Security Journal (2019) 32:435–456
https://doi.org/10.1057/s41284-019-00171-z

ORIGINAL ARTICLE

The rating model of corporate information for economic security activities

Onechul Na[1] · Lee Won Park[1] · Harang Yu[1] · Yanghoon Kim[2] · Hangbae Chang[3]

Published online: 22 February 2019

Abstract

Industrial technology outflow incidents negatively affect corporations, the industry, and countries. Yet, corporate information security is weak, and there is low awareness of the issue's seriousness. This study developed a rating model that can distinguish "importance" based on an objective standard. Fourteen components that can evaluate the importance of corporate information were derived from the related literature and verified for validity and reliability using factor analysis to organize final rating factors, such as Cost of Information Creation, Level of Information, Information Utilization, Effect of Internal Utilization, and Risk of External Leakage. A secondary survey targeted field experts to set the relative weights between five rating factors and give the relative weights for Effect of Internal Utilization Risk of External Leakage. A corporate information classification system was then designed to grades importance using the five factors. A final rating model of corporate information is suggested by defining security activity by level, granted by grade. This model is designed for corporate use and is expected to benefit economic security activity.

Keywords Industrial technology outflows · Corporate information · Rating model · Economic usefulness · Economical security activity

Overview

There has been an increase in the occurrence of industrial technology outflow incidents. Corporations that have been victims of technology leakages have suffered severe quantitative and qualitative damage (MOTIE 2015). South Korea alone witnesses over 100 outflow incidents of industrial technology occuring per year. Eighty-six percent of these incidents occur in small and medium-sized enterprises (SMEs). The rate of incidents has also increased since 2003—in fact, from 2013 to 2018, authorities registered 637 cases (NISC 2018). Notably,

✉ Hangbae Chang
hbchang@cau.ac.kr

Extended author information available on the last page of the article

outflow incidents occur more frequently in SMEs with relatively weak security than in major businesses (Park 2016).

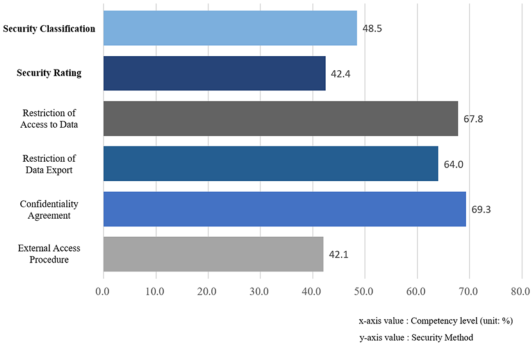
Industrial technology has many definitions; it involves technical information that is needed for development, production, supply, and use of products or services based on Korean law. An industrial technology outflow incident is generally an act of illegally disclosing an industrial technology to external parties (MTIE 2017). In this study, industrial technology is to be limited as an information being produced within a corporation, and consider it as critical information (henceforth “Corporate Information”).

Outflow incidents of corporate information negatively affect corporations, causing direct damage to the corporation, its employees, related industries, and to the country (Jo 2010; KAITS 2015a, b). Hwang and Lee (2016) notes that an outflow incidents of corporate information lowers most employees’ affinity toward the organization within the corporation, while Jeong (2009) states that it is directly connected to national competitiveness, leading to a negative effect on national security. An outflow incident of major information of a primary industry can not only weaken the competitiveness of related industries, but also destroy the business environment itself (Hyung 2005). Despite the severity of industrial technology, the security level of corporations (especially SMEs) is still low, and so is the awareness of this issue (Sungkyunkwan University Cooperation 2016; Lee and Kim 2015). Corporate information is produced continuously; if it is judged to have some value, it must be protected by security technologies (solutions) or security activity (KAITS 2013). However, increasing of security investment which includes increasing of security countermeasures, size of the security department etc. has become a burden for corporations (Kim et al. 2013). Eventually, the fundamental cause of weak security is that the security investment target is rapidly increasing due to the large amount of corporate information.

Effective security activity to protect corporate information in general follows a procedure (Statistics Korea 2017; Han 2006; TTA 2010). First, corporate information should be distinguished by type of corporate information (e.g., research and development [R&D], production, manufacture, human resources, etc.). Second, the grade of corporate information should be calculated. The grade of each item of information should be distinguished as per the objective and valid factors, and classified accordingly. Third, a grade classification system of corporate information should be created based on “importance.” Finally, corporate information should be safely protected using distinctive security countermeasures and the level of grade. According to a survey by the KAITS (2015a, b) effective and efficient security activity has been made difficult owing to the issue of grading the target information. Figure 1 shows the results of survey; it is notable that the activities of “Security Classification” and “Security Rating,” which are done preemptively, are relatively insufficient compared with other security activities.

The fourth industrial revolution has led to a rapid increase in digital data (Tien 2013). After they are processed, data gain value as information, which propels the growth of corporate information (McAfee et al. 2012). Corporations that are unable to proactively catch up with these changes and manage corporate information

Fig. 1 Survey of technology protection security activities in a corporation



with consistency and reliability will increase their consumption of human and physical resources, among others (Ko et al. 2014).

The increase of information also includes unimportant information. Thus, economic and effective return on investment requires efficient security activities to be conducted after autonomously distinguishing the importance of information within the corporation and only focusing on important information (Soonchunhyang University Cooperation 2010; Gordon and Loeb 2002; Moore et al. 2010).

Corporate information management: status quo

The purpose of grading corporate information is to differentiate security activities according to the importance of corporation information after it is evaluated (Jouini et al. 2014; KISA 2009). Most corporations currently use the confidentiality, integrity, and availability (CIA) triad as a standard when evaluating the importance of corporate information (Kang and Kim 2014; MSIT 2013). Confidentiality refers to keeping an information secret; integrity, to keeping information invariable; and availability, to immediately using information irrespective of geographic or time constraints (Von Solms and Van Niekerk 2013). However, a contradiction rises when using confidentiality for evaluating the importance of corporate information because various standards (e.g., integrity or availability) for rating also have identical meanings for judging the degree of confidentiality. In other words, judging the degree of confidentiality can be interpreted as judging the grade of corporate information. Furthermore, evaluating the importance of corporate information only by the CIA triad can be limiting as it does not further consider task status of corporation or business process, and so on (Parker 2012). Thus, in this study, establishing a rating model of corporate information by not only CIA triad, but also by deriving a new standard through analyzing a relevant previous studies is desired to be designed, so that corporate information can be accessible from various perspectives.

Most corporate information can be protected selectively based on the business environment and corporation strategy (Suzuki 2015). A typical protection method can be sorted into two forms: formal and informal appropriation (Zobel et al. 2017). Here, appropriation is an act of using something without permission; in other words, it is a concept of ownership (Strang and Busse 2011). The best example of formal appropriation is a patent. For patents, a corporation allows public access to their own important information and instead, they are empowered with legally monopolistic and exclusive patent for certain periods (Munson 1996). A typical example of informal appropriation is a trade secret. In this case, the strategy is to disallow public access to important corporate information, that is, protect it as a secret (McGurk and Jia 2015). If maintaining this status of secrecy is possible, a permanent monopoly can be sustained; but if an outflow incident occurs, legal compensation becomes impossible (KIPO 2011). If important corporate information is protected under informal appropriation, the respective corporation is left with the full responsibility of that information; this can be considered highly risky. Accordingly, a corporation should effectively select a protection method depending on the characteristics of its corporate information. It must precisely consider importance, and focus more on relatively important information when conducting security activities (Dhillon and Torkzadeh 2006).

A rating model of corporate information

Research methodology

The research methodology that was used in this study to design a rating model of corporate information is as Fig. 2.

First of all, study was conducted on characteristics of rating model of corporate information that were mainly used and analyzed a problem. As mentioned in section "Corporate information management: status quo", the CIA triad is primarily used to design a rating model of corporate information. However, the ambiguity of standards and absence of variety were noted as a problem. To address these

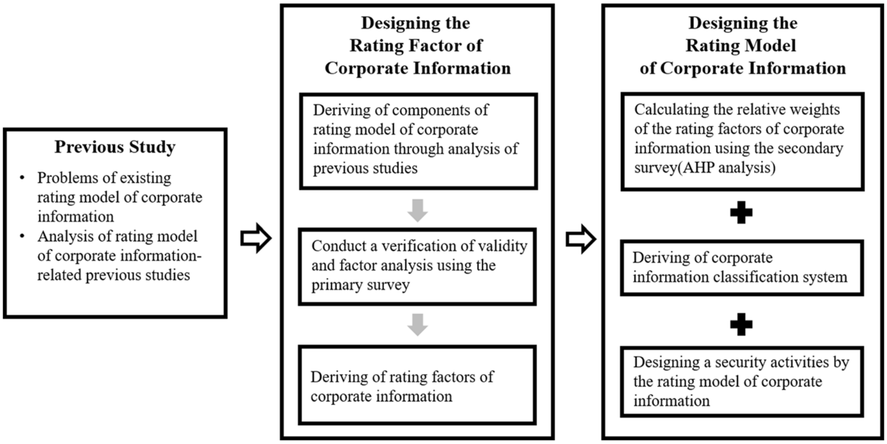

Previous Study
• Problems of existing rating model of corporate information
• Analysis of rating model of corporate information-related previous studies
Designing the Rating Factor of Corporate Information
Deriving of components of rating model of corporate information through analysis of previous studies
Conduct a verification of validity and factor analysis using the primary survey
Deriving of rating factors of corporate information
Designing the Rating Model of Corporate Information
Calculating the relative weights of the rating factors of corporate information using the secondary survey(AHP analysis)
Deriving of corporate information classification system
Designing a security activities by the rating model of corporate information

Fig. 2 Research methodology

problems, relevant previous studies are analyzed and the various perspectives of components of rating model are outlined.

A statistical verification procedure was conducted to derive components that would be used as a standard for the rating model of corporate information. First, a primary survey was done to distinguish the appropriateness of components; this uses a five-point Likert scale. Then, reliability is to be verified by combining components using factor analysis. These steps allow us to develop the final rating model.

To design a usable rating model, prioritizing a derived factor by analyzing relative weights is done first, classifying the corporate information classification system and designing differentiated security activities according to the grade is conducted. Then, a secondary survey is conducted to distinguish relative weights. This survey uses pairwise comparison, and AHP analysis is used to derive results. Then, based on relevant previous studies, corporate information classification system is categorized, place differentiated security countermeasures by the grade and design a final rating model of corporate information.

Components derivation of rating model of corporate information: analysis of previous studies

To derive new factors for the rating model of corporate information, a solution for the problems which were mentioned in section "Research methodology" was considered. The need for deciding on a components of rating model in various perspectives came first. Accordingly, multi-dimensional perspective of factors of rating model was to be set by analyzing a previous studies that are relevant to various types of information (personal information, information assets, information system, information resource, intellectual property right, patent, etc.) which falls under corporate information. In addition, there is a need to derive (or identify?) not only corporate information itself, but also its components by considering the life cycle of corporate information and the business flow. A number of efforts form the (input) to settle the level of quality, availability, convenience, and so on, which form the (output). This corporate information is then used at various levels, standards(use) and finally, internally and externally for business(outcome) or comes to a natural end of lifespan(destruction by needs) (Bernard 2007; Tipton and Nozaki 2007). In this study, qualitative comparative analysis research using numerical method was conducted by coding components which were derived from various rating-related previous studies based on corporate information life cycle.

Recently, Park et al. (2015) conducted similar rating of personal information using diverse factors, such as value of assets, sensitivity, importance, and identification. The author measured the use of personal information (use) and risk of abuse of this information (outcome) as components of rating model.

In MEST (2011), information assets' value rating was conducted by using qualitative and quantitative methods; the impact of the outflow incident of information assets (outcome) and accessibility in the perspective of information assets (output) was measured as components of rating model.

Despite the fact that each institution under the government falls under different regulations, manpower, organizational conditions and so on, of information security, MOI (2016) tried to prevent excess management expenses by systematically incorporating security activities and levels of information security to the institutions' information. This study desired to select an information security grade of institutions' information by considering the characteristics of the information system (range of service impact, information processing, related system, security of task continuity and amount of retaining information) and the characteristics of the institution (credibility). A degree of information usage of information system (use) and internal–external influential level on utilization of information system (outcome) were mainly measured as a components of rating model.

MOPAS (2013) composed a measurement view for deciding the grade of information resource with the characteristics of task priority, resource, and maintenance. Task priority measures the importance of the information system- or service-related task that is supported by information resource; and characteristics of resource measures the unique feature of information resource and complexity of formation. The characteristics of maintenance measure a level of difficulty for maintenance such as using range of information system(service) which is operated through information resource, method of organization, etc. In this study, the importance of the information resource (output), the preservation period and the degree of utilization (use) as the components of rating model.

Albert (1997) created institutions' technology evaluation process using technology information, organizing a technology evaluation team, and followed by primary investigation, data collection, detailed assessment, and reporting on evaluation results. The grades were from 0 to 10 according to the rating factors for each technology. In this study, cost of information creation (input), the level of derived technology and the degree of quality (output) and components of effects created by the use of technology (outcome) were measured as the components of rating model.

Park and Shin (2010) rated their scores as (+), (−), (0), and so on for the characteristics of each technology. They calculated the final grade as Low, Medium, and High. In this study, usefulness (use), availability of substitute technology and development maintainability (outcome), novelty and differentiation of technology (output) were mainly measured as the components of rating model.

Yoon et al. (2004) calculated the result of the grade from A to D by aggregating the score per evaluation subject for each technology. In this study, novelty and availability of realization (output) and marketability (outcome) were mainly measured as the components of rating model.

In a study reported by JPO (2017), the score of intellectual property rights are composed of filling in the scores of evaluation subjects. The evaluation subjects are classified into fundamental measure, inherent assessment of rights, evaluation for relocation of negotiability, and business assessment. In this study, completeness (output), business continuity and development continuity (outcome) were mainly measured as components of rating model.

KIPA-A (2013a) has developed a guide for evaluating the value of intellectual property rights. In this study, for the value evaluation of intellectual property

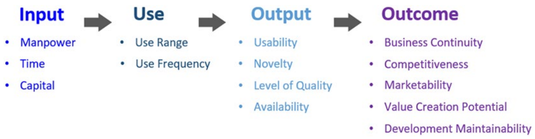


Fig. 3 Application of components of rating model based on the corporate information lifecycle

rights, technical value (output), and market value (outcome) were mainly measured as components of rating model.

KIPA-B (2013b) granted patent information a grade by scoring the evaluation of the degree of the rights, of technology, of utilization, dividing them into nine grades with AA being the highest and C being the lowest. In this study, safety (output), use range (use), and availability of commercialization (outcome) were mainly measured as a components of rating model.

The results of previous study on rating model of corporate information is applied to the lifecycle of corporate information as shown in Fig. 3, the components of rating model for the "inputs" (added to create corporate information) are manpower (labor force), time, capital (funds, expense), and so on. For "output", which is the internal and external level of corporate information that were available, ease of use, integrity, accurateness, inter-compatibility, and novelty (the degree of innovation). For the components of "use", which is a corporate information's level of utilization, there were use frequency (frequency of practical use), and use range (utilization range). Lastly, the components of rating model for "outcome" (the positive or negative effects of internal and external use are value creation potential, competitiveness, marketability, loss potential, business continuity, potential of competition and development maintainability.

Finally, based on an analysis of previous study, the components of the rating model (14) are derived and the operational definition is established (Bang 2014; Chung et al. 2004a, b; Lee 1992; Sung et al. 2016; Timothy 2016) (see Table 1). Since there are a number of aspects to consider when judging the relative value between each component at the present stage, a survey is conducted to judge whether components are valid as a standard for the rating model. Then, using factor analysis, 14 components are grouped into fewer factors, and the relative weights are then determined using AHP.

Proof analysis of the rating model of corporate information

Questionnaires are used to verify the validity of the derived components. The authors participated in both international and domestic conferences/symposiums and conducted primary survey, confirming whether survey respondents have a certain level of experience in the field of security. The number of corporations surveyed (51) is the same as the number of respondents (51). Details of corresponding survey is same with Fig. 4. The average period of the respondents' career in the security field is 17 years. Most of their positions were organizations' chief security officer (chief information security officer, as well as chief risk officer, 51%) or chief information officer, security business included (37%).

Table 1 Operational definition of components for the rating model of corporate information

Components	Definition
1. Manpower	Manpower (labor force) required to create and preserve corporate information
2. Time	The amount of time it takes to create and maintain corporate information
3. Capital	Capital (funds, costs) required to create and preserve (maintain) corporate information
4. Availability	The degree to which the corporate information can be accessed at anytime, anywhere, and on time
5. Usability	The degree to which the calculated corporate information can be easily used (convenience)
6. Level of Quality	The nature and performance inherent in the resulting corporate information (integrity, accuracy, and interoperability)
7. Novelty	New (differentiated) degree compared with other corporate information of calculated corporate information (degree of innovation, scarcity)
8. Use frequency	Usage to use with corporate information (degree of use)
9. Use range	Scope to use with corporate information (number of business information use departments, and depth of use)
10. Value creation Potential	The degree to which corporate information can stand out in competition with other corporations (competitive advantage)
11. Marketability	The degree to which corporate information can generate revenue in the marketplace (market growth potential)
12. Development maintainability	The degree to which corporate information is preserved or developed continuously (technical sustainability)
13. Business continuity	The possibility of continuing business activities when corporate information is leaked (recovery time)
14. Competitiveness	The degree to which competitive behavior of other corporations can appear when corporate information is leaked

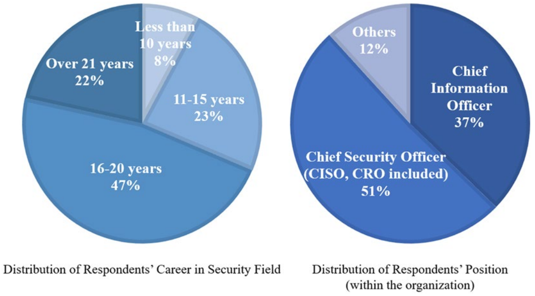


Fig. 4 Information of survey respondents for the rating model of corporate information

The topic of the survey was renamed to "Goodness-of-fit survey for rating factors of corporate information," and information was collected from various respondents (name of corporation, position, name, business in charge, contacts, e-mail, etc.). The survey aimed to investigate the degree of goodness-of-fit for the 14 components of

Table 2 Result of validation of component validity

Components	Validity
1. Manpower	3.65
2. Time	3.58
3. Capital	3.60
4. Availability	3.90
5. Usability	3.81
6. Level of quality	3.83
7. Novelty	3.96
8. Use frequency	3.54
9. Use range	3.51
10. Value creation potential	4.25
11. Marketability	4.31
12. Development maintainability	4.21
13. Business continuity	4.10
14. Competitiveness	4.04

rating model that were derived from relevant previous studies and composed a questions based on operational definition as derived above (see Table 1). The responses included five answers: Strongly Disagree, Disagree, Neutral, Agree, and Strongly Agree. Although the number of samples was low, the selected targets of this survey have high quality, that is, have the required qualifications for verifying the reliability of the measurement (Jeon and Park 2016). To collect the surveys smoothly, online surveys were used, and conducted offline surveys in parallel. The results of the measurement show that the validity of each component has a score of more than 3.5 points (out of 5 points) (see Table 2). Thus, it can be applied as a standard of the rating model of corporate information (Kim and Lee 2012; Hong et al. 2008; Noh 2017).

Second, an exploratory factor analysis was conducted to understand the correlation between components (Costello and Osborne 2005). The factor analysis showed the general direction of reliability, convergence validity, and discriminant validity of each factor in measuring theoretical variables. Reliability refers to the degree of consistent measurement of the outcome (Kang and Yoo 2009). Convergence validity is the correlation between each measurement tool and the theoretically assumed construction concept. Judgment feasibility is the judgment of how weakly each measurement item is related to other construction and theoretically related concepts (Kang 2013).

The factor analysis of this study used principal component analysis as a factor extraction method and the varimax rotation method, which is a right angle rotation method that simplifies the rotation method and seeks a clear interpretation between the factors (Chun and Oh 2009). The factors are categorized as Table 3: Factor 1 is the cost of information creation, Factor 2 is the level of information, Factor 3 is information utilization, Factor 4 is the effect of internal utilization, and Factor 5 is risk of external leakage.

Table 3 Results of exploratory factor analysis

Derived factor	Components	Factor					Reliability (Cronbach α)	Factor validity
		1	2	3	4	5		
Cost of information creation	Manpower	0.837	–	–	–	–	0.899	3.61
	Time	0.907	–	–	–	–		
	Capital	0.891	–	–	–	–		
Level of information	Availability	–	0.903	–	–	–	0.912	3.88
	Usability	–	0.825	–	–	–		
	Level of quality	–	0.880	–	–	–		
	Novelty	–	0.822	–	–	–		
Information utilization	Use frequency	–	–	0.892	–	–	0.907	3.50
	Use range	–	–	0.946	–	–		
Effect of internal utilization	Value creation potential	–	–	–	0.890	–	0.894	4.26
	Marketability	–	–	–	0.934	–		
	Development maintainability	–	–	–	0.874	–		
Risk of external leakage	Business continuity	–	–	–	–	0.941	0.903	4.07
	Competitiveness	–	–	–	–	0.938		

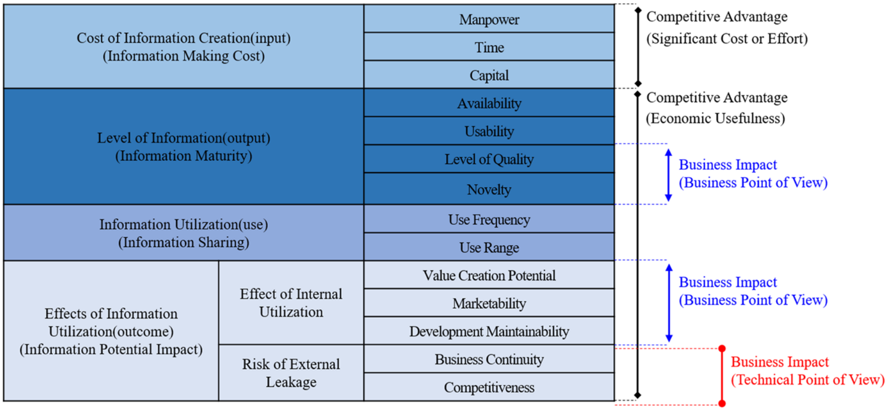
The reliability of the multi-item scale is analyzed using the Cronbach α coefficient—the most commonly used to test reliability (consistent measure of the same concept) by providing a more conservative value than other estimators (Carmines and Zeller 1979). The analysis shows that the reliability of the factors satisfies the criterion of 0.7 or more as preferred by Nunnall (Kim 1999). Thus, the convergence validity and the validity of discrimination among the factors are confirmed. The validity values of the five factors are found to be suitable for the average value of 3.5 or more.

The results of the exploratory factor analysis are linked to the determinants derived from previous studies. The concepts of "economic usefulness" and "business impact" are applied. Economic usefulness is one of the three requirements of trade secrets under domestic law. The concept of economic usefulness means that competitors can gain a competitive advantage or that significant cost or effort is required for the acquisition or development of the information (Yoon 2014). Competitive advantage refers to the value (output, use, and outcome) of the corporate information that is calculated, while significant cost or effort refers to the input before the corporate information is calculated (Devaraj et al. 2007). Prahalad and Hamel (2006) examined business impact from two perspectives: business and technical. From a technical point of view, business impact refers to business continuity planning, and it can be said that maintenance priority and service continuity are preserved in detail when a security incident occurs. This is the outcome of outflow in the rating model of corporate information in this study. From a business point of view, business impact refers to the need for differentiated (new, innovative) competencies and scalable (interoperable) and value-generating skills to have a competitive edge over other corporations. This corresponds to the output of information and the outcome of internal use, which is calculated from the rating model of corporate information of this study.

Thus far, the validity of the components of the model, the factor analysis of the model design, the convergence validity of the factor analysis, the validity of the discriminant validity, and the reliability verification have been examined. From this, the final rating model of corporate information is derived. This model is shown in the Fig. 5, and this model is linked with academic research theories.

Relative importance analysis for rating factors

To carry out the scoring process, it is necessary to calculate the relative weights of each factor. When assuming that certain corporation has used the five factors of the rating model of corporate information in this study to evaluate (rate) the importance of information "A," there is a necessity to raise doubt on whether evaluating the five factors in the same ratio can be a rational evaluating method (Saaty 2008). Thus, the relative weights of five factors were derived through AHP analysis to recognize the ratio of importance of each components. AHP is a tool for estimating weights; it provides a solid basis for expert decision-making. The AHP calculation model herein is a method to reach final decision-making by analyzing and resolving the entire decision-making process (Kim 2012). By establishing an evaluation method



Cost of Information Creation(input) (Information Making Cost)		Manpower
		Time
		Capital
Level of Information(output) (Information Maturity)		Availability
		Usability
		Level of Quality
		Novelty
Information Utilization(use) (Information Sharing)		Use Frequency
		Use Range
Effects of Information Utilization(outcome) (Information Potential Impact)	Effect of Internal Utilization	Value Creation Potential
		Marketability
		Development Maintainability
	Risk of External Leakage	Business Continuity
		Competitiveness

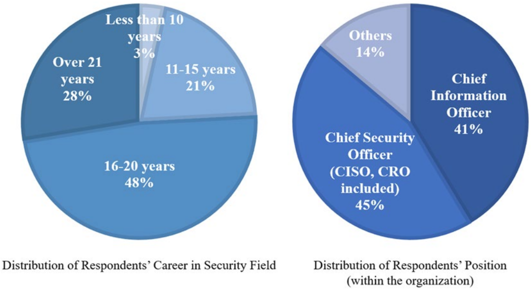
Fig. 5 Rating model of corporate information

for rating model or corporate information in detail, it can lead to a suggestion of model with high credibility (Yahya and Kingsman 1999; Bodin et al. 2005).

To estimate the relative weights of the five factors that compose a rating model of corporate information, a pairwise comparison survey was done for the five factors of 29 experts in the field of security, apart from the previous survey respondents for designing a rating model. Detailed content of corresponding survey is shown in Fig. 6. The number of corporations surveyed (29) is the same as the number of respondents (29). The average period of respondents' career in the security field is 19 years. Their positions are mostly as organizations' chief security officer (chief information security officer, as well as chief risk officer, 41%) or chief information officer, security business included (45%).

A 10-point scale is used for scoring, with calculations based on the consistency index. This index is an indicator of how much consistency a comparator has responded to. For example, if the consistency index is less than 0.1, the respondents' answers are considered reliable (Alonso and Lamata 2006). The topic of survey was named "Survey on Relative Weights of Rating Model of Corporate Information," and the questions were answered in the form of pairwise comparison between five components.

Fig. 6 Information of the survey respondents for the analytic hierarchy process



Distribution of Respondents' Career in Security Field

Distribution of Respondents' Position (within the organization)

Table 4 Relative weights on the rating model of corporate information

Factors		Relative priority (weight) (%)
Cost of information creation		9.7
Level of information		13.4
Information utilization		11.5
Effects of information utilization	Effect of internal utilization	36.1
	Risk of external leakage	29.2
Total		100

The AHP results are shown in Table 4, and the consistency index is 0.0026, indicating high reliability. The results are as follows: 36.1% of internal use and 29.2% of the risk from external leakage are responsible for more than half of the cases; information creation and maintenance costs are 9.7%; the calculated information level is 13.4%; and the information utilization rate is 11.5%.

Designing the economic security activity using a rating model

The basic security management procedures for protecting corporate information are conducted in four steps (Karabacak and Sogukpinar 2005; Lee 2004; Stoneburner et al. 2002). The first step involves identifying corporate information, such as technical information (e.g., research and development information or production and manufacturing information), and management information (e.g., personnel affairs information, accounting financial information, and purchase sales information). The second step calculates the corporate information classification system, which is the rating model derived from this study. The third step is the classification of corporate information. The fourth step is to prepare and implement a security management strategy by the rating model of corporate information. These four-stepped security procedures can be considered the ultimate resolution for effectively protecting corporate information.

Previous studies on rating model of existing information typically classified information into three or four grades (NSW Government 2015; Perkins 2012; Malcolm 2001). In the three-level classification, information was classified as follows: (1) general information (public information, non-confidential information, and general information) that can be disclosed; (2) confidential information used in the corporation (confidential and internal information for internal use only); and (3) only a small number of information that can be accessed (confidential information). A fourth classification includes extra information (e.g., Coca-Cola recipe) that a corporation would consider more important than confidential information; it ultimately controls its durability. In this study, the rating model is set to three grades, and the form is to add critical information as needed (see Table 5).

The basic security management measures to protect corporate information comprise three main areas (Peltier 2016; Soomro et al. 2016; Kim 2016; Noh and Lim

Table 5 Corporate information classification system

Component	Classification			
	Critical information (special grade)	Confidential information (first grade)	Internal information (second grade)	Public information (third grade)
Explanation	Information that is only exposed to very few people in the corporation (Component data and manufacturing technology of core technology of corporation, etc.)	(1) Information that may violate customer's privacy and laws (2) Integrity, confidentiality, and limited availability for corporation existence should be maintained at the highest level (3) Access to information is very limited, and information outflow can pose a very serious risk to the corporation	(1) Information for business activities and operations should be managed by internal approvals (2) Unauthorized access may result in financial loss to the corporation, and can be a significant detriment to operational efficiency and customer confidence	(1) Information that does not affect corporation when the information is disclosed (2) Loss of availability due to system downtime is considered an acceptable risk and is accessible to everyone

Table 6 Security activity design by corporate information classification system

Division		Critical information	Confidential information	Internal information	Public information
Institutional Management	Classification of general information and corporate information	Corporate Information			General Information
	Indicate that it is corporate information for anyone to know	"Critical" Indication	"Confidential" Indication	"Internal" Indication	–
	Establish and enforce security-related regulations	Designate dedicated personnel for security management of the information irrespective of the rating of corporate information			
	Establish and enforce security-related regulations	Establish and enforce security-related regulations regarding the information irrespective of rating of corporate information (production ~ utilize ~ discard)			
Human Resources Management	Obligations to protect corporate information for those with accessibility	Imposition of protection obligation under the handling of applicable corporate information			–
	Conduct periodic security training	Conduct a periodic security training to personnel (board of directors, manager, employees, etc.) related to information regardless of rating of corporate information			
	Notice corporate information and protection obligation	Periodic (once a month)	Annually	Upon joining or leaving a corporation	–

Table 6 (continued)

Division		Critical information	Confidential information	Internal information	Public information
Physical Management	Designate and manage separate corporate information development and storage locations	Access control system and security system construction and operation			–
		Designation and management of development and storage sites	–		
	Designate and manage separate corporate information development and storage locations	Some executives	Some administrators	Corporate staff	–
	Gain evidence of corporate information management against disputes	Always	Periodic (once a month)	When to change	–

2017). First, identification of corporate information, rating, indicating, designation of dedicated personnel for security management, and arrangement and implementation of security-related regulations, among others, are included as institutional management (Chung et al. 2004a, b). Next, physical management includes the designation and management of storage of corporate information, granting access control, arranging a solution for access control, and management evidence secure, among others (Cha 2008). Third, human resources management involves the implementation of the protection obligation, such as confidentiality oath or agreement, the obligation to protect the classified corporate information, and security education (Safa et al. 2016).

In this study, differentiated security activities were designed according to the new grade level as shown in Table 6. This design reflects the above security management procedures and measures of security management.

A corresponding study establishes the rating model of corporate information to support corporations' economic security activities. The objective rating factors that grade ratings according to the importance of the corporate information are suggested, calculated the relative weights per factors, and suggested a guide for security activities in the perspective of cost-effective institutional management, HR, and physical management to be available. For instance, if security activities in the perspective of institutional management are conducted according to the grade, the policy conversion for the protection of corporate information becomes easier. This, in turn, could reduce the role of security administrators, and allow corporations to conduct economic security activities.

Conclusion and future research

In South Korea, occurrences of industrial technology outflow incidents have reached critical levels. Nevertheless, distinction and the rating of information that currently inform the actions of security activities are insufficient and corporations' awareness of such incidents is still incomplete. Thus, in this study, objective factors for = rating were suggested, designed and verified a rating model of corporate information, which also includes a grade classification system of corporate information and security activities by the grade.

This study has pointed out a limitation of CIA triad of information security which is actively used as a rating factors of corporation information and desired to establish a model that can complement (considering working status and business flow) the CIA triad by addressing its limitation. Above all, 14 rating components of corporate information (Manpower, Time, Capital, Availability, Usability, Level of Quality, Novelty, Use Frequency, Use Range, Value Creation Potential, Marketability, Development Maintainability, Business Continuity and Competitiveness) were derived by analyzing ten previous studies that are related to ratings of corporate information. Using primary survey, validity of components was verified, and derived five factors (Cost of Information Creation, Level of Information, Information Utilization, Effects of Internal Utilization and Risk of External Leakage) through exploratory factor analysis; these were the final factors for ratings of corporate information. Moreover, reliability analysis was done using a Cronbach's alpha to verify if measured values of survey responses which were done to derive 14 components and 5 factors are reliable. Lastly, AHP was done through a secondary survey to calculate the relative weights of the five factors, with the results showing importance priority of 36.1% for effect of internal utilization, 29.2% for risk of external leakage, 13.4% for level of information, 11.5% for information utilization, and 9.7% for cost of information creation and maintenance. Subsequently, a corporate information classification system was designed, came up with the strategy of security activity based on the grade and designed economic rating model of corporate information. This research results have established a differential rating model that can proactively correspond with corporate information outflow incidents and is expected to enable an effective security management within the corporation by suggesting a multi-dimensional strategy of security activities.

The model derived in this study does have a structurally basic side that allows indiscriminate application to each corporation, and has a possibility of being inconsistent with practical business. To complement this for the future, establishment of further composite and integrative corporate rating model of corporate information which can be appropriately practicable in various business environment will be needed. As far as the model suggested in this study, is designed and verified the validity by aggregating relevant previous studies, opinions from experts, academic theories, and have not gone through the process of applying to reality. Thus, in the future research, verifying the process for the fulfillment of economic security activities should be conducted by directly applying a suggested model to corporations. Finally, this study desires to establish a safe and economic corporate information rating system by applying an integrity-protectable blockchain service technology.

Acknowledgements This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2018-0-01799) supervised by the IITP(Institute for Information & communications Technology Promotion).

References

Albert, S.R. 1997. NTTC TOP index: A technology assessment and management tool. National Technology Transfer Center at Wheeling Jesuit University.

Alonso, J.A., and M.T. Lamata. 2006. Consistency in the analytic hierarchy process: A new approach. *International Journal of Uncertainty Fuzziness and Knowledge-Based Systems* 14 (04): 445–459.

Bang, K. 2014. A study of information security maturity measurement methodology for banking system based on cyber-based transaction processing architecture diagnosis. *Journal of Digital Contents Society* 15 (1): 121–128.

Bernard, R. 2007. Information lifecycle security risk assessment: A tool for closing security gaps. *Computers & Security* 26 (1): 26–30.

Bodin, L.D., L.A. Gordon, and M.P. Loeb. 2005. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM* 48 (2): 78–83.

Carmines, E.G., and R.A. Zeller. 1979. *Reliability and validity assessment*, vol. 17. Thousand Oaks: Sage Publications.

Cha, I.H. 2008. A study on the development of personnel security management for protection against insider threat. *The Journal of The Korea Institute of Electronic Communication Sciences* 3 (4): 210–220.

Chung, H., J. Kim, and C. Lim. 2004a. A study on the development of an integrated evaluation system for levels of information protection for diagnosing levels of information security and maturity of enterprises. *Korea Institute of Information Security & Cryptology* 14 (4): 37–44.

Chung, H., J. Kim, and C. Lemm. 2004b. A study on the development of integrated evaluation system of information security level for diagnosing the level of information protection and maturity of enterprises. *Journal of the Korea Institute of Information Security and Cryptology* 14 (4): 37–44.

Chun, Y.T., and J.I. Oh. 2009. The relationship between the stage of exercise behavior change and physical self-concept and self-efficacy of casino security employees. *Korean Security Science Review* 21: 95–120.

Costello, A.B., and J.W. Osborne. 2005. Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research & Evaluation* 10 (7): 1–9.

Devaraj, S., L. Krajewski, and J.C. Wei. 2007. Impact of eBusiness technologies on operational performance: the role of production information integration in the supply chain. *Journal of Operations Management* 25 (6): 1199–1216.

Dhillon, G., and G. Torkzadeh. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal* 16 (3): 293–314.

Gordon, L.A., and M.P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* 5 (4): 438–457.

Han, J. 2006. *Prior knowledge for effective 'information protection consulting'*. AhnLab: Cyber Security Column.

Hong, Y., K.J. Hwang, M.J. Kim, and C.G. Park. 2008. Balanced scorecard for performance measurement of a nursing organization in a Korean Hospital. *Journal of Korean Academy of Nursing* 38 (1): 45–54.

Hwang, H., and C. Lee. 2016. A study on the relationship between industrial espionage, self-control, and organizational commitment. *Korean Security Science Review* 47: 119–137.

Hyung, M. 2005. Four strategies to prevent key technology outflows. *LG Business Insight* 1 (12): 21–25.

Japan Institute for Promoting Invention and Innovation. 2017. On the valuation of intellectual property. JPO(Japan Patent Office).

Jeong, B. 2009. A study for preventing industrial technology leakage in enterprise. *Korean Journal of Industry Security* 1 (1): 1–19.

Jeon, J., and J. Park. 2016. To increase effectiveness new change in member survey. LG Economic Research Institute Report, 1–10.

Jo, G.H. 2010. Causes and countermeasures of high technology leakage crime. *Intellectual Property* 21.

Jouini, M., L.B.A. Rabai, and A.B. Aissa. 2014. Classification of security threats in information systems. *Procedia Computer Science* 32: 489–496.

KAITS (Korea Association Industry Technology Security). 2013. *Investments in technology protection by corporations and countermeasures according to risk level*. Korea: KAITS (Korea Association Industry Technology Security).

KAITS (Korea Association Industry Technology Security). 2015a. *Investigation of technology protection competency of enterprise*. Korea: KAITS (Korea Association Industry Technology Security).

KAITS (Korea Association Industry Technology Security). 2015. Smart workplace for enhancing competitiveness and security of SMEs. Industrial Technology Protection ISSUE PAPER.

Kang, B.I., and S.J. Kim. 2014. Study on security grade classification of financial company documents. *Journal of the Korea Institute of Information Security & Cryptology* 24 (6): 1319–1328.

Kang, D.S., and S.H. Yoo. 2009. Assessing the construct validity of PMIS effectiveness measurement—focusing the administration DB construction projects. *Information Processing Society Journal* 16 (3): 417–422.

Kang, H. 2013. A guide on the use of factor analysis in the assessment of construct validity. *Journal of Korean Academy of Nursing* 43 (5): 587–594.

Karabacak, B., and I. Sogukpinar. 2005. ISRAM: Information security risk analysis method. *Computers & Security* 24 (2): 147–159.

Kim, H. 1999. A study on the quantification of information security level. *Asia Pacific Journal of Information Systems* 9 (4): 181–201.

Kim, H., K. Ko, and J. Lee. 2013. Status of corporate information protection system according to amendment of information and communication network act and comparison of certification standard of information protection management system. *Korea Institute of Information Security And Cryptology* 23 (4): 53–58.

Kim, M. 2016. A study on a model of convergence security compliance management for business security. *Journal of Information and Security* 16 (5): 81–86.

Kim, S.K., and S.J. Lee. 2012. Development of evaluation criteria and key indicators of research competence in university professors. *Korean Journal of Educational Administration* 30 (2): 233–252.

Kim, Y. et al. 2012. An analysis of the relative importance of patent valuation: Focused on high technology industry. *Report for the POSRI Business and Economic Review* 12(2).

KIPA (Korea Invention Promotion Association). 2013a. *Intellectual property valuation practical guide for intellectual property rights collateral*. Korea: KIPO (Korea Intellectual Property Office).

KIPA (Korea Invention Promotion Association). 2013b. *Patent analysis and evaluation system SMART (system to measure, analyze and rate patent technology)3*. Korea: KIPA (Korea Invention Promotion Association).

KIPO (Korea Intellectual Property Office). 2011. *Trade secret management practices and protection system studies for the prevention of corporation's skills drain*. Korea: KIPO (Korea Intellectual Property Office).

KISA (Korea Internet & Security Agency). 2009. *A guide to conducting a corporate privacy impact assessment*. Korea: MOIS (Ministry of the Interior and Safety).

Ko, B.K., J.S. Park, S.J. Chung, and G.H. Cho. 2014. A design of integrated security policies for enabling adaptive security in campus environment. *Journal of the Korea Institute of Information and Communication Engineering* 18 (3): 617–624.

Lee, C., and Y. Kim. 2015. An analysis of relationship between industry security education and capability: Case centric on insider leakage. *The Journal of Society for e-Business Studies* 20 (2): 27–36.

Lee, G. 1992. An evaluative framework for business information systems. *Asia Pacific Journal of Information Systems* 2 (1): 17–33.

Lee, M. 2004. A risk analysis methodology for information systems security management. *The Institute of Electronics Engineers of Korea—Computer and Information* 41 (6): 13–22.

Malcolm, E. et al. 2001. Development of information classification standard. Scalable Software Inc.

McAfee, A., E. Brynjolfsson, T.H. Davenport, D.J. Patil, and D. Barton. 2012. Big data: The management revolution. *Harvard Business Review* 90 (10): 60–68.

McGurk, M.R., and W.L. Jia. 2015. Intersection of patents and trade secrets. *Hastings Science and Technology Law Journal* 7 (2): 189–215.

MEST (Ministry of Education, Science and Technology). 2011. *Information security best practices guide*. Korea: MEST (Ministry of Education, Science and Technology).

Ministry of Trade, Industry and Energy. 2017. Act on Prevention of Divulgence and Protection of Industrial Technology.

MOI (Ministry of the Interior). 2016. *Grading system of government information protection*. Korea: MOI (Ministry of the Interior).

Moore, T., D.J. Pym, and C. Loannidis. 2010. *Economics of information security and privacy*. Berlin: Springer.

MOPAS (Ministry of Public Administration and Security). 2013. *The rating measurement manual for the maintenance of information resources*. Korea: MOPAS (Ministry of Public Administration and Security).

MOTIE (Ministry of Trade, Industry and Energy). 2015. *Comprehensive plan for prevention and protection of secondary industrial technology leakage ('16 ~ '18)*. Korea: MOTIE (Ministry of Trade, Industry and Energy).

MSIT (Ministry of Science, ICT and Future Planning). 2013. *Corporate information protection policy direction*. KOREA: Information Strategy Bureau.

Munson, D.C. 1996. The patent-trade secret decision: An industrial perspective. *Journal of the Patent and Trademark Office Society* 78: 689.

National Industrial Security Center. 2018. Press release. NIS (National Intelligence Service).

Noh, S., and J. Lim. 2017. A study for enterprise type realtime information security management system. *Journal of The Korea Institute of Information Security & Cryptology* 27 (3): 617–636.

Noh, Y. 2017. Research on development of social value evaluation indicators for public libraries. *Journal of the Korean Society for Information Management* 34 (2): 181–214.

NSW Government. 2015. NSW government information classification—labelling and handling guidelines. NSW Government.

Park, C., C. Kim, Y. Kim, H. An, and J. Bae. 2015. Improvement of personal information protection level in the military using the measurement of disclosure risk. *Journal of Security Engineering* 12 (6): 581–596.

Park, C.S. 2016. Industrial technology protection strategy for future society. *Science & Technology Policy STEPI Insight* 201.

Parker, D.B. 2012. Toward a new framework for information security?. In *Computer Security Handbook* 3-1.

Park, H., and W. Shin. 2010. Determinants and influential factors in technology valuation in korea. *International Journal of Contents* 6 (3): 53–58.

Peltier, T.R. 2016. *Information security policies, procedures, and standards: Guidelines for effective information security management*. Boca Raton: CRC Press.

Perkins, J. 2012. Information security—information classification. LSE Governance.

Prahalad, C.K., and G. Hamel. 2006. *The core competence of the corporation*. Berlin: Springer. **Strategische unternehmungsplanung - strategische unternehmungsführung**.

Saaty, T.L. 2008. Decision making with the analytic hierarchy process. *International Journal of Services Sciences* 1 (1): 83–98.

Safa, N.S., R. Von Solms, and L. Futcher. 2016. Human aspects of information security in organisations. *Computer Fraud & Security* 2016 (2): 15–18.

Soomro, Z.A., M.H. Shah, and J. Ahmed. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36 (2): 215–225.

Soonchunhyang University Cooperation. 2010. A study on development and methodology of globally standardized cybersecurity index. Korea Communication Commission.

Statistics Korea. 2017. *Information asset security management guidelines*. Korea: Published Rulings.

Stoneburner, G., A.Y. Goguen, and A. Feringa. 2002. Sp 800-30. Risk management guide for information technology systems.

Strang, V., and M. Busse (Eds.). 2011. Ownership and appropriation (Vol. 47). London: Bloomsbury Publishing.

Sungkyunkwan University Cooperation. 2016. Measures for strengthening technology protection capabilities of SMEs. Presidential Council on Intellectual Property.

Sung, T., D.S. Kim, J. Jang, and H. Park. 2016. An empirical analysis on determinant factors of patent valuation and technology transaction prices. *Journal of Korea Technology Innovation Society* 19 (2): 254–279.

Suzuki, K. 2015. Economic growth under two forms of intellectual property rights protection: patents and trade secrets. *Journal of Economics* 115 (1): 49–71.

Tien, J.M. 2013. Big data: Unleashing information. *Journal of Systems Science and Systems Engineering* 22 (2): 127–151.

Timothy, P.L. 2016. *Information security: Design, implementation, measurement, and compliance*. Boca Raton: CRC Press.

Tipton, H.F., and M.K. Nozaki. 2007. *Information security management handbook*. Boca Raton: CRC Press.

TTA(Telecommunications Technology Association). 2010. *The asset management guideline for information security of organization*. Korea: TTA(Telecommunications Technology Association).

Yahya, S., and B. Kingsman. 1999. Vendor rating for an entrepreneur development programme: A case study using the analytic hierarchy process method. *Journal of the Operational Research Society* 50 (9): 916–930.

Von Solms, R., and J. Van Niekerk. 2013. From information security to cyber security. *Computers & Security* 38: 97–102.

Yoon, J.H. 2014. Current criminal issues and the trends of Korean supreme court decisions on the protection of trade secrets. *Ewha Law Journal* 19 (1): 109–147.

Yoon, M.H., et al. 2004. *A study on development of standard model of patent technical evaluation*. Korea: KIIP(Korea Institute of Intellectual Property).

Zobel, A.K., B. Lokshin, and J. Hagedoorn. 2017. Formal and informal appropriation mechanisms: the role of openness and innovativeness. *Technovation* 59: 44–54.

Affiliations

Onechul Na[1] · Lee Won Park[1] · Harang Yu[1] · Yanghoon Kim[2] · Hangbae Chang[3]

Onechul Na
nastop@cau.ac.kr

Lee Won Park
lwpark@cau.ac.kr

Harang Yu
hryu356@cau.ac.kr

Yanghoon Kim
yhkim@kdu.ac.kr

[1] Department of Security Convergence, Graduate School, Chung-Ang University, Seoul 06974, Korea

[2] Department of Industrial Security, College of Engineering, Far East University, Eumseong-gun, Chungcheongbuk-do 27601, Korea

[3] Department of Industrial Security, College of Business and Economics, Chung-Ang University, Seoul 06974, Korea