sustainability

MDPI

Article

A Meta-Analysis of Industrial Security Research for Sustainable Organizational Growth

Harang Yu [1] and Hangbae Chang [2,*]

[1] Department of Security Convergence, Chung-Ang University, Seoul 06974, Korea; hryu356@cau.ac.kr
[2] Department of Industrial Security, Chung-Ang University, Seoul 06974, Korea
* Correspondence: hbchang@cau.ac.kr; Tel.: +82-2-820-5538

Received: 27 September 2020; Accepted: 13 November 2020; Published: 16 November 2020

Abstract: As the world enters a fourth Industrial Revolution, organizations worldwide face challenges in dealing with important assets such as industrial technology. Leaking these assets can not only damage organizations economically but also negatively affect customer relationships and brand image. This has led to an increased awareness of industrial security in both the business and academic spheres and a focus on identifying and implementing countermeasures against security incidents, as future computing environments will continuously face security threats. This study first examines the literature on industrial security and its current status in South Korea, which is considered an active industrial security research environment. Subsequently, meta-analyses are conducted on South Korea and abroad to compare their status and research trends in the industrial security field. The results confirm that South Korea has more actively conducted relevant studies compared to international research. This study contributes to the current literature by not only increasing the awareness of industrial security but also encouraging future studies in the field to facilitate a safe and sustainable computing environment.

Keywords: industrial security; technology leak; sustainable growth; meta-analysis

1. Introduction

Environments based on information and communications technology have widely incorporated innovative technologies in different business industries. As network connectivity has expanded, it has become necessary for industries to adopt information technology, compelling many organizations in various fields to continuously develop. In the computing environment, network connectivity functions have largely expanded in terms of their range and depth, which has enabled organizations to better collaborate and create new value through information-sharing. However, such connections can increase the possibility of security breaches [1] and therefore should be carefully considered from a security perspective. Devices involving the Internet of Things are particularly vulnerable to security attacks owing to their insufficient support for advanced cryptography mechanisms, cyber-attacks and low computational power, among other issues [2,3].

The number of technology leaks has also increased in South Korea, along with the magnitude of damage from such incidents. According to the Ministry of SMEs (small and medium-sized enterprises) and Start-ups in South Korea, sustainable business growth has been constrained owing to various technology leakage incidents, which have caused substantial damage [4], as illustrated in Table 1. As a country with relatively few natural resources, South Korea has increased its national competencies in cutting-edge technology to position new technology as a stable growth engine. To accomplish this goal, an environment should be established to safely secure state-of-the-art industrial technology [5].

Table 1. Status of technology leakage incidents in small and medium-sized enterprises (SMEs) (2013–2018).

Area	2013	2014	2015	2016	2017	2018	Total
Number of damaged organizations	155	63	59	52	52	32	413
Total amount of damage (in USD)	199 M	105 M	74 M	90 M	84 M	92 M	646 M
Damage per incident (in USD)	1.2 M	2 M	1 M	1.5 M	1 M	-	7 M

Economic power is the most important factor globally for nations to exert influence and establish their international superiority in modern society; further, industrial competitiveness is a main factor supporting this economic power. Many countries are actively conducting economic counter-intelligence activities, as weaknesses in industrial competitiveness impact core values, and industrial security is a method of protecting and enabling the sustainable growth of economic power. The worldwide status of and trends in the continuous development of industrial security must be recognized in order to create an advantage over other nations.

As technological security becomes more important, organizations have attempted to increase awareness of this issue while struggling to implement countermeasures. Although studies of industrial security have expanded, researchers have yet to examine the trends and research directions involving industrial security. Further, a comparison with international studies and an understanding of global research trends in industrial security are necessary in order to develop these technologies and compete in a globalized society. Therefore, this study aims to analyze the diverse works on industrial security in South Korea from different perspectives and compare these to research works conducted internationally.

2. Literature Review

2.1. Industrial Security and Its Characteristics

Industrial security is defined as a comprehensive effort to protect economic activities from criminal behavior; it specifically involves asset protections—securing industrial assets from illegal acts—and loss prevention—preventing damage to such assets [6]. Jeon and Chang [7] argues that, in a narrow sense, industrial security protects the core technologies of an organization; broadly, it includes the security processes reflecting each industry's business characteristics. Accordingly, the current study defines industrial security as protecting both the economy and technology. It is internalized in organizations' products or services, such as research and development output, design and manufacturing information, production equipment and personnel. Industrial security differs from information security in that the latter is limited to electronic information, while the former involves the protection of information as well as its critical elements [8]. As previously mentioned, information and technology leaks occur frequently and can significantly damage the targeted organizations. Traditionally, technical issues have been the main consideration in security; however, purported "human" and "organizational" issues have recently become items of discussion [9], further highlighting the importance of a human-centric security perspective. "People" have been increasingly recognized as a primary consideration; this clearly indicates that insiders—rather than people outside the organization—tend to cause technology leaks.

Insider threats are defined as threats posed by people who have the right to access information systems and can misuse this privilege [10]. An information security forecast from Igloo Security [11], an information security corporation based in South Korea, argues that the risk of insider threats will continuously increase owing to "frenemies"—a combination of "friend" and "enemy"—in that insider information leaks and their associated levels of risk will increase as the mobile office environment develops.

This prominent problem notwithstanding, industrial security technology leaks are characterized by two main features. First, it is difficult to perceive whether a security incident has occurred at all, as the leaked information remains with the owner instead of disappearing. Any intrusion or technology

leak is difficult to detect, as detection efforts require coordination among multiple stakeholders to include a well-organized detection system and corresponding technology [12]. Additionally, diverse industry fields have experienced intrusions or threats to their control systems, and this number continues to grow, while preventative security mechanisms are frequently insufficient to deter these attackers [13]. These issues emphasize that, on the one hand, detecting incidents is challenging; on the other hand, actual information infringement or leakage behavior can easily occur. Understandably, a case investigation can only proceed after an information technology leak is actually observed.

Second, although security incidents are rare, they create significant impacts. Technology leaks can critically damage organizations' competitiveness while generating serious economic damage [14]. Organizations experiencing security incidents face direct economic losses [15] owing to the unavailability of work; ultimately, this significantly degrades the future value represented by intangible assets such as reputation, brand image and customer trust [16]. Restoring value is difficult once an information technology leak occurs, which highlights the importance of proactive prevention. When we consider unreported or undiscovered incidents—purported "hidden crimes" or "dark figures"—we find that internal information technology leaks actually occur much more frequently than those reported in official announcements [17]. This raises questions regarding the reliability of official crime statistics [18]. Moreover, technology leaks that occur domestically may spread internationally owing to a lack of reporting. Meanwhile, cyber-attacks have recently evolved into full-scale cyber-technology leaks; for example, HSBC Bank notified its customers in November 2018 that they had detected an unauthorized access to users' online accounts. The crisis was assumed to have occurred through "credential stuffing", in which hackers steal passwords from other websites and use them on banking websites [19]. As this case indicates, the emergence of security threats coincides with information technology leaks, which emphasizes the need for both awareness and countermeasures.

2.2. Technology Leakage Incidents

Technology leaks refer to the stealing and hiding of confidential assets with economical or industrial value, such as trade secrets or ownership information. Three technology leakage methods have been identified based on the degree of technology used in conducting the crime: no-tech, low-tech and high-tech. Although these terms were originally used in the special education [20] and communications fields [21], this study adapts these to establish an operational definition (Table 2) and define leakage methods.

Table 2. Operational definition of technical methods by degree.

Term	Definition	Example
No-tech	Technology leaks occur through deception and the use of power or status, with no use of technology in cyberspace	Spear-phishing Joint ventures
Low-tech	Technology leaks occur through low degrees/levels of technology, such as installing programs	Screenshots Key-logging USB memory sticks Hard disk drives
High-tech	Technology leaks occur through high degrees of technology, such as targeting internal or external vulnerabilities	Persistent threats Dark web Cloud services Steganography

Corporation A, a producer of household appliances in South Korea, developed its own technology in 2009 after several years of effort and financial support amounting to 16 million dollars from the government. However, some retired employees stole confidential data through low-tech methods, such as USB memory sticks and external hard drives. They tried to sell this information to foreign companies for approximately six million dollars, but this illegal trade was exposed during the

price-negotiating process and raised awareness of organizational security [22]. No-tech leakage incidents have also occurred in the display industry. Corporation B intended to establish a manufacturing factory overseas but needed highly skilled manpower trained in manufacturing thin-film-transistor liquid-crystal displays (TFT-LCDs). They scouted for skilled personnel then employed by Corporation C by offering higher salaries. The employees they hired from Corporation C then smuggled TFT-LCD manufacturing technology using personal hard drives. Corresponding technology was developed with investments of approximately 305 million dollars to bridge Corporation B's technical gap within several years. One suspect was apprehended in the off-boarding process, and all of the technological data were confiscated [22]. This incident illustrates how employees can be corrupted and demonstrates their lack of ethical awareness as corporations persistently attempt to lure employees.

2.3. Industrial Security Countermeasures in South Korea

As a way of revitalizing the economy, South Korea has invested in developing a venture-based industry and pioneered a new technology-industry market, resulting in the growth of semi-conductors and displays, among other technologies. Meanwhile, global competitors have limited growth opportunities with domestic corporations, leading to increased attempts to steal domestic innovative technologies through multiple illegal means. These increasing security threats have created the need for organizations to undertake industrial technology security activities against espionage, leading to the concurrent implementation of security systems.

South Korea adopted a trade secret protection system by revising its Unfair Competition Prevention Act in December 1991, which reinforced its laws on trade secret leaks. Enacting this legislation also promoted diverse industrial technology security activities: developing and managing the protection of major technologies by designating them as national core technologies, increasing funds for technology protection equipment and infrastructure and operating remote-controlled security centers to prevent leaks among SMEs. Educational programs to increase security awareness were also offered in the country's *Guidelines for Industrial Technology Security*. Finally, the Korean Association for Industrial Technology Security (KAITS) was launched. Table 3 presents the details of these countermeasure systems and provides a comparison with those in the United States [22].

Table 3. Comparison of technology leakage countermeasure systems.

Purpose	Relevant Institutions	
	South Korea	**United States**
Policy establishment and execution (preventing leaks)	(Government) Ministry of Trade, Industry and Energy (Civil) Korean Association for Industrial Technology Security; Trade Secret Protection Center	(Government) Office of the United States Intellectual Property Enforcement Coordinator; The Committee on Foreign Investment in the United States (Civil) American Society for Industrial Security
Dispute conciliation institution (conflict resolution for technology leakage)	Committee of Dispute Conciliation for Industrial Technology (affiliated with the Ministry of Trade, Industry and Energy)	-
Countermeasures for illegal leakage (detection and investigation of leaked information)	National Intelligence Service (National Industrial Security Center), Public Prosecutors' Office (High-Tech and Financial Crimes Investigation Division), The National Police Agency (Industry Technology Leakage) Investigation Team	Defense Counterintelligence and Security Agency (affiliated with the United States' Department of Defense)

National-level legislation was also enacted to define related regulations that correspond to the Economy Espionage Act in the United States; specifically, the Act on the Prevention of Divulgence and Protection of Industrial Technology was enacted so as to secure superior technology and simultaneously prevent illegal outflows in order to ensure the sustainable growth of the national economy. This legislation also specifies the application target of industrial technology [23] and aims to provide a legal device to deter foreign corporations' legal mergers and acquisitions (M&A). The Act on Support for the Protection of Technologies of Small and Medium Enterprises was enacted to systematically protect technologies and support SMEs, which are especially vulnerable to technology leaks, as most have weak technology-protection capacities [24].

Aside from the law, as previously mentioned, specialized agencies have also been proactive: the diverse and substantial work of the KAITS included developing and collaborating on policies, spreading information on industrial technology leaks abroad and preventing industrial technology leaks through education [22]. One objective of establishing the KAITS was to facilitate collaboration between the government and civil organizations; the agency also manages a specialized certification system for industrial security experts to develop a specialized workforce [25]. Furthermore, academic foundations have been established and thoroughly examined, as departments (majors) were newly organized to systematically develop studies in this field. Industrial security is characterized by its strong operational convergence, which justifies the establishment of university departments to cultivate industrial security experts. The Korean Association for Industrial Security was also established to revitalize systematic, integrated research in industrial security. This organization aims not only to build industrial security as a discipline but also to support national economic growth, increase corporations' competencies and promote the internationalization of industries related to industrial security.

3. Research Methodology

This study conducts a dual meta-analysis of research conducted in South Korea and in other countries. This section first introduces the method for collecting relevant resources and data. Correlations between the selected data and keywords' frequency, degree of centrality and betweenness centrality are examined to determine the relevant keywords' relationships and characteristics.

3.1. Research Procedure

First, prior research on industrial security and related issues was analyzed. Data on relevant legislation and activities were then collected and assessed to clarify the current status of industrial security. Second, inclusion criteria were set to select accurate, meaningful data. Subsequently, selected data were identified and refined. After the final data selection, meta-analyses were conducted with Netminer V.4, which is commonly used for social network analyses. Using this software, we extracted the keyword frequency, degree of centrality and betweenness centrality to analyze the characteristics of—and relationships among—the relevant keywords. The South Korean and international data were separately examined to satisfy this study's objective. Finally, comparisons and common considerations were analyzed to provide a central perspective on industrial security. Figure 1 below illustrates the research methodology.

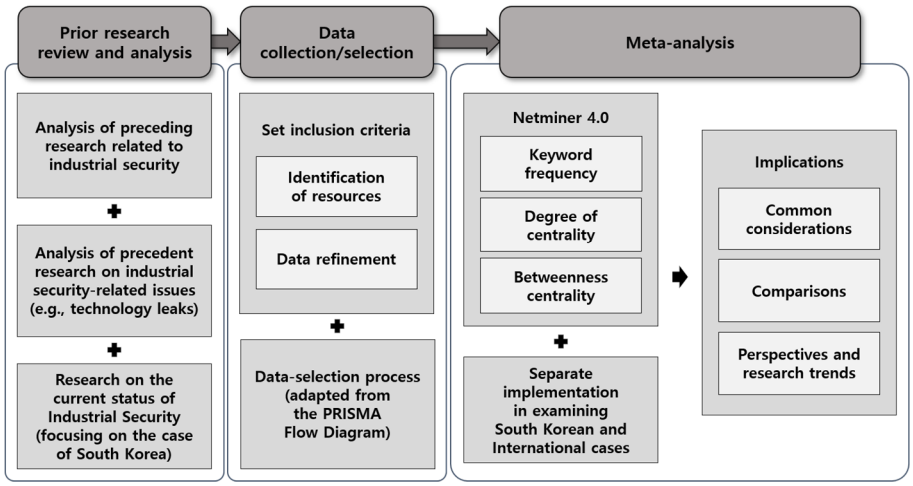


Figure 1. Research procedure.

3.2. Identification of Resources

First, this study considered research in South Korea by utilizing mainstream electronic academic databases, such as the National Digital Science Library and the Korean Studies Information Service System, and included specific journals, such as the *Korean Journal of Industrial Security*, *Journal of Convergence Security* and *Korean Security Journal*. Regarding international research, mainstream electronic academic databases were used—specifically, Web of Science, Springer, and Google Scholar—including the *Security Journal* and the *Journal of Applied Security Research*. Both data sets include five years of studies published from January 2014 to December 2019. The following inclusion criteria were used:

(a) The studies were empirical;
(b) They were available in either English or Korean;
(c) They addressed security in an industrial context;
(d) They were primarily conducted within the business, economics, psychology, legal, regulation, or educational fields.

Keywords regarding publication and document types were limited to journal articles. The search keywords included a combination of "industrial technology", "technology leakage", "research security" and "corporate security".

The exclusion criteria for the selection of studies were as follows:

(a) Systematic reviews and/or meta-analyses;
(b) Theses/dissertations.

3.3. Data Refinement

General verbs, unrelated nouns and prepositions were first excluded. Similar keywords, such as "leak" and "leakage", were considered synonyms. Abbreviations were also regarded as synonyms, such as "IS" and "industrial security", "HR" and "human resources" and "SMEs" and "small and medium-sized enterprises". Finally, plural nouns were treated together with their singular forms, such as "experts" and "expert". Keywords that satisfied the inclusion criteria were used to search the databases; consequently, 125 journal articles were found for South Korea and 19 journal articles for international journals. The data selection process was adapted from the Preferred Reporting Items for Systematic Reviews and Meta-Analysis, which is known as PRISMA flow diagram [26], as illustrated in Figure 2.

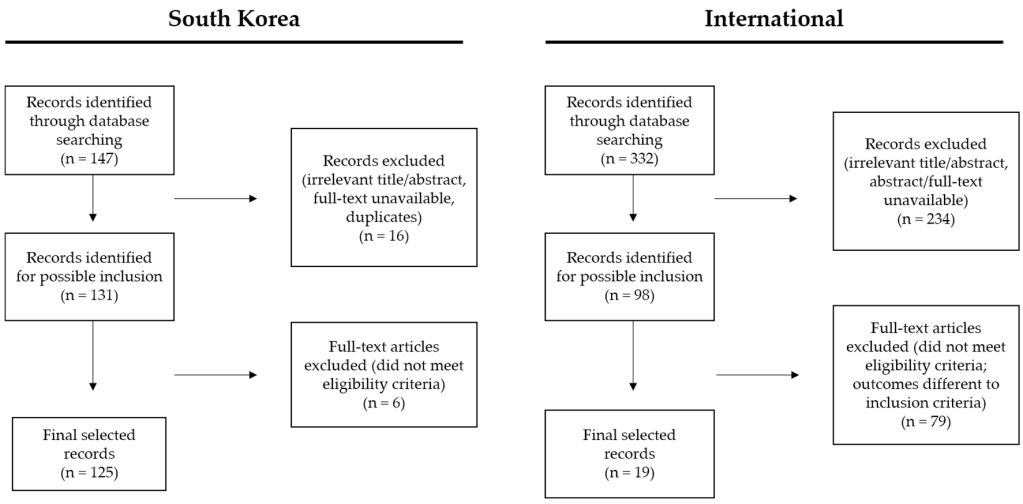
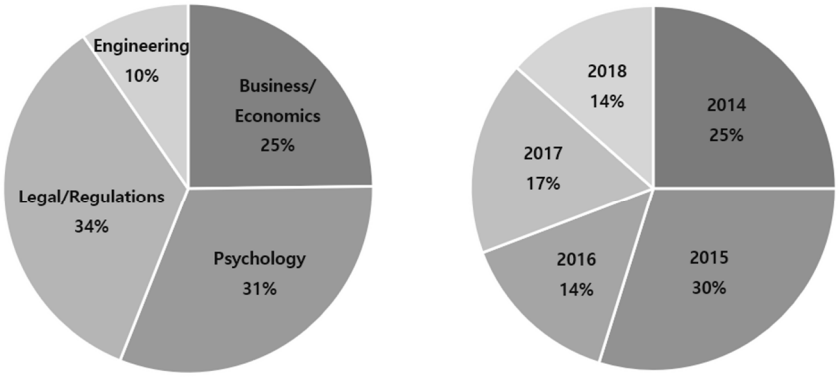


Figure 2. Data selection process.

4. Meta-Analysis Results

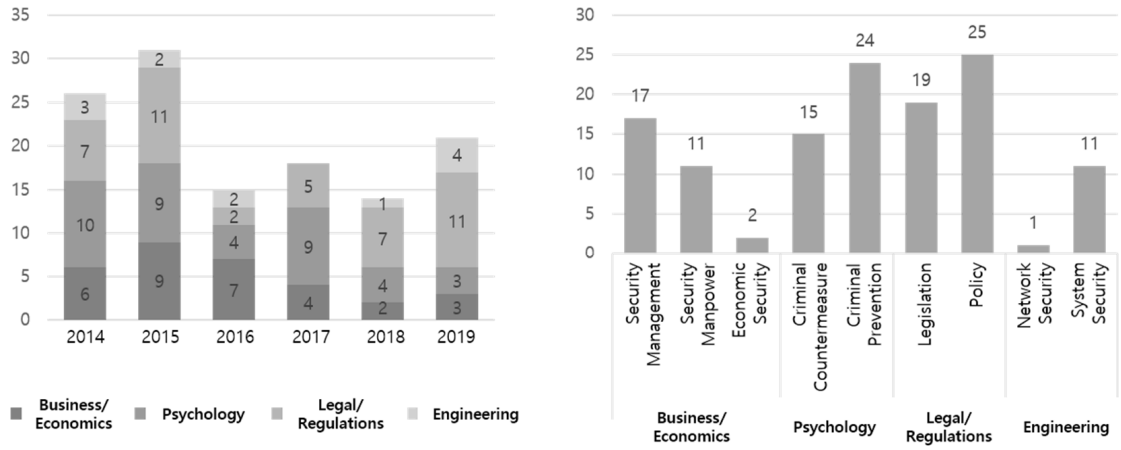
As mentioned in Section 3, this study has two research objectives that involve meta-analysis: to analyze and compare the trends and status of journals related to industrial security. Figure 3 displays the research trends in the industrial security field as well as the frequency of published papers by year in South Korea. We have analyzed the data manually by collecting and counting papers which were published during 2014–2019. Subsequently, we gathered the opinions from industrial security experts and conducted a classification. The left panel (Figure 3a) illustrates the research trends classified by area: business/economics, engineering, legal/regulations and psychology. Legal/regulations comprises the largest portion of all trends, or 34%; this reveals the importance of enacting industrial security-related laws. Psychology is ranked second at 25%, which indicates the increased number of security incidents related to human factors. This is followed by business/economics, which indicates industrial security needs in the business field—including industrial or core technologies—and represents the importance of the economic benefits gained from protecting technologies. Finally, engineering is ranked last, as technical or information-related security is considered "information security", which significantly differs from industrial security. The literature lacks well-defined concepts for each term [7], although studies focusing on the differences in these definitions have increased as industrial security research has expanded, providing corresponding results. The right panel of the figure (Figure 3b) illustrates the frequency of industrial security research published by year.



(a) (b)

Figure 3. Status of industrial security research (2014–2019). (**a**) Research trends by area; (**b**) Publication of frequency by year.

Figure 4a displays the changes in the number of published papers by research area. The right panel (Figure 4b) shows the number of published papers each year by research area in detail.



(a) (b)

Figure 4. Industrial security research areas (2014–2019). (**a**) Changes in number of published papers by research area; (**b**) Research areas in detail.

The significance for measuring relation of different keywords is that by recognizing the relationships between keywords which consists sentence and paragraph, leading to context of whole paper, can identify what certain keywords has co-appeared or formed relations. In order to identify relation of keywords, Netminer was utilized but moreover, this study considered a concepts of Semantic relations. It is classified into five families in large which are Contrasts, Class Inclusion, Similars, Case relations and Part-wholes [27]. The concept of Similars, Class Inclusion, Case relations and Part-wholes when considering a keyword relationships. Similars refer to consisting of terms which overlap in denotative, connotative meaning or both; for example, "laugh-smile". Class Inclusions is a relations involving oner term whose denotative definition subsumes that of the other term as in "animal"-"horse". Case relations has been largely used in network models of propositional knowledge as it refers to being involved in attribution or predication, for example, "dog"-"bark", "cut"-"knife". Lastly, Part-wholes refers to inclusion for pragmatic as in "sofa"-"living room", "tree"-"forest" [27]. We intended to identify keyword relevance in word sense and appearance degree by incorporating the concept of semantic relations between keywords and utilize Netminer.

4.1. Case Analysis Results: South Korean Research

4.1.1. Keyword Frequency and the Degree of Centrality

Keyword frequency is considered by the appearance degree in document. It referred as a density of association; the higher the density of association, the higher the appearance of related keywords. Figure 5 illustrates the keyword frequency, with the most frequently used keyword being "industrial technology leakage"—an issue often encountered in industrial security. "Trade secret" is the next most frequent keyword, which indicates the industry's emerging need to defend against illegal security incidents as well as the importance that South Korea places on the associated laws and regulations to handle the issue on a global level. This is followed by "industrial education", or education in terms of both providing a well-constructed curriculum and relevant security-related programs. Next, "management" refers to organizations' need for security management at the employee and executive levels. "Industrial technology" and "convergence security" follow, which refer to the stability and importance of tackling industrial security issues. Then, "compliance" demonstrates the importance of organizational members' participation in industrial security. "Prevention" and "strategy" follow,

which indicate the importance of identifying preventive countermeasures. "Awareness" represents the overall knowledge regarding industrial security that can help deter problematic security incidents, such as insider threats. The "training" of industrial security experts or employees is also an important keyword. Finally, the keyword "security crisis level" reveals that the industrial security field largely includes studies on how to properly evaluate levels of security.

Figure 5. Keyword frequency (South Korea).

The degree of centrality refers to the influence between keywords [28] and measures the centrality based on the connectivity around a node. Node in degree centrality refers to the number of connection of connection between each node [29] and therefore, appropriate for measuring a direct effect of each node [30]. This analysis present not only which node has the most connection within the network, but also shows node's distance from the center [31]. Table 4 displays the in-degree of centrality scores. The value varies from 0 which refers to non-central to 1 which indicates more-central [32]. The average value of node was deduced as 0.006 and the highest value was drawn as 0.089.

Table 4. Distribution of degree centrality scores. Std. dev.: standard deviation.

Measures	Value
	In-Degree Centrality
Mean	0.006
Std. dev.	0.008
Min.	0.000
Max.	0.089

Concentric map shows a visualization of analysis result of degree of centrality which presents a frequency and importance of keywords within the collected literature beforehand [33–35]. Figure 6 below partially shows a result for specific explanation and the full concentric map is presented in Figure A1 in Appendix A. In this study, a concentric map was visualized by applying Kamada and Kawai's algorithm and intends to find which node is carried out as a key node and figure the correlation between each nodes. The size of a node is determined by the degree of centrality of each keywords [36] and moreover, is located in center part as certain keyword has a high appearance or high degree of centrality [35].

The result of degree of centrality for South Korean research showed that "technology leakage", "trade secret", "industrial technology" was located near the main center part, which demonstrates that the mainly conducted research topic in South Korea was related to security incidents including technology leakage incidents, trade secret and data breach [37–41]. Also, this keyword group shows that among various assets owned by corporations, technology is considered as the highest protection target and conduct security activities accordingly. Following nodes were resulted as "industrial security crime", "insider threat", "Unfair competition prevention and trade protection act", "convergence

security". As shown on Figure 6, the frequency of appearance and location of each node supports the detailed classification of academic field, which are security psychology, security engineering, security legal/regulations and security business/economics [5]. Specifically, "industrial crime" which represents security psychology, explains that researches of drawing a measures to overcome security vulnerabilities resulted from organization members' psychological weakness [42] through not only technical security but also by performing a human-centric security is largely conducted as the definition of information security and industrial security was established [7] in industrial security field of South Korea [43,44]. Moreover, the result shows that malicious attack and espionage is considered as an act of crime in South Korea, also reflecting the frequent attention toward four related laws which is to be mentioned later. The next frequently appeared keyword was "insider threat", which represents security engineering, showed that traditional security activity focused on counteracting against security incidents at the boundary of organizations' inside and outside. This led to the limitation of recognizing insider threat which is reported to occur a lot more than attack from outside [45–47]. Furthermore, it reflects current direction of security incidents is arising from insiders attempt to breach security, information rather than attack from outside. "Unfair competition prevention and trade protection act" which presents security legal/regulations indicates that institutional ways of providing security infrastructure establishment for corporations in South Korea against industrial espionage as technical competitiveness improves and advocate for technology development expand. This also shows the increase in the enactment of related laws and regulations as South Korea developed and secured a leading technique [48,49]. There are mainly four related laws which are Act on Prevention of Divulgence and Protection of Industrial Technology, Unfair Competition Prevention and Trade Secret Protection Act, Act on Support for Protection of Technologies of Small and Medium Enterprises and Defense Technology Security Act, and the analysis result indicates that among four related laws, Unfair Competition Prevention and Trade Secret Protection Act is the most used and referred law. Lastly, security business/economics was not clearly clarified as a keyword however, "convergence security" emerged in light of research trend which pursue sustainable business environment and create profit by establishing enterprise-wide security management solutions and system [50–52]. This indicates security solutions and activities should not be limited in technical security, but integrate and make a connection between technical security and administrative security. In addition, while cyber attack from outside is counteracted with digitalized countermeasure, insider attack should be dealt with a collaboration of countermeasure. For instance, conducting DB security solely cannot prevent security incidents and instead, cooperation work of DB security, document security and network security is required. Accordingly the analysis reflects a frequent occurrence of "convergence security" as a need for collaboration of each countermeasures.

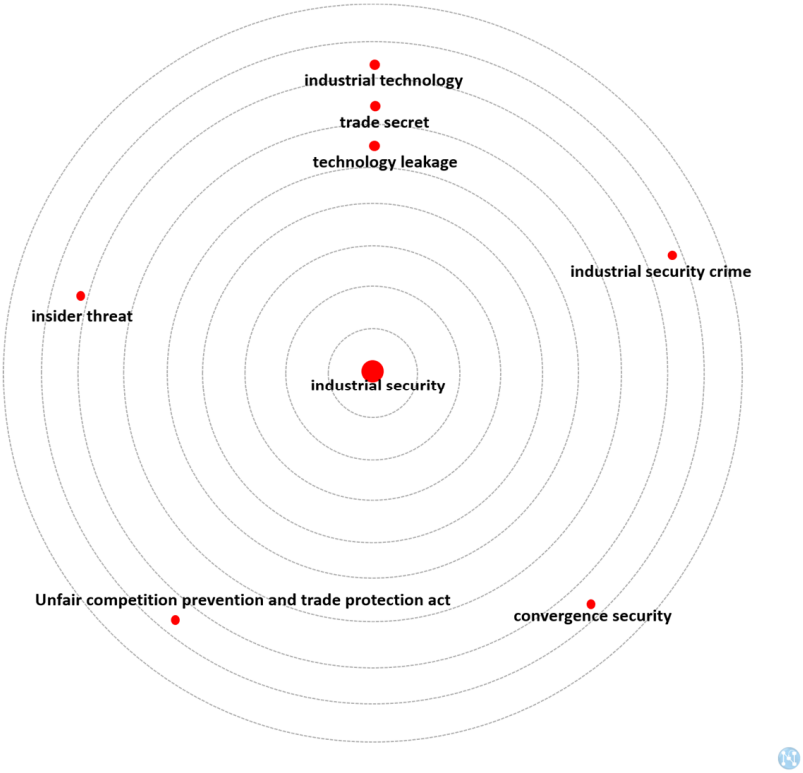


Figure 6. Concentric map of the degrees of centrality(partial).

4.1.2. Betweenness Centrality

The betweenness centrality represents the extent to which a node acts as an intermediary when establishing a network with another node [36]. Accordingly, a greater betweenness centrality implies a greater connection to sub-topics and thus the ability to be extended to other topics [53]. It also measures a particular node's extent of involvement, as illustrated in Figure A2 in Appendix A. The distance between nodes explains the extent of degree; the shorter the distance, the stronger the connection of each nodes [54]. Node with high betweenness centrality plays a role of bridging from one to other node and as a keyword appears in shorter route, it becomes higher level of centrality. Since node of high betweenness centrality can control the information flow, corresponding node will immensely affect in overall connection and communication flow [30]. Betweenness centrality is visualized as spring map which is presented in Figure 7 partially. The original map image is provided in Figure A2 in Appendix A and recommended to refer to Figure A2.

As higher nodes tend to be located in the center, Figure 7 explains that "technology outflow", "industrial technology protection", "industrial security crime", "Unfair competition prevention and trade protection act", "organizational culture", "industrial security-related organization" are highly connected to each keyword and the result demonstrates that corresponding words and related issues have been prominently recognized in the academic arena. Specifically, a connected node between "industry-related organization", "Will of compliance" and "organizational culture" in Figure 7, reflects that organizations' foremost target to protect is the organization in other words, human-centric security rather than encryption against cyberattack. Accordingly, related keywords were drawn as enhancing a security awareness to establish protected organizational culture and guide organization members to spontaneously raise will of compliance toward organization security overall. A security culture must be established to internalize security awareness throughout an entire organization; accordingly, studies on security culture are gaining importance [55–58], supporting the emergence of an "organizational culture". Therefore, outflows of industrial technology continuously increase with the high presence of "industrial espionage".

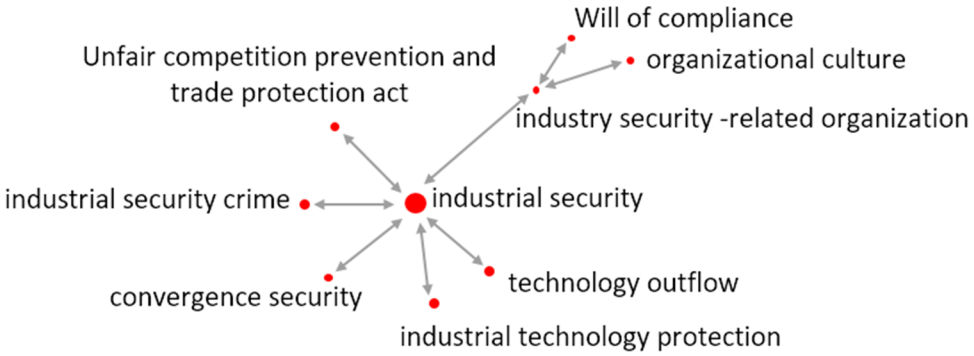


Figure 7. Spring map of the betweenness centrality(partial).

Component dendrogram, also known as tree diagram, marks the level of similarity among formulated nodes and the relation between each keywords can be statistically supported by dendrogram [59]. It includes a keyword network and a type of cluster analysis that repeatedly clusters after measuring similarities based on the patterns of formulated connections between the nodes [36]. Formulated connections refer to when certain word is used, the other, which is connected to the particular word, tends to appear at the same time frequently [59]. The dendrogram chart presented in Figure 8 indicates that the number of clusters decreases as the level of merging increase; specifically, it displays each node's clustering process, which also represents each node's cohesion. Component refers to the sub-network or sub-groups of nodes that use indicators. It demonstrates cohesiveness by binding the maximum number of nodes [53].

The result identified the pairs of [data, counterplan, leakage, protection], [competition, act, prevention, protection, secret, trade] which is a combination of cluster and word and [expert, education, convergence, certificate, security . . .] as a main pairs. Figure 8 is an image of particular part extracted from the original result for clarified visualization. The original dendrogram result is presented in Figure A3 in Appendix A. The first pair which refers to Figure 8a, indicates not only technology but also leakage incident continuously occurs and therefore need a protection toward organizations' assets. Also, in the field of industrial security, the appearance of "protection" and "counterplan" is reasonable, but the appearance of keyword "data" was notable. It can be construed as unlike information security which territory-centric, industrial security focuses on the needs of data-based security system. Second pair which refers to Figure 8b indicates that securing industrial technologies and developing a counterplan have a similar contextual meaning to enacting acts or laws to prevent leakage incidents. The term protection refers to a proper noun particularly used in the law, not a repetition of the other "protection" appeared in previous pair. Moreover, "trade" and "secret" was the most appeared keywords which indicates the importance of technology transfer and confidential management which lead to the practice of technology transfer based on agreement with each interested parties under secured environment. Last main cluster form which is presented in Figure 8c shows that many industrial studies focus on security education, as the importance of creating experts to proactively response against leakage incidents is being stressed which meets the intention of conducting this research. It also emphasizes that the research topics focuses on aligning security with business and conduct converged countermeasures and particularly suggest the necessity of security education for cultivating security experts.

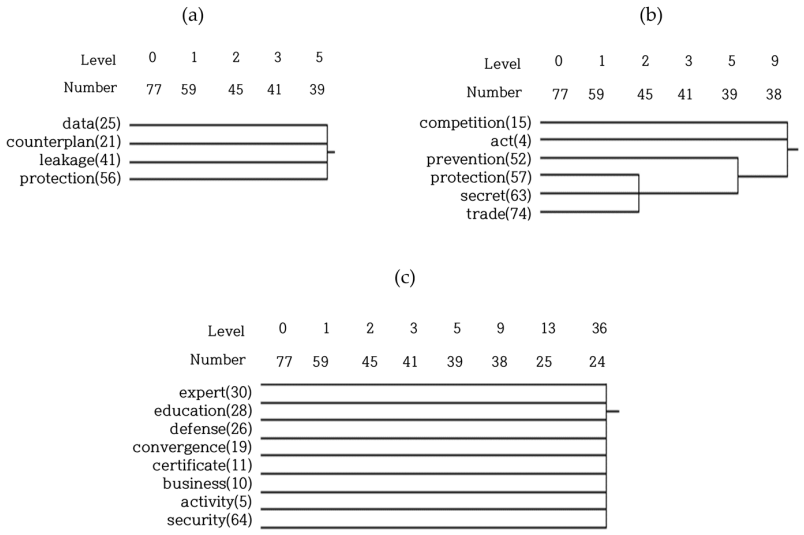


Figure 8. Component dendrogram(partial). (**a**) Data protection subgroup; (**b**) Trade secret prevention and protection subgroup; (**c**) Security education subgroup.

4.2. Case Analysis Results: International Research

As Figure 2 indicates, industrial security research was insufficient based on the inclusion criteria set in this study; only 19 studies qualified as eligible. Accordingly, the extracted articles' keyword frequency was first analyzed, followed by brief analyses of the degree of centrality and betweenness centrality. Additionally, the initial records, before any exclusions, incorporated inclusion data; based on this, most research included topics such as "physical security", "private security" and "guards". Figure 9 displays the keyword frequency, where "crime" is ranked the highest. Keywords such as "crime", "attack" and "victimization" indicate that many studies perceive security as simply a countermeasure for crime and fraud and as an act that involves guarding against these.

Figure 9. Keyword frequency (international).

The results imply that "crime" has a highly relevant relationship with security as illustrated in Figure 10. Various keywords, such as "theft", "victimization", "burglary", "airport" and "guardianship", represent the perspective toward security, in which a systematic concept for and range of industrial security has not yet been established. With "security" and "crime" as the highest nodes, "evidence", "regulation" and "attack" share a common relativity. These results also reveal that international studies reflect physical and private security as a part of industrial security, which must be distinguished and considered separately. This also addresses the scarcity of industrial security-related research.

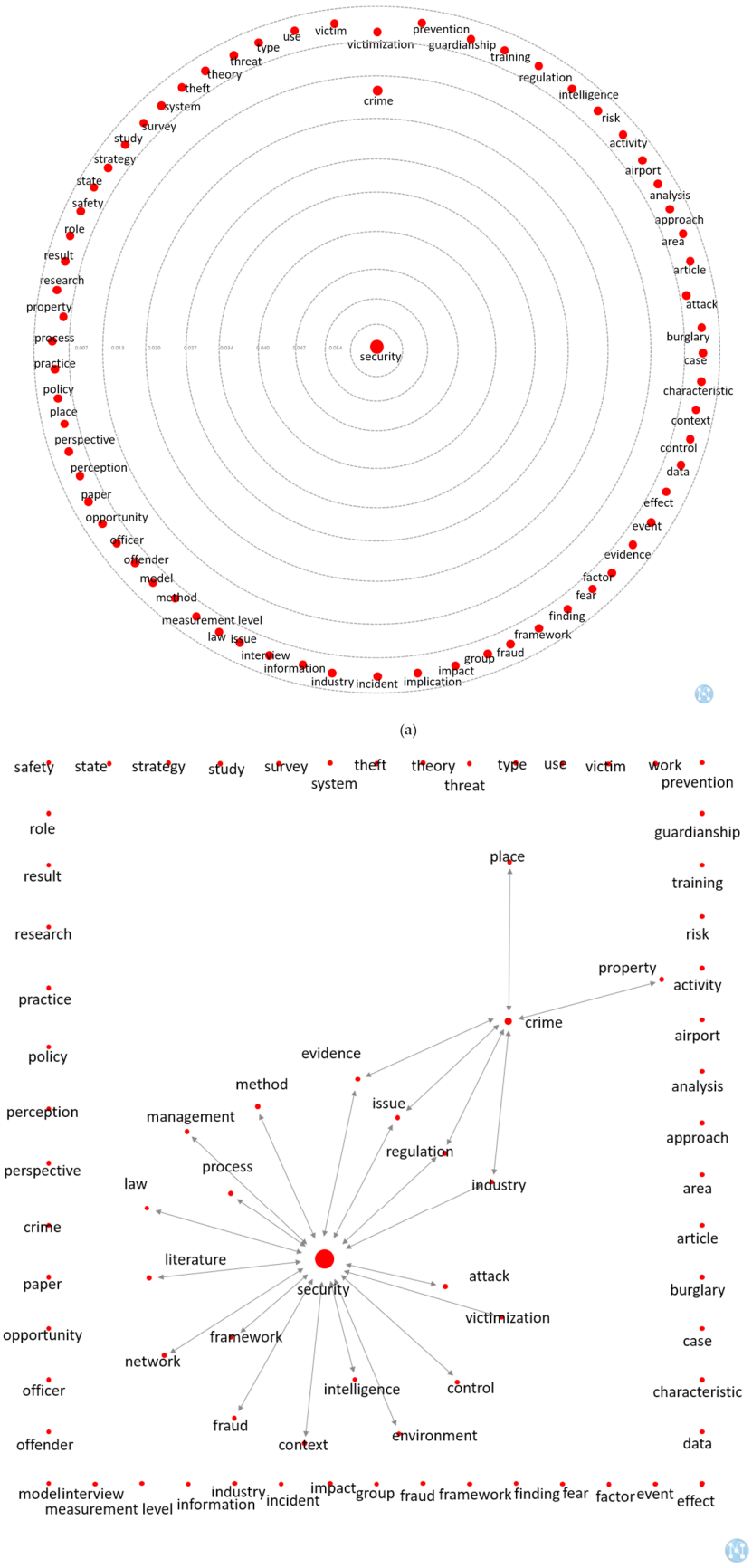


Figure 10. Results of international research. (**a**) Concentric map of the degree of centrality; (**b**) Spring map of the betweenness centrality.

4.3. Comparison of Case Analyses

The most prominent feature in comparing the characteristics among these trends was the different perspectives considering technology leaks. As previously mentioned, far more articles from South Korea satisfied this study's inclusion criteria than those in international journals. The two groups' most frequent keywords also differed. Keywords that commonly appeared in both journals were "law", "regulation" and "management"; this demonstrates the importance of legislation or regulations in ensuring effective and robust industrial security. In South Korea, keywords such as "technology leakage", "trade secrets", "industrial technology" and "industrial security education" were common, which indicates that the consideration of technology leaks originates with the "security" concept itself. This confirms the current status of industrial security in South Korea: the nation considers technology leaks as threats to assets and as threats to national competitiveness that should be addressed through a security system involving technical, administrative and physical security. By contrast, international journals consider technology leaks as crimes, as reflected by the most frequently related keywords in international journals: "crime", "attack", "fraud", "victimization" and "evidence". These words indicate a contrast to the case of South Korea, where industrial security is distinct and regarded as a separate academic field from crime and physical security. The research trends mentioned in this section are summarized in Table 5 below.

Table 5. Comparisons of the characteristics of research trends.

Fields	South Korea	International
Common keywords	Law Regulation Management	
Main keywords	Technology leakage Trade secret Industrial technology Industrial security education	Crime Fraud Victimization Evidence
Perspective (management area)	Security management	Crime

Additionally, multiple security-related disciplines are being investigated in South Korea. Diverse studies have largely incorporated security in the business/economics, legal/regulation, engineering and psychology fields. The meta-analysis results revealed that the business field tends to focus on evaluating levels, management systems and the cultivation of manpower in detail, while engineering focuses on control systems, sign predictions and digital forensics. The primary "industrial security" keywords were manifested in our results as "industrial technology leakage", "trade secrets", "industrial security education" and "management". These not only reflect the importance of the current industrial security aspects but also reveal the existence of studies on the detection of various security incidents, such as technology leaks. Additionally, training manpower as a countermeasure to defend against threats and security attacks can sustain an organization's well-being and thus the nation's sustainable growth.

5. Conclusions

In this rapidly changing world, in which state-of-the-art technology has become an important asset, risks and security threats have become crucial global challenges for organizations. Accordingly, efforts to secure these assets have grown, which has led to a recognition of the importance of industrial security. South Korea's industrial security field has also significantly expanded in recent years; a national university curriculum has been established, and organizations are prioritizing their security. This study examined the current status of industrial security in South Korea as a prominent, emerging industry, and compared it with the global level. The results revealed that a significant amount of academic research on industrial security has been published in South Korea, while the worldwide perspective has focused more on the broader concept of security, including information security. Further, searches

for academic journal articles with the keyword "industrial security" revealed that private security is also a major focus. This made it difficult to find any study that particularly focused on industrial security, which reflects the major gaps between the two groups and the lack of a fundamental concept of industrial security.

This study contributes to the current literature by identifying not only the status of industrial security worldwide but also the issues and trends surrounding industrial security. It aims to raise awareness regarding industrial security's importance in protecting organizations' assets, which are essential for stable management and facilitate long-term sustainable growth. However, this study is limited by the few suitable articles used to provide an analysis from an international perspective. Thus, future researchers should include more articles in their reviews. Moreover, while the terms using the Korean language were translated as accurately as possible into English, all researchers could not agree on the terms used given the language differences that exist. Consequently, future research should outline definitions for specialized terms in Korean to further clarify the context.

Author Contributions: Conceptualization, H.Y. and H.C.; methodology, H.Y. and H.C.; investigation, H.Y.; resources, H.Y.; writing—original draft preparation, H.Y. and H.C.; writing—review and editing, H.Y. and H.C.; visualization, H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

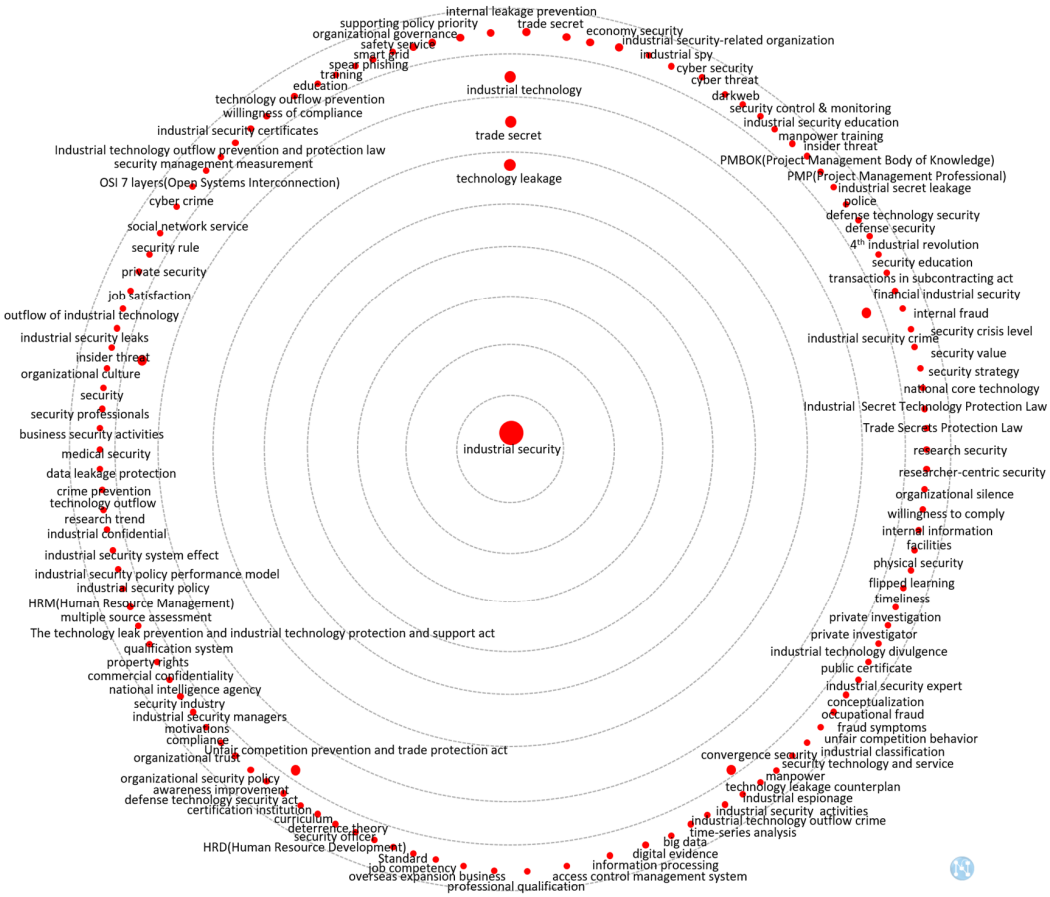


Figure A1. Concentric map of the degrees of centrality.

Figure A2. Spring map of the betweenness centrality.

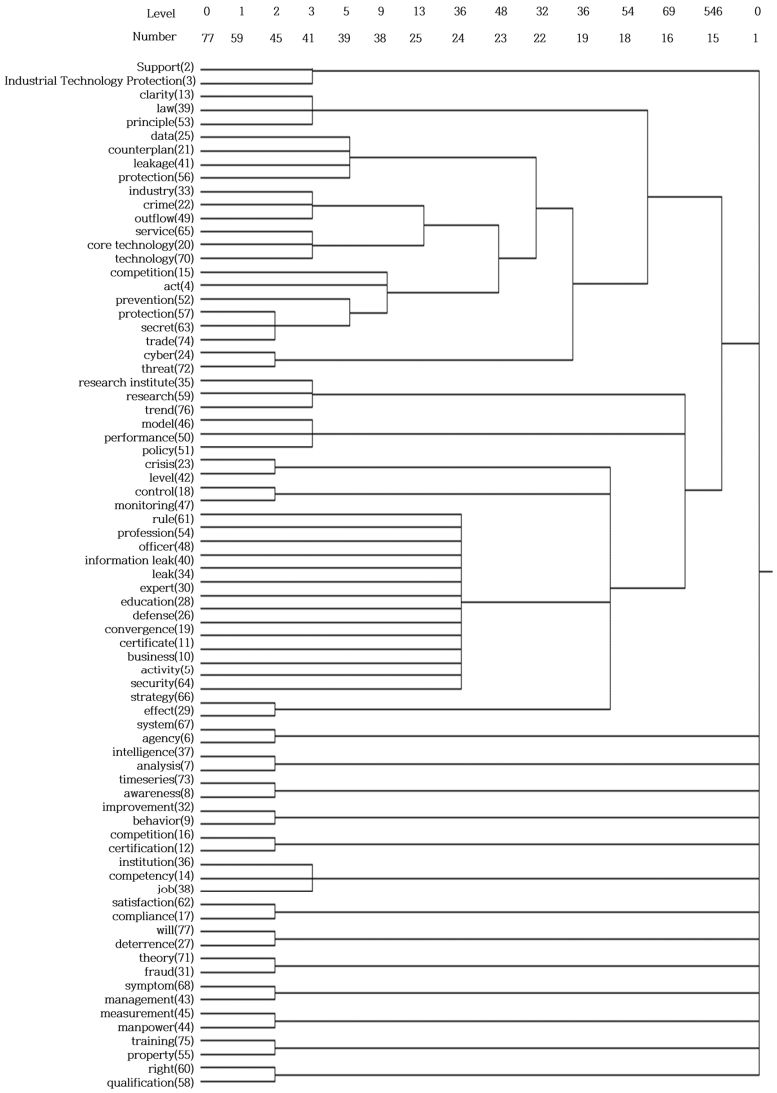


Figure A3. Component dendrogram.

References

1. Park, J.Y.; Huh, E.N. A cost-optimization scheme using security vulnerability measurement for efficient security enhancement. *J. Inf. Process. Syst.* **2020**, *16*, 61–82.
2. Gafurov, K.; Chung, T.M. Comprehensive survey on internet of things, architecture, security aspects, applications, related technologies, economic perspective, and future directions. *J. Inf. Process. Syst.* **2019**, *15*, 797–819.
3. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. In Proceedings of the 7th international Conference on Body Area Networks, Oslo, Norway, 24 September 2012.
4. IT Chosun. Available online: http://it.chosun.com/site/data/html_dir/2019/10/04/2019100401652.html (accessed on 4 October 2019).
5. Chang, H.B. An exploratory study of industrial security studies for science and technologies protection. *J. Adv. Navig. Technol.* **2013**, *17*, 123–131. [CrossRef]
6. Lee, C.M. A critical review of industrial security concepts. *Korean Secur. J.* **2017**, *50*, 285–303.
7. Jeon, M.; Chang, H. The Design Research on ICT Security Concepts and Domains. *Inf. Syst. Rev.* **2019**, *21*, 49–61.
8. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*, 4th ed.; Cengage Learning: Boston, MA, USA, 2014.
9. Hinde, S. The law, cybercrime, risk assessment and cyber protection. *Comput. Secur.* **2003**, *22*, 90–95. [CrossRef]
10. Theoharidu, M.; Kokolakis, S.; Karyda, M.; Kiountouzis, E. The insider threat to information systems and the effectiveness of ISO17799. *Comput. Secur.* **2005**, *24*, 472–484. [CrossRef]
11. Igloo Security. 2016 Security Threat Outlook Report. Available online: http://www.igloosec.co.kr/en/ig/PR%20CENTER_IGLOO\T1\textquoterights%20Press_IGLOO%20Released%20a%20Prediction%20Report%20on%20Security%20Threats%20for%202016?searchItem=ALL&searchWord=IGLOO+Released+a+Prediction+Report+on+Security+Threats+for+2016&bbsCateId=0&gotoPage=1 (accessed on 9 December 2015).
12. Goodall, J.R.; Lutters, W.G.; Komlodi, A. The work of intrusion detection: Rethinking the role of security analysis. In Proceedings of the Americas Conference on Information Systems (AMCIS), New York, NY, USA, 6–8 August 2004.
13. Ramotsoela, D.T.; Hancke, G.P.; Abu-Mahfouz, A.M. Attack detection in water distribution systems using machine learning. *Hum. Cent. Comput. Inf. Sci.* **2019**, *9*, 1–22. [CrossRef]
14. Chang, H.B. A study on the countermeasure by the types through case analysis of industrial secret leakage accident. *J. Converg. Secur.* **2015**, *15*, 39–45.
15. Hovav, A.; Han, J.Y. The impact of security breach announcements on the stock value of companies in South Korea. *Inf. Syst. Rev.* **2013**, *13*, 43–67.
16. Albladi, S.M.; Weir, G.R.S. User characteristics that influence judgement of social engineering attacks in social networks. *Hum. Cent. Comput. Inf. Sci.* **2018**, *8*, 5. [CrossRef]
17. Korea JoongAng Daily. Available online: https://news.joins.com/article/22478252 (accessed on 27 March 2018).
18. Kamruzzaman, M.D. A criminological study on the dark figure of crime as a socio-ecological bulk of victimization. *Am. J. Bus. Econ. Manag.* **2016**, *4*, 35–39.
19. American Banker. Available online: https://www.americanbanker.com/news/hsbc-suffers-data-breach-on-small-number-of-online-accounts (accessed on 6 November 2018).
20. Binger, C.; Kent-Walsh, J.; Ewing, C.; Taylor, S. Teaching educational assistants to facilitate the multisymbol message productions of young students who require augmentative and alternative communication. *Am. J. Speech Lang. Pathol.* **2010**, *19*, 108–120. [CrossRef]
21. Solymossy, D.S. High-Tec, Low-Tech, No-Tech: Communications Strategies during Blackouts. Master's Thesis, Naval Postgraduate School, Monetary, CA, USA, December 2013.
22. The Korea Association for Industrial Security. *Industrial Security White Paper*; The Korea Association for Industrial Security: Seoul, Korea, 2015.
23. Korea Legislation Research Institute, Korea Law Translation Center. *Act on Prevention of Divulgence and Protection of Industrial Technology*; Ministry of Trade, Industry and Energy: Sejong City, Korea, 2017.
24. Korea Legislation Research Institute, Korea Law Translation Center. *Act on Support for Protection of Technologies of Small and Medium Enterprises*; Ministry of SMEs and Startups: Seoul, Korea, 2017.
25. KAITS. Available online: http://www.kaits.or.kr/certificate/introduce.do? (accessed on 15 June 2018).

26. PRISMA. PRISMA Flow Diagram. Available online: http://www.prisma-statement.org/ (accessed on 17 March 2020).
27. Chaffin, R.; Herrmann, D.J. The similarity and diversity of semantic relations. *Mem. Cognit.* **1984**, *12*, 134–141. [CrossRef]
28. Kim, Y.H. Analysis of connection centrality degree of hot terminologies according to the discourses of privatization of health care. *J. Korea Contents Assoc.* **2012**, *12*, 207–214. [CrossRef]
29. Pryke, S.D. Towards a social network theory of project governance. *Constr. Manag. Econ.* **2005**, *23*, 927–939. [CrossRef]
30. Gim, E.; Koo, J. Analysis of Social Network Change Characteristics of Participants in Urban Regeneration Project Using Netminer. *J. Inf. Technol. Serv.* **2020**, *19*, 1–16.
31. Kang, M.S. *A Study on the Alignments Analysis Between Strategy and Budget of the Government R&D's Major Sectors*; Korea Institute of S&T Evaluation and Planning: Chungcheongbuk-do, Korea, 2019.
32. Cyram. *Getting Started with Netminer, 3.3 Version*; Cyram: Seoul, Korea, 2008.
33. Yang, Y.S. Can Social Network of Entrepreneurs be evolved to Strategic Network of Business?—A Case Study on Social Network Analysis of Daeduck High-tech Entrepreneurs. *J. Ind. Econ. Bus.* **2008**, *21*, 1041–1060.
34. Kim, W.J.; Chung, Y.M. A Study on Research Collaboration Among Asian Countries in Science and Technology. *J. Korean Soc. Inf. Manag.* **2010**, *27*, 103–123. [CrossRef]
35. Choi, Y.C. Analyzing Research Trends in the Study of Local Government Administrative and Area. *J. Local Gov. Stud.* **2018**, *30*, 57–79. [CrossRef]
36. Kim, H.S.; Kang, B.R. An analysis of the research topics of the academic papers published in the journal of korean society of archives and records management: From 2001 to 2017. *J. Korean Soc. Arch. Rec. Manag.* **2018**, *18*, 183–204.
37. Kim, Y.H. A Correlation Study of Core Technology Leakage and Security Capability: Centric SMEs Cases. *Korean J. Ind. Secur.* **2014**, *4*, 97–108.
38. Hwang, H.D.; Lee, C.M. A Study on the Relationship between Industrial Espionage, Self-Control, and Organizational Commitment. *Korean Secur. J.* **2016**, *47*, 119–138.
39. Yoo, I.J.; Park, D.H. A Study on Empirical Model for the Prevention and Protection of Technology Leakage through SME Profiling Analysis. *J. Inf. Syst.* **2018**, *27*, 171–191.
40. Lee, H.; Ryu, B.; Kim, H.; Lee, J.; Kim, Y.; Chang, H. A Study for Enhancing Necessity of Certain Industrial Security Charge Department through Investigating Domestic Industrial Security Organization. *J. Soc. e-Bus. Stud.* **2017**, *21*, 121–133. [CrossRef]
41. Gong, B.W. The Situation and Security Measures of Industrial Technology Security Management of SMEs. *J. Korean Soc. Priv. Secur.* **2019**, *18*, 1–26.
42. Jung, S.H.; Lee, C. A Study on the Psychological Security Vulnerabilities of Employees from a Perspective of Industrial Security—Focused on Dual Process Theory. *Korean Secur. J.* **2020**, *63*, 41–57.
43. Lee, C.H.; Lee, S.H. Enhancing industrial security of casino business by developing criminal profiling of deviant behaviors in casino. *Korean Secur. J.* **2016**, *48*, 113–146.
44. Jung, S.H.; Cho, S.P.; Lee, C. Effects of Sexual Violence in the Workplace upon Corporate Performance from a Perspective of Industrial Security. *Korean J. Ind. Secur.* **2019**, *9*, 135–156.
45. Hwang, Y.D.; Park, D.G. Security Requirement and Framework for IP-Based Video Surveillance System. *J. KIIT* **2017**, *15*, 11–20. [CrossRef]
46. Ryu, B.; Jeon, M.; Ji, J.; Lee, C.; Chang, H. Meta Analysis on Digital Forensics Research Trends for Securing its Admissibility of Digital Evidence. *J. Converg. Secur.* **2017**, *17*, 23–32.
47. Kim, J.; Kim, J.; Kim, J.; Choi, Y.; Chang, H. An Exploratory Study for Clustering of Technology Leakage Activities. *J. Converg. Secur.* **2019**, *2*, 3–9.
48. Lee, J.B. A Legal Study on the protection of industrial technology in corporate mergers and acquisitions (M&A). *World Const. Law Rev.* **2014**, *14*, 89–119.
49. Noh, J.; Ko, Z. Legal System Problems and Improvement Plan on Technology leakage of Overseas Expansion Businesses. *J. Law Res.* **2017**, *33*, 277–303. [CrossRef]
50. Kim, K.; Kim, J. The Values and Strategies of Industrial Security in Digital Economy. *Korean J. Ind. Secur.* **2018**, *8*, 61–74.
51. Na, O.; Park, L.W.; Yu, H.; Kim, Y.; Chang, H. The rating model of corporate information for economic security activities. *Secur. J.* **2019**, *32*, 435–456. [CrossRef]

52. Kim, S.H.; Han, I.J. A Study on the Relationship between Corporate Image and Employment Preference in Industrial Security Protection Activities. *Korean J. Ind. Secur.* **2019**, *9*, 87–107. [CrossRef]
53. Lee, S.S. *Network Analysis Methods*; NonHyung: Seoul, Korea, 2012.
54. Lee, S.M.; Rha, J.S. A network text analysis of published papers in service business, 2007–2017: Research trends in the service sector. *Serv. Bus.* **2018**, *12*, 809–831. [CrossRef]
55. Chung, J. The Study of Protective Solution and People in Technology Outflow about SMEs. *Int. Commer. Inf. Rev.* **2015**, *17*, 133–152.
56. Ahn, B.G. Development of the Corporate Participatory Security Culture Framework (CPSCF). Ph.D. Thesis, Chung-Ang University, Seoul, Korea, February 2019.
57. Lee, S.O. A Study on the effective method for the prevention of industrial Secrets Leakage. *CHUNG-ANG Law Rev.* **2019**, *21*, 39–80.
58. Kang, S.H. A Review of the application and scope of the Fair Transactions in Subcontracting Act on technology takeover. *CHUNG-ANG Law Rev.* **2019**, *21*, 441–474.
59. Choi, Y.C.; Choi, O.C.; Kim, H.S. Analysing Key Policy Concepts Underlying Saemaul Undong Policy Within Newspaper Editorials: Application of Network Text Analysis Method. *Korean Comp. Gov. Rev.* **2011**, *15*, 45–70. [CrossRef]