to solve the problem of supply and demand of manpower specialized in investigation of outflow of industrial technology. In addition, we intend to contribute to enhancing the professionalism of the investigation personnel for industrial technology outflow. The capacity system for industrial technology outflow investigation will be designed to foster expert personnel for industrial technology outflow investigation with multidimensional security capabilities.*

Keywords: Industrial technology outflow investigation, Demand capacity, Capacity system

1. **Introduction.** With the recent advent of the fourth industrial revolution and changing into a future industrial convergence environment, the scope of security risks is expanding in convergence and new security threats are emerging. Risk of leakage of industrial technology through various methods, such as industrial espionage, scouting and hiring of research technology personnel, information theft using hacking, camouflage infiltration, eavesdropping or eavesdropping, information gathering through information brokers or lobbyists, information gathering through accountants, lawyers or consultants, illegal trespassing and theft or robbery is increasing.

The use of information technology is increasing risks from outside companies as they increase their work efficiency and convenience. As many of the businesses' operations have changed to Internet-based forms of work, the method of leakage has been advanced and the route of leakage has also diversified. Most of the crime traces are left in digital data,

DOI: 10.24507/icicelb.11.09.881

as the traditional criminal forms that occurred offline in the past have been converted into online cybercrime via the Internet.

The National Police Agency detected a total of 90 industrial technology leaks over the past six years (from 2012 to 2017), including those involving the state core technologies such as electricity, electronics, information and communications, and violations of business secrets. Such leaks of technologies of great economic value are increasing the risk of national wealth being leaked [1].

In this study, with the aim of designing a "preemptive degree course" level curriculum according to the future convergence environment, a capacity system is designed to nurture expert personnel for industrial technology leakage investigation and to solve the problem of difference in supply and demand of expert personnel for industrial technology leakage investigation by fostering expert personnel with multi-dimensional security capabilities, and to contribute to enhancing the expertise of industrial technology leakage investigation personnel.

2. Previous Research.

2.1. **A study on the feasibility study and analysis of fitted degree.** Conformity reflects information about whether the indicators have faithfully measured what they intend to measure. A suitability survey is a survey that measures how appropriate and relevant a survey item is.

The survey format is conducted in a multiple-choice format with a five-point scale (1-very unsuitable, 2-inadequate, 3-infinite, 4-inadequate, 5-very suitable) to measure the validity of each influencing factor.

The reliability verification will be analyzed by the Cronbach Alpha (α) coefficient, and the feasibility (acceptibility, discrimination) verification is to be verified by the exploratory factor analysis [2].

2.2. **Priority survey and analysis.** The Analytic Hierarchy Process-Layer Analysis Method (AHP) is one of the many-reference decision-making methods developed by Saaty and Forman (1993) and has been applied in various fields. Because AHP analysis is determined by the evaluator's response, evaluators' responses should be consistent unlike general statistics, AHP analysis requires securing sufficient number of samples to maintain a normal distribution, but experts with sufficient experience and knowledge are more important [3,4].

2.3. **Industrial technology leakage and industrial security of companies.** Industrial security is the sum of industrial assets to be protected by businesses from criminal acts and industrial technology and confidential activities that can have technological competitiveness. Under the Industrial Security Practice published by the Graduate School of National Intelligence, industrial security as an activity protects all useful management, technical information, documents, facilities, materials, personnel, and others from leakage or encroachment to persons who are not related [5].

2.4. **Specialized personnel for industrial technology leakage investigation.** As the act of industrial technology leakage investigation indicates the nature of industrial technology leakage, it was emphasized that it was necessary to train professional investigation personnel to actively cope with the leakage of industrial technology. The education contents of the preceding studies of the experts in industrial technology leakage investigation remain in the short-term education process, and the subject form was shown in micro capacity form. The purpose of this study is to develop a macroscopic curriculum-type competency system for the purpose of designing pre-emptive degree-level curriculum based on the future convergence environment by organizing prior studies [6,7].

2.5. **Cybercrime Investigation Body of Knowledge (CIBOK).** Twelve legal, judicial, and industry leaders, as well as 14 selection judges from three countries, were first published in November 2016 with the approval of the CIBOK Steering Committee to create a knowledge system for developing cybercrime investigation standards. In conducting cybercrime investigation in the changing cyber environment, the aim is to help law enforcement agencies and cybercrime investigation teams deal with cases accurately and systematically. In this book, the cybercrime investigation execution framework is a classification-based framework of defined requirements for cybercrime investigation and security improvement that enables cybercrime to be processed and communicate efficiently. The figure below shows the correlation with the eight factors necessary for the proper process of cybercrime investigation, and each element contains the knowledge area and nature of the cybercrime investigation process. The CIBOK cybercrime investigation components are Scope of Cybercrime, Cybercrime Artifact, Type of Cyber time, Method of Analysis, Source of Evidence, Method of Collection, Information Sharing, and the details are shown below [8].

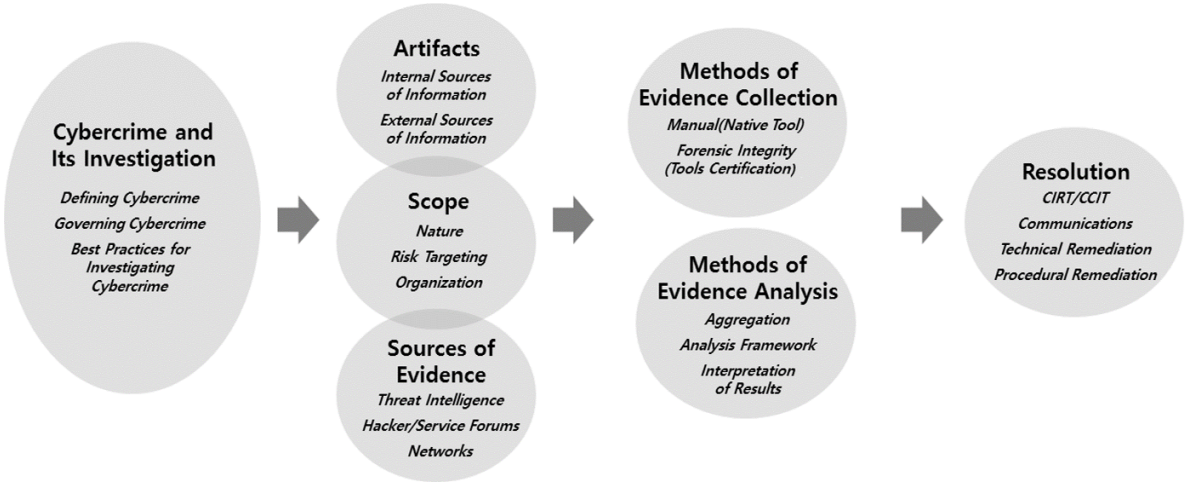

FIGURE 1. CIBOK cybercrime investigation components

3. Control Design.

3.1. **Design of capacity required for industrial technology leakage investigation.** It was derived from prior research in various related fields to design the required capacity for industrial technology leakage investigation. There are a total of 14 prior studies to be analyzed, consisting of various types of industrial technology leakage, digital forensics, cyber security, industrial security, etc. It also conducted an interview (FGI, Focus Group Interview) with eight experts on industrial technology leaks, including academia, the National Police Agency and the Ministry of Small and Medium Venture Business.

Demand for industrial technology leakage investigation derived through prior research and focus group interviews is found in the Act on the Prevention of Unfair Competition and the Protection of Trade Secrets, the Act on the Prevention and Protection of Industrial Technology, the Defense Industry Technology Protection Act, the Civil and Criminal Procedure, Criminal Psychology (Criminal Theory), Criminal Case, Detection and Inspection (Pure Investigation), and the seizure of initial detection and seizure.

3.2. **Research subjects and data collection methods.** In order to design the capacity system for industrial technology leakage investigation, which is the final goal of this study, the targets were selected for verifying suitability of the required capacity for industrial technology leakage investigation and for conducting surveys for verifying the capability system for industrial technology leakage investigation.

Verification of suitability of the required industrial technology leakage investigation is planned for 50 or more employees with more than three years experience in the field as an industrial security expert. Although the number of samples may be determined to be small, it is believed that the results will be sufficient to demonstrate the reliability of the study results, as the subjects of the study were selected and conducted with a high quality overall.

This study is conducted in five stages: related literature studies, design requirements for industrial technology outflow investigation, verification and analysis of core capabilities of industrial technology outflow investigation, weight analysis of core competencies for industrial technology outflow investigation, design of industrial technology outflow investigation capability system. The research method and procedure are as follows.

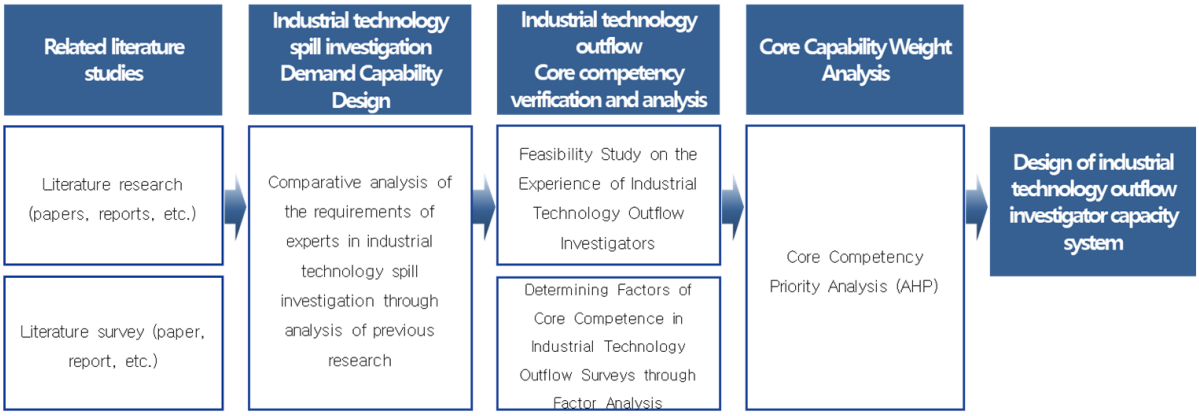

FIGURE 2. Design of industrial technology outflow investigator capacity system

4. Main Results.

4.1. Adequacy and feasibility of industrial technology leakage investigation.

The selection of a survey population to achieve the purpose of this study and to find out the adequacy of the items of measurement produced was made to experts with experience in "industrial technology outflow investigation".

(Using Advanced Technology) Evidence management and protection, digital forensics, evidence confirmation (pressure) procedures, computer forensics, storage media forensics (USB, hard disk, cloud, etc.) all showed high suitability of 4.5 or more, and the Act on the Prevention and Protection of Unfair Competition and Business Secrets, the Act on the Prevention and Protection of Industrial Technology (non-disclosure), management system and industrial technology (non-disclosure), mobile forensics, and exploration, mobile forensics, and forensics, mobile forensics. In addition, all industrial technology leakage investigation capabilities were verified with 3.5 points or more in all domestic and overseas industrial convergence issues, including crime theory (the latest trend), security and management of industrial sites, criminal psychology, and domestic and international convergence issues.

Although the suitability of all capacities was verified to be 4.5 or higher in the survey of compliance with the required capacity of industrial technology leakage investigation, it was determined that there would be a difference in the suitability figures as there were differences between the survey experts and those who thought each of the industrial security professionals was more important and suitable in the field. Although the results of deriving the average of the suitability of investigation professionals and industrial security professionals showed that they were suitable for all areas of expertise, there were differences in their suitability depending on the area of expertise in several capacities.

4.2. **Design of capacity system for industrial technology leakage investigation.** Data analysis was performed using SPSS Statistics 25. As a result of using principal component analysis as a factor extraction method, and using the varimax rotation method, a right-angled rotation method for pursuing concise interpretation, a total of six factors were derived. The detailed results are as follows.

No	Item	Mean	σ	priority
1	Unfair Competition Prevention and Trade Secret Protection Act	4.48	0.84	6
2	Act on the Prevention and Protection of Industrial Technology Leakage	4.44	0.76	7
3	Act on Support for SME Technology Protection	4.18	0.75	15
4	Defense Industry Technology Protection Act	4.2	0.7	13
5	Civil and Criminal Procedure	4.14	0.76	17
6	Crime Theory (Introduction to Criminology)	3.68	0.96	18
7	Criminal Psychology (Critical Psychology)	3.62	0.97	20
8	Cases of management system and industrial technology (trade secret) leakage	4.42	0.67	8
9	Incident detection (sign capture)	4.3	0.65	11
10	Evidence management and protection (using advanced technology)	4.6	0.64	1
11	Evidence (Seizure) Procedure	4.56	0.67	3
12	Digital forensic concept	4.58	0.57	2
13	Computer forensics	4.5	0.61	4
14	Network forensics	4.34	0.66	10
15	Mobile forensics	4.4	0.7	9
16	Storage media forensics (USB, hard disk, cloud, etc.)	4.5	0.65	4
17	Knowledge and response to anti forensics	4.3	0.68	11
18	Data collection strategy (data collection, purification, application)	4.18	0.75	15
19	Big Data Analysis (Statistics Method)	4.2	0.73	13
20	(Latest Trend) Industrial Security and Management	3.66	0.98	19
21	Domestic and Overseas Industrial Convergence Issues	3.6	1.01	21

FIGURE 3. Conformity validation results

The capacity system for industrial technology leakage investigation was designed with six factors derived. Storage media forensics (USB, hard disk, cloud, etc), computer forensics, mobile forensics, network forensics, digital forensics, anti-forensic, knowledge and response to anti-forensic are the use and investigation of advanced investigative devices, laws on the protection of small business technologies, defense industry protection and civil

engineering procedures evidence management and protection, evidence securing (pressure) procedures, management system and industrial technology (trade secrets) leakage cases and accident detection are industrial technology leakage prevention and accident detection response, big data analysis (statistics method), data collection strategy (data collection, refining and application) is analysis and interpretation of survey data, and management of domestic and international industrial convergence issues and (current trend industry) crime scene are the latest criminal investigation and psychological crime investigation and psychological crime investigation [9,10].

4.3. **Priority analysis of capacity system for industrial technology leakage investigation by analyzing AHP.** Analyzing AHP was performed to determine the weights of each item based on six previous capacity systems for industrial technology leakage investigations. AHP analysis, which is used to determine the relative priority of each capacity system, was conducted on all current and former experts with more than three years of experience in industrial technology leakage investigation (average of six years) and selected those with sufficient capacity to understand the industrial technology leakage investigation environment and the site to secure a high quality level of the survey target.

Prioritized analysis results showed that, in order of relative importance, "prevention of industrial technology leaks and accident response (0.2011)", "industrial technology protection laws and policies (0.1859)", "investigation of use and investigation of advanced investigative equipment (0.1843)", "interpretation of investigation data (0.1737)", "understanding of modern industrial convergence (0.1312)" and "criminal psychological analysis (0.1239)".

5. **Conclusions.** In this study, the capacity system was designed to train expert personnel for industrial technology leakage investigation with multi-dimensional security capability for the purpose of designing "preemptive degree courses" based on the progress of future convergence environment, and the required capacity for industrial technology leakage investigation was further designed through the literature survey and the interviews of industrial security experts focus group.

Therefore, in this study, we designed a competency system to foster experts in industrial technology outflow investigation with the aim of designing a "preemptive degree" level curriculum in accordance with the future convergence environment. In order to nurture the investigative experts, the requirements of industrial technology leakage investigation were designed through the literature survey and focus group interviews with industrial security experts.

We can find the result that all industrial technology outflow investigative capacities were verified. Prioritized analysis results showed, in a relatively important order, "prevention of industrial technology leaks and accident response", "industrial technology protection laws and policies", "investigation of use and investigation of advanced investigative equipment", "interpretation of investigation data" and "understanding of modern industrial convergence", "criminal psychological analysis".

This study conducted a study on the design of the capacity system for fostering experts in industrial technology leakage investigation. It is expected that the government will try to solve the problem of supply and demand of experts who are investigating industrial technology leaks and contribute to enhancing the expertise of those who investigate industrial technology leaks. Because the industrial convergence society is developing rapidly, the importance of knowledge or technology can also continue to change. Therefore, the importance of the research results currently derived will also continue to change, depending on the knowledge and skills that will emerge in the future, and new items can be added. Based on the results of this research, we hope that continued research on the

current curriculum, new educational institutions, college courses, qualification systems, and national vocational ability standards will help train experts in industrial technology leakage investigations that are more suited to the needs of the site.

Acknowledgment. This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist).

REFERENCES

[1] The Foreign Affairs Bureau of the National Police Agency, *Results of the National Police Agency's Planned Investigation into Industrial Technology Leakage Crimes*, 2017.

[2] E. G. Carmines and R. A. Zeller, *Reliability and Validity Assessment*, Sage Publications, Newbury Park, CA, 1979.

[3] T. Saaty, A scaling method for priorities in hierarchical structures, *Journal of Mathematical Psychology*, vol.15, no.3, pp.234-281, 1977.

[4] H. Yoon, S. Lee and J. Lee, A study on the digital forensics expert capability prioritization using AHP method, *Journal of the Electronic Trade Association of Korea*, vol.22, no.1, pp.107-122, 2017.

[5] H. Kim, *A Study on the Job Competency and Role of Human Resource Development Officer*, Ph.D. Thesis, Seoul National University, 1999.

[6] W. Na, *A Study on the Enterprise Information Rating Model for the Protection of Industrial Technology*, Master Thesis, Chung-Ang University, 2017.

[7] J. Jung and J. Park, Development of expert personnel through the establishment of industrial security education agencies, *Korean Journal of Industry Security*, 2016.

[8] Cybercrime Investigation Body of Knowledge, *About CIBOK/About CIBOK Editorial Committee*, 2019.

[9] J. Sun, *Reconsideration of the Criminal Investigation System of Karma Technology Leakage*, Gachon Law, 2014.

[10] C. Lee, *A Study on the Reference Model Design for Diagnosis of Industrial Technology Protection Level Based on Digital Information Analysis*, Ph.D. Thesis, Chung-Ang University, 2018.