Webology (ISSN: 1735-188X)
Volume 19, Number 4, 2022

Future Security Threats: Study On The Human Factor Of Industrial Security For The Prevention Of Security Leaks In South Korea

Jungbin Lim[1] , Dongkyu Kim[2]

[1]Department of Psychology, Sungkyunkwan University, Republic of Korea.

[2]Master's Program in Intellectual Property, Korea Advanced Institute of Science and Technology(KAIST), Republic of Korea.

Pritzker School of Law, Northwestern University, Illinois, United States of America.

ABSTRACT: With the advent of the fourth industrial revolution, rapid advancement in technology has blurred the distinction between the physical and digital worlds. Such advancement poses increased risk of security leakage by industrial spies, resulting in threats to industrial security. In response, there has been an increasing focus on "human factors" as one of the main factors of industrial security leakage. In order to examine the influence of human factors on industrial security, we measured the influence of individualistic-collectivistic value orientation on the perception of severity of industrial security leakage according to specific motives and contents of the leakage, and experience of security training according to the type of industry. As a result, differences in the perception of the severity of industrial security leakage were observed between people with collectivistic and individualistic value orientation. In addition, there were differences in perception of severity according to the specific motives and content of industrial security leakage. Finally, there was a difference in the completion rate of security training according to the type of industry. Implications of these findings for industrial security are further discussed.

ACKNOWLEDGEMENTS: This research paper won an Award from The Korea Association for Futures Studies Research Paper Contest in 2021.

1. Introduction

According to the 2021 International IP Index of the U.S. Chamber of Commerce, which evaluates the protection and execution level of intellectual property, Korea ranked 12th out of 53 countries with a total score of 83.73. Specifically, patent protection ranked third, copyright protection ranked seventh, trademark protection ranked third, and design protection ranked ninth. Overall, it received high recognition for system efficiency, including patents, copyrights, trademarks and design rights, but remained 16th with 70 points (U.S. Chamber of Commerce International IP Index and Global Innovation Policy Center 2021). Regarding trade secrets, Korea was evaluated as having high barriers to market entry for overseas intellectual property owners and excessive license registration requirements. Overall, Korea's industrial technology protection capability has significantly improved, but it still needs to be supplemented in some fields.

Since the mid-2000s, as Korean companies have begun to work in the global market with competitiveness, industrial spy activities have also increased. According to the National Intelligence

Service's Industrial Technology Protection Center, starting with 6 cases in 2003, the number of cases increased to 26, 29, 31, 32, 42, 43, 41, and 46 annually from 2004 to 2011, and increased significantly to 63 cases in 2016 (C. Park, 2016). In particular, the technology outflow of domestic SMEs was more serious (C. Park, 2016). In recent years, cybercrime has emerged as a side effect of informationization following technological development, and as a result, industrial spies have diversified their scope of action. Accordingly, the need to diversify the Korean government's response was also raised. Recently, the National Intelligence Service Industrial Confidentiality Protection Center established a council with the Korea Bio-Association for the protection of national core technologies in biotechnology (BioTimes, 2021). In addition, the National Intelligence Service, the Ministry of Trade, Industry, and Energy, the Ministry of SMEs and Startups, and the National Police Agency recognize the importance of industrial security and strengthen public-private cooperation.

The problem of industrial security and technology leakage is recognized as a problem of national security beyond just information theft. For example, the U.S. Federal Communications Commission last year designated Huawei and Zhongxing Telecom (ZTE) as a threat to U.S. national security, stating that they engaged in industrial espionage through internet networkS (BioTimes, 2021). With the ratification of the Defense Authorization Act in 2019, the products of five Chinese companies, including Huawei and Zhongxing Telecom, were excluded from government procurement. In February of the same year, U.S. Vice President Mike Pence urged allies to restrict the use of Huawei products (S. Kim, 2019).

2. Industrial Security and Human Factors as Emerging Security Threats

2.1. Emerging Security Threats and Industrial Security

In the 21st century, predicting the future at the national level is more important due to increased uncertainty in the knowledge base and rapid technological development (S. Yoo et al., 1985). In particular, in the field of security, the emergence of new security threats is deepening this complexity. S. Kim(2017) refers to emerging security threats as a phenomenon in which safety issues at the micro-level is expanded to large-scale security issues at the macro-level (S. Kim et al., 2017). The reason why emerging security issues are important is because while traditional security threats can be identified explicitly, risks of emerging security are not explicitly identified (S. Kim et al., 2017). If this importance of emerging security is overlooked, it can be triggered and expanded into a crisis in the field of traditional security, so special attention is required.

The problem of hacking, recently expanding into cyber warfare between countries is an example where emerging security threats and traditional security threats overlap (S. Kim et al., 2017). Kim emphasized the recent increase in hacking, computer viruses and the spread of malicious code, and said that such attacks will turn into national security issues and link them to international security issues when it comes to theft of high economic value (S. Kim et al., 2017). For example, the U.S. government stressed that Huawei should be viewed as a security threat, and not an industry issue, and that a de-geopolitical perspective is needed for competition and cooperation in the 4th Industrial Revolution and 5G telecommunications sector (S. Kim, 2019). In addition, it is said that the trend of U.S.-China competition, which is an international concern, will be based on technology competition for artificial intelligence, big data, cloud computing, and the Internet of Things represented by the 4th industrial revolution (S. Kim, 2019).

In the era of the Fourth Industrial Revolution, new security threats are already being discussed, and security issues based on difficult technologies will continue to expand. In particular, hyperconnectivity caused by the Fourth Industrial Revolution is likely to expand risks from the private sector to the industrial sector, which will deepen the vulnerability of industrial security (B. Jeong & J. Jeong, 2018; H. Son & J. Kang, 2019).

Industrial spies at the center of technology leaks are known to have existed since B.C. It is a well-known example that in 1712, before the Industrial Revolution, the French Jesuit priest stole the secret of hard porcelain, and some potters sent long letters explaining their findings. Industrial spies continued to exist from the 18th century, the first industrial revolution, the 19th to the early 20th century, the second industrial revolution, the computer- and Internet-based knowledge and information revolution, and the fourth industrial revolution, now based on hyperconnectivity and superautonomy. After the 4th Industrial Revolution, the types of industrial spies' behavior in the cyber domain will be more diversified, advanced, and intelligent.

In order to prevent technology leakage by industrial spies, the Korean government has been making pan-governmental efforts to protect industrial technology since the early 2000s. In October 2003, the National Intelligence Service established an industrial confidentiality protection center for industrial spy detection and prevention activities through industrial security education to prevent illegal leakage of Korea's advanced technology and management information. The following year, the Ministry of Science and Technology (currently the Ministry of Science and ICT) and the Ministry of Information and Communication formed and operated the "Industrial Security Policy Council" (H. Shin, 2019). In addition, the National Police Agency launched an industrial technology leakage investigation team in six local offices in 2010, and expanded it to 20 investigation teams in April 2019 (H. Shin, 2019). In November 2014, the Small and Medium Enterprises Technology Protection Support Act (hereinafter referred to as the "Small and Medium Enterprises Technology Protection Act") was enacted and enforced, and in January 2017, the Ministry's Integrated Small and Medium Enterprises Technology Protection Integrated Counseling Center was opened.

2.2 Industrial security and human factors

Industrial security refers to “response measures or activities to prevent infringement from acts for all technical and managerial information useful for industrial activities, personnel, documents, facilities, and information systems” (H. Moon et al., 2014). In addition, industrial security is defined as protecting all tangible and intangible industrial assets from illegal activities, including every lines of effort to protect all economic activities from criminal acts and prevent damage to industrial assets (S. Lee, 2019). As the risk of technology leakage increases due to the synchronization of the global industrial structure following the aforementioned industrial revolution, the importance of industrial security will continue to expand.

The convergence of ‘technology’ and ‘human’ is increasingly being emphasized as the core value of future society. In January 2016, World Economic Forum president Klaus Schwab expressed that the convergence of “people” and “science and technology” makes the 4th industrial revolution and autonomy possible as a “hyper-connected society” (C. Park, 2016). Also, regarding the post-human era, the “a human-computer symbiosis” combines natural and artificial elements into one system (W. Lee, 2014). In particular, one of the characteristics of recent industrial security research is that, due to the changing corporate environment, not only technological security measures but also human security measures are being focused (S. Jung & C. Lee, 2020).

The issue of the cognitive dimension regarding industrial security was covered in a number of previous studies (H. Moon et al. 2014). Most studies emphasized the severity of the "lack of overall security awareness" on industrial security awareness (S. Lee, 2019). For example, in 2003, the White House stated that the weakness identified in industrial security in the transition to advanced technology lies in personnel management, and the importance of personnel management also included the need for human intelligence (HUMINT) and performance capability enhancement. In April 2019, the Korean government is making efforts to protect the country, companies and individuals through efforts such as establishing a "national cybersecurity strategy" for the first time.

Previous studies show that the importance of human factors are increasing with respect to the core factors of industrial security, which was mainly studied in the technology and institutional fields. In order to further understand the issue of industrial security and technology leakage change as a future security threat, we focused on the human factors of industrial security from a behavioral science perspective, and derive implications on how the Korean government's industrial security policy on human factors. To this end, we conducted a survey to examine public perception on the severity of industrial security leak motives and routes according to individualistic-collectivistic value orientation, and further assessed the rate of security training completion according to the type of industry. We then presented data collected from the survey, followed by a discussion on the implications of the results in the implementation of industrial security policies.

3. Research Method and Design

3.1. Participants

A survey was conducted using a structured online questionnaire on 274 participants over the age of 19 with Korean nationality. The demographic composition of participants is presented in Table 1.

Type of Industry	Male	Female	Other	Sum
Large Corporation	42	8	0	50
SMEs	50	18	0	68
Self-Employed / Startups	32	8	0	40
Public Service	42	16	2	60
Other	55	21	0	76
Sum	198	70	2	274

Table 1. Demographic Composition of Participants

3.2. Measures

3.2.1. Individualistic-Collectivistic Value Orientation

Individualistic-Collectivistic value orientation refers to a system of beliefs regarding whether the individual or the group should be prioritized when individual goals and group goals conflict (Hofstede, 1980). People with individualistic value orientation prioritize individual goals and interests, while people with collectivistic value orientation prioritize group interests. Individualistic-Collectivistic value orientation is a constituent concept applied to various social behaviors. Therfore, we expected that individualistic-collectivistic value orientation will affect people's perception of severity of industrial security leakage.

Individualistic-Collective value orientation was measured through a reconstructed eight-item questionnaire widely used in previous studies (E. Choi et al., 2012). Conflicting sentences representing 'collective value orientation' and 'individualism value orientation' are presented on each side of the questionnaire respectively, and participants indicated the extent to which they agree with either of the two sentences (6-point scale). The questionnaire consisted of four questions measuring 'group-person goal priority' and four questions measuring 'cooperative-competitive behavior patterns'. If the average score of the responses to the eight questions exceeds 3.5, the participant was categorized as a collectivist, and if less than 3.5, the participant was categorized as an individualist.

3.2.2. Perception of Industrial Security Leak Motives

The perception of industrial security leak motives was measured by dividing organizational level motives and individual level motives. Organizationial level motives were measured by asking the perceived severity of “insufficient security management and supervision”, “insufficient security-related investments”, “lack of dedicated security personnel” and “lack of security awareness by employees”, and individual level motives were measured by asking the perceived severity of “pursuit of personal financial gain”, “dissatisfaction with the company” and “job insecurity and concerns of unemployment” on a 7-point scale (1=not serious at all, 7=very serious).

3.2.3. Perception of Industrial Security Leakers and Leak Routes

The perception industrial security leakers was measured by asking the perceived severity of the leak according to the leaker’s status (current or former employee), affiliation (primary contractor or subcontractor), and nationality of the leaker(Korean or foreigner) on a 6-point scale. Then, to measure the perceived severity of the leak according to the leak routes, participants were asked the perceived severity of the leak due to “theft of technical data”, “recruitment of key personnel by competitors”, “use of unauthorized e-mail or portable devices”, “external joint projects or research” and “bribery by competitors” on a 7-point scale (1=not serious at all, 7=very serious).

4. Results of the study

4.1. Awareness of industrial security leaks

4.1.1 Perception of Industrial Security Leak Motives according to Individualistic-Collectivistic Value Orientation

To examine the effect of collectivism-individualism value orientation on the perception of industrial security leak motives, a t-test was conducted to determine whether the difference in severity perception of organizational level motivation and individual level motivation according to individualistic-collectivistic value orientation was statistically significant, respectively. As a result of the t-test, there was a statistically significant difference (p=0.05) in the degree of severity perception between those with collectivistic value orientation and those with individualistic value orientation regarding organizational level motivation, but regarding individual level motivation, the difference was not statistically significant. For individual level motivation, both individualists and collectivists perceived them as key motives of industrial security leaks, but for organizational level motivation, only collectivists perceived them as primary motives of industrial security leaks. Analysis results are presented in Table 2.

	m		sd		t-value	p-value
	Individualist (n=100)	Collectivist (n=174)	Individualist (n=100)	Collectivist (n=174)		
Organizational Level Motivation	5.10	5.64	1.13	1.06	2.02	0.05
Individual Level Motivation	5.48	5.61	0.92	1.01	0.57	0.57

Table 2. Perception of industrial security leak motives according to value orientation

For a more detailed analysis, descriptive statistical analysis was conducted for each item. As a result of the analysis, the degree of severity perception of individual level motivation as serious motives of industrial security leaks was higher than organizational level motivation (m=5.60, m=5.57, respectively). More specifically, “pursuit of personal financial gain” was perceived as the most serious motivation of industrial security leakage (m=6.28). Analysis results are presented in Table 3.

	Item	m	sd
Organizational Level Motivation	Insufficient security management and supervision	5.50	1.34
	Insufficient security-related investments	5.53	1.36
	Lack of dedicated security personnel	5.36	1.42
	Lack of security awareness by employees	5.88	1.15
	Average	5.57	1.32
Personal Level Motivation	Pursuit of personal financial gain	6.28	0.98
	Dissatisfaction with the company	5.49	1.23
	Job insecurity and concerns of unemployment	5.02	1.59
	Average	5.60	1.27

Table 3. Industrial security leak motive perception descriptive statistics

4.1.2. Perception of Industrial Security Leakers and Leak Routes

Descriptive statistical analysis was performed on each item to find out the severity perception of industrial security leakers and specific leak routes. There was no difference in severity perception according to the status of the leaker. Regarding affiliation, leaks by the prime contractor was perceived as more serious than those by the subcontractor (61.31% and 38.69%, respectively), and regarding nationality, leaks by Koreans was perceived as more serious than those by foreigners (58.76%, 41.24%, respectively). Analysis results are presented in Table 4.

	Item	Responses	Rate
Status	Current Employee	137	50.00%
	Former Employee	137	50.00%
Affiliation	Prime Contractor	168	61.31%

	Subcontractor	106	38.69%
Nationality	Korean	161	58.76%
	Foreigner	113	41.24%

Table 4. Severity recognition descriptive statistics according to industrial security leakers

In addition, following analysis the severity of the industrial security leak routes, severity perception of industrial security leakage due to bribery by competitors (m=6.14) and theft of technical data (m=6.13) were relatively high, but the severity perception of external joint projects or research (m=5.45) was relatively low. Analysis results are presented in Table 5.

Item	**m**	**sd**
Theft of technical data	6.13	0.95
Recruiting key personnel by competitors	5.83	1.20
Use of unauthorized e-mail or portable devices	6.07	1.00
External joint projects or research	5.45	1.35
Bribery by competitors	6.14	1.05

Table 5. Severity recognition descriptive statistics according to industrial security leak path

4.2. Completion of Security Training according to Type of Industry

Descriptive statistical analysis was conducted to compare the completion rate of security education according to the type of industry. The security training completion rate was highest in the order of large corporations (92%), military and public service (76.67%), SMEs (73.53%), and self-employed and startups (25%). Analysis results are presented in Table 6.

Industry	**Total**	**Completed Training**	**Completion Rate**
Large Corporation	50	46	92.00%
SMEs	68	50	73.53%
Self-Employed / Startups	40	10	25.00%
Public Service	60	46	76.67%
Other	76	10	13.16%
Sum	270	162	62.96%

Table 6. Descriptive statistics of security training completion according to type of industry

5. Discussion

Through the present study, we were able to derive implications regarding the perception of severity of industrial security leaks according to the motives and routes of various leaks and the completion of security training according to the type of industry. The main results of the present study are summarized and presented in Table 7.

	Description	Results
1	Perception of Industrial Security Leak Motives According to Value Orientation	For individual level motives, both individualists and collectivists perceived them as serious, but for organizational level moties, collectivists perceived them as more serious than individualists.
2	Severity descriptive statistics according to industrial security leak motive, leaker, and leak path	Severity perceptions were higher for individual level leak motives than organizational level motives, and leaks by primary contractors and Koreans were perceived as more serious than by subcontractors and foreigners. Recruitment by competitors was perceived as the most serious leak route.
3	Completion Rate of Security Training According to Type of Industry	The security training completion rate was in the order of large corporations, military and public service, SMEs, and self-employed/startups.

Table 7. Summary of main results

5.1. Perception of severity according to value orientation and leakage process

The results indicate that both individualists and collectivists perceived industry security leaks due to individual level motives such as pursuit of individual financial gains, dissatisfaction with the company's treatment, job insecurity and concerns of unemployment. However, when it comes to organizational level motives such as the company's insufficient security management and supervision, insufficient investment in security, absence of a dedicated security personnel, and lack of security awareness among employees, the severity perception of collectivists were higher than individualists..

Collectivistic value orientation puts priority over group goals over individual gains and harmony among group members. Collectivistic culture in Korea is used to explain Koreans' tendencies to prioritize groups over individuals and form good relationships between oneself and group members (J. Yang, 2019). Collective efforts in the prevention of COVID-19, is a successful example of collectivism in Korea, and the media emphasized the merits of Korean collectivism, in which people shown a strong unity in refraining from pursuing individual gains for the common goal of the group (The Opinion News, 2021). In this regard, the present study shows the importance of raising collective consciousness in preventing industrial security leaks. In particular, collectivism can have a positive effect on improving organizational performance by providing institutional devices for job involvement and organizational commitment (H. Maeng & S. Kim, 2019).

In general, the results indicate that people with collectivistic value orientation who respond protectively to the ingroup are more demanding on organizational roles and responsibilities. Industrial security cannot be achieved with organizational technology and systems alone, and it is important for employees to take proactive responsibility to ensure industrial security.

5.2. Perception of the severity according to the motive of the leak, the nature of the leaker, and the route of the leak

As depicted in Table 8, the primary cause for technology leaks was the lack of proper security management and supervision for past 3 years from 2017 to 2019. However, participants of the present study responded that individual-level motives were more serious motivations for security leaks than organizational-level motives. While the number of technology leaks motivated by personal financial gain has been on the rise from 5.1% in 2017 to 20.2% and 29.6% in 2018, but most technology leaks has still occursed more frequently due to insufficient countermeasures at the organizational level. The severity perceived by people and the statistics of actual leaks show that there is a gap between public perception and reality.

Year	**2017**	**2018**	**2019**
Insufficient security management and supervision system	**46.5%**	**44.4%**	**34.9%**
Insufficient security-related investment	**11.6%**	**24.5%**	**30.6%**
Lack of dedicated security personnel	3.8%	14.5%	21.7%
Lack of security awareness among employees	**23.5%**	**35.9%**	**32.4%**
Pursuit of personal financial gain	5.1%	20.2%	29.6%
Dissatisfaction with the company's treatment	3.1%	17%	15.4%
Job instability and concerns of unemployment	3%	5.9%	12.9%
Other	1.5%	-	0.1%

Table 8. Primary cause for technology leaks (motive behind the leak)

* Reconstructed from the “Small and Medium Enterprises Technology Protection Fence” website

Second, the results indicate that people perceive industrial security leaks by the prime contractor as more serious than those by subcontractors, and leaks by Koreans than by foreigners as more serious. This shows that because of emotions toward the ingroup(prime contractor, Koreans), leaks by the ingroup lead to anger due to feelings of betrayal. In light of this, technology leaks by prime contractors or Koreans, pose a risk of adversely affecting the overall morale of employees at the organizational level. Therefore, in the event of such leaks, the leadership should show a responsible attitude and make efforts to restore fairness and transparency (C. Wi & S. Kwon, 2017).

Third, the results show that people perceived recruitment of key personnel by competitors as the most serious leak route (m=5.83). However, from 2017 to 2019, the rate of technology leaks of SMEs through recruitment of key personnel accounted for only 19.3%, 14.7%, and 17.6% of leaks respectively, as depicted in Table 9. On the other hand, in 2017 and 2018, security leaks through use of unauthorized e-mail and mobile devices accounted for 53.4% and 79.4% of leaks, and in 2019, leaks through theft of technical data accounted for 70.6% of leaks. These results shows a difference in public perception and actual technology leaks regarding leak routes.

Year	**2017**	**2018**	**2019**

Theft of technical data	18.2%	47.1%	**70.6%**
Recruitment of key personnel by competitors	19.3%	14.7%	17.6%
Use of unauthorized e-mail or portable devices	**53.4%**	**79.4%**	58.8%
External joint projects or research	3.4%	5.9%	29.4%
Bribery by competitors	2.3%	5.9%	5.9%
Other	29.5%	2.9%	17.6%

Table 9. Technology leak path and leaker (leakage process)

* Reconstructed from the "Small and Medium Enterprises Technology Protection Fence" website

Taken together, the results show a differences in perception regarding the motive of the leak, the nature of the leaker, and the route of the leak. Once the public perceives the severity of a given risk, they will seek to acquire relevant information or knowledge on prevention measures and coping methods (H. Song et al., 2014). Therefore, it is important to provide more accurate information on the motives and types of technology leaks that occur commonly in reality by disclosing accurate statistics on how technology leaks occur in companies. To this end, it would be important to raise awareness of industrial security leak prevention by raising awareness of common leak cases.

5.3. Descriptive statistics of completion of security training by place of work

The results from the present study shows that the completion rate of security training differed according to the type of industry. Security training completion rate by type of industry was in the order of large corporations, military and public service, SMEs, and self-employed/startups.

Companies conduct various training and education programs to enhance corporate development, individual career development, and job satisfaction, such as on-the-job training, apprenticeship programs, off-the-job training, and online training, and this includes security training (S. Kim et al., 2019). However, in the case of startup employees, the completion rate of security training was notably low. This may be due to the fact that most SMEs and startups have relatively limited capacity in providing security training due to lack of budget and resources (The Economic Review, 2015). Therefore, more efforts should be made to support SMEs and startups at the national level, especially for startup companies with low security training completion rates.

6. Conclusion

The advent of the fourth industrial revolution has increased the risk of industrial security leaks, and at the same time, methods and types of security leaks have been diversified. In addition, with the increasing importance of the cyber domain, the severity of cyber technology leaks through hacking has also been increasing. Such technology leaks can be viewed as a new axis of emerging future security risks.

Recently, the Korean government is making various efforts to strengthen the human factors of industrial security. Our findings suggest that collectivistic value orientation can promote stronger awareness of industrial security, but there are differences in public perception and reality regarding actual cases of industrial security leaks, and insufficient security training in SMEs and startups. As such, it is necessary to secure social consensus on the prevention of industrial security leaks through the sharing of accurate information on the status of industrial security and technology leaks, and recognition that individuals are also important actors in individual level efforts.

References

BioTimes. (2021). KoreaBIO and NIS, launches 'the Industrial Security Society in the field of Biotechnology.

Choi, E., Song, B., Lee, Y., Park, K. (2012). A Study on the Leaking Channels of Industrial Technology. The Journal of Police Policies, 26(1), 225-259.

Hofstede. (1980). Culture and Organizations. International Studies of Management & Organization, 10(4), 15–41.

Jeong, B. & Jeong, J. (2018). Digital Sharing Eonomy and Bockchain. Journal of Korean Social Trend and Perspective (KSTP), 103, 114-146.

Jung, S. & Lee, C. (2020). A Study on the Psychological Security Vulnerabilities of Employees from a Perspective of Industrial Security - Focused on Dual Process Theory. Korean Security Journal, 63, 41-58.

Kim, S., Min, B., Sohn, Y., Chun, C., & Jo, D. (2017). The World Politics of Emerging Security on the Korean Peninsula. Sapyoung Academy, 1.

Kim. S. (2019). The Huawei Incident and U.S.-China Technological Hegemony Competition: The Complex Geopolitics of Leading Sectors and Cyber Security. Review of International and Area Studies(RIAS), 28(3), 125-156.

Kim, S., Kim, J., & La, S. (2019). Introduction to Management, 1st Ed.

Lee, S. (2019). A Study on University Students' Recognition Attitude the Importance of Industrial Security. The Korean Association of Police Science Review (KAPS), 21(2), 139-160.

Lee, W., Son, S., Cho, S., Yoo, S., Kim S., Lee, S., Kang, J., Lee, J., Lee, J. (2014). A Multi-disciplinary Research on lnteractive Relationship Between Human and ICT in the Post-Human Era,Korea Information Society Development Institute.

Maeng, H., & Kim, S. (2019). The Effect of Individual Cultural Orientation on Organizational Commitment, Job Involvement and the Moderating Role of Perceived Organizational Support. Korean Corporation Management Review, 26(4), 159–183.

Moon, H., Chun, L. & Song, B. (2019). The Values of Koreans and the Preference Values of Futures in South Korea. Journal of Regional Studies(JRS), 27(2), 179-205.

Park, C. (2016). Strategies for Industrial Technology Protection in the midst of Future Social Change, Science and Technology Policy Institute.

Son, H. & Kang, J. (2019). The Values of Korean and the Preference Values of Futures in South Korea. Journal of Regional Studies(JRS), 27(2), 179-205.

Song, H., Kim, C., & Kim, W. (2014). Effects of Public's Media Dependency, Risk Severity, and Subjective Knowledge on Preventive Behavior Intention of Cyber Crime. Crisisonomy, 10(5), 83–100.

Shin, H. (2019). A Study on the Development of Industrial Security in Korea; Industrial Espionage Prevention Activities, Korean Journal of Indsutrial Security, 9(1), 35-67.

The Economic Review. (2016). [Cyber World War III] Cybersecurity. The Answer is in the People.

The Opinion News. (2021). [Korean Society and Culture Viewed by a Linguist] COVID-19 Prevention: Korean Collectivism and American Individualism.

U.S. Chamber of Commerce International IP Index and Global Innovation Policy Center. (2021). U.S. Chamber International IP Index 2021.

Wi, C. & Kwon S. (2017). The Effect of Cognition of Personal Information Leakage Controllability on Affection and Conation : Focused on Comparing between External Hacking and Internal Leakage. Korean Management Review, 46(6), 1,555-1,576.

Yang, J. (2019). The Influence of Korean Collectivism(Uri, we-ness) on Interpersonal Communication Behaviors. The Journal of the Korea Contents Association, 19(5), 1–14.

Yoo, S., Lee, M., Shin, S. (1985). Future Prediction Methodology, ITFind.