IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 23, Issue 2, Ver. 10 (February. 2018) PP 32-38
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Study on the concept and scope of industrial security in major countries

Ji-Yeon Yoo*, Min-Hyeok Lee**

** Department of Intelligent Engineering Informatics for Human in Sangmyung University, Republic of Korea*
*** Master's degree holder at Department of Information and Security Management in Sangmyung University, Republic of Korea*

Abstract: As global networking of digital economic activities has expanded and competition between countries has intensified, theft of information such as industrial technology and trade secrets has become more serious. Infringement accidents such as industrial technology leakage have increased enterprises' losses and hurt national competitiveness. This is a basic study of how industrial security is defined and maintained in four major countries. It examines the concept and scope of industrial security based on the industrial security-related legal systems of the USA, Japan, Germany and Korea and considers countermeasures against industrial security breaches.

Keywords : Industrial Security, Concept and Scope of Industrial Security, Economic Counterintelligence

---

Date of Submission: 10-02-2018 Date of acceptance: 26-02-2018

I. INTRODUCTION

After the Cold War, international politics shifted focus from the military to economics, and each nation needed information on new factors such as its ability to negotiate capital, technology and international trade[1]. Therefore, in order to strengthen each country's competitiveness, the gathering of information such as international economic conditions and policies, major companies' new product development trends, etc. has increased.

In this situation, the intelligence agencies of each country started to concentrate on acquiring and defending industrial information by promoting their own security, and by doing so, increasing the capacity of their economic counterintelligence. Criminal industrial technology spills are steadily increasing and can be very damaging to the competitiveness of companies and nations. It is therefore important to prevent criminal industrial technology leaks in advance and to have an industrial security system that can cope with the resulting damage.

This study intends to grasp the status of industrial security in major countries in order to establish new industrial security countermeasures. To this end, we will examine the concepts and scope of industrial security in the U.S., Japan, Germany, and Korea, and compare and contrast national responses to industrial security.

II. ACADEMIC DISCUSSION ON INDUSTRIAL SECURITY

Industrial security is a concept related to national security, which means 'the overall system for protecting internal assets'. Cunningham and Taylor (1985) defined the term "industrial security" in a broad sense as "any effort to protect all economic activity from crime." It is more specifically defined as "Asset protection and loss prevention to protect all assets, both intangible and intangible," and is used as a term limited to industry[2].

Hesse and Smith (2001) modeled integrated security by proposing four categories: security, general, business and management and IT and computing. This model was suggested for general supervisory or managerial tasks. The security category includes management-related elements such as security theories, security technologies, technical aspects, laws, physical security, asset protection and management duties. The 'business and management' category includes elements from the perspective of business rather than security, primarily business continuity, law, technology, accounting, contract management, and human resource management[3].

Table 1. Hesse and Smith's industrial security management model

Security	Business and Management	Generic	Computing and IT
Law	Law	Analytical	IT systems
Threats	Management theory	Research	
Security technology	Technology		
Security theory	Business		
Risk management	Accounting		
Technology	Cultural knowledge		
Investigative procedures	Industrial relations		
Security equipment	HRM		
Physical security	Contract management		
Security standards	Duty of care		
Life safety systems	Equal opportunity		
Cultural knowledge	Ethics		
Asset protection	Fraud		
Intelligence			
Duty of care			
Fraud			
Security perception			
Surveillance			

Since 2000, ASIS International has been developing security-related knowledge systems in the United States. ASIS defines industrial security as the work of protecting people, assets and information, and includes protection of property, safety, prevention and control of crime.

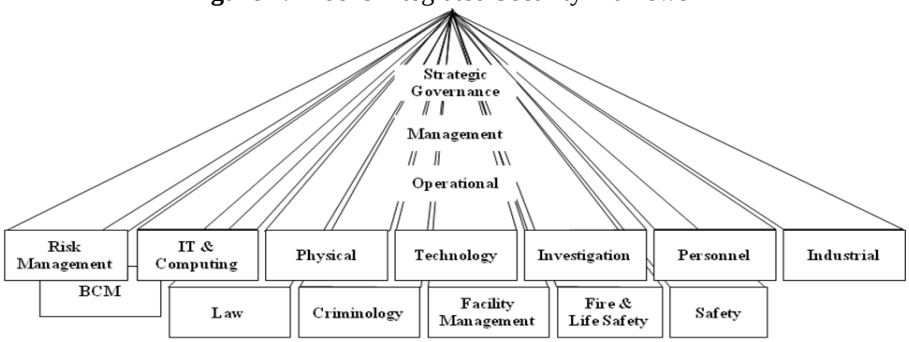
The scope of industrial security is not limited to trade secrets and national security, but various other security activities as well. This is because the various sectors of the industry such as business failures are determined to have significant importance. The main reason for damage caused by natural disasters or fire is human error, which is covered by a large category of industrial security because it is a crime[4]. It also covers various aspects of industrial security in terms of physical, technical, legal and administrative aspects[5].

Table 2. ASIS Security Model

Security	
Physical security	Crisis management
Personnel security	Disaster management
Information systems security	Counterterrorism
Investigations	Competitive intelligence
Loss prevention	Executive protection
Risk management	Violence in the workplace
Legal aspects	Crime prevention (general)
Emergency/contingency planning	CPTED
Fire protection	Security architecture and engineering

Brooks (2009, p. 11-12) defined industrial security as 'security applications in specific industries such as aviation security, maritime security, critical infrastructure protection, government security and retail security'. Brooks also proposed a security system that includes 13 types of criminology, business continuity management, fire and life safety, and facility management.

Figure 1. Brooks Integrated Security Framework



Note : BCM = Business Continuity management

The security system classified industrial security factors as either 'Level 1' or 'Level 2' according to whether or not the factors are related to core technologies, strategic governance, management, or operating systems[6].

The following is a summary of these discussions. Industrial security is defined as the safeguarding of all assets required for industrial activities from various kinds of infringement, and elements of a classification system necessary for industrial security are discussed.

Cunningham and Taylor (1985) categorized such elements for purposes such as asset protection and loss prevention. Hesse and Smith (2001) categorized the components based on the characteristics of their work in order to facilitate supervision and management of industrial security. ASIS classifies industrial security elements based on criteria such as industry type, threat, and space and treats industrial security in terms of physical, technical, and legal compliance. Brooks (2009) argued for 'integrated security' by defining industrial security as any of 13 factors such as criminology, business continuity management, fire and life safety and facility management. Brooks divides industrial security into elements such as business and industry based on a single standard and defines industrial security as one element of integrated security. This is because the scope of industrial security is expanding and classified by various standards.

Table 3. Concept and scope of industrial security

Level 1	Industrial technology protection	Physical security	Risk management	Emergency/ contingency planning	Security theory	Security standards	Surveillance	Security
			Security technology	Investigative procedures	Security equipment	Security perception	Disaster management	
				Duty of management	Fraud	Technology	Information protection	
	Asset protection	Personnel security			Industrial relations	Cultural knowledge	Accounting	Business and Management
						Analytical	Research	Generic
Level 2	BCM	Fire protection	Counterterrorism	Crime prevention	Loss prevention	Threats	Law	Security
	International safety	Homeland security	Contract management	HRM	Business	Ethics		Business and Management

Note : BCM = Business Continuity Management
HRM = Human Resource Management

Table 3. summarizes the industrial security concepts and scope that have been examined so far. The scope of the study was set up to reflect the areas identified in previous studies related to industrial security, and detailed components were derived by referring to ASIS' security model.

We can refer to Brooks' integrated security framework and classify the importance of the detailed components into 'Level 1' and 'Level 2'. The elements used for each criterion are classified by each area, but the elements used in other areas such as management obligation, fraud, and technology are duplicated.

III. LEGAL DEFINITION OF INDUSTRIAL SECURITY IN MAJOR COUNTRIES

The laws and policies of the United States, Japan, Germany and Korea protect their own respective industries. In the Uniform Trade Secrets Act and the Economic Espionage Act of 1996, the United States defines industrial security as protecting trade secrets and proprietary technology. The Uniform Trade Secrets Act defines misconduct with regards to trade secrets as "theft, bribery, misrepresentation, violation of confidentiality obligations, solicitation of violations, spying by electronic or other means".

In addition, "theft" of a trade secret is defined as (1) knowing that it is was procured by fraudulent means, (2) obtaining the business secret from another person, or (3) disclosing or using another person's trade secret without express or implied consent. Trade secrets are classified as "information, including formulas, patterns, compilations, programs, designs, methods, techniques or processes," as ① information not generally known to those who can obtain economic value by its disclosure or use, or ② In some situations, it is defined as the object of reasonable effort to maintain the secret[7].

In the Economic Espionage Act of 1996, trade secret infringement is interpreted as into 'violating trade secrets for the benefit of foreign governments or other foreign institutions' and 'to infringe on trade secrets with the aim of benefiting a person other than the owner of the trade secret'[8]. The National Security Act enacted in 1947 includes counterintelligence at the economic level and stipulates information activities and actions carried out to protect against espionage, sabotage, assassination, and other intelligence activities by governments, government agencies, and international organizations.

In Executive Order No. 12036, published in 1978, such information was collected from physical or security programs to protect economic counterintelligence from espionage, international terrorist activities and assassination[9]. In addition, the Foreign Investment and National Security Act (FINSA) defines economic counterintelligence as "including the same issues as homeland security including critical infrastructure"[10]. The National Intelligence Strategy (NIS), an official report on economic counterintelligence, describes economic counterintelligence as "defensive and aggressive activities ", thus extending the scope of economic counterintelligence[11].

Table 4. United States Industrial Security Area

<table>
<tr><td rowspan="5">Level 1</td><td rowspan="2">Industrial technology protection</td><td rowspan="2">Physical security</td><td>Risk management</td><td>Emergency/ contingency planning</td><td>Security theory</td><td>Security standards</td><td>Surveillance</td><td rowspan="2">Security</td></tr>
<tr><td rowspan="2">Security technology</td><td>Investigative procedures</td><td>Security equipment</td><td>Security perception</td><td>Disaster management</td></tr>
<tr><td rowspan="3">Asset protection</td><td rowspan="3">Personnel security</td><td rowspan="2"></td><td rowspan="2">Duty of management</td><td rowspan="2">Fraud</td><td rowspan="2">Technology</td><td rowspan="2">Information protection</td><td rowspan="2">Business and Management</td></tr>
<tr><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>Industrial relations</td><td>Cultural knowledge</td><td>Accounting</td></tr>
<tr><td rowspan="2">Level 2</td><td>BCM</td><td>Fire protection</td><td>Counterterrorism</td><td>Crime prevention</td><td>Loss prevention</td><td>Threats</td><td rowspan="2">Law</td><td>Security</td></tr>
<tr><td>International safety</td><td>Homeland security</td><td>Contract management</td><td>HRM</td><td>Business</td><td>Ethics</td><td>Business and Management</td></tr>
</table>

Note : BCM = Business Continuity Management

HRM = Human Resource Management

Japan defines industrial security as trade secrets in its Unfair Competition Prevention Act and Trade Secret Management Guidelines. The Unfair Competition Prevention Act defines a trade secret 'a technique that is useful for production methods, sales methods and other business activities that are managed in secret, and is not publicly known business information.[12]'

The Trade Secret Management Guidelines describe trade secrets by separating the definition of industrial security specified in the Unfair Competition Prevention Act into three categories: ① secrets, ② useful information, and ③ information not publicly known, and information is classified as a business secret only when it falls under one of these categories[13].

Table 5. Japan Industrial Security Area

Level 1	Industrial technology protection	Physical security	Risk management	Emergency/ contingency planning	Security theory	Security standards	Surveillance	Security
			Security technology	Investigative procedures	Security equipment	Security perception	Disaster management	
				Duty of management	Fraud	Technology	Information protection	Business and Management
	Asset protection	Personnel security			Industrial relations	Cultural knowledge	Accounting	
						Analytical	Research	Generic
Level 2	BCM	Fire protection	Counterterror ism	Crime prevention	Loss prevention	Threats	Law	Security
	International safety	Homeland security	Contract management	HRM	Business	Ethics		Business and Management

Note : BCM = Business Continuity Management
HRM = Human Resource Management

Germany defines industrial security as trade secrets in its Unfair Competition Prevention Act as (1) confidentiality or confidentiality in business, (2) drawings and models entrusted to them in transactions in business, and (3) prohibiting them from infringing[14].

Table 6. German Industrial Security Area

Level 1	Industrial technology protection	Physical security	Risk management	Emergency/ contingency planning	Security theory	Security standards	Surveillance	Security
			Security technology	Investigative procedures	Security equipment	Security perception	Disaster management	
				Duty of management	Fraud	Technology	Information protection	Business and Management
	Asset protection	Personnel security			Industrial relations	Cultural knowledge	Accounting	
						Analytical	Research	Generic
Level 2	BCM	Fire protection	Counterterror ism	Crime prevention	Loss prevention	Threats	Law	Security
	International safety	Homeland security	Contract management	HRM	Business	Ethics		Business and Management

Note : BCM = Business Continuity Management
HRM = Human Resource Management

Korea defines the concept and scope of industrial security in the Act on the Prevention and Protection of Industrial Technology Spills and the Act on the Protection of Unfair Competition and Trade Secrets.

The Act on the Prevention and Protection of Industrial Technology Spills refers to the scope of industrial security as industrial technology and refers to various methods and technological information necessary for the development, production, dissemination and use of products or services, as well as the need for technology. Accordingly, technology has been defined and announced in nine laws including the Industrial Development Act, the Industrial Technology Innovation Promotion Act and the Electric Power Technology Management Act.

In addition, if the technology or economic value of the market outside Korea is high or the growth potential of related industries is high, an informational security breach will cause serious harm to national security and the development of the national economy[15]. The Act on the Prevention of Unfair Competition and Protection of Trade Secrets shall not be publicly known but shall have independent economic value and shall be made up of technical or managerial information useful for production methods, trade secrets and their protection against infringement activities[16].

Table 7. Korea Industrial Security Area

Level 1	Industrial technology protection	Physical security	Risk management	Emergency/ contingency planning	Security theory	Security standards	Surveillance	Security
			Security technology	Investigative procedures	Security equipment	Security perception	Disaster management	
	Asset protection	Personnel security		Duty of management	Fraud	Technology	Information protection	Business and Management
					Industrial relations	Cultural knowledge	Accounting	
						Analytical	Research	Generic
Level 2	BCM	Fire protection	Counterterrorism	Crime prevention	Loss prevention	Threats	Law	Security
	International safety	Homeland security	Contract management	HRM	Business	Ethics		Business and Management

Note : BCM = Business Continuity Management
HRM = Human Resource Management

IV. CONCLUSION

The concept and scope of industrial security and legal regulations of major countries are summarized in the following table.

First, industrial security can be classified as 'Level 1' and 'Level 2' depending on its importance. Criminology, international security and homeland security can be classified as important elements of industrial security rather than industry. In addition, it can be divided into security and business and management of each area, which can also be classified in order of importance.

Level 1 information and management obligation can include both security and business and management and additionally, security standards are included in terms of security. The law is considered to be more important in the areas of security and business and management, and the threat is more important from the viewpoint of security. Ethics are important in business and management. Taken together, industrial security has many factors and areas, and considers criminology, international security, and homeland security factors, including industry. It can also be classified in terms of security and business and management. These two areas are dealt with by information and management obligation, which is treated as an upper concept. Therefore, industrial security protects industry from counterintelligence at the economic level and can be considered as a concept covered by security and business and management.

Table 8. Industrial Security Concepts and Scope

Domains / Importance	Security	Business and Management
Level 1	Industrial technology protection	Information protection
		Duty of management
		Security standards
Level 2	Crime prevention	Law
	International safety	Threats / Business
	Homeland security	Ethics

The results of this study show that the concept of industrial security in Korea is similar to the concept of industrial security in the United States. The concept of industrial security has been established around business and industry in Japan and Germany. In the case of the United States, the concept of counterintelligence in the overall economy was dominant, and the concept of industrial security was established in response. The concept of industrial security in Korea is similar to that of the U.S. because it includes most concepts of economic counterintelligence as understood in the United States, along with business factors.

Industrial security is a concept that refers to a series of security activities that protect resources and minimize risk and loss to prevent leakage of key technologies and confidential information at the enterprise level, and affect national problems as well. Therefore, industrial security should prepare against industrial technology leakage crimes in accordance with the international situation. It is also necessary to supplement industrial security systems through continuous research.

REFERENCES

[1] Yun Jeong-suk. (2014) Understanding of National Informatics.
[2] William C. Cunningham & Todd H. Taylor (1985) Private Security and Police in America.
[3] Hesse, L. and Smith, C. L. (2001) Core Curriculum in Security Science. In: H. Armstrong (ed.) Proceedings of the 5th Australian Security Research Symposium. Perth, Western Australia: School of Computing and Information Science, Edith Cowan University, p. 87 - 104.
[4] Lee Chang. (2011) A Study on the Conceptual Definition of Industrial Security.
[5] Kang Ju-young, Lee Bansu. (2015) A Study on Combined Education for Industrial Security Manpower Training).
[6] Brooks. (2009) What is security: Definition through knowledge categorization. p.11-12.
[7] United States (1979) Uniform Trade Protection Act.
[8] The United States (1996) The Economic Spy Act.
[9] The United States (1978) Executive Order No. 12036, 4-202.
[10] The United States (2007) FINSA: Foreign Investment and National Security Act.
[11] The United States (2014) The National Intelligence Strategy of the United States of America, P.6.
[12] Japan (2012) Unfair Competition Prevention Act.
[13] Japan (2015) Trade secret management guidelines.
[14] Germany (2002) Unfair Competition Prevention Act.
[15] Korea (2015) Act on the Prevention and Protection of Industrial Technology Spills.
[16] Korea (2015) Unfair Competition Prevention and Trade Secret Protection Act.

Ji-Yeon Yoo "Study on the concept and scope of industrial security in major countries."IOSR Journal of Humanities And Social Science (IOSR-JHSS), vol. 23, no. 2, 2018, pp. 32-38.