The Journal of Supercomputing (2023) 79:11707–11742
https://doi.org/10.1007/s11227-023-05101-w

Design of evaluation items of the security levels for suppliers in the manufacturing industry

Yurim Choi[1] · **Hangbae Chang**[2]

Accepted: 3 February 2023 / Published online: 2 March 2023

Abstract
Owing to the fourth industrial revolution, collaborations between companies and various technologies have become indispensable, particularly in the manufacturing industry. However, technology leakage is likely to occur among cooperative partners where the ratio of small- and medium-sized enterprises is relatively high because of low-security resources. To address this security management problem, we analyzed existing literature and designed a reference model and questions to evaluate security levels reflecting partners' characteristics to be managed by the manufacturing parent company. We conducted an expert survey to verify the designed model and calculated the weight of each evaluation area. Consequently, we designed a reference model to effectively evaluate, from the perspective of the parent company, partners in manufacturing. We anticipate that the results of this study will assist a parent company in securely sharing data and technologies with partners and being used as a self-diagnosis tool by partners to evaluate its security levels.

Keywords Security level evaluation · Parent company · Partners · Manufacturing industry

1 Introduction

With the advent of the fourth industrial revolution, technologies have advanced in various areas, and society has changed, rendering owning a technology more competitive. In particular, collaboration with other companies with specialized technologies has become indispensable to producing efficient and effective products as the

✉ Hangbae Chang
hbchang@cau.ac.kr

Yurim Choi
julie330@cau.ac.kr

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

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

manufacturing industry has been changed into a way of producing products by combining various technologies. Additionally, with the acceleration of digitalization, transmission of data and technology between parent–partner companies is increasing, and traditional manufacturing is changing into smart manufacturing, which includes manipulation of huge amounts of data processed with sensors, accumulators, and process machines [1]. Based on this change, although most parent companies, which are relatively affluent, use blockchain technologies with transparency and accountability to protect and secure assets, including their data, most partner companies have a limited budget to develop operating companies [2]. The concept of a parent company that entrusts the production of products to technology partner companies has emerged. However, security incidents are continuously occurring, targeting partners by abusing the characteristics of sharing competitive data of a parent company with partners.

In 2019, The Wall Street Journal announced that Russian hackers allegedly broke into the computer systems of dozens of contractors to hack into the US power grid for several years [3], exploiting small contractors with vulnerable security resources, which were expected to encompass at least 24 states. Deloitte's report (Fig. 1) announced statistics on security threats in the manufacturing industry [4]. Theft of intellectual properties, which include copyrights, patents, trademarks, industrial designs, geographical indications, and trade secrets [5], accounts for the highest rate (34%) of security threats/ attacks in the manufacturing industry. In addition, security threats are becoming sophisticated and proliferated, and security breaches involving third parties occupy 28%. Figure 1 shows that not only IT security threats but other security threats can also severely impact (technology leakage) in the manufacturing industry. Technology leakage refers to the stealing and hiding of industrial secrets of economic value, such as trade secrets or ownership information [6]. In particular, trade secrets become a sensitive issue when a parent company contracts with partners. However, with these risks, traditional security defenses, such as firewalls, antivirus, etc., provide limited protection against data breaches and theft from inside threats within a company [7]. To address this problem, an effective tool is required for managing partner companies for a parent company and for partner companies to store data and technology securely, such as big data management [8] (Fig. 2).

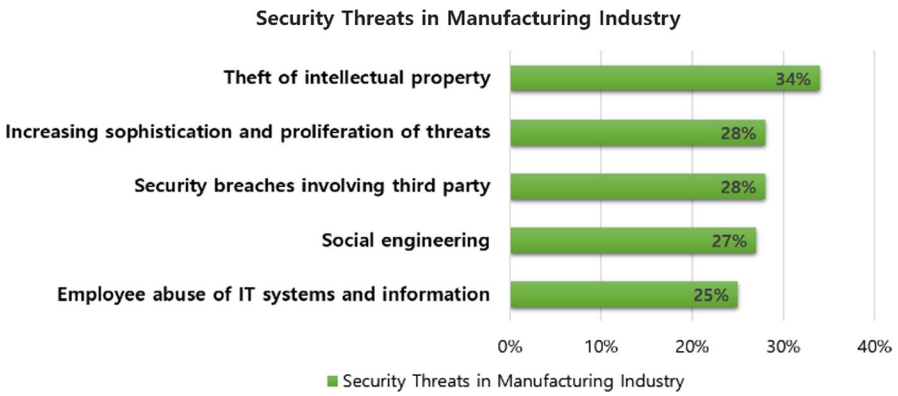

Fig. 1 Security threats/ attacks in manufacturing industry [4]

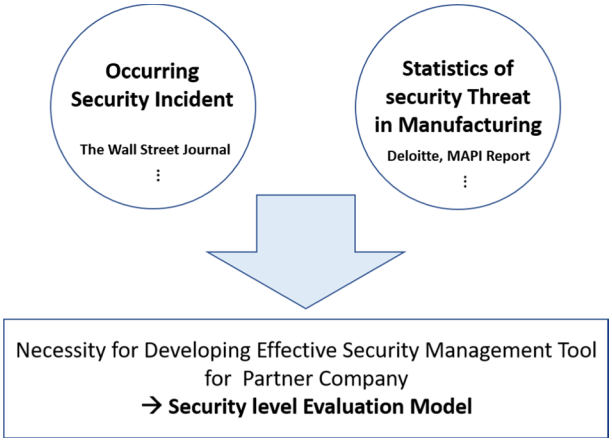

Fig. 2 Needs for developing security level evaluation model through security incidents and statistics

This study targets all work processes that may include technical and data leakage when attempting collaboration with partners from the parent company's perspective. The scope of this study includes a case of conducting joint research between a parent company and partners as well as the research security content. This study derived risks of partners and a countermeasure by analyzing previous studies in relation to the design of security management systems of partners in the manufacturing industry and the design of security level evaluation items. Subsequently, questions that can evaluate the security levels of partners were derived and designed based on previous studies and literature. This is not only an academic study, but also measures the relative importance through the analytic hierarchy process (AHP) of pairwise comparison of areas and items in the reference model to evaluate the security levels of partners, focusing on security experts employed in the manufacturing industry who have collaboration experience with partners to be used in real industries. It also calculated scores of areas and items through statistical verification that measures the importance and weights of the evaluation items by verifying the fitness, validity, and absolute importance of the questions on security level evaluation of partners in the manufacturing industry, thereby designing the final security level evaluation items of partners.

This study aims to design questions on evaluation items that can objectively and rationally evaluate whether partners have established security measures to some extent regarding security incident risks such as technical leakage during unavoidable technologies and data-sharing processes for collaboration with partners from the viewpoint of a parent company in the manufacturing industry through values (scoring). Based on this, items that can intuitively evaluate the security levels of partners required by a parent company in the manufacturing industry are used by partners to self-diagnose their security levels, thereby exhibiting objective values to a parent company, whereas partners collaborate to build their secure security environments. Based on their self-diagnosis results, a parent company can continue a secure collaboration with trustworthy partners.

2 Literature review

2.1 Design of the security management system model of partners

A study by Lee [9] presented a security management system model by dividing the scope of display manufacturing partners in the display industry, which is an example of a manufacturing industry, into manufacturing and development areas as well as management information areas. The security management areas of partners that should be managed by a contractor, which is a conglomerate, were classified and considered as intensively focused security areas. According to this classification, cultivating the response and management capabilities of the leakage of information entrusted and provided by a parent company, loss and theft of goods, infringement incidents, etc., were selected as the key security elements considered by partners. In conformity with the characteristics of partners, a total of nine inspection areas (i.e., security organization, regulations, asset management, personnel management, physical security, the security of personal computers and portable devices, the security of information technology, responses to accidents, as well as security inspection and audit) and 59 evaluation items were derived. In addition, this study verified the effectiveness of the designed security management system for partners by applying it to real partners, thereby comparing and evaluating the security levels before and after adoption of the system. However, this previous study lacks a discussion about the data sharing process between parent–partner companies. In this study, we supplement this by considering the transmission of data and using the inspection items in the security management systems of partners as a reference for designing the security level evaluation model framework of partners.

In a previous study [10], Kim conducted an analysis using the data envelopment analysis (DEA) model, targeting the primary parts and equipment companies, which were 36 subcontractors in the automobile industry, based on the results of the evaluation of a measure that built an efficient security operation system of technical data of subcontractors, and efficiency measurement results. Furthermore, Kim analyzed the problem of degraded efficiency, attributed to the fact that security levels under the same standards were required in all subcontractors after investigating the inspection status of technical data security management of subcontractors. This previous study proposed a method to use the measurement results of the efficiency of technical data security management for subcontractors based on the analyzed content in the evaluation results of the status of technical data management, such as drawings. Regardless of the consideration, it still has limitations in physical security, which is composed of access control only, and the factory operating rate is also high. We designed the security level evaluation model in detail, reflecting these attributes of the partner company in the manufacturing industry.

Kim [11] proposed a model to evaluate a security level consisting of four categories (security change management, security operation management, security support environment, and security culture) and 26 detailed items in relation to possible technical leakage risks from insiders within the company. It also collected digital evidence that satisfies the requirements using a digital forensic technique for electronic

protection systems of security operation management from the items in the security level evaluation model for more objective security level evaluation and proposed a method of objective digital tracking and analysis based on the collected digital evidence. This previous study focused on security management of enterprises generally; therefore, we manipulated some items and the overall model to fit a partner company in manufacturing industry.

2.2 Derivation of security level evaluation items

In Noh's study [12], a security management system was proposed that can be responded to at all times in a company by improving existing security management systems and establishing a life cycle system of security tasks. It also selects and suggests security indicators to check whether the established life cycle of security tasks is fulfilled, and proposes a measure to collect information by automating security operations for some security indicators to ensure constant collection. In the aforementioned study, he proposed the model with life cycle of security tasks; however, the degree of risks, such as impact or probability of risks, were not discussed. In our study, we designed evaluation items by referring to the security indicators with work processes proposed in this previous study.

According to a study by Ahn et al. [13], it proposed the need for an open organizational security culture where all employees, including executives, participate in sustained company growth. Based on this, it discussed the need to establish an organizational security culture for the technical protection of a company and developed a framework for security culture consisting of various items. However, this previous study has the limitation that it focuses only on secure culture. We aim to consider the overall manufactural business process and develop evaluation items on security awareness and trust, etc., from the security level evaluation items of partners in the manufacturing industry, which is the goal of this study, by referring to the items consisting of the security culture in the aforementioned previous study.

A study by Bae [14] proposed an evaluation model that can be effectively used in the self-diagnosis of research security levels by designing research security evaluation indicators based on the research management process. It divided the research management process into the four following categories: research planning, research agreement, research management, and research performance, as well as designed 138 security evaluation indicators for each process phase. This previous study suggested a security model for general research management processes that differed from research in the manufacturing industry. Therefore, in this study, we have developed and modified some research security evaluation items by referring to the research security of the aforementioned study that should be considered by partners in the process of joint research conducted with a parent company in the manufacturing industry.

In a study by Wei et al. [15], a recommendation mechanism was proposed to assist the risk assessor in selecting the most suitable threat-vulnerability pairs while performing risk identification. The recommendation list is created using predictive apriori with the historical selection data of the International Organization for

Standardization/International Electrotechnical Commission (ISO/IEC) 27,001:2013 certified business unit. In this research, we referred to this study as a way of classifying threat-vulnerability pairs with each information asset.

Through the analysis of previous studies, we set up our study scope and perspectives, as well as designed items and questions, whereby the security levels of partners can be evaluated. However, most previous studies that targeted partners conducted a study from the viewpoint of partners only, rather than from a parent company's viewpoint. Thus, those studies did not specifically distinguish between a parent company and partners, as their processes consisted of general work processes for companies. Furthermore, previous studies only proposed which indicators or areas were more important through the analysis of weights after proposing all evaluation indicators. However, they did not calculate a score for each indicator and area, rendering it difficult to use practically on-site.

To overcome the limitations of previous studies, we conducted research from the following viewpoints. First, this study designed a reference model to evaluate security levels based on the security environment required by partners when conducting a collaboration with partners from the parent company's viewpoint. The security levels that a parent company requires from its partners rather than from the partners' viewpoint have much more limited scope to be considered compared to the design of the security management system from general companies' viewpoints. Moreover, this study designed a reference model to evaluate security levels by reflecting the environment of specific partners as the characteristics of partners collaborating with various companies are reflected.

The final objective of this study is to develop items to evaluate the security levels of partners in the manufacturing industry. It is not only limited to academic research but also calculates a score by deriving a weight for each item to be directly used to evaluate security levels in practice. This study aims to calculate objective and reasonable scores by deriving the importance (weights) of evaluation areas and items of partners in the manufacturing industry.

3 Design of the model to evaluate security levels of partners

3.1 Design of the reference model

As shown in Fig. 3, the research methodology is designed to develop the security level evaluation items for secured data sharing with partners from a parent company's viewpoint in the manufacturing industry. Previous studies in relation to the design of security level evaluation model (Sect. 2.1) and items (Sect. 2.2), including laws about the prevention of technology leakage, designs of the security management systems of partners, as well as reports and guidelines on security level evaluation items, were also analyzed. Based on the analysis results, a reference model to evaluate security levels of partners, detailed evaluation items, and questions were designed. The validity of the designed evaluation items and the absolute importance of questions were derived using a 5-point scale, and a survey was conducted with experts in the relevant areas for AHP analysis of the relative

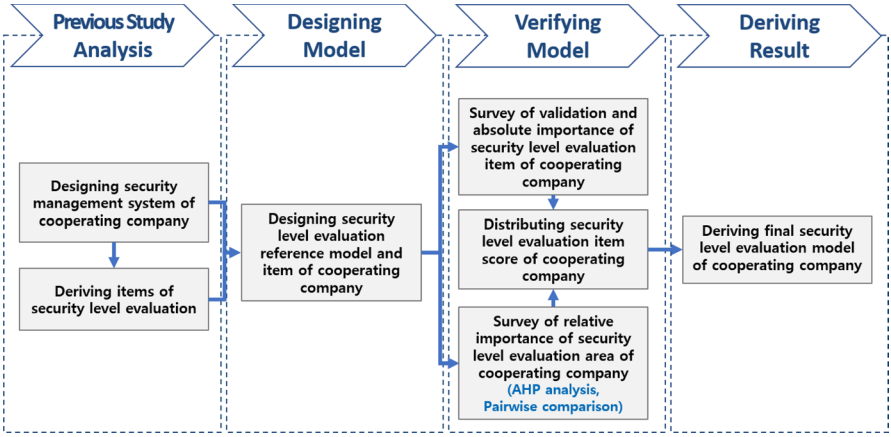

Fig. 3 Study methodology

importance of the security level evaluation areas and items (sub-categories) of partners. Then, the importance of the areas, items, and questions derived through the statistical verification was calculated as scores for each security level evaluation question of partners.

To design a model for evaluating the security level of manufacturing industry partner companies, we chose some items that fit with the partners, which are mostly SMEs. We also modified the model to reflect the characteristics of partners based on the reference model for evaluations of the industrial technology protection level designed in J. Kim et al.'s previous study [11]. We adjusted evaluation items to partners from the perspective of a parent company in the manufacturing industry.

The modified and added items by reflecting the characteristics of partners were "3-1-2. Security management of executives and employees who perform outsourcing process work (parent company)", "4-1-3. Evaluation of security grade of industrial assets (production facility assets + development (spot) assets + information assets) in the outsourcing process (parent company)", "4-4-1. Design of technology protection regulations and policies", "4-4-2. Establishment of security management guidelines of the supply chain in the partners' ordering process (outsourcing process) and fulfillment level", and "4-4-3. Awareness of the establishment of security management guidelines in the outsourcing process (parent company) and level of fulfillment". By contrast, the item "5-1-2. The level of efforts to improve security systems through the analysis of external best practice for security" was removed from the reference model to evaluate security levels required by partners from a parent company's viewpoint. The factor analysis on the areas and items of the designed reference model to evaluate the security levels of partners has already been performed in previous studies. Thus, in this study, instead of performing factor analysis, we performed validity and AHP pairwise comparisons for the reference model to evaluate security levels

3.2 Design of evaluation items of the security levels for partners in the manufacturing industry

Table 1 lists previous studies that were used to derive evaluation items and questions on security levels of partners in the manufacturing industry.

Table 2 describes the evaluation items and questions for partners designed through the analysis of related previous studies.

4 Verification of the model to evaluate security levels of partners

4.1 Derivation of the relative importance of security level evaluation areas and items (sub-category) for partners in the manufacturing industry

To calculate a score for each item in the sub-category and evaluation areas of partners' security levels in the manufacturing industry, which were designed through the analysis of previous studies, the relative importance (weight) of the evaluation areas and items (sub-category) was derived through a survey with experts. An AHP

Table 1 List of previous research for collaborator security level endpoints and question design

ID	List of Previous Studies
A	The Development of Security Evaluation Model-Focused Information Leakage Protection for the Sustainable Growth (Jawon Kim, Chanwoo Lee, Hangbae Chang, 2020)
B	A Research on Activating Factor for Cultivating a Proactive Organizational Security Culture (Byunggoo Ahn, Harang Yu, Hangbae Chang, 2020)
C	A Study on Development of the Evaluation Model on Level of Security in National R & D Program (Sangtae Bae, Juho Kim, 2013)
D	Industrial Technology Protection Guidelines and Manuals (Ministry of Trade, Industry, and Energy, Korean Association for Industrial Technology Security, 2017)
E	Genian GPI Product Introduction (Genians, 2019)
F	A cooperation security checklist for a company (A cooperation, 2019)
G	SME Technology Protection Guidelines (Small and Medium Business Administration, Korea Foundation for Cooperation of Large and Small Business, Rural Affairs, 2016)
H	National R & D Business Security Management Standard Manual (Ministry of Science and ICT, 2014)
I	Manual to respond to technology leakage for SMEs (Korea Industrial Technology Association, Small and Medium Business Administration (SMBA), Korea Technology and Information Promotion Agency for SMEs, 2007)
J	Regulations on management of national R & D projects
K	A review of cybersecurity guidelines for manufacturing factories in industry 4.0. (Mullet Valentin, Patrick Sondi, Eric Ramat, 2021)
L	Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry. (Johansson Kevin, Paulsson Tim, Bergström Erik, Seigerroth Ulf, 2022)
M	Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. (Corallo Angelo, Lazoi Mariangela, Lezzi Marianna, Pontrandolfo Pierpaolo, 2021)

Table 2 Design of security level evaluation items and questions for partners

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	No. of questions on security level evaluation items of partners
1. External environment of technology protection			
1-1. Legal requirements and regulations (compliance) in the industry where the company belongs to			1
2. Organizational culture of technology protection			
2-1. The intent to promote technology protection (executive team)		2-1-1. The level of participation in security training of the executive team	1
		2-1-2. The level of support to security organization by the executive team	5
2-2. (Mutual) security credibility of technology protection		2-2-1. The level of cooperation in work by general employees regarding security activities designed by security manager	2
		2-2-2. The level of enduring the inconvenience due to changed work procedures by general employees concerning security (security acceptance)	1
3. Support environment of technology protection			
3-1. Personnel arrangement of technology protection		3-1-1. Whether personnel in charge of security (or dedicated security department) are assigned	5
		3-1-2. Security management of executives and employees who perform outsourcing process work (parent company)	3
3-2. Investment in technology protection		3-2-1. Investment scale of technology protection (security personnel + security training + security consulting + installation and operation of security system, etc.)	2

Table 2 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	No. of questions on security level evaluation items of partners
4. Operational management of technology protection			
4-1. Identification and classification of the importance of technology development and deliverables		4-1-1. The level of security management on research assets (environmental assets + performing assets) (inspection of security contracts with joint and entrusted institutions and security activities, etc.)	5
		4-1-2. The level of security management of joint entrusted research (security contract with joint and entrusted institutions)	6
		4-1-3. Evaluation of security grade of industrial assets (production facility assets + development (spot) assets + information assets) in the outsourcing process (parent company)	1
		4-1-4. The level of performance management of research results (security activities concerning technology rights (patents, etc.), technology implementation and transfer (trade))	4
		4-1-5. Improvement of the research environment in the research institute (making researchers full-time employment, operation of work-related invention reward system, etc.)	1

Table 2 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	No. of questions on security level evaluation items of partners
4-2. Physical technology protection system		4-2-1. Setup of security zone (equipment) and level of management	19
		4-2-2. The installation of security systems and level of use (security personnel (security guards) + access control + intrusion alarm + video surveillance, etc.)	5
4-3. Electronic technology protection system		4-3-1. The security level of personal computers (user authentication, version update, the installation and operation of security software, etc.)	17
		4-3-2. Server's security levels (user authentication, (shared folders) access right management, version update, the installation and operation of security software, etc.)	10
		4-3-3. Database security level (user authentication, version update, the installation and operation of security software, etc.)	6
		4-3-4. Computer network security level (user authentication, version update, the installation and operation of security software, etc.)	7

Table 2 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	No. of questions on security level evaluation items of partners
4-4. Managerial technology protection system		4-4-1. Design of technology protection regulations and policies	2
		4-4-2. Establishment of security management guidelines of the supply chain in the partners' ordering process (outsourcing process) and fulfillment level	2
		4-4-3. Awareness of the establishment of security management guidelines in the outsourcing process (parent company) and level of fulfillment	3
5. Change management of technology protection			
5-1. Measurement of technology protection level and improvement activities		5-1-1. The level of internal security audit activities (fulfillment of management standards of security policies)	3
		5-1-2. The level of acquired security certification proven by third parties (ISO 27001 certification, K-ISMS certification, etc.)	1

Table 2 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	No. of questions on security level evaluation items of partners
5-2. Response to incidents of technology protection (recovery)		5-2-1. The level of activities to respond to system outage (establishment of the business continuity plan, system redundancy, backup, etc.)	2
		5-2-2.The level of corrective actions taken during technology leakage incidents (incident response plan, recurrent incident prevention measures, analysis of incident causes, putting a recovery system in place, and establishment and execution of recovery plans, etc.)	9
Total sum			123

analysis was conducted to derive the relative importance (weight) of the evaluation areas and items (sub-category) as the survey method. AHP analysis is one of the decision-making support techniques for systematically evaluating mutually exclusive alternatives and constitutes quantitative analysis methods. AHP analysis is highly reliable because it is performed by experts in related fields [23].

The experts who participated in the survey were chosen among those who are employed by a parent company, security experts who have collaboration experience with partners, and experts in the industrial security area. Because the number of experts who satisfied the aforementioned qualifications was small, we surveyed 18 experts because it was important to obtain meaningful results from experts who have a strong understanding of the manufacturing industry's characteristics and collaborative process with partners, as well as expertise in security, according to the characteristics of this study and survey. The sample size was relatively small, although evaluators who participated in pairwise comparisons in AHP analysis should have been chosen from experts with sufficient knowledge of the subject to be evaluated in the relevant areas according to the Korea Development Institute (KDI). With this recommendation, AHP analysis was previously conducted with three to four experts, despite the risk that the entire decision-making process could be distorted because of the bias of some evaluators, owing to the limited number of evaluators. Thus, recently, the number of evaluators has been extended to 7 ~ 8 experts [24]. Based on this rationale, a study found that the selection of experts in the research area and whether the evaluators responded consistently can be more important factors for the reliability of AHP analysis than the number of samples [25].

For the survey tool, a respondent questionnaire with a 9-point scale pairwise comparison format was used. For the analysis method, five security level evaluation items of partners in the manufacturing industry were set to the top hierarchy in the survey, and 11 evaluation items (sub-category) for each evaluation area, which were put in the lower hierarchy, were inquired in the survey. Among the evaluation areas, "1. External environment of technology protection" had only one item "1-1. Legal requirements and regulations (compliance) in the industry where the company belongs to." Thus, its verification was not conducted. The derived results of the relative importance (weight) of evaluation areas and items (sub-category) of partners' security levels in the manufacturing industry are presented in Tables 3, 4, 5, 6, and 7.

Table 3 Derived results of the relative importance of security level evaluation areas of partners

Security level evaluation areas of partners	Importance (Weight)	Consistency Rate (CR)
1. External environment of technology protection	0.114	0.00838
2. Organizational culture of technology protection	0.310	
3. Support environment of technology protection	0.217	
4. Operational management of technology protection	0.239	
5. Change management of technology protection	0.119	

Table 4 Derived results of the relative importance of security level evaluation items (2. Organizational culture of technology protection) of partners

Security level evaluation items of partners (sub-category)	Importance (Weight)	Consistency Rate (CR)
2-1. The intent to promote technology protection (executive team)	0.843	0.000
2-2. (Mutual) security credibility of technology protection	0.157	

Table 5 Derived results of the relative importance of security level evaluation items (3. Support environment of technology protection) of partners

Security level evaluation items of partners (sub-category)	Importance (Weight)	Consistency Rate (CR)
3-1. Personnel arrangement of technology protection	0.632	0.000
3-2. Investment in technology protection	0.368	

Table 6 Derived results of the relative importance of security level evaluation items (4. Operational management of technology protection) of partners

Security level evaluation items of partners (sub-category)	Importance (Weight)	Consistency Rate (CR)
4-1. Identification and classification of the importance of technology development and deliverables	0.429	0.0315
4-2. Physical technology protection system	0.109	
4-3. Electronic technology protection system	0.282	
4-4. Managerial technology protection system	0.181	

Table 7 Derived results of the relative importance of security level evaluation items (5. Operational management of technology protection) of partners

Security level evaluation items of partners (sub-category)	Importance (Weight)	Consistency Rate (CR)
5-1. Measurement of technology protection level and improvement activities	0.702	0.000
5-2. Response to incidents of technology protection (recovery)	0.298	

Table 3 lists an AHP pairwise comparison analysis of five security level evaluation areas of partners, which exhibits the analysis results of importance (weight). The derived most important area was "2. Organizational culture of technology protection" followed by "4. Operational management of technology protection," "3. Support environment of technology protection," "5. Change management of technology protection," and "1. External environment of technology protection" as the importance (weight). The ratio of the importance (weight) of each evaluation area is as follows: "2. Organizational culture of technology protection (approximately

30%)," "4. Operational management of technology protection (approximately 25%)," "3. Support environment of technology protection (approximately 20%)," "5. Change management of technology protection (approximately 15%), and "1. External environment of technology protection (approximately 10%)."

The consistency ratio (CR) was further analyzed to verify the reliability of the AHP analysis. The random index proposed by Saaty [26] was used to calculate the CR. When the CR is smaller than 0.1, it is considered that respondents in the survey consistently analyze pairwise comparisons [27]. The calculated CR in the AHP analysis of the security level evaluation areas of partners was 0.00838, which verified that the survey was highly consistent.

Table 4 presents the derived results of the importance (weight) of security level evaluation items (sub-category) by evaluation areas of partners. Table 4 describes the analysis results of the importance (weight) of the evaluation items (sub-category) that belong to the item "2. Organizational culture of technology protection." The derived most important evaluation item was "2-1. The intent to promote technology protection (executive team)" followed by "2.2. (Mutual) security credibility of technology protection." The ratio of the importance of each evaluation item was "2-1. The intent to promote technology protection (executive team) (approximately 80%) followed by "2-2. (Mutual) security credibility of technology protection (approximately 20%)." The derived CR of the evaluation item in the area "2. Organizational culture of technology protection" was 0.000, which verified that the survey was highly reliable.

Table 5 lists the analysis results of importance (weight) of the evaluation items (sub-category) that is applicable to the evaluation area "3. Support environment of technology protection." The derived most important evaluation item was "3-1. Personnel arrangement of technology protection" followed by "3-2. Investment in technology protection." The ratio of the importance of each evaluation item was "3-1. Personnel arrangement of technology protection (approximately 60%)" followed by "3-2. Investment in technology protection (approximately 40%)." The derived CR of the area "3. Support environment of technology protection" was 0.000, which verified that the survey was highly reliable.

Table 6 lists the analysis results of importance (weight) of the evaluation items (sub-category) that is applicable to the evaluation area "4. Operational management of technology protection." The derived most important evaluation item was "4.1. Identification and classification of the importance of technology development and deliverables" followed by "4-3. Electronic technical protection system," "4-4. Managerial technical protection system," and "4-2. Physical technology protection system." The ratio of the importance of each evaluation item was "4-1. Identification and classification of the importance of technology development and deliverables (approximately 40%)," "4-3. Electronic technology protection system (approximately 30%)," "4-4. Managerial technology protection system (approximately 20%)," and "4-2. Physical technology protection system (approximately 10%)." The derived CR of the evaluation item in the area "4. Operational management of technology protection" was 0.0315, which verified that the survey was highly reliable.

Table 7 lists the analysis results of the importance (weight) of the evaluation items (sub-category) that is applicable to the evaluation area "5. Change management

of technology protection." The derived most important evaluation item was "5-1. Measurement of technology protection level and improvement activities" followed by "5-2. Response to incidents of technology protection (recovery)." The ratio of the importance of each evaluation item was "5-1. Measurement of technology protection level and improvement activities (approximately 70%)" and "5-2. Response to incidents of technology protection (recovery) (approximately 30%)." The derived CR of the evaluation item in the area "5. Change management of technology protection" was 0.000, which verified that the survey was highly reliable.

4.2 Verification of validity and feasibility (absolute importance) of partner's security levels in the manufacturing industry

To verify the validity (absolute importance) of questions on the security level evaluations of partners in the manufacturing industry derived through the analysis of the previous studies, we surveyed experts equivalent to deriving the relative importance of evaluation areas and items (sub-category). The survey method was as follows: the respondent determined whether the evaluation-related questions were adequate, and if they responded that the questions were adequate, and they evaluated the absolute importance of the item on a 5-point scale. The survey tool was a respondent questionnaire consisting of 123 questions. The survey was conducted with security experts who were employed in a parent company in the manufacturing industry and had collaboration experience with partners, which was conducted in a similar way to the survey with experts to derive the relative importance.

On a 5-point scale, 3.5 points refer to a 70% ratio of five points when the same criterion is applied with the adoption of questions whose response score is 3.5 points or higher. In this study, when the ratio of the respondents who considered the questions in the questionnaire fit was more than 70% of the total respondents, that is, if more than 13 out of a total of 18 respondents replied that the questions were fit, those questions were considered fit and adopted. As shown in Fig. 4, 10 questions with a red edge were responded to as unfit (under 70% of validity) out of 123 questions and thus removed. Table 8 shows the remaining 113 questions. The model in this study was based on Kim's previous study, which processed factor analysis. Therefore, we placed additional items in related areas and skipped the factor analysis in this study.

The verification of the validity of questions on the security level evaluation items of partners was conducted, and 10 questions in seven evaluation items (sub-sub-categories) were removed. In particular, two questions from the evaluation item (sub-sub-category) "2-1-2. The level of support on the security organization by the executive team" were removed. Furthermore, one question from "2-2-1. The level of work collaboration by general employees on security activities designed by security manager" and one question from "3-1-2. Security management of executives and employees who perform outsourcing process work (parent company)" were removed. In addition, two questions from "4-2-1. Setup of security zone (equipment) and level of management," one question from "4-3-1. The security level of personal computers (user authentication, version update, the installation and operation of security software, etc.)" and one question from

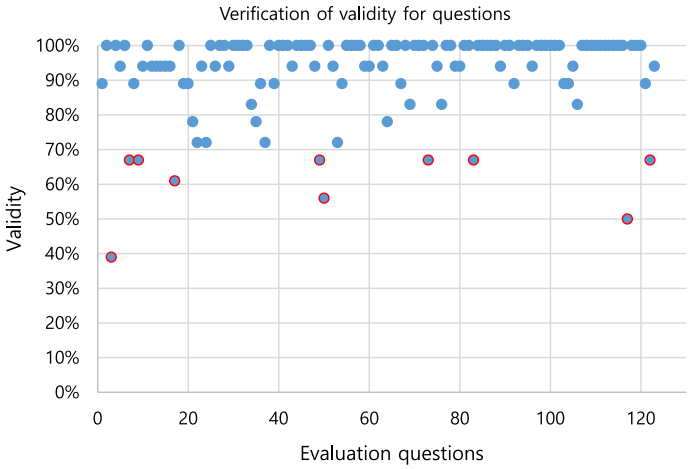

Fig. 4 Verification result of question validity

"4-3-2. Server's security levels (user authentication, (shared folders) access right management, version update, the installation and operation of security software, etc.)" were removed. Finally, two questions were removed from "5-2-2. The level of corrective actions taken during technology leakage incidents (incident response plan, recurrent incident prevention measures, analysis of incident causes, putting a recovery system in place, as well as establishment and execution of recovery plans, etc.). Table 9 lists the derived absolute importance of the security level evaluation items of partners in the manufacturing industry.

5 Results and analysis

Based on the derived results of the fitness and validity of questions on security level evaluations of partners in the manufacturing industry and relative importance of the areas and questions, scores can be calculated by evaluation areas, items (sub-category), and questions. The scores of each evaluation area were calculated by converting the weights of the areas calculated in Table 3 into a perfect-100 point-scale mark. Figure 5 shows the formula for the evaluation item (sub-category) score, and Fig. 6 shows the formula for the evaluation-related question score.

$$\begin{aligned}&\text{EvaluationItem(SubCategory)}Score\\&\quad = EvaluationAreaScore * \frac{EvaluationItem(SubCategory)Weight}{100}\end{aligned}$$

$$\begin{aligned}&\text{EvaluationQuestion}Score\\&\quad = SubCategoryScore * \frac{QuestionImportance}{QuestionImportanceTotalSuminSubCategory}\end{aligned}$$

Table 8 Verification results of validity

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	No. of questions on security level evaluation items of partners	finally derived No. of questions on evaluation items
1. External environment of technology protection				
1-1. Legal requirements and regulations (compliance) in the industry where the company belongs to			1	1
2. Organizational culture of technology protection				
2-1. The intent to promote technology protection (executive team)		2-1-1	1	1
		2-1-2	5	3
2-2. (Mutual) security credibility of technology protection		2-2-1	2	1
		2-2-2	1	1
3. Support environment of technology protection				
3-1. Personnel arrangement of technology protection		3-1-1	5	5
		3-1-2	3	2
3-2. Investment in technology protection		3-2-1	2	2
4. Operational management of technology protection				
4-1. Identification and classification of the importance of technology development and deliverables		4-1-1	5	5
		4-1-2	6	6
		4-1-3	1	1
		4-1-4	4	4
		4-1-5	1	1
4-2. Physical technology protection system		4-2-1	19	17
		4-2-2	5	5
4-3. Electronic technology protection system		4-3-1	17	16
		4-3-2	10	9
		4-3-3	6	6
		4-3-4	7	7

Table 8 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	No. of questions on security level evaluation items of partners	finally derived No. of questions on evaluation items
4-4. Managerial technology protection system		4-4-1	2	2
		4-4-2	2	2
		4-4-3	3	3
5. Change management of technology protection				
5-1. Measurement of technology protection level and improvement activities		5-1-1	3	3
		5-1-3	1	1
5-2. Response to incidents of technology protection (recovery)		5-2-1	2	2
		5-2-2	9	7
Total			123	113

Table 9 Derived results of importance from questions on security level evaluation of partners

Security level evaluation area of partners	Security level evaluation items of partners (sub-category)	Final evaluation item/ No. of questions	Importance of each question
1. External environment of technology protection			
1-1. Legal requirements and regulations (compliance) in the industry where the company belongs to		1	4.3
2. Organizational culture of technology protection			
2-1. The intent to promote technology protection (executive team)		1	4.5
		3	4.2
			4.4
			4.4
2-2. (Mutual) security credibility of technology protection		1	4.3
		1	4.6
3. Support environment of technology protection			
3-1. Personnel arrangement of technology protection		5	4.1
			4.1
			4.6
			4.3
			4.5
		2	4.5
			4.4
3-2. Investment in technology protection		2	4.1
			4.4

Table 9 (continued)

Security level evaluation area of partners	Security level evaluation items of partners (sub-category)	Final evaluation item/ No. of questions	Importance of each question
4. Operational management of technology protection			
4-1. Identification and classification of importance of technology development and deliverables		5	4.4
			4.1
			4.6
			4.1
			4.8
		6	4.5
			4.6
			4.6
			4.6
			4.5
			4.7
		1	4.6
		4	4.4
			4.5
			4.5
			4.4
		1	4.2

Table 9 (continued)

Security level evaluation area of partners	Security level evaluation items of partners (sub-category)	Final evaluation item/ No. of questions	Importance of each question
4-2. Physical technology protection system		17	4.4
			4.1
			4.7
			4.6
			4.4
			4.4
			4.4
			4.3
			4.6
			4.4
			4.3
			4.4
			4.1
			4.5
			4.5
			4.3
			4.7
		5	4.5
			4.6
			4.5
			4.2
			4.4

Table 9 (continued)

Security level evaluation area of partners	Security level evaluation items of partners (sub-category)	Final evaluation item/ No. of questions	Importance of each question
4-3. Electronic technology protection system		16	4.7
			4.5
			4.4
			4.3
			4.7
			4.6
			4.6
			4.5
			4.4
			4.1
			4.4
			4.7
			4.5
			4.4
			4.6
			4.4

Table 9 (continued)

Security level evaluation area of partners	Security level evaluation items of partners (sub-category)	Final evaluation item/ No. of questions	Importance of each question
		9	4.5
			4.6
			4.6
			4.7
			4.5
			4.6
			3.9
			4.4
			4.4
		6	4.6
			4.6
			4.4
			4.3
			4.5
			4.1
		7	4.3
			4.4
			4.7
			4.7
			4.7
			4.6
			4.4

Table 9 (continued)

Security level evaluation area of partners	Security level evaluation items of partners (sub-category)	Final evaluation item/ No. of questions	Importance of each question
4-4. Managerial technology protection system		2	4.3
			4.3
		2	4.3
			4.6
		3	4.1
			4.2
			4.3
5. Change management of technology protection			
5-1. Measurement of technology protection level and improvement activities		3	4.1
			4.2
			4.2
		1	3.9
5-2. Response to incidents of technology protection (recovery)		2	4.6
			4.6
		7	4.4
			4.4
			4.6
			4.5
			4.6
			4.4
			4.2

$$\text{Evaluation Item(Sub Category)}Score = Evaluation\ Area\ Score * \frac{Evaluation\ Item(Sub\ Category)Weight}{100}$$

Fig. 5 Formula for evaluation item (sub-category) score

$$\text{Evaluation Question}\ Score = Sub\ Category\ Score * \frac{Question\ Importance}{Question\ Importance\ Total\ Sum\ in\ Sub\ Category}$$

Fig. 6 Formula for evaluation-related question score

Table 10 lists the final security level evaluation items of partners in the manufacturing industry that reflect the scores of evaluation areas, items (sub-category), and questions derived based on the aforementioned calculation formulas.

The final result of this study is different from the traditional security level evaluation model for general enterprises. In this study, we designed the model to evaluate the security level of a partner company as a security manager of parent company in the manufacturing industry. For more effective evaluation, we considered the weight of each area and sub-category. Based on the weight of five areas and 11 sub-categories, we calculated priority and score of each evaluation item. The score was distributed based on the number of questions included in each sub-category. Thus, if many questions exist in a subcategory, then the score will be distributed as a small score for each question. However, the priority of each area and subcategory is understandable with the total sum of scores.

6 Conclusion and future research

In most industries, managing companies with general security evaluation models that do not consider the attributes of each industry has some limitations. Particularly in the manufacturing industry, business processes, such as supply chain, differ significantly, rendering it difficult to effectively manage companies, including the company and others (partners). In this study, we developed evaluation items that can objectively and reasonably evaluate the security levels of partners from the parent company's viewpoint in the manufacturing industry. The items were designed based on related literature, and the absolute importance of the fitness and validity of questions was derived by conducting surveys of current and previous employees in the manufacturing industry, using a five-point scale. The relative importance of evaluation areas and items was derived through an AHP pairwise comparison analysis. Based on the statistical verification results, final security level evaluation items and questions for partners were developed, and their scores were calculated based on the weights of the derived areas, items (sub-category), and questions. By verifying the validity of evaluation items, most of the removed questions were designed for general enterprise in the previous study except one (one question from 3-1-2 sub-category) out of 10 from the final result of statistical verification. We concluded that the proposed model can reflect

Table 10 Final questions on security level evaluation of partners

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	Security level evaluation-related questions for partners (score)
1. External environment of technology protection (10)	1-1. Legal requirements and regulations (compliance) in the industry where the company belongs to (10)		10
2. Organizational culture of technology protection (30)	2-1. The intent to promote technology protection (executive team) (24)	2-1-1	6
		2-1-2	6
			6
			6
	2-2. (Mutual) Security credibility of technology protection (6)	2-2-1	3
		2-2-2	3
3. Support environment of technology protection (20)	3-1. Personnel arrangement of technology protection (12)	3-1-1	1.6
			1.6
			1.8
			1.7
			1.8
		3-1-2	1.8
			1.7
	3-2. Investment in technology protection (8)	3-2-1	4
			4

Table 10 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	Security level evaluation-related questions for partners (score)
4. Operational management of technology protection (25)	4-1. Identification and classification of importance of technology development and deliverables (10)	4-1-1	0.6
			0.5
			0.6
			0.5
			0.6
		4-1-2	0.6
			0.6
			0.6
			0.6
			0.6
			0.6
		4-1-3	0.6
		4-1-4	0.6
			0.6
			0.6
			0.6
		4-1-5	0.6

Table 10 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	Security level evaluation-related questions for partners (score)
	4-2. Physical technical protection system (2.5)	4-2-1	0.11
			0.11
			0.12
			0.12
			0.11
			0.11
			0.11
			0.11
			0.12
			0.11
			0.11
			0.11
			0.11
			0.11
			0.12
			0.11
			0.12
		4-2-2	0.12
			0.12
			0.12
			0.11
			0.11

Table 10 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	Security level evaluation-related questions for partners (score)
	4-3. Electronic technical protection system (7.5)	4-3-1	0.21
			0.20
			0.19
			0.19
			0.21
			0.20
			0.20
			0.20
			0.19
			0.19
			0.19
			0.21
			0.20
			0.19
			0.20
			0.19

Table 10 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	Security level evaluation-related questions for partners (score)
		4-3-2	0.20
			0.20
			0.20
			0.21
			0.20
			0.20
			0.18
			0.19
			0.19
		4-3-3	0.20
			0.20
			0.19
			0.19
			0.20
			0.19
		4-3-4	0.19
			0.19
			0.21
			0.21
			0.21
			0.20
			0.19

Table 10 (continued)

Security level evaluation areas of partners	Security level evaluation items of partners (sub-category)	Security level evaluation items of partners (sub-sub-category)	Security level evaluation-related questions for partners (score)
	4-4. Managerial technical protection system (5)	4-4-1	0.7
			0.7
		4-4-2	0.7
			0.8
		4-4-3	0.7
			0.7
			0.7
5. Change management of technology protection (15)	5-1. Measurement of technology protection level and improvement activities (10.5)	5-1-1	2.6
			2.7
			2.7
		5-1-3	2.5
	5-2. Response to incidents of technology protection (recovery) (4.5)	5-2-1	0.5
			0.5
		5-2-2	0.5
			0.5
			0.5
			0.5
			0.5
			0.5
			0.5
Total			100

the attributes of the necessity of parent company to manage partners in manufacturing. We expect that this proposed model can help parent and partner companies to manage them (or themselves) securely in the manufacturing industry.

Academically, this study contributed to research considering the characteristics of life cycle and work process in detail when pursuing collaboration in the manufacturing industry. Furthermore, this study contributed to the analysis and design of the industrial process by reflecting a difference between a parent company and partners in the manufacturing industry. In practice, this study contributed to providing a framework of evaluation items and questions that can evaluate security levels of partners in the manufacturing industry with objective values by developing questions based on literature used in the industry.

By contrast, this study has a limitation in that the evaluation items were derived from the characteristics of the overall manufacturing industry to be uniformly applied to industries with diverse but distinctive characteristics, including semiconductors, displays, and automobiles in the manufacturing industry. In addition, an AHP pairwise comparison analysis was used to calculate the importance and weight only in the sub-category of evaluation areas and items, and an inconsistent weight analysis was conducted by calculating absolute importance using a five-point scale for evaluation-related questions, which are also the limitations of this study.

For follow-up studies in the future, we will evaluate whether the security level evaluation items of partners in the manufacturing industry, which were the deliverables of this study, will be applied to real industries, and whether security level evaluation items of partners will be developed by reflecting the features of the industry, specifying detailed sub-industries in the manufacturing industry. Moreover, we will conduct the development of items that can evaluate security levels of outsourcing companies, which reside in a company and perform tasks as another form of collaboration in the manufacturing industry.

7 Data availability statement

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Acknowledgements This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist).

Declarations

Conflict of interest The authors declared that they have no conflicts of interest to this work.

References

1. Vimal S, Jesuva AS, Bharathiraja S, Guru S, Jackins V (2021) Reducing latency in smart manufacturing service system using edge computing. J Platform Technol 9(1):15–22

2. Gul MJ, Rehman A, Paul A, Rho S, Riaz R, Kim J (2020) Blockchain expansion to secure assets with fog node on special duty. Soft Comput 24(20):15209–15221. https://doi.org/10.1007/s00500-020-04857-0
3. Smith R, Barry R (2019) America's Electric grid has a vulnerable back door – and russia walked through it. Wall Street J. https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112?mod=article_inline, Accessed 2022/06/02.
4. Deloitte, MAPI (2016) cyber risk in advanced manufacturing. United States of America
5. WIPO https://www.wipo.int/tradesecrets/en/, last accessed 2022.06.04.
6. Yu HR, Chang HB (2020) A meta-analysis of industrial security research for sustainable organizational growth. Sustainability 12(22):9526. https://doi.org/10.3390/su12229526
7. Gul MJ, Rabia R, Jararweh Y, Rathore MM, and Paul A. (2019). Security flaws of operating system against live device attacks: a case study on live linux distribution device. In: 2019 Sixth International Conference on Software Defined Systems (SDS), IEEE, pp 154–159
8. Khalil MI, Kim R, Seo CY (2020) Challenges and opportunities of big data. J Plat Tech 8(2):3–9
9. Lee JM (2013) Internal control management methodology designed for the industrial technology protection and leakage prevention: case studies on the improved security management system of the manufacturer's suppliers. Dissertation, Korea University
10. Kim IH, Lee KH (2017) Evaluation model of the contracting company's security management using the DEA model. J Korea Inst Inf Security Cryptol 27(3):687–704. https://doi.org/10.13089/JKIISC.2017.27.3.687
11. Kim JW, Lee CW, Chang HB (2020) The development of a security evaluation model focused on information leakage protection for sustainable growth. Sustainability 12(24):10639. https://doi.org/10.3390/su122410639
12. Noh SY, Lim JI (2017) A study for enterprise type realtime information security management system. J Korea Inst Inf Security Cryptol 27.3:617–636. https://doi.org/10.13089/JKIISC.2017.27.3.617
13. Ahn BG, Yu HR, Chang HB (2020) A research on activating factor for cultivating a proactive organizational security culture. Converg Security J 20(2):3–13. https://doi.org/10.33778/kcsa.2020.20.2.003
14. Bae ST, Kim JH (2013) A study on development of the evaluation model about level of security in national R&D program. J Korean Assoc Comput Educ 16(1):73–80
15. Wei YC, Wu WC, Chu YC (2018) Performance evaluation of the recommendation mechanism of information security risk identification. Neurocomputing 279:48–53. https://doi.org/10.1016/j.neucom.2017.05.106
16. Ministry of Trade, Industry and Energy, Korean Association for Industrial Technology Security (2017) Industrial technology protection guidelines and manuals. Korea.
17. Small and Medium Business Administration of Korea (SMBA), Large & Small Business Cooperation Foundation Korea, Rural Affairs (2016) SME technology protection guidelines. Korea.
18. Ministry of Science and ICT (2014). National R & D Business Security Management Standard Manual. Korea
19. Korea Industrial Technology Association, Small and Medium Business Administration (SMBA), Korea Technology and Information Promotion Agency for SMEs (2007). Manual to respond to technology leakage for SMEs. Korea.
20. Mullet V, Sondi P, Ramat E (2021) A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access 9:23235–23263. https://doi.org/10.1109/ACCESS.2021.3056650
21. Johansson K, Paulsson T, Bergström E, Seigerroth U (2022) Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry. In: SPS2022. IOS Press, Amsterdam, pp 209–220. https://doi.org/10.3233/ATDE220140
22. Corallo A, Lazoi M, Lezzi M, Pontrandolfo P (2021) Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. IEEE Trans Eng Manage. 1109/TEM.2021.3084687
23. Saaty TL, Vargas LG (2012) The seven pillars of the analytic hierarchy process. In: Models, methods, concepts and applications of the analytic hierarchy process. Springer, Boston, MA, pp 23–40
24. Korea Development Institute (2008) Study on Modification and improvement of general guidelines to perform preliminary feasibility study, the 5th edn. Korea
25. Kim DG, Park YW, Lee SM (2007) Assessment of tourism resource development by the analytic hierarchy process: focusing on the planning process. Int J Tour Hosp Res 21:5–18

26. Saaty TL (2008). Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors in the analytic hierarchy/network process. RACSAM-Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas, 102(2):251–318. https://doi.org/10.1007/BF03191825
27. Chen X, Chen R, Yang C (2022) Research to key success factors of intelligent logistics based on IoT technology. J Supercomput 78(3):3905–3939. https://doi.org/10.1007/s11227-021-04009-7