BOJ Reports & Research Papers

Financial System Report Annex Series

Financial System Report – Annex

Results of the Cybersecurity Self-Assessment for Regional Financial Institutions (FY2023)

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

December 2024

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 in fiscal 2023, this paper introduces the overview of cybersecurity management posture of regional financial institutions as a whole and key points for further strengthening relevant posture.

Abstract

For financial institutions in Japan, it has become a significant challenge to develop cybersecurity management posture and to ensure their effectiveness, in light of the increasing threat of cyberattacks, in their efforts for improving customer services and operational efficiency by the use of digital technologies. Following fiscal 2022, the BOJ and the FSA conducted the CSSA in fiscal 2023, targeting regional financial institutions (99 regional banks, 254 *shinkin* banks, and 145 *shinkumi* banks).

The results found that many of the regional financial institutions consider ensuring cybersecurity to be an important management issue and are steadily making efforts to enhance the effectiveness of their cybersecurity controls through the introduction of measures concerning both technological and organizational aspects. On the other hand, the results also found that they still 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 the CSSA in their efforts for further strengthening their cybersecurity management posture, and will continue supporting those efforts through conducting inspections/examinations, monitoring and various seminars.

I. Introduction

Financial institutions in Japan are promoting development of new businesses through the use of digital technologies, enhancement of customer services in collaboration with companies of different business types such as FinTech companies, and operational reforms by utilizing cloud services.[1] As a result, they have increasingly come to have contact with cyberspace. 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 posture and securing their effectiveness are significant challenges in consideration of the growing threat of cyberattacks.

Following fiscal 2022,[2] the BOJ and the FSA conducted the cybersecurity self-assessment (CSSA) in fiscal 2023 as well, targeting regional financial institutions. The BOJ and the FSA requested targeted regional financial institutions to assess their own cybersecurity management posture based on the CSSA Check Sheet and fed back the overall results to them.[3] 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.

The CSSA Check Sheet was prepared with reference to domestic and international key cybersecurity risk management frameworks.[4] In consideration of changes in the environment surrounding domestic and overseas financial institutions, the Check Sheet for the previous CSSA was reviewed and updated by adding questions concerning more advanced initiatives as well as taking into account the feedback from regional financial institutions. 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.

---

[1] For the status of the utilization of cloud services, see "Status of and Challenges in Utilization of Cloud Services by Financial Institutions – Results of the Questionnaire Survey –," *Financial System Report Annex Series*, January 2024 (available only in Japanese).

[2] For the status for fiscal 2022, see "Results of the Cybersecurity Self-Assessment for Regional Financial Institutions (FY2022)," *Financial System Report Annex Series*, April 2023.

[3] In fiscal 2023, the CSSA covered 99 regional banks, 254 *shinkin* banks, and 145 *shinkumi* banks (the same as in the previous CSSA). Self-assessments were conducted from July to August 2023. The overall results were fed back to those banks in November 2023. The CSSA in fiscal 2023, which was the second one, also covered other types of financial institutions, such as insurance companies and securities companies (see the FSA's website).

[4] 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), and the "FY2023 Questionnaire Survey for Financial Institution" conducted by the FISC were referred to.

Main points of the questions in the CSSA Check Sheet in fiscal 2023 are as follows. (Chart 1; See the Appendix for the Check Sheet.)

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

Major Classification	Medium Classification	Number of questions	Points
Governance	Involvement of executives concerning cybersecurity	5	Management policy and management plan concerning cybersecurity, and periodic reports and ad-hoc reports to executives, etc.
	Identification and responses to risks concerning cybersecurity	7	Ascertaining of cyberattacks, collection of information, risk assessment, guidelines to refer to, and decisions of policies for risk control, 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
	Securing and fostering cybersecurity human resources	3	Status of securing cybersecurity human resources by function, efforts for securing and training cybersecurity human resources
Identification	Evaluation of digital technologies	1	Status of recognition of threat on cybersecurity upon introduction of digital technologies and countermeasures being taken
	Asset management	4	Status of maintenance of a system management register, status of management of hardware and software, information managed in a register, etc.
Protection	Access control	2	Status of management of rights to access material systems and control of remote access
	Data protection	2	Measures for data protection (encryption, restriction on transmission) and for backup data, etc.
	Measures against threat of illegal remittances and phishing attempts	1	Status of implementation of measures against illegal remittances and phishing attempts
	Zero trust security	1	Status of introduction of a zero trust architecture
	Vulnerability management	6	Status of conducting vulnerability assessments and penetration testing, policies for applying a patch, and criteria for deciding on the application of a patch, etc.
	Technical measures against cyberattacks	5	Technical measures for terminals, borders, website and internet banking systems, and mobile application., and status of introduction of pioneering measures
Detection	Detection of cyber incidents	2	Status of conducting monitoring and analyses, etc., and monitoring targets
	Log management	1	Log management policies for material systems
Responses and recovery	Incident response and recovery	6	Arrangement of staff for making responses upon a cyber incident, rules and procedures for responses, etc.
Related to third parties	Management of third parties	5	Status of management of third parties, security measures for cloud services, etc.
	Total	55	Includes 5 questions common to the FISC questionnaire survey

(Note) Newly added points from the previous CSSA are underlined.

II. Overview of the Results of the CSSA

Based on the results of cybersecurity self-assessments against the Check Sheet, the following sections introduce the overview of the status of cybersecurity management posture of regional financial institutions as a whole and key points to further strengthen such posture. 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.

1. Involvement of Executives

Formulation of management policies and management plans, and roles of personnel in charge of cybersecurity

In promoting a digitalization strategy to enhance customer services and promote operational reforms, it is important for regional financial institutions to formulate and implement concrete plans, including how to allocate management resources, with the involvement of the chief executive, concerning the development of cybersecurity management posture in accordance with their own cyber risks. While most of the respondents answered that they have set up a management policy to ensure cybersecurity with the involvement of the chief executive, it turned out that around 8% of the respondents have not formulated a management policy (Chart 2). In addition, around 15% of the respondents have not formulated management plans concerning cybersecurity (Chart 3). It is important to first set up a management policy and then to formulate concrete plans and implement them.

Chart 2: Formulation of management policies concerning cybersecurity

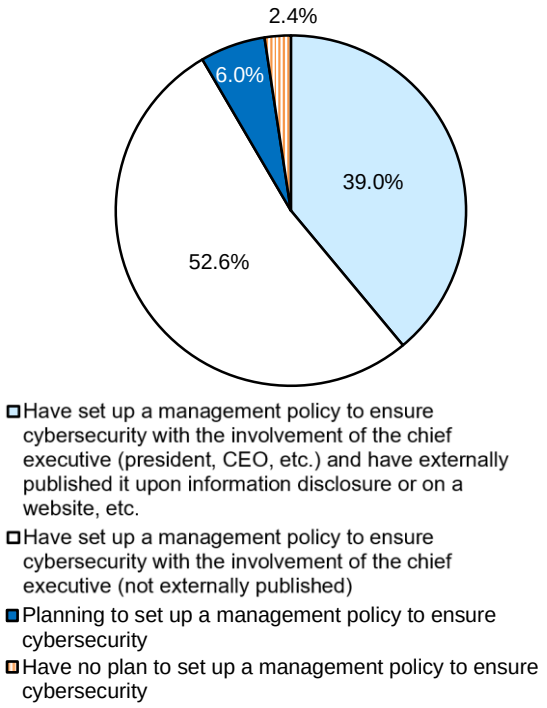
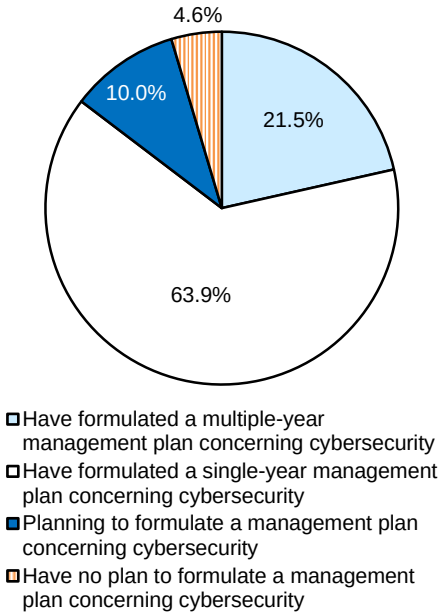


Chart 3: Formulation of management plans concerning cybersecurity



Regarding the responsibility of cybersecurity of the organization, most of the respondents answered that one of their executives is in charge (Chart 4). As for the contents periodically reported to executives regarding cybersecurity, the results show that a large number of respondents reported cyber incidents that had occurred within the organization and the state of progress of cybersecurity control measures. Over 70% of the respondents reported cyber incidents of other companies. While the percentage of those who reported cyber incidents of other companies has improved compared with the results of the previous CSSA, it was smaller than that of the respondents who reported cyber incidents within the organization (Chart 5). It is important to report a broad range of information on recent trends of cyber threats, including other companies' incidents, to executives and review the implementation status of countermeasures of their own organization.

Chart 4: Personnel in charge of cybersecurity

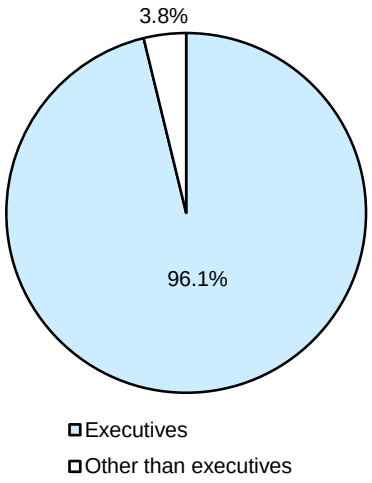
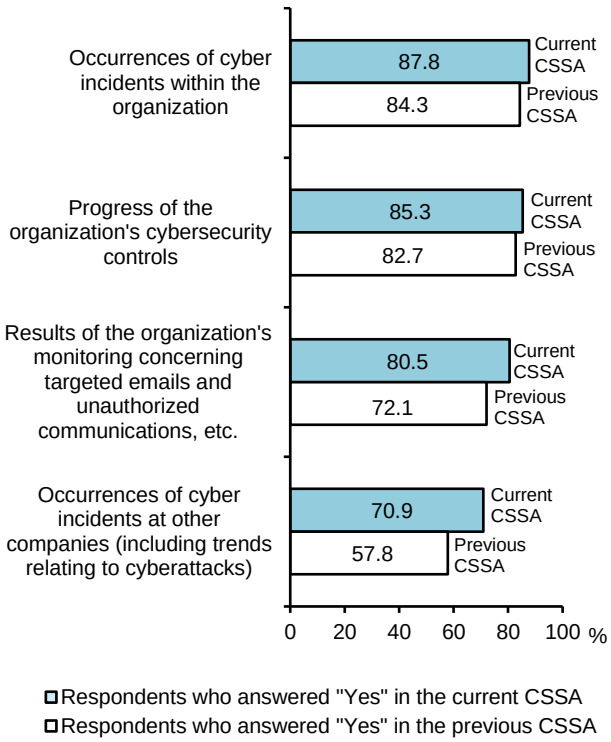


Chart 5: Contents periodically reported to the personnel in charge of cybersecurity



Risk management and involvement of executives

It is important for financial institutions to conduct a risk assessment concerning cybersecurity with regard to material systems[5] that they use, under the initiative of executives. The results have found that nearly 80% of the respondents are conducting risk assessments regularly, and so are over 70% when introducing a new system and/or conducting a large-scale renewal (Chart 6). On the other hand, when it comes to decisions concerning responses to risks (mitigating, avoiding, transferring, or accepting risks) and prioritization in response policies based on risk assessments, just over 40% of the respondents answered that executives make decisions (Chart 7).

[5] For the purpose of this 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: Status of conducting risk assessments concerning cybersecurity of material systems

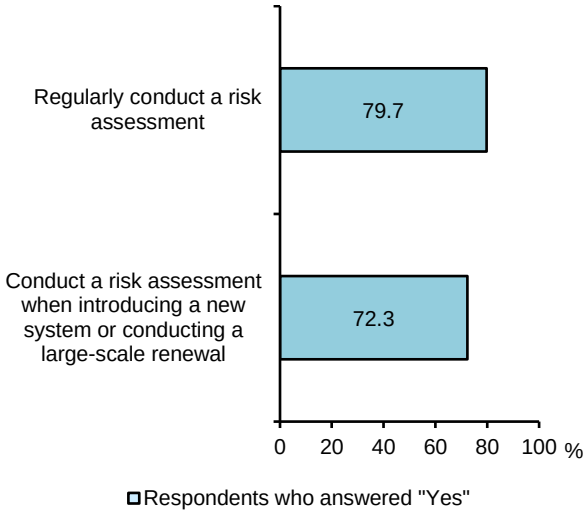
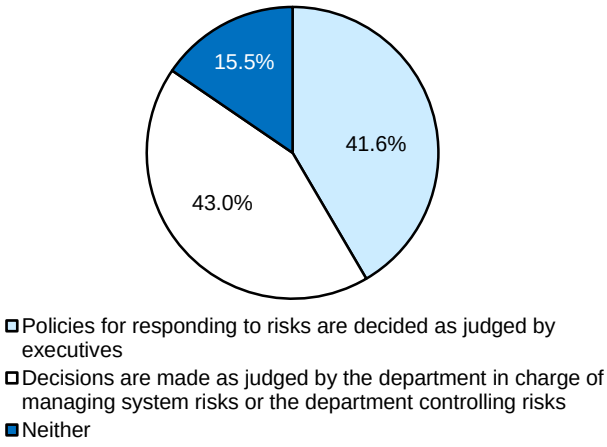


Chart 7: Decision maker for response policies based on risk assessments



When any serious vulnerability is found, a security patch (vulnerability remediation program) should, in principle, be applied promptly. If there is a situation in which a patch cannot be applied, executives might make a decision to accept risks. Looking at policies for applying a patch when a serious vulnerability is found, nearly 90% of the respondents answered that they apply a patch promptly or within a certain period of time for systems that are connected to the Internet, whereas only over 30% do so for systems that are not connected to the Internet (Chart 8). In addition, only over 30% of the respondents answered that decisions not to apply a security patch for a serious vulnerability are made with the involvement of executive officers (Chart 9).

Recently, there are ransomware attacks via a closed network of the organization that are not connected to the Internet, the cause of which is a vulnerability in VPN devices at an affiliated company or an outsourcee. Therefore, it cannot necessarily be said that the organization is free from risks because its network is not connected to the Internet. If a patch for a serious vulnerability is not applied promptly, financial institutions are required to decide on the acceptance of risks with approval of executives.

Chart 8: Policies for applying a patch when a serious vulnerability is found

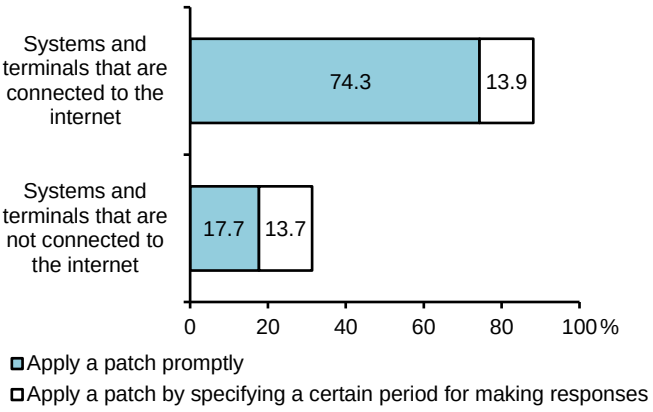
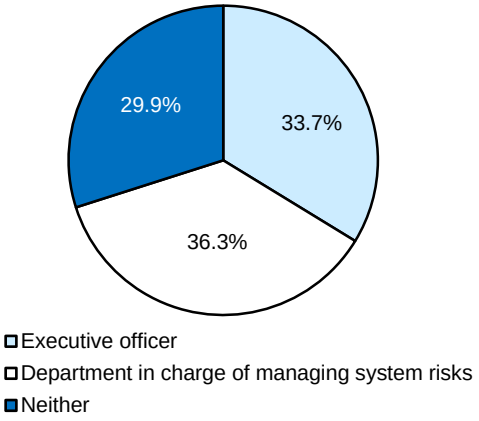


Chart 9: Approver for a decision not to apply a patch for a serious vulnerability



Controls over third-party risks

As supply chains supporting digital business are becoming broader and increasingly complicated, the importance of appropriate management of third parties has been increasing. From the perspective of ensuring consistent management of third parties, cross-organizational actions are preferable. However, looking at the status of management of cybersecurity risks relating to important third parties,[6] only around 60% of the respondents answered that their control department centrally oversees third-party risk management, while 10% or so do not manage third-party risks at all (Chart 10).

Regarding cloud services provided by third parties, the results have found that more than 50% of the respondents are using them. With regard to agreements between service users and cloud service providers, 60% to 70% of the respondents answered that they have agreements concerning a liaison system in the event of a system failure, boundaries of responsibilities, and the handling at the time of terminating cloud services. Meanwhile, only 30% to 40% of the respondents have clarified the location of operational data and the cloud base subject to control (Chart 11). While agreements with cloud service providers may often be concluded according to their own model contracts, it is important to sufficiently confirm substantive matters with the providers and prepare additional documents as needed to clarify the content when intending to use cloud services in material fields of business operations.

[6] For the purpose of this 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 IT 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).

Chart 10: Status of managing cybersecurity risks for important third parties and services provided thereby

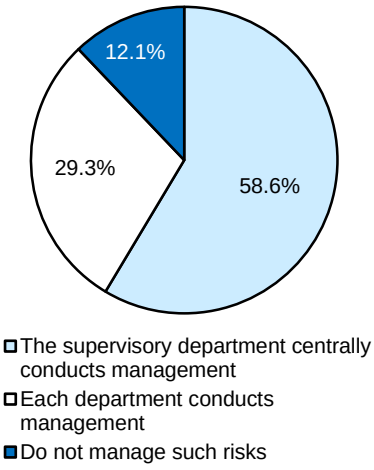
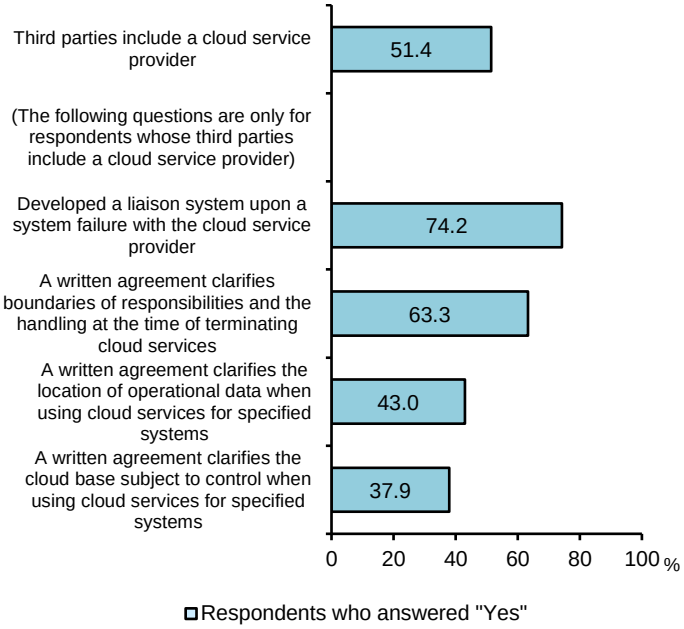


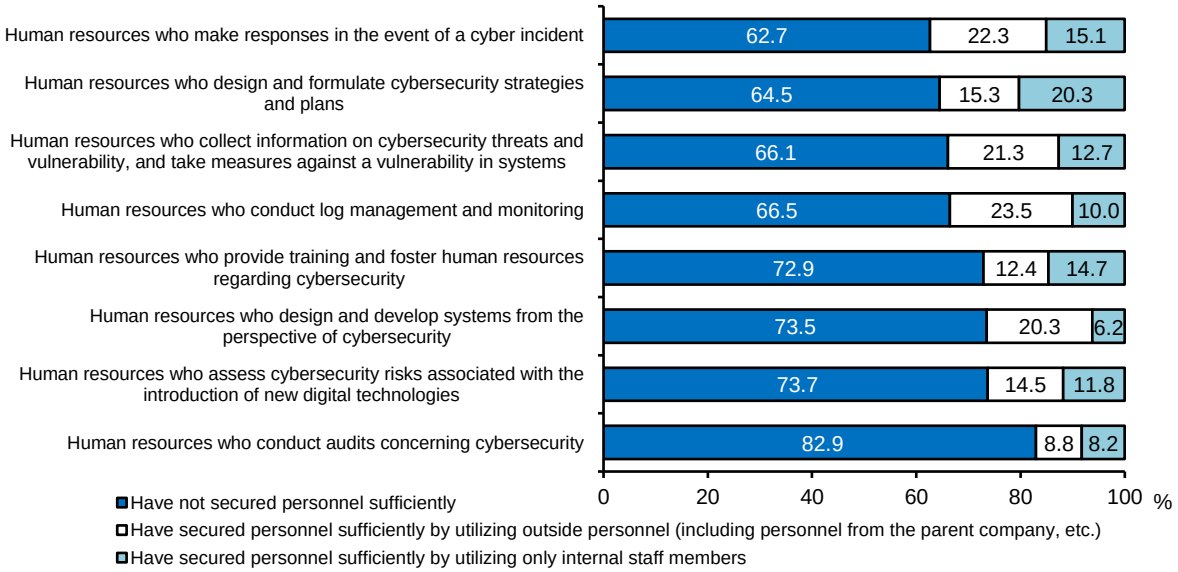
Chart 11: Matters specified in agreements concluded with cloud service providers



Securing cybersecurity human resources

Regarding the status of securing cybersecurity human resources by function, it was found that human resources for material functions for the organization, such as those who make responses in the event of a cyber incident and those who design and plan cybersecurity strategies, are prioritized. It was observed that individual organizations were endeavoring to cover their staff shortages with outside personnel. Meanwhile, most respondents answered that they are suffering an overall labor shortage, and failing to secure sufficient staff for all functions (Chart 12).

Chart 12: Status of securing cybersecurity human resources by function



In order to secure staff members in charge of cybersecurity, more than half of the respondents answered that they are making efforts for human resources development to seek immediate effects, such as encouraging staff members to participate in external training sessions or seminars and holding internal lecture classes and study sessions. On the other hand, those making medium- to long-term efforts, such as implementing personnel rotations with the aim of fostering cybersecurity human resources in longer term and formulating relevant human resources development plans, were limited in number (Chart 13). Considering the possibility that a shortage of cybersecurity human resources will remain unresolved, it is important for financial institutions to make efforts to secure personnel within the organization and to bottom-up their abilities from a medium- to long-term perspective. For this purpose, it would be effective to share information and knowledge concerning cybersecurity measures with other financial institutions, or to work together to collect in-depth information on technical measures and to perform related business operations. Such initiatives based on mutual assistance to enhance personnel's practical capabilities through cross-industrial collaboration and cooperation are desirable.

Efforts for recruiting cybersecurity human resources from outside were weak as a whole (Chart 14). This may be due to the fact that skilled professionals are concentrated in large cities and it is difficult to secure professionals in local areas.

Chart 13: Efforts for fostering human resources

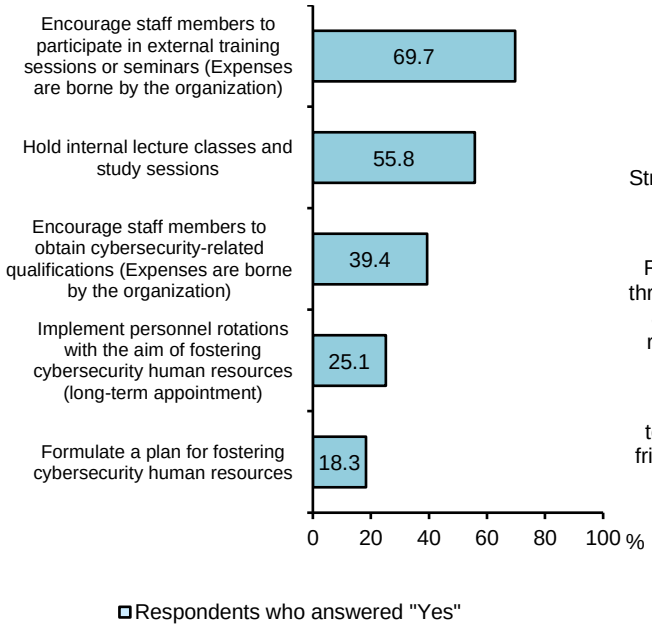
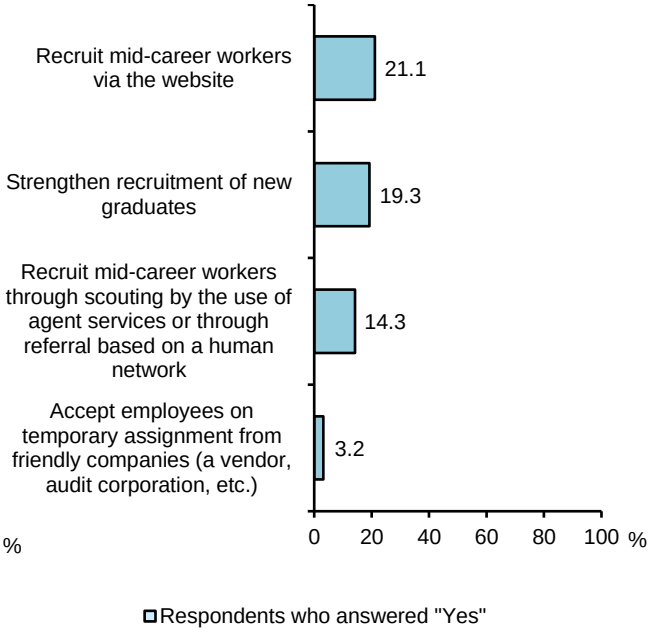


Chart 14: Efforts for recruiting human resources



2. Measures against risks

Zero trust security model

Conventionally, perimeter defense controls focusing on how to prevent the penetration from the outside were prioritized. However, the limitation of perimeter defense controls is now broadly recognized given the increased connection with the Internet, and more organized and sophisticated cyberattacks along with further utilization of digital technologies. It has become important to constantly verify the authenticity of access to the organization's internal environment including those not connected to the Internet in order to protect the organization's information assets (to apply measures based on the so-called zero trust security model) on the premise that the possibility of penetration into the organization's network of unknown malware due to a vulnerability in systems cannot be eliminated completely.

In light of such changes in cybersecurity measures, it has come to recognize the importance of the introduction of a mechanism of multi-factor authentication at the time of accessing terminals and systems, and also the introduction of behavior-based anti-malware products (including EDR[7]), the establishment of a body to conduct cybersecurity-related monitoring and analyses (SOC[8]), and the implementation of threat-led penetration testing[9] (TLPT) so that they can detect and make responses even in the event of internal penetration.

Controls against cyberattacks taken for OA terminals

For OA terminals[10] that often become entry points for cyberattacks, 80% to 90% of the respondents answered that they have taken such measures as separation of network(s) from the Internet, restriction of connections of external storage devices, and introduction of

---

[7] 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.

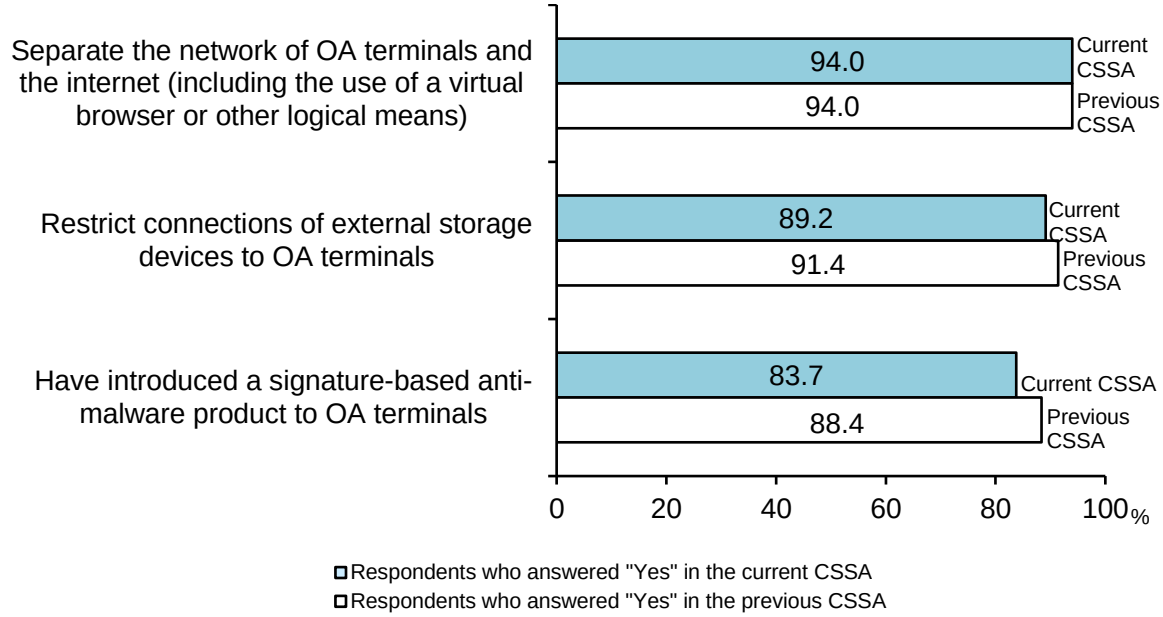
[8] Abbreviation of Security Operation Center; A center to monitor and analyze cybersecurity-related situations, such as attacks to networks, servers, or firewalls, etc.

[9] For the purpose of this CSSA, "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 such means as using simulated malware or abusing a vulnerability or a defect in settings." "Threat-led penetration testing" is defined as a "more practical 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 imitating strategies and means that attackers are supposed to adopt, after first analyzing risks faced by the organization individually and specifically."

[10] For the purpose of this CSSA, "OA terminals" are defined as "standard terminals that staff members normally use for preparing documents, etc."

signature-based anti-malware products (Chart 15).[11] When financial institutions intend to further promote digitalization, they need to strengthen their cybersecurity measures based on the zero trust security model, by such means as introducing a mechanism of multi-factor authentication and behavior-based anti-malware products (including EDR) (see BOX1 for measures against attacks abusing a vulnerability in systems).

Chart 15: Controls against cyberattacks taken for OA terminals

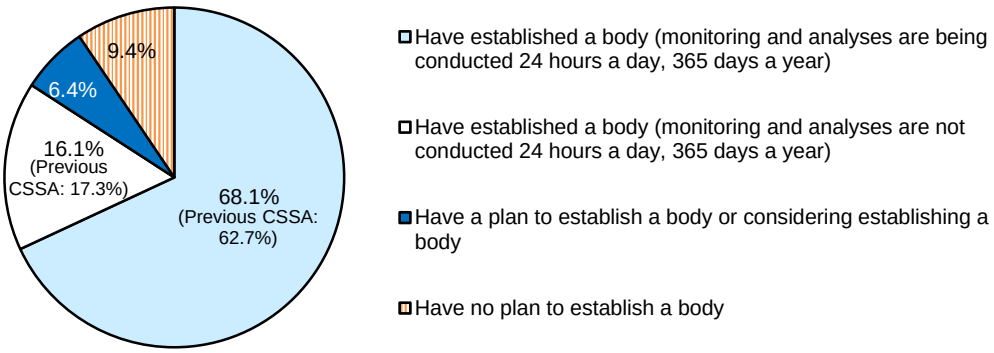


Posture for monitoring and analyzing cyber incidents

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). The respondents who answered that they have established an SOC, including those using external services, accounted for over 80%, showing an increase compared with the results of the previous CSSA. However, nearly 20% of them are not conducting monitoring and analyses on a constant basis (24 hours a day, 365 days a year) (Chart 16). If financial institutions intend to further expand service hours in their efforts for digitalization, they are expected to accelerate detection of and responses to cyber incidents through 24/7 operation in accordance with their service hours.

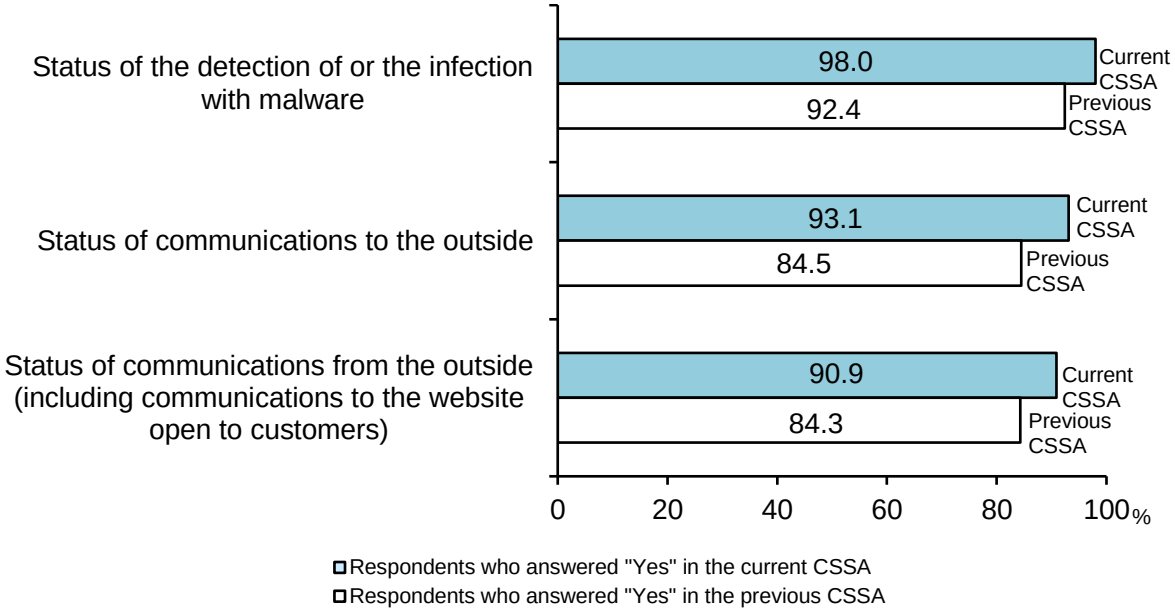
[11] Some measures were less cited in this CSSA, and the increasing introduction of EDR and VDI for terminals is considered to be one of the possible causes thereof. Virtual Desktop Infrastructure (VDI): a mechanism to virtualize a desktop environment of an OA terminal and to make it operate on a server

Chart 16: Status of establishing a body that conducts monitoring and analyses of cybersecurity-related issues (including outsourcing)



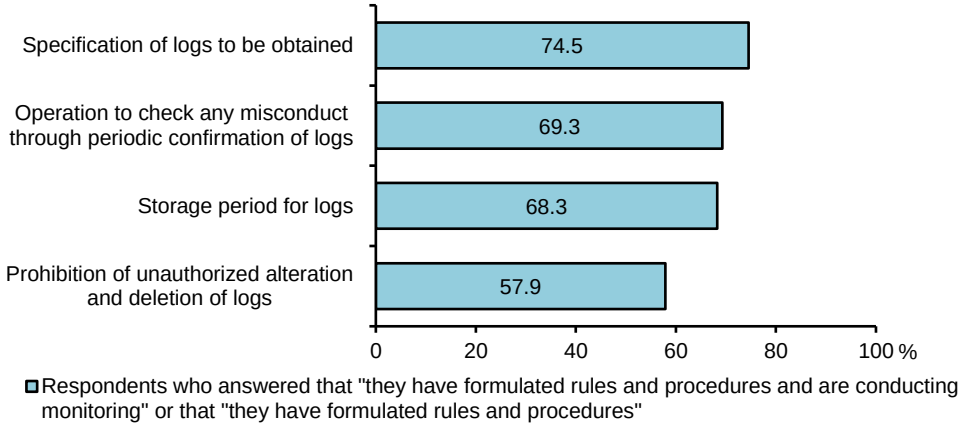
As for the coverage of monitoring by an SOC, most of the respondents answered that the relevant body conducts perimeter defense controls by monitoring and analyzing the status of the detection of or infection with malware and the status of communications with the outside (Chart 17). If financial institutions intend to further promote digitalization, they are encouraged to expand the coverage of systems under monitoring, including internal systems, and to monitor suspicious behavior while assuming the possibility of internal penetration and insider crime (i.e. illegal acts by staff members and outsourcees), thereby further strengthening frameworks for monitoring, from the perspective of early detection and prompt responses (i.e. prevention of the spread of damage).

Chart 17: Coverage of monitoring by an SOC or other department that monitors cybersecurity-related issues



System logs are indispensable to detect cyber incidents, examine the extent of the impact of cyber incidents and consider measures for recovery. It is therefore important to ensure their accuracy and comprehensiveness. Looking at how logs for material systems are handled, around 70% of the respondents have established rules concerning the specification of logs to be obtained, periodic confirmation of logs, and storage period for logs, while only around 60% have established rules to prohibit unauthorized alteration of logs (Chart 18). It is important to develop proper posture for managing logs for material systems with an intent to prevent and deter insider crime.

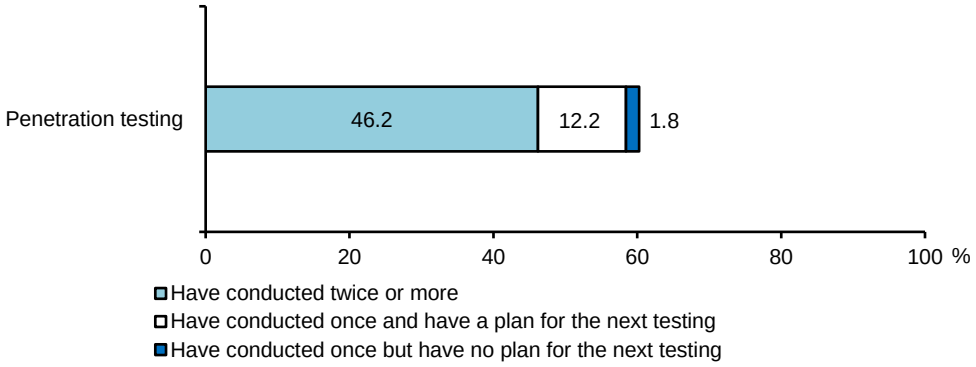
Chart 18: Matters prescribed regarding logs (audit trails) for material systems



Confirmation of the effectiveness of posture for monitoring and analyses

It is important to first establish and develop the organization's posture for monitoring and analyzing cyber incidents and conduct penetration testing and TLPT to confirm the effectiveness of the posture from an objective perspective. Regarding the implementation status of testing, over 60% of the respondents answered that they have conducted penetration testing at least once (Chart 19). Financial institutions are encouraged to conduct penetration testing to find challenges regarding the effectiveness of their own posture for monitoring and analyses.

Chart 19: Status of conducting penetration testing



Measures against illegal remittances and phishing attempts

Damage of illegal remittances presumably caused by phishing scams is growing rapidly.[12] Those phishing scams target customers of financial institutions, in which perpetrators direct

[12] See a notice to call for attention published jointly by the FSA and the National Police Agency, "Rapid Increase of Damage Caused by Illegal Remittances via Internet Banking Suspected of Phishing Scams (Warning)" (December 2023; Available only in Japanese).

Internet banking users to fraudulent websites for login by sending emails or via SMS under banks' names, and thereby acquire personal information such as IDs and passwords. Financial institutions should put in place countermeasures in advance of any damage. In addition to calling for users' attention, it is important for financial institutions to take measures in a planned manner such as introducing a mechanism of multi-factor authentication at the time of login and for each transaction, giving notices on the utilization status of Internet banking services to each user, developing procedures for detecting phishing websites and taking them down, and introducing sender domain authentication mechanisms (SPF, DKIM, DMARC).[13]

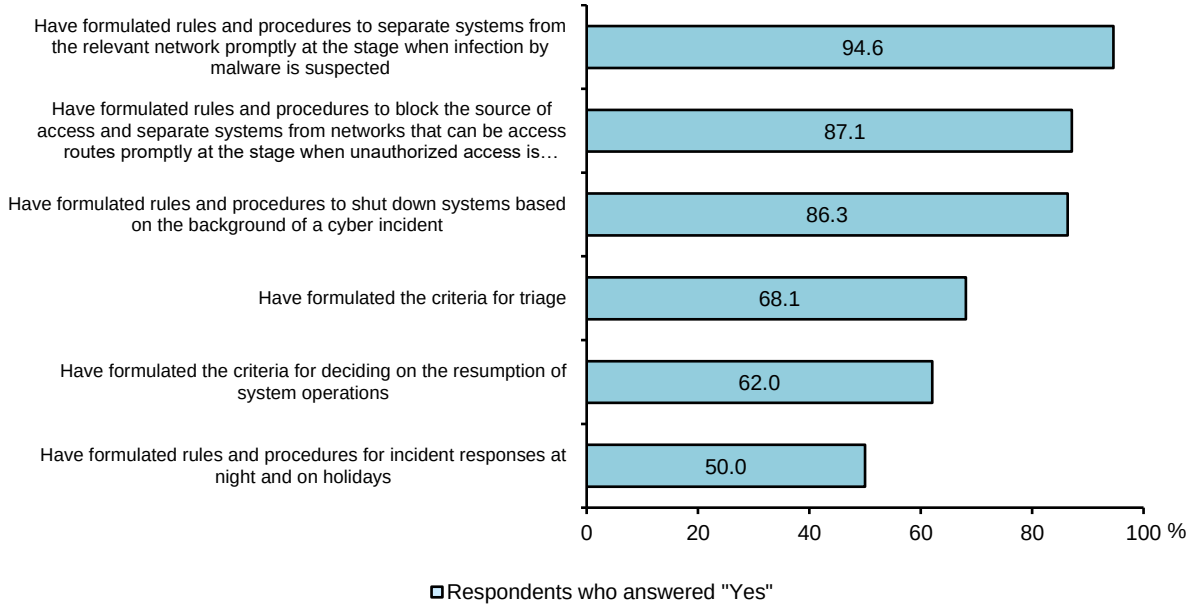
3. Preparations for Contingencies

Development of procedures for measures to prevent the spread of damage

In the event of a cyber incident, it is important to accurately understand the event and endeavor to resume operations promptly, while taking measures to prevent the spread of damage. As for the status of development of procedures for such measures, the results have found that most of the respondents have formulated rules and procedures for an initial response while only 50% to 70% have formulated the criteria for the prioritization in response policies (i.e. triage) and for decision making with regard to the resumption of system operations, and procedures for responses at night and on holidays (Chart 20). Financial institutions should envisage possible situations upon the occurrence of an incident in a concrete manner and should formulate practical rules and procedures.

[13] Sender Policy Framework (SPF): a mechanism to check whether or not the domain of a sender of an email is fraudulent; Domain Keys Identified Mail (DKIM): a mechanism to require a sender to affix an electronic signature upon sending an email and have a receiver verify it, thereby detecting impersonation of senders and falsification of emails; Domain-based Message Authentication, Reporting, and Conformance (DMARC): one of the email sender domain authentication technologies, which is a mechanism to have a sender present to a receiver a record called a policy regarding how to deal with an email for which the authentication failed, by way of disclosing it on DNS

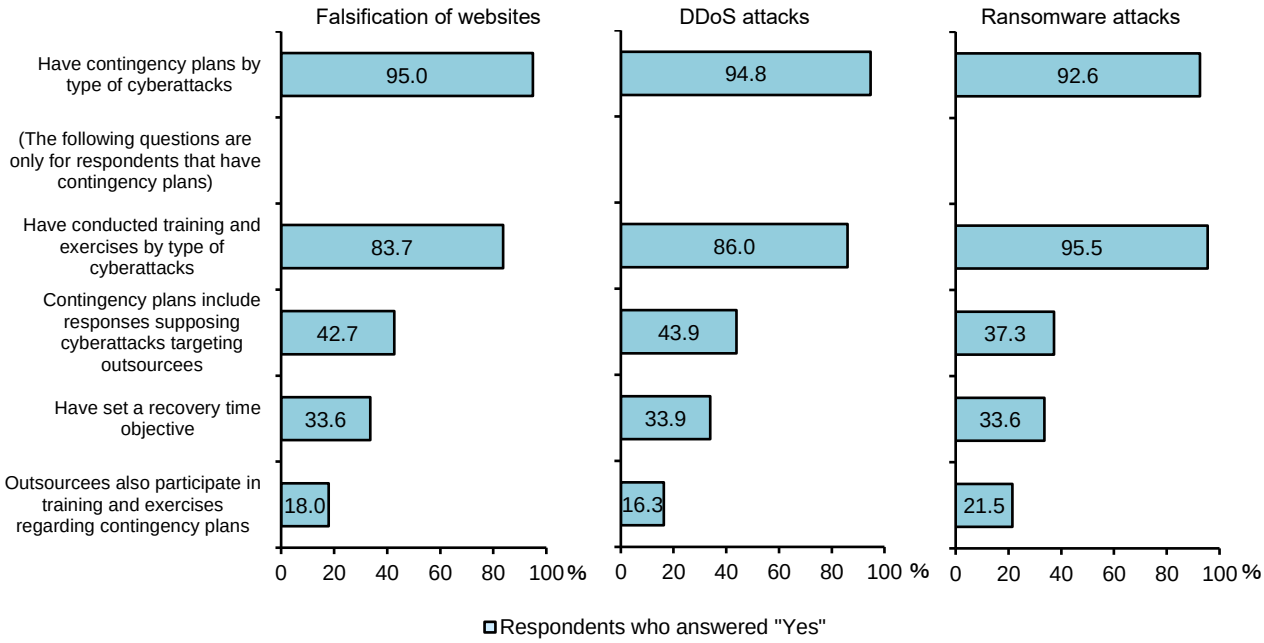
Chart 20: Status of formulating rules and procedures to prevent the spread of damage



Formulation of contingency plans and implementation of training and exercises

According to the results, most of the respondents have formulated plans by type of cyberattacks and are conducting training and exercises (Chart 21). However, less than half have formulated contingency plans with the assumption of cyberattacks made to their outsourcees, conducted training and exercises with the participation of outsourcees, and set a recovery time objective. It is important for financial institutions to develop practical contingency plans, while considering the possibility that cyberattacks to outsourcees may exert influences on the organization and setting a realistic recovery time objective based on the organization's system environment.

Chart 21: Status of formulating contingency plans by type of cyberattacks and their content



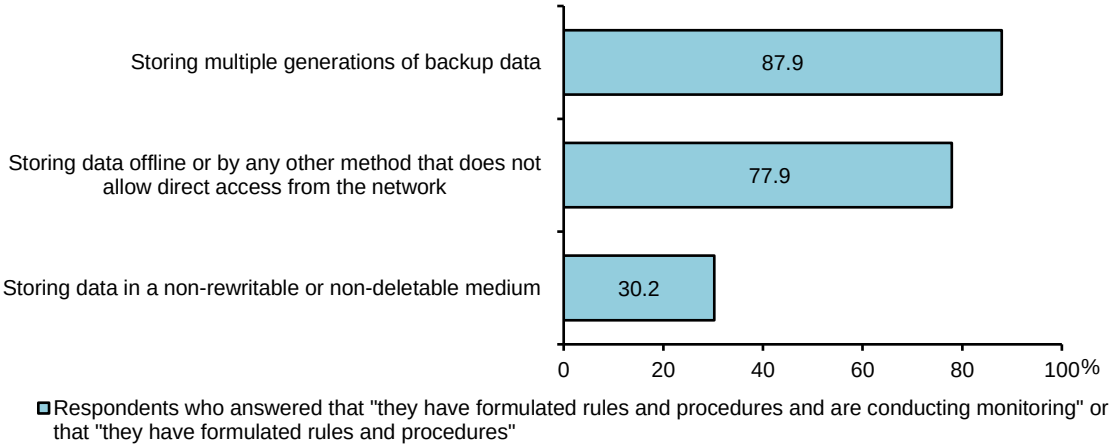
Protection of backup data with the assumption of ransomware attacks

One of the effective measures as a preparation for ransomware attacks, which are increasing in recent years, is to regularly obtain backup data to recover a system. However, there have also been cases where the backup data, which had been obtained in advance, were also encrypted via the network from a device infected with ransomware, which made it difficult to recover the IT system (see BOX2).

Looking at the status of measures in consideration of the possibility of destruction or falsification of backup data in material systems, the results indicate that majority of the respondents are taking measures to protect data by such means as storing multiple generations of backup data and storing the data by a method that does not allow direct access from the network (Chart 22). From the perspective of recovering business operations earlier in case of a ransomware attack, measures to prevent destruction and falsification of backup data are important.[14]

[14] Regarding the importance of controls to prevent destruction and falsification of backup data, see BOX 3 of "Results of the Cybersecurity Self-Assessment for Regional Financial Institutions (FY2022)," *Financial System Report Annex Series*, April 2023.

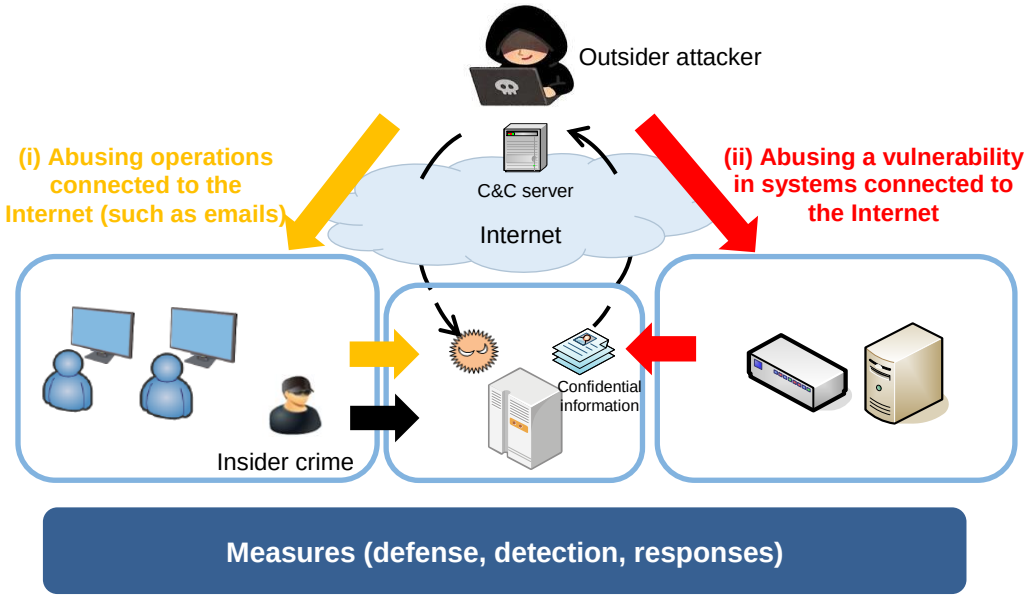
Chart 22: Measures in consideration of the possibility of destruction or falsification of backup data in material systems



BOX1 Measures against Attacks Abusing a Vulnerability in Systems

Major penetration routes from outside include (i) attacks targeting operations of OA terminals through accessing websites or using emails, and (ii) attacks abusing a vulnerability in systems (including appliances and other devices) connected to the Internet (Chart B1-1). Measures against attacks of the latter type are discussed below (see the main text (Chapter II, Section 2, "Controls against cyberattacks taken for OA terminals") for attacks targeting OA terminals).

Chart B1-1 Attackers' penetration routes

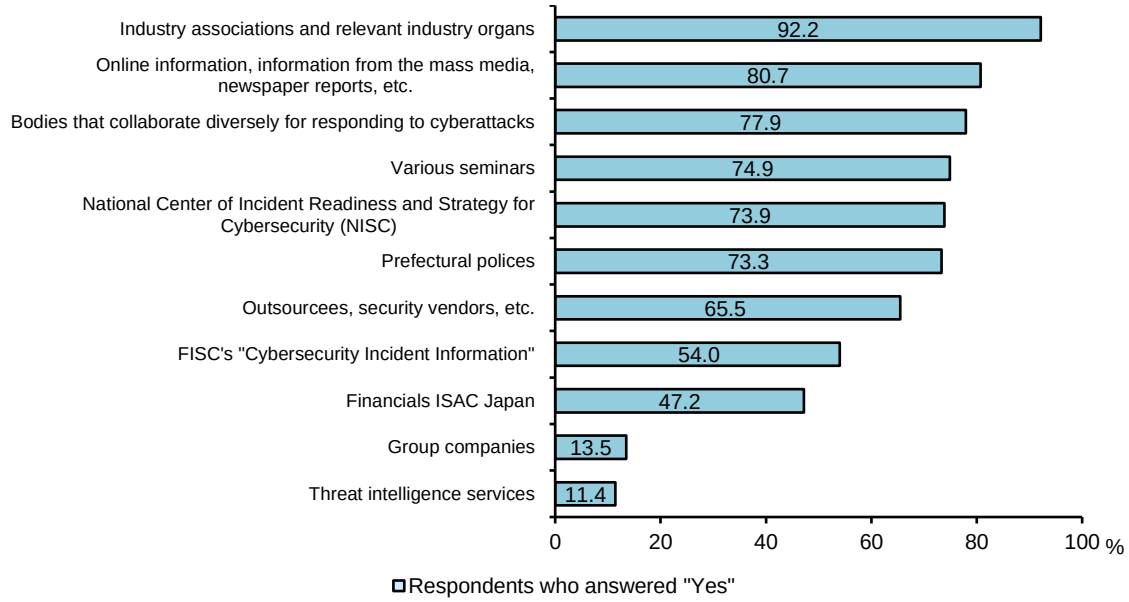


The first step in responding to an attack that abuses a vulnerability in systems is to collect accurate information on the vulnerability. According to the results of the CSSA, it was confirmed that many of the respondents are collecting information from diverse sources (Chart B1-2). Among them, those collecting information from industry associations and relevant industry organs accounted for the highest percentage. This may be partially because cooperative structured financial institutions often jointly use the same system companies.[15] In addition, this fact may imply the effectiveness of information provision by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which supports efforts for ensuring cybersecurity in critical infrastructures in Japan, including the financial sector, and information sharing via the Financials ISAC Japan, which is a cybersecurity-related mutual assistance organization covering the financial industry. Amid

[15] For example, *shinkin* banks are considered to be using the Shinkin Banks Information System Center (SSC), and *shinkumi* banks are considered to be using the Shinkumi Information Service (SKC).

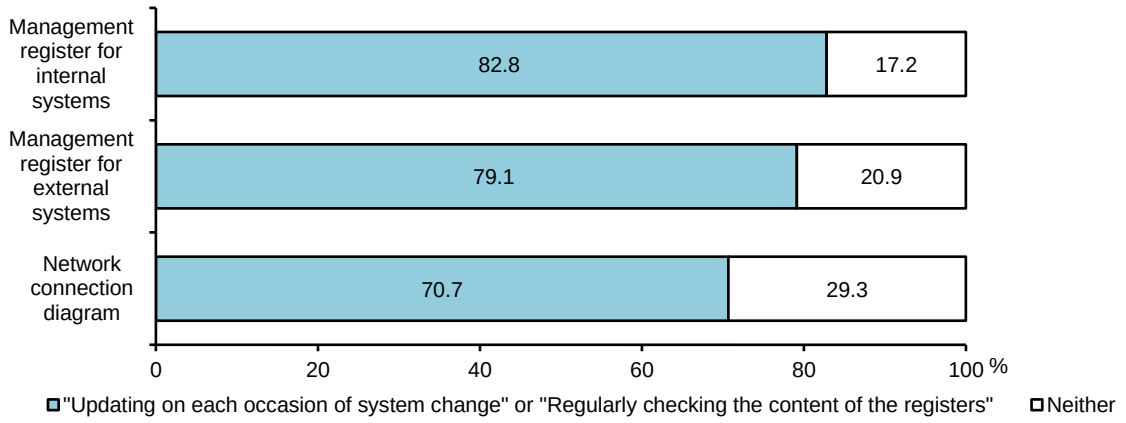
changes in external environments, it is important that such mutual assistance organizations serve as a hub for the industry to facilitate collaboration in collecting information on vulnerability and other risks. The financial industry is encouraged to continue strengthening industry-wide efforts.

Chart B1-2: Sources of information on cybersecurity



When obtaining information on vulnerability, financial institutions are required to promptly ascertain the level of possible impact of that information on their organizations and make responses as necessary. For that purpose, they should make visible the entirety of their own system-related assets and the latest status thereof so that they can identify systems connected to the Internet and check whether versions of OS and software of their systems are subject to relevant vulnerability and whether they have concluded maintenance service agreements to receive security patches. Regarding the status of maintaining registers of system-related assets, around 70% to 80% of the respondents update the registers on each occasion of system change or regularly check the content of the registers, while around 20% to 30% do not manage their system-related assets in such a manner (Chart B1-3). It is important to appropriately manage system-related assets and system configuration information.

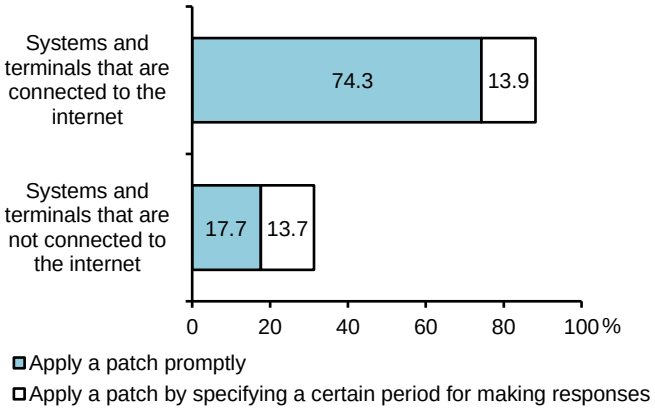
Chart B1-3: Status of maintaining management registers, etc. for systems



(Note) For the current CSSA, "internal systems" are defined as "systems operated within the own organization," and "external systems" are defined as "systems operated outside the own organization (including cloud services)."

When any serious vulnerability is found, a security patch (vulnerability remediation program) should be applied promptly, in principle. As explained in the main text (Chapter II, Section 1 "Risk management and involvement of executives"), financial institutions' systems connected to the Internet are often prioritized for applying security patches (Chart B1-4; <same as Chart 8 in the main text>).

Chart B1-4: Policies for applying a patch when a serious vulnerability is found

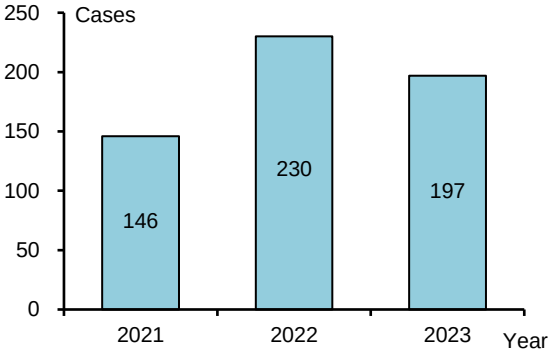


Recently, there are ransomware attacks abusing a vulnerability in VPN devices at third parties via a closed network of the organization that are not connected to the Internet. Therefore, it is not appropriate to consider a closed network risk-free and to put off responses for internal systems that are not connected to the Internet. When a serious vulnerability is found, it is important to apply a security patch promptly for internal systems, thereby strengthening efforts to cover security holes due to a vulnerability in the entirety of the organization's system environment (such efforts are sometimes called cyber hygiene as they intend to control hygiene in the cyberspace).

BOX 2 Trends Relating to Ransomware Attacks

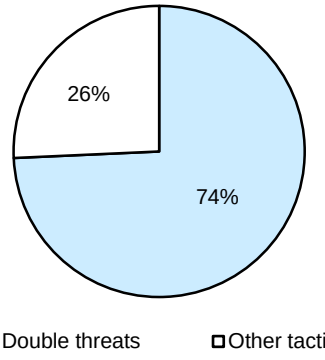
According to the data published by the National Police Agency,[16] the number of incidents of reported damage due to ransomware attacks has stayed high (Chart B2-1). A ransomware attack is an attack undertaken by encrypting data of a system and demanding ransom in form of crypto-assets or money in exchange for decryption of the encrypted data. However, in over half of the recent cases, perpetrators encrypt and steal data at the same time entailing 'double threats' (i.e. refusing to give decryption keys and threatening to leak the relevant information) (Chart B2-2).

Chart B2-1: Damage due to ransomware attacks sustained by companies



(Source) National Police Agency

Chart B2-2: Tactics for threats

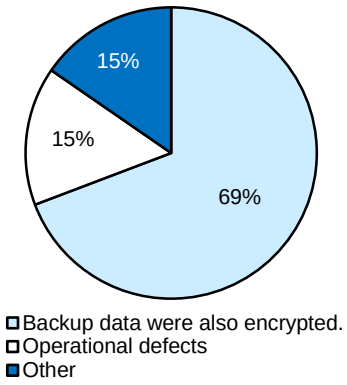


(Note) Breakdown of 175 cases, out of total number of cases for 2023, for which tactics could be confirmed
(Source) National Police Agency

Regarding reasons for failures in recovering systems despite of having backup data in advance, nearly 70% of the respondents answered that backup data were also encrypted (Chart B2-3). With an awareness that backup data may also be targeted by ransomware attacks, financial institutions should take measures to prevent destruction and falsification (encryption) of backup data.

[16] See "The Situation of Threats in Cyberspace in 2023" by the National Police Agency (March 2024; Available only in Japanese).

Chart B2-3: Reasons that victimized companies failed to recover data from backup data



(Note) Breakdown of 104 cases, out of total number of cases for 2023, for which reasons for failures in recovering data from backup data could be confirmed
(Source) National Police Agency

III. Conclusion

This report compiles the results of the CSSA from the viewpoints of (i) involvement of executives, (ii) measures against cyber risks, and (iii) preparations for contingencies. Many of the regional financial institutions consider ensuring cybersecurity to be an important management issue and are steadily making efforts to enhance the effectiveness of their cybersecurity controls through the introduction of measures concerning both technological and organizational aspects. On the other hand, the results also found that they still have challenges in securing and fostering cybersecurity human resources and managing third-party risks.

A contact point with the Internet, which can be the starting point for a cyberattack (i.e. an attack surface), varies depending on individual financial institutions' businesses, the way in which they utilize digital technologies, and the structure of their IT systems. This makes controls required for ensuring cybersecurity differ among financial institutions. Nevertheless, it is important for Japanese financial institutions, including regional financial institutions, to continue efforts for developing better cybersecurity management posture and securing the effectiveness of their controls based on the zero trust security model. This is even more so given that they intend to further utilize digital technologies and threats of cyberattacks are growing accordingly. For fiscal 2024 onward, the BOJ and the FSA plan to continue the initiative of the CSSA to encourage regional financial institutions to strengthen their spontaneous efforts for ensuring cybersecurity with accurate recognition of their own challenges based on their self-assessments.

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