Journal of Applied Finance & Banking, Vol. 15, No. 1, 2025, 91-110
ISSN: 1792-6580 (print version), 1792-6599(online)
https://doi.org/10.47260/jafb/1515
Scientific Press International Limited

Determinants of Information Security Risks in Multinational Enterprises: A Comprehensive Analysis

Cheng-Wen Lee[1] and Ming-Yung Chen[2]

Abstract

This study seeks to systematically identify and evaluate the critical factors influencing information security risks in multinational enterprises (MNEs). To develop a robust framework for assessing these risks, a preliminary set of indicators was constructed through an extensive review of existing literature and in-depth expert interviews. To ensure the validity and reliability of the framework, the Delphi method was employed to achieve expert consensus, while the Analytic Hierarchy Process (AHP) was utilized to quantify and establish the relative weights assigned to each indicator. The findings reveal that information security risk management is significantly influenced by six interrelated dimensions: technical factors, organizational management practices, personnel-related issues, regulatory compliance, external environmental conditions, and Environmental, Social, and Governance (ESG) practices. These dimensions collectively shape the vulnerability landscape of enterprises, emphasizing the need for a holistic and structured approach to mitigating information security risks in complex multinational business environments.

JEL classification numbers: H25, I115, J48.
Keywords: International Enterprises, Information Security, Risk Management, Cloud Security, ESG.

[1] Department of International Business, College of Business, Chung Yuan Christian University. Taoyuan City, Taiwan.
[2] Ph. D. Program in Business, College of Business, Chung Yuan Christian University. Taoyuan City, Taiwan.

Article Info: *Received:* February 5, 2025. *Revised:* February 19, 2025.
Published online: February 26, 2025.

1. Introduction

The background and motivation for this study arise from the swift progress of globalization, which has caused enterprise information systems to face an increasing number of internal threats and external attacks. These threats may emanate from hackers, competitors, or even partners within the supply chain. Therefore, developing a robust information security risk management framework is crucial to ensure business continuity and maintain a competitive edge.

The research questions guiding this study are as follows. First, what are the primary determinants of information security risks within multinational enterprises (MNEs)? This question aims to identify and analyze various contributing factors, including technological vulnerabilities, human behavior, regulatory compliance, and organizational culture, all of which influence the security posture of MNEs on a global scale. Second, what is the relative significance of these identified factors concerning information security risks? This question seeks to assess and prioritize each factor's impact, determining which aspects are most critical to address to effectively mitigate risks and enhance the overall security framework. Third, how can a comprehensive and practical framework of indicators be developed to support effective information security risk management? This inquiry focuses on constructing a robust set of metrics and indicators that can be applied in real-world scenarios to evaluate and improve information security practices, enabling organizations to proactively manage and respond to security threats.

This study begins by identifying an initial set of indicators through a comprehensive review of the existing literature. Subsequently, in-depth interviews are conducted with experts in the field of information security to evaluate and refine these indicators. Following this, the revised set of indicators undergoes multiple rounds of expert consultation using the Delphi method to achieve consensus. Finally, the Analytic Hierarchy Process (AHP) is employed to determine the relative weights of each indicator, thereby establishing a structured and quantifiable framework for information security risk management.

2. Literature Review

In the context of globalization and digitalization, MNEs are facing an increasing variety of complex and diverse information security risks. To effectively address these challenges, organizations must identify and manage these risks from six critical perspectives: technical factors, organizational management factors, personnel factors, regulatory and compliance factors, external environmental factors, and ESG (Environmental, Social, and Governance) factors.

2.1 Technical Factors

First and foremost, technical factors form the cornerstone of information security within enterprises. Network security is essential for protecting enterprise information systems against unauthorized access and cyberattacks. This is achieved through the use of tools such as firewalls, intrusion detection systems, and antivirus

software (Whitman and Mattord, 2009). Data protection includes mechanisms such as encryption, backup, and recovery, which ensure the confidentiality and integrity of data during both storage and transmission (Pfleeger, et al. 2006).
Application security focuses on implementing protective measures throughout the software development lifecycle, with an emphasis on vulnerability management to address security flaws during development, testing, and operation. This proactive approach aims to prevent application-layer attacks (McGraw, 2012). Endpoint security, which involves protecting terminal devices such as computers and mobile devices used by employees, requires the installation, updating, and configuration of security software (Easttom, 2019). As cloud services become increasingly prevalent, cloud security has emerged as a vital component of information security. This encompasses practices such as data encryption, identity authentication, and access control within the cloud environment (Chen and Zhao, 2012).

2.2 Organizational Management Factors

Organizational management factors play a vital role in establishing the foundation for effective enterprise information security management. The development and implementation of robust security policies and procedures are essential for guiding security activities, as they provide clear direction and standards under ISO/IEC 27005:2018 (Fahmi et al., 2021). Risk management is a critical component that involves identifying, assessing, and addressing information security risks, enabling organizations to respond swiftly to potential threats. By implementing security awareness and training programs, organizations can enhance employees' understanding of information security and their motivation to adhere to established policies, which is crucial for mitigating human errors and internal threats (Ifinedo, 2012). Additionally, formulating and executing incident response plans allows organizations to react promptly and recover effectively from information security incidents, thereby minimizing their impact on business operations (Whitman and Mattord, 2009).

2.3 Personnel Factors

Personnel factor play a significant role in the internal risk management of enterprise information security, encompassing employee behavior, internal threats, and staff turnover. The conduct of employees is vital for upholding information security; research shows that employees' awareness and compliance with information security policies have a considerable impact on the overall security posture of organizations (Bulgurcu, et al. 2010). Internal threats often stem from security risks associated with both the intentional and unintentional actions of employees, which can include data theft, sabotage, and fraud (Cappelli, et al. 2012). Furthermore, high staff turnover may lead to insufficient security training for new employees, consequently increasing security risks (D'Arcy and Hovav, 2009).

2.4 Regulatory and Compliance Factors

Regulatory and compliance considerations are vital for ensuring that enterprises function within legal frameworks. Adhering to legal regulations is essential for maintaining enterprise information security, with standards such as GDPR establishing stringent guidelines for the handling and protection of personal data in 2018 (Yu et al., 2021). Regular compliance reviews are essential for ensuring that enterprises adhere to applicable laws, regulations, and internal policies across their operations. These reviews play a critical role in strengthening the effectiveness of information security management systems by identifying potential gaps and facilitating continuous improvement by the National Institute of Standards and Technology (NIST) in 2013 (Kurii and Opirskyy, 2022).

2.5 External Environmental Factors

External environmental factors include supply chain security, external threats, and industry competition, all of which present various security risks and shape the competitive landscape for businesses. Supply chain security focuses on the information security status of suppliers and third-party partners; therefore, businesses need to ensure that every aspect of their supply chain meets established security standards to prevent incidents arising from vulnerabilities within it (Boyson, 2014). External threats predominantly stem from hackers, malware, and other types of attackers. As these threats have grown increasingly sophisticated and destructive, businesses must continuously enhance their defenses to mitigate the risk of external attacks (Schneier, 2015). Additionally, industry competition can impact information security, as competitors may seek to acquire sensitive information through unethical means, compelling businesses to adopt measures that protect their competitive advantage (Porter, 2008).

2.6 ESG Practices

ESG factors encompass environmental responsibility, social responsibility, corporate governance, board engagement, and the roles played by audit committees, highlighting the commitments and actions of organizations in these crucial areas. Environmental responsibility refers to the initiatives that businesses undertake to safeguard the environment and promote sustainable development. Such efforts not only enhance corporate reputation but also help mitigate potential environmental risks to their operations (Eccles, et al. 2014).

Social responsibility encompasses a company's commitment to investing in community-oriented initiatives, which include community development, employee welfare, and charitable activities (McWilliams and Siegel, 2001). The framework of corporate governance—specifically the composition and functioning of the board of directors, along with management transparency and independence—is essential for fostering transparent and effective decision-making. This approach minimizes information security risks (Larcker and Tayan, 2020).

Table 1: Factors Influencing Information Security Risks in MNEs

Factors	Attributes	Sources
Technical	1. Network Security	Whitman and Mattord (2009)
	2. Data Protection	Pfleeger,Pfleeger, and Margulies, (2006)
	3. Application Security	McGraw (2012)
	4. Endpoint Security	Easttom (2019)
	5. Cloud Security	Chen and Zhao (2012)
Organizational Management	6. Security Policies and Procedures	Fahmi et al. (2021)
	7. Risk Management	Fahmi et al. (2021)
	8. Security Awareness and Training	Ifinedo (2012)
	9. Incident Response Plan	Whitman and Mattord (2009)
Personnel	10. Employee Behavior	Bulgurcu, Cavusoglu, and Benbasat (2010)
	11. Internal Threats	Cappelli, Moore, and Trzeciak (2012)
	12. Staff Turnover	D'Arcy and Hovav (2009)
Regulatory and Compliance	13. Legal and Regulatory Compliance	Yu et al. (2021)
	14. Compliance Review	Kurii & Opirskyy (2022)
External Environment	15. Supply Chain Security	Boyson (2014)
	16. External Threats	Schneier (2015).
	17. Industry Competition	Porter (2008)
ESG Practices	18. Environmental Responsibility	Eccles, Ioannou, and Serafeim (2014)
	19. Social Responsibility	McWilliams and Siegel (2001)
	20. Corporate Governance	Larcker and Tayan (2020)
	21. Board Participation	Adams and Ferreira (2009)
	22. Audit Committee	DeFond and Francis (2005)

Board engagement encompasses the active attention and strategic involvement of directors in a company's information security initiatives, which is crucial for strengthening the overall effectiveness of information security management (Adams and Ferreira, 2009). In this context, the audit committee assumes a pivotal role in overseeing the organization's information security risk management framework, ensuring compliance with relevant legal, regulatory, and internal policy requirements, while also assessing the efficacy of existing risk mitigation strategies (DeFond and Francis, 2005). Therefore, by systematically integrating these six key dimensions and their corresponding factors, as outlined in Table 1, enterprises can enhance their ability to identify, assess, and manage information security risks. This, in turn, fosters a more resilient security posture and strengthens organizational competitiveness in an increasingly complex digital landscape.

3. Research Methodology

3.1 Research Methods

This study employs a combination of the Delphi method and the Analytic Hierarchy Process (AHP) to comprehensively identify and quantify the critical factors that contribute to information security risks within large multinational organizations. By utilizing the Delphi method, we gather expert opinions through a series of structured rounds, allowing for the refinement of ideas and the establishment of consensus among participants. The AHP then facilitates the systematic evaluation of these factors by assigning weights, thereby prioritizing them based on their influence on security risk levels. The research process is meticulously illustrated in Figure 1, which outlines the various stages involved in data collection, expert consultation, and subsequent analysis. This approach ensures a robust framework for assessing information security risks, ultimately leading to actionable insights for organizations aiming to enhance their security posture in a complex global environment.

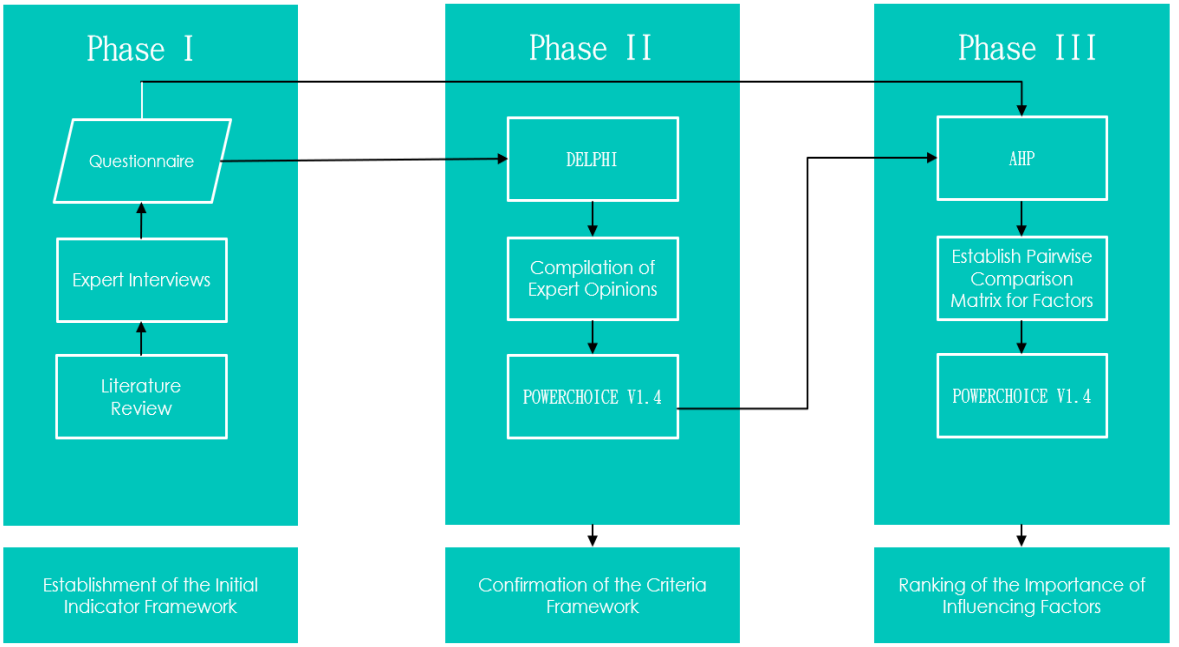

Figure 1: Research Process

3.2 Delphi Method

The Delphi Method is a structured communication technique primarily employed for forecasting, decision-making, and collecting expert opinions on a particular subject. Developed by the RAND Corporation in the 1950s, it has since become a widely utilized tool in research, planning, and policy formulation. Below is a comprehensive overview of the Delphi Method, encompassing its purpose, process, and key principles. This systematic expert consultation technique achieves consensus through multiple rounds of anonymous questionnaires. The Delphi Method seeks to gather and refine expert opinions to achieve a consensus on complex issues, forecast future trends or outcomes based on expert insights, and enhance decision-making in scenarios characterized by uncertainty or incomplete information (Skulmoski, et al. 2007). This method is especially valuable when the problem at hand is intricate and cannot be resolved by an individual alone, when experts with varied perspectives are accessible yet geographically distributed, and when objective data is limited, necessitating the use of subjective judgments.

The Delphi Method is based on the following principles (Fish and Busby, 1996):

(1) Anonymity of Participants: Experts provide their opinions anonymously to avoid the influence of dominant personalities and groupthink. (2) Iterative Process: Multiple rounds of questionnaires are used to refine opinions and move toward consensus. (3) Controlled Feedback: Participants receive summarized feedback from previous rounds, allowing them to reconsider their views based on the group's collective input. (4) Statistical Aggregation: Responses are analyzed quantitatively, often using measures like median, mean, or interquartile range to represent group consensus.

The Delphi Method typically involves the following steps:

1. Selection of Experts

A group of experts is selected based on their knowledge and experience related to the topic. The group can include 10 to 50 participants, depending on the goals and scope of the study.

2. Development of Questionnaires

The initial questionnaire typically consists of open-ended questions, inviting participants to express their views, predictions, or priorities regarding the topic. Follow-up questionnaires are structured according to the responses from the prior round.

3. First Round

Experts respond to the initial questionnaire, sharing their insights and opinions. The responses are collected, analyzed, and then summarized.

4. Feedback and Refinement

A summary of the first-round results is provided to participants as controlled feedback. Experts then review this feedback and respond to a more focused questionnaire in the next round. This process enables participants to adjust their opinions based on the collective input of the group.

5. Iterative Rounds

The feedback and refinement process lasts for two to four rounds, or until a consensus is reached. In later rounds, experts may be asked to justify outlier opinions or rank their preferences.

6. Final Consensus

The process ends when a stable consensus is reached or when further rounds show diminishing returns. The final findings are analyzed and compiled into a report that highlights the group's collective insights along with areas of agreement and disagreement.

In this study, a total of 15 experts in the field of information security were invited to participate in a Delphi survey aimed at assessing and refining the initial indicator framework. Among the participants, there were 9 experts with over 20 years of experience, 3 experts with 10 to 20 years of experience, and 3 experts with 5 to 10 years of experience, as detailed in Table 2.

Table 2: Experts Profile

No	Job Title	Expertise	Industry Field	Years of Experience
01	Sr. Security PM	Threat Intelligence	Cybersecurity	10
02	Sr. Security PM	Threat Intelligence	Cybersecurity	25
03	Sr. Security Director	SOC	Cybersecurity	25
04	Sr. Security Director	Security Technical	Cybersecurity	20
05	Security Director	Security Technical	Cybersecurity	26
06	Sr. Security Engineer	Information Security Laws and Regulations	Cybersecurity	8
07	Sr. Security Engineer	Security Technical	Cybersecurity	10
08	Sr. Security PM	SOC	Cybersecurity	23
09	Sr. Security PM	Security Technical	Cybersecurity	15
10	Sr. Security PM	Information Security Laws and Regulations	Cybersecurity	28
11	Security VP	Security Technical	Cybersecurity	25
12	Sr. Security Engineer	SOC	Cybersecurity	7
13	Sr. Security Engineer	SOC	Cybersecurity	8
14	Sr. Security PM	Security Technical	Cybersecurity	20
15	Application Director	Application Development	Cybersecurity	30

3.3 Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP) is a quantitative decision analysis method that determines the relative weights of each indicator by constructing a hierarchical model and utilizing pairwise comparison matrices (Darko, et al, 2019). In this study, the AHP method was employed to calculate the weights of various dimensions and criteria. AHP is a structured decision-making approach used to prioritize and select among multiple alternatives by assessing their relative significance based on different criteria. Developed by Thomas Saaty in the 1970s, this method is widely applied in fields such as project management, resource allocation, and policy planning. The steps in the AHP are as follows.

Step 1: Define the Problem and Goal

- Clearly state the decision problem and objective.
- Example: Selecting the best supplier for a company.

Step 2: Structure the Hierarchy

- Divide the problem into levels:

1. Goal: The ultimate objective (e.g., "Select the best supplier").
2. Criteria: Key factors influencing the decision (e.g., Cost, Quality, Delivery Time, and Reliability).
3. Alternatives: The options available (e.g., Supplier A, Supplier B, Supplier C).

Step 3: Pairwise Comparison of Criteria

- Compare criteria in pairs to evaluate their relative importance using a scale of relative importance:

1: Equal importance.
3: Moderate importance of one over the other.
5: Strong importance.
7: Very strong importance.
9: Extreme importance.
2, 4, 6, 8: Intermediate values.

- Construct a pairwise comparison matrix where:

Rows and columns represent criteria.
The diagonal values are always 1 (a criterion is equally important to itself).

Step 4: Calculate the Priority Weights

- Normalize the matrix by dividing each value in a column by the column total.
- Compute the average of each row to determine the weight of each criterion.

Step 5: Pairwise Comparison of Alternatives for Each Criterion

- For each criterion, compare alternatives pairwise to determine their relative preference.
- Repeat the steps of creating a pairwise comparison matrix, normalizing, and calculating priority weights.

Step 6: Synthesize Results

- Combine the weights of criteria with the weights of alternatives to calculate an overall score for each alternative.
- Use a weighted sum approach:

Identify the criteria C_1, C_2,…, C_n relevant to the decision problem and assign weights W_1, $W2$,…, W_n to each criterion, where:

$$\sum_{i=1}^{n} w_i = 1$$

Then, list the alternatives A_1, A_2,…, A_m. For each alternative, determine its performance score X_{ij} under each criterion C_i. The scores can be raw data or normalized values (e.g., scaled between 0 and 1). After this process, we calculate

the weighted sum for each alternative using the formula. In the final, we rank the alternatives based on their overall scores S_j, with the highest score indicating the best alternative.

$$S_j = \sum_{i=1}^{n} w_i \cdot x_{ij}$$

Step 7: Perform Consistency Check

We obtain the Pairwise Comparison Matrix (A) to first create the pairwise comparison matrix, where each entry a_{ij} indicates the relative importance of criterion i over criterion j. Then, calculate the Priority Vector (w) to normalize each column of the matrix A by dividing each entry by the sum of its column. Then, compute the priority vector (w) by averaging the rows of the normalized matrix. This gives the weights for the criteria. After that, to calculate the Weighted Sum Vector, multiply the pairwise comparison matrix (A) by the priority vector (w): $A \cdot w$=Weighted Sum Vector. In the following, we calculate the Consistency Index (CI) and determine the Consistency Ratio (CR).

$$CR = \frac{CI}{RI}$$

Step 8: Make the Decision

To arrive at a decision using the Analytic Hierarchy Process (AHP), we first conduct a thorough pairwise comparison of the alternatives under consideration (Satty, 1980). This involves evaluating each option against the others based on specific criteria and assigning relative importance scores. Once these comparisons are completed, we perform a consistency check to ensure that the judgments made are logically sound and reliable. Following this, we employ the weighted sum approach, where we calculate a weighted total for each alternative by multiplying the scores by their respective weights derived from the criteria. By integrating the consistency check results with the weighted sums, we can effectively identify the most suitable alternative for our decision-making process.

4. Research Results and Discussion

4.1 The Research Framework

Through a rigorous analysis of existing literature and in-depth consultations with domain experts, we systematically developed an initial indicator framework for assessing information security risks. This framework is structured around six fundamental dimensions, each representing a critical facet of information security, thereby ensuring a holistic and multidimensional evaluation of risk factors. Within these dimensions, we identified twenty-two specific criteria that function as quantifiable indicators, enabling a precise and systematic assessment of

vulnerabilities and threats. By integrating theoretical insights with expert perspectives, this framework enhances the robustness and applicability of risk assessment methodologies in the field of information security.

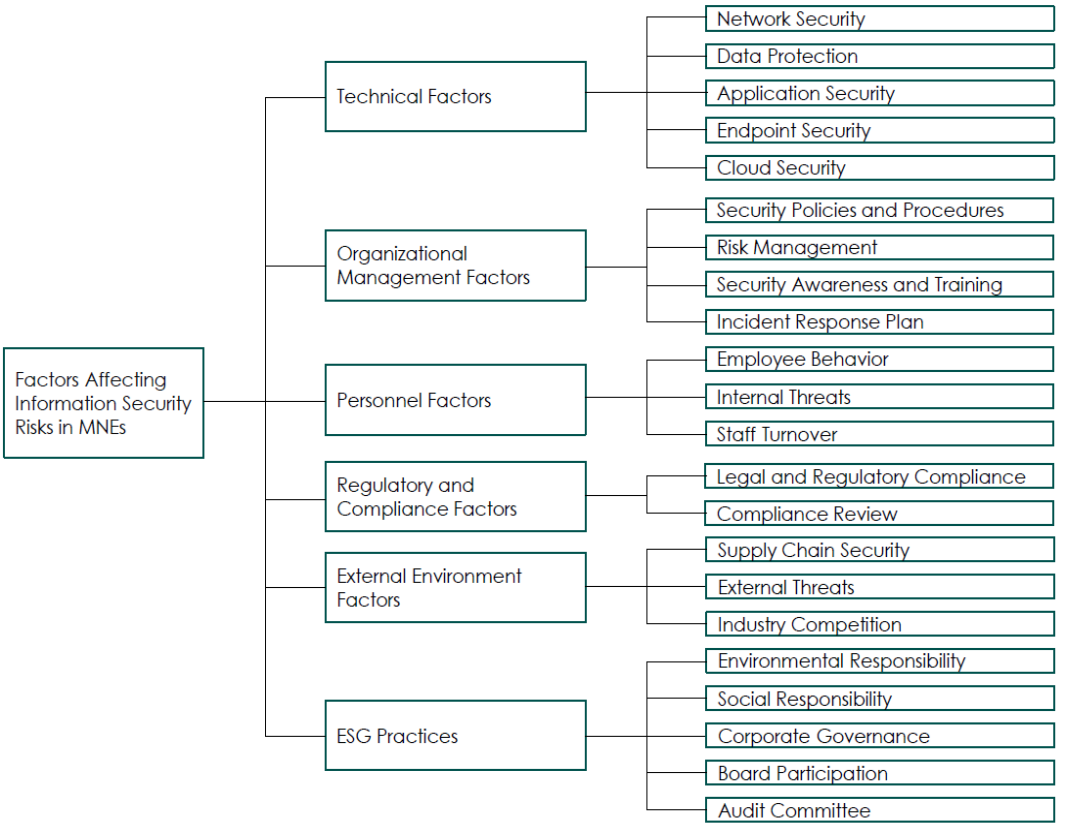

Figure 2: The Research Framework

Figure 2 presents a structured categorization of factors affecting information security risks in multinational enterprises (MNEs) and systematically organizes the critical dimensions and evaluation criteria essential for a comprehensive risk assessment, incorporating technical, organizational, personnel, regulatory/ compliance, external environmental factors, and ESG practices. Figure 2 highlights key components such as threat identification, impact assessment, mitigation strategies, compliance with international security standards, and the role of emerging technologies in risk management. By synthesizing these elements, the research framework facilitates a structured approach to understanding and addressing information security risks, ensuring a more robust and proactive security posture. Table 3 shows the description of the initial indicators.

Table 3: The Description of Initial Indicators

Factors	Attributes	Description
Technical	1. Network Security	Firewalls, intrusion detection systems, antivirus software, etc.
	2. Data Protection	Data encryption, data backup and recovery mechanisms
	3. Application Security	Security measures during the software development process and application vulnerability management
	4. Endpoint Security	Security protection measures for terminal devices
	5. Cloud Security	Security management and protection measures for cloud services
Organizational Management	6. Security Policies and Procedures	Development and implementation of information security policies
	7. Risk Management	Effectiveness of risk assessment and management mechanisms
	8. Security Awareness and Training	Security awareness and training programs for employees
	9. Incident Response Plan	Incident response and recovery plans for information security events
Personnel Factors	10. Employee Behavior	Safe behavior of employees using information systems
	11. Internal Threats	Intentional or unintentional security threats from internal personnel
	12. Staff Turnover	Impact of employee turnover on information security
Regulatory and Compliance	13. Legal and Regulatory Compliance	Compliance with relevant laws and regulations
	14. Compliance Review	Conducting regular compliance inspections and audits
External Environment	15. Supply Chain Security	Security status of suppliers and third-party partners
	16. External Threats	External attack risks from hackers and malicious actors
	17. Industry Competition	Impact of industry competition on enterprise information security
ESG Practices	18.Environment Responsibility	Measures taken by enterprises in environmental protection and sustainable development
	19. Social Responsibility	Investment in corporate social responsibility
	20. Corporate Governance	Corporate governance structure, management transparency, and independence
	21. Board Participation	Attention and participation of the board of directors in information security strategies
	22. Audit Committee	Supervision and evaluation of information security risks by the audit committee

4.2 Descriptive Insights into Influential Factors

Based on the results of the Delphi analysis, which employed a rigorous selection criterion of an average score greater than 3 and a coefficient of variation (CV) less than or equal to 0.5, the key indicators influencing information security risks were systematically identified and validated. These thresholds ensured that only indicators with a high degree of expert consensus were retained in the final framework. Among the assessed indicators, all except the 18th item, "environmental responsibility," met the predefined consensus standards. Specifically, the average scores and CVs of the remaining indicators demonstrated a strong level of agreement among experts, reinforcing their relevance and reliability in assessing information security risks (Table 4). This outcome underscores the robustness of the Delphi method in refining and prioritizing key risk factors, thereby contributing to the development of a comprehensive and empirically grounded framework for information security risk management.

According to Chang et al. (2007), the expert evaluation process employs the coefficient of variation (CV) as a statistical measure to assess the degree of consensus among expert groups regarding the weighting of indicators. The CV serves as an essential criterion for determining the reliability and consistency of

expert judgments. A CV value of ≤ 0.3 signifies a high level of agreement among experts, indicating strong consistency in their evaluations. When the CV is ≤ 0.5, expert opinions are considered to fall within an acceptable range, suggesting a moderate yet sufficient level of consensus for decision-making. However, if the CV is ≥ 0.5, it denotes significant variability in expert opinions, necessitating further analysis and justification to identify potential sources of divergence. In such cases, additional rounds of expert consultation or qualitative explanations may be required to resolve discrepancies and enhance the reliability of the assessment process.

Table 4: Descriptive Analysis of Factors in Information Security Risks

Factors	Attributes	Mean	Coefficient of Variation (CV)	Results
Technical	1. Network Security	5	0	O
	2. Data Protection	4.8	0.086258	O
	3. Application Security	4.866667	0.072301	O
	4. Endpoint Security	4.866667	0.072301	O
	5. Cloud Security	4.933333	0.052338	O
Organizational Management	6. Security Policies and Procedures	4.6	0.137490	O
	7. Risk Management	4.533333	0.163946	O
	8. Security Awareness and Training	4.933333	0.052338	O
	9. Incident Response Plan	4.333333	A0.167019	O
Personnel Factors	10. Employee Behavior	4.8	0.116794	O
	11. Internal Threats	4.733333	0.125412	O
	12. Staff Turnover	3.733333	0.213967	O
Regulatory and Compliance	13. Legal and Regulatory Compliance	4.266667	0.187221	O
	14. Compliance Review	4.4	0.143740	O
External Environment	15. Supply Chain Security	4.533333	0.113911	O
	16. External Threats	5	0	O
	17. Industry Competition	3.6	0.273781	O
ESG Practices	18.Environment Responsibility	2.6	0.350100	X
	19. Social Responsibility	3.066667	0.379213	O
	20. Corporate Governance	3.933333	0.203087	O
	21. Board Participation	4.533333	0.163946	O
	22. Audit Committee	4	0.163663	O

4.3 Importance Ranking of Influencing Factors

The weights were determined using POWERCHOICE V4.1, a decision analysis tool designed to facilitate pairwise comparisons in multi-criteria decision-making. Each pair of factors was systematically compared based on their relative importance using a nine-point scale, which is commonly employed in Analytic Hierarchy Process (AHP) methodologies.

(1) Pairwise Comparison Scale
Each factor was assessed against another, with a score ranging from 1 to 9, where:

- 1 represents equal importance between the two factors.
- 2 to 9 (right side) indicate the increasing importance of factor B over factor A.
- 2 to 9 (left side) indicate the increasing importance of factor A over factor B.

A higher numerical value in either direction signifies a stronger preference for one factor over the other.

(2) Example of a Pairwise Comparison
To illustrate this process, consider the comparison between two factors as follows:
Example: Technical Factors (A) vs. Organizational Management Factors (B)

9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9

- Selecting 1 means both factors are equally important.
- Choosing a value toward 9 on the left indicates that Technical Factors (A) are significantly more important than Organizational Management Factors (B).
- Conversely, choosing a value toward 9 on the right suggests that Organizational Management Factors (B) are significantly more important than Technical Factors (A).

By systematically comparing all factor pairs, POWERCHOICE V4.1 calculates the relative weights, enabling an objective and data-driven prioritization of decision criteria.

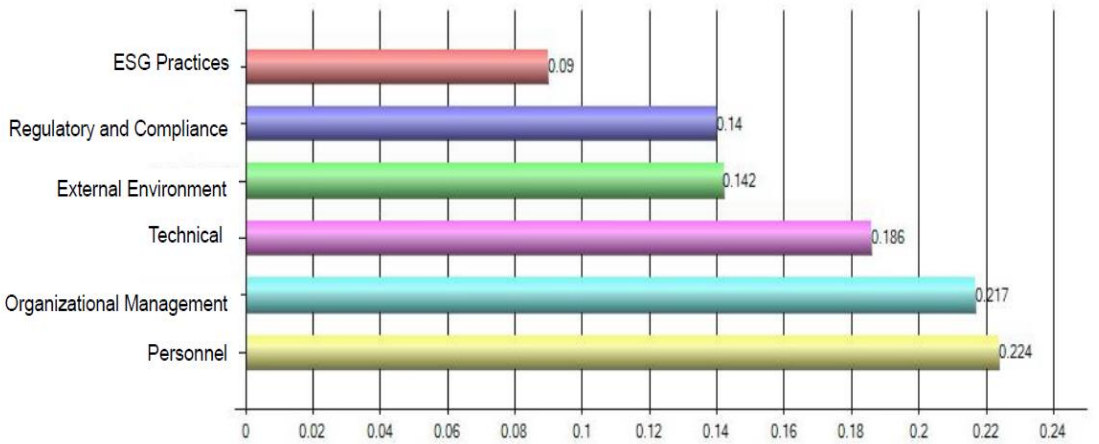

Figure 3: Dimensional Weights of Factors

Experts in the information security industry have identified personnel factors as the most critical dimension influencing information security risks in multinational enterprises (MNEs), as depicted in Figure 3. The results, derived from a pairwise comparison analysis using POWERCHOICE V4.1, indicate that among various risk dimensions, human-related factors hold the highest weight, emphasizing their significant role in shaping cybersecurity vulnerabilities and resilience.

As observed, the highest weight (0.224) assigned to personnel factors underscores their critical influence on information security risks in MNEs. This finding highlights the significant role of employee behavior, cybersecurity awareness, adherence to security protocols, and insider threats in shaping an organization's security posture. It emphasizes the urgent need for comprehensive training programs, stringent access controls, and robust insider threat mitigation strategies to enhance resilience against human-related security vulnerabilities.

Organizational management ranked second-highest in weight (0.217), highlighting its crucial role in mitigating information security risks**.** This underscores the importance of well-defined organizational policies, strong leadership commitment, and effective security governance in fostering a secure environment. A robust organizational framework ensures the implementation of security best practices, adherence to compliance requirements, and the development of efficient crisis response strategies, ultimately enhancing an organization's resilience against security threats.

With a weight of 0.186**,** technical factors—including cybersecurity infrastructure, encryption, firewalls, and security software—are recognized as essential but rank secondary to personnel and organizational management. This indicates a strategic shift from a purely technology-driven security approach to a more holistic model that prioritizes human-centric and management-integrated strategies. While technology remains a critical defense layer, its effectiveness is ultimately dependent on proper implementation, user awareness, and strong organizational oversight.

The moderate weights assigned to the external environment (0.142) and regulatory/compliance (0.14) indicate that while external threats—such as **c**yberattacks, geopolitical risks, and market dynamics—and legal frameworks play a significant role in cybersecurity, they are less impactful than internal factors. This suggests that effective risk management in MNEs relies more heavily on internal controls, personnel behavior, and organizational governance than solely on external regulations or environmental conditions.

ESG practices received the lowest weight (0.09), suggesting that while sustainability, corporate ethics, and governance are important in broader corporate strategies, they have a minimal direct impact on information security risks. This indicates that, although ESG initiatives contribute to overall organizational resilience and reputation, they are not primary factors in cybersecurity risk management compared to personnel, organizational governance, and technical measures.

The findings reinforce the notion that people, rather than technology alone, are the biggest risk factors in cybersecurity. Strengthening security culture, awareness

training, and organizational governance is essential for mitigating human-related vulnerabilities. A balanced approach integrating personnel management, technical security, and regulatory compliance is necessary for effective risk management in MNEs.

Table 5 presents a structured ranking of various cybersecurity and governance attributes based on their relative importance, categorized into six key factors: Technical, Organizational Management, Personnel, Regulatory and Compliance, External Environment, and ESG Practices. The findings indicate that Internal Threats (Rank 1, Global Weight = 0.100770646), categorized under the Personnel factor, is the most critical attribute, underscoring the significance of insider risks in cybersecurity. Similarly, Employee Behavior (Rank 2, 0.093872439) ranks highly, further emphasizing the pivotal role of human factors in organizational security.

Among the regulatory aspects, Compliance Review (Rank 3, 0.079634396), classified under Regulatory and Compliance, emerges as a crucial determinant, highlighting the necessity of rigorous adherence to regulatory frameworks. In the mid-ranked attributes, Security Awareness and Training (Rank 6, 0.058635695) and Risk Management (Rank 7, 0.053730511) are identified as essential components of organizational preparedness. Additionally, Legal and Regulatory Compliance (Rank 5, 0.059980109) remains a fundamental aspect of cybersecurity governance.

Conversely, attributes categorized as lower in importance include Industry Competition (Rank 21, 0.015032675) under the External Environment factor, which is deemed the least critical. Similarly, attributes related to ESG Practices, such as Social Responsibility (Rank 20, 0.016004155) and Corporate Governance (Rank 19, 0.019224828), exhibit relatively lower global weights, indicating their comparatively lesser influence in the cybersecurity and governance landscape.

Overall, the findings underscore the predominance of human-related risks (Personnel), regulatory compliance, and organizational security awareness as the most critical dimensions in cybersecurity management. In contrast, external threats and ESG-related factors are identified as comparatively lower-priority considerations. These insights provide a valuable framework for organizations seeking to optimize their cybersecurity strategies by prioritizing key risk factors effectively.

In conclusion, human-related risks (Personnel), regulatory compliance, and organizational security awareness are the most important factors in cybersecurity and governance, while external threats and ESG factors are comparatively less critical. This insight can help organizations prioritize investments and strategies for risk mitigation.

Table 5: Criteria Weights of Factors Influencing Information Security Risks

Factors	Attributes	Local Weights	Global Weights	Ranking
Technical	1. Network Security	0.244553013	0.045607342	12
	2. Data Protection	0.159586594	0.029761729	14
	3. Application Security	0.249624619	0.04655316	11
	4. Endpoint Security	0.148941385	0.027776475	17
	5. Cloud Security	0.197294389	0.036793956	13
Organizational Management	6. Security Policies and Procedures	0.243990572	0.05290573	8
	7. Risk Management	0.247815047	0.053735011	7
	8. Security Awareness and Training	0.270416014	0.058635695	6
	9. Incident Response Plan	0.237778367	0.051558706	9
Personnel	10. Employee Behavior	0.418498478	0.093872439	2
	11. Internal Threats	0.449251798	0.100770646	1
	12. Staff Turnover	0.132249724	0.029664634	15
Regulatory and Compliance	13. Legal and Regulatory Compliance	0.429612304	0.059980109	5
	14. Compliance Review	0.570387696	0.079634396	3
External Environment	15. Supply Chain Security	0.345976548	0.049258014	10
	16. External Threats	0.548437525	0.078083163	4
	17. Industry Competition	0.105585926	0.015032675	21
ESG Practices	18. Social Responsibility	0.177083893	0.016004155	20
	19. Corporate Governance	0.212714246	0.019224288	19
	20. Board Participation	0.30767693	0.027806647	16
	21. Audit Committee	0.302524931	0.027341029	18

5. Conclusion and Suggestions

The results of this study underscore the critical role of personnel factors and regulatory compliance in effectively managing information security risks within multinational enterprises. Specifically, internal threats, employee behavior, and compliance reviews emerge as the three most influential indicators shaping the overall security risk landscape. Our research survey includes key findings as follows.

1. Technical Factors: A strong technical security foundation, encompassing network security, data protection, application security, endpoint security, and cloud security, is fundamental in preventing external cyber threats. Enterprises should adopt a layered security approach, integrating advanced encryption, multi-factor authentication, intrusion detection systems, and zero-trust architectures to safeguard critical assets.
2. Personnel Factors: Internal threats and employee behavior represent primary sources of information security risks, emphasizing the need for organizations to implement robust internal security controls. Strengthening employee security awareness training, enforcing access control policies, and continuously monitoring insider threats are essential measures for mitigating these risks.
3. Regulatory and Compliance Factors: Ensuring adherence to relevant legal frameworks and conducting periodic compliance audits are crucial for maintaining a secure operational environment. Given the diverse regulatory requirements across different regions, multinational enterprises must establish a comprehensive compliance strategy that aligns with local, national, and international regulations to prevent legal and financial repercussions.

To further enhance enterprises' capabilities in managing information security risks, this study suggests refining and expanding the proposed indicator framework through the following approaches:

1. Dynamic Risk Evaluation: Regularly updating risk assessment indicators to reflect technological advancements and emerging cyber threats will ensure that security measures remain relevant and effective in an evolving digital landscape.
2. Empirical Validation: Conducting field studies and case analyses across diverse industries and organizational structures will help validate the applicability and effectiveness of the proposed framework, enabling its adaptation to specific enterprise needs.
3. Global Collaboration: Strengthening partnerships with international regulatory bodies, industry leaders, and cybersecurity organizations will facilitate the exchange of best practices, fostering a more unified and proactive approach to information security risk management on a global scale.

This study presents a structured and scientifically grounded framework for managing information security risks, offering valuable insights for multinational enterprises seeking to enhance their cybersecurity resilience. By integrating personnel, regulatory, and technical considerations into their security strategies, organizations can establish a more comprehensive and proactive risk management approach. Future research should continue refining this framework to address the increasingly complex and dynamic challenges posed by global cybersecurity threats.

References

[1] Adams, R. B. and Ferreira, D. (2009). Women in the boardroom and their impact on governance and performance. Journal of Financial Economics, 94(2), 291-309.

[2] Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353.

[3] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 523-548.

[4] Chang, C. W., Wu, C. R., Lin, C. T., and Chen, H. C. (2007). An application of AHP and sensitivity analysis for selecting the best slicing machine. Computers & Industrial Engineering, 52(2), 296-307.

[5] Cappelli, D. M., Moore, A. P., and Trzeciak, R. F. (2012). The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.

[6] Chen, J. and Zhao, J. X. (2012). Upconversion nanomaterials: synthesis, mechanism, and applications in sensing. Sensors, 12(3), 2414-2435.

[7] D'Arcy, J. and Hovav, A. (2009). An integrative framework for the study of information security management Research. In Handbook of Research on Information Security and Assurance (pp. 55-67). IGI Global.

[8] Darko, A., Chan, A. P. C., Ameyaw, E. E., Owusu, E. K., Pärn, E., and Edwards, D. J. (2019). Review of application of analytic hierarchy process (AHP) in construction. International Journal of Construction Management, 19(5), 436-452.

[9] DeFond, M. L. and Francis, J. R. (2005). Audit research after Sarbanes-oxley. Auditing: A Journal of Practice & Theory, 24(s-1), 5-30.

[10] Easttom, C. (2019), Computer Security Fundamentals. Pearson IT Certification.

[11] Eccles, R. G., Ioannou, I., and Serafeim, G. (2014). The impact of corporate sustainability on organizational processes and performance. Management Science, 60(11), 2835-2857.

[12] Fahmi, K., Mustofa, A., Rochmad, I., Sulastri, E., Wahyuni, I. S., and Irwansyah, I. (2021). Effect of ISO 9001: 2015, ISO 14001: 2015 and ISO 45001: 2018 on operational performance of automotive industries. Journal of Industrial Engineering & Management Research, 2(1), 13-25.

[13] Fish, L. S. and Busby, D. M. (1996). The Delphi method. Research Methods in Family Therapy, 469, 482.

[14] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

[15] Kurii, Y. and Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013. NIST Special Publication, 800(53), 10.

[16] Larcker, D. and Tayan, B. (2020). Corporate Governance Matters. FT Press.

[17] McGraw, G. (2012). Software security: Building security in. Datenschutz und Datensicherheit-DuD, 36(9), 662-665.
[18] McWilliams, A. and Siegel, D. (2001). Corporate social responsibility: A theory of the firm perspective. Academy of Management Review, 26(1), 117-127.
[19] Pfleeger, C. P., Pfleeger, S. L., and Margulies, M. (2006). Security in Computing. Boston, MA: Prentice Hall.
[20] Porter, M. E. (2008). The five competitive forces that shape strategy. Harvard Business Review, 86(1), 78.
[21] Saaty, T. (1980). The analytic hierarchy process (AHP) for decision making. In Kobe, Japan (Vol. 1, p. 69).
[22] Schneier, B. (2015). Secrets and lies: digital security in a networked world. John Wiley & Sons.
[23] Skulmoski, G. J., Hartman, F. T., and Krahn, J. (2007). The Delphi method for graduate research. Journal of Information Technology Education: Research, 6(1), 1-21.
[24] Whitman, M. E. and Mattord, H. J. (2009). Principles of Information Security. Boston, MA: Thomson Course Technology.
[25] Yu, H., Liao, L., Qu, S., Fang, D., Luo, L., and Xiong, G. (2021). Environmental regulation and corporate tax avoidance: A quasi-natural experiments study based on China's new environmental protection law. Journal of Environmental Management, 296, 113160.