Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2271–2279
https://doi.org/10.54941/ahfe1007039

A Framework for Aligning Cybersecurity and Business Strategy - From Cost to Investment

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

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

ABSTRACT

In recent years, the situation surrounding cyberattacks has continued to grow increasingly sophisticated and cunning. Amidst this situation, companies, particularly operating businesses, need to advance their countermeasures against cyberattacks. However, it is difficult to say that cybersecurity measures are necessarily well-established. 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. Furthermore, due to additional regulations and heightened security awareness among client companies, security measures are increasingly being demanded by business partners. In this environment, companies must develop medium- to long-term security strategies, rather than focusing solely on short-term costs. In this paper, we analyze why companies struggle to advance security measures, examining the causes of the gap between business strategy and security strategy, and proposes solutions. The gap analysis references the Balanced Scorecard (BSC) and is conducted across four perspectives: financial, customer, internal processes, and people. It analyzes the causes within each category and suggests countermeasures. Furthermore, in this paper, we implement one countermeasure: creating a "Security Scorecard" that maps cybersecurity measures based on the BSC.

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 Ministry of Economy, Trade and Industry (METI) established the "Cybersecurity Management Guidelines" in 2015, advocating that business leaders themselves recognize cybersecurity as a critical risk

management issue within corporate governance (IPA, 2025). These guidelines were subsequently revised in 2017 and 2023 to align with evolving trends. The Information Security Measures Guidelines for SMEs were also established in 2016 and revised to version 3.1 in 2025. These guidelines highlight the significant impact cybersecurity has on SME management and outline approaches for advancing countermeasures (IPA, 2025).

While companies, particularly operating businesses, 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 IPA also report that implementing countermeasures reduces the damage from cyberattacks. Furthermore, due to additional regulations and increased security awareness among client companies, security measures are increasingly being requested by business partners. In this environment, companies must develop medium- to long-term security strategies rather than focusing solely on short-term costs.

In chapter 2, we analyze the gap between corporate management strategy and security strategy. The analysis describes a methodology focusing on existing frameworks for management strategy. Based on the gap analysis results, an approach method is proposed. In chapter 3, we explains a concrete example of one such approach method. Finally, in chapter 4, we summarizes this paper, presenting the conclusions reached and future challenges.

Background (Application of the Balanced Scorecard)

According to the METI, it is recommended that cybersecurity measures be incorporated as part of an organization's management risk and that 'cyber security be positioned as an investment in management,' with greater involvement and responsibility on the part of management. In addition, organizations are required to appoint a Chief Information Security Officer (CISO), and security measures are being promoted by senior executives such as the CISO.

On the other hand, it is challenging to advance cybersecurity measures in companies based solely on financial perspectives such as 'investment' and 'cost.' When viewed as an 'investment,' many cases fall under 'capital expenditures,' and reducing organizational risks (e.g., lowering incident occurrence rates) alone is insufficient to promote the advancement of measures.

A survey of 55 individuals, primarily from Japan's critical infrastructure, manufacturing, and government sectors, yielded 24 responses, with 78.1% indicating that cybersecurity is included in their company's business strategy. This suggests that large Japanese companies, in particular, tend to view cybersecurity as an organizational risk issue (see Figure 1).

According to a report published by the IPA in fiscal year 2024, 59.7% of SMEs surveyed (4,191 responses) have not invested in security measures. This indicates that it is taking longer for cybersecurity measures to become a management priority among SMEs than among large enterprises.

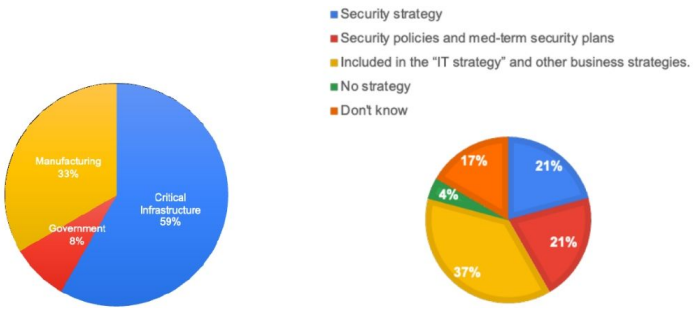


Figure 1: Respondent affiliation trends and survey on the existence of strategies.

Furthermore, the reasons cited for not investing were "do not feel it is necessary," "cannot see the cost-effectiveness," and "costs are too high," accounting for 90.2% of responses. Among those citing "no perceived need," reasons included: not holding critical information (36.5%), no network connections with other companies (31.6%), minimal impact on business continuity (25.9%), and belief they would not suffer cyberattacks (24.0%) (IPA, 2025).

The METI is also considering an evaluation system for SMEs from a supply chain security perspective. It is possible that requests and verifications for security measures may come from large enterprises, which are upstream in the supply chain, in the future.

Furthermore, even when patches for vulnerabilities are released, there tends to be a long delay before they are applied. Some survey results indicate that 39.2% of companies do not even set a timeframe for this process. Many companies allocate less than 5% of their overall IT budget to security, and a significant 64.5% feel their security budget is insufficient (KPMG Japan, 2025).

Under these circumstances, it is difficult to say that security measures are prioritized, indicating that security efforts are lagging in existing business operations.

Within companies, roles can be divided into three layers: management, operational staff, and security personnel responsible for overseeing security. Security measures are likely to progress when these three layers collaborate organically. This paper analyzes the gap between the "executive layer" and the "security personnel layer" and devises an approach to bridge it. For this analysis, it employs the concept of the "Balanced Scorecard" used in management studies, rather than frameworks commonly used in the security field (see Figure 2).

The balanced scorecard is a management support system designed to disseminate corporate management strategies throughout the entire organization.

The background to this is that, until now, performance evaluation has been based on financial criteria and constructed by financial experts, but there has been a sense of unease and crisis regarding the lack of involvement of top management and the tendency for management decisions to be biased towards financial results. This does not mean that financial-centric

measurement methods are inherently flawed, but rather that they fail to accurately reflect the true state of the organization (Umeda, 2023).

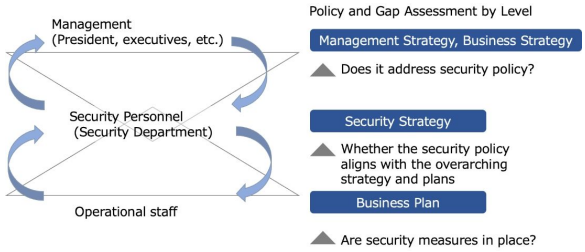


Figure 2: Security gap between upper and lower levels.

It is not that financial measurement is being downplayed, but rather that the BSC, as a framework for strategic management practice, is characterized by top management participating in the creation of the BSC by demonstrating the organization's priorities centered on its vision, thereby guiding employees to think for themselves and work towards achieving the vision, rather than being (Takahashi, 2020) (Sakurai, 2008).

In BSC, it is important to classify four perspectives: financial, customer, internal processes, and human resources. BSC categorizes these four areas to create a 'strategic map' and 'BSC basic table,' thereby integrating management control.

BSC is not limited to business strategy but is also used in a wide range of fields, such as human resources and IT (Matsuyama, 2003).

In the field of cybersecurity, the BSC is used to map cybersecurity measures based on the four perspectives. Cybersecurity measures managed solely based on costs tend to be simplified. Therefore, this field requires a new management approach beyond cost-based management. Since the BSC includes categories such as customers, internal processes, and human resources in addition to financial management, it is considered compatible with cybersecurity concepts.

Analyze the gap between "business strategies" and "business plans" formulated by the "executive management layer" and the "security strategy/medium-term security plan" developed by the "security personnel layer" using the four perspectives of the Balanced Scorecard (BSC) (see Figure 3).

Regarding the "financial" perspective, security measures are often viewed as 'costs' within the "business strategy," or the business side, leading to lower investment priority. This is also one cause of the aforementioned "budget shortfall" for security measures. From the "Customer" perspective, while customers desire a certain level of security measures, they also want to minimize their cost burden. Past surveys on customer awareness regarding purchasing IoT devices at personal expense indicate growing awareness, yet customers still seek realistic costs, necessitating consideration of the balance between price and security measures (MS&AD InterRisk Research Institute & Consulting, Inc., 2021).

Regarding the "internal processes" perspective, the business side prioritizes "improving efficiency" when planning measures. This is essential

for advancing business operations. Since cybersecurity falls under risk management, the key lies in whether it can be considered a necessary countermeasure against business risks. From the "human resources" perspective, the primary issue is the shortage of personnel engaged in security operations. ISC^2 research indicates Japan faces a shortage of approximately 110,000 personnel (ISC2, 2023). Additionally, there is the problem of insufficient security awareness among personnel performing business-side operations. While the analysis employs four perspectives, human factor issues represent the most fundamental aspect. How to cultivate personnel involved in security operations and those performing business-side tasks, and how to change their mindset, also become critical solutions.

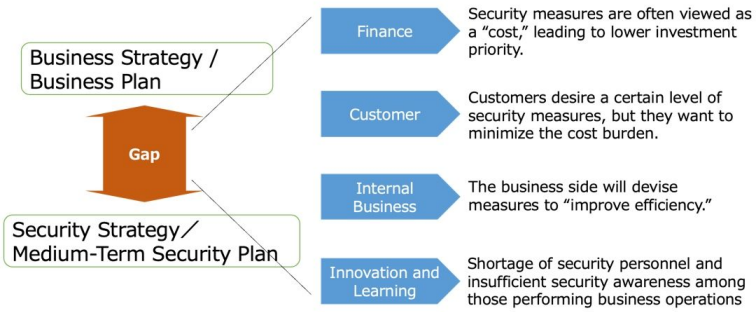


Figure 3: The gap between business and cybersecurity.

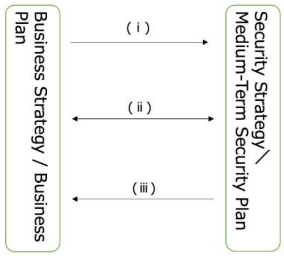
Proposed Method

To bridge the gap described in the previous chapter, it is necessary to establish the correct policies within a company's "business strategy" and "security strategy." There are three approaches. They are outlined below.

Means to Bridge the Gap Between Business Strategy and Security Strategy

i. Align security strategy with business strategy/business plans.
ii. Develop both strategies with equal emphasis to close the gap.
iii. Control business strategy/business plans from the security strategy side.

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. The second approach involves creating a coordinated strategy that balances both sides to bridge any gaps. Most companies are likely suited to either approach i or ii. Traditionally, only approach i was considered, but recently, due to security risks within the supply chain, the need for approach ii has emerged. The third approach involves prioritizing the security strategy to control the business strategy/business plan. This applies to sectors with strong regulations where security measures must be incorporated, such as the critical infrastructure (see Figure 4).



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

Figure 4: Proposed method.

In this paper, we illustrate how security management should be conducted in the case of scenario i, considered a conventional model, using a security scorecard applying the Balanced Scorecard (BSC).

The security scorecard consolidates cybersecurity measures into four perspectives as a means for companies to achieve strategic goals by integrating them into management control. Suppose the organization's strategic goal is to enhance its brand image. From a financial perspective, advancing cybersecurity measures likely involves aiming for appropriate security costs. Beyond achieving this, the customer perspective considers maintaining usability and the trustworthiness gained through security measures. Furthermore, to achieve internal process goals, Security by Design is introduced. Security by Design involves incorporating security measure evaluation processes from the development stage. From a human resources perspective, achieving these goals involves enhancing teamwork and deepening collaboration between system development teams and security teams. Using a security scorecard enables companies to consider security measures beyond just cost.

We collected security scorecard questionnaires from 55 respondents in the previously mentioned critical infrastructure, manufacturing, and government sectors. Referencing these elements, we illustrate a strategic map using the security scorecard (see Figure 5).

Figure 5: Example of security scorecard.

Strategic maps are also an important performance evaluation phase in balanced scorecards. From a financial perspective, security scorecards include "rapid response to attacks." This means preventing the loss of business opportunities due to severe or prolonged damage caused by attacks, which can indirectly reduce the impact on a company's stock price. Another goal that can be set is the optimization of security costs. Important success factors include the ability to detect attacks early at the Security Operations Center (SOC) and the ability to share attack information with the team responsible for security response (CSIRT). KPIs are set for each communication time, and the action plan focuses on "whether detection is possible" and "whether communication is possible after detection."

Next, from the "customer" perspective, system users can be either employees or customers. The goal is to ensure that security measures do not compromise usability and that incidents such as opening virus emails can be reported. The key success factor is usability = complexity of business processes, and it is important to ensure that security measures do not lead to increased communication speeds or business processes. One measure is to increase the reporting rate through training on opening virus emails.

From the perspective of "business processes," the proposal includes security by design initiatives, such as whether security measures can be reflected in the design by the system development team from the outset. It is also necessary to have a flow in place for the development team to detect attacks and report them to the security team. KPIs include 100% involvement in security by design and conducting joint training with the development team. Action plans include establishing rules for security by design.

Finally, from the "human resources" perspective, it is necessary to build relationships between the development team and the security team and establish security governance. It is also important to educate development team members on security. In Japan, such personnel are referred to as "plus security personnel," meaning they acquire security knowledge in addition to their regular duties. The key success factor for this item is whether the development team can independently consider and implement security measures. Therefore, KPIs should be set for security education for the development team, and action plans should include creating security education content and conducting regular education (see Figure 6).

A questionnaire was distributed to 31 individuals associated with SMEs regarding the usefulness of security scorecards. The session received ratings from 11 participants, achieving an average score of 4.5 out of 5 points, and garnered high praise for its effectiveness and potential for practical application (see Table 1).

Table 1: The evaluation of security scorecard.

Date	Participants	Evaluation Point Avg.	Availability
August 26, 2025	31	4.5	3.9

	Strategy Goals	Critical Success Factors	KPI	Action Plan
Finance	• Quick response when an attack happens (minimising impact on stock price) • Optimising security costs	• Early detection with SOC • Early launch of incident response team	• Reporting time from SOC to CSIRT within 60 minutes • Time from receiving a report to CSIRT launch within 30 minutes	• Organizing detection information from security products • Organizing information to be communicated to CSIRT based on detection information from SOC • Establishing a CSIRT launch process
Customer	• Maintaining usability • Improving security reliability • Reporting rate in the event of a cyber attack	• Implement measures without increasing work flow • Prompt reporting from employees	• 100% report rate after opening email training	• Email Training Implementation
Internal Business	• Incorporate security from the initial stages of designing and developing development systems and software. • Establish a reporting system for when attacks occur (or when there is a possibility of an attack).	• Involvement of the security team during development • Establishing rules for when an attack occurs	• 100% involvement of the security team • Incident training once a year based on cyber attacks	• Establish security-by-design rules. • Inform the development team. • Plan and implement training that simulates cyber attacks.
Innovation and Learning	• Building relationships with development teams • Raising awareness of security governance • Promoting basic security education (plus security personnel)	• Consideration of autonomous security measures by the development team	• Annual security training for development teams	• Creating security training content for development teams • Implementing security training for development teams

Figure 6: Example of a strategic map for a security scorecard.

CONCLUSION

In this paper, we analyzed the gap between executive management and security personnel in the cybersecurity field using the Balanced Scorecard (BSC) methodology and proposed an approach to resolve it. It also focused on the scarcity of frameworks for advancing countermeasures despite cybersecurity becoming a critical risk issue in corporate management, employing the Balanced Scorecard concept—a management evaluation method for corporate governance. The Balanced Scorecard recognizes that financial management alone cannot accurately evaluate business performance, advocating the inclusion of non-financial elements to provide a more appropriate assessment of corporate management. Similarly, in cybersecurity, focusing solely on the financial perspective of countermeasure costs makes it difficult to drive countermeasure implementation. Therefore, a methodology employing the concept of a "Security Scorecard" was devised.

Moving forward, we aim to devise concrete solutions for the three approaches to addressing gaps and establish mechanisms to enhance security measures. Furthermore, we intend to present more detailed methods for countermeasures from the perspective of "human resources".

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

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.

Information-technology Promotion Agency (2025), 2024 Survey on Information Security Measures in Small and Medium-sized Enterprises - Report.
Information-technology Promotion Agency (2025), Cyber Security Management Guidelines.
Information-technology Promotion Agency (2025), Information Security Measures Guidelines for Small and Medium-sized Enterprises.
ISC2(2023), ISC2 Cybersecurity Workforce Study 2023.
KPMG Japan, Cybersecurity Survey 2025, April 2025.
Michiharu Sakurai (2008) Balanced Scorecard: Theory and Case Studies, Revised Edition, Dobunkan.
MS&AD InterRisk Research Institute & Consulting, Inc., Survey Report on Awareness of Cybersecurity Measures for Consumer IoT Devices (2021).
Shinnosuke Matsuyama (2003), How to Run a Company Strategically: A Book That Clearly Explains How to Use Balanced Scorecards.
Toshiro Takahashi (2020), Shogaku Shuishi, Vol. 90, No. 1.