BOJ Reports & Research Papers

Financial System Report Annex Series

Financial System Report – Annex

Results of the Cybersecurity Self-Assessment for Regional Financial Institutions (FY2022)

Financial System and Bank Examination Department, Bank of Japan
Strategy Development and Management Bureau, Financial Services Agency

October 2023

Examination Planning Division,
Financial System and Bank Examination Department, Bank of Japan
csrbcm@boj.or.jp

Background

The Bank of Japan's *Financial System Report* has two main objectives: to assess the stability of Japan's financial system from a macroprudential perspective and to communicate with all relevant parties on any tasks and challenges ahead in order to ensure the system's stability.

The *Financial System Report* provides a comprehensive assessment of the financial system twice a year and is occasionally supplemented by *Financial System Report Annex Series* papers, which provide more detailed analyses and insights on specific topics. Based on the results of the cybersecurity self-assessment (CSSA), which the BOJ and the Financial Services Agency (FSA) jointly conducted for regional financial institutions for the first time in fiscal 2022, this paper introduces the overview of cybersecurity management frameworks of regional financial institutions as a whole and key points for further strengthening relevant frameworks.

Abstract

With cyberattacks increasing, the development of cybersecurity management frameworks and ensuring of their effectiveness have come to be recognized as significant challenges. Against this background, the BOJ and the FSA developed a tool for conducting a self-assessment of cybersecurity management frameworks, with which individual financial institutions are to identify their own positions in comparison with other financial institutions and also identify areas of their own challenges. The BOJ and the FSA requested regional financial institutions (99 regional banks, 254 *shinkin* banks, and 145 *shinkumi* banks) to conduct cybersecurity self-assessment using the tool for the first time and then fed back the overall results to them.

The results found that many of the regional financial institutions consider ensuring cybersecurity to be an important management issue and are making efforts to enhance the effectiveness of their cybersecurity controls, such as conducting exercises based on contingency plans, in addition to developing relevant frameworks and taking technological controls. On the other hand, the results also found that they have challenges in securing and fostering cybersecurity human resources and managing third-party risks.

The BOJ and the FSA expect that regional financial institutions will fully utilize CSSA in their efforts for further strengthening their cybersecurity management frameworks, and will support those efforts through conducting inspections/examinations, monitoring and various seminars.

I. Cybersecurity Self-Assessment (CSSA)

1. Background

In the recent environment surrounding financial institutions in Japan, moves to promote operational reforms, such as the introduction of remote working[1] and utilization of cloud services,[2] are progressing, in addition to the enhancement of customer services including the development of applications for mobile terminals[3] and the collaboration with companies of different business types such as FinTech companies, through the use of digital technologies. On the other hand, in cyberspace, complicated and skillful ransomware attacks as well as other organized and sophisticated cyberattacks are increasing, and thus the threat of cyberattacks is growing. Accordingly, for financial institutions continuing making efforts for improving customer services and operational efficiency by the use of digital technologies, developing cybersecurity management frameworks and securing their effectiveness are significant challenges in consideration of the growing threat of cyberattacks.

2. Objectives of CSSA

When checking the status of cybersecurity management, large financial institutions in Japan conduct maturity assessments using an international framework,[4] but regional financial institutions have not necessarily broadly used such a tool to identify their own positions in comparison with other financial institutions and areas of their own challenges. Against this background, the BOJ and the FSA developed a self-assessment tool (a Check Sheet) for regional financial institutions and conducted cybersecurity self-assessment (CSSA) for the first time in fiscal 2022. More specifically, the BOJ and the FSA requested regional financial institutions to assess their own cybersecurity management frameworks based on the CSSA Check Sheet and fed back the overall results to them. Individual regional financial institutions are expected to understand their own problems based on self-assessments and endeavor to further strengthen their cybersecurity controls on a voluntary basis.

---

[1] For the status of the introduction of remote working by financial institutions, see "Expansion of Remote Working, and System and Security Problems at Financial Institutions – Results of the Questionnaire Survey –," *Financial System Report Annex Series*, October 2020 (available only in Japanese).

[2] For the status of the utilization of cloud services by financial institutions, see "Key Considerations for Risk Management in Using Cloud Services," *Financial System Report Annex Series*, November 2020.

[3] For the status of the provision of applications for mobile terminals by financial institution, see "Status of Financial Institutions' Provision of Mobile Apps and Management frameworks – Results of the Questionnaire Survey –," Financial System Report Annex Series, November 2022 (available only in Japanese).

[4] For example, some large financial institutions use the Cybersecurity Assessment Tool (CAT) developed by the Federal Financial Institutions Examination Council (FFIEC).

3. Covered Financial Institutions

The CSSA covered regional financial institutions (99 regional banks, 254 *shinkin* banks, and 145 *shinkumi* banks).[5] The CSSA is envisaged to be conducted annually in and after fiscal 2023, while updating the questions in light of environmental changes and also considering expanding the coverage of the CSSA to other types of financial institutions, such as insurance companies and securities companies.

4. Outline of the CSSA Check Sheet

The BOJ and the FSA prepared the CSSA Check Sheet with the cooperation of the Center for Financial Industry Information Systems (FISC).

Questions in the Check Sheet was developed with reference to key cybersecurity risk management frameworks including the Cybersecurity Framework (CSF) of the National Institute of Standards and Technology (NIST) (see BOX1 below for the five functions of the NIST CSF) as well as questions of questionnaire surveys [6], with the aim to structure the CSSA in a way that enables financial institutions to comprehensively assess their organizations' cybersecurity management frameworks. Each question was developed in light of the sizes and characteristics of regional financial institutions operating mainly in specific areas in Japan, and in consideration of changes in system environments, such as the expansion of the use of the remote access system and cloud services, as well as the recent trend of the threat of cyberattacks, including the increase in ransomware attacks. It should be noted that the Check Sheet was designed to encourage regional financial institutions to voluntarily strengthen their cybersecurity controls based on their own self-assessments, and does not represent the views of the BOJ or FSA regarding best practices or minimum standards.

Main points of the questions in the Check Sheet are summarized as follows (Chart 1; See the Appendix for the Check Sheet itself).

---

[5] Self-assessments for financial institutions were conducted from July to August 2022, and the overall results were returned in November 2022.

[6] Specifically, the "FISC Security Guidelines on Computer Systems for Financial Institutions," which are utilized by financial institutions in Japan, the "CRI Profile," which is the framework for assessing cyber risk managed and updated by The Cyber Risk Institute (CRI), the "Questionnaire Survey on Cybersecurity for financial institutions (2019)" conducted by the BOJ, and the "FY2022 Questionnaire Survey for financial Institution " conducted by the FISC were referred to.

Chart 1. Main points of the questions in the CSSA Check Sheet

Item	Number of questions	Points
Involvement of executives concerning cybersecurity	4	Management policy and management plan concerning cybersecurity, and periodic reports and ad-hoc reports to executives, etc.
Identifying and responding to risk concerning cybersecurity	4	Sources of Information on cybersecurity, risk assessment, decision of policies for responding to risks, etc.
Audit concerning cybersecurity	3	Audit subjects, where to report audit results, and confirmation of the status of improvements made for matters pointed out
Education and training concerning cybersecurity	1	Status of calling attention to and providing education and training concerning cybersecurity
Evaluation of new digital technologies	2	Organizational structure for assessing risks upon introduction of new digital technologies, etc.
Asset management	3	Status of maintenance of a system management register of hardware and software, etc.
Access control	2	Status of management of rights to access material systems and control of remote access, etc.
Data protection	2	Measures for data protection (encryption) and destruction of backup data, etc.
Log Management	1	Log management policies for material systems
vulnerability management	4	Status of conducting vulnerability assessments and penetration testing, policies for applying a patch, etc.
Technical measures against cyberattacks	3	Technical measures for terminals, borders, and website and internet banking systems
Detection	2	Status of conducting monitoring and analysis, etc., and monitoring targets
Incident response and recovery	6	Arrangement of staff for making responses upon a cyber incident, rules and procedures for responses, etc.
Management of third parties	5	Status of management of third parties, security measures for cloud services, etc.
Total	42	(includes 3 questions common to the FISC questionnaire survey)

Based on the results of cybersecurity self-assessments against the Check Sheet, the following sections introduce the overview of the status of cybersecurity management frameworks of regional financial institutions as a whole and key points to further strengthen such frameworks. As the results of self-assessments contain a great deal of technological information about the cybersecurity controls of regional financial institutions, this report pays attention to ensure their security in disclosing the results.

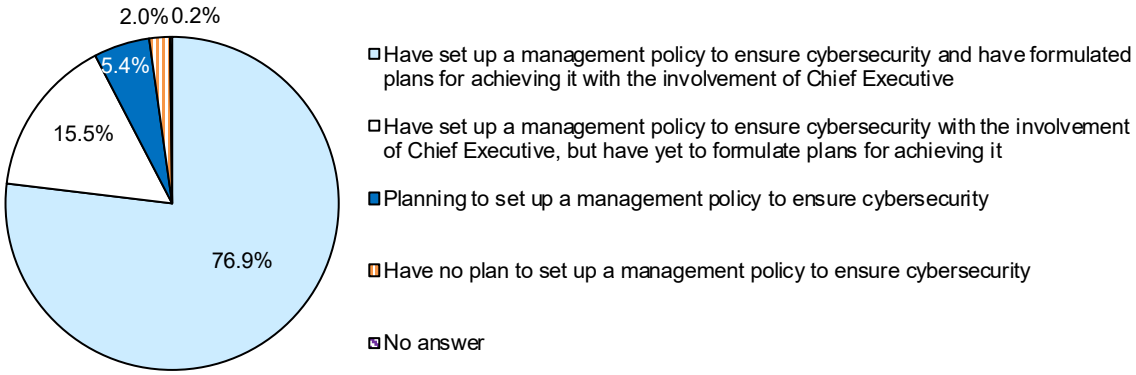
II. Overview of the Results of the CSSA

1. Involvement of Executives

Establishment of management policy and frameworks for its implementation

In promoting a digitalization strategy to enhance customer services and promote operational reforms, it is important to develop cybersecurity management frameworks in accordance with that strategy by formulating concrete plans including how to allocate management resources and to implement those frameworks in a planned manner with the involvement of Chief Executive. Regarding the status of the formulation of management policies and plans concerning cybersecurity, almost 80% of the respondents answered that they have set up a management policy to ensure cybersecurity and have formulated plans for achieving it with the involvement of Chief Executive (Chart 2).

Chart 2. Management policies and plans concerning cybersecurity



Next, more than 90% of the respondents answered that one of their executives was in charge of cybersecurity of the organization (for a governance model of cybersecurity, see BOX2 below). Approximately 80% of such executives[7] are those who administer IT system risks (CIOs[8]). Financial institutions that appoint an officer who is solely in charge of cybersecurity (CISO[9]): which is observed in some major banks, are less than 7% (Chart 3).

As for the contents of periodical reporting to executives regarding cybersecurity, the results find that a large number of respondents reported to executives cyber incidents that had occurred within

[7] In this report, executive officers and other employees with senior positions are all included in the category of "executives" for convenience.

[8] Abbreviation of Chief Information Officer

[9] Abbreviation of Chief Information Security Officer

the organization and the state of progress of cybersecurity controls, whereas fewer respondents referred to incidents of other companies in reporting to executives(Chart 4). It is important to report a broad range of information on recent trends of threat of cyberattacks including cases of other companies, to executives and check the status of the organization's own controls. Cases of other companies are available free of charge from industry associations and public offices in addition to media information.

Chart 3. Personnel in charge of cybersecurity

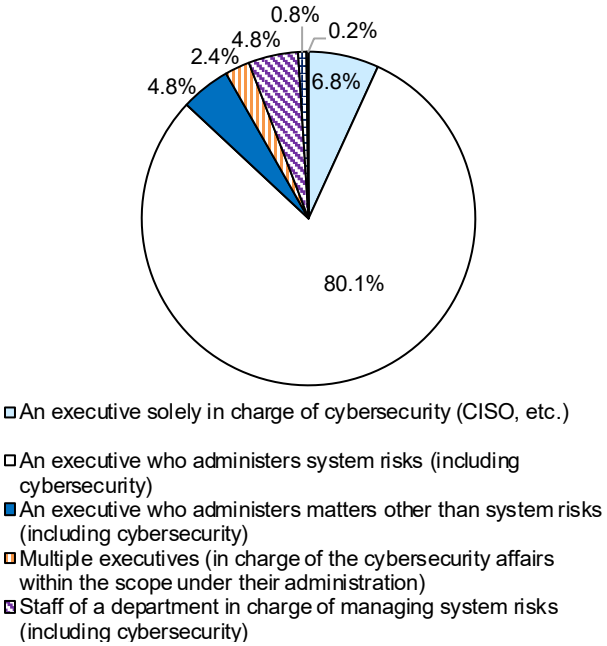
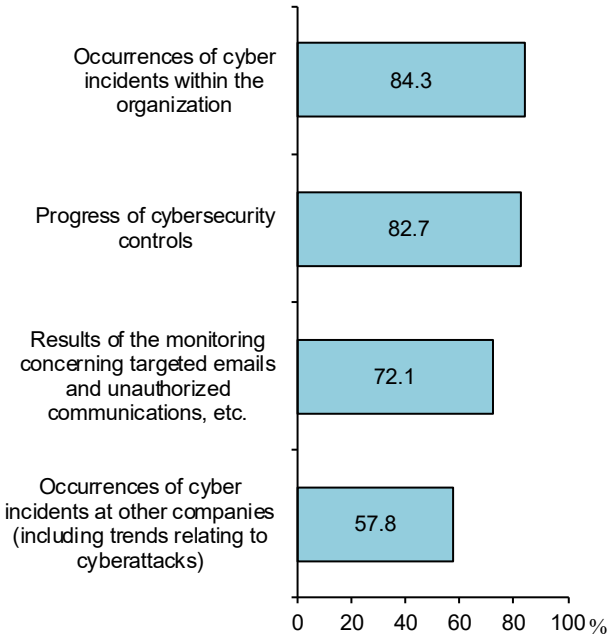


Chart 4. Contents periodically reported to executives regarding cybersecurity



Risk assessment concerning cybersecurity

It is important for financial institutions to conduct a risk assessment concerning cybersecurity with regard to material systems[10] in an appropriate manner on a timely basis. Many of the respondents conduct risk assessments regularly and/or when introducing a new system and/or conducting a large-scale renewal (Chart 5).

It is important that decisions concerning responses to risks (reduction, avoidance, transfer, or acceptance of risks) and prioritization in response policies based on risk assessments are made organizationally with the involvement of executives. Many of the respondents answered that decisions are made by the IT system risk management department or the department in charge of systems, whereas only over 40% of the respondents answered that executives make decisions

[10]For the current CSSA, "material systems" are defined as "accounting systems, systems handling customer information, or other systems that an organization recognizes as especially important in its business operations."

(Chart 6).

Chart 5. Status of conducting risk assessments concerning cybersecurity of material systems

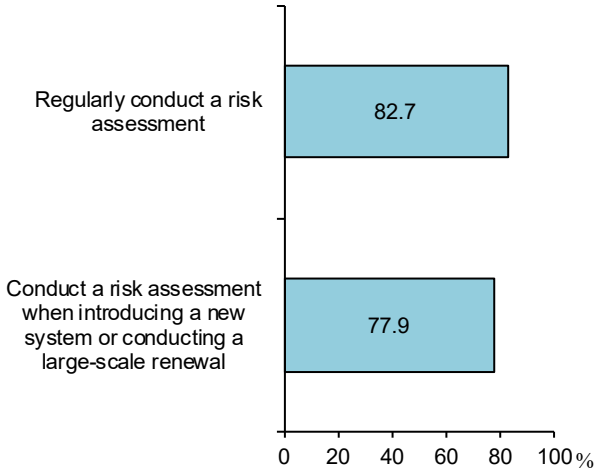
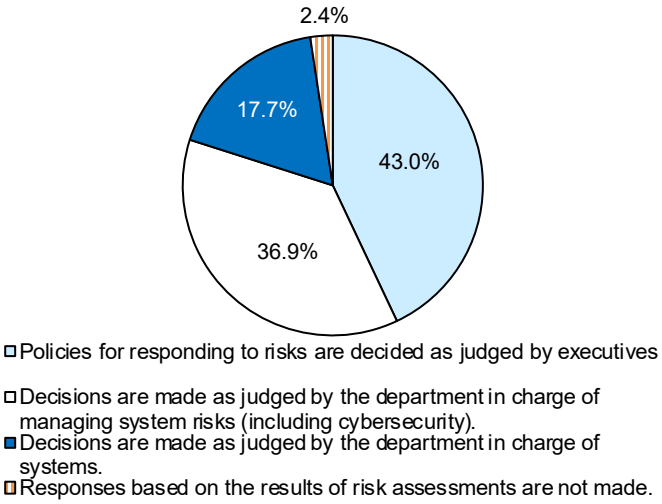


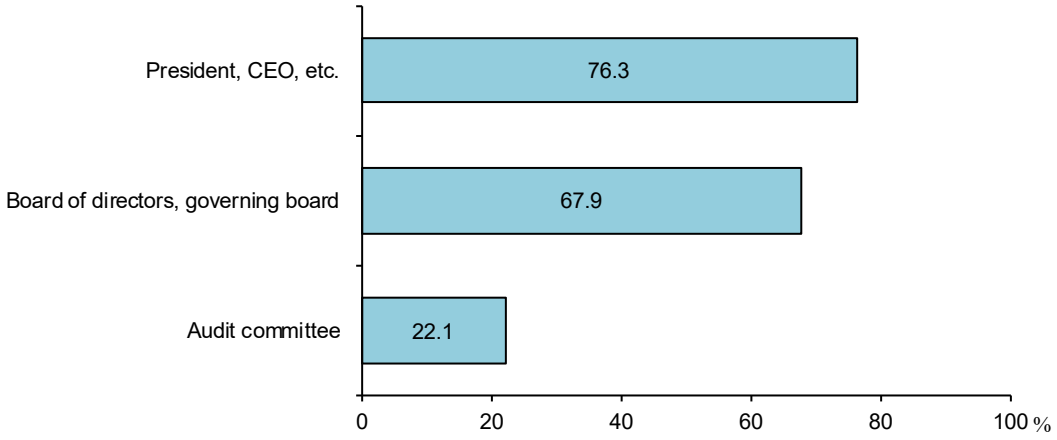
Chart 6. Decision maker for response policies based on risk assessments



Audit concerning cybersecurity

The results of an audit concerning cybersecurity are mostly reported to executives (Chart 7). Considering that a cyber risk is one of the significant issues on business for financial institutions, it is not sufficient that executives are only informed of audit results. It is important for the audit department to fulfill its function as the third line of defense including through confirming the status of the implementation by audited departments of remedial controls for the matters pointed out in an audit.

Chart 7. Where to report the results of an audit concerning cybersecurity



Frameworks for securing cybersecurity human resources

In enhancing customer services and promoting operational reforms by use of digital technologies, it is also important to secure human resources who can assess and manage associated cybersecurity risks. Looking at the status of securing such human resources, over 70% of the respondents answered that they have not sufficiently secured personnel (Chart 8).

Acknowledging the shortage of cybersecurity human resources, financial institutions have been making multiple efforts for strengthening their organizational frameworks by means such as utilizing outside professionals, in addition to fostering internal staff. Regarding the staff targeted for e-learning for raising awareness concerning cybersecurity (including learning using videos and documents), which is one of the controls for fostering and strengthening human resources, while over 80% of the regional financial institutions covered staff of the department in charge of systems, only around 60% to 70% of them targeted executives or other staff (Chart 9). It is encouraged that each financial institutions will provide training to executives and broader range of staff, such as those in the operation department, public relations department and other departments: not limited to those in the department in charge of systems, thereby fostering cybersecurity human resources and bottoming up knowledge on an organization-wide basis.

Chart 8. Status of securing human resources who can assess cybersecurity risks that may arise as a result of introducing new digital technologies

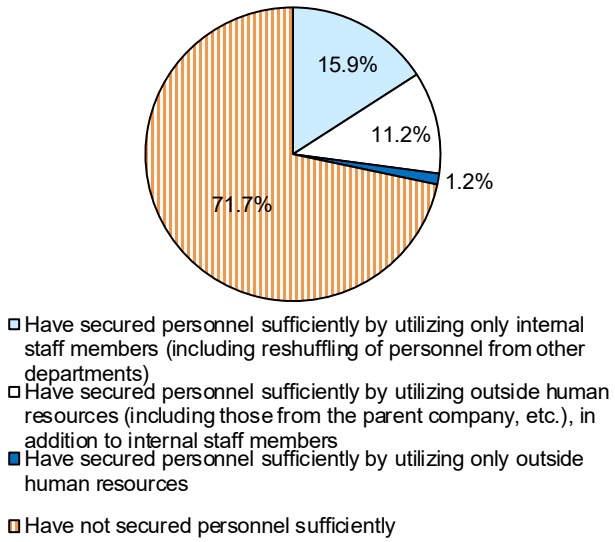
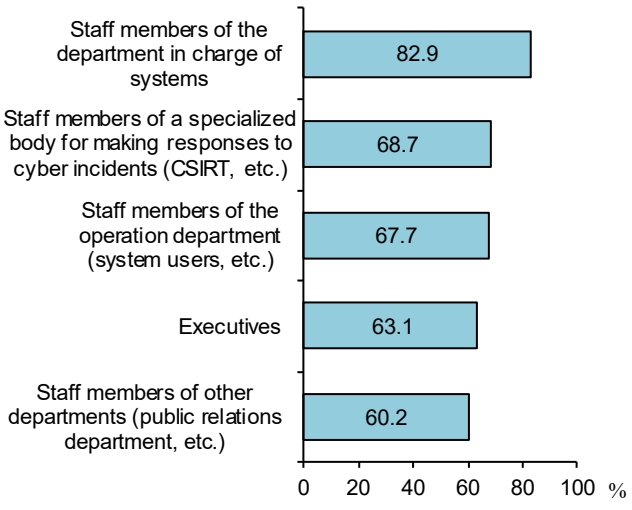


Chart 9. Staff targeted for e-learning (including learning using videos and documents, etc.) for awareness-raising

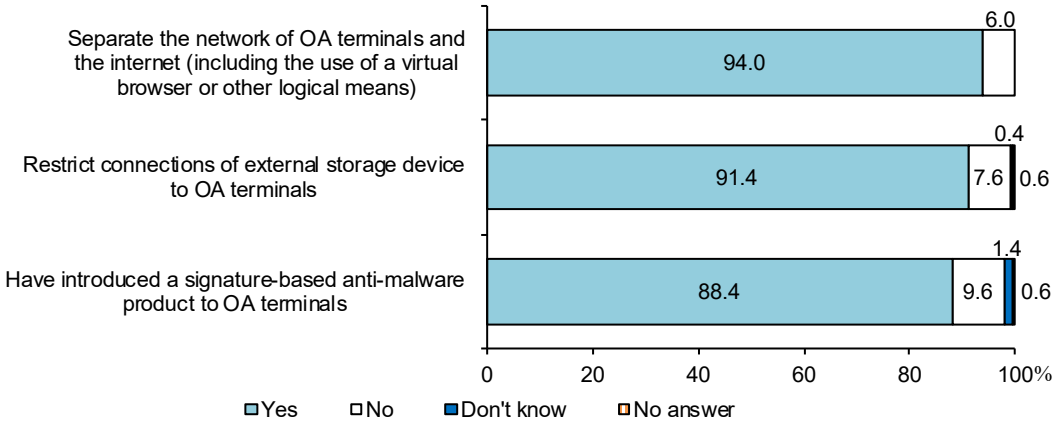


2. Readiness for cyber risks

Technical controls against cyberattacks

As controls against cyberattacks taken for OA terminals,[11] separation of the network from the internet, restriction of connections of external storage device, and introduction of signature-based anti-malware products have been progressed (Chart 10). When financial institutions intend to further promote digitalization, they need to enhance their cybersecurity controls according to new risks, keeping an eye on changes in trends of cyber threats.

Chart 10. Controls against cyberattacks taken for OA terminals



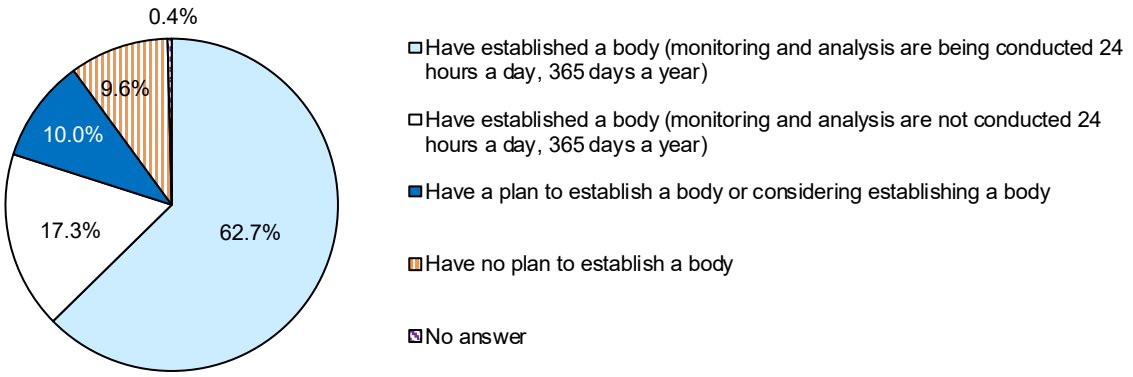
Frameworks for monitoring and analyzing cyber incidents

In order to detect a cyber incident at an early stage and make responses promptly, it is important to establish a body that monitors and analyzes cybersecurity-related issues (SOC[12]). Nearly 80% of the respondents answered that they have established such a body. Over 60% of the respondents indicated that the relevant body monitors and responds to incidents on a constant basis (Chart 11). It is encouraged that financial institutions will make further efforts for early detection and responses, including 24/7 operation.

[11]For the current CSSA, "OA terminals" are defined as "standard terminals that staff members normally use for preparing documents, etc."

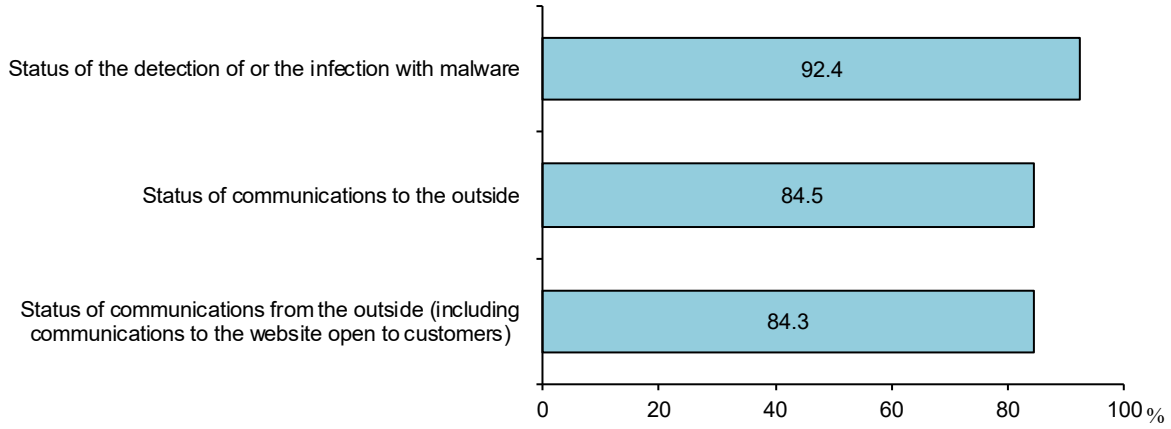
[12]Abbreviation of Security Operation Center. It is a body in charge of monitoring and analyzing cybersecurity-related issues, such as the status of attacks to the network or equipment, including a server and a firewall.

Chart 11. Status of establishing a body that conducts monitoring and analysis of cybersecurity-related issues (including outsourcing)



As for the coverage of monitoring by an SOC or other department that monitors cybersecurity-related issues, over 80% of the respondents answered that the relevant body monitors and analyzes the status of the detection of or infection by malware and the status of communications to the outside (Chart 12). Financial institutions are encouraged to expand the coverage of systems under monitoring and further enhance their quality.

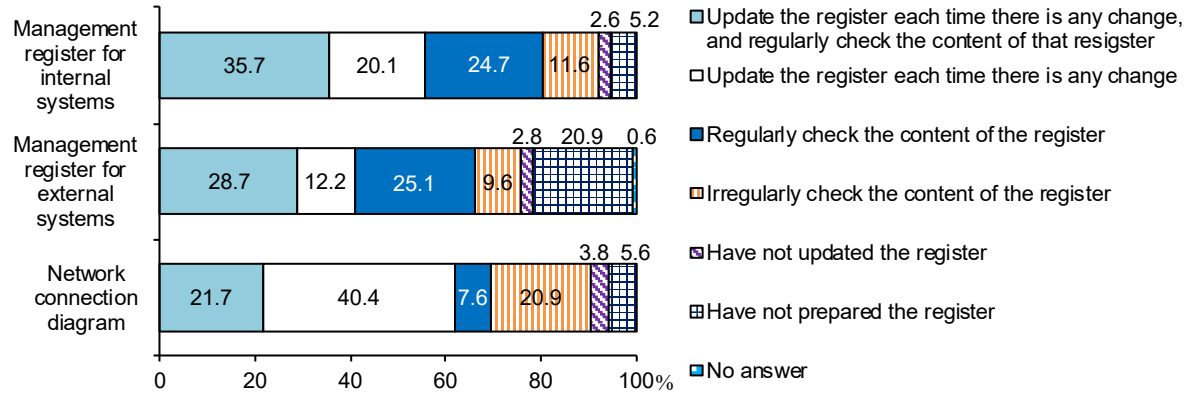
Chart 12. Coverage of monitoring by an SOC or other department that monitors cybersecurity-related issues



Management of system-related assets and controls against vulnerability

Attacks taking advantage of the vulnerability of OS or software of systems are often observed as a cause of cyber incidents. First of all, looking at how a register for managing systems is maintained, from the perspective of whether financial institutions' management of their system-related assets is appropriate, it was found that the frequency of updating and checking external systems[13] is lower than that for internal systems[14] (Chart 13). It is important for financial institutions to consider systems for providing services to customers or storing material internal information as their own systems even if they are external, and thereby develop and keep updating a register for managing the systems to make it possible to check their vulnerability and manage maintenance contracts promptly and accurately.

Chart 13. Status of maintaining a management register, etc. for systems



As there may be cases where a new vulnerability is found, it is important to conduct a vulnerability assessment not only at the time of introducing a new system but regularly thereafter. Many of the respondents answered that they are conducting a vulnerability assessment regularly even after introducing a system (Chart 14). In addition to vulnerability assessments, financial institutions that have developed and established their own detection and monitoring frameworks also need to conduct a penetration testing[15] and a threat-based penetration testing to check the effectiveness of their detection and monitoring frameworks from an objective viewpoint.

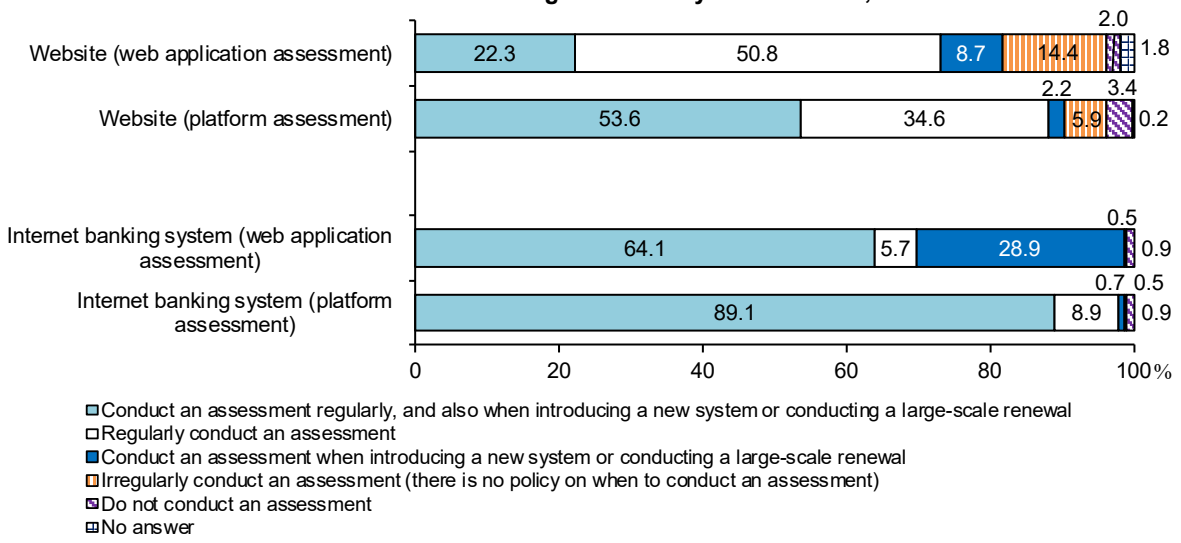
---

[13]For the current CSSA, "external systems" are defined as "systems operated outside the own organization (including cloud services)."

[14]For the current CSSA, "internal systems" are defined as "systems operated within the own organization."

[15]For the current CSSA, a "penetration testing" is defined as a "test for checking whether penetration or falsification is possible and whether any attack can be detected and for verifying the promptness and appropriateness of responses by launching simulated attacks by means such as using simulated malware or abusing a vulnerability or a defect in settings."

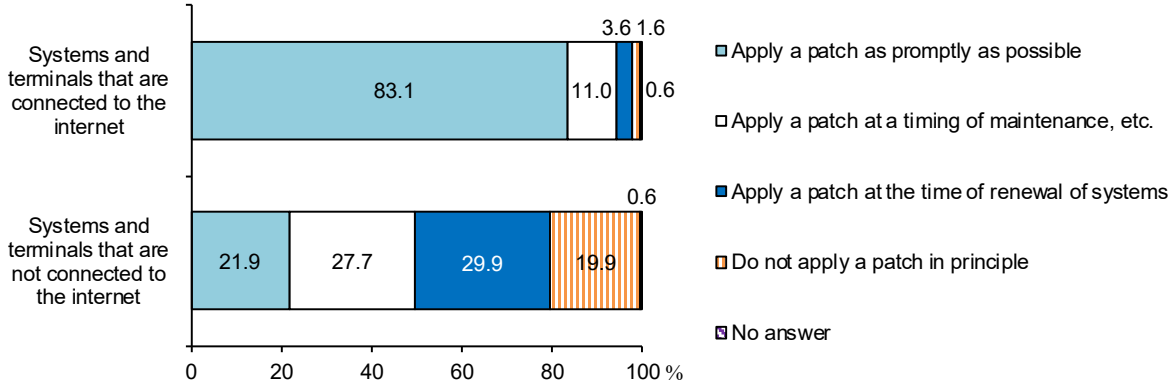
Chart 14. Status of conducting vulnerability assessments, etc.



Note: Answers that they conduct an assessment includes cases where they outsource system operations and check the outsourcees' implementation of an assessment, etc.

Furthermore, when any serious vulnerability is found in the organization's own system, it is important to promptly apply a security patch (vulnerability remediation program). Regarding policies for applying a patch in such cases, over 80% of the respondents answered that they apply a patch as promptly as possible for systems that are connected to the Internet, whereas nearly 50% of the respondents indicated that they apply a patch only when renewing a system or do not apply a patch in principle when it comes to systems that are not connected to the Internet (Chart 15). In general, it is important to take a risk-based approach in making responses in consideration of the possibility of being attacked. In particular, it is important for financial institutions to consider the necessity of applying a patch instead of placing too much trust in a closed network in light of recent cases of cyber incidents.

Chart 15. Policies for applying a patch when serious vulnerability is found

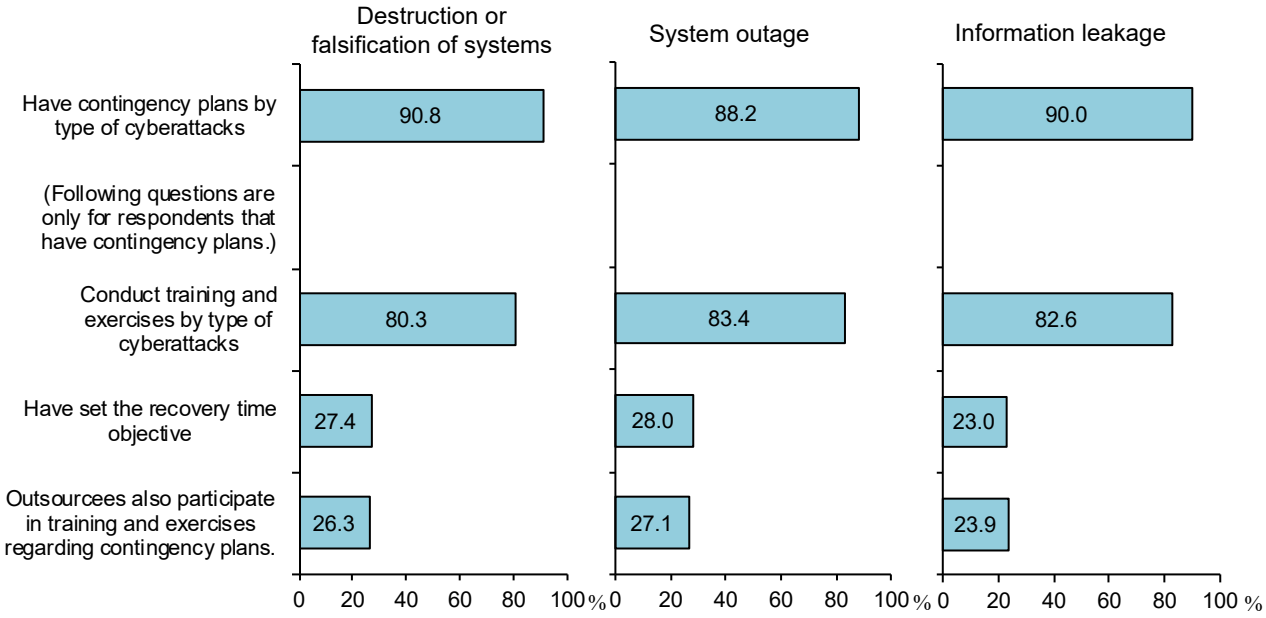


3. Preparations for Contingencies

Formulation of contingency plans and implementation of training and exercises

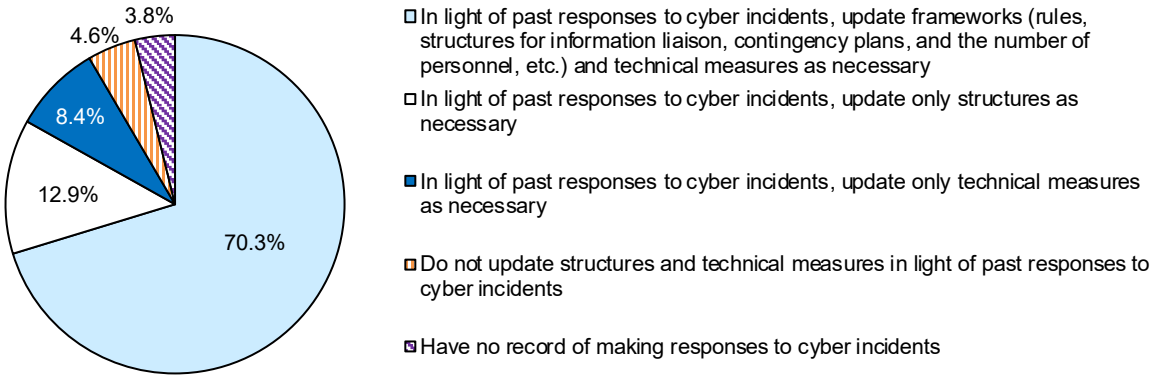
It is important to envisage a case where a cyber risk becomes a reality and be ready to take controls for prompt recovery. Most of the respondents have formulated plans by type of cyberattacks (damage) (Chart 16). Going forward, it is important for financial institutions to set a recovery time objective depending on the impact on business operations and endeavor to further enhance the effectiveness of their contingency plans by such means as developing contingency plans with the assumption of cyberattacks made to their outsourcees and other important third parties and conducting exercises (see BOX3 below for controls against destruction or falsification of backup data that are important regarding conducting recovery work).

Chart 16. Contingency plans against cyberattacks (damage) and concrete controls



Additionally, in light of past responses to cyber incidents and training and exercises actually conducted, it is important for financial institutions to review their relevant frameworks, such as rules relating to responses to incidents, frameworks for information liaison, contingency plans, and the number of personnel, and endeavor to enhance the effectiveness of those frameworks. Most of the respondents answered that they use their past performances to update their frameworks or technical controls (Chart 17).

Chart 17. Status of strengthening frameworks based on past responses to incidents (including training and exercises)



Controls against third-party risks

It is becoming more and more important to manage broad and complicated supply chains that are the backbone of digital business as demonstrated by discussions such as a high-level guidance on third parties released by G7 last year.[16] With regard to the status of managing cybersecurity risks relating to important third parties,[17] over 50% of the respondents answered that their supervisory department centrally oversaw third-party risk management (Chart 18).

With regard to whether cybersecurity-related matters are specified with outsourcees in a contract or in other forms, more than a few respondents answered that: they did not specify the boundaries of responsibilities for cybersecurity controls in outsourced operations or services to be provided; or that they did not appoint personnel responsible for the management of cybersecurity risks (Chart 19). Given that agreements with third parties may often be concluded in line with the counterparties'

[16] For the G7's high-level guidance on third parties, see "G7 Fundamental Elements of Ransomware Resilience and Third Party Cyber Risk Management" (October 2022) on website of the Bank of Japan or the FSA.

[17] For the current CSSA, an "important third party" is defined as a "third party which the organization recognizes as being important for its business operations." A "third party" is defined as "another organization with which the organization has a business relationship or has concluded an agreement, etc. for providing services" (e.g. an information system subsidiary, a vendor or other outsourcee, a cloud service provider or other service provider, or other business partner such as a fund transfer service provider.).

model contracts, it is important to sufficiently confirm the material matters with the counterparties and prepare additional documents as needed to clarify the content.

Chart 18. Status of managing cybersecurity risks for important third parties and services provided thereby

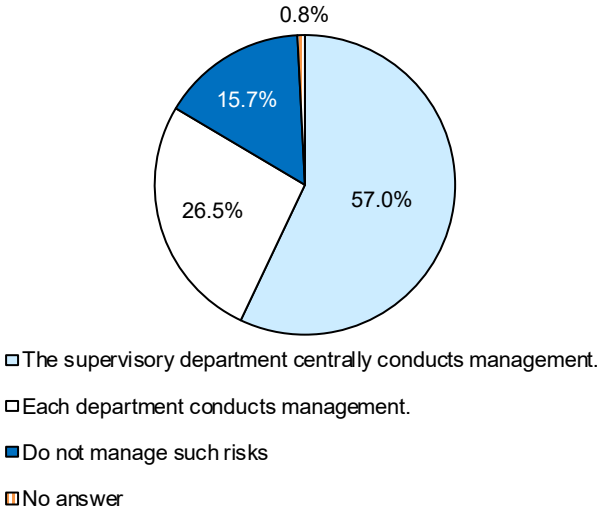
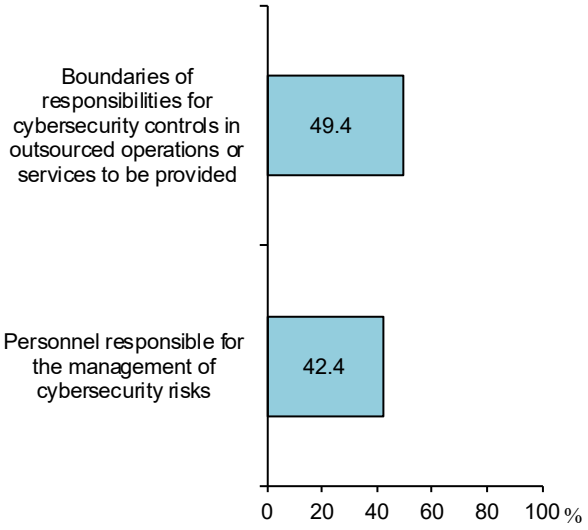


Chart 19. Matters specified in contracts, etc. with outsourcees



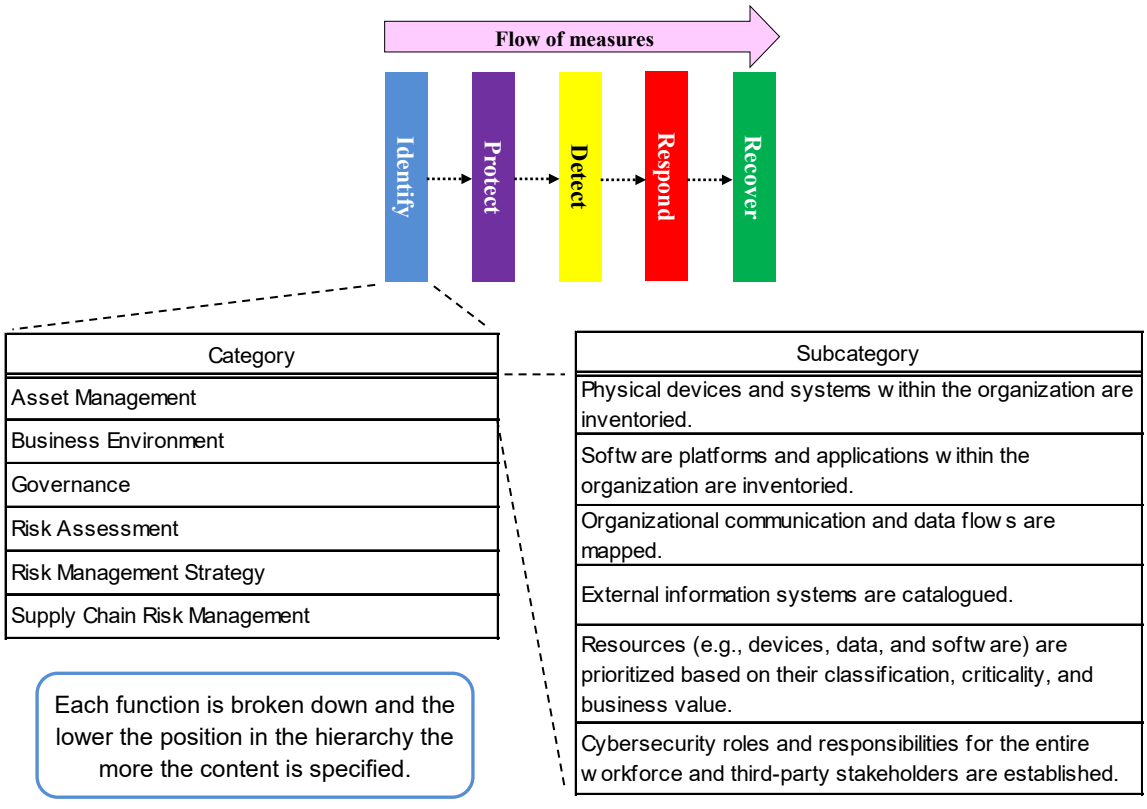
BOX1 Five Functions in the NIST CSF

The NIST CSF is a framework for cybersecurity controls created by the U.S. National Institute of Standards and Technology, which is also referred to in Japan in a wide range of industries including critical infrastructures for the measurement and improvement of an organization's own cybersecurity frameworks

The NIST CSF sorts out matters to be addressed in cybersecurity controls and presents them in an orderly sequence. The top classification consists of the most basic elements called the "five functions" (Chart B1).

Then, each of such functions is broken down into categories and further into subcategories, which makes it useful when considering specific cybersecurity controls to be taken.

Chart B1. Five functions in the NIST CSF



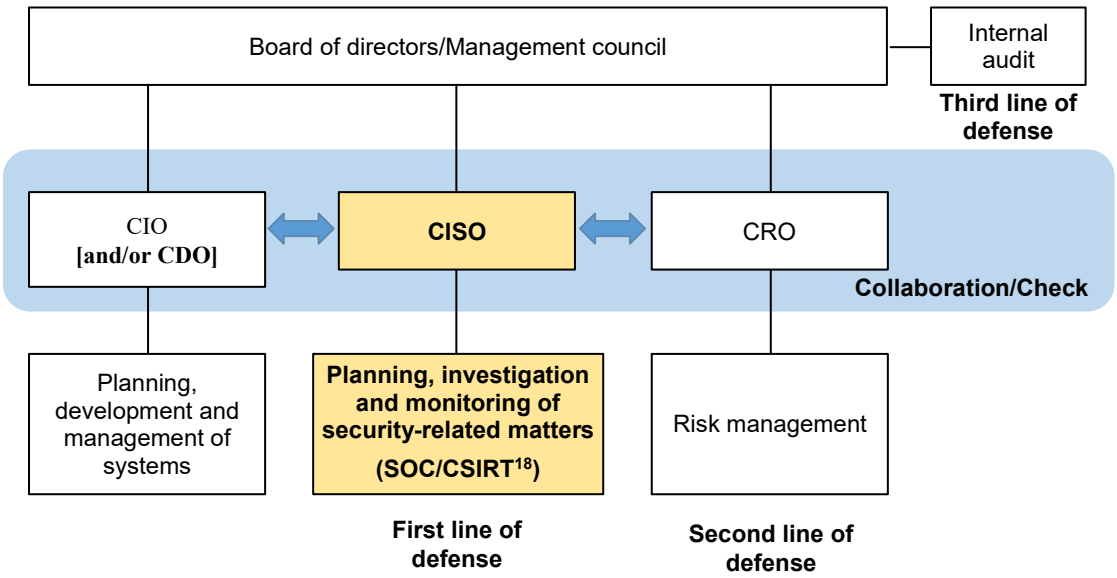
BOX2 Governance Model for Cybersecurity

Conventionally, the Chief Information Officer (CIO) in charge of supervising a system department has been responsible for each organization's framework for managing system risks including cybersecurity. However, in recent years, as the importance of ensuring cybersecurity has been broadly recognized, an increasing number of financial institutions in foreign countries have come to adopt a governance model in which the Chief Information Security Officer (CISO), independent of the CIO, takes charge of the management of cybersecurity risks and various controls. Also in Japan, some major financial institutions have adopted this new governance model (Chart B2).

Additionally, there is also a move to appoint a Chief Digital Officer (CDO) in order to strategically engage in a digital business. From the perspective of well balancing offensive approaches and defensive approaches, the CISO who independently verifies the controls taken by the CDO is becoming increasingly important.

The CISO mainly fulfils functions of planning, investigating, and monitoring cybersecurity-related matters, in which it is important for the CISO to closely collaborate with the CIO, CDO, and Chief Risk Officer (CRO) to share recognition of risks with them and promote the implementation of effective controls. It is important that the CRO as the second line of defense and the internal audit as the third line of defense act as checks and balances against the CISO's activities.

Chart B2. Example of a governance model for cybersecurity management



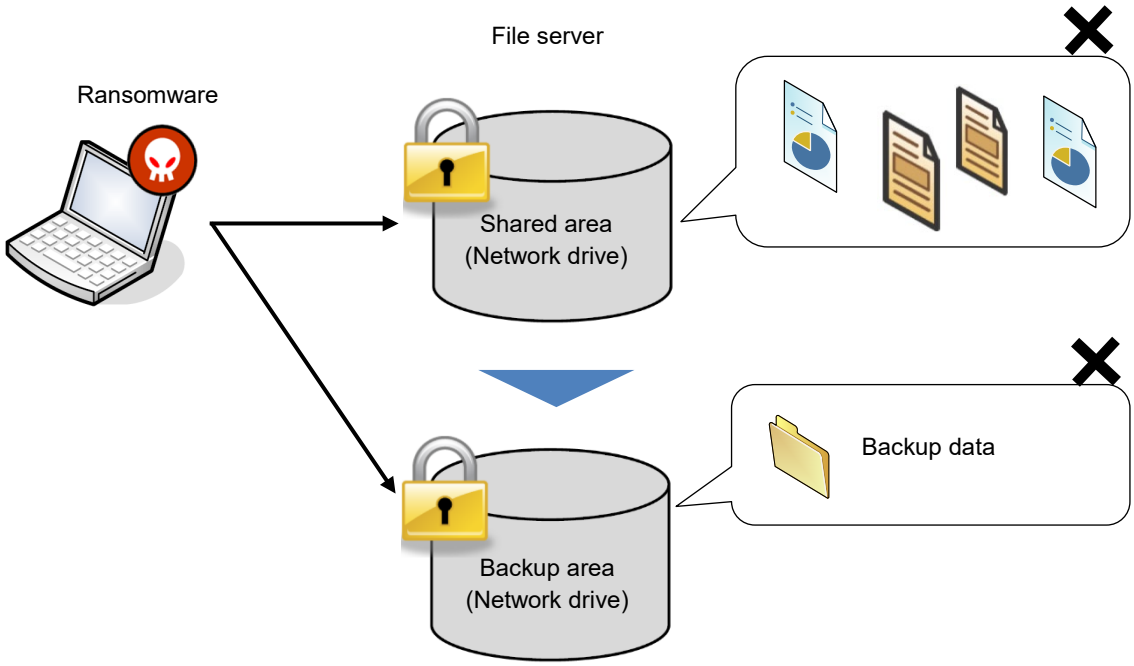
[18]Abbreviation of Computer Security Incident Response Team, which is a body for making responses to cyber incidents.

BOX3 Controls to Prepare for Destruction or Falsification of Backup Data

As a form of attacks leading to damage of destruction or falsification of IT systems, ransomware attacks are increasing in recent years. A ransomware attack is an attack undertaken by encrypting data of a system and demanding ransom in form of crypto-assets or money in exchange for decryption of the encrypted data. One of the effective controls as a preparation for a ransomware attack is to regularly obtain backup data for recovering a system.

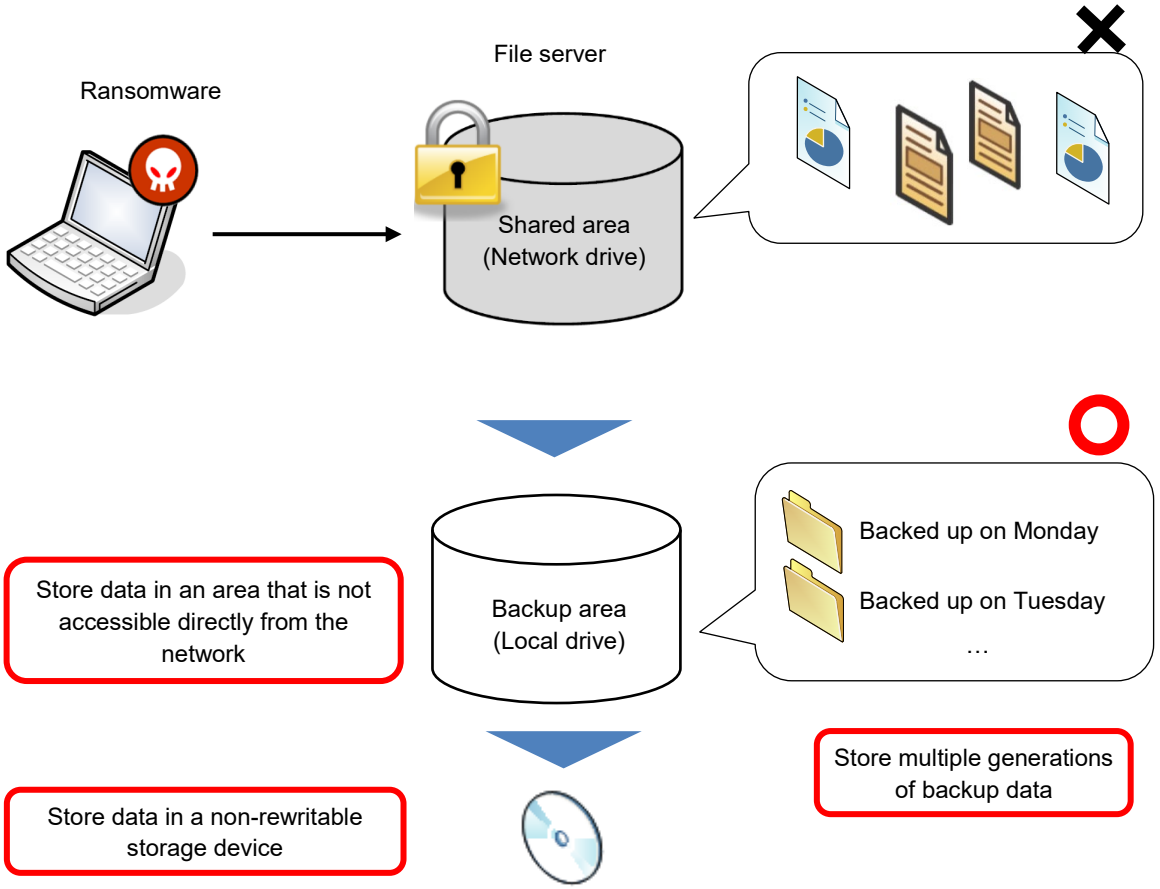
However, there have also been cases where the backup data obtained in advance were also encrypted, which made it difficult to recover the IT system because the area where the obtained data were stored was accessible via the network from a device infected with ransomware(Chart B3-1).

Chart B3-1. Case where backup data may also be encrypted via the network



From the perspective of recovering business operations earlier, controls to prevent destruction and falsification of backup data are important. Technical controls for destruction or falsification of backup data in material systems include storing the data in an area that is not accessible directly from the network and storing the data in a non-rewritable storage device to prevent a damage caused by ransomware attack. Storing multiple generations of backup data is another option to address the risk of the most recent data being encrypted(Chart B3-2). It is important to make preparations appropriately in light of the significance of each IT system and system environments.

Chart B3-2. Storage of backup data to prepare for possible destruction or falsification of backup data due to a ransomware attack.



Furthermore, relevant procedures should be established in advance to ensuring prompt recovery by the use of obtained backup data. It is important to check the feasibility and the time required for recovery through conducting exercises, thereby confirming the effectiveness of the prepared controls.

When actually carrying out recovery work after an attack, the security of the backup data should be confirmed in advance so as to avoid a situation where backup data infected with malware are used for recovery work, rendering the recovered data become encrypted again. In this regard, it is important to scan backup data using anti-malware products. It is also important to develop procedures in advance to confirm the security of the data by such means as testing a recovery in a virtual environment or a development environment in consideration of the possibility that the data may be infected with unknown malware that cannot be detected at the stage of conducting recovery work.

III. Toward the Future

As financial institutions are enhancing customer services and promoting operational reforms by utilizing digital technologies, the threat of cyberattacks is becoming imminent. The threat of cyberattacks faced by each financial institutions varies depending on their businesses, the way in which they utilize digital technologies, and the framework of their IT systems. Therefore, controls required for ensuring cybersecurity are not uniform. Nevertheless, it is important for financial institutions to recognize the growing threat and continue efforts for developing better cybersecurity management frameworks and securing the effectiveness of their controls.

In this regard, it used to be that perimeter defense controls focusing on how to prevent the penetration of malware from the outside at the border were prioritized. However, given that connection with the Internet has increased and that cyberattacks have been more organized and sophisticated along with utilization of digital technologies, there is a recent trend that multi-layered controls, including those for the inside of organizations' own networks, are taken based on the assumption that errors cannot be avoided and that the possibility of penetration of unknown malware cannot be eliminated completely (this idea is also called the "zero trust security model"). In light of such trend, financial institutions are expected to introduce controls using behavior-based anti-malware products (including EDR[19]) and a mechanism of multi-factor authentication, and to promote sophistication of monitoring functions of the SOC, IDs and access rights control as well as controls against vulnerability[20] in a planned manner.

Considering such circumstances, CSSA is envisaged to be conducted annually in and after fiscal 2023, while updating the questions in light of environmental changes.

The BOJ and the FSA expect that regional financial institutions will fully utilize CSSA in their efforts for further strengthening their cybersecurity management frameworks, and will support those efforts through conducting, inspections/examinations, monitoring and various seminars.

[19] Abbreviation of Endpoint Detection and Response. It is a mechanism to detect suspicious behavior of terminals and servers through monitoring and offer support for prompt responses.

[20] Activities to ascertain the vulnerability of systems and the status of conclusion of maintenance service agreements and take controls such as applying the latest patch are also called "cyber hygiene."