British Journal of Business and Management Research
Vol.1, No.2, pp.103-114, June 2014
Published by British Research Institute UK (www.gbjournals.org)

AN ANALYSIS ON THE INDUSTRIAL TECHNOLOGY LEAKAGE CASES IN SOUTH KOREA

Yongtae Chun

Ju-Lak Lee

Kyonggi University, Suwon, Korea

ABSTRACT: *In this study, economy and technology development in South Korea is discussed and a problem that has accompanied the advancement is examined. Industrial technology leakage, which has been increasing in the South Korean society among the nation's major industry sectors has resulted in immeasurable financial consequences; it can also threaten the country's status as the world's leading manufacturer in shipbuilding, semiconductor, and electronics. A total of twelve technology espionage cases, three from each industry, that have received substantial attention by the media and been introduced in the "Technology Leakage Cases and Security Tips" published by the Korean Association for Industrial Technology Security are analyzed in order to find common patterns, actors involved, and characteristics of the leakage activities. The results show that in most cases assessed, a former employee is motivated by the monetary rewards and utilized the external devices to transmit the information. Furthermore, viable policy implications are suggested to provide a possible solution to the problem.*

KEYWORDS: Industrial technology, Technology leakage, Industrial security, Information security, Espionage

SOUTH KOREA AND ITS DEVELOPMENT

Economic, Cultural, and Technological Development

Over the past six decades, South Korea has accomplished an unprecedented economic, cultural, and technological growth. Also referred to as the "Miracle on the Han River," the perseverance and the diligent spirit of both the government and the citizens have paid off, helping the country rank fifteenth in the world by nominal Gross Domestic Product (GDP) and become one of the G-20 major economies. In addition, the country has overcome its disadvantage of having almost no natural resources and being overpopulated by adapting an export-oriented economic strategy and became the seventh largest exporter and tenth largest importer in the world in 2010. Moreover, by hosting various international events, South Korea has demonstrated its competence in international affairs (Song 1997).

Downside of the Rapid Growth

The economy and technology growth in South Korea has led to its strengthened ties and active interactions with other countries around the world. However, despite the merits, one critical side effect of the development has been a growing number of industrial technology leakages (Jeon 2009). According to the statistics provided by the National Industrial Security Center (NISC) of the National Intelligence Service (NIS) in South Korea, the number of technology leakage is increasing each year and a total of 264 cases were recorded from 2005 to 2011. As this continuing trend will damage the South Korean economy in the long term, and the country can possibly lose its current position as the leader in some of the main industries, the next challenge for South Korea is secure its industrial technologies (Park & Kim 2011).

RESEARCH METHOD

For an accurate evaluation of the ongoing issue of the technology leakage in South Korea, the authors have examined 264 cases that have been reported by the media. Then policy implications for effective preventive measures are discussed with a basis on the results from the analysis. The subjects of the analysis include four representative cases in each of the three main Korean industries: Shipbuilding, semiconductor, and electronics; and the twelve companies involved in the cases are considerable in size, revenue, and number of employees (The Korean Association for Industrial Technology Security & The Korean Association for Industrial Security 2013).

CONCEPT OF INDUSTRIAL SECURITY AND CURRENT STATE OF TECHNOLOGY LEAKAGE IN KOREA

Industrial Security

It was not until recently that the term “industrial security” became generalized in the South Korean society. In 2003, NISC was established and the Act on Prevention and Protection of Industrial Technology Outflow came into effect. Moreover, the term has started to be used in the media more frequently as the issue of industrial technology leakage and outflow has been placed under the spotlight (Lee 2011). The concept of industrial security can be viewed from both broad and narrow perspectives; it can be understood as all the acts that are carried out to protect economic activities from criminal endeavors. Specifically, it includes “asset protection” and “loss prevention” that protect both tangible and intangible assets. On the other hand, it can be restricted to preventing the outflow or leakage of industrial technologies. (Lee 2011).

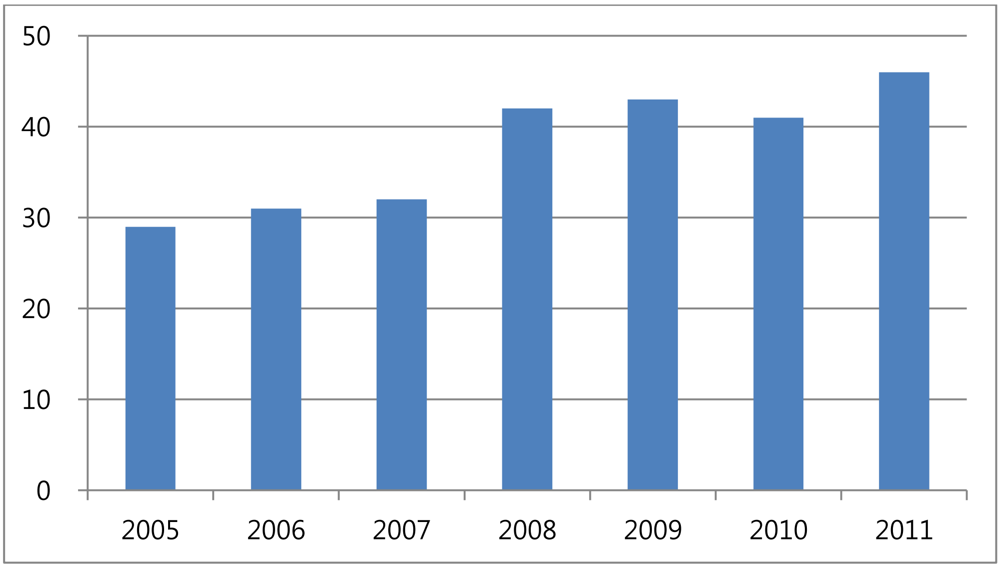
In South Korea, “industrial technology” is viewed with the narrow definition; and it is generally focused on the protection of Information Technology (IT). For instance, the project proposed by the Ministry of Knowledge Economy in December, 2008, “Knowledge Information and Nurturing Plans for Protection Industries,” was expected to invest one trillion five-hundred billion won in the research and development in the fields of three main fundamental technologies; but in reality, the IT sector and the related academia have received a majority of the investment through expert training and certificate vitalization (Kim & Shin 2013).

Also, as mentioned earlier, the technology leakage cases in South Korea have been increasing since 2005. Therefore, authors have focused on the analysis of the three areas that are most frequently exposed to the danger of technology leakage, and in the next section, the current state of technology outflow and specific incidents are examined.

Current State of Technology Outflow

The computer literacy rate in South Korea is well-matched with its advanced technologies in information communications, semiconductor, shipbuilding, electronics, etc. and the country's reputation as an IT powerhouse. South Korean industries, therefore, have been benchmarked by many of the comparable corporations around the world. However, despite various advantages of being a leader in the industries, the downside of it also exists. First of all, the domestic issue of private information leakage has not been tackled properly and cybercrime is diversifying with its number increasing. Recently, though many efforts have been made to protect individual information and privacy, preventing the outflow of the national technologies to other countries remains a challenging task (The Korean Association for Industrial Security 2012). As can be seen in the graph below (provided by NIS), the technology leakage cases are steadily increasing, except for a temporary fall during 2010.

Figure 1. Number of Technology Leakage Cases in South Korea (2005-2011)



CASE ANALYSIS

Shipbuilding Industry in South Korea

South Korea became a leading producer of ships during the 1970s and 1980s. The country's major manufacturer was Hyundai in the 1970s and Daewoo joined the shipbuilding industry in 1980. The nation's shipbuilding industry declined in the mid-1980s due to the oil glut and a worldwide recession. Moreover, there was a sharp decrease in new orders in the late 1980s; and this was the result of labor unrest, Seoul's unwillingness to provide financial assistance, and Tokyo's new low-interest export financing in support of Japanese shipbuilders. Despite the difficult times, South Korea eventually became the world's dominant shipbuilder with a 50.6% share of the global shipbuilding market as of 2008. In addition to Hyundai Heavy Industries and Daewoo Shipbuilding & Marine Engineering, Samsung Heavy Industries and STX Offshore & Shipbuilding are the main corporations of the industry. In this section, four notable leakage cases occurred in the shipbuilding industry in South Korea are discusses (Kwak et al 2005).

Case #1

In this case, a suspect was accused of taking the information related to the integrative production planning system of the company he had worked for and trying to sell it to a Chinese company after founding his own. It was revealed that he used a Universal Serial Bus (USB) and electronic mail (e-mail) to steal the information.

Case #2

The accused worked at the company as a manager of design techniques and used an external storage device to save the drawings for ships and technical data before taking up another job at a rival firm. Also, he founded a venture with Chinese partners and engaged in the bidding battles. The affected company confirmed a large amount of technology data being deleted from its former employee’s personal computer and started an investigation.

Case #3

The suspect worked as a designer at the damaged company. While serving as a dispatched officer, he took charge of the blueprints and technical data supporting work, which allowed him to gain access to different confidential materials. Soon after returning from his post, the accused resigned from the company and established his own design engineering company. The investigation began upon the request from the accused’s former employer. The accused was indicted for engaging in a bidding battle with a new medium size shipbuilding company.

Case #4

This case involved a person that held a position as a supervisor of technology security of the accusing company; he stole the crucial data of the company, including then-current state of research and development, design techniques, data from the computerized system and management regulations, etc. and replaced them with music files before accepting the job offer from a competitor company located in China and providing them with the information.

Table 1. Leakage Cases in Shipbuilding

Case	Information Leaked	Motivation	Leakage Route	Punishment Imposed/Estimated Damage
1	Design drawings and technology data	Discontentment with personnel procedure and personal profit	External storage device	1-year imprisonment (3 related others on probation), Estimated amount of damage: 35 trillion won
2	Design drawings and technology data	Personal profit and business	External storage device	1-year and 6 month imprisonment and 3-year probation (2 related others on probation, 3 others imposed with fines), Estimated amount of damage: 57 billion 4 hundred million won
3	Design drawings and technology data	Recruiting from a competitor company	External storage device	1-year imprisonment and 2-year probation
4	Shipbuilding Enterprise Resource Planning (ERP) material	Recruiting from a competitor company	E-mail	Suspension of indictment, estimated amount of damage: 3 billion won

Semiconductor Industry

South Korea is one of the dominating countries in the global semiconductor industry. In 2011, the country's computer chip exports were expected to reach 52.5 billion U.S. dollars as the overseas demand for system semiconductors rose. Furthermore, the country's leading producer, Samsung Electronics, ranked number two in revenue (28,137 million US dollars) and market share (9.3%) from 2009 to 2011 according to the information provided by the iSuppli Corporation. In addition, another South Korean semiconductor company, Hynix ranked number eight in the world in 2011 with the revenue of 10,577 million US dollars and 3.5% of the world market share, making the semiconductor Industry is a crucial part of South Korea not only for its economic value but for its symbol as a national pride (Mathews & Cho 2007). Therefore, the technology leakage incidents including the following cases must be understood and properly addressed and prevented in the future.

Case #1

Mr. Kim worked as a senior researcher at the company with an intention to apply for a position at a foreign company. For the purpose of being hired by the rival company, he secretly stored the data related to process technology into his personal CDs and external drives. He was arrested after returning from an interview overseas and while continuing to collect the company's confidential data.

Case #2

A person named "K" was the supervisor of the investment planning team of the damaged company and planned to build a semiconductor factory in China after his retirement. He also offered high salaries and stock options to four engineers that had worked with him. He requested critical technology-related information from them, including the development state, the process data, and the blueprint of the manufacturing factory; and had the engineers file their resignation to recruit them. After starting a venture in China and while trying to recruit additional employees from his former employer, he was arrested and the investigation began.

Case #3

Taking advantage of his position as a person in charge of the company's computerized system, "A" illegally collected confidential information by using another person's password, the remote sign-in method, etc. Then, he e-mailed the collected material by breaking the File Transfer Protocol (FTP) and storing it to his personal computer at his house. However, since no evidence had been found of him distributing the data or using it for financial gain, no criminal charges were filed against him.

Case #4

This was a case in which a person obtained the "capital goods investment plan" data by asking his former colleague at the damaged company. With the required data, the accused's company was able to participate in the bidding battle after taking the information on the investment items and period, budget, etc. into account.

Table 2. Leakage Cases in Semiconductor

Case	Information Leaked	Motivation	Leakage Route	Punishment Imposed
1	R&D and process technology of new products	Discontentment with company's treatment and intention to leave the job	Online folder	1-year and 6-month imprisonment
2	Semiconductor process technology	Recruiting from a competitor company	USB, CD	1-year and 9-month imprisonment
3	Personnel-related confidential data	Curiosity	E-mail	Dismissal from position
4	Capital goods investment plans	Personal relationship	Hard copies of the documents	Salary reduction

Electronics Industry

Samsung Electronics which is headquartered in Suwon, South Korea, is the world's largest information technology company by revenues and has assembly plants and sales networks in sixty-one countries. It is also the largest mobile phone, television, and LCD panels manufacturer in the world. In addition, another South Korean electronics corporation, LG Electronics is the world's second-largest television manufacturer and the fifth largest mobile phone maker in the world. Furthermore, along with the two electronics conglomerates, there are numerous other companies of all size that contribute to South Korea's status as the world's leading nation in electronics industry. Also, the Ministry of Trade, Industry, and Energy has anticipated an annual average of 4.15 percent increase in production until 2018, which will help stabilize the country's position at the forefront of the industry (Wikipedia).

Case #1

It was a case where an employee attempted to leak the data composed during his time at the "A" research institute. For the purpose of possessing it for personal record, the suspect compressed the files and tried to get around the PC security software by copying the data into his cellular phone.

Case #2

"L" of the "P" research institute worked as a cellphone designer and tried to steal the design files from the project he participated in, which was revealed by the company's intelligence security team during the monitoring process. Using the unauthorized software, "L" got around the company's PC security software and leaked a large amount of former and future cellphone design images (in seven separate files) and stored it into the computer at his residence.

Case #3

After leaving his former position and starting to work as a technology consultant at a Chinese firm, “A” colluded with “B” (former colleague) and “C” (who worked at the PDP product technology department) and leaked the PDP production equipment layout and utility-related drawings to the Chinese company via e-mail; “A” and “B” took out the accusing company’s documents and stored them in their computers without permission, and “B” and “C” transferred them.

Case #4

“K” who showed an intention to resign from the development team of a research institute, tried to leak the confidential documents to the new company that he wanted to work for. His actions were uncovered by the company’s system designed to monitor former employees. “K” printed out various document, including product development standards and other related materials provided by other departments, and stored them into his computer at home to use it at the time of transferring to another job. He was also charged with taking out and using the corporate laptop for personal use.

Table 3. Leakage cases in electronic

Case	Information Leaked	Motivation	Leakage Route	Measures by Company and Punishment Imposed
1	Strategic plans and standardization business-related data	Personal possession	Cellphone	The tool developed to get around the company’s PC security software banned unless authorized by the company.
2	Cellphone designs	Personal gain (studying abroad)	Unknown	All the documents collected and the PC software reinforced.
3	Production facilities layout, utility sketches	Personal gain (business)	External drive, e-mail	Every partaker of the incident received criminal charges according to the related laws.
4	Documents for product development and defect consulting	Personal gain (business/new job)	Hard copies, corporate laptop	Dismissed from the position and charged for misappropriation and violation of trade secret prevention laws.

ANALYSIS AND PREVENTIVE MEASURES

TREND OF TECHNOLOGY LEAKAGE

Target

The result of the analysis indicates that all the leakage cases in shipbuilding, semiconductor, and electronics involve then-current and former employees. This demonstrates that those who can gain access to the confidential information of their companies with ease could use it for their own profitable businesses.

Methodology

Another interesting finding is that portable storage devices are most widely used for stealing technologies. It can be understood that these devices have advantages of being convenient and large in capacity, making them suitable for copying files. Moreover, e-mail is another popular form used to transmit confidential files; and in the case where an employee in charge of the company's computerized system gets involved in technology leakage, his goal is often achieved through manipulating the system. In the five out of the twelve cases examined in this paper, the culprits used external storage devices, and e-mail was used in three other cases. In addition, cellphones and online folders were also preferred tools for carrying out the crime.

Type

In every case analyzed in this study, the employees committed the crime through internal collusion, bribery, or financial enticement. Particularly, when compared to conglomerates, small and medium companies were exposed to a higher risk and were in a more urgent need of a reinforced security management system.

Motivation

As mentioned in Winkler (1997), in nine out of the twelve cases studied, personal profits and financial temptation acted as main motivators and curiosity and personal possession were also the causes of the crime. Specifically, business purposes, change of occupation, studying abroad were among the strongest stimulants. Also, it seemed as though the accused did not consider possible consequences of their actions and took the crime lightly (Whitney & Gaisford 1999).

SUGGESTION FOR COUNTERMEASURES

Employee Education

By taking the current trend into account, the authors provide viable policy implications that will help prevent similar technology leakage cases in the future. First of all, regular educational sessions should be provided to new and existing employees to raise industrial security awareness. Past cases of technology leakage cases can be introduced and the employees can learn about the crime's possible consequences for the damaged corporations, which will provide them with an opportunity to increase their loyalty for their companies (Choi et al 2012). Furthermore, the media could place the topic of industrial security under the spotlight by creating programs and producing articles on the related stories, which will expand people's insights and stimulate their interest in industrial security (Jeong 2009).

Reinforcing Security Policies

A server that can fend off external access is an important component in establishing security policies. A way to acquire such server can be realized by utilizing the corporate data protection system and the security infrastructure developed through cooperation among different professional organizations (Sennewald 2003). Furthermore, a background check should be required for every employee and selection of the person in charge of security maintenance should be prioritized. Also, employees should be required to sign a written oath of data security and confidentiality, and the employer must promote security awareness among new workers and clearly define their responsibilities (The Korean Association for Industrial Security 2012).

In regard to the use of USB and other external drives along with other portable disks, only the ones distributed by the company should be allowed within in the buildings. Also, setting a detector at each entrance will be necessary to deter unauthorized outflow of the devices, and those who attempt to bring them off the premise without authorization should be severely punished (Hiles 2010).

Development of Security Technology

Chang and Song (2009) conducted an in-depth interview with fifteen companies that provided industrial security system and fifteen other companies on the receiving end to analyze the key components demanded in the industrial security system. The results of the study showed that the components that were most commonly considered as critical included security of e-mail and messengers, portable storage devices, and documents, database activity monitoring, network access control, and contents monitoring and filtering. With a basis on their findings, the researchers established the "technological industrial security structure" after consulting with a group of experts in the related fields (Choi 2010). An important thing to remember in constructing the security system is that the technology used has to keep pace with the rapidly advancing mobile, communications, and network technologies (Robert & Lajtha 2002).

Implementation of Effective Laws

The trade secrets that are subject to industrial security in South Korea are primarily protected by the "Unfair Competition Prevention and Trade Secret Protection Act." However, protection processes and methods-related laws should be improved for a more efficient reinforcement of the industrial security system.

Moreover, to promote consistency in the related tasks, repetitive and contradictory clauses must be removed or revised. The subjects of industrial security are diverse and major technologies, but there are numerous other industrial technologies that are unprotected by the law despite their confidentiality and importance (Cohen 2000). In many cases, industrial crimes are committed by first-time offenders, which tend to reduce their sentences. However, the punishments for those who violate industrial security laws have to be much harsher than now as the consequences of their crime can cause immeasurable economic damage to the country (Green & Farber 1987). By making an example of the offenders, industrial security awareness can be promoted among possible culprits (The Korean Association for Industrial

Security 2012).

FUTURE DIRECTIONS

In this study, the current state of technology leakage is examined and suggestions are made to protect the critical technologies and data of three major industries in South Korea. In the three industries, possible consequences of a technology leakage can lead to secondary and tertiary damages that could not only affect the target companies, but the nation as a whole. As the incidents are caused from internal members of the companies, effective preventive policies are urgently needed; and implementation of security education/training sessions, reinforcing security policies, and revision and improvement of the current laws are expected to help protect the key technologies.

Despite their applicability, the mere suggestions are not sufficient enough to help the industrial security of South Korea develop as needed. A more profound statistical analysis should be carried out and the cases in foreign countries must be reviewed comprehensively to draw implications for South Korea; and by continuing the effort to protect the country's assets and being willing to learn from the past mistakes, the future of the major South Korean industries will be more secure.

REFERENCES

Chang, H.B. & Song, J. H. 2009, 'The Exploratory Study on the Evaluation of Security System for Industrial Technology Leakage Prevention', *The Korean Association for Industrial Security*, vol.1, no.1, pp. 50-61.

Choi, E.R., Song, B.G., Lee, Y.I. & Park, K.M. 2012, 'A Study on the Leaking Channels of Industrial Technology', *Police Science Institute*, vol. 26, no.1, pp. 225-259.

Choi, J.H. 2010, 'A Study on the Institutional Improvement Directions of Industrial Security Programs', *Korea Security Science Association*, vol. 22, pp. 197-230.

Cohen, M. A. 2000, 'Economics of Crime and Punishment: Implications for Sentencing of Economic Crimes and New Technology Offenses', *The. Geo. Mason L. Rev.*, vol. 9, pp. 503.

Green, G. & Farber, R. C. 1987, *Introduction to security*, Boston, Butterworths.

Hiles, A. 2010, *The definitive handbook of business continuity management*, Oxford, Wiley.

Jeon, J.W. 2009, 'A Study on the Measuring of Damage in Technology Leakage', *The Korean Association for Industrial Security*, vol.1, no.1, pp. 20-32.

Jeong, B.I., 2009, 'A Study for Preventing Industrial Technology Leakage in Enterprise', *The Korean Association for Industrial Security*, vol.1, no.1, pp. 1-19.

Kim, S.S. & Shin, J. C. 2013, *Industrial Information Security*, Green Press

Kwak, S. J., Yoo, S. H. & Chang, J. I. 2005, 'The role of the maritime industry in the Korean national economy: an input–output analysis', *Marine Policy*, vol. 29, no.4, pp. 371-383.

Lee, C. M., 2011, 'A Study on the Conceptual Definition of Industrial Security', *The Korean Association for Industrial Security*, vol. 2, no.1, pp. 73-90.

Mathews, J. A. & Cho, D. S. 2007, *Tiger technology: The creation of a semiconductor industry in East Asia*, Cambridge, University Press.

Park, I.B. & Kim, J.D., 2011, 'A Study on the Policy Management for Industrial Security's Culture', *The Korean Association for Industrial Security*, vol. 2, no. 1, pp. 33-46.

Robert, B. & Lajtha, C., 2002, 'A new approach to crisis management', *Journal of Contingencies and Crisis Management*, vol. 10, no. 4, pp. 181-191.

Sennewald, C. A. 2003, *Effective security management*, Butterworth-Heinemann.

Song, B. N. 1997, *The rise of the Korean economy*, Oxford, Oxford University Press.

The Korean Association for Industrial Security 2012, *Industrial Security*, Seoul, Pakyoungsa.

The Korean Association for Industrial Technology Security & The Korean Association for Industrial Security 2013, *Technology Leakage Cases and Security Tips*, The Korean Association for Industrial Technology Security.

Whitney, M. E. & Gaisford, J. D. 1999, 'An Inquiry Into the Rationale for Economic Espionage',

International Economic Journal, vol. 13, no. 2, pp. 103-123.

Winkler, I. 1997, *Corporate Espionage: what it is, why it is happening in your company, what you must do about it*, Prima Pub.

(Internet Sources)

http://en.wikipedia.org/wiki/Samsung_Electronics
http://en.wikipedia.org/wiki/Lg_electronic