Human-centric Computing and Information Sciences

July 2022 | Volume 12

www.hcisjournal.com

KIPS Korea Information Processing Society

KIPS CSWRG Korea Information Processing Society Computer Software Research Group

HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) Open Access

Human-centric Computing and Information Sciences (2022) 12:33
DOI: https://doi.org/10.22967/HCIS.2022.12.033
Received: September 9, 2021; Accepted: April 7, 2022; Published: July 30, 2022

The Impact of Enterprise Security Performance on Business Performance in Industrial Convergence Environment

Eunhee Shin[1], Harang Yu[2], Sungyun Bae[2], and Hangbae Chang[3,*]

Abstract

In recent industrial convergence environment where environment changes rapidly with continuous technology development, the needs for management system of sprawled data, network, etc., is increasing in order to higher the efficiency. Moreover, along with an increasement in telecommuting, securing intelligent and trusted networks has become one of the major assignments for organizations, aiming a secured connectivity. While strong security is being emphasized on managing data, networks, etc., by utilizing diverse technical solution along with artificial intelligence, machine learning, it is to be no use if appropriate evaluation is not performed for corresponding security activities. Currently, a numerous organization is focusing on technical development and put secured approach as a priority, however, fails to conduct an evaluation on corresponding activities which can lead to severe security threats, causing a failure of maintaining a sustainable, human-centric computing environment and ultimately threats business performance. This paper intends to confirm security evaluation as a business strategy and moreover, raise awareness on security performance evaluation which can results in effective intelligent network management, and secured computing environment, enabling a secured and sustainable industrial convergence environment.

Keywords

Enterprise Security Performance, Business Performance, Security Management, Security Evaluation, Industrial Convergence Environment

1. Introduction

Technologies are constantly being developed and growing, making industrial environments go through a continuous change. Crucial information and communication technologies (ICT) such as artificial intelligence, machine learning, the Internet of Things (IoT), etc. has led to escalation of sensor technology, geolocalization, etc., and is being competitively developed by companies. Among these cutting-edge technologies, IoT innovated industry process [1] and fostering a new smart devices and application in 5G environment [2]. Blockchain technology is also widely utilized to develop business

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
***Corresponding Author:** Hangbae Chang (hbchang@cau.ac.kr)
[1]Korea Security Evaluation Corp., Seoul, South Korea
[2]Department of Security Convergence, Chung-Ang University, Seoul, South Korea
[3]Department of Industrial Security, Chung-Ang University, Seoul, South Korea

models in expectancy of enabling advanced methods of conducting economic activities in diverse field [3, 4]. These innovative technologies offer both industry and end-users convenient working environment [5–7]. However, this also indicates working environment is gradually transitioning to telecommuting [8, 9], a remote working environment which can result in data sprawl, posing a diverse and potential security threat to organization [10]. In 6G environment, security threats such as breach of privacy and confidentiality, etc., can occur [11, 12]. Moreover, security risks including data leakage during the process of data mining, which handles an actively sharing data [13] due to a characteristics of ICT-based environment which tends to be connected to each other for example, controlled under heterogeneous network or management system, or operated under decentralized account, etc. which all can result in presenting potential security vulnerabilities [14]. Accordingly, urgent needs for security in current environments is continuously increasing [15, 16] and countermeasure against potential security threats on massive data is actively discussed to protect organizations' security [17], since severe security threat can affect an existence of organization. These industrial environments made security, an act of protecting an asset, an essential business management strategy for both countries and companies, to survive and gain a profit from new business opportunities [18–20]. Although the importance of security is widely known, organization have difficulties in relating security performance with business level, since security performance is evaluated only by the reduction rate of security incidents or the implementation rate of annually planned projects. To this day, a number of organizations do not require security performance as performance evaluation since it is considered to have less economic effect on business performance and management [21]. Moreover, in globalized business environment, it is inevitable for organizations to avoid collaborating with one another. Therefore, it is necessary to makes companies perceive security as a key element of management, as a business strategy and value that should be evaluated in order to maintain a sustainable business growth in industrial convergence environment.

In this study, security is regarded as a way of creating new business opportunities including a concept of strategic value [22]. This study intends to establish a research model which can identify correlation between enterprise security performance and business performance as a way of raising an awareness of security as business strategic value.

2. Literature Review

2.1 Business Performance in Industrial Convergence Environment

In industrial convergence environment, data sharing, collaboration, telecommuting, inter-organizational system or management, etc., appears commonly and inevitable for business organizations. Especially, as mentioned above, crucial technologies representing ICT environment is being operated under either centralized or decentralized system, making secured protection of organizations' asset important. Moreover, new technology and services lead to creating economic benefits which contributes to expanding business performance. Robey et al. [23] conducted a theoretical study on adopting an inter-organizational systems and Fig. 1 shows a relationship in the process of adopting inter-organizational working system. Readiness level, degree of collaboration, and following business performance has correlation relationships which enables automated information management system to safely share and cooperate with each departments/division. As shown in readiness level with detailed indicators, each item is proactively conducted, continuously evaluate, monitor, etc., in order to perform a well-prepared work task and put up a high business performance [23]. Meanwhile, business performance can be shown in many different forms since it is determined by its organization but mostly refers to benefits that can lead organizations to better and sustainable business. Although detailed items for evaluating business performance is developed, indicators from the security perspective are not included as a way of business strategy. Absence of security performance can cause diverse security threats. As the importance of security increases, it is essential for both academic and working field to establish a related model specifying an impact and relationship between security performance and business performance.

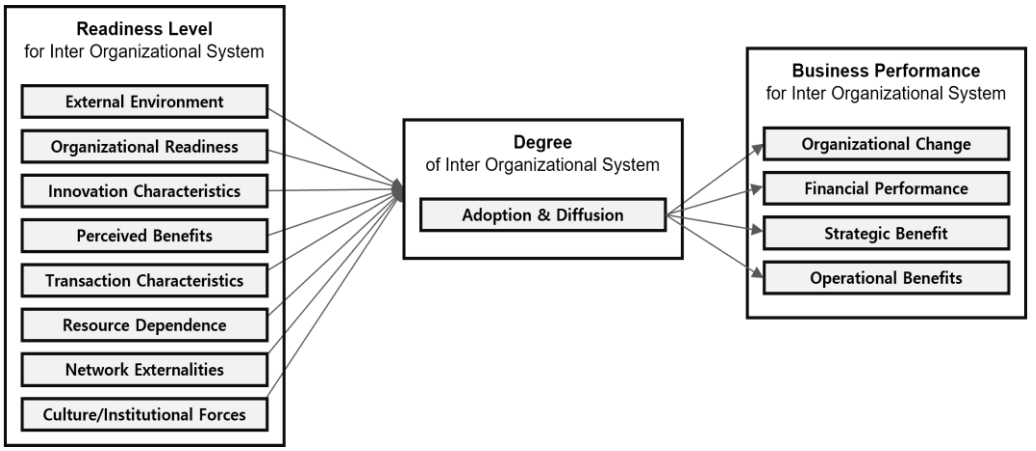

Fig. 1. Relationships in inter-organizational adoption process. Adapted from [23] (edited for summarization).

2.2 Performance Management and Business Performance

Defining performance can be widely varied by situation, subject, and purpose. In this study, performance mainly refers to business purpose and relevant activities set by organization. The term "performance" includes not only a financial evaluation indicator, which used to be a core value, but also include intangible assets such as technology, intellectual property, etc. Due to limitation of existing business value evaluation, new concept of performance management was introduced.

Performance management has several different concepts as well, such as "setting strategic goals and performance, designing, and implementing the project" [24], also refer to as "act of goal setting, indicator developing, measuring a performance, providing feedback, etc., that can systematically manage individual and organizational tasks and provide information for decision-making" [25]. It was also studied that conducting performance evaluation have a higher performance result than organizations that has no certain preparation [26]. Performance management also benefits public sector where business goal such as profits do not exit and can contribute to enhancing social responsibility by focusing on general perspective [27, 28].

2.3 Balanced Scorecard Model and Security Evaluation

In rapidly changing industry, especially manufacturing industry, organizational performance is mainly accomplished by production activity based on a performance of research and development which lead to organizational performance. As research and development performance gain improvement in such as quality, new product development, technology development, production process innovation, etc., security will take crucial part and achieve higher security performance.

One of the most well-known examples of performance management model is balanced scorecard (BSC) model. It is introduced to act a role such as decision-making for organizational structure, assigning responsibility, system setting for performance evaluation and supplementing the performance [29]. BSC model focus on organizations' vision and strategy from four different perspectives and emphasize the importance of business strategy: finance, customer, internal business process, and learning and growth [30] as shown in Fig. 2. BSC model consider both financial and non-financial goals to balance the performance and evaluate not only an internal issue but also an external issue. It also can be related to long-term business goals followed by business strategy [31] and supports establishing and sharing an opinion within organizations [32].

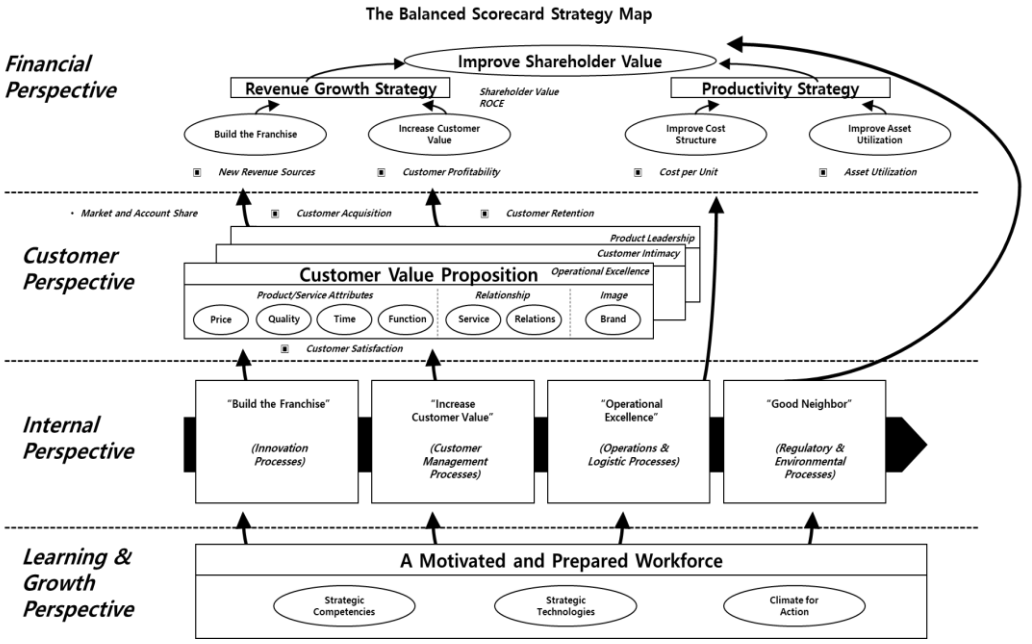

Fig. 2. Four perspectives and strategy map in balanced scorecard (BSC).

2.4 Security Performance and Indicators

Security performance as a term should be preemptively defined for conceptual definition in both academic and in business work field. If business performance refers to the amount of business' achieved ultimate goal, security performance is about measurement of the goal or goal to be achieved by conducting security activities. According to prior studies, corporate security performance is defined as "achieving a specified goal while maintaining a state of protecting individual or organizational performance from risk, loss and crime" [33].

To measure security performance, required indicators are widely have been studied in various fields. Response time after conducting a mock hacking is also analyzed to measure the security performance regarding the level of quick response in case of security incident [34]. Lee [35] analyzed the asset by the degree and rating for security policy. Research on the range and effectiveness in implementing a security education was also conducted in order to effectively utilize security performance [36]. Additionally, Kang and Chang [37] analyzed a competitive advantage, customer satisfaction, public image, information security stability and reliability, and work security applicability as an indicator.

3. Research Methodology

3.1 Research Procedure

This study desires to analyze correlation between enterprise security performance and business performance to increase the awareness of the importance of recognizing security as business management. In order to establish final research model, following process was conducted. Traditional definition of business performance, security activities and performance is analyzed beforehand. First step is to conduct literature review, and analysis on prior studies regarding business performance, relationships between security performance and business performance was conducted. Then, to draw

appropriate indicators for research model, studies regarding BSC model and security evaluation were conducted. Moreover, security performance and indicators that are currently performed in industry is analyzed. For second step, in order to design research model, Focused Group Interview (FGI) was conducted after establishing an operational definition and organizing a performance measurement items. In this process, hypothesis and survey questionnaire were designed for performance measurement items. Next step was to verify the results which includes reliability verification, statistical verification, regression analysis and testing differences between groups. Fig. 3 briefly shows a research procedure of this research.

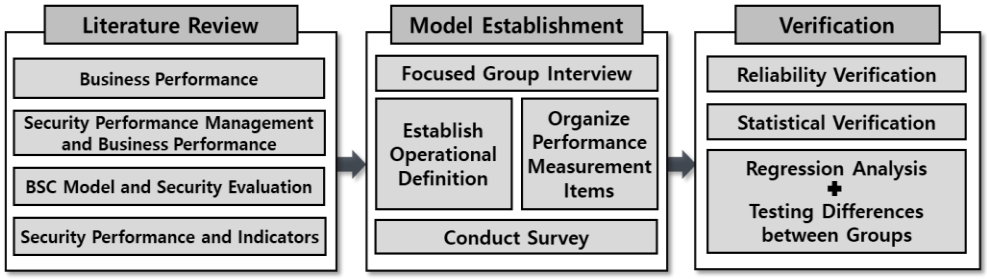

Fig. 3. Research procedure.

3.2 Research Model Establishment

3.2.1 Operational definition and applicable scope of terms

The term “business performance” is frequently used in diverse organizations in order to evaluate their economic goal, the term “security performance” is far less known when it comes to performance evaluation. The term “security performance” is used separately from “business performance” in this paper due to the fact that security is unrecognized as vital task to be associated with business strategy. Although security nowadays is considered as one of the business activities in lot of organizations, “security performance” is not regarded as an essential activity which requires performance evaluation and sometimes considered as a task to perform only in case of particular security incident occurs, settling security as a separate activity to perform from business management performance. As can be seen in such cases, “security performance” and “business performance” is used separately in this paper.

In order to prevent this confusion in the use of existing terminology and bring awareness, FGI was conducted for the purpose of defining an operational term. Literature reviews on performance indicators regarding business performance and security performance was conducted and then, FGI method was established into three steps. Variables for each business performance and security performance were primarily analyzed based on literatures. Secondly, interview targeting three security experts was done in order to draw indicators. During this process, performance indicators of similar characteristics were grouped together based on BSC model [29]. Lastly, FGI targeting three organization managers was done in order to confirm and revise a drawn item. By conducting FGI, this study established an operational definition of business performance and security performance and contributed to raising an awareness of recognizing security performance as essential activity in the working field. Each operational definition of security performance and business performance is as follows:

- Business performance: Creating profits and the degree of achieving a goal settled toward it. In this study, security performance is not included in business performance.
- Security performance: Degree of goal achievement accomplished through security activities.

FGI also resulted in deriving performance indicators for both business and security which is shown in Table 1.

Table 1. Business performance and security performance indicators based on literature review

Business performance		Security performance	
Sales	Increasing customer	Personnel	Access control
Net profit	Customer loyalty	Willingness toward security	Security guard (facility)
Market share	Customer retention	Security awareness level	Information system protection
Positive image	Reputation	Compliance level	Countermeasure (security incident)
Social reliability		Policy	

3.2.2 Research model factors

This study intends to analyze the relation of the security activities performance and business performance. Hypothesis written below begins with the assumption that the higher the enterprise security activity and security level, the higher the enterprises' business performance and the customer satisfaction and financial performance. Moreover, in case of manufacturing companies, the level of production division's security performance depends on the presence of organizational performance of R&D division. According to manufacturing value chain, production activities occur based on R&D performances, which eventually lead to growth of business performance. New technology, innovative production process, etc., would lead to more active production work activities, requiring higher level of security. According to the assumptions mentioned above, two hypotheses to be verified in this research was established.

- Hypothesis 1: Depending on the presence or absence of the R&D organizational performance, the production division department's security performance will be different.
- Hypothesis 2: Depending on the presence or absence of the enterprise's (major) security performance, the level of enterprise business management performance will be different.

Based on the established hypothesis, each performance indicators were reviewed by three security managers of large corporations who are actively engaged in R&D, manufacturing, and security departments/divisions in order to derive appropriate final performance measurement items. The final questionnaire of the survey based on indicators drawn above (Table 1) was finally organized as Table 2, after confirming a composition, expression, vague definition, and responsiveness of questions. For example, variable "policy" in security performance, refers to policy regarding protecting and securing technology and information and therefore, named as "Technology · Information Protection Policy" as can be seen in Table 2.

Table 2. Final performance measurement items

Variable	Performance item
Security performance	Technology · Information Protection Policy
	Security Organization · Personnel
	Information System Protection
	Access Control · Facility Protection
	Business Executives' Willingness toward Security
	Employees' Security Awareness Level
Business performance	
Financial performance	Sales
Customer performance	Customer Loyalty
	Market Share
	Social Reliability and Image

Based on the established security performance and business performance items, survey was done to get results of current status of security performance in manufacturing company engaged in both R&D, production, and security activities. Among these enterprises, subject with team unit or higher of R&D and security was determined as a target company. For Employees, survey was limited to employees who had capability to answer the survey questions regarding a performance of each business unit and

management of the company. Total of 138 data were collected in the first round and 113 data was shown as valid in final after removal of insincere, repetitive responses.

4. Research Results

4.1 Statistical Verification

This study intends to design a research model on correlation between enterprise security performance and business performance and made a hypothesis. Reliability verification for variable items and descriptive statics of the scale items were primarily conducted and then, the differences between groups was analyzed. Data collected from survey, reliability analysis, descriptive statics was analyzed by utilizing SPSS (Statistical Package for Social Sciences) as well as SPSS Amos, both in version 22 for Windows. SPSS is a world widely used analytic program for social science researchers and is divided into three products which are SPSS Statistics, SPSS Modeler, and SPSS Amos. SPSS Statistics supports planning for data analysis, data collection and whole process of creating a report. SPSS Modeler is a professional data mining tool for establishing hypothesis and prediction modeling. SPSS Amos assists verifying hypothesis of relations between variables by using structural equation modeling method and used in this research. Survey results are converted into SPSS for data analysis. In this research, statistical verification applies 95% confidence interval ($p<0.05$).

Firstly, reliability verification of the data was conducted. Reliability is referred as the value that is obtained identically even after repeated surveys [38–40], mostly by utilizing an internal consistency through Cronbach's α [38, 40]. It has a numeral value from 0 to 1, and the higher the value, the higher the reliability. Generally, 0.8 or higher is considered as high or non-problem with internal consistency [40, 41]. In this study, 0.8 is adopted as the standard value. The value of Cronbach's α coefficient was high which was 0.868 and confirmed that collected data in this study verified high internal consistency. Table 3 shows a result of descriptive statistic. Every variable excepts "Sales" had average of more than 4, and "Information System Protection" had the highest average score which indicates current manufacturing companies' well-structured protection level of information system.

Table 3. Descriptive statistic results

Variable	Average	Standard deviation
Sales	3.83	1.652
Market Share	4.20	1.087
Customer Loyalty	4.28	1.004
Social Reliability and Image	4.50	1.111
Technology · Information Protection Policy	4.59	1.074
Security Organization · Personnel	4.65	1.092
Information System Protection	5.00	1.009
Access Control · Facility Protection	4.62	1.160
Business Executives' Willingness toward Security	4.78	1.193
Employees' Security Awareness Level	4.63	1.037

To verify hypothesis suggested in this research, analyzing on one-to-one influential between each variable was considered to be effective and the most representative method of analyzing correlation between dependent and independent variables is simple linear regression analysis. Simple linear regression is used to assure the linear relation between dependent and independent variable and examines an existence of autocorrelation, which refers to validating an independency of residual. The formula of simple linear regression is shown below when X (independent variable) and Y (dependent variable) is a linear relationship. β_0 refers to the predicted value of Y when the X is given as 0, β_1 is the regression

coefficient which shows how much Y transform as X changes and ε refers to the error of predicting the value.

$$y = \beta_0 + \beta_1 x + \varepsilon$$

In this study, simple linear regression analysis conducted through SPSS with Durbin-Watson (D-W) statistic in order to verify independency of residual and confirm availability of linear regression analysis for both dependent and independent variable. The value of d is drawn from Durbin-Watson statistic and examines the existence of autocorrelation and the formula is shown below. It is calculated by the size of specimen and the number of independent variables.

$$d = \frac{\sum_{t=2}^{n}(e_t - e_{t-1})^2}{\sum_{t=1}^{n} e_t{}^2}$$

If regression analysis is disapproved in D-W statistic, Independent Samples T-test on the difference between groups is conducted. T-test refers to verifying homoscedasticity and then verify the T value which show differently by the verification result. Homoscedasticity means dispersion of dependent variable's value being consistent and is evaluated by Levene' test verification.

For verification of Hypothesis 1, regression analysis between two variables were conducted. The D-W value was 1.344 and failed to fall within the range of 1.7–2.3, which means that the autocorrelation between errors exists. Therefore, regression analysis for Hypothesis 1 was inappropriate which led to testing differences between groups. Groups were divided by the presence and absence of R&D performance. "Business with R&D performance" group was determined by the survey result which had exceeded median score 4 among 7-point Likert scale. In order to confirm average differences between two group, Levene's test verification was conducted. T value resulted in 3.424, which is significant under the 95% confidence interval, confirming that the difference of security level does exist between business that has R&D performance and that does not. This shows that depending on presence or absence of target to protect, security activities occurs and result in security performance. Moreover, in the respect of correlation between R&D and production based on value chain in manufacturing industry, production division of business retaining R&D performance which contributes to business performance gets influenced by security level, it reflects that security performance has impact of growing business performance. Table 4 summarizes a result of statistical verification.

Table 4. Security level difference of production department depending on R&D organizational performance (T-test)

Group	Levene's test verification			T-test result				
	F	p-value	Test result	Levene's test result	t	df	p-value	Test result
Business with R&D Performance	3.669	0.058*	ANOVA (statistically significant)	ANOVA (statistically significant)	3.24**	111	0.001***	Adopted
Business with no R&D Performance				Statistically NOT significant	3.793	107.474	0.000	-

*p<0.05, **p<0.01, ***p<0.001.

Regarding Hypothesis 2, enterprise security performance security performance and business performance, D-W statistic was also conducted. Among six security performance indicators and four business performance indicators, only three regression formula were approved to fall within D-W value of 1.7–2.3. However, the main purpose of this research is to confirm on the enterprise security performance and business performance, which led to conducting differences between groups after dividing groups by the existence of security performance in organizations. Accordingly, T-test was also

conducted between six enterprise security performance and business performance. Table 5 briefly shows the results of differences between groups. It reflects that "Sales," one of business performance variable, is influenced by enterprise security performance such as "Technology · Information Protection Policy", "Security Organization · Personnel," "Business Executives' Willingness toward Security," and "Employees' Security Awareness Level." "Reliability and Image" and "Market Share" is significantly influenced by entire enterprise security performance, while "Customer Loyalty" is impacted by "Business Executives' Willingness toward Security," "Employees' Security Awareness Level." This reflects that business performance executed in organizations has significant influence on improving business performance.

Table 5. Verification result: business performance followed by enterprise security performance

Dependent variables	Independent variables					
	Technology ·Information Protection Policy	Security Organization · Personnel	Information System Protection	Access Control · Facility Protection	Business Executives' Willingness toward Security	Employees' Security Awareness Level
Sales	Adopt	Adopt	Dismissal	Dismissal	Adopt	Adopt
Market Share	Adopt	Adopt	Adopt	Adopt	Adopt	Adopt
Customer Loyalty	Dismissal	Dismissal	Dismissal	Dismissal	Adopt	Adopt
Reliability and Image	Adopt	Adopt	Adopt	Adopt	Adopt	Adopt

4.2 Final Research Model

Table 6. Literature review for final research model

Study	Year	Title
Joyce [27]	1993	Using performance measures for federal budgeting: proposals and prospects
Lingle and Schiemann [26]	1996	From balanced scorecard to strategy gauge: is measurement worth it?
Kaplan and Norton [31]	1998	Balanced performance management indicator BSC
Kaplan and Norton [30]	2001	Transforming the balanced scorecard form performance measurement to strategic management: part I
Koh et al. [24]	2004	The performance management of public institutions
Robey et al. [23]	2008	Theoretical foundations of empirical research on inter organizational systems: assessing past contributions and guiding future directions
Alfawaz et al. [34]	2010	Information security culture: a behavior compliance conceptual framework
Siponen et al. [36]	2010	Compliance with information security policies: an empirical investigation
Lee [35]	2011	A study on the influential factors for the security policy
Jung et al. [33]	2015	The study on industrial security system effect on security performance
Kang and Chang [37]	2016	The influence of information security behaviors on information security performance in shipping and port organization
ACCA [32]	2017	P5 Advanced performance management
Hwang and Yoon [25]	2018	Improving government performance indicators II: focusing on the field of diplomacy and security
Lee and Lee [28]	2018	An analysis of the production and use of performance information in the Korean National Police Agency: the perspective of effective performance measures
Kaplan Financial Knowledge Bank [29]	2020	Performance management

This study aims to raise awareness on the lack of security perspective of business strategy and empirically conduct research to verify correlation between enterprise security performance and business performance. Accordingly, a research question was raised by analyzing a business performance and relevant factors in recent environment and went through basic concept of security performance management briefly. Then, to secure enterprise security performance as one of the main business strategies to accomplish its business goal, performance evaluation should be equally conducted just like other work tasks which led to analyzing a BSC model and relevant works. Lastly, literature review on indicators for research model was conducted. Table 6 summarizes relevant studies for research model.

Fig. 4 shows a final research model which reflects correlation between enterprise security performance and business performance. Lined arrow indicates in detail, “Technology · Information Protection Policy” which has a characteristic of administrative security, and “Security Organization and Personnel” which has a characteristic of security governance performance, significantly effect on business performance except customer loyalty. “Information System Protection” and “Access Control · Facility Protection” which has a characteristic of technical security and physical security, have significant influence on business performance except “Customer Loyalty,” “Sales.” It was shown that “Business Executives’ Willingness toward Security” and “Employees’ Security Awareness Level” from enterprise security performance had influenced all four of business performance.

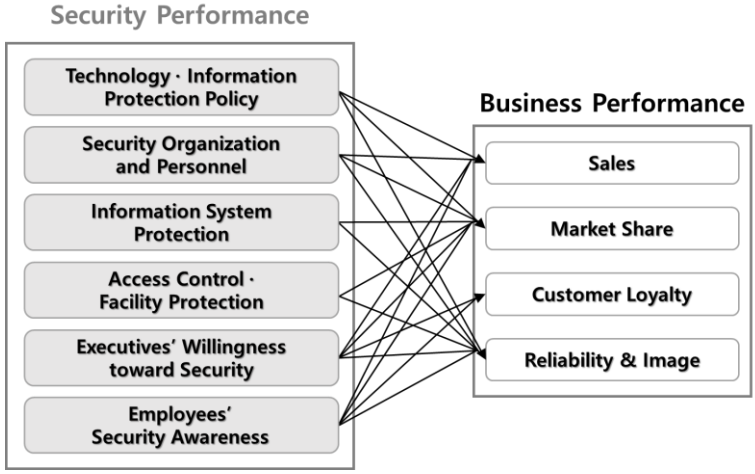

Fig. 4. Final research model.

5. Conclusion

Industrial environment is changing speedily with innovative technologies continuously being developed and global competition regarding knowledge, technology, etc., deepens. Security incidents such as technology leakage, data breach, etc., on core assts including manpower, new technology, etc., is constantly happening. Corporates nowadays have relatively high awareness toward security, however, in work field, a number of organizations still handle security as secondary, or have difficulties in dealing with security budget, investment, etc. This status led to lack of security-perspective of readiness level or evaluation which can cause random, unprepared security threats.

Therefore, this paper aims to design a research model reflecting a correlation between enterprise security performance and business performance. Based on literature reviews, FGI conducted regarding a security and business performance indicator and surveys on security performance and business performance targeting security experts who have more than three years of work experience. Then, statistical verification was performed to support the validation of data. It was shown that enterprise security performance which consists of six indicators have significant correlation with business performance.

This paper is expected to contribute to providing new perspective toward security. While prior literatures focused on security activities such as corporates' changes in value in short term in accordance with security incidents or countermeasures after an outbreak of security incidents by analyzing security certification, etc., will somehow affect its value awareness, this study differentiates its contribution in finding out that security activity has positive impacts on business performance and how each security performances are related to business performance which enables organizations to have better access on setting a sustainable security strategy in accordance with its own business goal. Moreover, rather than recognizing it as a "cost," security can be regarded as an act of "investing," such as perform more security activities, improve security performance, conduct evaluation, etc., which will return in as a grown business performance, enabling a sustainable business environment. The limitation of this study is that the research was done targeting manufacturing industry. Due to timely characteristic of security and future work environment where everything changes rapidly can lead to new types of environments. Security threats will always occur in many different types and ways, regardless of under any circumstances. To proactively countermeasure an unexpected future security threats, a way to establish an appropriate security performance in different environments should be studied for future work.

Author's Contributions

Conceptualization, ES, HC, Investigation and methodology, ES, HY, SB, Data Curation, ES, Writing of the original draft, ES, HY, Writing of the review and editing, ES, HY, HC, Supervision, HC. All the authors have proofread the final version.

Funding

This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (No. P0008703, The Competency Development Program for Industry Specialist).

Competing Interests

The authors declare that they have no competing interests.

References

[1] A. Maryam, U. Ahmed, M. Aleem, J. C. W. Lin, M. Arshad Islam, and M. A. Iqbal, "cHybriDroid: a machine learning-based hybrid technique for securing the edge computing," *Security and Communication Networks*, vol. 2020, article no. 8861639, 2020. https://doi.org/10.1155/2020/8861639

[2] Y. Djenouri, G. Srivastava, A. Belhadi, and J. C. W. Lin, "Intelligent blockchain management for distributed knowledge graphs in IoT 5G environments," *Transactions on Emerging Telecommunications Technologies*, vol. 2021, article no. e4332, 2021. https://doi.org/10.1002/ett.4332

[3] J. Weking, M. Mandalenakis, A. Hein, S. Hermes, M. Bohm, and H. Krcmar, "The impact of blockchain technology on business models: a taxonomy and archetypal patterns," *Electronic Markets*, vol. 30, no. 2, pp. 285-305, 2020.

[4] D. Kimani, K. Adams, R. Attah-Boakye, S. Ullah, J. Frecknall-Hughes, and J. Kim, "Blockchain, business and the fourth industrial revolution: whence, whither, wherefore and how?," *Technological Forecasting and Social Change*, vol. 161, article no. 120254, 2020. https://doi.org/10.1016/j.techfore.2020.120254

[5] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, 2019.

[6] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "A sequential scheme for detecting cyber attacks in IoT environment," in *Proceedings of 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data*

Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 2019, pp. 238-244.

[7] D. Sehrawat and N. S. Gill, "Smart sensors: analysis of different types of IoT sensors," in *Proceedings of 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2019, pp. 523-528.

[8] K. Stalmachova, R. Chinoracky, and N. Strenitzerova, "Changes in business models caused by digital transformation and the COVID-19 pandemic and possibilities of their measurement: case study," *Sustainability*, vol. 14, no. 1, article no. 127, 2021. https://doi.org/10.3390/su14010127

[9] Y. K. Dwivedi, D. L. Hughes, C. Coombs, I. Constantiou, Y. Duan, J. S. Edwards, et al., "Impact of COVID-19 pandemic on information management research and practice: transforming education, work and life," *International Journal of Information Management*, vol. 55, article no. 102211, 2020. https://doi.org/10.1016/j.ijinfomgt.2020.102211

[10] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Working from home during COVID-19 crisis: a cyber security culture assessment survey," *Security Journal*, vol. 35, no. 2, pp. 486-505, 2022.

[11] J. C. W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, "Privacy-preserving multiobjective sanitization model in 6G IoT environments," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5340-5349, 2020.

[12] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195-202, 2020.

[13] J. C. W. Lin, P. Fournier-Viger, L. Wu, W. Gan, Y. Djenouri, and J. Zhang, "PPSF: an open-source privacy-preserving and security mining framework," in *Proceedings of 2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, Singapore, 2018, pp. 1459-1463.

[14] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-centric Computing and Information Sciences*, vol. 10, article no. 9, 2020. https://doi.org/10.1186/s13673-020-0214-5

[15] L. Megouache, A. Zitouni, and M. Djoudi, "Ensuring user authentication and data integrity in multi-cloud environment," *Human-centric Computing and Information Sciences*, vol. 10, article no. 15, 2020. https://doi.org/10.1186/s13673-020-00224-y

[16] J. Y. Park and E. N. Huh, "A cost-optimization scheme using security vulnerability measurement for efficient security enhancement," *Journal of Information Processing Systems*, vol. 16, no. 1, pp. 61-82, 2020.

[17] H. He, L. H. Zheng, P. Li, L. Deng, L. Huang, and X. Chen, "An efficient attribute-based hierarchical data access control scheme in cloud computing," *Human-centric Computing and Information Sciences*, vol. 10, no. 49, 2020. https://doi.org/10.1186/s13673-020-00255-5

[18] H. Chang, "A study on the countermeasure by the types through case analysis of industrial secret leakage accident," *Convergence Security Journal*, vol. 15, no. 7, pp. 39-45, 2015.

[19] E. G. Booz, J. L. Allen, and C. L. Hamilton, "Convergence of enterprise security organization," in *ASIS International Conference*. Alexandria, VA: The Alliance for Enterprise Security Risk Management, 2005.

[20] PricewaterhouseCoopers, "Convergence of security risks," 2010 [Online]. Available: https://gisf.ngo/wp-content/uploads/2014/09/0254-PriceWaterhouseCoopers-et-al-2010-Convergence-of-Security-Risks.pdf.

[21] G. Campbell, *Measures and Metrics in Corporate Security*. San Diego, CA: Elsevier, 2014.

[22] C. S. Park, "Industrial security ecosystem trend and policy: approach towards innovation system," 2020 [Online]. Available: http://www.kais.or.kr/notice/view.php?idx=6167&page=1search=&find=.

[23] D. Robey, G. Im, and J. D. Wareham, "Theoretical foundations of empirical research on interorganizational systems: assessing past contributions and guiding future directions," *Journal of the Association for Information Systems*, vol. 9, no. 9, pp. 497-518, 2008.

[24] Y. S. Koh, H. S. Yoon, and J. H. Lee, "The performance management of public institutions," 2004 [Online]. Available: https://www.kdi.re.kr/research/subjects_view.jsp?pub_no=8906.

[25] H. S. Hwang and S. J. Yoon, "Improving government performance indicators II: focusing on the field of diplomacy and security," 2018 [Online]. Available: https://www.kipa.re.kr/site/eng/research/selectBasicView.do?seqno=302.

[26] J. H. Lingle and W. A. Schiemann, "From balanced scorecard to strategy gauge: is measurement worth it?," *Management Review*, vol. 85, no. 3, pp. 56-61, 1996.

[27] P. G. Joyce, “Using performance measures for federal budgeting: proposals and prospects,” *Public Budgeting & Finance*, vol. 13, no. 4, pp. 3-17, 1993.
[28] J. C. Lee and J. W. Lee, “An analysis of the production and use of performance information in the Korean National Police Agency: the perspective of effective performance measures,” *The Korean Association of Police Science Review*, vol. 20, no. 3, pp. 267-304, 2018.
[29] Kaplan Financial Knowledge Bank, “Performance Management,” 2020 [Online]. Available: https://kfknowledgebank.kaplan.co.uk/management-accounting/performance-management.
[30] R. S. Kaplan and D. P. Norton, “Transforming the balanced scorecard from performance measurement to strategic management: Part 1,” *Accounting Horizons*, vol. 15, no. 1, pp. 87-104, 2001.
[31] R. S. Kaplan and D. P. Norton, *Balanced Performance Management Indicator BSC*. Seoul: Han-eon, Seoul, 2014.
[32] BPP Learning Media, “ACCA P5 Advanced Performance Management,” 2017 [Online]. Available: https://play.google.com/books/reader?id=6_0uDwAAQBAJ&hl=ko&pg=GBS.PA635.
[33] S. B. Jung, J. S. Park, and Y. H. Choi, “The study on Industrial security system effect on security performance,” *Korean Police Studies Review*, vol. 14, no. 4, pp. 521-538, 2015.
[34] S. Alfawaz, K. Nelson, and K. Mohannak, “Information security culture: a behaviour compliance conceptual framework,” in *Information Security 2010: AISC'10 Proceedings of the Eighth Australasian Conference on Information Security*. Sydney, Australia: Australian Computer Society, 2010, pp. 51-60.
[35] C. H. Lee, “A study on the influential factors for the security policy,” Ph.D. dissertation, Department of Public Administration, Kyungwon University, Seongnam, South Korea, 2011.
[36] M. Siponen, S. Pahnila, and M. A. Mahmood, “Compliance with information security policies: an empirical investigation,” *Computer*, vol. 43, no. 2, pp. 64-71, 2010.
[37] D. Y. Kang and M. H. Chang, “The Influence of information security behaviors on information security performance in shipping and port organization,” *Journal of Navigation and Port Research*, vol. 40, no. 4, pp. 213-222, 2016.
[38] D. R. Cooper and P. S. Schindler, *Business Research Methods*, 12th ed. New York, NY: McGraw-Hill, 2014.
[39] C. H. Cho, *Statistical Analysis of Structural Equation Models using SPSS/AMOS*, 2nd ed. Seoul, Korea: Cheongram, 2016.
[40] G. S. Kim, *Amos 18.0 Structural Equation Modeling Analysis*. Seoul, Korea: Hannarae, 2010.
[41] S. H. Cho and S. H. Kim, "Suggestion for collaboration-based UI/UX development model through risk analysis," *Journal of Information Processing Systems*, vol. 16. no. 6, pp. 1372-1390, 2020.