systems

MDPI

Article

Impact of Security Management Activities on Corporate Performance

Hyunwoo Cho [1] and Keuntae Cho [2,*]

[1] Graduate School of Management of Technology, Sungkyunkwan University, Suwon 16419, Republic of Korea; hyeonwoo11539@gmail.com or cho7001@g.skku.edu
[2] Department of Systems Management Engineering, Sungkyunkwan University, 2066 Seobu-ro, Jangan-gu, Suwon 16419, Republic of Korea
* Correspondence: ktcho@skku.edu; Tel.: +82-031-290-7602

Abstract

The digital business environment is rapidly evolving with advancements in information technology (IT), increasing the risk of information security incidents. Grounded in the resource-based view and in contingency theory, this study adopts a different approach from prior research by conceptualizing security management activities not as mere risk control mechanisms, but as strategic innovation drivers that can enhance corporate performance (sales revenue and operating profit). The authors develop a research model with six independent variables, including internal and external security management activities, CISO role configuration (independent or dual-role with CIO), and investment levels in IT and information security. The dependent variables include sales revenue and operating profit, with ISMS or ISO certification as a moderating variable. Using information security (IS) disclosures and financial data from 545 Korean firms that have reported their security management activities to the Ministry of Science and ICT, multiple regression and moderation analyses reveal that high IT investment negatively impacts performance, but this effect is mitigated when formal security systems, like ISMS or ISO, are in place. The results suggest that integrating recognized security frameworks into management strategies can enhance both innovation and financial outcomes, encouraging a proactive approach to security management.

Keywords: resource-based view (RBV); contingency theory; security management activities; CISO (Chief Information Security Officer); CIO (Chief Information Officer); multiple regression analysis; moderation effect analysis; ISMS (Information Security Management System); ISO (International Organization for Standardization)

check for updates

Academic Editor: Zongjun Wang

Received: 17 June 2025
Revised: 13 July 2025
Accepted: 21 July 2025
Published: 28 July 2025

Citation: Cho, H.; Cho, K. Impact of Security Management Activities on Corporate Performance. *Systems* **2025**, *13*, 633. https://doi.org/10.3390/systems13080633

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In 2024, an information security incident occurred that was considered the worst telecommunications hack in US history. The hacker group, "Salt Typhoon", believed to be linked to the Chinese government, breached several US telecommunications companies, including AT&T, Verizon, and T-Mobile. The hack included communications from the presidential campaign teams of Donald Trump and Kamala Harris, which ultimately became a national issue [1].

The private sector was no exception. In February 2024, Change Healthcare, a medical billing and insurance processing company, suffered a ransomware attack by the Russian hacker group ALPHV/BlackCat. This incident resulted in the leak of patient data for

more than 100 million people. The leaked information included not only patient contact information but financial and health information, forcing the company to pay a ransom of $22 million [2]. These security incidents have caused severe economic losses and significant national and societal repercussions. Consequently, security management strategies have become essential components of national institutions and corporate strategies [3]. Moreover, they are increasingly seen as sources of external competitiveness for organizations [4].

In this study, the term "security management activities" is used from a business administration perspective. Specifically, it refers to activities aimed at proactively preventing hidden security vulnerabilities and improving operational efficiency when delivering products and services based on an understanding of IT. Ultimately, these activities can be defined as part of a management strategy to secure competitive advantage in the market.

Previous studies have predominantly focused on the preventive function of information security in response to incidents such as cyberattacks. Unlike this study, they have not approached security management activities as potential innovation drivers linked to corporate performance (sales revenue and operating profit). As such, prior research lacks explanatory power regarding the role of security management as a strategic innovation influencing firm outcomes [5].

By contrast, this study adopts the resource-based view (RBV), which considers security management activities as internal strategic assets that enhance organizational competitiveness, and contingency theory, which views them as essential adaptive innovations required to cope with a dynamic external environment [6,7].

To empirically test this perspective, this study uses quantitative, real-world data on security management activities as proxies for innovation performance. Specifically, it draws on information security disclosure data from 545 Korean firms that have reported to the Ministry of Science and ICT, matched with financial data collected by financial institutions.

Unlike prior research, which has relied primarily on survey methods due to the difficulty of accessing practical data, this study minimizes subjective bias through the use of officially reported data. These objective findings provide valuable managerial insights, enabling firms not only to reduce costly security incidents and improve operational efficiency and external credibility, but to strategically allocate limited managerial resources for enhanced market competitiveness. Although previous studies have attempted similar approaches, they were often constrained by limited empirical data.

In this study, security management variables are conceptualized as internal sources of competitive advantage from the RBV perspective and as adaptive innovations for technological change from the contingency theory perspective. Based on this dual lens, the research constructs hypotheses and verifies them using objective data reported to government agencies [8–10].

The independent variables are classified into three dimensions. From the non-financial security management perspective, they include internal security management activities [11–13] and external security management activities [14–16]. From the organizational innovation perspective, they include CISO (Chief Information Security Officer) independence [17,18] and dual-role configurations (CISO + CIO) [19–21]. From the financial investment perspective, they include overall IT investment levels [22–25] and security-specific IT investment levels [26–28]. These variables are analyzed for their direct impact on dependent variables, such as actual sales revenue and operating profit [29–35].

Additionally, this study introduces a moderating variable, namely whether the firm holds a certified security management system (e.g., ISMS or ISO). This factor is examined to assess whether it positively moderates the relationship between security activities and firm performance by acting as a credible innovation infrastructure. This moderation analysis

has not been sufficiently explored in prior studies, and offers practical strategic options for managers pursuing innovation through security initiatives [36–39].

The core research questions are as follows:

1. Do security management activities positively affect corporate performance?
2. Do the differences in CISO management strategies, as organizational innovation, influence corporate performance?
3. Do the differences in total IT investment versus focused information security investment levels affect corporate performance, and if so, how?
4. Does the implementation of information security management tools, such as an ISMS, positively moderate the relationship between security management activities and corporate performance?

Section 2 systematically reviews the literature on security management activities. Section 3 describes the research methods, including data collection and analysis techniques. Section 4 presents the research results, verifying the multiple regression analysis of independent variables with the simultaneous input of control variables. It also examines the interaction effects of the moderator variables for each independent variable. Section 5 discusses the research findings based on the interpretation of the results, and Section 6 summarizes the significance and limitations, offering implications for future research.

2. Literature Review and Hypothesis Setting

2.1. Theoretical Consideration

2.1.1. Security Management Activities and the Resource-Based View (RBV)

Barney emphasized that the source of sustained competitive advantage lies more in firm-specific internal resources than in external environmental factors. He argued that such advantages arise from resources that are valuable, rare, inimitable, and non-substitutable, and that these resources generate economic value through organizational efficiency. Internal resources include physical assets, such as equipment, human resources, such as managerial capabilities, and intangible assets, such as organizational culture. According to Dyer and Singh [40], these internal resources also encompass assets developed through collaboration with external partners. From this perspective, security management assets that contribute to competitive advantage can be considered strategic resources.

In the context of security management activities, managerial decisions and their execution—driven by top management's commitment—can significantly influence both financial and non-financial outcomes. In growth-oriented corporate cultures where financial performance is prioritized, security management may be viewed as a regulatory burden that impedes growth. However, prior research has suggested that efforts to prevent security incidents can lead to enhanced operational efficiency and improved corporate image, thereby contributing indirectly to financial performance, such as increased sales [41].

2.1.2. Security Management Activities and Contingency Theory

Lawrence and Lorsch posited that organizations must be flexibly designed in response to environmental conditions, and that differentiation among departments should be accompanied by integrative coordination. From this perspective, security management activities can be seen as internal innovation mechanisms that enable adaptation to external environmental uncertainties. Given the rapidly evolving IT and digital business landscape and increasing cybersecurity threats, firms must tailor their security management strategies according to their industry-specific environments and levels of external risk.

In particular, Zhang [42] highlighted that the adoption of IT should not be limited to infrastructure for external growth, but rather serve as a means to enhance organizational flexibility, ultimately improving profitability. Accordingly, security management activities

capable of responding effectively to dynamic external environments can become critical drivers of organizational innovation.

2.1.3. Theoretical Justification for Variable Selection and Hypothesis Development

To conceptualize security management activities as drivers of managerial innovation, the research variables must qualify as strategic assets that offer competitive advantage and possess the capacity to convert external environmental pressures into internal innovations [43]. From this perspective, the two aforementioned theories provide a robust theoretical foundation for selecting the variables under investigation.

Nonetheless, these theories represent distinct yet complementary viewpoints. While the resource-based view attributes competitive advantage to internal capabilities, contingency theory focuses on how external environmental factors act as triggers for internal adaptation and innovation. Despite these differences, both perspectives align with the overarching goal of maximizing organizational performance by integrating internal and external strategies. Thus, the research variables selected in this study are consistent with these dual theoretical orientations [44,45].

Based on the legitimacy of prior studies, this research categorizes independent variables into three domains. To measure financial performance—considered the core objective of managerial activities—this study adopts both sales revenue and operating profit as dependent variables, unlike previous studies that often avoided using operating profit due to data limitations. Furthermore, this study introduces Information Security Management Systems (ISMS) and ISO/IEC certifications as moderating variables. These systems, conceptualized as tools for efficient resource management and IT operations, offer measurable and objective indicators for evaluating performance—an approach not commonly found in earlier research.

All research hypotheses and variables are formulated on the basis of prior empirical findings, which suggest that security management activities have a positive influence on financial outcomes, such as sales revenue and operating profit.

2.2. Non-Financial Security Management Activities

2.2.1. Internal Security Management Activities and Corporate Performance

Internal security management activities refer to information security initiatives implemented within the organization based on managerial decisions. These activities are conducted routinely and are formally reported on an annual basis to the Ministry of Science and ICT in South Korea.

Managers carry out several security management activities internally, either due to legal obligation or corporate initiative, to ensure information security.

First, annual information security education is mandated for all organization members under Article 28 of South Korea's Personal Information Protection Act. Training requirements include six hours for CISOs, three hours for other executives, nine hours for IT staff, and at least six hours for other employees. The results must be reported to the Korean Internet and Security Agency (Ministry of Science and ICT).

Second, regular and ad hoc security audits and other self-inspection activities are conducted by executives, such as the CEO or CISO. These activities serve as the basis for recognition as a self-regulated security company by government authorities, such as the Financial Supervisory Service. From the company's perspective, this provides an opportunity to maintain internal security management while enhancing its external image as a security-conscious company.

Third, the activities of the Information Security Committee include reviewing and deciding on major security management actions. These actions involve the introduction of

IT security equipment and disciplinary measures for security violations. This serves as the basis for external auditors to assess a company's security management level during ISMS certification or major audits.

These provide non-financial benefits, such as an enhanced external reputation, and offer managers valuable insights into internal security management through the Information Security Committee. This is a proactive security management activity that enables the swift resolution of security vulnerabilities and control of future risks through rapid decision-making.

Previous studies have supported the positive impact of internal security management activities on corporate performance. Son argued that managerial, technical, and physical security activities lower costs, improve the external image, and support management goals. Shin found that security training and internal processes promote innovation and enhance the performance of manufacturing firms. Furthermore, Jeon and Jang demonstrated that various security incidents that occur when internal security management activities break down can cause significant damage to corporate performance.

Ultimately, internal security management activities are expected to have a positive impact on corporate performance. Therefore, this study proposes the following hypothesis:

Hypothesis 1. *Internal security management activities have a positive impact on corporate performance.*

2.2.2. External Security Management Activities and Corporate Performance

External security management activities involve organizational participation in cybersecurity-related initiatives conducted by external institutions, such as the Ministry of Science and ICT. These include activities, such as cyberattack response exercises, undertaken voluntarily at the discretion of the organization's top management.

Companies may participate in external information security-related activities per the national security policies. These external activities include initiatives such as the Integrated Security Support Program for Critical Information and Communications Infrastructure. Another example is the Cyber Threat Information Analysis and Sharing System. Additionally, security threat response simulation exercises are hosted by agencies such as the Ministry of the Interior and Safety and the National Intelligence Service.

These activities go beyond mere participation in events or joining safety networks to prevent accidents. Collaborating with external security experts helps companies gain security insights and drive digital innovation. Previous studies have reported that such external factors can lead to internal innovation and improved corporate performance.

Oh et al. explained that external factors can drive internal innovation linked to corporate performance. Similarly, Donaldson highlighted the innovative impact of external environmental conditions on organizations. Participation in external security activities helps institutions and companies demonstrate their IT security readiness. This, in turn, enhances the credibility of national security policy initiatives.

Thus, it is valuable to examine whether participation in external security management activities is driven by managerial intentions. It is also important to assess whether participation serves as an innovation factor that enhances corporate performance. Accordingly, this study proposes the following hypothesis:

Hypothesis 2. *External security management activities have a positive impact on corporate performance.*

2.3. The Strategic Role of the CISO in Organizational Innovation

CISO's Work Independence and Corporate Performance

Under Article 45-3, Paragraph 3 of South Korea's Information and Communications Network Act, a CISO cannot perform other executive roles under certain conditions. In the case of financial institutions, specific regulations apply if total assets exceed $8 billion and the number of employees exceeds 1000. According to the Electronic Financial Supervision Regulations, the CISO cannot hold the position of CIO in such cases.

A CISO is responsible for protecting IT systems and critical data from internal and external threats. However, if they are involved in developing and operating these systems, they may prioritize the interests of the CEO or shareholders over security. This could harm the interests of customers, business partners, and other stakeholders.

However, this may not apply to SMEs with agile cultures or to those unable to appoint a separate CISO due to their organizational characteristics. Some companies may expect greater operational efficiency if the CISO serves as a CIO or works within other technical departments. This efficiency may outweigh the security benefits of maintaining the CISO's operational independence.

Examining differences in CISO operations as innovation factors influencing performance is supported by prior studies on organizational structure innovation. This implies that changes in the internal organizational structure during the process of adapting to situational changes can enhance organizational efficiency and productivity.

Thus, the status and role of the CISO are becoming increasingly important. Security management outcomes achieved through independent operations can positively impact corporate performance through organizational efficiency and an enhanced external image.

Nonetheless, for small and medium-sized ventures, combining the CISO and CIO roles is often necessary due to limited resources. Technology-focused companies may also prefer this structure, based on their organizational characteristics. It is important to assess whether this approach effectively drives organizational innovation from a managerial perspective [46]. Therefore, this study proposes the following hypotheses:

Hypothesis 3. *Having the CISO perform duties independently will have a positive impact on corporate performance.*

Hypothesis 4. *Having the CISO also serve as CIO will have a positive impact on corporate performance.*

2.4. Strategic Differences in Information Systems Investment Decisions

2.4.1. IT Investment Activities and Corporate Performance

Despite the IT productivity paradox [47], many researchers consider IT infrastructure an important innovation resource and strategic factor in corporate management. The average IT investment ratio in Korea is 2%, which varies by industry: 1.5% in agriculture, 2.2% in manufacturing and finance, and 5.9% in information and communications, with some telecommunications firms exceeding 10%.

The digital business environment stimulates investment in the information technology (IT) sector, making it a strategic priority for companies. After the 2011 NongHyup hacking incident, the Korean government advised financial firms to allocate at least 5% of their staff to IT roles and invest 7% of their IT budgets in information security.

Considering industry and company characteristics, investment ratios may differ depending on IT informatization requirements. However, given that 70% of the annual IT budget is allocated to personnel costs, an investment ratio of 3–5% of a company's revenue is appropriate [48–50]. Additionally, from 2022 to 2024, the average IT investment ratio in

non-IT industries was approximately 30% of that in IT-related industries. When financial services are included in the IT sector, this gap becomes even more pronounced. Considering that the average IT investment ratio in IT-related industries during the study period (2022–2024) was 7.3%, a 3% investment threshold is deemed an appropriate benchmark for evaluating IT investment levels [51]. Ultimately, government regulations and market competition continue to drive IT demand [52], supporting corporate growth [53]. Thus, the following research hypothesis is established:

Hypothesis 5. *A higher investment ratio in the IT information technology sector will have a positive effect on corporate performance.*

2.4.2. Information Security Sector Investment Activities and Corporate Performance

Investment in information security differs conceptually from investment in general information technology (IT), as previously discussed. While investment in IT refers broadly to expenditures related to the acquisition, development, and maintenance of IT infrastructure across the organization, investment in information security specifically pertains to expenditures allocated solely for security purposes—such as the implementation of security solutions, adoption of new security technologies, and licensing of security-related software. These security investments are often delineated from general IT expenditures and are subject to advisory oversight by government authorities.

The information security sector faces emerging IT threats, such as quantum computing, cloud growth, and artificial intelligence (AI), which require ongoing security upgrades that often overlap with those of broader IT system investments [54]. Ultimately, managers must ensure that the IT and security departments work together through integrated IT governance to achieve business goals.

Previous studies have suggested that adopting IT security technologies is an innovation that positively influences corporate performance [55,56]. Research has shown that investments in information security can boost corporate performance, reflecting growing expectations for new technology adoption [57–59].

However, the difference in investment ratios between the two sectors relative to sales revenue may vary depending on the business environment in which a firm operates, and managers may make strategic choices that are appropriate to the situation [60]. For instance, rather than allocating resources broadly across the entire IT sector, firms may prioritize proactive investments in specific information security areas—such as the adoption of advanced security technologies—to prevent external attacks. Such a security management strategy can have a more significant impact on corporate performance.

These managerial decisions are often based on the expectation that the anticipated benefits from concentrated investments in the information security sector will outweigh the short-term costs incurred, and that such investments will enable the more efficient allocation of limited managerial resources.

For the purposes of this study, the appropriateness of the investment ratio in the information security sector is determined based on the Korean government's recommendation of 7%. Accordingly, an allocation equivalent to 8% of the total IT investment is considered appropriate.

Hypothesis 6. *A higher proportion of investment in the information security sector will have a positive effect on corporate performance.*

Based on the prior literature, this study has thus far presented research hypotheses assuming that the independent variables would have a positive effect on the dependent variables. Building upon these findings, the authors further propose that the presence of an

ISMS (Information Security Management System) will strengthen the positive impact of these independent variables on the dependent variables.

2.5. ISMS (Information Security Management System) Certification System

The British Standards Institution (BSI) introduced the ISMS concept through ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 27,001 in 2005. Since then, public institutions and companies have adopted certification as an international standard for systematic information security management.

In Korea, it was introduced in 2011, and the personal information protection sector was integrated in 2018, establishing the ISMS-P (Information Security Management System-Personal) certification system.

Notably, an ISMS certification is used not only by private companies but by public national institutions. For Critical Information Infrastructure Protection (CIIP), agencies such as the National Intelligence Service and the Ministry of Science and ICT apply a security-level management system. This evaluation system requires that ISMS certification be operated and maintained for at least one year. Key areas include administration, broadcasting and communications, finance, energy, construction and transportation, social welfare, and insurance networks [61].

2.6. Justification for ISMS as a Moderating Variable and Hypothesis Development

2.6.1. The Significance of the ISMS Certification System in Relation to Internal and External Security Management Activities and Corporate Performance

The ISMS certification system serves as an objective tool for measuring the outcomes of security-management activities. It allows for the evaluation of both non-financial and financial security management activities based on management commitment. This assessment evaluates the effectiveness of these activities. It also examines their alignment with the company's management objectives, such as management systems, information handling, IT system protection, and customer protection.

Identifying the role of information security management tools in linking internal and external security activities to corporate performance is crucial. This understanding can help companies focus on their management resources more effectively [62–64].

Therefore, this study examines whether an ISMS certification serves as a significant moderating variable. This study investigates the interaction effects between internal and external security management activities and corporate performance. Based on this, the following hypotheses are proposed:

Moderating Hypothesis 1

Obtaining or maintaining an ISMS-P and ISO/IEC certification will strengthen the positive effect of internal security management activities on corporate performance.

Moderating Hypothesis 2

Obtaining or maintaining an ISMS-P and ISO/IEC certification systems will strengthen the positive effect of external security management activities on corporate performance.

2.6.2. The Significance of the ISMS Certification Systems in Relation to CISO Work Independence and Corporate Performance

The CISO uses the ISMS tool to assess security levels and advise top management, who can then address vulnerabilities and align security policies with business goals. The ISMS objectively measures security levels and enhances efficiency, regardless of whether the CISO operates independently or concurrently serves as CIO or as another executive. If an organization aims to enhance its business performance by integrating its CIO role while

ensuring security management, a careful strategy is required. In such cases, adopting an ISMS certification system can be an effective information security management tool.

Previous studies have shown that a CISO's independence or dual role with the CIO can positively impact performance depending on company traits and strategies. Therefore, it is important to examine the interaction between ISMS certification and the CISO's operational independence. This study sets the following research hypotheses based on variations in CISO operational structures:

Moderating Hypothesis 3

The acquisition or maintenance of ISMS-P and ISO/IEC certification systems will strengthen the positive effects on corporate performance when the CISO performs duties independently without concurrent roles in other executive organizations.

Moderating Hypothesis 4

Obtaining or maintaining ISMS-P and ISO/IEC certification will strengthen the positive effect on corporate performance when the CISO concurrently serves as the CIO, overseeing the IT organization.

2.6.3. The Significance of ISMS Certification in Relation to the Proportion of Investment in IT and Information Security and Corporate Performance

It has become difficult for companies to supply products and services without relying on IT. Depending on the company's characteristics or strategy, investments in security equipment or personnel may need to be increased. A representative industry is the financial sector.

Security equipment, personnel, and new technologies are part of IT systems, and are closely tied to customer-facing products and services. Therefore, investment in both areas is essential to maintain corporate performance. Technology adoption and IT system competitiveness for agile market responses are the key drivers of corporate competitiveness.

Competitiveness is linked directly to corporate performance. Production activities that use IT platforms are not limited to the IT industry. IT platforms serve as important management tools even in traditional manufacturing and other non-IT industries. They are essential not only for customer-facing activities but for internal management.

From a security management perspective, the following key questions arise: Should continuous investment in the broader IT sector be prioritized? Alternatively, should concentrated investments in the information security sector take precedence?

Therefore, it is important to examine how an ISMS influences the impact of investment in these areas on corporate performance. Thus, the following research hypotheses are established:

Moderating Hypothesis 5

Obtaining or maintaining ISMS-P and ISO/IEC certification will strengthen the positive effect on corporate performance as the investment ratio in the IT information technology sector increases.

Moderating Hypothesis 6

Obtaining or maintaining ISMS-P and ISO/IEC certification will strengthen the positive effect on corporate performance as the investment ratio in the information security sector increases.

Building on the resource-based view (RBV) and on contingency theory, the authors have formulated research hypotheses regarding the effects of various security management variables and moderating factors on the dependent variables—sales revenue and operating profit. These hypotheses are grounded in insights drawn from prior studies. Table 1 below provides a summary of the theoretical linkages.

Table 1. Summary of Research Hypotheses and Their Theoretical Foundations.

Research Hypotheses	Theoretical Foundations		References
	Resource-Based View (RBV)	**Contingency Theory**	
H1/H2	Security management activities are strategic managerial assets unique to the organization that can demonstrate a competitive advantage.	The appropriateness of security management activities may vary depending on external stakeholders and environmental changes, making context-specific external responses essential.	Donaldson, L. (2003) [16]. Barney, J. B. (1991) [9].
H3/H4	An independent CISO, as a human capital resource with security expertise, can enhance organizational capabilities, while the integration of the CISO and CIO roles may function as synergistic capabilities that combine technology and security.	The decentralization and integration of authority within an organization should be adjusted according to its structural characteristics and environmental complexity. In environments where both technology and security are critical, role integration can enhance operational efficiency.	Dyer, J. H., & Singh, H. (1998) [40]. Lawrence, P. R., & Lorsch, J. W. (1967) [10].
H5/H6	IT investment strengthens a company's technological infrastructure and enables sustained competitive advantage, while security investment is considered a core capability that contributes to long-term performance.	The contribution of IT investment to performance varies depending on industry characteristics and the technological environment, while the level of security investment should be strategically adjusted based on factors such as regulatory requirements, threat landscape, and customer expectations within the industry.	Zhang, M. J. (2005) [42]. Galbraith, J. R. (1973) [43].
MH1~MH7	ISMS and ISO certifications serve as systematic management resources possessed by the firm, enhancing the effectiveness of the existing activities.	Standardized certification systems function as adaptive strategies to organizational environments and moderate the effects of existing variables on performance.	Donaldson, L. (2003) [16]. Barney, J. B. (1991) [9].

3. Materials and Methods

3.1. Research Model

This study aims to examine the relationship between corporate security management activities and corporate performance, as illustrated in Figure 1. It also aims to examine the moderating effect of information security management tools, such as the ISMS. Six independent variables and four control variables were defined to reflect differences in the general characteristics of the research sample. Additionally, two dependent variables—sales revenue and operating profit—were identified to measure corporate performance.

3.2. Variables

This study measured the impact of corporate security management activities on corporate performance, focusing on managers. Unlike previous studies, this study identifies both non-financial and financial information security activities within managerial decision-making processes. Research variables were defined for this study based on previous studies. Table 2 lists the contents of the independent variables.

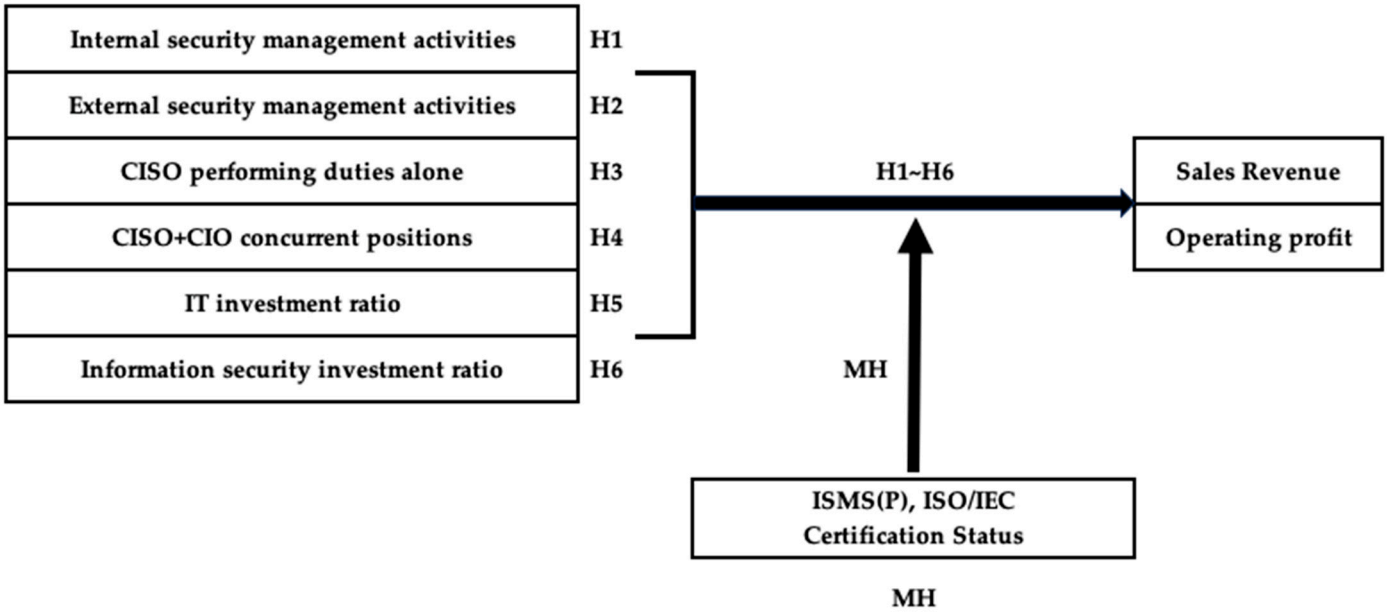


Figure 1. Research Model.

Table 3 presents the moderating and dependent variables to be tested, along with the independent and control variables, all of which were included simultaneously. Moderating variables, such as ISMS-P and ISO/IEC certification status, are dummy variables. The control variables, reflecting general company characteristics, are dummy variables, similar to the independent variables. By contrast, the dependent variables, sales revenue and operating profit, are continuous variables.

Table 2. Independent Variables.

Research Variables		Operational Definition	Measurement Method	References
Independent Variables	Internal Security Management Activities	2024 Information Security Activities Disclosure Contents ① Implemented information security training for all employees, ② Established an information security committee, or ③ whether an internal information security audit was conducted.	If one or more of ①, ②, or ③ were implemented, dummy 1; if no implementation was conducted, dummy 0.	Jeon, S. J. (2020) [11]; Jang, S. S. (2020) [12]; Posey, C., et al. (2013) [13].
	External Security Management Activities	2024 Disclosure Contents National-level security events ① Participated in the Integrated Security Support Project ② Participated in the Cyber Threat Information (C-TAS), or ③ Participated in security threat simulation exercises (KISA).	If one or more of ①, ②, or ③ were implemented, enter dummy 1; if none were implemented, enter dummy 0.	Kim, A., & Kim, Y. J. (2021) [14]. Garavan, T., & O'Brien, F. (2024) [15]. Donaldson, L. (2003) [16].
	CISO performing duties independently	As of the end of June 2024, based on information disclosed, CISO performing duties independently.	If sole responsibility, dummy 1; if concurrent roles, dummy 0.	Ciekanowski, M., et al. (2024) [17]. Choi, D., & Kim, T. (2024) [18].

Table 2. *Cont.*

Research Variables		Operational Definition	Measurement Method	References
Independent Variables	CISO + CIO concurrent positions	As of the end of June 2024, based on information disclosed, CISO concurrent positions with CIO.	If concurrently performing CIO duties, dummy 1; otherwise, dummy 0.	Kim, K. (2024) [19]. Oh S., et al. (2024) [20]. Vehent, J. (2018) [21].
	IT Information Technology Sector Investment Ratio	Average sales from 2022 to 2024, the effective disclosure period, compared to the average IT information technology sector investment performance over three years.	1 if 3% or more. If less than 3%, dummy 0.	Sun, J., & Jiao, H. (2024) [22]. Agustina, N., & Pramana, S. (2019) [23]. Gartner. (2024) [24]. Information and Communications Policy Research Institute. (2024) [25].
	Information Security Sector Investment Ratio	Effective Disclosure Period 2022–2024 IT Information Technology Sector Average Investment Amount. Ratio 3-Year Average Information Security Sector Investment Execution Performance.	8% or higher: dummy 1. If less than 8%, dummy 0.	Lee, S., et al. (2022) [26]. Electronic Financial Supervision Regulations. (2011) [27]. Shariffuddin, N., & Mohamed, A. (2020, March) [28]. Rudner, M. (2013) [54].

Table 3. Moderating Variables, Dependent Variables, and Control Variables.

Research Variables		Operational Definition	Measurement Method	References
Moderating variables	ISMS (P), ISO/IEC possession	Valid disclosure period 2022–2024 ① ISMS-P or ② ISO 27001 certification acquisition/renewal maintenance status.	①, ② Among If one or more are met, dummy 1; otherwise, dummy 0	Humphreys, E. (2016) [36]. Broderick, J. S. (2006) [37]. Song. H., et al. (2024) [38]. Hong, S., & Park, J. (2020) [39].
Dependent Variable	Sales Revenue, Operating Profit	Average performance from 2022 to 2024.	Public Institutions or Financial Institutions Survey Data (Continuous).	Go, B., & Kim, S. (2023) [29]. Science and Technology Policy Institute. (2023) [30]. Kim, J. (2023) [31]. Lee, K. (2011) [32]. Moon, S. (2024) [33]. Kim, H. (2023) [34]. Korea Credit Guarantee Fund. (2023) [35].
Control Variables	IT Industry group status	Based on disclosure content registered as of the end of June 2024 Corporate Industry Classification.	IT industry group: dummy 1. Non-IT industry group: dummy 0	Information and Communications Policy Research Institute. (2024) [25]. Korea Institute of Science and Technology Evaluation and Planning. (2024) [48]. Li, X., et al. (2024, December) [65].
	Industry Classification	Based on disclosure content registered as of the end of June 2024 Corporate Industry Classification.	Manufacturing industry: Dummy 1. Service industry: Dummy 0.	Korean Standard Industrial Classification (2024) [66]. Kakushadze, Z., & Yu, W. (2017) [67].
	Information Security Disclosure Type	Information security disclosure content as of the end of June. 2024 Information security disclosure type classification.	Dummy 1 for companies with disclosure obligations. Dummy 0 for companies with voluntary disclosure.	Kim, S. J. & Kim, T. S. (2023) [68]. National Intelligence Service (2024) [69].

Table 3. *Cont.*

Research Variables		Operational Definition	Measurement Method	References
Control Variables	Asset Size	Asset valuation amounts measured through surveys of public institutions or financial institutions from 2022 to 2024.	$1.5 billion to $4 billion is dummy 1. $250 million to $1.5 billion is dummy 0.	Kim, S. C. & Park, Y. S. (2022) [70]. Lim, J., & Han, J. (2022) [71]. Rizka, N. R., & Ulfida, D. (2024) [72]. Rahima, A. Y., & Muid, D. (2023) [73]. Utami, S. W. (2023) [74]. Fiana, F., & Endri, E. (2025) [75].
		Asset valuation amounts measured through surveys of public institutions or financial institutions from 2022 to 2024.	1 if $4 billion or more. $250 million to $1.5 billion is 0.	

Among the performance measurement indicators for corporate management, sales revenue is a widely used growth indicator. Sales revenue analysis is used to evaluate growth potential, innovation capacity, and the effectiveness of the support policies of industries and companies.

Additionally, operating profit was used as an indicator to assess the quality of corporate growth, specifically profitability and sales revenue. It is calculated by subtracting general administrative expenses, such as sales and labor costs, from the gross profit generated during the fiscal year. Operating profit is considered to be the performance metric most faithful to a company's fundamental business objectives. It is widely used to measure performance in core areas of business management, such as R&D outcomes and financial analysis. In this study, sales revenue and operating profit are used as dependent variables to verify the impact of security management activities on corporate performance.

3.3. Analysis Method

In the first stage of the research analysis, a multiple regression analysis was conducted on the independent and control variables. In this study, the two dependent variables were analyzed separately, and the significance of the results was assessed. In other words, changes in the sales revenue (a growth indicator) and operating profit (a profitability indicator) were compared from the perspective of security management strategies.

A multiple regression analysis helps identify the relative magnitude and direction of each independent variable's influence on the dependent variable. It also reveals the interactions between the independent variables. This approach facilitates the analysis of complex and realistic research problems.

In particular, it is effective in confirming the pure influence of the main independent variable when the control variables that require control are included. For this purpose, IBM SPSS version 30.0 was utilized [76–78].

In the second stage of the analysis, the presence or absence of an ISMS certification system was defined as a moderating variable. This study examined how the interaction between each independent variable and the moderating variable affected the dependent variables. As in the multiple regression analysis, both dependent variables were verified using the same control variables for each independent variable. For this purpose, we used the Process macro version 4.2 (Model 1) proposed by Hayes (2013) [79,80].

The statistical significance of the estimated regression coefficients was evaluated by considering the characteristics of the sample companies and the research objectives. Bootstrapping was conducted 5000 times with a significant level set at 0.1. The 90% confidence intervals (LLCI and ULCI) were checked to determine whether they included zero.

3.4. Model Specification

To test the proposed research hypotheses, the following models were employed. Specifically, the relationships and moderating effects between security management activities and corporate performance were examined using the multiple regression and moderated regression models specified below.

3.4.1. Multiple Regression Model

$$\ln(Y) = \beta_0 + \beta_1 \cdot X_1 + \beta_2 \cdot X_2 + \beta_3 \cdot X_3 + \beta_4 \cdot X_4 + \beta_5 \cdot X_5 + \beta_6 \cdot X_6 + \beta_7 \cdot C_1 + \beta_8 \cdot C_2 + \beta_9 \cdot C_3 + \beta_{10} \cdot C_4 + \beta_{11} \cdot C_5 + \varepsilon$$

Notation
Y: Dependent Variable (Sales Revenue, Operating Profit)
β_i: Estimated Regression Coefficient (i = 0,1,. . .,11)
X_1: Internal Security Management Activities
X_2: External Security Management Activities
X_3: CISO performing duties independently
X_4: CISO + CIO concurrent positions
X_5: IT Information Technology Sector Investment Ratio
X_6: Information Security Sector Investment Ratio
C_1: Voluntary/Mandatory
C_2: Industry
C_3: IT Industry group status
C_4: Asset size ($1.5 billion or more but less than $4 billion = 1)
C_5: Asset size ($4 billion or more = 1)

3.4.2. Moderated Regression Model

$$\ln(Y) = \beta_0 + \beta_1 \cdot X + \beta_2 \cdot W + \beta_3 \cdot XW + \beta_4 \cdot C_1 + \beta_5 \cdot C_2 + \beta_6 \cdot C_3 + \beta_7 \cdot C_4 + \beta_8 \cdot C_5 + \varepsilon$$

Notation
Y: Dependent Variable (Sales Revenue, Operating Profit)
β_i: Estimated Regression Coefficient (i = 0,1,. . .,8)
X: Independent Variable
W: Moderator Variable
XW: Interaction Term between X and W
C_1: Voluntary/Mandatory
C_2: Industry
C_3: IT Industry group status
C_4: Asset size ($1.5 billion or more but less than $4 billion = 1)
C_5: Asset size ($4 billion or more = 1)

3.5. Data Collection

Data on the sample companies were obtained from the "Information Security Disclosure Status" section of the Information Security Disclosure Comprehensive Portal (isds.kisa.or.kr). This portal is operated by the Korean Internet and Security Agency under the Ministry of Science and ICT. The dataset is based on disclosure information that companies began reporting in 2022 under the directive of the Ministry of Science and ICT of Korea. As such, only three years of data (2022–2024) are available. Prior to 2022, awareness of security management among both the Korean government and corporations was relatively low, and there was no mandatory disclosure requirement, resulting in a lack of reported security management activities. From the 600 to 700 companies that submitted

reports during the three-year period, a final sample of 545 companies was selected based on the availability of measurable financial indicators, such as sales revenue and operating profit. The financial data for each company were obtained from the statistical records of the Samsung Securities Research Center.

4. Results

4.1. General Characteristics of the Research Variables

Before proceeding with the main analysis, a frequency analysis was conducted to understand the general characteristics of the research sample. The four variables representing the general characteristics of the research participants included disclosure type (voluntary or mandatory), industry type, IT industry status, and asset size.

In particular, one of the general characteristics of the sample companies—mandatory versus voluntary disclosure—is governed by Article 13 of the Act on the Promotion of the Information Security Industry in Korea. Under this law, companies that meet specific criteria are required to submit mandatory reports to the Korea Internet and Security Agency (KISA). By contrast, voluntary disclosure is available to all businesses that operate through information and communication networks.

However, both mandatory and voluntary reporters must submit reports to the disclosure portal by June 30 of each year. Thus, the information security disclosure systems have a regulatory nature. This provides evidence that the research data obtained are objective and credible. Table 4 lists the characteristics of the 545 companies in the research sample.

Table 4. Characteristics of Research Subject.

Characteristic	Category	Frequency (Number)	Percentage (%)
		545	**100**
Voluntary/Mandatory	Voluntary	41	7.5
	Mandatory	504	92.5
Industry	Service Industry	182	33.4
	Manufacturing Industry	363	66.6
IT Industry group status	Non-IT Industry	459	84.2
	IT Industry	86	15.8
Asset Size	$250 million or more to less than $1.5 billion	369	67.7
	$1.5 billion or more to less than $4 billion	78	14.3
	$4 billion or more	98	18

By confirming the general characteristics of the research participants, we found differences in the ratios between the variables. Therefore, we dummy-coded these variables and used them as control variables in the regression analysis. We also performed descriptive statistical analyses of the independent, moderator, and dependent variables. First, we calculated the frequencies and ratios of the independent variables and moderator variables, which were categorical variables. The results of the analysis are shown in Table 5.

Next, we calculated the mean and standard deviation of the dependent variable, which was continuous. We then analyzed the skewness and kurtosis to assess whether the assumption of normality was satisfied. The assumption was considered met when the absolute value of skewness was less than 2 and the absolute value of kurtosis was less than 7, indicating that the data approximated a normal distribution. The detailed analysis results are presented in Table 6.

Table 5. Descriptive statistical analysis of research variables (categorical variables).

Research Variable	Category	Frequency (Number)	Percentage (%)
		545	**100**
Internal Security Management Activities	Not implemented	423	77.6
	Implemented	122	22.4
External Security Management Activities	Not implemented	463	85
	Implemented	82	15
CISO performing duties independently	No	433	79.4
	Yes	112	20.6
CISO + CIO concurrent positions	No	453	83.1
	Yes	92	16.9
IT Information Technology Sector Investment Ratio	Less than 3%	468	85.9
	3% or more	77	14.1
Information Security Sector Investment Ratio	Less than 8%	328	60.2
	8% or more	217	39.8
ISMS (P), ISO/IEC possession	Not certified	337	61.8
	Certified	208	38.2

Table 6. Descriptive statistics analysis of dependent variables.

	N	Minimum Value	Maximum Value	Average	Standard Deviation	Skewness	Kurtosis
Sales revenue ($80 thousand)	545	23.13	3,058,374.17	47,085.4145	180,592.4621	11.084	159.028
ln_Sales revenue ($80 thousand)	545	3.140	14.930	9.341	1.505	0.194	1.851
Operating profit ($80 thousand)	545	0.860	378,114.710	3634.744	21,247.921	13.569	209.631
ln_Operating profit ($80 thousand)	545	−0.150	12.840	6.289	1.796	0.013	0.876

The results of checking the skewness and kurtosis of the sales revenue and operating income, which measured as dependent variables, indicated that the normality assumption was not met. Therefore, in the actual research analysis, the data were transformed using a natural logarithm (ln). After applying a natural logarithm transformation, the skewness of the sales revenue and operating profits ranges from 0.013 to 0.194, satisfying the criterion of less than 2. The kurtosis ranged from 0.876 to 1.851, meeting the criterion of less than 7, thereby fulfilling the assumption of a normal data distribution [81].

4.2. Correlation Analysis Among Research Variables

To validate the appropriateness of the regression model design, a correlation analysis was conducted to examine the relationships among the variables and to assess the potential for multicollinearity. Table 7 presents the correlation coefficients among the research variables.

The results of the correlation analysis among the research variables showed that all correlation coefficients were below the absolute value of 0.8, indicating that multicollinearity was not a concern [82].

Table 7. Correlation Analysis among Research Variables.

Research Variables	1	2	3	4	5	6	7	8	9	10	11	12	13
1. ln_Sales revenue ($80 thousand)	1.000												
2. ln_Operating profit ($80 thousand)	0.784 ***	1.000											
3. Voluntary/ Mandatory	0.217 ***	0.086 *	1.000										
4. Industry	0.097 *	0.024	0.167 ***	1.000									
5. IT Industry group status	−0.176 ***	−0.046	−0.239 ***	−0.611 ***	1.000								
6. Asset Size	0.753 ***	0.695 ***	−0.003	−0.107 *	0.102 *	1.000							
7. Internal Security Management Activities	0.130 **	0.111 **	−0.030	−0.198 ***	0.166 ***	0.167 ***	1.000						
8. External Security Management Activities	0.055	0.078	−0.211 ***	−0.105 *	0.128 **	0.143 ***	−0.226 ***	1.000					
9. CISO performing duties independently	0.097 *	0.085 *	0.025	−0.064	0.017	0.126 **	0.032	0.053	1.000				
10. CISO + CIO concurrent positions	−0.115 **	−0.117 **	0.017	−0.003	−0.074	−0.096 *	−0.042	0.030	−0.229 ***	1.000			
11. IT Information Technology Sector Investment Ratio	−0.345 ***	−0.202 ***	−0.224 ***	−0.539 ***	0.663 ***	−0.052	0.199 ***	0.168 ***	0.028	0.014	1.000		
12. Information Security Sector Investment Ratio	−0.105 *	−0.066	−0.152 ***	0.067	−0.033	−0.116 **	−0.005	0.046	−0.033	0.044	−0.072	1.000	
13. ISMS-P, ISO/IEC possession	0.233 ***	0.291 ***	−0.177 ***	−0.365 ***	0.344 ***	0.404 ***	0.366 ***	0.155 ***	0.124 **	−0.082	0.419 ***	−0.068	1.000

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

4.3. Verification Results of Research Hypotheses H1–H6

Table 8 presents the results of the multiple regression analysis of sales revenue. First, in the analysis of the control variables related to a company's general characteristics, differences in autonomy/obligation, IT industry classification, and asset size were statistically significant. The analysis shows that companies with mandatory information security disclosure and those with larger asset sizes exhibit a positive (+) effect on sales revenue.

Table 8. Relationship analysis of the impact of security management activities on sales revenue.

Research Variable		B	β	SE	t	*p*	LLCI	ULCI	VIF
Independent Variables	Internal Security Management Activities	0.327	0.217	0.094	3.471 **	0.001	0.172	0.482	1.207
	External Security Management Activities	0.262	0.062	0.110	2.379 *	0.018	0.081	0.444	1.216
	CISO performing duties independently	−0.042	−0.011	0.092	−0.455	0.650	−0.194	0.110	1.087
	CISO + CIO concurrent positions	−0.191	−0.048	0.100	−1.919 +	0.056	−0.355	−0.027	1.087
	IT Information Technology Sector Investment Ratio	−1.115	−0.258	0.148	−7.543 ***	0.000	−1.359	−0.872	2.075
	Information Security Sector Investment Ratio	−0.063	−0.020	0.075	−0.830	0.407	−0.187	0.062	1.063
Control Variables	(constant)	7.999		0.178	44.888 ***	0.000	7.705	8.292	
	Voluntary/Mandatory	0.922	0.162	0.145	6.368 ***	0.000	0.684	1.161	1.141

Table 8. *Cont.*

Research Variable		B	β	SE	t	*p*	LLCI	ULCI	VIF
Control Variables	Industry	−0.040	−0.013	0.100	−0.401	0.688	−0.204	0.124	1.729
	IT Industry group status	−0.320	−0.078	0.147	−2.180 *	0.030	−0.561	−0.078	2.234
	Asset size ($1.5 billion or more but less than $4 billion = 1)	1.207	0.281	0.107	11.320 ***	0.000	1.032	1.383	1.091
	Asset size ($4 billion or more = 1)	2.805	0.717	0.102	27.464 ***	0.000	2.637	2.974	1.204
F = 112.275 *** ($p < 0.001$); $R^2 = 0.699$									

Note 1. + $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. Note 2. dependent variable: ln_Sales revenue.

Among the independent variables, both internal and external security management activities had a statistically significant positive (+) effect. The other variables exhibited negative (−) effects. As shown in Table 8, which presents the results for the dependent variable "sales revenue", Hypothesis 3 (independent CISO role) was not statistically significant, as its *p*-value exceeded the minimum significance threshold of 0.10. Hypothesis 4 (dual role of CISO and CIO) was statistically significant at the 0.10 level; however, the direction of the effect was contrary to the proposed hypothesis. Similarly, Hypothesis 5, concerning the proportion of investment in the IT sector, was statistically significant at the 0.001 level, but the direction of the relationship was also opposite to the hypothesized effect. By contrast, Hypothesis 6, which addressed the proportion of investment in the information security sector, was neither statistically significant nor aligned with the expected direction. However, the results of the CISO + CIO dual role and IT investment ratio were also statistically significant, indicating research relevance despite the direction of the effect. Although the positive (+) effects were not confirmed, the observed negative (−) effects were statistically significant.

Based on the verification of the research hypotheses regarding sales revenue, H1 and H2 were accepted, while H3 through H6 were rejected.

Table 9 presents the results of the multiple regression analysis of the operating profit. Unlike with sales revenue, the effect of the control variables was not statistically significant for IT industry classification. However, similar to the sales results, autonomy/obligation and asset size showed statistically significant correlations. Mandatory disclosure and larger asset size had a positive effect on operating profit, consistent with the sales findings.

The analysis of independent variables revealed that all were either statistically insignificant or showed effects contrary to the research hypotheses. However, similar to the sales analysis, the CISO + CIO dual role and IT investment ratio had statistically negative effects, contrary to the research hypotheses. These contrary effects differences were statistically significant.

These findings diverge from the conventional expectations, as was also observed in the results for sales revenue. This suggests that managers should adopt flexible security strategies tailored to their company's characteristics and market conditions.

The results of the hypothesis testing for operating profit showed that H1 through H6 were rejected.

As shown in Tables 8 and 9, all VIF values were below 3, which is well within the acceptable threshold (VIF < 10), indicating that multicollinearity was not a concern.

Table 9. Relationship analysis of the impact of security management activities on operating profit.

Research Variable		B	β	SE	t	*p*	LLCI	ULCI	VIF
Independent Variables	Internal Security Management Activities	0.171	0.095	0.142	1.201	0.230	−0.063	0.405	1.207
	External Security Management Activities	0.164	0.033	0.166	0.988	0.324	−0.110	0.439	1.216
	CISO performing duties independently	−0.055	−0.012	0.139	−0.394	0.693	−0.284	0.174	1.087
	CISO + CIO concurrent positions	−0.258	−0.054	0.150	−1.716 +	0.087	−0.505	−0.010	1.087
	IT Information Technology Sector Investment Ratio	−0.810	−0.157	0.223	−3.629 ***	0.000	−1.178	−0.442	2.075
	Information Security Sector Investment Ratio	0.036	0.010	0.114	0.314	0.754	−0.152	0.223	1.063
Control Variables	(constant)	5.204		0.269	19.350 ***	0.000	4.761	5.647	
	Voluntary/Mandatory	0.418	0.061	0.219	1.911 +	0.057	0.058	0.778	1.141
	Industry	0.031	0.008	0.150	0.205	0.837	−0.217	0.279	1.729
	IT Industry group status	−0.027	−0.005	0.221	−0.122	0.903	−0.392	0.338	2.234
	Asset size ($1.5 billion or more but less than $4 billion = 1)	1.505	0.294	0.161	9.354 ***	0.000	1.240	1.771	1.091
	Asset size ($4 billion or more = 1)	3.114	0.666	0.154	20.198 ***	0.000	2.860	3.368	1.204
F = 52.080 *** ($p < 0.001$); $R^2 = 0.518$									

Note 1. + $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. Note 2. dependent variable: ln_Operating profit.

4.4. Results of the Moderating Effect Analysis for Research Hypothesis (MH)

4.4.1. Analysis of the Moderating Effects of ISMS-P and ISO/IEC Certification Status on the Relationship Between Security Management Activities and Sales Revenue

Table 10 presents the results of the moderating effect analysis of the ISMS-P and ISO/IEC certification system ownership on the relationship between security management activities and sales revenue. Unlike the previous multiple regression analysis, the independent variables were analyzed individually along with the control variables. Therefore, the findings for the same research variables varied slightly due to changes in the analytical model.

For the control variables, the same results were observed as those in the multiple regression analysis. The differences in autonomy/obligation, IT industry sector, and asset size are statistically significant for all six independent variables. Mandatory information security disclosure and larger asset size had a positive effect on sales revenue. By contrast, a negative effect was observed in the IT industry.

First, the F-test and R-squared (R^2) values were examined to confirm the model fit for each independent variable. All six independent variables were statistically significant at the 0.001 level, with appropriate explanatory power. In particular, the R-squared (R^2)

statistic for the IT sector investment ratio is the highest at 0.708. All six regression models were statistically significant.

Individual regression coefficients were used to test the hypotheses based on the validated regression models. Internal security management activities (B = 0.312) had a statistically significant positive (+) effect at a 0.05 significance level. Companies that implement internal security management are expected to have higher sales revenue than those that do not.

However, the interaction term with the moderating variable was not statistically significant. Therefore, the presence or absence of ISMS-P and ISO/IEC certification does not moderate this relationship.

Table 10. Analysis of the moderating effect of ISMS-P, ISO/IEC certification on the relationship between security management activities and sales revenue (Process Macro Model 1).

Research Variable		Internal Security Management Activities		External Security Management Activities		CISO Performing Duties Independently		CISO + CIO Concurrent Positions		IT Information Technology Sector Investment Ratio		Information Security Sector Investment Ratio	
		B	*p*	B	*p*	B	*p*	B	*p*	B	*p*	B	*p*
Independent Variable (X)		0.312 *	0.048	0.059	0.707	−0.196	0.129	−0.080	0.510	−2.340 ***	0.000	0.053	0.586
Moderating variable	ISMS (P), ISO/IEC possession (W)	0.132	0.217	0.125	0.204	0.042	0.677	0.185 +	0.061	0.248 **	0.009	0.172	0.122
Interaction Term (XW)		−0.254	0.206	−0.052	0.811	0.373 *	0.049	−0.468	0.034	1.364 ***	0.000	−0.141	0.382
Control Variables	(constant)	7.664 ***	0.000	7.691 ***	0.000	7.730 ***	0.000	7.773 ***	0.000	7.900 ***	0.000	7.682 ***	0.000
	Voluntary/ Mandatory	0.990 ***	0.000	0.995 ***	0.000	0.987 ***	0.000	0.969 ***	0.000	0.993 ***	0.000	0.983 ***	0.000
	Industry	0.141	0.175	0.132	0.202	0.142	0.170	0.094	0.365	−0.045	0.647	0.137	0.187
	IT Industry group status	−0.837	0.000	−0.838	0.000	−0.835	0.000	−0.886 ***	0.000	−0.310	0.031	−0.833	0.000
	Asset size ($1.5 billion or more but less than $4 billion = 1)	1.293 ***	0.000	1.3 ***	0.000	1.302 ***	0.000	1.310 ***	0.000	1.199 ***	0.000	1.307 ***	0.000
	Asset size ($4 billion or more = 1)	2.972 ***	0.000	2.977 ***	0.000	2.977 ***	0.000	2.934 ***	0.000	2.759 ***	0.000	2.980 ***	0.000
Model Fit		F = 132.286 *** ($p < 0.001$); $R^2 = 0.664$		F = 130.804 *** ($p < 0.001$); $R^2 = 0.661$		F = 132.214 *** ($p < 0.001$); $R^2 = 0.664$		F = 134.163 *** ($p < 0.001$); $R^2 = 0.667$		F = 162.319 *** ($p < 0.001$); $R^2 = 0.708$		F = 131.033 *** ($p < 0.001$); $R^2 = 0.662$	

Note 1. + $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. Note 2. dependent variable: ln_Sales revenue.

External security management activities are not statistically significant. In other words, they are expected to be unrelated to the sales revenue. Furthermore, the interaction term was also not statistically significant, confirming the absence of a moderating effect.

The CISO's sole responsibility was not statistically significant, but the interaction term with the moderator variable (B = 0.373) was statistically significant at the 0.05 level. In the Hayes' process macro-analysis, the moderating effect in the research model is acknowledged if the effect of the interaction model is acknowledged [83–85]. In other words, the CISO alone is not a significant factor in influencing sales revenue. However, possessing ISMS-P and ISO/IEC certifications is expected to have a reinforcing effect that positively moderates this relationship.

Further analysis is needed to understand how the interaction term, which was statistically significant, manifests itself. Therefore, the participants were divided into certified and non-certified groups. Significance was re-confirmed using a 90% confidence interval (LLCI, ULCI) from 5000 bootstrapping iterations. Table 11 presents the results of the analysis.

The results showed that the effect of the CISO's sole performance on sales revenue was relatively higher in companies that held ISMS-P and ISO/IEC (B = 0.177) than in

those that did not (B = −0.196). However, the regression coefficients for all groups were not statistically significant because 0 was included in the 90% confidence interval of the bootstrapping method.

In other words, the moderating variable strengthens the relationship between the independent and dependent variables. However, because the influence of the independent variable was not significant, the effect could not be interpreted clearly. Figure 2 presents the results of the analysis.

Table 11. Analysis of the moderating effect of ISMS-P, ISO/IEC certification on the relationship between the impact of CISO sole responsibility on sales revenue (Bootstrapping method).

Moderating Variable	B	SE	t	*p*	Bootstrapping CI	
					LLCI	ULCI
ISMS (P), ISO/IEC Not certified	−0.196	0.129	−1.519	0.129	−0.409	0.017
ISMS (P), ISO/IEC Certified	0.177	0.139	1.275	0.203	−0.052	0.405

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

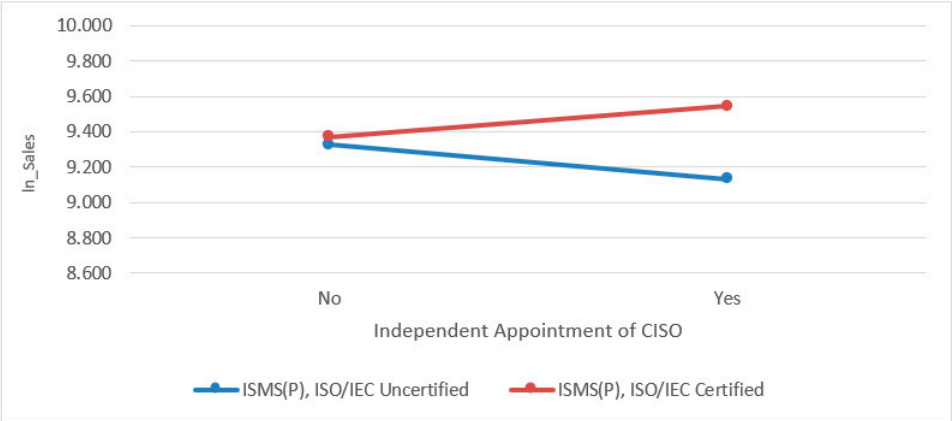


Figure 2. Influence of ISMS-P, ISO/IEC possession status on the correlation between CISO's independent work performance and sales amount.

The CISO + CIO dual responsibility was not statistically significant. In other words, the dual roles of the CISO + CIO and sales revenue are expected to be unrelated. However, the interaction term (B = −0.468) was statistically significant at the 0.05 level. That is, the dual role of the CISO + CIO is not a variable that significantly affects sales revenue. However, the presence or absence of ISMS-P and ISO/IEC certification was found to have reinforcing effects in the same direction (negative).

Additionally, to confirm the significance of the interaction term, the sample group was divided based on the possession of certification systems. Bootstrapping was then performed 5000 times to verify significance using a 90% confidence interval (LLCI, ULCI). Table 12 presents the results of this analysis.

The results show that companies with ISMS-P and ISO/IEC (B = −0.548) had a greater relative impact than companies without them (B = −0.080). Furthermore, the regression coefficient of the group holding ISMS-P and ISO/IEC was statistically significant, as it did not include zero within the 90% confidence interval of bootstrapping. Thus, the moderating variable strengthens the negative relationship between the independent and dependent variables. Although the directionality differs from the research hypotheses, it is significant. Figure 3 illustrates the results.

Table 12. Moderating effect analysis of ISMS-P, ISO/IEC certification status on the relationship between the impact of CISO + CIO dual roles on sales revenue (Bootstrapping method).

Moderating Variable	B	SE	t	*p*	Bootstrapping CI	
					LLCI	ULCI
ISMS (P), ISO/IEC Not certified	−0.080	0.121	−0.659	0.510	−0.279	0.120
ISMS (P), ISO/IEC Certified	−0.548	0.184	−2.971 **	0.003	−0.852	−0.244

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

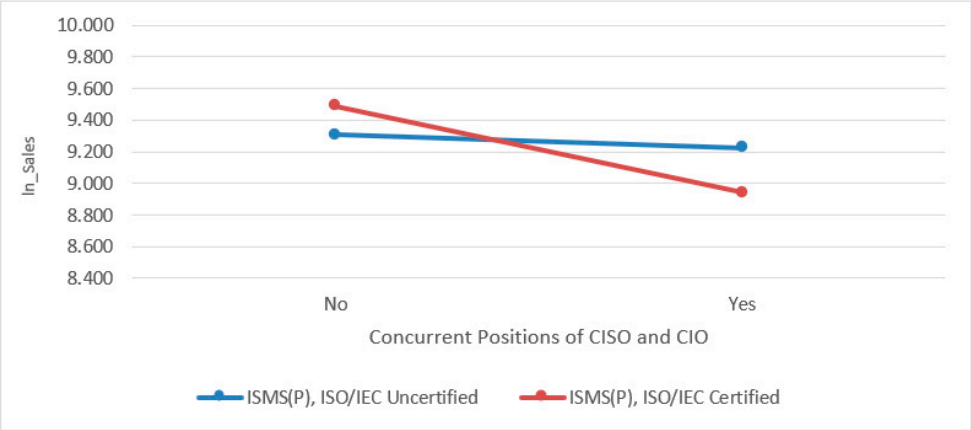


Figure 3. Influence of ISMS-P, ISO/IEC certification on the correlation between CISO + CIO dual roles and sales revenue.

The proportion of investment in the IT sector (B = −2.340) had a statistically significant negative effect at the 0.001 level. Companies with an IT sector investment ratio of 3% or more relative to sales were expected to have lower sales than those with a lower ratio. Notably, the interaction term (B = 1.364) was statistically significant at the 0.001 level.

In other words, the IT investment ratio had a significantly negative impact on sales revenue. However, the presence or absence of ISMS-P and ISO/IEC certification moderated this effect, reversing the relationship in a positive direction. Additionally, to confirm the significance of interaction term, the sample was divided, and 5000 bootstrap resamples were conducted to generate 90% confidence intervals (LLCI and ULCI). Table 13 presents the results of this analysis.

Table 13. Analysis of the moderating effects of ISMS-P, ISO/IEC certification status on the relationship between IT investment ratio and sales revenue (Bootstrapping method).

Moderating Variable	B	SE	t	*p*	Bootstrapping CI	
					LLCI	ULCI
ISMS (P), ISO/IEC Not certified	−2.340	0.294	7.963 ***	0.000	−2.824	−1.856
ISMS (P), ISO/IEC Certified	−0.975	0.158	6.164 ***	0.000	−1.236	−0.715

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

The results showed that companies with ISMS-P and ISO/IEC certification (B = −0.975) experienced a less negative effect than companies without such certifications (B = −2.340). Additionally, the regression coefficients of the two groups were statistically significant because the bootstrapping 90% confidence interval did not include 0. This indicates that

the moderating variable had a positive (+) effect on mitigating the relationship between the independent and dependent variables. Figure 4 illustrates the results.

The investment ratio in the information security sector, however, was not statistically significant. In other words, it did not appear to be related to sales revenue. The interaction term is not statistically significant, confirming the absence of a moderating effect.

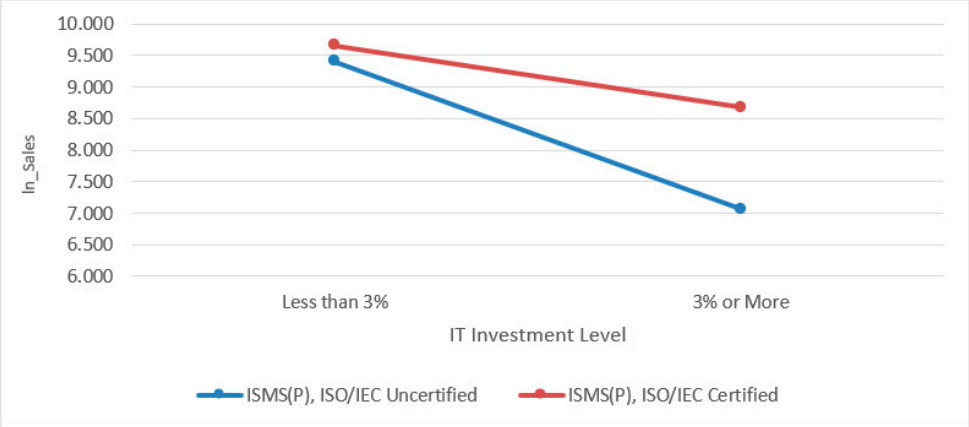


Figure 4. Influence of ISMS-P, ISO/IEC certification on the correlation between IT investment ratio and sales revenue.

To summarize the results of the moderation effect analysis for the significant hypotheses, we found that, in MH3, the interaction between independent CISO operation and the possession of information security management tools, such as an ISMS, reversed the negative impact of CISO independence on sales revenue into a statistically significant positive effect (interaction term = 0.373, $p < 0.05$). Although the independent variable itself was not statistically significant in the regression analysis, nor was the group difference significant in the moderation analysis, Hayes asserts that a statistically significant interaction term alone is sufficient to confirm a moderation effect.

Furthermore, in MH5, the interaction between increased IT investment ratio and the possession of an ISMS exhibited a significant positive moderating effect, mitigating the negative impact of increased IT investment on sales revenue (interaction term = 1.364, $p < 0.001$). In this case, both the independent variable and the group difference in the moderation analysis were statistically significant, and the bootstrapped 90% confidence interval for the interaction term did not include zero, confirming the robustness of the moderation effect.

By contrast, the interaction terms in the remaining moderation hypotheses were not statistically significant.

The results of the hypothesis testing for the moderating effect on sales revenue showed that MH3 and MH5 were accepted, while MH1, 2, 4, and 6 were rejected.

4.4.2. Analysis of the Moderating Effect of ISMS-P and ISO/IEC Certification Status on the Relationship Between Security Management Activities and Operating Profit

Table 14 presents the results of the analysis of the moderating effects of ISMS-P and ISO/IEC certification status on the relationship between security management activities and operating profits. The analysis was conducted in the same manner as for sales revenue.

The control variables yielded different results compared to the analysis of sales revenue. The statistical significance of the differences in autonomy/obligation and asset size remained the same. However, among the independent variables, only the IT investment ratio was not statistically significant. This specifically relates to whether the company belongs to the IT industry.

However, as in the sales revenue analysis, all independent variables show a positive (+) effect on operating profit as the information security disclosure method becomes more mandatory and asset size increases. Similar to the sales results, this indicates a consistent positive trend. However, no correlation was found between the operating profits across different industries.

Table 14. Analysis of the moderating effect of ISMS-P, ISO/IEC certification on the relationship between security management activities and Operating profit (Process Macro Model 1).

Research Variable		Internal Security Management Activities		External Security Management Activities		CISO Performing Duties Independently		CISO + CIO Concurrent Positions		IT Information Technology Sector Investment Ratio		Information Security Sector Investment Ratio	
		B	*p*	B	*p*	B	*p*	B	*p*	B	*p*	B	*p*
Independent Variable (X)		−0.020	0.931	0.023	0.918	−0.213	0.253	−0.193	0.271	−2.129 ***	0.000	0.154	0.276
Moderating variable	ISMS (P), ISO/IEC possession (W)	0.306 *	0.049	0.308 *	0.030	0.225	0.122	0.328 *	0.022	0.407 **	0.005	0.380 *	0.018
Interaction Term (XW)		0.007	0.982	−0.038	0.904	0.381	0.162	−0.220	0.490	1.292 **	0.005	−0.198	0.394
Control Variables	(constant)	4.864 ***	0.000	4.86 ***	0.000	4.891 ***	0.000	4.937 ***	0.000	5.034 ***	0.000	4.777 ***	0.000
	Voluntary/ Mandatory	0.487 *	0.024	0.486 *	0.027	0.485 *	0.024	0.476 *	0.027	0.494 *	0.019	0.503 *	0.021
	Industry	0.229	0.127	0.229	0.125	0.238	0.111	0.199	0.184	0.072	0.629	0.230	0.124
	IT Industry group status	−0.441	0.024	−0.439	0.025	−0.437	0.024	−0.419	0.014	0.020	0.925	−0.430	0.027
	Asset size ($1.5 billion or more but less than $4 billion = 1)	1.514 ***	0.000	1.511 ***	0.000	1.510 ***	0.000	1.522 ***	0.000	1.420 ***	0.000	1.524 ***	0.000
	Asset size ($4 billion or more = 1)	3.128 ***	0.000	3.127 ***	0.000	3.125 ***	0.000	3.091 ***	0.000	2.936 ***	0.000	3.134 ***	0.000
Model Fit		F = 68.801 *** ($p < 0.001$); $R^2 = 0.507$		F = 68.801 *** ($p < 0.001$); $R^2 = 0.507$		F = 69.312 *** ($p < 0.001$); $R^2 = 0.508$		F = 69.708 *** ($p < 0.001$); $R^2 = 0.510$		F = 76.377 *** ($p < 0.001$); $R^2 = 0.533$		F = 69.115 *** ($p < 0.001$); $R^2 = 0.510$	

Note 1. + $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. Note 2. dependent variable: ln_Operating profit.

The F-test and R-squared (R^2) values for all six independent variables were significant at the 0.001 level, confirming a good model fit and explanatory power. All six regression models were statistically significant. Hypothesis testing was performed by interpreting the individual regression coefficients based on the validated regression models.

Among the interaction terms between the six independent and moderator variables, only the IT sector investment ratio was statistically significant (B = 1.292, $p < 0.01$). The independent variable effect (B = −2.129) was also found to have a significant negative impact at the 0.001 significance level. This result is similar to the sales revenue findings. In other words, companies with an IT investment ratio of 3% or more relative to sales revenue are expected to have lower sales revenue than those without such an investment ratio.

However, it was confirmed that ISMS-P and ISO/IEC certifications have a moderating effect that reverses this relationship to have a positive (+) effect on operating profit. Additionally, the significance of the interaction term was confirmed by dividing the sample group and conducting 5000 bootstrapping runs to obtain 90% confidence intervals (LLCI and ULCI). Table 15 presents the results of this analysis.

Companies with ISMS-P and ISO/IEC certification (B = −0.837) showed a relatively lower impact than companies without such certifications (B = −2.129). In addition, because the regression coefficients of the two groups did not include zero within the 90% confidence interval of bootstrapping, the results were statistically significant. In other words, the moderating variable had a positive (+) effect on mitigating the relationship between the independent and dependent variables. Figure 5 illustrates these results.

Table 15. Analysis of the moderating effect of ISMS-P, ISO/IEC certification on the relationship between IT investment ratio and operating profit (Bootstrapping method).

Moderating Variable	B	SE	t	*p*	Bootstrapping CI	
					LLCI	ULCI
ISMS (P), ISO/IEC Not certified	−2.129	0.443	4.800 ***	0.000	−2.860	−1.398
ISMS (P), ISO/IEC Certified	−0.837	0.239	3.505 ***	0.000	−1.231	−0.444

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

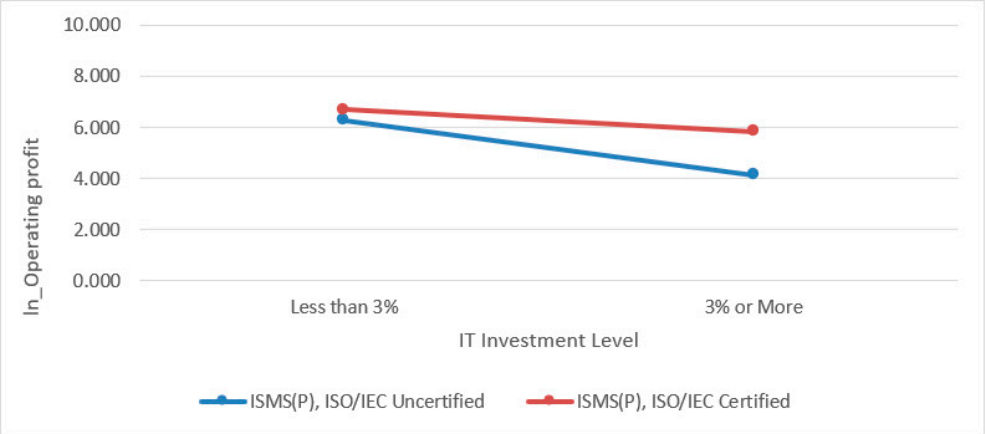


Figure 5. Influence of ISMS-P, ISO/IEC certification on the correlation between IT investment ratio and operating profit.

To summarize the results of the moderation hypothesis tests, we found that, in MH5, the interaction between increased IT investment ratio and the possession of information security management tools, such as an ISMS, had a significant positive moderating effect on operating profit, mitigating its previously negative impact (interaction term = 1.292, $p < 0.01$). Moreover, the independent variable was statistically significant in the regression analysis, and the group difference in the moderation effect was also significant. The bootstrapped 90% confidence interval for the interaction term did not include zero, further supporting the robustness of the moderation effect.

By contrast, the interaction terms in the remaining moderation hypotheses were not statistically significant.

Among the moderating effects on operating profit, only MH5 was accepted, whereas MH1, 2, 3, 4, and 6 were rejected. The final results of the hypothesis testing are summarized in Appendix A.

5. Discussion

This study yielded five meaningful points for discussion.

First, although sales revenue and operating profits share commonalities as dependent variables for verifying corporate performance, they are not identical. They produced different results in terms of independent and moderating variables and responses. This indicates that managers should adopt flexible strategic decisions when seeking to achieve management goals through security management activities.

Specifically, H1 (internal security management activities) and H2 (external security management activities) were adopted for sales revenue, but were not supported for operating profits. This suggests that internal and external security management activities incur costs related to information security, which may negatively impact operating profits. How-

ever, the positive benefits gained from these activities, such as improved work efficiency and an enhanced external image, are relatively greater. As a result, the overall effect may be favorable for corporate performance.

Seo [86] argued that security management activities can enhance corporate profits by overcoming the cost-related challenges associated with managerial resource investments and by improving operational efficiency and market competitiveness. Similarly, Shin confirmed that security activities in the manufacturing sector can lead to improved business performance by enhancing the business processes within production systems.

However, the rejection of hypotheses H3 to H6 for both sales revenue and operating profit suggests that organizational restructuring through variations in CISO roles and differences in IT investment types may not have a direct impact on corporate performance. As noted by Ciekanowski et al. and Choi and Kim, internal resistance and conflicting perspectives stemming from the potential role conflicts of CISOs within organizations may lead to diminished organizational efficiency. Moreover, Lee et al. and Robert Solow emphasized the potential lag effect of new technology adoption and IT investment, including in the security domain. This aligns with the arguments of Mithas and Rust [87] and Alharbi and Gregg, who asserted that investments in IT and information security contribute positively to corporate performance when they are aligned with business strategy. These findings underscore the need for further longitudinal research, with sufficient time-series data, to examine industry- and firm-specific characteristics in relation to the hypotheses proposed in this study.

Second, the perception that security management activities lead only to unnecessary investments in information security or increased management costs should be discarded. These activities should not be viewed as obstacles to management. Instead, they should be accepted as essential elements of management innovation.

Specifically, while H3—the direct effect of establishing a dedicated CISO structure—was not statistically significant in relation to sales revenue, the moderating hypothesis, MH3, revealed a significant positive interaction between the implementation of an Information Security Management System (ISMS) and sales performance. This finding suggests that security governance tools, such as an ISMS, can strengthen the positive relationship between independent CISO operation and sales revenue, thereby acting as a moderating mechanism that enhances corporate performance.

The present study demonstrates that the adoption of ISMS and similar certification frameworks play a crucial structural moderating role by potentially alleviating intra-organizational conflicts involving the CISO and facilitating alignment with overall business strategy.

Moreover, MH5—the interaction effect between ISMS adoption and IT investment—was found to significantly mitigate the negative impact of IT-related expenditures on both sales revenue and operating profits. These findings support the view that the adoption of ISMS and comparable security management systems constitutes a valid and impactful innovation element within corporate security management practices.

In addition, in a multiple regression analysis of the control variables, companies obligated to disclose information security showed a statistically significant positive effect on corporate performance. This is in comparison with companies that voluntarily disclose. These results further support this hypothesis.

Furthermore, Byun stated that personal information protection activities regulated by legal systems can enhance the competitiveness of IT companies. Jung argued that government regulations paradoxically stimulate technological innovation in companies. This demonstrates that information security, although regulated, has broader implications.

It can also act as an innovative element that enhances corporate competitiveness through the improved operational efficiency resulting from regulatory compliance.

Third, in small, technology-oriented firms where the dual roles of CISO and CIO are necessary for efficient managerial operations—such as IT service providers or early-stage biotech startups—as well as in growth-driven organizational structures that require strategic IT investment—such as IT platform companies or electronic communications firms—the effects of security management activities may not be immediately reflected in short-term financial performance. It is important to recognize that the realization of such effects may require a longer time horizon.

The results of multiple regression analysis of the control variables support this view. They showed that the positive effect on corporate performance is more pronounced in manufacturing industries and companies with larger asset sizes, whereas the negative effect is more noticeable in the IT industry.

Additionally, in the multiple regression analysis of the independent variables, H4 (when the CISO and CIO are combined) and H5 (when the investment ratio in the IT sector increases) also show a significant negative impact.

In other words, firms that are small and technology-focused—where the dual role of CISO and CIO may be necessary for efficient management—and those with growth-oriented structures characterized by high overall IT investment ratios are more likely to fall into this category. This implies that security management activities should not be applied uniformly across all firms or industry contexts; rather, they should be implemented flexibly, taking into account firm- and industry-specific characteristics. This interpretation is partially supported by the findings of Park et al. and Winarno et al. [88].

Fourth, as discussed in the third point, firms characterized by small-scale, technology-oriented structures or growth-driven managerial models should adopt a flexible approach when considering the implementation of security governance tools, such as an ISMS, as evidenced by the results of MH4 and MH5. The moderation analysis revealed that the possession of an ISMS tends to amplify the negative effect of a dual-role CISO/CIO structure on sales revenue. By contrast, an ISMS mitigates the negative impact of overall IT investment on sales revenue, turning it into a positive effect. These findings underscore the importance of tailoring security management activities to the specific characteristics of firms, industries, and managerial environments. Hong and Park likewise recommended applying the ISMS framework in consideration of firm- or industry-specific contexts.

Therefore, based on the third and fourth discussion points outlined above, the authors propose two distinct security management strategies.

First, for small and medium-sized venture companies or technology-based firms, where R&D is a core management strategy, having a CISO + CIO dual role may be unavoidable. In such business environments, the timing of adopting information security management tools, such as an ISMS, should be flexibly applied based on the company's situation. For example, when small-scale, R&D-focused IT-based technology companies need to launch products or services quickly, the strict adoption of tools, such as an ISMS, may not be suitable. In such cases, these tools may hinder competitiveness in fast-paced environments.

The second strategy is directed toward growth-oriented firms that require sustained and focused investment in IT. For such firms, even if short-term external performance may decline or managerial burdens increase, proactive adoption of information security tools, such as an ISMS, should be pursued. In particular, large firms with greater financial capacity may absorb short-term financial burdens more easily, and as shown in the MH5 results, the adoption of an ISMS has a positive moderating effect on both sales revenue and operating profits.

Ilmudeen and Bao [89] also empirically demonstrated the full mediating effect of IT resource management capabilities on firm performance, indirectly supporting the moderating effect proposed in this study—namely, that increasing the overall IT investment ratio through ISMS adoption can enhance corporate performance.

Finally, a fifth insight emerges from the finding that selective increases in information security investment do not significantly affect firm performance. In practice, investments in new security technologies and equipment are typically integrated into broader IT system infrastructures and, due to their technical nature, tend to be treated as dependent or subordinate investments. This reflects the structural reality that information security cannot be easily separated from the overall IT governance environment.

Prior studies on IT governance, including Symons et al. [90], have emphasized that organizational goals, IT investments, and IT security must be aligned, with consistent and immediate communication being essential. This provides a basis for the notion that internal controls, such as security audits, may also positively impact firm performance. Shariffuddin and Mohamed, in discussing the importance of IT governance, similarly argued that investments in overall IT and in information security are inherently inseparable.

However, some earlier studies regarded the introduction of security technologies and equipment as innovation drivers, interpreting security management activities as internal technological innovation efforts aimed at adapting to external environmental changes, and ultimately enhancing firm performance.

Now, however, it is time to reconsider this view in light of the rapidly evolving digital IT business environment. This study leads to the conclusion that there is no longer a need to conceptually separate overall IT investment from information security investment. The results support this integration, indicating that these domains are now so interdependent that they can no longer be meaningfully analyzed in isolation. This recognition may serve as the starting point for the development of new research variables and models.

6. Conclusions

This study verifies whether the security management activities implemented by managers in business practices affect the financial performance of companies, such as sales revenue and operating profits. In particular, this study confirms the moderating effect of information security management tools, such as the ISMS. It contributes academically by proposing practical policies and indirectly demonstrating that security management activities are elements of innovation.

6.1. Practical Implications

This study underscores that security management activities should no longer be viewed solely as passive measures for risk control, but as strategic innovation drivers that contribute directly to financial performance—including sales revenue growth and operational profit.

First, by empirically confirming the impact of security management activities on financial metrics, this study raises managerial awareness of cybersecurity not only as a threat but as a business opportunity. This perspective encourages executives to integrate tailored security initiatives into corporate strategy as a source of value creation.

Second, it emphasizes the strategic role of the Chief Information Security Officer (CISO). Beyond technical oversight, the CISO's function must be repositioned as a value-generating role, critical for improving operational efficiency, enhancing external stakeholder trust, and ultimately driving innovation-led performance.

Third, it promotes the adoption of institutionalized frameworks, such as an ISMS, as innovation enablers rather than compliance checklists. When implemented effectively, such

frameworks can help align security priorities with long-term financial goals and ensure proactive adaptability in digital business environments.

6.2. Academic Implications

This study contributes to the academic discourse by reframing security management activities as innovation-oriented practices that enhance corporate performance, rather than viewing them as mere defensive routines. This paradigm shift bridges the traditional divide between cybersecurity and the corporate innovation literature.

First, it expands the scope of information security research by empirically validating that strategic security initiatives contribute not only to risk mitigation but to quantifiable financial outcomes. This redefines security management as a core component of technological and strategic innovation.

Second, it lays the groundwork for future research that treats security investments and executive security roles as innovation inputs within organizational performance models. This perspective opens avenues for follow-up studies exploring how various configurations of security governance, investment, and culture can drive different types of innovation and business results.

6.3. Limitations of the Study

This study carries inherent limitations. There is a potential risk of endogeneity arising from unobserved variables—such as managerial quality or organizational culture—which may influence the results. In addition, the sample is restricted to Korean firms, and is based on a government-led disclosure framework, which may limit the generalizability of the findings across different industries. Furthermore, the data on security management activities were derived from self-reported disclosures by firms, raising concerns about possible reporting bias, such as overstatement of compliance or selective disclosure.

Author Contributions: Conceptualization, H.C. and K.C.; methodology, H.C.; validation, H.C. and K.C.; formal analysis, H.C.; writing—original draft preparation, H.C.; writing—review and editing, H.C. and K.C.; and supervision, K.C. All authors have read and agreed to the published version of the manuscript.

Funding: This study received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

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

Appendix A

Table A1. Summary of research hypothesis verification results.

Research Hypothesis	Verification Results	
	Sales Revenue	Operating Profit
Hypothesis 1: Internal security management activities have a positive impact on corporate performance.	Adopted	Rejected
Hypothesis 2: External security management activities have a positive impact on corporate performance.	Adopted	Rejected

Table A1. *Cont.*

Research Hypothesis	Verification Results	
	Sales Revenue	**Operating Profit**
Hypothesis 3: Having the CISO perform duties independently will have a positive impact on corporate performance.	Rejected	Rejected
Hypothesis 4: Having the CISO also serve as CIO will have a positive impact on corporate performance.	Rejected	Rejected
Hypothesis 5: A higher investment ratio in the IT information technology sector will have a positive effect on corporate performance.	Rejected	Rejected
Hypothesis 6: A higher proportion of investment in the information security sector will have a positive effect on corporate performance.	Rejected	Rejected
Moderating Hypotheses 1: Obtaining or maintaining an ISMS-P and ISO/IEC certification will strengthen the positive effect of internal security management activities on corporate performance.	Rejected	Rejected
Moderating Hypotheses 2: Obtaining or maintaining an ISMS-P and ISO/IEC certification systems will strengthen the positive effect of external security management activities on corporate performance.	Rejected	Rejected
Moderating Hypotheses 3: The acquisition or maintenance of ISMS-P and ISO/IEC certification systems will strengthen the positive effect on corporate performance when the CISO performs duties independently without concurrent roles in other executive organizations.	Adopted	Rejected
Moderating Hypotheses 4: Obtaining or maintaining an ISMS-P and ISO/IEC certification will strengthen the positive effect on corporate performance when the CISO concurrently serves as the CIO overseeing the IT organization.	Rejected	Rejected
Moderating Hypotheses 5: Obtaining or maintaining an ISMS-P and ISO/IEC certification will strengthen the positive effect on corporate performance as the investment ratio in the IT information technology sector increases.	Adopted	Adopted
Moderating Hypotheses 6: Obtaining or maintaining an ISMS-P and ISO/IEC certification will strengthen the positive effect on corporate performance as the investment ratio in the information security sector increases.	Rejected	Rejected

References

1. Wikipedia Contributors. 2024 United States Telecommunications Hack. Wikipedia. 22 April 2024. Available online: https://en.wikipedia.org/wiki/The_Washington_Post (accessed on 27 August 2024).
2. Newman, L.H. The Worst Hacks of 2024 So Far. *WIRED*, 20 March 2024.
3. *Global Cybersecurity Outlook 2024*; World Economic Forum: Cologny, Switzerland, 2024.
4. Mmango, N.; Gundu, T. Cybersecurity as a competitive advantage for entrepreneurs. In *Annual Conference of South African Institute of Computer Scientists and Information Technologists*; Springer Nature: Cham, Switzerland, 2024; pp. 374–387.
5. Son, T.H. The Impact of Corporate Information Protection Activities on Information Security and Information Management Performance. Ph.D. Dissertation, Graduate School, Myongji University, Seoul, Republic of Korea, 2015.
6. Byun, J. *A Study on the Impact of Personal Information Protection Regulatory Compliance on the Competitiveness of IT Companies Based on Regulatory Perception*; Graduate School of Soongsil University: Seoul, Republic of Korea, 2019.
7. Jung, S. *The Impact of Government Regulation on Corporate Technological Innovation Behavior*; Policy Research 2007-13; Science and Technology Policy Institute: Sejong-si, Republic of Korea, 2007.
8. Hameed, M.A.; Arachchilage, N.A.G. On the impact of perceived vulnerability in the adoption of information systems security innovations. *arXiv* **2019**, arXiv:1904.08229. [CrossRef]
9. Barney, J.B. Firm resources and sustained competitive advantage. *J. Manag.* **1991**, *17*, 99–120. [CrossRef]
10. Lawrence, P.R.; Lorsch, J.W. *Organization and Environment: Managing Differentiation and Integration*; Harvard Business School Press: Boston, MA, USA, 1967.
11. Jeon, S. *Information Security Incidents That CISOs and DPOs Must Know: Hacking Judgments Analyzed by a Hacker-Turned-Lawyer*; Samil Info Mine: Seoul, Republic of Korea, 2020.
12. Jang, S. *Introduction to Information Security and Personal Information Protection Management Systems*; Saengneung Publishing Co., Ltd.: Paju, Republic of Korea, 2020.

13. Posey, C.; Roberts, T.L.; Lowry, P.B.; Bennett, R.J.; Courtney, J.F. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *Mis Q.* **2013**, *37*, 1189–1210. [CrossRef]
14. Kim, A.; Kim, Y.J. Digital Entrepreneurship and Corporate Performance. *Bus. Adm. Res.* **2021**, *50*, 1–22.
15. Garavan, T.; O'Brien, F. Contingency theory. In *A Guide to Key Theories for Human Resource Management Research*; Edward Elgar Publishing: Cheltenham, UK, 2024; pp. 67–72.
16. Donaldson, L. *The Theory of Organizational Fit*; Gyeongmunsa: Seoul, Republic of Korea, 2003.
17. Ciekanowski, M.; Żurawski, S.; Ciekanowski, Z.; Pauliuchuk, Y.; Czech, A. Chief information security officer: A vital component of organizational information security management. *Eur. Res. Stud. J.* **2024**, *27*, 35–46. [CrossRef]
18. Choi, D.; Kim, T. The Concurrent Role of the Chief Information Security Officer and Information Security Performance: Focusing on Information Security Disclosure Data. *Korean Manag. Assoc.* **2024**, *28*, 49–63.
19. Kim, K. A Study on the Comparison of Effective Organizational Leadership According to Organizational Type: Focusing on Situational Theory. *Soc. Welf. Manag. Res.* **2024**, *11*, 1–22.
20. Oh, S.; Son, T.; Lee, C. *Major Theories of Organization*, 6th ed.; Beomunsa: Paju, Republic of Korea, 2024.
21. Vehent, J. *DevOps Security in Cloud Environments*; Hong, S., Joo, S., Translators; Wikibooks: Paju, Republic of Korea, 2018.
22. Sun, J.; Jiao, H. Emerging IT investments and firm performance: A perspective of the digital options. *Chin. Manag. Stud.* **2024**, *18*, 506–525. [CrossRef]
23. Agustina, N.; Pramana, S. The impact of development and government expenditure for information and communication technology on Indonesian economic growth. *Asian J. Bus. Environ.* **2019**, *9*, 5–13. [CrossRef]
24. Gartner. 2024 Report. In *Korea IT Spending Forecast*; Gartner: Stamford, CT, USA, 2024.
25. Information and Communications Policy Research Institute. *ICT Technology Policy Cooperation*; Policy Report No. 24-21-01; Korea Information Society Development Institute (KISDI): Jincheon, Republic of Korea, 2024; pp. 1–440. Available online: www.kisdi.re.kr (accessed on 27 August 2024).
26. Lee, S.; Shin, G.; Lee, J. A Study on the Relationship between the Adoption of 4th Industrial Revolution Technologies and Productivity in Enterprises: Absolute Level and Relative Position. *J. Korean Innov. Soc.* **2022**, *17*, 251–279.
27. Financial Services Commission. Electronic Financial Supervision Regulations, Article 8, Paragraph 2. 2011. Available online: https://www.fsc.go.kr (accessed on 27 August 2024).
28. Shariffuddin, N.; Mohamed, A. IT security and IT governance alignment: A review. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, New York, NY, USA, 31 March–2 April 2020; pp. 1–8.
29. Ko, B.; Kim, S.-T. Study on the determinants of growth in SMEs: Focusing on the characteristics based on various growth measurement methods. *Financ. Plan. Rev.* **2023**, *16*, 1–28.
30. Science and Technology Policy Institute. *A Study on the Innovation Characteristics of High-Growth Service Companies: Focusing on Innovation Activities and Innovation Outcomes*; Science and Technology: Seoul, Republic of Korea, 2023.
31. Kim, J. *A Study on the Current Status and Support Policies for Deep Tech Startups*; Korean Chamber of Commerce and Industry in America: New York, NY, USA, 2023.
32. Lee, K. Operating Profit Sustainability and Managerial Accuracy in Predicting Operating Profit. *Tax Account. Res.* **2011**, *30*, 1–17.
33. Moon, S. A Comparative Study of Global R&D Firm Performance and R&D Investment Support Systems. *Asia-Pac. Res.* **2024**, *31*, 114–143.
34. Kim, H. A Review of Research Trends on the Financial Performance of Medical Institutions. *J. Korean Soc. Nurs. Adm.* **2023**, *29*, 76–85.
35. Korea Credit Guarantee Fund. *A Study on Predicting the Risk of Default in Equipment Construction Companies Using Corporate Financial Data*; Korea Credit Guarantee Fund: Daegu, Republic of Korea, 2023.
36. Humphreys, E. *Implementing the ISO/IEC 27001: 2013 ISMS Standard*; Artech House: Minto, NSW, Australia, 2016.
37. Broderick, J.S. ISMS, security standards and security regulations. *Inf. Secur. Tech. Rep.* **2006**, *11*, 26–31. [CrossRef]
38. Song, H.; Lee, Y.; Kang, J. Analysis of major defects repeatedly identified in information security and personal information protection management system (ISMS-P) certification audits. *J. Korean Soc. Ind. Technol.* **2024**, *25*, 427–432.
39. Hong, S.; Park, J. Effective Operation of the Information Security and Personal Information Protection Management System (ISMS-P) Certification System. *J. Korean Soc. Ind. Technol.* **2020**, *21*, 634–640.
40. Dyer, J.H.; Singh, H. The relational view: Cooperative strategy and sources of interorganizational competitive advantage. *Acad. Manag. Rev.* **1998**, *23*, 660–679. [CrossRef]
41. Shin, E. *The Impact of Security Performance on Business Performance in the Manufacturing Industry: Focusing on the Production Department*; Chung Ang University, Graduate School: Seoul, Republic of Korea, 2021.
42. Zhang, M.J. Information systems, strategic flexibility and firm performance: An empirical investigation. *J. Eng. Technol. Manag.* **2005**, *22*, 163–184. [CrossRef]
43. Galbraith, J.R. *Designing Complex Organizations*; Addison-Wesley: Boston, MA, USA, 1973.

44. Lee, H.B.; Kim, Y. The effects of Information System Operating Environment on the Productivity and Performance of Small and Medium Sized Manufacturing Enterprises. *J. Korea Soc. Comput. Inf.* **2021**, *26*, 91–102.
45. Alharbi, A.; Gregg, D. The Impact of IT Investment and IT Security Intensity on Firm Performance. In Proceedings of the 2022 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, Denver, CO, USA, 7–8 October 2022; pp. 1–21. Available online: https://ifip.org/ (accessed on 16 June 2025).
46. Chawla, R.N.; Goyal, P.; Saxena, D.K. The role of CIO in digital transformation: An exploratory study. *Inf. Syst. E-Bus. Manag.* **2023**, *21*, 797–835. [CrossRef]
47. Solow, R. We'd Better Watch Out. *Newyork Times Book Review*, 12 July 1987.
48. Korea Institute of Science and Technology Planning and Evaluation. *2022 Research and Development Activity Survey*; Korea Institute of Science and Technology Planning and Evaluation: Eumseong, Republic of Korea, 2024.
49. Park, S.; Koo, B.; Ham, Y.; Lee, G. Information Technology Investment Costs and Effects: Analysis and Empirical Study of Domestic Companies. *Inf. Syst. Rev.* **2006**, *8*, 201–223.
50. Lee, S. A study on the management of corporate information technology expenditures: An empirical study focused on large enterprises. *J. Manag. Inf. Syst. Res.* **1999**, *9*, 1–23.
51. Korea Internet & Security Agency. In *Introduction to the Information Security and Personal Information Protection Management System Certification Information Security Rating System*; Korea Internet & Security Agency: Naju, Republic of Korea, 2024.
52. Yu, J.Y.; Lee, J.I. Information Security for the Diffusion of New IT Services. *Korea Inf. Process. Soc. Rev.* **2010**, *17*, 10–17.
53. Alghorbany, A.; Che-Ahmad, A.; Abdulmalik, S.O. IT investment and corporate performance: Evidence from Malaysia. *Cogent Bus. Manag.* **2022**, *9*, 2055906. [CrossRef]
54. Rudner, M. Cyber-threats to critical national infrastructure: An intelligence challenge. *Int. J. Intell. CounterIntelligence* **2013**, *26*, 453–481. [CrossRef]
55. Kosutic, D.; Pigni, F. Cybersecurity: Investing for competitive outcomes. *J. Bus. Strategy* **2022**, *43*, 28–36. [CrossRef]
56. Park, J.H.; Lee, J.S.; Bae, J.T. Technology introduction through licensing and innovation performance: Focusing on domestic manufacturing SMEs. *SME Res.* **2015**, *37*, 99–125.
57. Onibere, M.; Ahmad, A.; Maynard, S.B. Dynamic information security management capability: Strategising for organisational performance. *arXiv* **2021**, arXiv:2104.07141. [CrossRef]
58. Marhad, S.S.; Abd Goni, S.Z.; Sani, M.K.J.A. Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environ.-Behav. Proc. J.* **2024**, *9*, 197–203. [CrossRef]
59. Bokhari, S.A.A.; Manzoor, S. Impact of information security management system on firm financial performance: Perspective of corporate reputation and branding. *Am. J. Ind. Bus. Manag.* **2022**, *12*, 934–954. [CrossRef]
60. Weishäupl, E.; Yasasin, E.; Schryen, G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Comput. Secur.* **2018**, *77*, 807–823. [CrossRef]
61. Ministry of Science and ICT. *Notice on the Granting of Information Security Management Grades (No. 2017-7)*; Ministry of Science and ICT: Seoul, Republic of Korea, 2017.
62. Lee, S.W. The Impact of ISO 22301 and ISMS Certification on Business Continuity Performance: Focusing on Corporate Culture and Processes. Domestic Doctoral Dissertation, Soongsil University Graduate School, Seoul, Republic of Korea, 2021.
63. Jo, J.-K. A Study on Changes in Corporate Value after Obtaining Information Security Management System (ISMS) Certification. Master's Thesis, Chungbuk National University Graduate School, Cheongju-si, Republic of Korea, 2016.
64. Bae, Y. A Study on the Impact of Information Security Management System (ISMS) Certification on Organizational Performance. *J. Korean Soc. Ind. Technol.* **2012**, *13*, 4224–4233.
65. Li, X.; Zhao, L.; Ren, J.; Sun, Y.; Tan, C.F.; Yeo, Z.; Xiao, G. A Unified Framework to Classify Business Activities into International Standard Industrial Classification through Large Language Models for Circular Economy. In Proceedings of the 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 15–18 December 2024; IEEE: New York, NY, USA, 2024; pp. 1422–1426.
66. Statistics Korea. Korea Standard Industrial Classification (KSIC). 2024. Available online: https://kostat.go.kr (accessed on 27 August 2024).
67. Kakushadze, Z.; Yu, W. Open Source Fundamental Industry Classification. *Data* **2017**, *2*, 20. [CrossRef]
68. Kim, S.J.; Kim, T.S. Analysis of Information Security Management System Certification and Organizational Characteristics Using Information Security Disclosure Data. *Korean Soc. Manag. Inf.* **2023**, *25*, 205–231.
69. National Intelligence Service. National Information Security White Paper. 2024. Available online: https://www.nis.go.kr (accessed on 27 August 2024).
70. Kim, S.C.; Park, Y.S. Corporate Asset Composition and Performance: The Impact of Intangible Assets on Corporate Growth and Value. *Account. Policy Res.* **2022**, *27*, 59–84.
71. Lim, J.; Han, J. The Impact of ESG Activities on Management Performance: Focusing on Corporate Size and Disclosure Roles. *Commer. Educ. Res.* **2022**, *36*, 29–51.

72. Rizka, N.R.; Ulfida, D. Asset growth and firm performance: The moderating role of asset utilization. *BAJ: Behav. Account. J.* **2024**, *7*, 118–135. [CrossRef]
73. Rahima, A.Y.; Muid, D. The effect of financial performance and firm size on firm value: Case study of banking companies listed on the Indonesia Stock Exchange in 2018–2020. *Tax Account. Appl. J.* **2023**, *2*, 1–8. [CrossRef]
74. Utami, S.W. The effect of financial performance and capital structure on company value with company size as a moderation variable. *Asian J. Econ. Bus. Account.* **2023**, *23*, 112–123. [CrossRef]
75. Fiana, F.; Endri, E. Corporate social responsibility and financial performance: The moderating role of firm size. *Int. J. Econ. Financ. Issues* **2025**, *15*, 244–251. [CrossRef]
76. Bhandari, P. Control Variables | What Are They & Why Do They Matter? 2023. Scribbr. Available online: https://www.scribbr.com/methodology/control-variable/ (accessed on 16 June 2025).
77. Field, A. *Discovering Statistics Using IBM SPSS Statistics*, 5th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2018.
78. Cohen, J.; Cohen, P.; West, S.G.; Aiken, L.S. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, 3rd ed.; Routledge: Oxfordshire, UK, 2013.
79. Hayes, A.F. *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*; Guilford Press: New York, NY, USA, 2013.
80. Hayes, A.F. *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*, 2nd ed.; Guilford Publications: New York, NY, USA, 2017.
81. West, S.G.; Finch, J.F.; Curran, P.J. Structural equation models with nonnormal variables: Problems and remedies. In *Structural Equation Modeling: Concepts, Issues, and Applications*; Hoyle, R.H., Ed.; SAGE: Atlanta, GA, USA, 1995; pp. 56–75.
82. Hair, J.F., Jr.; Black, W.C.; Babin, B.J.; Anderson, R.E. Multivariate data analysis. In *Multivariate Data Analysis*; Prentice Hall: Saddle River, NJ, USA, 2010; p. 785.
83. Han, J.; Lee, J. The influence of behavioral inhibition temperament on internalizing behavioral problems in infants: The moderating effect of maternal overprotection. *J. Emot. Behav. Disord.* **2024**, *40*, 65–84.
84. Moon, Y.K. The influence of temperamental fear on emotional and anxiety problems in infants: Focusing on the moderating effect of attention regulation and the moderated moderating effect of attention regulation and parental co-parenting. *Play Ther. Res.* **2022**, *26*, 1–20. [CrossRef]
85. Lee, C.S.; Shin, E.M.; Kim, Y.S. *Analysis of Mediating Effects, Moderating Effects, and Moderated Mediating Effects Using the Case-Centered PROCESS Macro*; Saeron: Cheonan-si, Republic of Korea, 2024.
86. Seo, S. *Security Economics: An Information Security Investment Guide for CEOs*; Seoul National University Press: Seoul, Republic of Korea, 2015.
87. Mithas, S.; Rust, R.T. How information technology strategy and investments influence firm performance. *Mis Q.* **2016**, *40*, 223–246. [CrossRef]
88. Winarno, W.A.; Tjahjadi, B.; Irwanto, A. Time lag effects of IT investment on firm performance: Evidence form Indonesia. *J. Ekon. Malays.* **2021**, *55*, 89–101.
89. Ilmudeen, A.; Bao, Y. Mediating role of managing information technology and its impact on firm performance: Insight from China. *Ind. Manag. Data Syst.* **2018**, *118*, 912–929. [CrossRef]
90. Symons, C.; Cecere, M.; Young, G.O.; Lambert, N. *IT Governance Framework: Structures, Processes and Communication*; Forrester Research Inc.: Cambridge, MA, USA, 2005.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.