JCIC
Japan Cybersecurity Innovation Committee

May 2022

Set Internal Security Resources at 0.5% or More
Cyber-risk estimation model to realize DX with Security

[Summary]

- About 90% of listed companies in Japan are challenging for digital transformation (DX). If the long-term benefits of DX are to be achieved, cybersecurity must be promoted at the same time. **Failure to take security measures may not only risk a system shutdown and information leakage, but could also result in significant financial loss**.
- JCIC investigated the stock prices of companies that made timely disclosures of unauthorized access, etc., and **found that their stock prices fell by an average of 6.3% after 50 days**. Inadequate security measures may also result in having to pay compensation for damages and breaches of the duty of care of a prudent manager. It can be said that "DX with Security," a cybersecurity strategy to promote DX, is no longer an issue only for IT and security departments. It has become a **management issue that should be tackled by the entire company, involving directors, managers, and other officers**.
- A DX with Security strategy is essential to promote DX, to increase companies' productivity and efficiency, and to avoid financial loss. In order to develop and implement your DX with Security strategy, JCIC recommends you follow the approach below.

Recommended approach to strategy development for DX with Security leading companies

- Visualize risks using a cyber-risk estimation model
- Develop a DX with Security strategy
  - Use a framework to explain the strategy as a story
  - Security investment should be **0.5% or more** of consolidated sales revenue
  - Security personnel should be **0.5% or more** of the total number of employees
- Set security key performance indicators (KPIs) and monitor them regularly

- Departments promoting DX tend to repeat trial and error methods daily for business transformation, in an attempt to achieve results quickly. The security department should not exert strong control at this stage, as it will hinder DX. Instead, IT security managers should assist DX merely by developing a secure proof of concept (PoC) environment and formulating guidelines. **IT security managers should become actively involved when commercial services are being considered in concrete terms**.

1. Introduction

JCIC has been conducting research on management and cybersecurity as a cybersecurity think tank. This report is a fully revised version of JCIC's "A cyber-risk estimation model to discuss in board of directors meetings" published by JCIC in 2018. In response to the wide spread of digitization and remote working and the dramatic increase in the number of companies working on DX, due to the COVID-19 pandemic, we have reconsidered the position of security in DX and have now reorganized our approach to promoting DX with Security.

In this report, DX is used **to develop revolutionary new businesses and fundamentally transform business processes through the use of digital technology**. It does not mean simply digitizing analog operations that were previously performed manually or on paper. There are various risks associated with new business and business process transformation, including financial and legal risks. Among them, **cyber risks are a common issue to be considered in all DXs. They are an imminent challenge because of the significant effects on business when risks materialize and threats are evolving daily**.

The target readers for this report are mainly IT security managers (chief information security officers (CISOs), department heads, etc.). But it is also recommended reading for management personnel, including directors, auditors, and executives, and managers in corporate planning, general affairs, risk management, human resources, finance, information systems & DX promotion, PR, IR, sustainability, purchasing & procurement, and other departments.

The primary target companies of this report are "DX with Security leading companies" that invest human resources and budgets in DX as much as IT companies do, to transform their business models and processes. Such companies can be described as those that seek to achieve high levels of convenience and security management across the entire company (convenience-oriented and monitoring type[1]). It is also informative for "DX with Security follower companies" that are trying to adapt DX partially, while maintaining their existing businesses and operations.

We hope you will make good use of the advice in this report for promoting DX with Security.

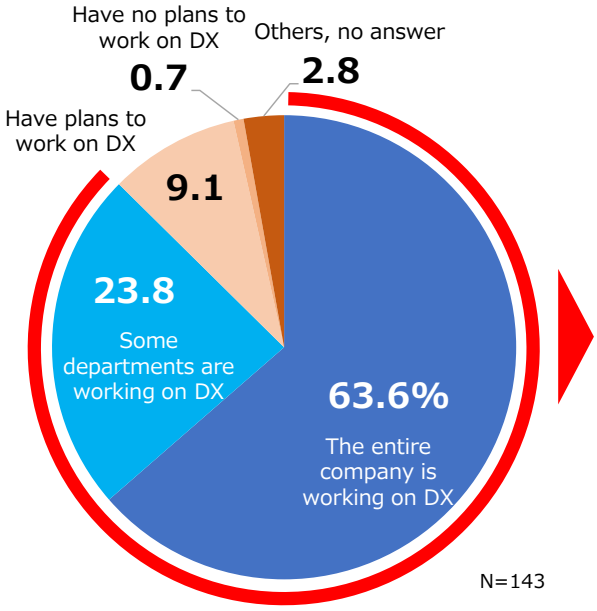
[1] JCIC's "Rebalancing convenience and security to contend with 2025" stated that companies can be classified into four types: (1) Usability and Monitoring, (2) Discretion and Self-responsibility, (3) Ad-hocism or Flexibility, and (4) Security Fundamentalism. https://www.j-cic.com/pdf/report/Rebalancing.pdf.

2. The importance of DX with Security

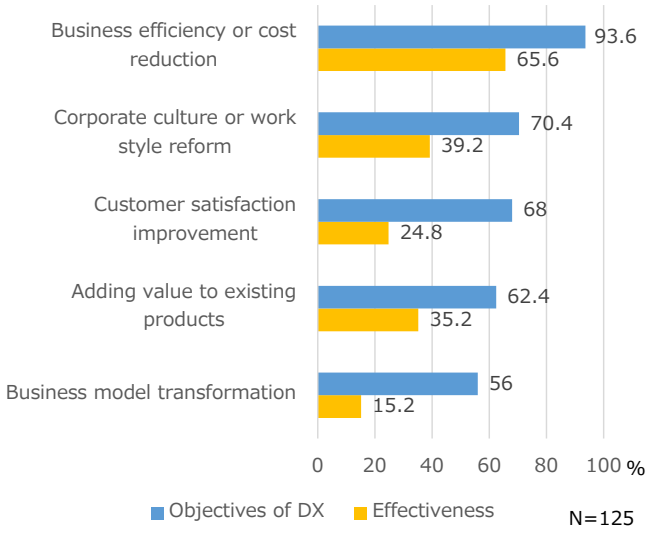
According to a survey by the Innovation Council of the Japan Productivity Center,[2] approximately 90% of executives at listed companies replied that they are working on DX. Of that 90%, 64% are engaged in company-wide efforts and 24% in departmental efforts.

The top objective of DX is "business efficiency and cost reduction," with two-thirds of the respondent companies stating that it is already showing results. The second and subsequent objectives were "corporate culture and work style reform" and "customer satisfaction improvement" and "adding value to existing products."

During the COVID-19 pandemic, it was socially proven that remote working is sufficient to keep a business running, and is even more efficient in many cases. In addition, the change from a real society to a digital society promoted a shift in values from "tangible goods consumption" to "intangible goods consumption." As the world undergoes significant changes in the post-COVID-19 era, it is inevitable that companies will engage in DX to maintain and improve their corporate value.



[Question] Does your company implement DX? (Single choice)



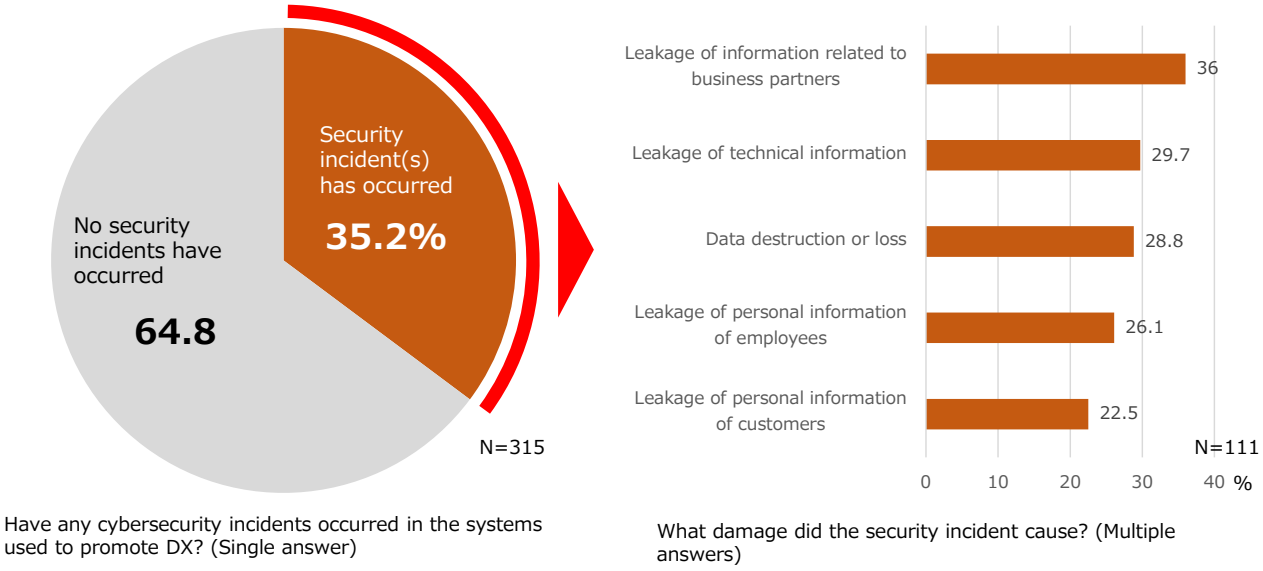
[Question] What are the objectives of DX in your company? Is it effective in meeting those objectives? (Multiple choices)

Figure 1: Implementation status and objectives of DX

[2] Japan Productivity Center, "Urgent Questionnaire on Expectations for the New Government and DX" (December 2021), https://www.jpc-net.jp/research/detail/005615.html

While most of the listed companies are thus working on DX, cybersecurity must be promoted at the same time, in order to achieve long-term benefits of DX. Failure to take security measures will not only risk system shutdowns and information leakage, but could also result in tens of billions of yen in financial losses.

According to a survey by Trend Micro,[3] about 35% of DX professionals have experienced a security incident. Such incidents are often related to information leaks. This indicates that, in promoting DX, data protection is not sufficiently thorough when a new system is introduced.

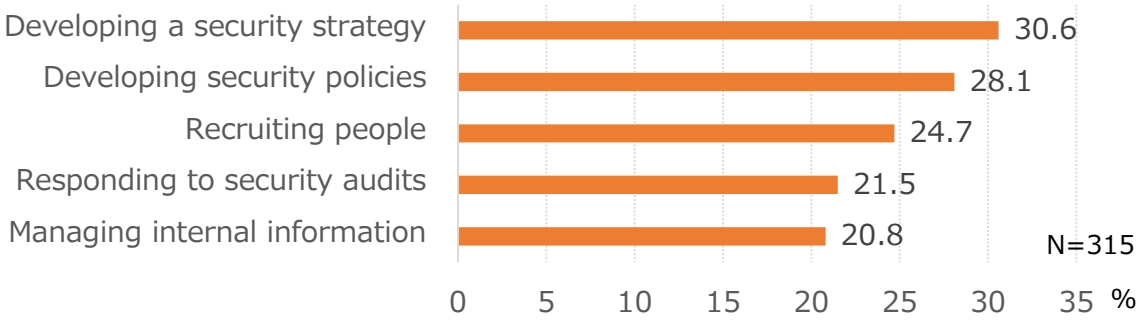


Have any cybersecurity incidents occurred in the systems used to promote DX? (Single answer)

What damage did the security incident cause? (Multiple answers)

Figure 2: Occurrence of security incidents in DX

When asked if they have concerns about cybersecurity measures in the DX efforts at their companies, about 31% of respondents said that they were concerned about "developing a security strategy" and 28% about "developing security policies." This indicates that many companies are concerned about developing strategies and policies that are the axes of security measures for organizations.



Do you have any concerns about cybersecurity measures in your company's DX promotion? Please select all that apply to your company's DX promotion in which you are most deeply involved. (Multiple answers)

Figure 3: Cybersecurity concerns in DX

[3] Trend Micro, "Security Trend Survey of Corporate Organizations in DX Promotion" (November 2021), https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20211130-01.html. Copyright (©) 2022 Trend Micro Incorporated. All rights reserved. Trend Micro is a registered trademark of Trend Micro Incorporated.

We will look at examples of actual DX failures due to security reasons.

Figure 4 shows major domestic cases where DX services (new businesses using new digital technologies) were discontinued due to inadequate security. In the cases of a major telecommunications carrier and a major retailer, inadequate authentication functions caused financial losses to users and others throughout Japan. In the case of a major human resource services provider, the provision of personal data to companies and others without the subjects' consent caused a major social problem, leading to the discontinuation of the service.

Thus, if security measures in DX are neglected, not only could confidential information be leaked due to unauthorized access, etc., but the service itself could be forced to discontinue.

But deciding when to put security controls into effect is a critical matter. In general, departments promoting DX tend to develop many prototypes in a short period of time and develop systems through repeated PoC. It is undesirable for the security department to exert strong control during this trial-and-error stage. Security should not hinder DX. Rather than slowing down DX, IT security managers should seek to assist DX by developing a secure PoC environment and formulating guidelines. It is desirable that IT security managers become actively involved once the PoC is approved and commercial services are being considered in concrete terms.

Although this information is not publicly available, we have also heard about companies that made their internal security management systems too robust, resulting in significant delays in system releases for DX and many project members leaving their jobs due to becoming demotivated and exhausted from dealing with security issues. The balance between DX promotion and security management will become increasingly important in the future.

Company category	Time of occurrence	DX activities	Security issue	Result
Major telecommunications carrier	2019	Electronic payment services using smartphones	Unauthorized withdrawals due to inadequate authentication functions	Discontinued stand-alone services (Some of the functions were integrated into another application)
Major retailer	2019	Barcode payment services using smartphones	Unauthorized charge or use due to inadequate authentication functions	Discontinued services
Major human resource services provider	2019	Services that use artificial intelligence (AI) to analyze students' personal information and predict the rate at which they decline job offers	Failed to obtain permission to give personal data to third parties	Discontinued services
Internet-based services provider	2019	Marketplace specializing in download sales of digital contents	Credit card information leaked due to unauthorized access	Discontinued services (Later transferred the marketplace business to another company)

Figure 4: Major domestic cases where DX services were discontinued due to inadequate security measures

3. Financial impact of cyber risks

A JCIC survey of 47 companies in Japan that made timely disclosures of information leaks and other events found that 50 days after such disclosures, stock prices fell by an average of 6.3%. In the 2018 survey the average decline was 10%, so while there was a slight improvement, the adverse effect on stock prices remains. In addition to the financial impact of incident response, the reasons for the decline in stock prices could be concerns about system shutdowns and new sales activity, which could decrease the value of the companies.

The survey also looked at changes in sales and net income of companies that made timely disclosures. However, due to the significant impact of COVID-19 on their performance, we were unable to obtain precise figures. Therefore, we have not published the survey data in this report.

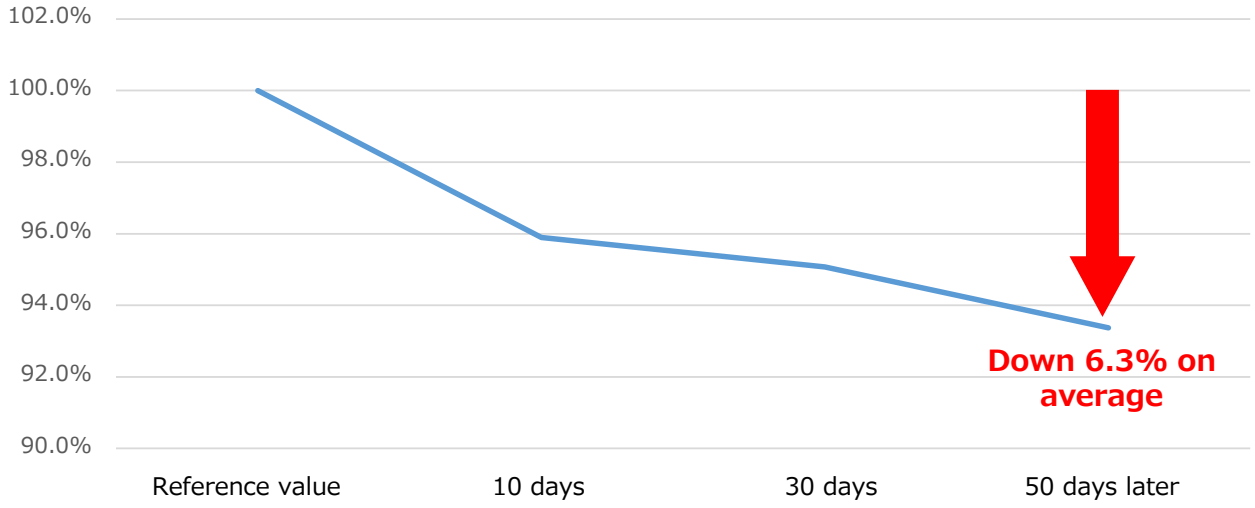


Figure 5: Stock price changes after timely disclosure of unauthorized access, etc. (n = 47)

Survey method
- 47 companies that made timely disclosures of unauthorized access, etc., to stock exchanges
- Companies that disclosed information in a timely manner since July 2014 are targeted
- The value ten days before the disclosure date was set as 100% (reference value)
- Variations are adjusted in accordance with the Nikkei Stock Average

Figure 6 shows examples of security incidents caused by cyberattacks in recent years. It is evident that cases of large-scale financial damage caused by a single cyberattack are occurring around the world. It can be said that DX with Security, the cybersecurity strategy to promote DX, is no longer an issue only for IT directors, CISOs, and security departments, but that it has become a management issue that directors, managers, and other executives should work on together.

No.	Time	Country or region	Organization	Type of impact	Financial impact (yen)	Outline
1	November 2021	Japan	Hospital	Repair costs	200 million	Construction costs of a new electronic medical record system
2	August 2021	Japan	Construction	Extraordinary loss	750 million	Investigation and recovery costs of ransomware infection
3	May 2021	Brazil	Meat processing	Ransom	1.2 billion	Infected by ransomware and paid the ransom
4	October 2020	United Kingdom	Airline	Penalty	2.7 billion	Violated GDRP due to leakage of personal information
5	October 2020	United Kingdom	Hotel	Penalty	2.5 billion	Violated GDRP due to leakage of personal information
6	March 2019	Norway	Manufacturer	Suspension of business	4.5 billion	Decrease in production volume due to ransomware infection
7	October 2018	Hong Kong	Airline	Market capitalization	22.6 billion	The share price declined by 3.8% due to unauthorized access
8	August 2018	Taiwan	Semiconductor	Suspension of business	27.5 billion	Production stopped for three days due to ransomware infection
9	January 2018	Japan	Cryptocurrency	Financial damage	58 billion	Crypto assets leaked by unauthorized access
10	December 2017	United States	Transportation	Suspension of business	44 billion	Significant effects of ransomware infection
11	August 2017	Denmark	Transportation	Suspension of business	33 billion	Delays and disruptions in transportation due to ransomware infection
12	June 2017	Germany	Pharmaceuticals	Suspension of business	36 billion	Network shutdown due to ransomware infection
13	February 2016	Bangladesh	Banking	Financial damage	108 billion	Unauthorized remittance to overseas accounts by unauthorized access
14	July 2014	Japan	Education	Extraordinary loss	26 billion	Invested in countermeasures after information leakage by an insider

Figure 6: Examples of security incidents that resulted in financial damage

4. Responsibilities of directors and officers

When companies promote DX with Security, the technical aspects often become the focus of attention. But it is also essential to consider the legal factors, such as the legal liability of officers and employees, and liability for damages. Since security measures are of fundamental managerial significance in promoting DX, they are considered an essential element to be discussed when establishing an internal control system under the Companies Act. In other words, failure to have adequate security measures may result not only in damage to the company, but also in awards of compensation for damages and breaches of the duty of care of a prudent manager.

In addition, shareholders, institutional investors, and others may file class action lawsuits against the company, claiming that it has stalled DX implementation and decreased corporate value. Or they may demand that the board of directors return remuneration, or resign. In the U.S., class action lawsuits concerning personal information leaks are particularly active, and many cases have resulted in massive amounts of settlements. In Japan, the number of class action cases is small. However, there have been many cases of management resignations and returns of remuneration.

Business category	Outline	Amount of settlement, etc.
Insurance company	About 80 million customer data items leaked in the U.S.	Settlement of 12.7 billion yen
Retailer	About 7,000 credit card details leaked in the U.S.	Settlement of 3.1 billion yen
Retailer	About 5,600 credit card details leaked in the U.S.	Settlement of 2.8 billion yen
Internet-based services provider	36 million data items leaked at a matching site in Canada	Settlement of 1.4 billion yen
Manufacturer	Employee information and other content not yet published, etc., leaked due to unauthorized access	Settlement of 0.9 billion yen
Internet-based services provider	A large amount of user information leaked in the U.S.	Settlement of 5.5 billion yen
Vehicle dispatching services provider	57 million pieces of personal information leaked in a cyberattack in the U.S.	Settlement of 17.0 billion yen
Retailer	Two million pieces of information leaked, leading to a class-action lawsuit for violation of CCPA	Under dispute
Telecommunications carrier	One hundred billion yen in damages claimed for taking trade secrets and moving to a competitor	One hundred billion yen in damages claimed
Educational services provider	A class-action lawsuit was filed for the inadequacy of 500-yen gift coupons as an apology	Under dispute

Figure 7: Examples of lawsuits related to information security

Business category	Time	Outline	Impact
Internet-based services	2021	Member information leaked due to unauthorized access	Remuneration of CEO reduced by 30% for three months
Stock exchange	2020	Service shutdown due to system failure	Resignation of CEO
Retailer	2019	Service shutdown due to inadequate authentication	Resignation of CEO
Game industry	2018	Service shutdown due to unauthorized access	President and Representative Director received no compensation for one year
Local municipality	2019	Extraction of personal information by a staff member	Salary of mayor reduced by 10% for two months

Figure 8: Examples of management resignations and returns of remuneration.

Furthermore, it should be noted that privacy and data security also affects a company's environmental, social and governance (ESG) rating, and other sustainability ratings. Disclosure of non-financial information, such as security measures, can benefit various corporate ratings made by institutional investors. In contrast, ratings may be lowered if rating agencies cannot obtain such information from a company. A company's ESG rating being downgraded could cause severe damage due to increased financing costs and the risk of a decrease in its number of business partners.

It is essential to publish, widely and routinely, information on the company's security initiatives on the company website, shareholder website, etc., to improve credibility among customers and stakeholders. When publishing information, it is not necessary to disclose information that could lead to cyberattacks; rather, the attitude of management to such efforts should be widely disseminated. For more information on reducing losses, please refer to the Corporate Cybersecurity Disclosure Report.[4]

Rating Agency	Dow Jones Sustainability Indices (DJSI)	Morgan Stanley Capital International (MSCI)
Overview	Leading rating agency, selected as the number one "Quality ESG Rating Agency" in a survey of experts	One of the world's largest index providers, with its MSCI ESG Research division conducting ESG assessments of approximately 7,500 issuers
Sources	– Questionnaire survey – Publicly available information on companies	– Publicly available information on the company
Assessment Methodology	Scores are calculated from ESG data on each company (approximately 5,000 companies), and those with the highest ratings are selected for the index	Scored and rated at seven levels: AAA, AA, A, BBB, BB, B, and CCC
Privacy and Data Security Assessment Positioning	"Cybersecurity & System Availability" and "Privacy Protection" are rated on a 100-point scale, depending on the industry	Within the "Social" score, there is a "Safety of Products and Services; Privacy & Data Security" category, which is rated on a 10-point scale

Figure 9: Privacy and data security assessment policies of major ESG rating agencies

[4] JCIC, "Corporate Cybersecurity Disclosure Report – Management's Attitude of Dealing With Cybersecurity is Important"; https://www.j-cic.com/pdf/report/Disclosure-Report.pdf

5. Recommended approach to realize a DX with Security strategy

A DX with Security strategy is essential to promote DX, improve corporate productivity and efficiency, and avoid significant financial losses. A DX with Security strategy means “a security policy to achieve the objectives of DX.” In addition, a medium- to long-term security resource plan (budget, human resources, etc.) must be considered and approved by the board of directors, etc.

For DX with Security leading companies to develop their strategies, JCIC recommends the following approach.

Recommended approach to strategy development for DX with Security leading companies

(1) Visualize risks using a cyber-risk estimation model

(2) Develop a DX with Security strategy

- **Use a framework to explain the strategy as a story**
- **Security investment should be 0.5% or more of consolidated sales revenue**
- **Security personnel should be 0.5% or more of the total number of employees**

(3) Set security KPIs and monitor them regularly

(1) Visualize risks using a cyber-risk estimation model

When discussing cybersecurity, it is easy to end up discussing it from a technical perspective. However, when explaining to management, IT security managers should report from a business perspective. The most effective way to explain cybersecurity from a business perspective is to use the common language of management: money. While managers may be unfamiliar with IT terminology, no manager does not understand money.

Various studies have been conducted around the world on quantifying cyber risks, but there is no established method of risk quantification because of the evolution of the attacks. In recent years, research on the quantification of cyber risk has been conducted overseas. That is not necessarily suitable for Japanese companies, because in-house resources are required for data collection and complex computational processing (see reference material).

Therefore, JCIC has updated its cyber-risk estimation model, released in 2018. The latest version enables Japanese companies to easily calculate the maximum loss (probable maximum loss, or PML). The model roughly estimates the maximum loss, and an Excel document for simple simulation is available on JCIC's website.

By using this estimation model, cybersecurity can be discussed in terms of "money," the common language of management, instead of having a technical discussion. If the loss amount is used as a starting point for discussion, it should provide an opportunity for management and workers to develop a common understanding of the issues, and for management to view cyber risks as being important to them.

		Probable maximum loss	Basis of calculation
Direct loss	Loss due to personally identifiable information leakage	▲1.2B yen	Estimated damages per person are calculated based on the JO model by JNSA (for 100,000 leaked details: damages of 1.2 billion yen)
	Loss due to business downtime	▲2B yen per five business days	Maximum business impact in the event of a large-scale system shutdown due to ransomware infection
	Fines and penalties due to violation of law	▲100M yen	Fine imposed under Japan's revised Act on the Protection of Personal Information.
	Incident response costs	▲60M yen	Forensic investigation, call center costs, dark web investigations, cost of preventing recurrence, etc.
Indirect loss	Loss of market capitalization	▲6.3B yen	Calculated from JCIC survey results (Market capitalization of 100 billion yen × 6.3% = 6.3 billion yen)

Figure 10: Cyber-risk estimation model (for a manufacturing and sales company with annual sales of 100 billion yen)

(2) Develop a DX with Security strategy

- **Use a framework to explain the strategy as a story**

The security policy to achieve the objectives of DX (a DX with Security strategy) should be simple, so that everyone will understand it the same way. It should not use technical jargon. It should explain the challenges and solutions (see references). It is helpful to use a framework to tell the story of the strategy. The following is a framework for a DX with Security strategy that can be used as a reference.

Item	Description
Objectives of DX	Describe the objectives of implementing DX
Security Challenges	Describe security and privacy protection issues in promoting DX
Solutions and Effects	Describe the measures taken to resolve the issues and the benefits of implementing them
Investment Plan	The security investment is recommended to be 0.5% or more of consolidated sales revenue
Workforce Planning	The number of security personnel is recommended to be 0.5% or more of the total number of employees

Figure 11: Framework for DX with Security strategy

Model Case A: Pharmaceutical company with annual sales of 500 billion yen and 5,000 employees

Item	Security policy to achieve the objectives of DX (a DX with Security strategy)
Objectives of DX	To build cutting-edge drug discovery technological capabilities, the company will collaborate with universities and hospitals in Japan and abroad, to establish within three years an innovative new drug creation process that uses AI, health tech, and other digital technologies.
Security Challenges	Medical research data is a target of cyberattacks and requires strict security measures. In the event of an information leak, direct damage of 37 billion yen and indirect damage of 33 billion yen could be caused.
Solutions and Effects	Implement secure cloud services, zero-trust architecture, enhanced access management for collaborating partners, etc. New drug discovery processes (such as AI drug discovery and clinical trials using wearable devices) can be securely established with external partners, thus shortening new drug development.
Investment Plan	2.5 billion yen per year
Workforce Planning	25 (20 full-time employees, five outsourced)

Model Case B: Manufacturing and sales company with annual sales of 100 billion yen and 2,000 employees

Item	Security policy to achieve the objectives of DX (a DX with Security strategy)
Objectives of DX	To add value to customers, increase online membership registration and develop new annual subscription-based services. Achieve a 20% increase in sales within three years.
Security Challenges	Since the company handles a large amount of personal information, information theft could cause direct damage of 3.4 billion yen and indirect damage of 6.6 billion yen. This would significantly affect the company's business strategy.
Solutions and Effects	Achieve high levels of development convenience and security management by developing and introducing secure systems, training employees, and increasing numbers of security personnel. As a result, the company will establish a value-added, safe brand and differentiate itself from its competitors.
Investment Plan	500 million yen per year
Workforce Planning	10 (seven full-time employees, three outsourced)

Model Case C: Cram school with annual sales of 30 billion yen and 1,000 employees

Item	Security policy to achieve the objectives of DX (a DX with Security strategy)
Objectives of DX	New online classes and content using external data will be developed within two years, to improve the quality of class service. The company will also establish a specialized online school to attract students from remote areas.
Security Challenges	While making the service easy to use, even for students unfamiliar with IT, it is necessary to strictly protect sensitive information such as grades and career paths. A large incident could cause direct damage of 1.7 billion yen and indirect damage of 1 billion yen.
Solutions and Effects	Implement multi-factor authentication for user accounts, prevent unauthorized access, educate employees, and raise awareness among students. Improve unit costs for existing students, and attract new students in remote areas by providing secure digital tools.
Investment Plan	150 million per year
Workforce Planning	Five (four full-time employees, one outsourced)

- **Security investment should be 0.5% or more of consolidated sales revenue**

For a DX with Security strategy to be approved by management and others, a medium- to long-term security resource plan (investment budget, personnel, etc.) must also be developed.

First, it is recommended that security investment for DX with Security leading companies should be planned at 0.5% or more of consolidated sales revenue. That guideline is based on survey data from financial institutions.[5] The rationale is that DX with Security leading companies should invest to the level of financial institutions that use IT systems to generate added value. This investment includes the costs of personnel, outsourcing, and purchasing and using security systems. For example, a company with annual sales of one billion yen should invest five million yen per year in security, while a company with annual sales of 100 billion yen should invest 500 million yen per year in security.

At this stage, the companies to which the guideline of 0.5% or more should apply are DX with Security leading companies that invest human resources and budgets in DX as much as IT companies do, and reform their business models and business processes. In other words, companies seeking a high level of usability and security management across the entire company (usability and monitoring type) should use this figure as a guide to their security investment. It is assumed that DX with Security follower companies will also use this as a target value in the future.

Consolidated sales revenue	Guideline for security investment (0.5% of consolidated sales revenue)
1 trillion yen or more	5 billion yen or more
500 billion yen	2.5 billion yen
100 billion yen	500 million yen
50 billion yen	250 million yen
10 billion yen	50 million yen
5 billion yen	25 million yen
1 billion yen	5 million yen

The security investment amount can be calculated either from the percentage of the IT budget or from the amount spent per employee. As a rough estimate of the former, many Japanese companies invest 5% to 9.99% of their IT budgets on security.[6] As a rough estimate of the latter, survey data show that financial institutions invest approximately 310,000 yen (US$2,691) in security per full-time employee.[7]

[5] According to a survey of financial institutions conducted by the Financial Services Information Sharing and Analysis Center (FS-ISAC) and Deloitte, cybersecurity spending as a percentage of total revenue was expected to increase from 0.34% in 2019 to 0.48% in 2020.
https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/risk/cr/jp-cr-reshaping-the-cybersecurity.pdf
In addition, JP Morgan invests more than 66 billion yen annually in cybersecurity, which is 0.5% of its sales revenue.
https://reports.jpmorganchase.com/investor-relations/2018/ ar-ceo-letters.htm
The rate of 0.5% was chosen as the guideline because the percentage of spending on cybersecurity is increasing, and companies seeking DX with Security should be making investments comparable to those of financial institutions.

[6] PwC, “Digital Trust Insights To Raise the Resilience Quotient,”
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/resiliency-quotient2002-02.pdf

[7] FS-ISAC and Deloitte, “Rebuilding the Cybersecurity Outlook,” https://www2.deloitte.com/jp/ja/pages/risk/articles/cr/reshaping-the-cybersecurity.html

The following items that should be included in the security investment amount. The investments can be divided into the following categories: personnel costs, training costs, system costs,[8] outsourcing costs, and evaluation and audit costs. Since the budgeting process differs from company to company, this information should be used only as a reference.

Classification	Primary security investment items
Personnel costs	Labor costs for dedicated security personnel
Training costs	Security training costs
System costs	Security system purchase and maintenance costs
	Security service usage costs
	Consulting costs
	Outsourcing costs
Outsourcing costs	Temporary staffing costs
	Consulting costs
	Contracting and outsourcing costs
Evaluation and audit costs	Certification acquisition and renewal costs
	External audit costs

Figure 12: Primary security investment items

It is not always easy to distinguish between IT costs and security costs. For example, security options included in cloud services are difficult to distinguish. In such cases, rather than strictly managing cost allocation, it would be more practical to record them as items that provide key functions; i.e., IT costs for cloud services. Similarly, for personnel concurrently engaged in security operations and in the core business, it is more practical to record their costs in the core business category.

By ensuring adequate internal security resources and implementing key measures, the aforementioned security issues will be resolved, and the benefits of achieving the objectives of DX will be realized. It is also expected to improve the evaluation and maturity of various security assessments. Companies wondering where to start implementing security measures are recommended to conduct an IT Security Diagnosis[9] by the Information-technology Promotion Agency (IPA) of Japan. The flow of the security evaluation is as follows. Since the recommended measures are visualized, it is easy to take the subsequent actions.

1. Answer questions on the Cybersecurity Management Visualization Tool.
2. Diagnostic results are displayed, and benchmark comparisons and recommended initiatives are provided.
3. Related practices (examples of measures) are provided.

[8] Rent for SOCs or data centers, etc., may be included for some companies.
[9] Information-technology Promotion Agency (IPA), “IT Security Diagnosis,” https://security-shien.ipa.go.jp/diagnosis/

Notes about security resources of “0.5% or more”

- The figure of 0.5% or more is only a guideline. Regardless of changes in consolidated sales revenue or the number of employees, it is necessary to set an appropriate target for the company, based on multiple sources of information.
- Security resources may be required that exceed the guideline of 0.5%, depending on the situation, such as installation of a new system or incident response. Conversely, an investment of less than 0.5% may be adequate because an investment program is “over the hump” and falling.
- The amount of security investment and the number of dedicated security personnel are company-wide resource totals. They are not figures for only parts of systems, or only some departments.
- At this stage, the companies for which investments of 0.5% or more should apply are DX with Security leading companies. DX with Security follower companies can also use this as a target for the future.
- If it is difficult to distinguish between IT costs and security costs, it is preferable to record them in the item to which the primary function is provided.

[Column] Security resources that should be spent on new DX systems

The figure of 0.5% or more of consolidated sales revenue, as quoted in this document, is a guideline for the security investment that a company should make.

We have also received many questions about the quantity of security resources required in the development of a new DX system.

Although appropriate security investment rates will vary, depending on the characteristics of the newly developed system, we believe that 10% of the new DX system investment should be allocated to security investment.

According to the abovementioned survey of financial institutions conducted by FS-ISAC and Deloitte, security investment accounts for 8.2–11.9% of IT spending. In a new DX challenge, 10% would be a good target, based on the idea that security investment equivalent to that of financial institutions is required.

- **Security personnel should be 0.5% or more of the total number of employees**

When considering the number of dedicated security personnel, we recommend DX with Security leading companies plan to dedicate 0.5% or more of their total number of employees. This percentage takes into account various reports and the JCIC survey.[10] It includes dedicated security personnel, IT subsidiary employees, and outsourced personnel. If there are personnel engaged in security operations at overseas subsidiaries or affiliates, they too should be counted. But "plus (+) security human resources" (personnel required to have security skills in order to perform their primary duties and while using IT) are not counted as dedicated security personnel.

For example, at a company with 500 employees, there should be three security personnel; if there are 3,000 employees, there should be 15 security personnel. For a large company with 10,000 employees, the number of security personnel is assumed to be 50 or more, as that number is highly variable, depending on the industry and the type of business. For companies with 100 or fewer employees, the number of security personnel is set at two, instead of one, considering the necessity of a backup.

The guideline of 0.5% or more is intended for DX with Security leading companies at this stage, with an assumption that DX with Security follower companies can use this same guideline in the future.

Total number of employees	Number of dedicated security personnel (0.5% of the total number of employees)
10,000 or more	50 or more
5,000	25
3,000	15
1,000	5
750	4
500	3
250	2
100	2

The primary tasks (job descriptions) of dedicated security personnel are as shown below. Tasks can be divided into governance (policy development and internal control) and assessment (evaluation and audit), both performed by the security management division and CISO office, and operations (operation and incident response), performed by the Security Operation Center (SOC) and Computer Security Incident Response Team (CSIRT). When planning the security structure and recruiting people, it is necessary to consider how many security personnel should be allocated to which tasks, and which parts should be outsourced.

[10] (a) According to ITR's "Japan IT Budget & Spending Trends 2021," the rate of IT staff to total employees is "7.2% on average" and is increasing every year. https://enterprisezine.jp/article/detail/12656
(b) Carnegie Mellon University surveyed 555 organizations in four countries with annual sales of over $6 billion. The average percentage of security employees to IT department employees was 5.2%. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf
From (a) and (b) above, security staff as a percentage of total employees = total employees × (a) 7.2% × (b) 5.2% = 0.37%.
In addition, Korea's Regulation on Supervision of Electronic Financial Transactions stipulates that security employees must comprise 0.25% or more of the total number of employees, and that the security budget must be 7% or more of the total IT budget.
http://www.law.go.kr/행정규칙/전자금융감독규정 (Article 8)
The rate of 0.5% was set as a reference because the rate of IT staff has been increasing year by year, and because companies aiming for DX with Security should strengthen their staffing above the industry average. To verify the validity of the value of 0.5%, we used JNSA's "Survey Report on the Current Status of Personnel Responsible for Security Operations" and JCIC's internal knowledge.

Classification	Task
Governance	Security strategy development (including budget and structure)
	Security policy development and revision
	Security education and awareness
	Compliance and privacy response
Assessment	Risk assessment
	Vulnerability assessment, penetration testing
	Security audit
Operations	Security service installation and operation
	Security monitoring, detection, and response
	Incident response
	Forensic and malware analysis
	Collection, analysis, and use of threat and vulnerability information

Figure 13: Primary tasks of dedicated security personnel[11]

Recruiting and training security personnel has become a problem for many companies, and various research studies have been conducted in Japan and abroad. The following is a list of information that may be of particular interest to companies building a security structure and training security personnel.

- **Security structure considerations**
  - The Ministry of Economy, Trade and Industry's "Guidebook for Establishing Cybersecurity Systems and Securing Necessary Human Resources"
  - JNSA's "Survey Report on the Current Status of Personnel Responsible for Security Operations"
  - CRIC CSF's "Security Control Unit Establishment and Operation Kit for User Companies (Control Unit Kit)"
- **Personnel training**
  - NISC's "Cybersecurity Portal Site"
  - JCIC's "Realizing DX with Security through Proactive Plus Security Human Resources"
  - Japan Trusted Alliance Group for cybersecurity's (JTAG's) "VisuMe"
  - NIST in the U.S. "NICE Framework"

[11] Prepared by JCIC with reference to the Ministry of Economy, Trade and Industry's "Guidebook for Establishing Cybersecurity Systems and Securing Necessary Human Resources."

(3) Set security KPIs and monitor them regularly

It is effective to use cybersecurity KPIs to monitor whether cybersecurity measures are functioning correctly. JCIC proposes that IT security managers select from the 47 KPIs in the model, according to the stages that their organizations have reached (maturity level), and use them to set targets and evaluate performance. For more information, please refer to the Cybersecurity KPI Model.[12]

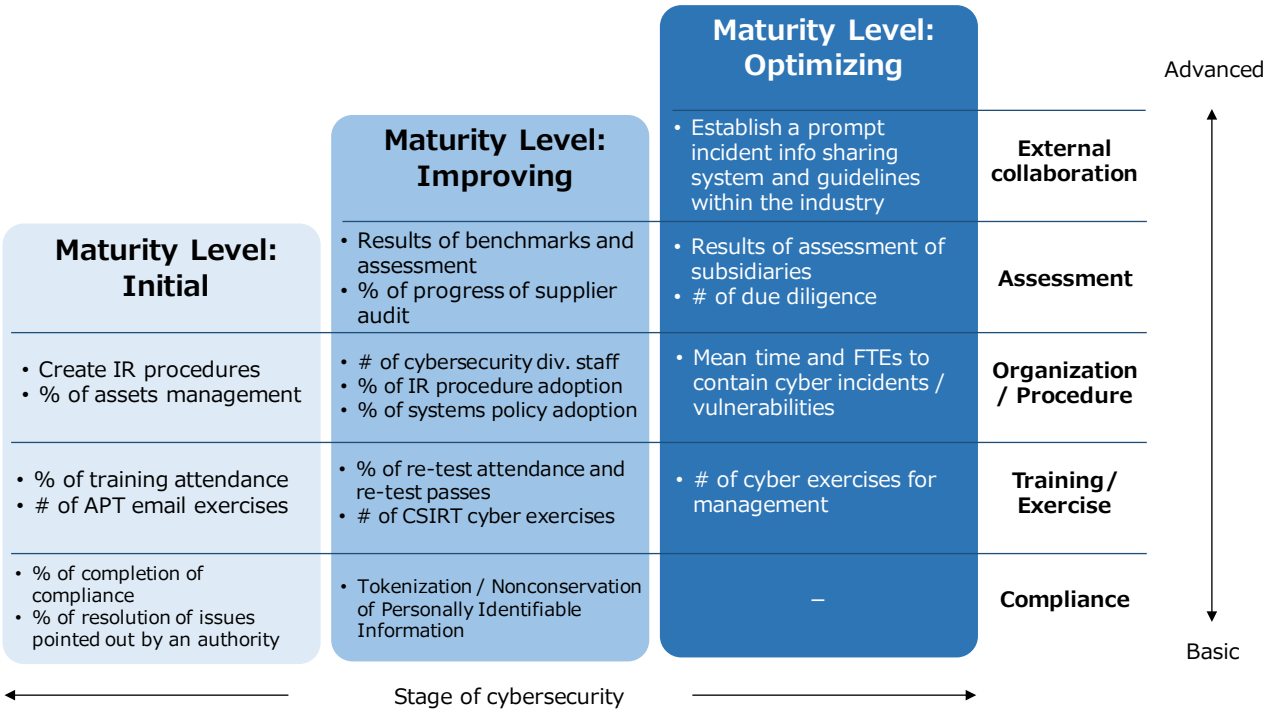


Figure 14: Cybersecurity KPI Model

The status of monitoring by KPIs should be reported periodically to the board of directors and other relevant parties. In addition, information on the trend of attacks occurring in cyberspace, efforts being made by other companies, and trends in applicable laws and regulations will also help company directors.

FY 2022 Security investment	Plan	Result	YoY
	¥200 M	¥195 M	18% ↑

Implementation status

Security measures		KPI	Result
Risk management system	Increase in cybersecurity-related personnel	CSIRT: from 7 to 10	Employee +1 person
			Contractor +2 persons
		Operation personnel: from 3 to 5	Contractor +2 persons
Supply chain	Confirmation of security measures implemented by affiliates and business partners	+ 5 companies (from 68% to 82%)	Performed on four companies (76%)
Information sharing in the industry	Establishment of information provision scheme	Completed	Completed
	Establishment of information acquisition scheme	Completed	Delayed to March 2023

Operation status

Management item			Result	YoY
Security incident	Number of occurrences		124	-5%
	Estimated loss		¥20 M	-6%
	Restoration costs		¥1 M	+5%
Risk identification	Risk assessment target system		231	+1%
	Number of findings	High	53	+2%
		Medium	230	-3%
		Low	78	-4%
	Remedial action progress rate		43%	+6%pt
Education	Security education attendee		1,936	+1%
	Security training sessions		36 times	±0%
	Training attendance rate		85%	+2%

Figure 15: Example of a periodic report to management

[12] JCIC's "Cybersecurity KPI Model (tentative)," https://www.j-cic.com/pdf/report/KPI-Report-JA.pdf

6. Summary

In this report we explained that a DX with Security strategy is essential to promote DX, improve corporate productivity and efficiency, and avoid significant financial losses. Cyber risks are a common and imminent issue to be considered in all DXs, where digital technology is used to develop innovative new businesses and fundamentally reform business processes. As digitization and remote work became widespread during the COVID-19 pandemic, and the number of companies working on DX increased dramatically, many companies are struggling to balance DX and security. We hope you will use this report as a guide to promoting DX with Security in your organization.

Until a few years ago, IT and security departments were sometimes viewed as cars, with the IT department being the engine and the security department the brakes. The logic is that a car needs high-performance brakes to travel safely at high speed. However, DX with Security requires the security department to play the role of an electronic control unit (ECU) in an electric car, guiding the departments promoting DX in the right direction and helping it to achieve results. In other words, the role of the security department should not be limited to the defensive position it has played in the past. In the future it must work closely with the business divisions and assist them while accompanying them in DX. To this end, a fundamental review of the security department's policies and resources will be required, including the development of a DX verification environment and guidelines, active involvement in DX projects, and quicker reviews.

Finally, we present a checklist of the key points of this report. It lists not only the approaches mentioned above, but also attitudes and dispositions. We hope you will find it useful for your future reference.

Key points of this report

- ✓ Visualize risks using a cyber-risk estimation model
- ✓ Develop a DX with Security strategy, using a framework to explain the strategy as a story
- ✓ Security investment should be 0.5% or more of consolidated sales revenue
- ✓ Dedicated security personnel should comprise 0.5% or more of the total number of employees
- ✓ Set security KPIs and monitor them regularly
- ✓ Widely disclose information on the status of security initiatives
- ✓ Do not apply strong controls during the prototype or PoC stage
- ✓ IT security managers should be involved at the stage when commercial services are being considered in concrete terms

End of report

Reference material 1: Explanation of "Probable Maximum Loss" cyber-risk estimation model

JCIC has released an Excel document for simple simulation, so that Japanese companies can easily calculate their probable maximum loss (PML). It is calculated by selecting and entering all the items in the yellow cells.

Item	Input item	Description
(1)-1 to (1)-3 Loss due to personally identifiable information leakage	• Degree of information sensitivity • Degree of ease in identifying • Number of items of personally identifiable information	Assumed damages if personal information is leaked due to a security incident. Calculated using the JO Model published by JNSA as a formula for calculating damages. To reduce the input burden, the "Degree of social responsibility" was set to "High" for companies with annual sales of 100 billion yen or more, and "Others" for companies with annual sales of less than 100 billion yen. The "Appraisal of post-incident response" was set to "Unknown" in all cases.
(2)-1 to (2)-2 Loss due to business downtime	• Sales per day • Business downtime	The amount of lost sales opportunities during the suspension of operations caused by the shutdown of internal systems and e-commerce sites due to ransomware infection. For simplicity, it is calculated as "sales per day × business downtime."
(3) Fines and penalties due to violation of law	• Annual global turnover • EU personal information • China personal information • Japan personal information	Assumes penalties under the EU's General Data Protection Regulation (GDPR), China's Personal Information Protection Law, and Japan's revised Act on the Protection of Personal Information.
(4) Incident response costs	• Forensic investigation • Call center costs • Dark web investigations • Cost of preventing recurrence	Cost of investigating whether or not a company has suffered a cyberattack, and if it has, the effects and the cause of the attack (forensic costs), data recovery costs, and security enhancement costs for emergency measures and to prevent recurrence of such an attack. Assumed amounts are based on JNSA's Incident Losses Survey Report 2021. It is recommended that each company consult with security firms, etc., to calculate the amount.
(5) Loss of market capitalization due to decline in stock prices	Market capitalization	Calculated from JCIC survey results. Surveyed 47 companies and found a 6.3% decrease in stock price 50 days after timely disclosure of a security incident.

Cyber-risk Estimation Model "Probable Maximum Loss"

Japan Cybersecurity Innovation Committee

version 2.0

Please answer the following questions below.

#	Category-1	Category-2	Question	Answer	
①-1	Loss of Personal Identified Information(PII) Leakage	Degree of Information Sensitivity	Please select the degree of information sensitivity your organization has.	1-1_Name, Adress, E-mail, Birth Date_1	
①-2		Degree of Ease in Identifying	Please select the degree of ease in identifying PII your organization has.	6_Easy	
①-3		Number of Personal Identified Information	Please select the number of PII your organization has.	100,000	
②-1	Loss of Business Downtime	Sales Per A Day	Please input your organization's sales amount per a day.	400,000,000	JPY
②-2		Maximum Downtime	Please input your organization's maximum downtime due to critical incident. (If you have not estimated, please input 5 days for average downtime.)	5.0	Day
③	Fines and Penalties by Violation	Annual Global Turnover	Please input your organization's annual global turnover of last fiscal year	¥100,000,000,000	JPY
③-1		EU GDPR	Does your organization have EU PII?	No	
③-2		China PIPL	Does your organization have Chinese PII?	No	
③-3		Japan PIPL	Does your organization have Japanese PII?	Yes	
④-1	Incident Response Fee	Forensic Cost	Outsource the forensic investigation for 10 hosts?	Yes	
④-2		Call Center Cost	Consider to outsource the call center for 3 month?	Yes	
④-3		Dark Web Monitoring	Outsource the dark web monitoring service for 3 month?	No	
④-4		Recovery Cost	Consider the recovery cost (such as security tool implementation, re-organization or training) ?	Yes	
⑥	Loss of Market Capitalization	Market Capitalization	Please input your organization's market capitalization.	¥100,000,000,000	JPY

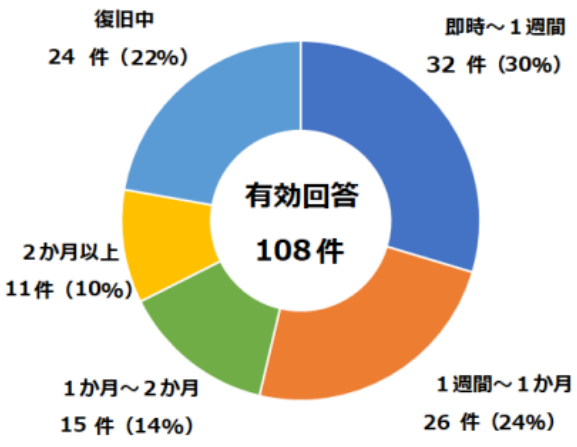
Probable Maximum Loss of Your Organization

Direct Loss	①Loss of Personal Identified Information Leakage	-¥1,200,000,000	▲ 1.2	B JPY
	②Loss of Business Downtime	-¥2,000,000,000	▲ 2.0	B JPY
	③Fines and Penalties by Violation of Law	-¥100,000,000	▲ 0.1	B JPY
	④Incident Response Fee	-¥55,000,000	▲ 0.1	B JPY
Indirect Loss	⑤Loss of Market Capitalization	-¥6,300,000,000	▲ 6.3	B JPY

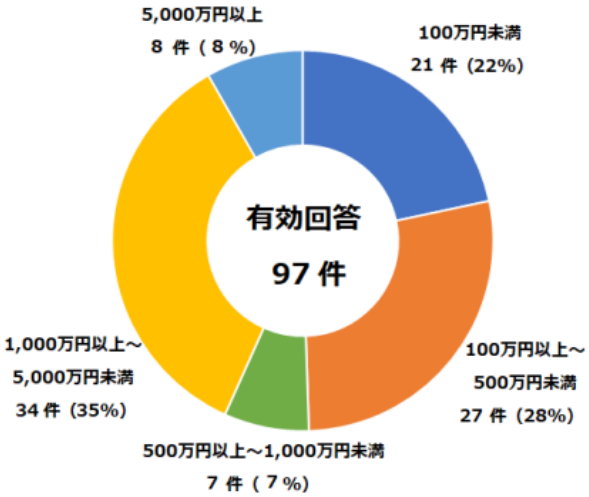
Reference material 2: Numerical data on ransomware

Item	Description	Supplemental information
Average ransom payment[*1]	US$322,168 (approximately 37 million yen)	Increased by 130% from the previous quarter, because of inconspicuous targeting of large companies.
Median ransom payment[*1]	US$117,116 (approximately 13.5 million yen)	Up 63% from the previous quarter.
Average downtime[*1]	20 days	Down 9% from the previous quarter, due to an increase in the number of companies that could recover, using backups.
Ransomware repair costs[*2]	US$1.85 million (approx. 210 million yen)	Almost doubled from the previous year
Ransom payment rate[*2]	32%	Up six points from the previous year
Number of reports of ransomware damage per year (Japan)[*3]	146 cases	Small to medium-sized companies: 54% Large companies: 34%
Time required to recover from damage (Japan)[*3]	Immediately to one week, typically	See figure below
Total amount spent on investigation and recovery from damage (Japan)[*3]	The largest number of respondents were in the 5–10 million yen range	See figure below

被害からの復旧に要した期間



被害の調査・復旧に要した総額



*1 Coveware's Quarterly Ransomware Report. https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021
*2 Sophos: The state of ransomware – 2021. https://secure2.sophos.com/ja-jp/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
*3 National Police Agency, "Threats in Cyberspace in 2021," https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03 cyber jousei sokuhou.pdf

Reference material 3: Domestic and international trends in cyber risk quantification

According to the aforementioned FS-ISAC-Deloitte survey of financial institutions, cybersecurity spending varies by the financial sector. In 2020, cybersecurity spending expressed as a percentage of total revenue was 0.8% for financial utilities and 0.3% for consumer/financial services (non-bank) and insurance companies. The rate in IT spending ranged from 8.2% to 11.9%. Annual security spending per employee ranged from US$1,984 to US$4,375, which is 228,000–503,000 Japanese yen.

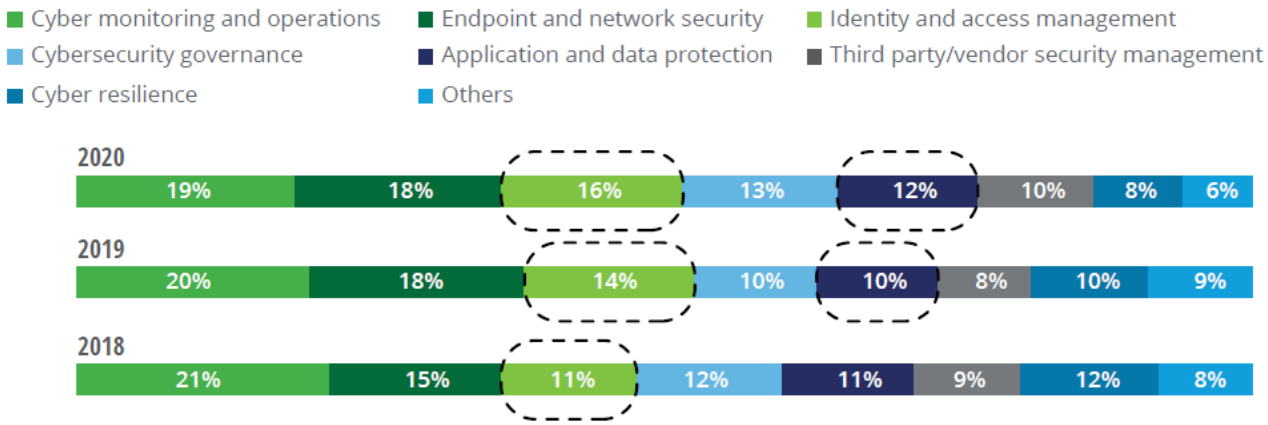
Cybersecurity spending across sectors

Percentage of revenue ■ Percentage of IT spending ■ Per FTE

	2019	2020
Retail/corporate banking	0.3% 10.1% US$2,074	0.6% 9.4% US$2,688
Consumer/financial services (nonbanking)	0.3% 9.7% US$2,817	0.4% 10.5% US$2,348
Insurance	0.3% 9.3% US$2,245	0.4% 11.9% US$1,984
Service provider	0.6% 8.9% US$1,956	0.6% 7.2% US$3,226
Financial utility	0.8% 15.2% US$3,630	0.8% 8.2% US$4,375
Aggregated total	0.3% 10.1% US$2,337	0.5% 10.9% US$2,691

In addition, budget allocations have changed little over three years. The three fields of cyber monitoring and operations, endpoint and network security, and identity and access management (IAM) accounted for more than 50% of the budget allocation.

Budget allocation across cybersecurity domains by survey respondents



Reference material 4: Domestic and international trends in cyber risk quantification

Various studies have been conducted in Japan and overseas on quantifying cyber risks. However, since attacks are evolving on a daily basis, there is no established method of risk quantification yet.

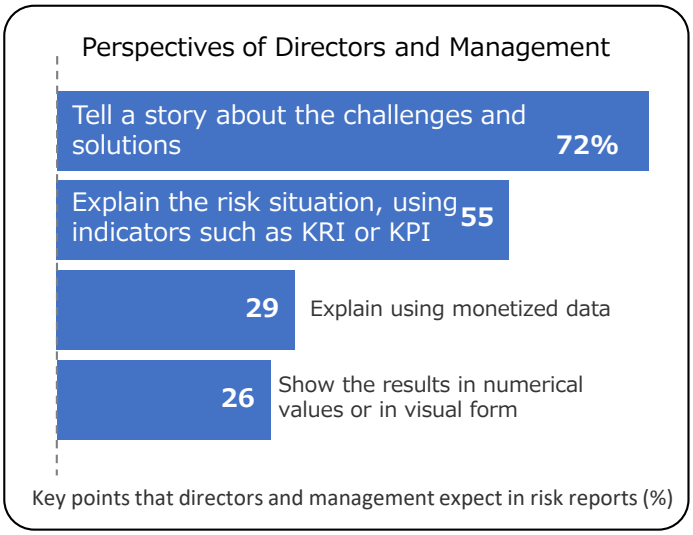
Title	Organization	Publication date	Outline
Cost of a data breach report	Ponemon Institute	September 2021	Surveys aimed at understanding trends in data breaches, such as their average total cost, and the variation in those factors and costs
Simulation of expected losses	Tokio Marine & Nichido Fire Insurance	March 2020	Calculate the expected loss amount in the event of damage caused by cyberattacks, based on a certain logic.
A cyber-risk estimation model to discuss in board of directors meetings	JCIC	September 2018	Cyber risk indicator model that converts cyber risk into monetary value
A framework for quantitative assessment	International Monetary Fund (IMF)	June 2018	Conducted quantitative analysis of cyber risk by Value at Risk (VaR, maximum loss), using the latest damage cases from 50 countries for analysis.
The impact of data breaches on reputation and share value	Ponemon, Centrify	May 2017	The stock prices were examined of 113 companies worldwide that experienced security incidents. Their stock prices dropped on average by 5%.
The cyber-value connection	CGI IT UK	April 2017	Investigated stock prices after security incidents. They dropped permanently by 1.5% after the incident.
Factor Analysis of Information Risk (FAIR) model	Fair Institute	February 2016	Quantitative risk analysis model. Potential future losses (risk) are calculated as a monetary value by evaluating one or more risk scenarios.
A framework for categorizing disruptive cyber activity and assessing its impact	University of Maryland	July 2015	A calculation method called the Cyber Disruption Index (CDI) is used to analyze the impact of cyberattacks.

Reference material 5: Key points that directors and management in the U.S. expect when reporting cyber risks

According to a survey of U.S. companies, the most common response from directors and management as to what they expect in cyber risk reports was “Tell a story about the challenges and solutions,” followed by “Explain the risk situation, using indicators such as KRI* or KPI.”

* KRI: key risk indicators; risk indicators that measure a company’s degree of risk.

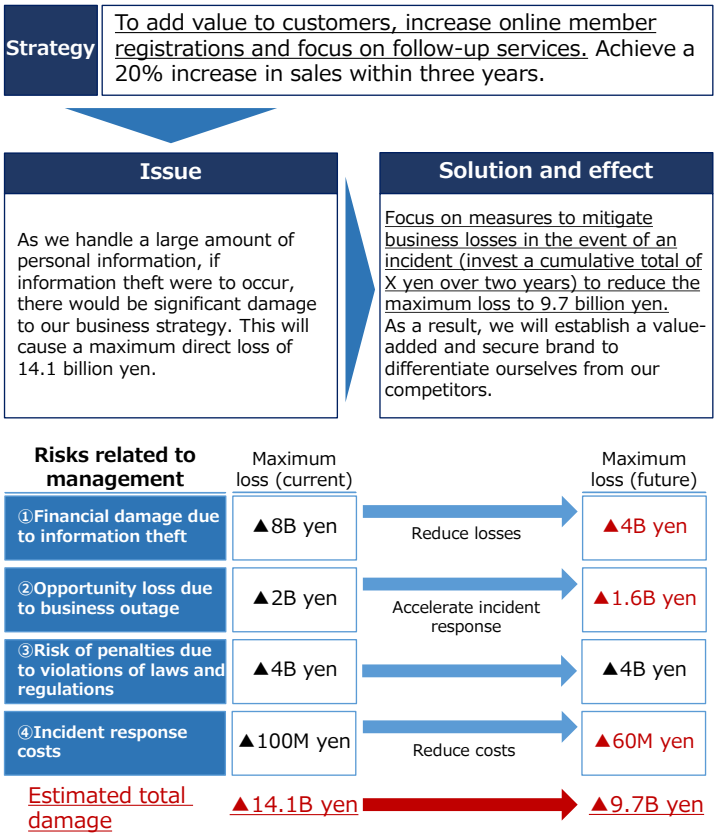
Source: Cyber Balance Sheet 2017 Report (Cyentia Institute survey, n = 85)



Reference material 6: Example of explanation to managements

IT security managers should report from a business perspective when explaining to management, without using technical terms. The most effective way to explain cybersecurity from a business perspective is to use the common language of management: money.

The following is an example of a manufacturing company with annual sales of 100 billion yen. It deals with air conditioning equipment for commercial and residential use. Air conditioning equipment is a mature market, and the company faces strong competition from overseas manufacturers. In its medium-term management plan, the company has adopted the strategy of "value-adding focused on customers' voices," making online membership registration mandatory for product purchases and emphasizing after-sales services such as notifications of when to replace consumable parts.

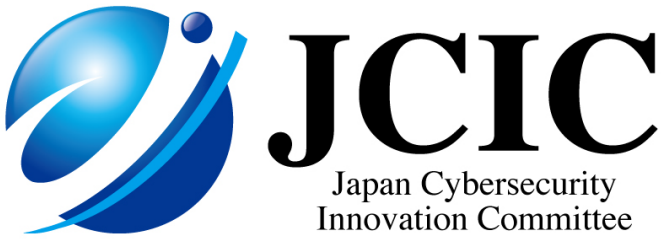


First, explain the purpose and importance of cybersecurity in the company's business strategy by telling a story. Its management strategy is "value-adding focused on customers' voices." If information theft were to occur, it would greatly affect that strategy and prevent the strategy of increasing membership.

By focusing on security measures to reduce losses in the event of an incident, the IT security manager has shown management that the maximum loss can be reduced from 14.1 billion yen to 9.7 billion yen. The maximum loss amount was converted into a monetary value using JCIC's cyber-risk estimation model.

References

- Japan Productivity Center, "Urgent Questionnaire on Expectations for the New Government and DX" (December 2022), https://www.jpc-net.jp/research/detail/005615.html
- Trend Micro, "Security Trend Survey of Corporate Organizations in DX Promotion" (November 2021), https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20211130-01.html
- PwC, "Digital Trust Insights To Raise the Resilience Quotient," https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/resiliency-quotient2002-02.pdf
- FS-ISAC and Deloitte, "Rebuilding the Cybersecurity Outlook," https://www2.deloitte.com/jp/ja/pages/risk/articles/cr/reshaping-the-cybersecurity.html
- ITR, "Japan IT Budget & Spending Trends 2021," https://enterprisezine.jp/article/detail/12656l
- Carnegie Mellon University, "Structuring the Chief Information Security Officer Organization," https://resources.sei.cmu.edu/asset files/TechnicalNote/2015 004 001 446198.pdf



[Inquiries about this study]
Kenji Uesugi, senior fellow: uesugi@j-cic.com