Human Interaction and Emerging Technologies (IHIET-FS 2026), Vol. 235, 2026, 217–226
https://doi.org/10.54941/ahfe1007276

Formulating Cybersecurity Strategies in Corporate Management: Business Strategy and Cybersecurity

Hiroyuki Hasegawa[1], Kenji Watanabe[2], Ichiro Koshijima[2], and Masahiro Arakawa[2]

[1]Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Japan
[2]Manufacturing and Innovation DX Laboratory, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Japan

ABSTRACT

In recent years, the landscape surrounding cyberattacks has been steadily becoming more sophisticated and cunning. Amidst this situation, companies, particularly operating companies, need to advance countermeasures against cyberattacks, yet it is difficult to say that cybersecurity measures are necessarily robust. On the other hand, a survey on the actual state of information security measures among small and medium-sized enterprises (SMEs), published by the Information-technology Promotion Agency (IPA), an external organization of the Ministry of Economy, Trade and Industry (METI) which oversees Japan's information security sector, also reports that implementing countermeasures has reduced the damage from cyberattacks. Under this situation, cybersecurity must be recognized as a "management issue." This paper focuses on the fact that while cybersecurity has become a critical risk issue in corporate management, there are few frameworks to advance countermeasures. It employs the concept of the Balanced Scorecard, a management evaluation method used in corporate management. The Balanced Scorecard holds that financial management alone cannot accurately evaluate business performance; it incorporates non-financial elements to appropriately assess corporate management. Similarly, in cybersecurity, promoting countermeasures based solely on the financial perspective of countermeasure costs is difficult. Therefore, this paper proposes a methodology using the concept of a "Balanced Scorecard." Furthermore, to bridge the gap between management and security personnel in the cybersecurity field, it proposes solutions through two distinct approaches.

Keywords: Cybersecurity, Business strategy, Investment

INTRODUCTION

In recent years, cyberattacks targeting businesses have become increasingly sophisticated and frequent, with ransomware attack damage showing an upward trend almost every year. Amidst these escalating risks, cybersecurity measures have become one of the top priorities for companies seeking to prevent damage to their operations.

In Japan, the "Cybersecurity Management Guidelines" established by the Ministry of Economy, Trade and Industry (METI) in 2015 advocate that business executives themselves should recognize cybersecurity as a

Received February 9, 2026; Revised March 1, 2026; Accepted March 16, 2026; Available online June 22, 2026

critical risk management issue within corporate management (IPA, 2025). These guidelines were revised in 2017 and again in 2023 to align with evolving trends. The Information Security Measures Guidelines for Small and Medium-sized Enterprises (SMEs) were established in 2016 and updated to Version 3.1 in 2025. This version highlights the significant impact cybersecurity has on SME management and outlines approaches for implementing countermeasures (IPA, 2025).

While companies, particularly operating companies, need to advance countermeasures against cyberattacks, it is difficult to say that cybersecurity measures are necessarily robust. Surveys on the actual state of information security measures in SMEs published by the Information-technology Promotion Agency, Japan (IPA) also report results showing that implementing countermeasures reduces the damage from cyberattacks. Furthermore, due to additional regulations and increased security awareness among client companies, demands for security measures are also being made by business partners. Given this context, companies must develop medium- to long-term security strategies rather than focusing solely on short-term costs.

This paper first describes previous research and clarifies the positioning of this research. Next, we introduce the proposed method, which utilizes the gap between a company's management strategy and security strategy. After that, we explain the learning effect of using this proposed method. Finally, we summarize this paper, summarizing the conclusions obtained and future challenges.

Previous Research

In modern corporate management, cybersecurity should be viewed not merely as a technical "countermeasure," but as a "business strategy" directly linked to corporate survival and value enhancement. Previous research indicates that by 2025, Yaniv et al. argue that corporate boards of directors must focus their oversight not on technical details (How), but on strategic significance (What). Boards must appropriately execute the processes of "scanning (information gathering)," "interpretation," and "action (decision-making/execution)" across three phases: normal operations, attack occurrence, and recovery (Yaniv et al., 2025). The board's role is defined as a "dynamic capability" that goes beyond mere monitoring, enhancing organizational resilience and flexibly evolving governance to align with long-term value creation (Yaniv et al., 2025).

Furthermore, according to Taras et al. (2020), for companies in the industrial sector, particularly those in regions with high environmental volatility (such as Eastern Europe), selecting flexible strategies aligned with their current security level is crucial (Taras et al., 2020). Three basic strategic variants—"Survival," "Stabilization," and "Supporting"—are proposed based on a company's situation. It is recommended to prioritize internal and external threats using methods like the Analytic Hierarchy Process (AHP) and implement tactical countermeasures.

In 2024, a systematic review by Chelsea et al., analyzing over 200 empirical studies, systematized the factors and impacts of cyber risk (Chelsea Liu et al., 2024). It identified four key factors influencing risk: management attributes

(e.g., presence of IT expertise), corporate operations (size and financial status), IT practices, and institutional factors like legal regulations. Cyberattacks inflict broad and long-term negative impacts, including on stock prices, corporate reputation, business operations, IT practices, executive turnover, and ripple effects to competitors. Therefore, establishing a "learning mechanism" to learn from past breaches and strengthen governance and defenses is essential (Chelsea Liu et al., 2024).

Previous research has identified "executive involvement" in security strategy, "tactical countermeasures" as part of corporate strategy, and "risk factors." This paper outlines conceptual approaches for developing actual strategies, translates these into Key Performance Indicators (KPIs) aligned with corporate goals, and proposes methodologies for efficient implementation.

Research Objectives

The purpose of this paper is to empirically verify whether a cybersecurity strategy formulation method based on the Balanced Scorecard (BSC) framework can enhance business-security alignment and strategic awareness among practitioners in the industrial and critical infrastructure sectors.

While previous research has clarified "management commitment," "tactical countermeasures," and "risk factors" in security strategy, empirical verification of a specific framework that bridges business strategy and cybersecurity remains limited. This paper fills this gap by verifying the effectiveness of a BSC-based cybersecurity strategy formulation approach through a structured exercise.

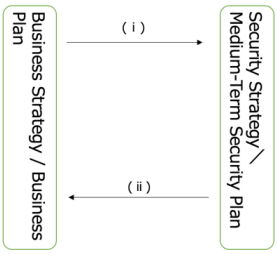
Proposed Method

Regarding the relationship between a company's "business strategy" and "security strategy," there are two approaches for effectively formulating a security strategy (see Figure1).

<Means to Bridge the Gap Between Business Strategy and Security Strategy>

i. Align security strategy with business strategy/business plans (Business-aligned security strategies)
ii. Control business strategy/business plans from the security strategy side (Security-Driven Business Controls)

The first approach focuses primarily on business strategy/business plans, formulating security strategy to align with those policies. In this case, since the business side takes precedence, the security strategy is viewed from the perspective of how it supports the business. While previous papers considered methods to balance these two aspects (Hasegawa, 2025), achieving this balance can be encompassed within approach i, so this paper omits detailing that method. The second approach centers on the security strategy to control the management strategy/business plan. This applies to sectors with stringent regulations requiring mandatory security measures, such as the defense industry or critical infrastructure.



	Approach target	Example
i	Businesses that advance security whilst prioritising business	General organization
ii	Businesses that advance business from a security perspective, operating under stringent regulations related to economic security and similar matters	Critical Infrastructure

Figure 1: Proposed method.

RESEARCH HYPOTHESES

Based on previous research and the conceptual framework proposed in this study, the following hypotheses are formulated.

H1 (Strategic Understanding Hypothesis):

Participants who formulated a cybersecurity strategy using the Balanced Scorecard framework will demonstrate a statistically significant improvement in their understanding of the relationship between business strategy and cybersecurity compared to their pre-exercise baseline.

H2 (Strategic Flexibility Hypothesis):

Presenting two distinct strategic approaches—(i) a business-aligned security strategy and (ii) security-driven business control—will significantly improve participants' understanding of cybersecurity as a dynamic and context-dependent management strategy.

H3 (Industry Experience Moderation Hypothesis):

Participants with specialized experience in critical infrastructure sectors (e.g., energy, transportation, manufacturing) will evaluate the proposed methodology as more applicable and important than participants without such experience.

i) Align security strategy with business strategy/business plans

This paper utilizes the model company "ABC Chemical" introduced by Hiroshi Sasaki et al. (Sasaki, 2021). The IT/OT environment at ABC Chemical during the early stages of its DX initiative reflects common challenges faced by many chemical manufacturers.

Availability-focused OT environment: 24/7 operation takes absolute priority, making security measures requiring patching or system shutdowns difficult to implement. Direct IT-OT connections: To enhance production efficiency, information systems (IT) and control systems (OT) are connected without firewalls in some areas. Internet connectivity in OT environments: For purposes like predictive maintenance, parts of the OT network—which should be closed—are partially connected to the internet. Inadequate Management of Maintenance Vendors: Access management during remote maintenance

by external vendors is insufficient. Increase in Accidents Due to Operational Errors: As systems become more complex, minor production issues caused by operational mistakes are increasing. To systematically evaluate these challenges and determine countermeasure priorities, leveraging frameworks like the NIST Cybersecurity Framework (CSF) or factory security guidelines is highly effective.

Under these circumstances, the security strategy formulated should fundamentally adopt a "business-first, security-follows" approach that does not hinder the management goal of promoting DX. The strategy's primary focus lies in how to address risks newly introduced by DX strategies, such as cloud migration and remote maintenance, while safely supporting business growth. Decomposing the strategy using the Balanced Scorecard yields the following proposed policy framework (see Figure2).

In this case, the security strategy must be integrated by understanding and aligning with the management strategy and business plan. Therefore, the key challenge lies in effectively translating the content of the management strategy and business plan into security terms.

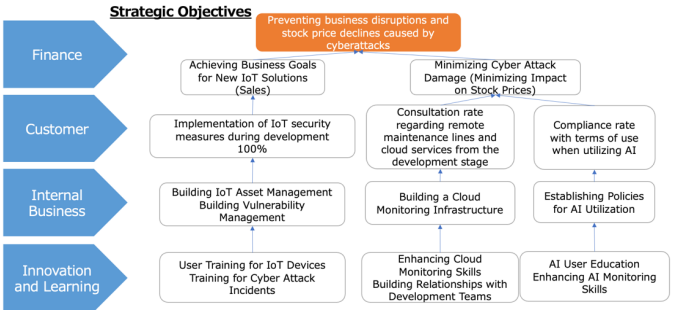


Figure 2: Balanced scorecard (Pattern 1).

ii) Control business strategy/business plans from the security strategy side Next, assume a dramatic change in ABC Company's business environment occurs: as part of its business diversification, it expands its self-generation facilities and enters the energy business (power generation).

This entry designates the company as a "critical infrastructure operator" under the Economic Security Promotion Act, subjecting it to stringent legal regulations imposed on the power industry. Introducing critical equipment or outsourcing its maintenance requires prior government review, and cybersecurity measures become essential requirements for business continuity.

This change fundamentally alters the approach to security strategy. This forces a strategic shift from the previous "business-first, security-follows" approach to a "security-driven" model where regulatory compliance becomes a prerequisite for business. This change in the business environment directly impacts the strategic planning approach. New regulatory requirements redefine the security objectives that must be met. Security is no longer a 'cost' but becomes the "foundation" for maintaining the business license, elevating it to a critical element that controls the business strategy itself.

This scenario shift indicates that cybersecurity strategy is not static—something set once and forgotten—but must be dynamically reviewed in response to changes in the business environment, such as M&A or new business ventures.

Security strategies developed under these circumstances will primarily focus on meeting regulatory requirements. Policies that follow the business will then be incorporated. Decomposing the strategy using the Balanced Scorecard yields the following policy proposals(see Figure3).

In this case, to meet legal requirements, the initial focus will be on establishing incident response procedures and security requirements for procurement. Following this, fundamental countermeasures will be verified. The top priority here is understanding the legal requirements, translating them into detailed company-specific countermeasures, and implementing any missing components. Therefore, clearly identifying these gaps is crucial.

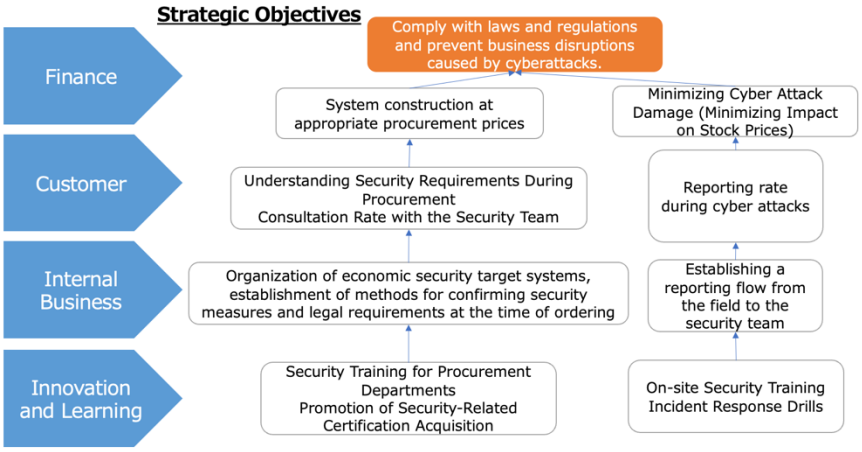


Figure 3: Balanced scorecard (Pattern 2).

EVALUATION

Participants

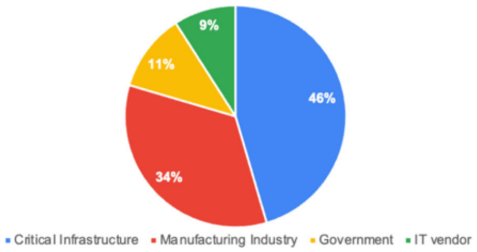
The empirical evaluation was conducted on participants enrolled in the Industrial Cybersecurity Human Resources Development Program (ICSCoE)*12, operated by the Information-Technology Promotion Agency (IPA). Participation in the program requires IT Passport certification or at least one year of experience in an IT- or OT-related role.

Furthermore, trainees consist of personnel seconded from critical infrastructure companies (e.g., power, railways) and manufacturers. Consequently, exercise results are expected to be highly reliable and directly applicable to real-world operations. Furthermore, the first two months of the ICSCoE program consist of foundational IT/OT lectures to supplement knowledge. Therefore, by the time this exercise was conducted, participants possessed at least Level 1 to 2 equivalent skills according to the IT Skills Standard (IT skill standard, 2025), ensuring a minimum baseline of knowledge among attendees.

The number of participants on the exercise day, the number of survey respondents, and the industry classifications are as follows (see Table1).

Table1: Responders information.

Date	Participants	Number of Respondents
1, October, 2025	17	8
4, November, 2025	19	15
4, December, 2025	19	14



Experimental Procedure

The evaluation was based on a within-subjects, pre-post design and consisted of the following three phases.

Pre-exercise Survey

Participants self-evaluated the following:

- Understanding of the relationship between business strategy and cybersecurity
- Recognition of the importance of cybersecurity in corporate management
- Recognition of strategic diversity in cybersecurity approaches

Strategy Formulation Exercise

Participants conducted a cybersecurity strategy formulation exercise using the following items:

Model Company Scenario

Two Strategy Patterns

Business-Aligned Security Strategy

Security-Driven Business Control Strategy

Balanced Scorecard Perspective (Finance, Customers, Internal Processes, and Human Resources)

Post-exercise Survey

The same survey items were administered again, with additional questions regarding the applicability and importance of the methodology.
All survey items were rated using a 5-point Likert scale.

Measured Variables

Variable Description

Strategic Understanding: Level of understanding of the relationship between business strategy and cybersecurity
Strategic Flexibility: Recognition that cybersecurity strategies are dynamic and context-dependent
Perceived Applicability: Practicality of the Methodology
Perceived Importance: Importance of the Methodology in Corporate Management

Data Analysis

To test the hypotheses, the following analyses were conducted:

H1: Pairwise comparison of pre- and post-exercise scores
H2: Descriptive and comparative analysis of post-exercise responses regarding strategic diversity
H3: Group comparison between participants with and without critical infrastructure experience

Due to the exploratory nature of this study and limited sample size, we focused on verifying trends rather than strict causal inference.

Hypothesis H1: Strategic Understanding

Post-exercise results showed consistent improvements in participants' self-assessed understanding of the alignment between cybersecurity strategy and business strategy. This supports hypothesis H1 and indicates that a BSC-based methodology improves strategic understanding (see Table2).

Table 2: Evaluation.

#	Item	Changes in Awareness Before and After the Exercise
1	The Importance of a Strategic Approach	20/29 (68.97%)
Number of respondents		29

Hypothesis H2: Strategic Flexibility

The majority of participants reported an increased awareness that cybersecurity strategy should change depending on the business stage, regulatory environment, and organizational context. This result supports hypothesis H2, demonstrating that exposure to the dual strategy pattern increases perceptions of strategic flexibility (see Table3).

Table 3: Evaluation.

#	Item	Average Rating (5-point scale)
1	Feasibility of Approach 1 for Developing Security Strategies	3.64
2	Feasibility of Approach 2 for Developing Security Strategies	3.57
Number of respondents		44

Hypothesis H3: The Impact of Industry Experience

Participants in the critical infrastructure sector rated the applicability and importance of the proposed methodology higher than participants in other sectors, supporting hypothesis H3. This suggests that regulatory stringency and operational importance increase the perceived value of a structured cybersecurity strategy framework (see Table 4).

Table 4: Evaluation.

#	Item	Number of Respondents	Exercise Evaluation	Feasibility of Approach 1 for Developing Security Strategies	Feasibility of Approach 2 for Developing Security Strategies
1	Critical Infrastructure Sector Participants	19	4.21	3.79	3.74
2	Other than the above	25	4.12	3.52	3.44

CONCLUSION

Discussion

The results demonstrate that a balanced scorecard-based cybersecurity strategy formulation approach is effective in improving practitioners' strategic understanding and awareness. Importantly, these findings support the idea that cybersecurity strategies are not static but must evolve in response to business growth, regulatory constraints, and environmental changes.

The moderation effect observed in the critical infrastructure sector highlights the importance of contextual factors in cybersecurity governance research.

Limitations and Future Research

This study has several limitations. First, evaluation is primarily based on self-reported measures rather than objective performance indicators. Second, the lack of a control group limits causal inference. Third, long-term behavioral and organizational impacts were not assessed.

Future research should incorporate controlled experimental designs, objective outcome measures, and longitudinal analyses to further validate the proposed hypotheses.

CONCLUSION

This study reformulates cybersecurity strategy formulation as a hypothesis-driven management practice and empirically demonstrates the effectiveness of a balanced scorecard-based approach. By validating strategic understanding, flexibility, and contextual relevance, the findings of this study contribute to both cybersecurity governance research and the practical formulation of strategies in industrial environments.

ACKNOWLEDGMENT

The authors would like to acknowledge the IPA Industrial Cyber Security Center Trainees who participated in this exercise, as well as Prof. Koshijima and Prof. Hashimoto for their support in conducting the exercise. This work has been partially supported by Information-Technology Promotion Agency, Japan, however all remaining errors belong to the authors.

REFERENCES

Chelsea Liu, Muhammad Ali Babar (2024), Corporate cybersecurity risk and data breaches: A systematic review of empirical research, Australian Journal of Management,1–31,he Author(s) 2024.

Hiroshi Sasaki (2021), Cybersecurity in Manufacturing, Japan Society for the Promotion of Science Press.

Hiroshi Umeda (2023). Organising and examining the purposes of BSC implementation by listed companies in Japan: An analysis based on published data. Journal of the Japan Intellectual Asset Management Society, 2023, Vol. 9, pp. 65–77.

Hiroyuki Hasegawa, Kenji Watanabe, Ichiro Koshijima, and Masahiro Arakawa (2025), A Framework for Aligning Cybersecurity and Business Strategy - From Cost to Investment, Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2271–2279.

Human Resource Development Program Program Overview, https://www.ipa.go.jp/en/it-talents/ics/humandev.html, (October, 2023).

Information-technology Promotion Agency (2025), Cyber Security Management Guidelines.

Information-technology Promotion Agency (2025), Information Security Measures Guidelines for Small and Medium-sized Enterprises.

IT skill standard, https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr7000 0004x60-att/000024840.pdf, (January, 2025).

Michiharu Sakurai (2008) Balanced Scorecard: Theory and Case Studies, Revised Edition, Dobunkan. *9 Shinnosuke Matsuyama (2003), How to Run a Company Strategically: A Book That Clearly Explains How to Use Balanced Scorecards.

Takahashi, Yoshio (2003). "How Did the Balanced Scorecard (BSC) Come About?" Shōgaku Shūshi, Vol. 90, No. 1 (July 2003), pp. 55–88.

Taras SHYRA, Oleksandr SHTYROV, Ivan KORCHYNSKYY, Anastasiia ZERKAL, Halyna SKORYK (August 2020), Providing the Corporate Security Strategy in the Management System of the Enterprise,Verslas: Teorija ir praktika / Business: Theory and Practice,ISSN 1648-0627 / eISSN 1822–4202, A2020 Volume 21 Issue 2: 737–745.

Yaniv Harel and Abraham Carmeli (2025) A strategic cybersecurity oversight framework: a board's imperative, Journal of Cybersecurity, Volume 11, Issue 1, 2025, tyaf021.