ACCESS Journal:
Access to Science, Business, Innovation in Digital Economy
2026, 7(1), 43-60, https://doi.org/10.46656/access.2026.7.1(3)

ISSN 2683-1007 (Online)

https://journal.access-bg.org/

ASSESSING INFORMATION LEAKAGE RISKS IN JAPANESE ENTERPRISES: STRATEGIC MANAGEMENT AND CORPORATE ATTRIBUTES

Takaaki Ishikawa[1, 2]*, Hiroyuki Suzuki[1], Kiminori Gemba[3], Tetsuaki Oda[2]

1) SingleID K.K., Tokyo, Japan
2) Graduate School of Technology Management (MOT), Ritsumeikan University, Osaka, Japan
3) Graduate School of Innovation Management, Hosei University Business School, Tokyo, Japan

e-mails: [1]t.ishikawa1106@gmail.com, [2]hsuzuki@singleid.jp, [3]gemba@hosei.ac.jp, [4]odatetsuaki@gmail.com

Received: August 3, 2025 Accepted: 18 October 2025 Online Published: 03 November 2025

ABSTRACT

As cybersecurity threats intensify, understanding the organizational drivers of information leakage has become a critical priority, especially in the context of Japanese enterprises where structural and technological legacies often persist. This study provides empirical insight into how corporate attributes shape data leakage risks, particularly focusing on email-related incidents that pose significant reputational and financial consequences.
Objectives: *The objective of this study is to examine how specific organizational characteristics—such as the number of affiliated sites, site density, presence of legacy systems, and employee-induced leakage frequency—influence the risk of information leakage in Japanese firms operating in an increasingly digitized environment.*
Methods/Approach: *The study uses a dataset of 399 Japanese enterprises collected from both public databases and private sources. Multiple regression analysis is employed to evaluate the impact of these attributes on the frequency of email leakage incidents, allowing for quantifiable insights into structural vulnerabilities and organizational exposure.*
Results: *The findings show that firms with a higher number of affiliated sites are more susceptible to data leaks, whereas those with denser site distributions experience lower risks. The presence of legacy systems, especially in older firms, significantly increases vulnerability. Furthermore, a higher frequency of employee-induced incidents highlights gaps in internal governance and employee awareness.*
Conclusions: *Information leakage risks are strongly influenced by structural and organizational factors rather than being random occurrences. These results underscore the importance of tailoring cybersecurity strategies to firm-specific attributes. The study offers a novel contribution by empirically linking corporate structure to data security outcomes, bridging strategic management and cybersecurity as an emerging interdisciplinary challenge in the digital era.*

Keywords: Information leakage, Corporate attributes, Cybersecurity, Japanese enterprises, Legacy systems, Organizational structure, Risk management
JEL classification: L86, M15, D22

Paper type: Research article

Citation: Ishikawa, T., Suzuki, H., Gemba, K., Oda, T. (2026). Assessing information leakage risks in Japanese enterprises: strategic management and corporate attributes. *Access to science, business, innovation in digital economy, ACCESS Press*, 7(1), 43-60, https://doi.org/10.46656/access.2026.7.1(3)

INTRODUCTION

In recent years, information leakage has emerged as a critical business risk for Japanese enterprises. According to a 2023 survey by Tokyo Shoko Research, the number of leaked personal information records reached approximately 40.9 million, a sevenfold increase compared to the previous year. These breaches often involve highly sensitive data such as names, addresses, email addresses, and account IDs, resulting in substantial reputational damage and financial losses for the affected companies. These incidents are attributed to diverse factors, including cyberattacks, employee misconduct, and system configuration errors, highlighting the challenges in personal information management and security measures among Japanese firms.

The importance of information security varies depending on the size of the enterprise. Large corporations face complex challenges due to geographically dispersed operations across domestic and international locations, whereas small and medium-sized enterprises (SMEs) often lack the human and financial resources to implement even basic security measures. A 2022 report by the Small and Medium Enterprise Agency revealed that approximately 60% of SMEs had not adequately addressed security measures, citing human error and governance deficiencies as critical issues.

Understanding the impact of corporate attributes, such as years in operation and the number of affiliated sites, on information leakage risks is crucial for addressing these security challenges. For instance, while older firms often rely on legacy systems that can introduce vulnerabilities, their established governance structures may help mitigate risks. Similarly, organizations with many sites may experience elevated risks due to the complexity of decentralized information management, whereas high site density can lead to more efficient resource allocation and strengthened governance. Analysing the interplay of these corporate attributes and their influence on information leakage risks is therefore of significant importance.

This study empirically examines the impact of corporate attributes—such as the number of affiliated sites, site density, leakage rates associated with years in operation, and employee-driven leakage frequencies—on information leakage risks among Japanese enterprises. By doing so, the study aims to elucidate the nature of risks stemming from decentralized organizational structures and human factors and to propose a framework for managing information leakage risks that account for corporate attributes.

Previous research has predominantly focused on technical aspects or industry-wide trends in assessing information leakage risks, with limited attention given to the specific impact of corporate attributes. This study addresses this research gap by providing novel insights that support the development of sustainable competitive advantages tailored to the unique characteristics of enterprises.

LITERATURE REVIEW

Information leakage poses a significant challenge to corporate management, with substantial research conducted on its causes and underlying factors. Existing studies primarily focus on technical vulnerabilities and the increasing prevalence of cyberattacks as key risk factors. However, these discussions often remain generalized, offering limited empirical analysis of the specific impact that corporate attributes have on information leakage risks. This study seeks to address this research gap.

The factors contributing to information leakage risks can be broadly categorized into technical, human, and organizational dimensions. Technical factors include the sophistication of cyberattacks and inherent vulnerabilities, such as zero-day exploits within corporate systems. The proliferation of cloud technologies and the Internet of Things (IoT) has further introduced new security challenges for enterprises. Human factors, on the other hand, encompass employee errors and internal misconduct, which often stem from a lack of security education and low awareness within organizations. Organizational factors include the difficulties of managing security in decentralized structures and the increased risks associated with insufficient governance and resource constraints.

These risk factors manifest differently depending on the size and internal structure of an enterprise. For instance, large corporations face challenges in applying consistent security standards due to their dispersed operations across multiple domestic and international locations. Conversely, small and medium-sized enterprises (SMEs) often struggle to implement even basic security measures due to limited human and financial resources. Addressing information leakage risks therefore requires flexible and tailored solutions that consider the specific attributes of the organization.

This study aims to elucidate the role of corporate attributes in information leakage risks, expanding on the existing discourse concerning technical, human, and organizational factors. By doing so, it seeks to provide actionable insights that help companies mitigate risks while maintaining their competitive edge. Through this approach, the research contributes to both theoretical understanding and practical risk management strategies for information security.

NUMBER OF AFFILIATED SITES AND INFORMATION LEAKAGE RISKS

Information leakage risks in decentralized organizations have been a focal point of numerous studies. As the number of affiliated sites increases, the complexity of security management rises, potentially elevating the likelihood of information leakage. This section synthesizes findings from the literature to analyze the impact of affiliated site numbers on information leakage risks from technical, organizational, and cultural perspectives.

Vallabhaneni et al. (2024) highlight how OWASP vulnerabilities in cloud environments significantly amplify security risks in decentralized systems. Their study emphasizes the challenges of standardizing security protocols in distributed environments and underscores the importance of ensuring data integrity during transfer and maintaining system coherence. In contrast, Patel (2024) discusses the effectiveness of implementing Secure Access Service Edge (SASE) architectures to address the expanding attack surface associated with an increased number of sites. While these studies underscore the importance of technical solutions for managing risks in decentralized organizations, they provide limited insights into applicability across industries and organizational scales.

From an organizational perspective, Bade et al. (2024) examine sustainability practices within the pharmaceutical industry's decentralized supply chains. Their findings suggest that enhanced transparency and the implementation of consistent sustainability and security standards across sites can strengthen overall supply chain resilience and reduce operational vulnerabilities. Albert (2024) analyzes the impact of decentralized organizational structures on security management through the lenses of "activity allocation," "decision-making processes," and "legal entities," noting that higher site independence often correlates with an increased likelihood of security gaps. These studies emphasize the potential for increased site numbers to undermine cohesive management frameworks within organizations.

From a cultural standpoint, Riahi and Islam (2024) identify discrepancies in information security awareness (ISA) among organizations with diverse cultural backgrounds as a factor exacerbating inconsistencies in security standards in decentralized environments, ultimately heightening information leakage risks. Additionally, Neri et al. (2024), focusing on SMEs in the ICT sector, demonstrate how disparities in security awareness and capabilities across sites amplify information leakage risks, advocating for the importance of uniform security education. These findings highlight the critical role of human factors and cultural dimensions in decentralized organizations.

Kävrestad et al. (2024) argue that enhancing cybersecurity awareness (CSA) mitigates information leakage risks in decentralized organizations, with support from top management being essential for unifying security standards. Similarly, Abrahams et al. (2024) comprehensively analyze the role of security culture, technological integration, and regulatory factors in managing risks in decentralized organizations. They suggest that the adoption of advanced technologies and the establishment of regulatory frameworks are key to mitigating risks associated with increasing site numbers.

Through these studies, a multifaceted understanding of how the number of affiliated sites impacts information leakage risks in decentralized organizations emerges. Technical approaches such as SASE and cloud-based security solutions are shown to effectively mitigate risks. Organizational perspectives highlight the importance of transparency and consistent standards. However, integrated approaches addressing cultural factors and human risks remain underexplored. Future research clarifying the quantitative causal relationships between site numbers and information leakage risks will contribute to developing comprehensive security management models for decentralized organizations.

SITE DENSITY AND INFORMATION LEAKAGE RISKS

The impact of site density on information leakage risks has garnered significant attention in academic research. High-density environments are suggested to enhance resource management and consistency in security measures, thereby mitigating risks. Conversely, low-density environments, characterized by resource dispersion, pose challenges in management and may increase risk exposure.

Jiang et al. (2020) analyzed privacy protection mechanisms in location-based services (LBS), demonstrating that encryption techniques and dummy location generation in high-density settings improve security efficiency through centralized resource management. Similarly, Saeidian et al. (2021), utilizing the concept of "Maximal Leakage," quantitatively demonstrated that high-density environments enhance the accuracy of predictive models, achieving a balance between privacy protection and security. However, these studies predominantly focus on technical aspects, with limited discussion of cultural and organizational factors.

Karabaev and Saitkamolov (2024) highlighted the efficacy of unified frameworks based on Defense in Depth and Zero Trust Security in high-density environments, emphasizing their role in reducing site-to-site variations in security practices. Nonetheless, practical implementation strategies leveraging AI and automation remain underexplored. Ashley and Preiksaitis (2022) further suggested that efficient resource allocation in high-density settings contributes to risk mitigation but identified gaps in the discussion of value creation as an area for future research.

Focusing on SMEs, Alahmari and Duncan (2021) demonstrated the effectiveness of centralized resource management and emphasized the critical role of decision-maker support and employee collaboration in strengthening security culture. Ambreen et al. (2023) found that applying the NIST Cybersecurity Framework (CSF) improved the consistency of security measures in high-density environments while noting that resource dispersion in low-density settings complicates security management.

From a technological perspective, Kiruthiga et al. (2021) proposed the integration of encryption techniques and intrusion detection systems (IDS) to enhance risk management efficiency in high-density environments. In contrast, Van Haastrecht et al. (2021) advocated for threat-based risk assessment models, highlighting the importance of data-driven decision-making in prioritizing security investments. However, these studies lack sufficient discussion of human and cultural factors, leaving practical implementation challenges unaddressed.

The reviewed literature confirms the potential of high-density environments to reduce information leakage risks. Conversely, low-density settings face challenges associated with resource dispersion and management complexity, with research on specific impacts and solutions remaining insufficient. Additionally, there is a need for integrative approaches addressing non-technical factors such as cultural and human risks. Furthermore, empirical studies examining how security measures proposed for high-density environments can be adapted to different organizational scales and site configurations are necessary. Addressing these gaps is essential for developing comprehensive and flexible security frameworks that account for variations in site density.

LEGACY SYSTEM DEPENDENCY AND INFORMATION LEAKAGE RISKS

Established firms are often characterized by a higher reliance on legacy systems, a significant factor contributing to increased information leakage risks. Previous studies have focused on how technical debt and system complexity influence these risks.

Pang and Tanriverdi (2022), using Routine Activity Theory (RAT), analyzed why the complexity of legacy systems makes them attractive targets for attackers. Their research revealed that older firms tend to accumulate valuable data over time, while outdated access management and intricate system architectures exacerbate security vulnerabilities. Similarly, George et al. (2022) highlighted how insufficient application of security patches, and a lack of network segmentation amplify risks unique to long-established organizations.

One proposed solution to these challenges is the reduction of technical debt. Ponnusamy and Eswararaj (2023) advocated for phased modernization approaches such as rehosting, replatforming, and refactoring, which improve both security and operational efficiency while maintaining cost-effectiveness. Nawaz et al. (2024) further demonstrated that cloud migration and AI-driven threat detection can significantly mitigate information leakage risks, particularly by enhancing defenses against advanced attacks.

The security challenges faced by older firms are not solely technical. Savin and Anysz (2021) noted that integrating outdated operational technology (OT) with modern IT introduces new vulnerabilities, particularly against zero-day exploits and DDoS attacks. Aslan et al. (2023) emphasized the effectiveness of using cloud computing and machine learning for threat detection, especially in combating contemporary threats like malware infiltration and DDoS attacks.

Moreover, a lack of security culture exacerbates information leakage risks. Adewusi et al. (2022) illustrated this by examining the interoperability issues of IoT devices in agricultural supply chains, emphasizing the importance of fostering security awareness and implementing education programs. Val et al. (2024) proposed the adoption of zero-trust architecture to address the absence of network segmentation, thereby strengthening organizational security frameworks.

The reviewed literature underscores the role of technical debt, system complexity, and a deficient security culture in increasing information leakage risks in long-established firms. However, there remains a lack of quantitative research that clearly defines the extent to which these factors contribute to risk. Additionally, further empirical studies are needed to validate the implementation processes of proposed modernization strategies and cultural reforms. Such insights are essential for developing effective measures tailored to the unique challenges faced by older organizations.

EMPLOYEE-LEVEL LEAKAGE FREQUENCY AND INFORMATION LEAKAGE RISKS

The frequency of information leakage incidents per employee is a critical indicator reflecting an organization's security awareness and level of training. Higher leakage frequency at the employee level is associated with increased information leakage risks, emphasizing the need to understand how human errors and insider threats impact an organization's overall security posture.

Dash and Ansari (2022) empirically demonstrated that Security Education Training and Awareness (SETA) programs are effective in mitigating information leakage risks. Their study identified "low-security awareness among employees" as the primary factor contributing to heightened risks, linking insufficient training to higher leakage frequencies per employee. Similarly, Ansari et al. (2022) highlighted that AI-powered security awareness training enhances employees' threat recognition capabilities, particularly against phishing attacks. These findings suggest that the format and technological integration of training programs play a pivotal role in influencing employee behavior.

Hughes-Lartey et al. (2021), through statistical analysis of data breach incidents, confirmed the direct impact of employee actions on risk. Their study identified unauthorized access and improper information disclosure as significant contributors to leakage risks, exacerbated by the lack of adequate security training. Additionally, Rao Faizan Ali et al. (2021) examined the relationship between adherence to information security policies and organizational culture, revealing that poor governance and insufficient training significantly undermine compliance rates.

The influence of human factors on security risks has also been discussed by Zwilling et al. (2020), who demonstrated that targeted education for employees with low self-efficacy can effectively reduce information leakage risks. Their study provided concrete evidence that security awareness programs improve employee behavior and mitigate risks. On the other hand, Georgiadou et al. (2022) argued that the lack of training in remote work environments increases leakage frequency at the employee level, emphasizing the challenges of implementing security guidelines in such settings.

In Lee (2021) identified human factors as the greatest challenge in cybersecurity risk management, noting that employee negligence increases the success rates of attacks. Georgiadou et al. (2021) further highlighted the practical application of the MITRE ATT&CK framework in evaluating security culture and designing effective training programs, demonstrating the direct link between education and cultural improvements.

The reviewed literature underscores the importance of employee-level leakage frequency as a key metric for assessing information leakage risks. However, there is limited quantitative research on how this metric impacts an organization's overall risk. Furthermore, the specific effects of training programs and governance on employee behavior require further investigation. Addressing these gaps will facilitate the development of risk assessment frameworks that incorporate employee-level indicators, broadening their practical application.

Through this literature review, significant insights were gained regarding the impact of affiliated site numbers, site density, company age, and employee-level leakage frequency on information leakage risks. Nonetheless, the role of these corporate attributes in risk evaluation has been underexplored. Factors such as affiliated site numbers and site density have been discussed only superficially. Moreover, quantitative empirical studies that clarify the causal relationship between these attributes and information leakage risks remain scarce.

This study aims to quantitatively analyze the impact of corporate attributes on information leakage risks among Japanese firms, addressing overlooked elements in existing research. The hypotheses of this study are intended to contribute both practically, by improving risk management, and academically, by providing novel insights into the relationship between corporate attributes and information leakage risks. By doing so, this research seeks to enhance the comprehensive understanding of information leakage risks and lay the groundwork for more effective risk management strategies.

HYPOTHESES

This study aims to empirically examine the impact of corporate attributes on information leakage risks, establishing the following four hypotheses. These hypotheses adopt a multifaceted approach by analyzing organizational, operational, historical, and human aspects of information leakage risks, providing a framework for comprehensively understanding the risk factors faced by companies.

HYPOTHESES 1

The greater the number of affiliated sites a company has, the higher its information leakage risks. An increase in affiliated sites is likely to decentralize information management, making the consistent application of unified security standards more challenging. Additionally, the frequency of data transfers between sites increases, which may elevate the risk of data breaches. Testing this hypothesis will clarify the challenges of information management in decentralized organizations and propose measures for risk mitigation.

HYPOTHESES 2

Companies with higher site density are likely to experience lower information leakage risks. Higher site density can facilitate efficient resource allocation and create an environment where security measures are more effectively implemented. Furthermore, higher density strengthens employee collaboration, potentially enhancing governance in information management. This hypothesis seeks to elucidate how the efficiency of site configuration affects information leakage risks.

HYPOTHESES 3

Companies with a higher leakage rate based on the length of establishment are more likely to face increased information leakage risks. Older companies often depend on legacy systems and outdated information management processes, which can lead to vulnerabilities in their security framework. By examining this hypothesis, the study aims to reveal how a company’s historical background influences information leakage risks and provides insights into improving legacy systems.

HYPOTHESES 4

Companies with a higher frequency of information leakage incidents per employee are likely to experience increased information leakage risks. A high frequency suggests deficiencies in security education or internal governance. Employee errors or insider threats may constitute primary causes of information leakage, making this metric a critical component in risk evaluation. This hypothesis will investigate the impact of human factors on information leakage risks and highlight the importance of improving education and governance.

METHODOLOGY

In this study, the corporate information database of Tokyo Shoko Research (TSR) was used as the population, encompassing over 850,000 companies with valid corporate information as of 2023. Given the impracticality of analyzing all companies, a random sampling method was employed to extract a manageable subset. Specifically, a Python-based random number generation script was utilized to randomly select 399 companies from the database.

The sample size of 399 was determined to be statistically valid, as it meets the theoretical value of approximately 384 companies required for a 95% confidence level with a 5% margin of error. Considering the study's analytical objectives and practical constraints, 399 companies were finalized as the sample size.

Employee email address breach data was collected from publicly available internet sources using SHODAN (Sentient Hyper-Optimized Data Access Network). SHODAN, a tool capable of searching for information on internet-connected devices and services, was deemed appropriate for this study due to its comprehensive data collection capabilities. Specifically, SHODAN's API was utilized with keywords such as "email" and "company" to identify the number of breaches associated with each company.

- **Email address breach incidents (dependent variable)**: The primary indicator of the scale of data breaches.
- **Number of related locations (independent variable 1)**: The number of locations a company owns, extracted from TSR's data.
- **Location density (independent variable 2)**: The ratio of the number of locations to the number of employees. For example, a company with 10 locations and 100 employees would have a value of 0.1.
- **Breach rate based on years of establishment (independent variable 3)**: The breach rate based on the company's years of establishment.
- **Leak frequency per employee (independent variable 4):** The number of breach incidents divided by the number of employees.

In the analysis, simple linear regression was first used to assess the individual effects of each independent variable on the number of email address breaches. However, due to the complexity of the relationships, multiple regression analysis was adopted to account for interactions between variables and perform multivariate analysis. To address potential multicollinearity, the Variance Inflation Factor (VIF) was calculated. Since all VIF values were below 10, multicollinearity was not deemed to be an issue. The results of these analyses provide foundational data for evaluating the impact of corporate characteristics on information leakage risks, with specific relationships discussed in the following chapter.

RESULTS

In this study, descriptive statistics were conducted to understand the overall characteristics of the data and to identify the corporate characteristics influencing information leakage risks in Japanese companies (Table 1). This analysis revealed the basic trends and distribution characteristics of both the independent and dependent variables.

Table 1. Descriptive Statistics

Variable	Observations	Mean	Std. Dev.	Min	0.25	0.50	0.75	Max
Email address breach incidents	399	39.54	79.37	0.00	4.00	15.00	43.00	1000.00
Number of related locations	399	7.86	15.60	1.00	2.00	5.00	8.00	130.00
Location density	399	0.13	0.36	0.00	0.02	0.05	0.12	5.00
Breach rate based on years of establishment	399	0.85	1.78	0.00	0.09	0.34	0.96	26.32
Leak frequency per employee	399	0.33	0.52	0.00	0.05	0.16	0.41	4.87

Next, multiple regression analysis was conducted to identify the factors influencing information leakage risks in Japanese companies. The results show that the model has a high goodness of fit and that several explanatory variables have a significant impact on information leakage risks (Table 2).

2026, 7(1), 43-60, https://doi.org/10.46656/access.2026.7.1(3)
ISSN 2683-1007 (Online)
https://journal.access-bg.org/

Table 2. Results of Multiple Regression Analysis

Indicator	Value
R-squared	0.850
Adjusted R-squared	0.849
F-statistic	558.4
Prob (F-statistic)	7.61E-161*
Durbin-Watson	1.540

The regression results indicate that the model's R-squared value is 0.850, meaning that approximately 85.0% of the variance in email address breach incidents is explained by the model. This suggests that the independent variables—number of related locations, location density, breach rate based on years of establishment, and leak frequency per employee—are highly explanatory of email address breach incidents. Furthermore, the adjusted R-squared value is 0.849, which closely matches the R-squared value, confirming that the model does not include excessive explanatory variables, and the overall fit is good.

The F-statistic for evaluating the overall significance of the model is 558.4, with a corresponding p-value of 7.61E-161, which is very small. This result strongly supports the significance of the model and confirms that at least one independent variable significantly affects email address breach incidents. Additionally, the Durbin-Watson statistic is 1.540, indicating potential weak autocorrelation in the residuals. The results should be interpreted with this consideration of autocorrelation. The regression coefficients for each independent variable are presented in Table 3.

Table 3. Detailed Regression Coefficients

Variable	Coefficient	Standard Error	t-value	p-value	95% CI [0.025]	95% CI [0.975]
Number of Related locations	0.3472	0.131	2.644	0.009*	0.089	0.605
Location density	-16.3381	5.684	-2.874	0.004*	-27.513	-5.164
Breach rate based on years of establishment	37.9378	1.048	36.212	<0.001***	35.878	39.997
Leak frequency per employee	16.2896	3.554	4.583	<0.001***	9.302	23.277

1. Number of related locations: Expansion of management scope increases risk
   The regression coefficient for the number of related locations is 0.3472, which is statistically significant (p = 0.009). This result indicates that for each additional location, the number of email address breaches increases by approximately 0.35 incidents. A higher number of locations leads to a broader data management scope and makes it more challenging to maintain control, thereby increasing the risk of

2026, 7(1), 43-60, https://doi.org/10.46656/access.2026.7.1(3)
ISSN 2683-1007 (Online)
https://journal.access-bg.org/

leakage. This finding suggests the importance of developing unified security policies across multiple locations and standardizing data protection methods between sites.

2. Location density: Higher density reduces leakage incidents
   The regression coefficient for location density is -16.3381, which is statistically significant ($p = 0.004$). This result shows that as the number of locations per employee increases, the number of email address breaches decreases by an average of 16.34 incidents. A higher location density facilitates more efficient monitoring and management, making it easier to implement centralized security measures. This finding supports the view that efficient location placement and resource allocation contribute to reducing information leakage risks.
3. Breach rate based on years of establishment: Vulnerabilities of legacy systems
   The regression coefficient for the breach rate based on years of establishment is 37.9378, indicating a very high statistical significance ($p < 0.001$). This result suggests that for each unit increase in the breach rate based on years of establishment, the number of email address breaches increases by approximately 37.94 incidents. Particularly for older companies, the use of legacy systems or a lack of regular updates may introduce security vulnerabilities. This finding implies that older companies need to adopt the latest technologies and security measures and modernize their systems to mitigate risks.
4. Leak frequency per employee: Challenges in education and management
   The regression coefficient for leak frequency per employee is 16.2896, which is highly statistically significant ($p < 0.001$). This result indicates that for each unit increase in the leak frequency per employee, the number of email address breaches increases by approximately 16.29 incidents. A lack of security awareness among employees can lead to higher internal risks. This finding highlights the importance of implementing security education programs for employees and tightening access management.

Additionally, a residual plot (Figure 1) was created to visually assess the goodness of fit and the validity of the model's assumptions. The horizontal axis represents the predicted values, while the vertical axis represents the residuals (the difference between observed and predicted values). It was confirmed that the residuals are randomly scattered around zero.

ACCESS Journal:
Access to Science, Business, Innovation in Digital Economy
2026, 7(1), 43-60, https://doi.org/10.46656/access.2026.7.1(3)
ISSN 2683-1007 (Online)
https://journal.access-bg.org/

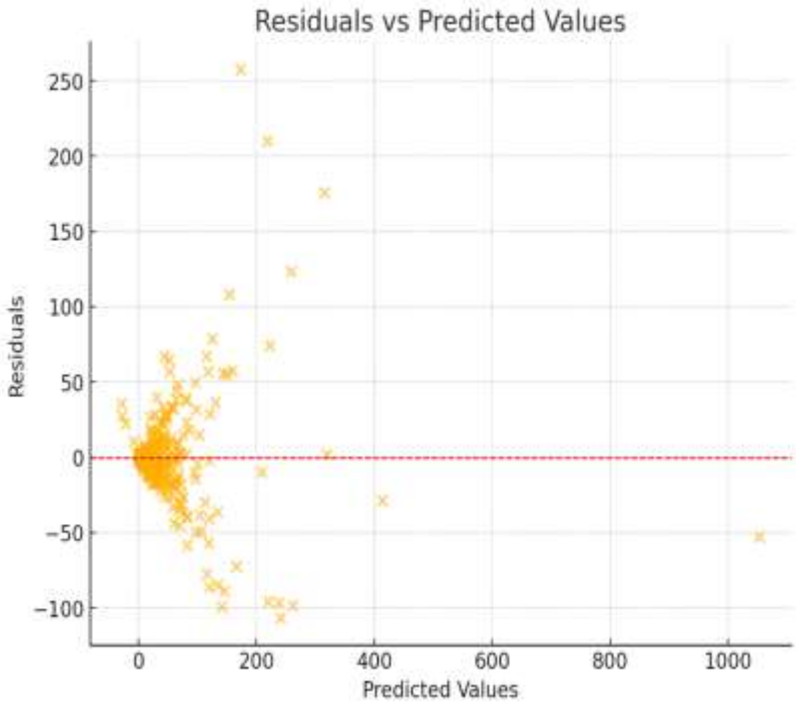

Figure 1. Residual Plot (Residuals vs. Predicted Values)

Figure 1 is a residual plot created to evaluate the goodness of fit and the validity of assumptions for the regression model. The plot shows the residuals against the predicted values, with the residuals randomly scattered around zero, confirming that there are no significant biases or nonlinearity in the model. Moreover, the plot shows no specific patterns or biases, supporting the assumption of homoscedasticity. The absence of outliers or influential data points further indicate that the model's estimates are reliable. This result suggests that the independent variables effectively explain the impact on email address breach incidents.

DISCUSSION

This study empirically analyzed the impact of corporate characteristics on information leakage risks in Japanese companies. The results reveal that corporate characteristics such as the number of related locations, location density, breach rate based on years of establishment, and leak frequency per employee influence information leakage risks through different mechanisms. These findings systematically demonstrate how specific corporate characteristics contribute to the increase or decrease of information leakage risks.

In Hypothesis 1, it was shown that an increase in the number of related locations amplifies information leakage risks. Specifically, when it is difficult to maintain standardized security standards across locations, decentralized management becomes a factor that creates security holes. Lehto & Limnéll (2021) point out that decentralized management hinders effective risk response, highlighting the need for unified security management. Additionally, Fadziso et al. (2023) demonstrate that the increase in supply chain attacks poses the risk of security incidents at one location spreading to other locations. The results of this study align with these previous findings and reinforce the argument that an increase in the number of related locations is a

 ISSN 2683-1007 (Online)
https://journal.access-bg.org/

primary factor amplifying information leakage risks. Furthermore, the introduction of unified security policies and the Zero Trust model is suggested as an effective strategy to mitigate this issue.

In Hypothesis 2, it was confirmed that higher location density helps reduce information leakage risks. In environments with high location density, resource centralization and efficient allocation enhance security governance. Anwar & Abdullah (2021) show that resource efficiency promotes rapid decision-making and improved governance, which supports the findings of this study. Mughal (2022) also demonstrates that centralized security architectures preserve policy consistency and play a key role in reducing security holes. This study clearly illustrates that higher location density contributes to the reduction of information leakage risks, emphasizing the importance of efficient resource allocation and management systems.

In Hypothesis 3, it was found that companies with a longer establishment period tend to have higher information leakage risks. The main cause of this risk lies in reliance on legacy systems and outdated information management processes. Solms & Niekerk (2013) point out that static security models cannot address the latest threats, emphasizing the need for dynamic and adaptive frameworks. Schatz et al. (2017) argue that the historical structures of long-established companies lead to a lack of consistency in security management, which increases risks. The results of this study specifically demonstrate the amplification mechanism of information leakage risks in long-established companies and stress the necessity of implementing dynamic risk management systems.

In Hypothesis 4, it was confirmed that companies with a higher leak frequency per employee experience amplified risks due to human factors. Bulgurcu et al. (2010) show that information security awareness (ISA) promotes policy compliance and contributes to risk mitigation, supporting the importance of employee training. Alahmari & Duncan (2020) highlight that the absence of education programs leads to operational errors and internal fraud, which amplify information leakage risks. The results of this study indicate that, in addition to technical measures, fostering a security-conscious culture across the organization is essential.

Overall, this study clarifies the mechanisms behind information leakage risks based on corporate characteristics and presents concrete strategies for risk reduction. Unified security management, resource optimization, dynamic risk management systems, and enhanced employee education are elements that, when combined, contribute to information leakage risk management. The findings of this study provide a theoretical foundation while offering practical guidance for addressing challenges in this area.

CONCLUSION

This study empirically analyzed the impact of corporate characteristics on information leakage risks in Japanese companies, highlighting the intersection between management strategy and information security. The analysis revealed that for companies with a higher number of related locations, the complexity of information management increases, thereby amplifying the risk. Conversely, companies with a higher location density benefit from efficient resource allocation and enhanced governance, which reduce risk. Additionally, for companies with a longer establishment period, system aging may increase risk, while mature management systems may contribute to risk mitigation. Furthermore, companies with a higher leak frequency per employee underscore the importance of internal controls and employee education. These findings provide a critical foundation for developing a framework for information leakage risk management that takes corporate characteristics into account.

This study has several limitations. It focuses on Japanese companies and does not consider factors such as organizational culture and leadership. Moreover, the applicability of the findings to companies in other regions or industries has not been tested. Future research should address these gaps by conducting comparative analyses across industries and incorporating a comprehensive approach that includes organizational culture to further clarify the mechanisms of information leakage risk.

This research contributes to the academic field by complementing previous information security studies, which often focused on technical approaches or industry-wide trends, with a systematic investigation of how corporate characteristics affect information leakage risk. Notably, this study quantitatively examined characteristics such as the number of related locations, location density, breach rate based on years of establishment, and leak frequency per employee, clarifying the mechanisms of their interactions and impacts on risk. Additionally, by proposing a framework for risk management that considers corporate characteristics, this study offers a practical foundation for improving practices within the information security domain. It presents a roadmap for companies to reduce information leakage risks, strengthen competitiveness, and achieve sustainable growth.

The outcomes of this study contribute not only to the academic advancement of information security but also provide practical guidelines that can be utilized in practice. These insights are beneficial for enhancing the sustainable growth and international competitiveness of Japanese companies.

Author Contributions: T.I., H.S., and T.O. contributed to the conceptualization of the study; T.I. and H.S. developed the methodology; T.I. and K.G. performed the formal analysis; K.G. and T.O. conducted the investigation; project administration was managed by T.I., H.S., and T.O.; data curation was handled by T.I., H.S., and T.O.; resources were provided by T.I., H.S., and K.G.; T.O. supervised the study; validation was carried out by K.G. and H.S.; the original draft was prepared by T.I., and the manuscript was reviewed and edited by T.I., H.S., and T.O. All authors have read and agreed to the published version of the manuscript.

Informed Consent Statement: Not applicable.

Data Availability Statement:

The data presented in this study are available on request from the corresponding author.

Institutional Review Board Statement: Not applicable.

Conflict of interest:

The authors declare no conflict of interest.

References

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal,* 5(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699

Adewusi, A. O., Chiekezie, N. R., & Eyo-Udo, N. L. (2022). Cybersecurity threats in agriculture supply chains: A comprehensive review. *World Journal of Advanced Research and Reviews*, 15(3), 490–500. https://doi.org/10.30574/wjarr.2022.15.3.0888

Alahmari, A. A., & Duncan, R. A. (2021). Towards cybersecurity risk management investment: A proposed encouragement factors framework for SMEs. 2021 IEEE International Conference on Computing (ICOCO). https://doi.org/10.1109/ICOCO53166.2021.9673554

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). https://doi.org/10.1109/CyberSA49311.2020.9139638

Albert, D. (2024). What do you mean by organizational structure? Acknowledging and harmonizing differences and commonalities in three prominent perspectives. *Journal of Organization Design,* 13, 1–11. https://doi.org/10.1007/s41469-023-00152-y

Ambreen, L., Jain, M., Yadav, R. K., & Loonkar, S. (2023). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. Multidisciplinary Reviews, 6, e2023ss080. https://doi.org/10.31893/multirev.2023ss080

Anwar, G., & Abdullah, N. N. (2021). The impact of human resource management practices on organizational performance. International Journal of Engineering, Business and Management, 5(1), 35–46. https://doi.org/10.22161/ijebm.5.1.4

Ansari, M. F., Sharma, P., & Dash, B. (2022). Prevention of phishing attacks using AI-based cybersecurity awareness training. International Journal of Smart Sensor and Adhoc Network, 3(3), 61–72. https:/doi.org/10.47893/ijssan.2022.1221

Ashley, C., & Preiksaitis, M. (2022). Strategic cybersecurity risk management practices for information in small and medium enterprises. *Business Management Research and Applications: A Cross-Disciplinary Journal*, 1(2), 109–157. Retrieved from https://bmrajournal.columbiasouthern.edu/index.php/bmra/article/view/3421

Aslan, Ö., Aktuğ, S. S., Özkan-Okay, M., Yılmaz, A. A., & Akın, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics,* 12(6), 1–42. https://doi.org/10.3390/electronics12061333

Bade, C., Olsacher, A., Boehme, P., Truebel, H., Bürger, L., & Fehring, L. (2024). *Sustainability in the pharmaceutical industry: An assessment of sustainability maturity and effects of sustainability measure implementation on supply chain security.* Corporate Social Responsibility and Environmental Management, 31(1), 224–242. https://doi.org/10.1002/csr.2564

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. https://doi.org/10.2307/25750690

Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy. *International Research Journal of Engineering and Technology*, 9(4), 2002. Retrieved from https://ssrn.com/abstract=4335361

Fadziso, T., Ballamudi, V. K. R., Desamsetti, H., Thaduri, U. R., & Dekkati, S. (2023). Evolution of the cybersecurity threat: An overview of the scale of cyber threat. *Digitalization & Sustainability Review*, 3(1), 1–12. https://doi.org/10.6084/m9.figshare.24189921.v1

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal (PUIIJ*), 2(1), 51–75. https://doi.org/10.5281/zenodo.10639463

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a cyber-security culture framework. *Sensors,* 21(9), 2–14. https://doi.org/10.3390/s21093267

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal*, 35, 486–505. https://doi.org/10.1057/s41284-021-00286-2

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of Things. *Heliyon*, 7(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z., & Iyengar, A. (2020). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys*, 54(1), 1–36. https://doi.org/10.1145/3423165

Kävrestad, J., Nilsson, P., & Smith, L. (2024). A taxonomy of factors that contribute to organizational cybersecurity awareness (CSA). *Information and Computer Security*. https://doi.org/10.1108/ICS-11-2023-0209

Kiruthiga, T., Vaniprabha, A., & Sutharsan, M. (2021). An improved intelligence approach to handling data leakage risks in the corporate information security process. *BOHR International Journal of Smart Computing and Information Technology*, 2(1), 39–45. https://doi.org/10.54646/bijscit.2021.17

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cybersecurity: Case Finland. *Information Security Journal: A Global Perspective*, 30(3), 139–148. https://doi.org/10.1080/19393555.2020.1813851

Mughal, A. A. (2022). Well-architected wireless network security. *Journal of Humanities and Applied Science Research*, 5(1), 32–41. Retrieved from https://journals.sagescience.org/index.php/JHASR/article/view/52

Nawaz, H., Sethi, M. S., Nazir, S. S., & Jamil, U. (2024). Enhancing national cybersecurity and operational efficiency through legacy IT modernization and cloud migration: A US perspective. *Journal of Computing & Biomedical Informatics*, 7(2). https://doi.org/10.56979/702/2024. Article ID: 536-0702/2024.

Neri, M., Niccolini, R., & Martino, G. (2024). Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment. *Information and Computer Security*, 32(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

Obioha-Val, O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). *Strengthening cybersecurity measures for the defense of critical infrastructure in the United States. Asian Journal of Research in Computer Science, 17*(11), 25–45. https://doi.org/10.9734/ajrcos/2024/v17i11517

Pang, M.-S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government. *The Journal of Strategic Information Systems,* 31(1), 1–40. https://doi.org/10.1016/j.jsis.2022.101707

Patel, N. (2024). SECURE ACCESS SERVICE EDGE (SASE): Evaluating the impact of converged network security architectures in cloud computing. *Journal of Emerging Technologies and Innovative Research*, 11(3), e703–e714

Ponnusamy, S., & Eswararaj, D. (2023). Navigating the modernization of legacy applications and data: Effective strategies and best practices. *Asian Journal of Research in Computer Science*, 16(4), 239–256. https://doi.org/10.9734/AJRCOS/2023/v16i4386

Rao, F. A., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 2–38. https://doi.org/10.3390/app11083383

Riahi, S., & Islam, M. (2024). Employees' information security awareness (ISA) in public organisations: Insights from cross-cultural studies in Sweden, France, and Tunisia. *Journal of Information Security and Privacy*, 12(1), 45–67. https://doi.org/10.1080/0144929X.2024.2311734

Saeidian, S., Cervia, G., Oechtering, T. J., & Skoglund, M. (2021). *Quantifying membership privacy via information leakage.* IEEE Transactions on Information Forensics and Security, 16, 3096–3109. https://doi.org/10.1109/TIFS.2021.3073804

Savin, V. D., & Năstase Anysz, R. (2021). *Cybersecurity threats and vulnerabilities of critical infrastructures. American Research Journal of Humanities and Social Science, 4*(7), 90–96. http://www.arjhss.com

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2), Article 8. https://doi.org/10.15394/jdfsl.2017.1476

Vallabhaneni, R., Vaddadi, S. A., Pillai, S. E. V. S., Addula, S. R., & Bhuvanesh, A. (2024).MobileNet-based secured compliance through open web application security projects in cloud system. *Indonesian Journal of Electrical Engineering and Computer Science*, 35(3), 1661–1669. https://doi.org/10.11591/ijeecs.v35.i3.pp1661-1669

Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A threat-based cybersecurity risk assessment approach addressing SME needs. ARES '21: Proceedings of the 16th International Conference on Availability, Reliability and Security, 158, 1–12. https://doi.org/10.1145/3465481.3469199

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Zafarovich, K. R., & Sabirkhoja ugli, S. M. (2024). Information security in the era of the digital economy: Challenges and strategies. *Journal of Economics and Business Management*, 7(4), 50–59. https://doi.org/10.5281/zenodo.11082055

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cybersecurity awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

About the authors

Takaaki ISHIKAWA

Ph.D. in Technology Management. Visiting Research Fellow, OIC Research Organization, Ritsumeikan University, Osaka, Japan. Co-Founder and CEO of SingleID K.K., a cybersecurity startup.

Research interests: technology management, competitive strategy, startup management.

ORCID ID: 0009-0003-1720-9193

Hiroyuki SUZUKI

Chief Technology Officer (CTO), SingleID K.K., Tokyo, Japan. Co-Founder of SingleID K.K., a cybersecurity startup specializing in secure authentication and network access control.

Research interests: cybersecurity engineering, IT infrastructure, applied innovation in digital enterprises.

ORCID ID: 0009-0004-7848-6482

Kiminori GEMBA

Professor, Graduate School of Innovation Management, Hosei University Business School, Tokyo, Japan.

Research interests: business strategy, innovation strategy, science and technology policy.

ORCID ID: 0000-0002-0309-0764

ACCESS Journal:
Access to Science, Business, Innovation in Digital Economy
2026, 7(1), 43-60, https://doi.org/10.46656/access.2026.7.1(3)

ISSN 2683-1007 (Online)

https://journal.access-bg.org/

Tetsuaki ODA

Professor, Graduate School of Technology Management (MOT), Ritsumeikan University, Osaka, Japan.

Research interests: intellectual property strategy, intellectual property management, healthcare and welfare.

ORCID ID: 0000-0002-6484-8460