information

MDPI

Article

The Effective Factors on Continuity of Corporate Information Security Management: Based on TOE Framework

Yongho Kim and Boyoung Kim *

Seoul Business School, Seoul School of Integrated Sciences and Technologies (aSSIST), Seoul 03767, Korea; felix@stud.assist.ac.kr

* Correspondence: bykim2@assist.ac.kr; Tel.: +82-70-7012-2728

Abstract: In the Fourth Industrial Revolution era, data-based business management activities among enterprises proliferated are mainly based on digital transformation. In this change, the information security system and its operation are emphasized as essential business activities of enterprises the research aims to verify the relationship among the influence factors of corporate information security management based on the TOE framework. This study analyzes the effects of technical, organizational, and environmental factors on the intention, strengthening, and continuity of information security management. To this, a survey was conducted on professional individuals who are working in areas related to information security in organizations, and 107 questionnaires were collected and analyzed. According to major results of the analysis on adopted hypotheses. In results, as to the intention of information security management, organization and environment factors were influential. In the other side, technology and environment factors were affected to the strengthening of information security management. Hence this study pointed out that the environmental factors are most significant for the information security administration of an organization. In addition, it turned out that the strengthening of information security management was influential on the continuity of information security management more significantly than the intention of information security management.

Keywords: information security management; information protection; TOE framework; continuity

Citation: Kim, Y.; Kim, B. The Effective Factors on Continuity of Corporate Information Security Management: Based on TOE Framework. *Information* **2021**, *12*, 446. https://doi.org/10.3390/info12110446

Academic Editor: Sokratis Katsikas

Received: 14 October 2021
Accepted: 25 October 2021
Published: 27 October 2021

1. Introduction

Disastrous situations such as natural disasters and the COVID-19 pandemic, which are hardly expected, extend over a long period, and most enterprises pay keen attention to the contact-focused business environment. Particularly in the Fourth Industrial Revolution era, data-based business management activities among enterprises proliferated mainly based on digital transformation, from big data to IoT, AI, and cyber currency. In these backgrounds the information security system and its operation are emphasized as essential factors for business activities among enterprises [1].

Information security activity in organization is regarded as one of the critical business administration activities among business entities for maintaining and operating relevant laws and institutions and for substantial alleviation of legal and financial risks [2]. Furthermore, highly advanced technology—innovative models such as secondary cell batteries, smartphones, and semiconductors—have become common in industrial development waves. Against this background, the importance of technology protection and leakage preventive systems is emphasized. Recently, one IT security management service operator in the U.S. has been exposed to ransomware attacks, with more than 1000 subscribing enterprises incurring damages as a result. A large pipeline enterprise and a multinational refinery enterprise also were attacked by ransomware and paid a tremendous amount of money to a hacking group. As business management activity relies heavily on

IT and data technology in the digitalized industry, information security management is increasingly emphasized.

For example, in South Korea, the necessity of technology protection became an issue, and the Unfair Competition Prevention and Trade Secret Protection Act was established in 1998 accordingly. In 2007, the Act on Prevention of Divulgence and Protection of Industrial Technology was also established [3]. However, as ways to utilize international standards based on an integrated technology security system are emphasized rather than legal approaches among enterprises, the Korea Internet and Security Agency (KISA) developed the Information Security Management System (ISMS) based on the international standard 'ISO27001' in 2013. The ISMS includes criteria of 80 protective measures, including those for cyberattacks, presenting legal requirements for information communication businesses based on their annual sales and system operation conditions [4]. In addition, the ISMS was integrated into the personal information security management system in 2019, which had been separated previously, and became the advanced personal information and ISMS (ISMS-P) system. Accordingly, 22 more criteria of protective measures were added [5].

However, such activities have limitations in protecting information and technology assets. Furthermore, the importance of corporate management systems for information security operation and strategic approaches is ever more emphasized than before due to the lack of a specialized workforce and security knowledge among corporate executives [6]. Every activity in planning, implementing, and inspecting the information security management system process affects the performance of information protection directly [7]. For this reason, enterprises have become determined to invest more in information protection to manage IT disaster recovery, security incidents, and relevant items under the information security management system (ISMS), an industrial standard for information security management activity [8]. In addition, previous studies [9] have pointed out that in organizational perspectives, information security awareness programs can induce information security behaviors in the long run, thus rendering activities to raise awareness on information security and related policies and promote compliance with security policies essential [10].

Nonetheless, there has been no clear research verifying the effects and essential factors of an information security management system to be introduced, so enterprises have been reluctant to adopt or actively manage such an information security management system [11]. Many empirical studies derive important factors for information security management to lead to information protection performance or business performance, organizational effectiveness, or information protection. Many others also examine executives' participation in such activity. However, it is also necessary to analyze management factors in terms of business management system since strengthening and continuity of information security management can affect sustainable management directly and substantially.

Through this, ultimately, this study examines important factors most significantly affecting information security management, specifically, those affecting the intention and strengthening of information security management among technical, organizational, and environmental factors. By deriving the importance of information protection continuity, this study presents findings that can be utilized in establishing sustainable management strategies for subjects that need to prepare for strategic approaches in this respect. Hence, this study will suggest the implications of information security management to support for sustainable business management, and to reduce actual legal or financial risks of corporations.

2. Literature Review and Hypothesis Development

2.1. Corporate Information Security Management

Securing the reliability of information protection affects the transaction reliability as well positively. As such, ISMS (information security management system) certification affects corporate values directly [12]. In addition, establishing and operating an information security management system should be practiced continually and repeatedly according to the PDCA cycle of plan, do, check, and act [13]. As long as the PDCA cycle continues properly, its plan, do, and check steps can affect information security performance [14]. After all, as an enterprise obtains a certificate of the information security management system, promoting it improves the corporate image indirectly and increases its sales.

Recently customers' information protection is a key activity when it comes to corporate information security management. The measure to adopt protection technologies for users' personal information is one primary method in terms of active problem prevention and information protection, which affects users' awareness and thus may lead to increase of corporate values positively [9]. Furthermore, ongoing information security management is directly related to legal and financial risks in terms of sustainable management. According to one previous study on the effect of information security incidents on the enterprise's revenues, such incidents affect the enterprise's profits in the stock market [15].

Especially information security performance is an essential factor in the perspective of concerning corporate information risk management, protection and corporate value increase, and long-term management performance. Eloff and Von Solms [16] states that risks to an information system is an attempt to avoid threats and reduce the effect of attacks since such risks are substantial when organizational assets are in a state vulnerable to threats or attacks. In literatures of the corporate security risk management and method development, the perception of the necessity and importance of security risk management plays a key role in an organization's efficient security risk management [17]. In addition, information security incidents in finance, education, and medicine significantly affect legal risks such as lawsuits in accord with relevant laws [18]. For this reason, previous studies emphasize that to maintain information security management activity continually, it is necessary to obtain and renew the certificates, widely adopted at home and abroad, and manage businesses in terms of sustainability [19].

Thus, organizational activity of information security management can play an important role in managing the organization's security risks [20]. Kritzinger and Smith [21] conducted on the effects of information security administration on the factors; cost, security, support from the management, and regulation, affect the willing and managing of corporate information security. An enterprise is more likely to be willing to establish and operate an effective information security management system if the method is appropriate for the condition and principal business of the information security organization [22]. In addition, security management perception factors—organization members' security management behaviors, security compliance, perceived gain, social pressure, and security risk experience—affect a company's awareness of security risk management's importance and the intention of security risk management and method development. Further, if executives show active attitudes and behaviors towards information security management and relevant issues, information security management on the level of the entire organization will be more efficient and successful [23].

2.2. Corporate Information Security Management

The technology–organization–environment (TOE) framework is utilized widely by several studies as a technology acceptance model that nicely explains the organizational condition where new technology is adopted and implemented from the organization's perspective. Factors that affect the process where an organization adopts information technology are divided mainly into three: technological, organizational, and environmental factors [24].

According to previous studies that apply the TOE framework in information security, compatibility is one technical factor to consider checking whether the newly introduced technology suits the organization's needs. First, technical factors include common interpretation, proper use, and classification of shared information; information quality variables in quality management; establishment and standardization of the informatization system, and compatibility system quality components. Second, organizational factors include the management's perception and extent of support, the CEO's interest, and information security's maturity. Technical factors include the IT capability of the dedicated team and its members [25]. Notably, such factors as operation resources of shared information, budget, organizational innovation, and education/training directly affect the easiness and usefulness of cyber security information management. Third, environmental factors include policy makers' supportive measures such as information security laws regarding TOE frameworks. Such factors as legal/institutional variables, information sharing between organizations, and institutional prevention of shared information misuse should be considered part of the security system and used as the legal basis for information-sharing policies, procedures, and mechanisms. In addition, such factors as the corporate culture of information security, attitude towards security technology acceptance, maturity of information security, and IT ability of the dedicated team may be considered [26].

Based on the TOE factors and related previous studies [27,28], this study established the hypotheses on the basis the relationship between technology, organization, and environment factors and intention, strengthening, and continuity of information security management.

An enterprise's intention of information security management indicates to adopt the developed system and determination to fulfill the intended behavior [29]. Based on the TOE framework, Ullah et al. [30] selected factors of usefulness and easiness related to the activity of internal leakage prevention of industrial technologies, relating that most factors affected usefulness and easiness. Ahmad et al. [31], defined the variables based on the TOE framework—compatibility, organizational scale, support from the management, and policy regulations—and relates that compatibility which is a technological factor is most influential on the intention of use. Following the definition that the TOE framework, as an organizational characteristic of information security, related to the corporate intention of information security management development and maintenance, the study as established on the hypotheses below:

Hypothesis 1. *Technological factors related to the corporate activity of information security management would positively (+) affect the intention of information security management.*

Hypothesis 2. *Technological factors related to the corporate activity of information security management would positively (+) affect the intention of information security management.*

Hypothesis 3. *Environmental factors related to the corporate activity of information security management would positively (+) affect the intention of information security management.*

Strengthening of information security management means for the organization to introduce information technology and spread innovations. Steinbart et al. [32] emphasized the importance of TOE influences to the facilitation of sharing information on cyber threats. Further, Hong et al., [33] turned out that not only the CEO but also legal responsibility, autonomy, and quality evaluation affected each of the technological, organizational, and environmental factors of essential information. Based on such findings of the previous study, the following hypotheses were established:

Hypothesis 4. *Technological factors related to the corporate activity of information security management would positively (+) affect the strengthening of information security management.*

Hypothesis 5. *Organizational factors related to the corporate activity of information security management would positively (+) affect the strengthening of information security management.*

Hypothesis 6. *Environmental factors related to the corporate activity of information security management would positively (+) affect the strengthening of information security management.*

Lebek et al. [34] defined the intention of acceptance can affect behaviors substantially on the technology acceptance model (TAM). The intention of acceptance corresponds to the intention of information security management, while actual behaviors correspond to the strengthening of information security management. Sun et al. [35] also organizational willing to information security operation can improve the corporate information security management capability. Accordingly, in this study, Hypothesis 7 was designed.

Hypothesis 7. *The intention of corporate information security management would positively (+) affect the strengthening of information security management.*

In addition, the intention and strengthening of information security management can affect the continuity of information security management. According to one study by Pérez-González [36] regarding the continuity of information security management, the process of the information security management system can be a part of the circulation cycle of the security PDCA in a series of defined procedures such as establishing information security policies, forming an organization, assigning responsibilities, identifying the scope and assets, taking measures for risk and information security management, and conducting constant monitoring and reviews [37]. As explained in the above-stated definition, the intention and strengthening of information security management affect the continuity of information security management activity. Based on such previous studies, this study presents Hypotheses 8 and 9 as follows:

Hypothesis 8. *The intention of corporate information security management would positively (+) affect the continuity of information security management.*

Hypothesis 9. *The strengthening of corporate information security management would positively (+) affect the continuity of information security management.*

3. Methods

3.1. Research Model

This study empirically analyzes the effects of corporate information security's technological, organizational, and environmental factors on the enterprise's intention and strengthening of information security management. To this end, three major factors—technological, organizational, and environmental factors—were classified as independent variables, and dependent variables included the intention of information security management, strengthening of information security management, and continuity of information security management. The causal relations among such variables were assumed. Figure 1 shows the designed research model.

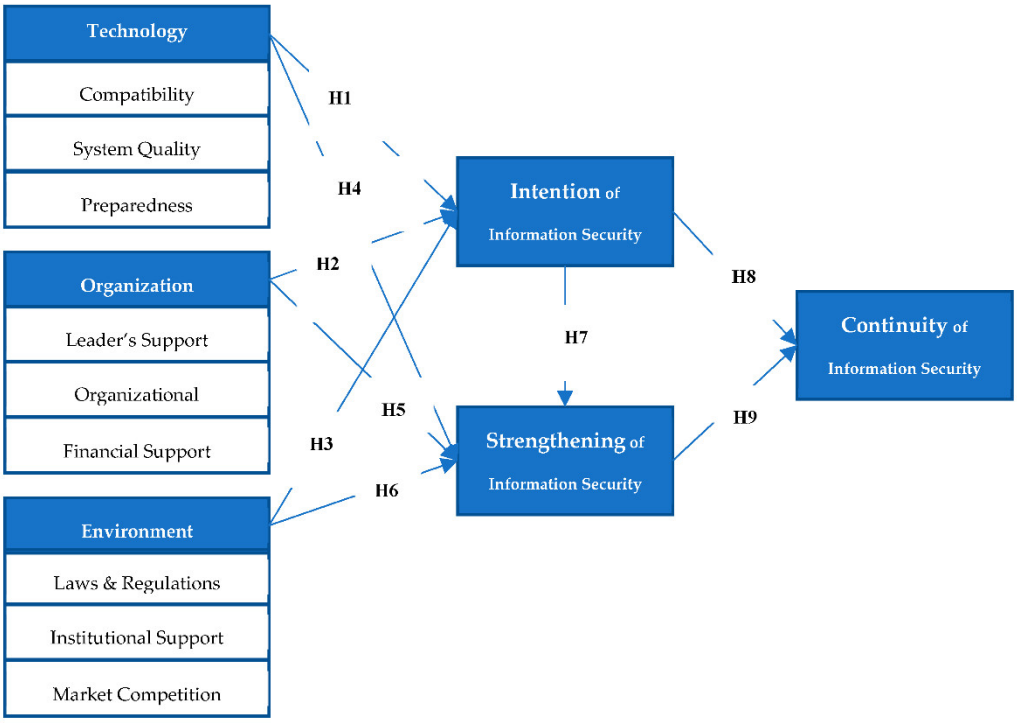

Figure 1. Research model.

3.2. Measurement Variable and Data Collection

For the survey to analyze the hypotheses stated above, 36 questionnaire items were developed in reflection of six major variables as listed in Table 1 below: As to technology factors, three questions were developed respectively for each factor—compatibility, system quality, and preparedness—based on Jeyaraj et al. [38], Kamal [39], Al-Natour and Benbasat [40], and Hossain and Quaddus [41]. As to organization factors, three questions were developed respectively for each factor—support from the leader, organizational innovativeness, and financial support—based on the previous studies of Ajzen [42], Alsene [43], and Grandon and Pearson [44]. As to environmental factors, three questions were developed respectively for each factor—laws and regulations, institutional support, and market competition—based on the previous studies of Davis [45], Caldeira and Ward [46], and Eze et al. [47]. As to the intention of information security management, three questions were developed based on the previous study of Rajab and Eydgahi [48]. As to strengthening of information security management, three questions were developed based on the study of Ritzman and Kahle-Piasecki [49], Järveläinen [50]. As to the continuity of information security, three questions were developed based on the study of Aleksandrova et al. [51]. The Likert five-point scale was applied: For each item, No. 1 indicates 'not at all,' and No. 5 indicates 'very much.'

Table 1. Research variables and survey items.

Factors	Survey Items	References
Technology	(1) Various types for information security management activity; (2) the enterprise's organizational culture and environment; (3) relevant technologies appropriate; (4) managing in a centralized manner; (5) the technology operation system; (6) cooperation between organizations; (7) the capability to conduct the activity; (8) the technical workforce; (9) IT infrastructures	Jeyaraj et al. [38], Kamal [39], Al-Natour and Benbasat [40], Hossain and Quaddus [41]

Organization	(1) The executives show a solid; (2) the executives are well-aware; (3) the executives provide active support; (4) various related departments actively participate; (5) the organization and system capable of sharing and learning; (6) there is a process being operated; (7) clear plans; (8) capital budgets; (9) if necessary, other budgets too may be used.	Ajzen [42], Alsene [43], Grandon and Pearson [44]
Environment	(1) There are reasonable regulations and instructions; (2) the current operating standards and procedures; (3) supportive measures in line with governmental legislation; (4) various supportive policies of the government; (5) the government's institutional support related; (6) the government's policies; (7) a competitive edge over other competitors; (8) conducted in cooperation with partners or customers; (9) the current status of competitors is being monitored.	Davis [45], Caldeira and Ward [46], Eze et al. [47]
Intention of information security management	(1) Intending to increase the level; (2) Willing to invest more in the activity; (3) Recognized as one of the major strategic means.	Rajab and Eydgahi [48]
Strengthening of information security management	(1) Transmission of information out of the acceptable range; (2) Information asset is well-managed; (3) Laws, institutions, and regulations are well-complied with.	Ritzman and Kahle-Piasecki [49] Järveläinen [50]
Continuity of information security management	(1) Relevant technologies appropriate continue to be developed; (2) Follow-up measures are always established and taken; (3) Company-wide activity is conducted continually.	Aleksandrova et al. [51]

This study includes an online survey conducted among industrial security workers in the IT/information communication industry in Seoul and the metropolitan area. The survey was conducted for 14 days in total in August 2021. A total of 118 questionnaires were collected, and 107 of them were analyzed with incomplete ones excluded. Technical statistics and exploratory factors were analyzed employing SPSS 24.0. For hypothesis verification, confirmatory analysis and route analysis were conducted utilizing AMOS 25.0.

3.3. Demographic Information of the Data

Among survey participants, 96.3% were male and 3.7% were female. The majority were in their 30–40 s. Those in their 40 s accounted for 55.1%, and those in their 30s 26.2%. Those under 30 years of age accounted for 2.8%, and those in their 50 s or older were 15.9%. As to the career in the field, 42.1%, the largest percentage, had 15 or longer years of work experience, 21.5% had 5–10 years, and 21.5% had 10–15 years of work experience; most of them had long careers. As to the academic background, college graduates accounted for 60.8%, those with a master's degree 32.7%, and those with a doctor's degree 6.5%. As to the position at work, executives accounted for 37.4%, the largest percentage, managers 33.7%, general directors 20.6%, and employees 8.3%. As to the scale of the enterprises that they belonged to, 31.8% (the most significant percentage) were working at an enterprise with 50–300 employees, 29.9% were working at an enterprise with 1000 or more employees, 28% 50 or less, and 10.3% 300–1000 (see Table 2).

Table 2. Demographic information of survey participants.

Classification		Frequency (n)	Percentage (%)
Sex	Male	103	96.3
	Female	4	3.7
Age	Less than 30	3	2.8
	30-less than 40	28	26.2
	40-less than 50	59	55.1
	50 or older	17	15.9

Working experience	1-less than 5 years	16	14.9
	5-less than 10 years	23	21.5
	10-less than 15 years	23	21.5
	15 or longer	45	42.1
Academic background	College graduate	65	60.8
	Master's degree	35	32.7
	Doctor's degree	7	6.5
Position	Employee	9	8.3
	Manager	36	33.7
	General director	22	20.6
	Executive	40	37.4
Corporate scale (no. of employees)	Less than 50	30	28.0
	50-less than 300	34	31.8
	300-less than 1000	11	10.3
	1000 or more	32	29.9

4. Results

4.1. Analysis Results of Reliability and Validity

The range of factor loading was between 0.857 and 0.952. The value was over 0.5 in general, which is satisfactory. The value of t was over 6.5, which is statistically significant. The reliability was between 0.903 and 0.928, which is highly significant. The value of Cronbach α was between 0.921 and 0.948; thus, the convergent validity was also secured (see Table 3), and the reliability and validity of the measurement model were both satisfactory. Regarding the fitness of the measurement model, the value of goodness-of-fit-index (GFI) was 0.878, and that of adjusted goodness-of-fit-index (AGFI) was 0.862, which was a bit lower than 0.9. The normal fit index (NFI) was 0.920, that of the Tucker Lewis index (TLI) was 0.953, and that of the root mean square error of approximation (RMSEA) was 0.083. Most values turned out to be statistically significant, and thus the model proved to be reliable.

Table 3. Results of reliability and convergent validity test.

Variables	Measurement Item	Non-Standard Loading	Standard Loading	SE	t Value	*p*	CR	AVE	Cronbach α
Technology	T1-3	1	0.887				0.907	0.765	0.939
	T4-6	1.002	0.880	0.077	12.925	***			
	T7-9	1.089	0.869	0.086	12.599	***			
Organization	O1-3	1	0.881				0.913	0.778	0.948
	O4-6	1.123	0.948	0.071	15.800	***			
	O7-9	1.088	0.874	0.102	10.661	***			
Environment	E1-3	1	0.890				0.914	0.779	0.945
	E4-6	0.983	0.857	0.077	12.734	***			
	E7-9	1.043	0.925	0.068	15.265	***			
Intention of information security management	DM1	1	0.889				0.903	0.756	0.921
	DM2	1.207	0.952	0.076	15.864	***			
	DM3	1.156	0.862	0.091	12.717	***			
Strengthening of information security management	DI4	1	0.900				0.928	0.810	0.941
	DI5	1.064	0.948	0.063	16.796	***			
	DI6	0.953	0.907	0.064	14.893	***			

Continuity of Information Security Management	DS7	1	0.902				0.904	0.759	0.929
	DS8	0.967	0.903	0.065	14.945	***			
	DS9	0.932	0.903	0.062	14.965	***			

Measurement model fit: χ^2(df) 204.800, χ^2/degree of freedom 1.736, RMR 0.049, GFI 0.878, AGFI 0.862, NFI 0.920, TLI 0.953, CFI 0.964, RMSEA 0.083. *** $p < 0.001$.

As shown in Table 4, The average sampling variance (AVE) value was between 0.759 and 0.810, which is satisfactory. As the correlation coefficient was analyzed, it turned out that the correlation coefficient of each latent variable was significant. Hence, it was verified that the discriminant validity was secured.

Table 4. Correlation matrix and AVE.

Classification	Technology	Organization	Environment	Intention of ISM	Strengthening of ISM	Continuity of ISM
Technology	**0.765**					
Organization	0.853 **	**0.778**				
Environment	0.787 **	0.890 **	**0.779**			
Intention of ISM	0.696 **	0.829 **	0.800 **	**0.756**		
Strengthening of ISM	0.740 **	0.820 **	0.860 **	0.686 **	**0.810**	
Continuity of ISM	0.783 **	0.900 **	0.877 **	0.834 **	0.873 **	**0.759**

ISM information security management/The square root of AVE is shown in bold letters. ** $p < 0.01$.

4.2. Analysis Results of Structural Model

As the fitness of the structure model was analyzed, $\chi^2(p)$ was 204.831, χ^2/degree of freedom was 1.736, and the GFI was 0.897. The NFI was 0.920, the comparative fit index (CFI) was 0.964, and the TLI, which indicates the structure model's explanatory power was 0.953. The root mean square (RMR) residual was 0.049, the AGFI was 0.879, and the RMSEA was 0.083; thus, component values of the structural equation model turned out to be significant.

Based on the result of hypothesis verification analysis, three out of nine hypotheses were rejected. First of all, organizational factors (2.478, $p < 0.01$) and environmental factors (2.228, $p < 0.05$) positively affected factors of information security management intention. However, it turned out that technology factors did not affect the intention of information security management. As to strengthening of information security management, it turned out that environmental factors were highly influential (4.436, $p < 0.001$), and technology factors also (1.347, $p < 0.05$) showed significant effects; thus, the hypotheses were selected. Organizational factors, however, failed to show any significant effect, and thus Hypothesis 5 was rejected. It also turned out that the intention of information security management affected the strengthening of information security management (−2.123, $p < 0.05$), but it showed negative effects. Since the strengthening of information security management affected its continuity (3.188, $p < 0.001$), Hypothesis 9 was selected. In contrast, the intention of information security management did not affect its continuity (see Table 5).

Table 5. Results of a hypothesis test.

	Hypothesis (path)	Standardized Regression Weights	t-Value (*p*)	Hypothesis Adoption
H1	Technology > Intention of information security management	−0.348	−1.737	Rejected
H2	Organization > Intention of information security management	0.714	2.478 **	Supported
H3	Environment > Intention of information security management	0.503	2.228 *	Supported
H4	Technology > Strengthening of information security management	0.394	1.347 *	Supported
H5	Organization > Strengthening of information security management	0.102	0.335	Rejected
H6	Environment > Strengthening of information security management	1.201	4.436 ***	Supported
H7	Intention of information security management > Strengthening of information security management	−0.339	−2.123 *	Supported
H8	Intention of information security management > Continuity of information security management	0.244	1.953	Rejected
H9	Strengthening of information security management > Continuity of information security management	0.505	3.188 ***	Supported

Structural model fit: χ^2(df) 204.831, χ^2/degree of freedom 1.736, RMR 0.049, GFI 0.897, AGFI 0.879, NFI 0.920, TLI 0.953, CFI 0.964, RMSEA 0.083. Note: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

5. Conclusions

This study analyzed the essential factors that affect the intention and strengthening of information security management based on the TOE model to establish continuous strategies and operations to corporate sustainability. In addition, this study verifies the effects of the intention and strengthening of information security management on the continuity of information security management. Three major findings derived from this study may be summarized as follows:

First, as to the adopted Hypothesis 7, it turned out that the intention of information security management negatively affected the strengthening of information security management. This finding is related to the previous study of Lindström et al. [52], where it turned out that in every object institution with the intention of investment into information security, risks of data leakage incidents were relatively high. Such inconsistency is related to the assertion that investments in information security are not used for proper types of information security regulation. In other words, as Mitchell et al. [53] mentioned, the intention of information security management itself does not substantially affect the strengthening of information security management. Only when the intention of information security management leads to proper plans for implementation and practice of the intention at proper times and places can it substantially affect the strengthening of information security management.

Second, it turned out regarding the intention of information security management that among TOE frameworks, organizational factors were the most influential. Most previous research [54,55] has explored information security on technology management and adoption of the related law and regulation. Further, an information security system and solutions have been introduced preferentially for tangible achievements [56]. However, this result indicates that when it comes to information security management, the CEO's interest in information security is significantly influential in this regard. Such

management activity can be highly effective when the entire organization and its members positively support and accept the information security management system.

Third, it turned out that environmental factors most significantly affected the strengthening of information security management. Kamal [39] suggest that the technology factors such as compatibility and system quality is the most important to manage the corporate information security system. In addition, Alsene [43] commented that corporate governance must be considered for the information security management. However, when it comes to strengthening information security management, legal risks such as punitive damages following relevant laws or institutions or introducing and strengthening an information security system for a competitive edge contribute to positive financial effects and improvement of corporate trust and recognition. As research findings support this, such environmental factors can be viewed as most influential.

Hence this study turned out that rather than the intention of information security management, the strengthening of information security management affected the continuity of information security management significantly. These findings suggest that in the corporate activity of information security management for sustainable business management, mere document-based seeming verification of an information security management with no effectiveness verified cannot guarantee the continuity of powerful information security management. Normally it is common that the environmental and managerial factors may be applied only for formality purposes of information security or neglected for short-term goals. However, recently, enterprises need to consider the current circumstances thoroughly and plan appropriate information security strategies. In order to strengthen organizational information security, an information security management system and organization should be supported in preventive administration approach.

In addition, in the long run, they also need to employ a specialized workforce, build an efficient information security system, share the system among all the organization members, and induce their active participation. In the governance perspective, the corporates should consider the corporate information security system and efficient factors as the sustainable business discussion issues in enterprise's decision-making process.

Because of the findings of this study, it is of great significance that in addition to legal and institutional improvement and support regarding information security for sustainable business management, enterprises need to continuously implement effective information security management to reduce actual legal or financial risks.

Despite such implications stated above, this study has the following limitations: First, this study was conducted only among information security workers in South Korea. Second, this study examines general components of technological, organizational, and environmental factors based on the TOE model, however, it is necessary to consider more specific and differentiating factors of information security management. To overcome these limitations, future studies need to include empirical research on information security workers at global enterprises, improve research reliability, and present more generalized research findings. In addition, research in the future needs to derive information security management operation factors in applying the grounded theory method and present more specialized and detailed information security management system factors.

Author Contributions: Funding acquisition, Y.K.; methodology, B.K.; resources, Y.K.; supervision, B.K.; writing—original draft, B.K. and Y.K.; writing—review and editing, B.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Gangwar, H.; Date, H.; Raoot, A. Review on IT adoption: Insights from recent technologies. *J. Enterp. Inf. Manag.* **2014**, *27*, 488–502, doi:10.1108/jeim-08-2012-0047.
2. von Solms, R. Information security management: The second generation. *Comput. Secur.* **1996**, *15*, 281–288, doi:10.1016/0167-4048(96)88939-5.
3. Jeong, S.; Yoon, J.; Lim, J.; Lee, K. Studies on the effect of information security investment executive. *J. Korea Inst. Inf. Secur. Cryptol.* **2014**, *24*, 1271–1284.
4. Choi, W.N.; Kim, W.J.; Kook, K.H. An evaluation of the efficiency of information protection activities of private companies. *Converg. Secur. J.* **2018**, *18*, 25–32.
5. Lee, H.; Chai, S. An empirical study of relationship between information security investment and information security incidents. *J. Korea Inst. Inf. Secur. Cryptol.* **2018**, *28*, 269–281.
6. Henriksen, H. Motivators for IOS adoption in Denmark. *J. Electron. Commer. Organ.* **2006**, *4*, 25–39.
7. Barnard, L.; von Solms, R. A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. *Comput. Secur.* **2000**, *19*, 185–194, doi:10.1016/s0167-4048(00)87829-3.
8. Da Veiga, A.; Eloff, J. An Information Security Governance Framework. *Inf. Syst. Manag.* **2007**, *24*, 361–372, doi:10.1080/10580530701586136.
9. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225, doi:10.1016/j.ijinfomgt.2015.11.009.
10. Eloff, J.H.P.; Eloff, M. Integrated information security architecture. *Comput. Fraud. Secur.* **2005**, *11*, 10–16.
11. Posthumus, S.; Von Solms, R. IT governance. *Comput. Fraud. Secur.* **2005**, *6*, 11–17.
12. Richards, N. The critical importance of information security to financial institutions. *Bus. Credit.* **2002**, *104*, 35–36.
13. Siponen, M.; Willison, R. Information security management standards: Problems and solutions. *Inf. Manag.* **2009**, *46*, 267–270.
14. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Q.* **2010**, *34*, 523, doi:10.2307/25750690.
15. Baker, W.H.; Wallace, L. Is Information Security Under Control? Investigating Quality in Information Security Management. *IEEE Secur. Priv. Mag.* **2007**, *5*, 36–44, doi:10.1109/msp.2007.11.
16. Eloff, M.M.; Von Solms, S.H. Information Security management: A hierarchical framework for various approaches. *Comput. Secur.* **2000**, *19*, 243–256.
17. Von Solms, B. Information security—The third wave? *Comput. Secur.* **2000**, *19*, 615–620.
18. Hedström, K.; Kolkowska, E.; Karlsson, F.; Allen, J. Value conflicts for information security management. *J. Strat. Inf. Syst.* **2011**, *20*, 373–384, doi:10.1016/j.jsis.2011.06.001.
19. Vroom, C.; von Solms, R. Towards information security behavioural compliance. *Comput. Secur.* **2004**, *23*, 191–198, doi:10.1016/j.cose.2004.01.012.
20. Ma, Q.; Johnston, A.C.; Pearson, J.M. Information security management objectives and practices: A parsimonious framework. *Inf. Manag. Comput. Secur.* **2008**, *16*, 251–270, doi:10.1108/09685220810893207.
21. Kritzinger, E.; Smith, E. Information security management: An information security retrieval and awareness model for industry. *Comput. Secur.* **2008**, *27*, 224–231, doi:10.1016/j.cose.2008.05.006.
22. Wiley, A.; McCormac, A.; Calic, D. More than the individual: Examining the relationship between culture and Information Security Awareness. *Comput. Secur.* **2019**, *88*, 101640, doi:10.1016/j.cose.2019.101640.
23. Singh, A.N.; Gupta, M.; Ojha, A. Identifying factors of "organizational information security management". *J. Enterp. Inf. Manag.* **2014**, *27*, 644–667, doi:10.1108/jeim-07-2013-0052.
24. Awa, H.O.; Ojiabo, O.U. A model of adoption determinants of ERP within T-O-E framework. *Inf. Technol. People* **2016**, *29*, 901–930, doi:10.1108/itp-03-2015-0068.
25. Farn, K.J.; Lin, S.K.; Fung, A.R.-W. A study on information security management system evaluation—Assets, threat and vulnerability. *Comput. Stand. Interfaces* **2004**, *26*, 501–513.
26. Steven, W.; Karen, G.; Catherine, J.; Joseph, C.; Collin, G. An Extended TOE Framework for Cybersecurity Adoption Decisions. *Commun. Assoc. Inf. Syst.* **2020**, *47*, 51–77.
27. Awa, H.O.; Ojiabo, O.U.; Emecheta, B.C. Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. *J. Sci. Technol. Policy Manag.* **2015**, *6*, 76–94, doi:10.1108/jstpm-04-2014-0012.
28. Awa, H.O.; Ukoha, O.; Emecheta, B.C. Using T-O-E theoretical framework to study the adoption of ERP solution. *Cogent Bus. Manag.* **2016**, *3*, 1196571, doi:10.1080/23311975.2016.1196571.
29. Kitsios, F.; Kamariotou, M. Business strategy modelling based on enterprise architecture: A state of the art review. *Bus. Process. Manag. J.* **2018**, *25*, 606–624, doi:10.1108/bpmj-05-2017-0122.
30. Ullah, F.; Qayyum, S.; Thaheem, M.J.; Al-Turjman, F.; Sepasgozar, S.M. Risk management in sustainable smart cities governance: A TOE framework. *Technol. Forecast. Soc. Chang.* **2021**, *167*, 120743, doi:10.1016/j.techfore.2021.120743.
31. Ahmad, S.K.; Janczewski, L.; Beltran, F. SEC-TOE framework: Exploring security determinants in big data solutions adoption. In Proceedings of the 19th Pacific Asia Conference on Information Systems, Singapore, 5–9 July 2015.
32. Steinbart, P.J.; Raschke, R.L.; Gal, G.; Dilla, W.N. The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Account. Organ. Soc.* **2018**, *71*, 15–29, doi:10.1016/j.aos.2018.04.005.

33. Hong, K.-S.; Chi, Y.-P.; Chao, L.R.; Tang, J.-H. An integrated system theory of information security management. *Inf. Manag. Comput. Secur.* **2003**, *11*, 243–248, doi:10.1108/09685220310500153.
34. Lebek, B.; Uffen, J.; Neumann, M.; Hohler, B.; Breitner, M.H. Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev.* **2014**, *37*, 1049–1092, doi:10.1108/mrr-04-2013-0085.
35. Sun, J.; Ahluwalia, P.; Koong, K.S. The more secure the better? A study of information security readiness. *Ind. Manag. Data Syst.* **2011**, *111*, 570–588, doi:10.1108/02635571111133551.
36. Pérez-González, D.; Preciado, S.T.; Solana-Gonzalez, P. Organizational practices as antecedents of the information security management performance: An empirical investigation. *Inf. Technol. People* **2019**, *32*, 1262–1275.
37. Alzahrani, L.; Seth, K.P. The Impact of Organizational Practices on the Information Security Management Performance. *Information* **2021**, *12*, 398, doi:10.3390/info12100398.
38. Jeyaraj, A.; Rottman, J.W.; Lacity, M.C. A Review of the Predictors, Linkages, and Biases in IT Innovation Adoption Research. *J. Inf. Technol.* **2006**, *21*, 1–23, doi:10.1057/palgrave.jit.2000056.
39. Kamal, M.M. IT innovation adoption in the government sector: Identifying the critical success factors. *J. Enterp. Inf. Manag.* **2006**, *19*, 192–222, doi:10.1108/17410390610645085.
40. Al-Natour, S.; Benbasat, I. The adoption and IT artefacts: A new interaction-centric model for the study of user artefact relationships. *J. Assoc. Inf. Syst.* **2009**, *10*, 661–685.
41. Hossain, M.A.; Quaddus, M. The adoption and continued usage intention of RFID: An integrated framework. *Inf. Technol. People* **2011**, *24*, 236–256, doi:10.1108/09593841111158365.
42. Ajzen, I. The theory of planned behaviour. *Organ. Behav. Hum. Decis. Process.* **1991**, *20*, 179–211.
43. Alsene, E. ERP systems and the co-ordination of the enterprise. *Bus. Process. Manag. J.* **2007**, *13*, 417–432.
44. Grandon, E.; Pearson, J. Electronic commerce adoption: An empirical study of small and medium US businesses. *Inf. Manag.* **2004**, *42*, 197–216, doi:10.1016/j.im.2003.12.010.
45. Davis, F. Perceived usefulness, perceived ease of use and acceptance of information technology. *MIS Q.* **1989**, *3*, 319–340.
46. Caldeira, M.M.; Ward, J.M. Understanding the successful adoption and use of IS/IT in SMEs: An explanation from Portuguese manufacturing industries. *Inf. Syst. J.* **2002**, *12*, 121–152, doi:10.1046/j.1365-2575.2002.00119.x.
47. Eze, S.; Awa, H.; Okoye, J.; Emecheta, B.; Anazodo, R. Determinant factors of information communication technology (ICT) adoption by government-owned universities in Nigeria: A qualitative approach. *J. Enterp. Inf. Manag.* **2013**, *26*, 427–443.
48. Rajab, M.; Eydgahi, A. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Comput. Secur.* **2018**, *80*, 211–223, doi:10.1016/j.cose.2018.09.016.
49. Ritzman, M.E.; Kahle-Piasecki, L. What Works: A Systems Approach to Employee Performance in Strengthening Information Security. *Perform. Improv.* **2016**, *55*, 17–22, doi:10.1002/pfi.21614.
50. Järveläinen, J. Information security and business continuity management in interorganizational IT relationships. *Inf. Manag. Comput. Secur.* **2012**, *20*, 332–349, doi:10.1108/09685221211286511.
51. Aleksandrova, S.V.; Aleksandrov, M.N.; Vasiliev, V.A. Business Continuity Management System. In Proceedings of the 2018 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS), St. Petersburg, Russia, 24–28 September 2018; pp. 14–17.
52. Lindström, J.; Samuelsson, S.; Hägerfors, A. Business continuity planning methodology. *Disaster Prev. Manag. Int. J.* **2010**, *19*, 243–255, doi:10.1108/09653561011038039.
53. Mitchell, R.C.; Marcella, R.; Baxter, G. Corporate information security management. *New Libr. World* **1999**, *100*, 213–227, doi:10.1108/03074809910285888.
54. Vermeulen, C.; Von Solms, R. The information security management toolbox—taking the pain out of security management. *Inf. Manag. Comput. Secur.* **2002**, *10*, 119–125, doi:10.1108/09685220210431872.
55. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.-P. Game theory meets network security and privacy. *ACM Comput. Surv.* **2013**, *45*, 1–39, doi:10.1145/2480741.2480742.
56. Yildirim, E.Y.; Akalp, G.; Aytac, S.; Bayram, N. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *Int. J. Inf. Manag.* **2011**, *31*, 360–365, doi:10.1016/j.ijinfomgt.2010.10.006.