Financial System Report – Annex

[Summary] 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

Outline

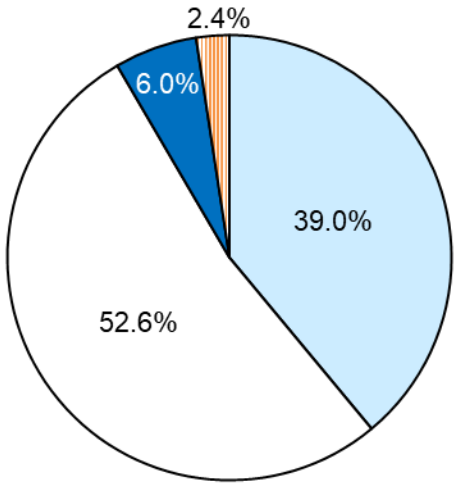
- ✓ Objectives: To have financial institutions identify their own positions in comparison with other financial institutions and areas of their own challenges and encourage them to strengthen their cybersecurity controls on a voluntary basis.
- ✓ Implementation: The Bank of Japan (BOJ) and the Financial Services Agency (FSA) developed a tool (a check sheet) for conducting a self-assessment of cybersecurity management posture, requested regional financial institutions to assess their own cybersecurity frameworks, and fed back the overall results to them. The CSSA in fiscal 2023 was the second one.
- ✓ Organizer: The BOJ and the FSA
- ✓ Subjects: 498 regional financial institutions (99 regional banks, 254 shinkin banks, and 145 shinkumi banks)
- ✓ Period: Self-assessments for financial institutions were conducted in July to August 2023, and the overall results were returned in November 2023.

Summary of the Results 1. Involvement of Executives (i)

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

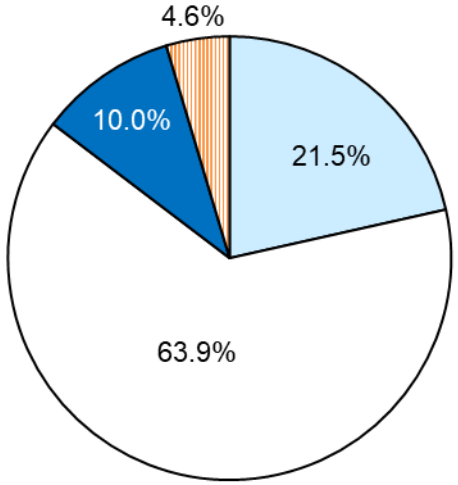
✓ Most of the respondents answered that they have set up a management policy to ensure cybersecurity, but around 8% of the respondents have not formulated a management policy. In addition, around 15% of the respondents have not formulated management plans concerning cybersecurity.

▽ Formulation of management policies concerning cybersecurity (Chart 2. in the report)



- Have set up a management policy to ensure cybersecurity with the involvement of the chief executive (president, CEO, etc.) and have externally published it upon information disclosure or on a website, etc.
- Have set up a management policy to ensure cybersecurity with the involvement of the chief executive (not externally published)
- Planning to set up a management policy to ensure cybersecurity
- Have no plan to set up a management policy to ensure cybersecurity

▽ Formulation of management plans concerning cybersecurity (Chart 3. in the report)



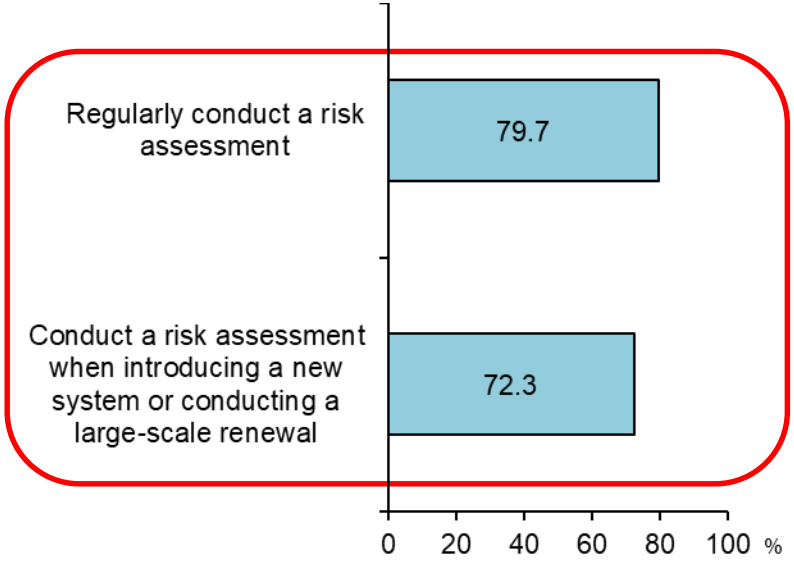
- Have formulated a multiple-year management plan concerning cybersecurity
- Have formulated a single-year management plan concerning cybersecurity
- Planning to formulate a management plan concerning cybersecurity
- Have no plan to formulate a management plan concerning cybersecurity

Summary of the Results 1. Involvement of Executives (ii)

■ Risk management and involvement of executives

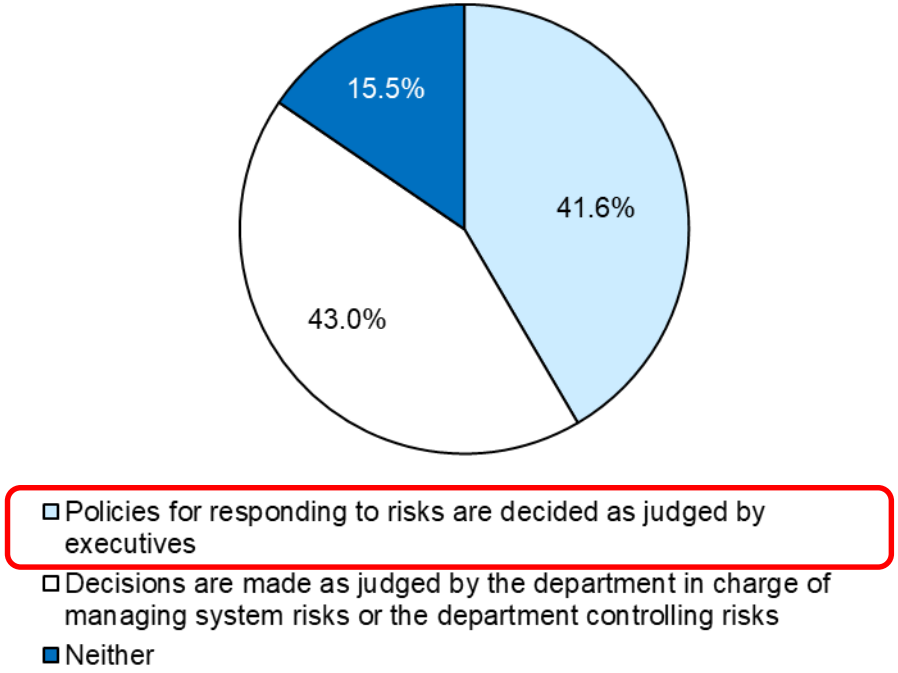
- ✓ Many of the respondents conduct risk assessments regularly and/or when introducing a new system.
- ✓ On the other hand, just over 40% of the respondents answered that policies for responding to cyber risks are decided as judged by their executives.

▽ Status of conducting risk assessments concerning cybersecurity of material systems (Chart 6. in the report)



(Note) 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."

▽ Decision maker for response policies based on risk assessments (Chart 7. in the report)

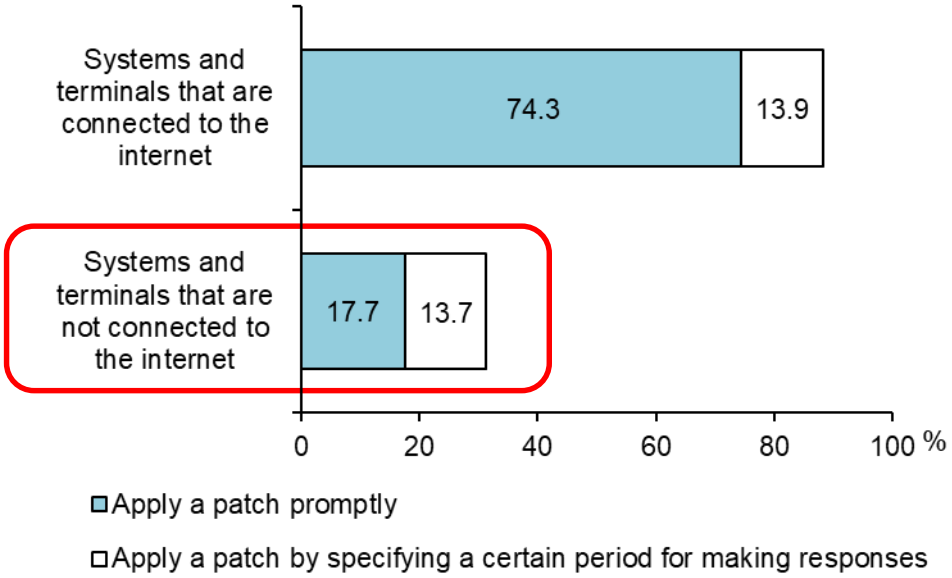


Summary of the Results 1. Involvement of Executives (iii)

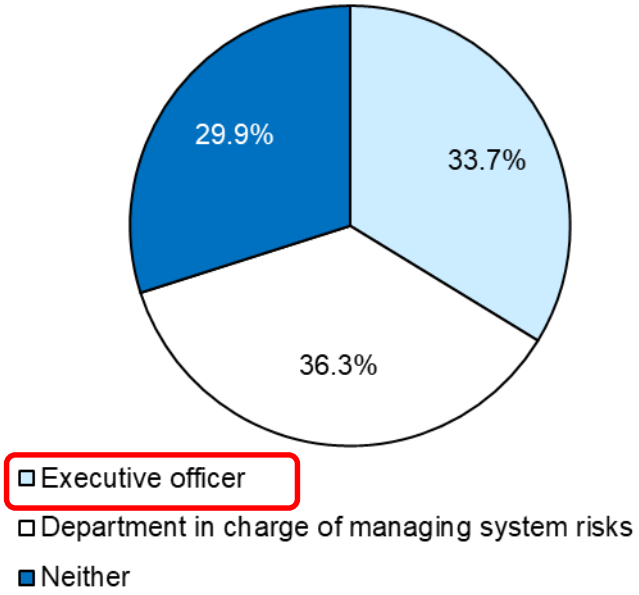
■ Risk management and involvement of executives

- ✓ Nearly 90% of the respondents answered that they apply a security 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.
- ✓ Just over 30% answered that decisions not to apply a security patch for a serious vulnerability are made with the involvement of executive officers.

▽ Policies for applying a patch when a serious vulnerability is found (Chart 8. in the report)



▽ Approver for a decision not to apply a patch for a serious vulnerability (Chart 9. in the report)

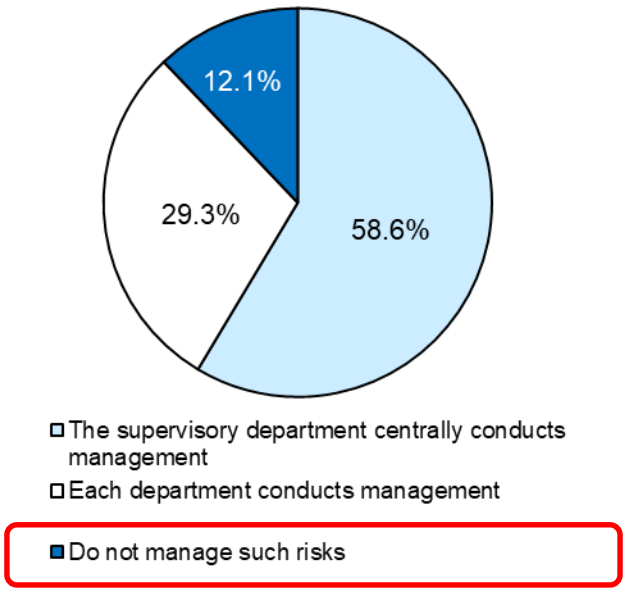


Summary of the Results 1. Involvement of Executives (iv)

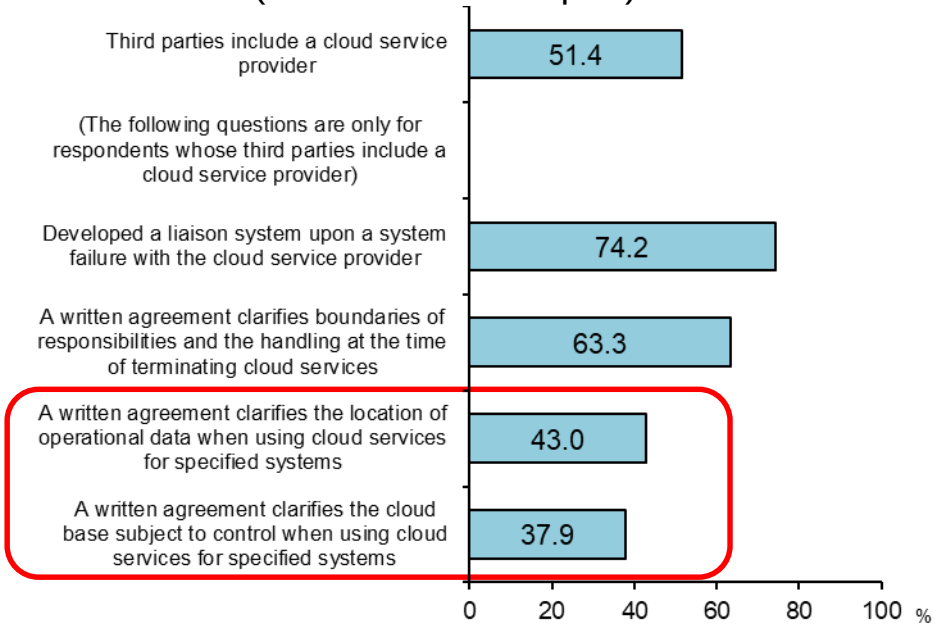
■ Controls against third-party risks

- ✓ Just around 60% of the respondents answered that their control department centrally manages cybersecurity risks in relation to important third parties, while around 10% do not manage third-party risks at all.
- ✓ The respondents who answered that they have clarified the location of operational data and the cloud base subject to control in agreements with cloud service providers accounted for only 30% to 40%.

▽ Status of managing cybersecurity risks for important third parties (Chart 10. in the report)



▽ Matters specified in agreements concluded with cloud service providers (Chart 11. in the report)



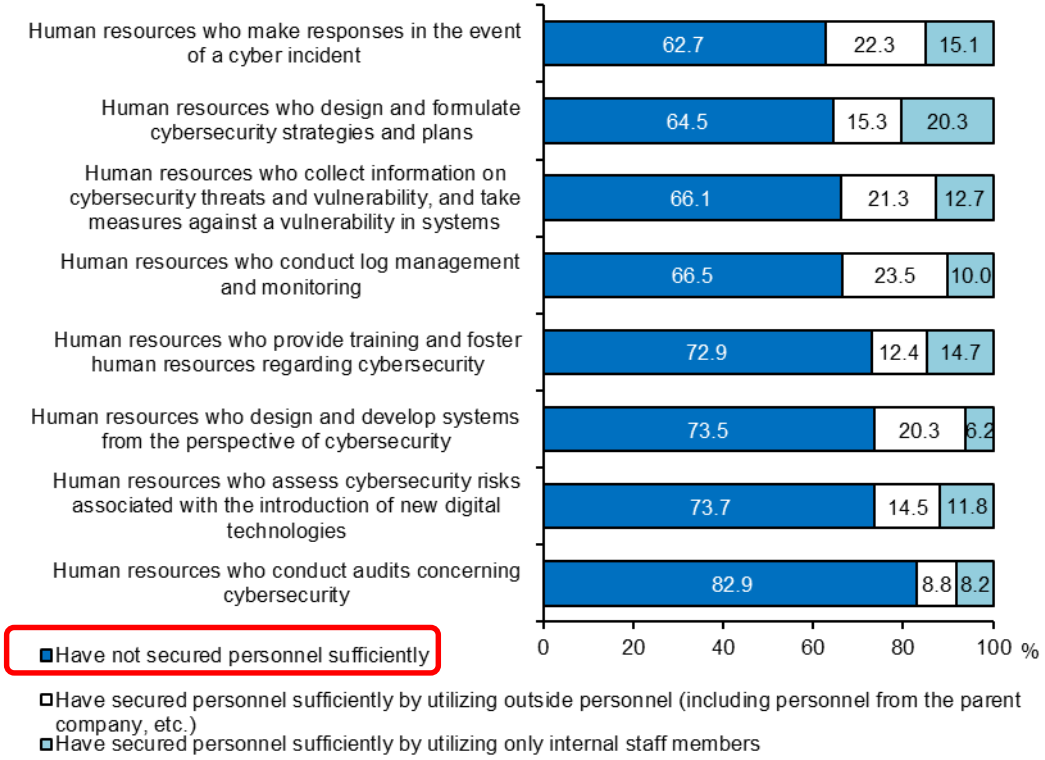
(Note) For the purpose of this CSSA, an "important third party" is defined as a "third party which the organization recognizes as being important for its business operations."

Summary of the Results 1. Involvement of Executives (v)

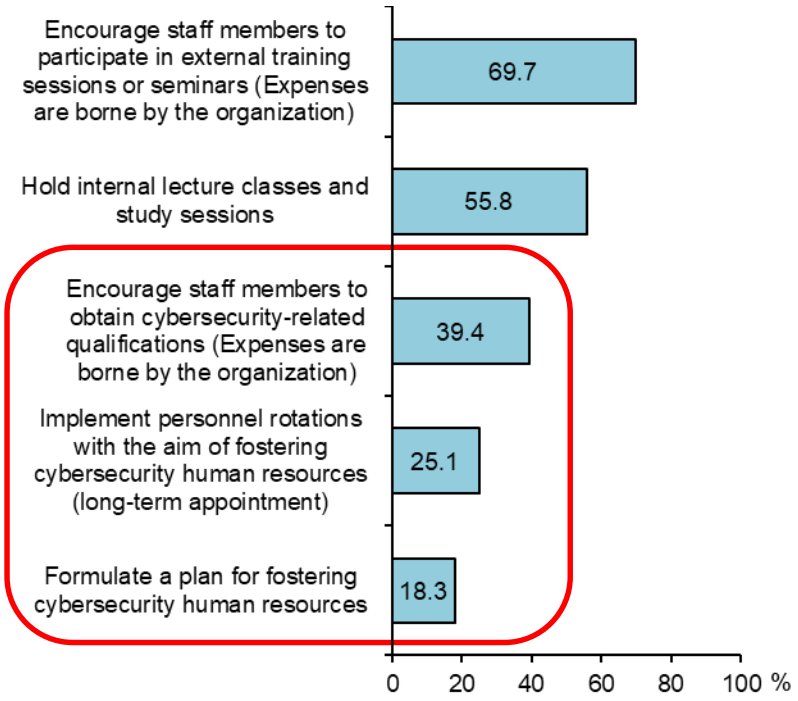
■ Securing cybersecurity human resources

- ✓ Most respondents answered that they have failed to sufficiently secure cybersecurity human resources for all functions, and an overall labor shortage was observed.
- ✓ More than half of the respondents are making efforts for human resources development to seek immediate results, while those making medium- to long-term efforts were limited in number.

▽ Status of securing cybersecurity human resources by function (Chart 12. in the report)



▽ Efforts for fostering human resources (Chart 13. in the report)

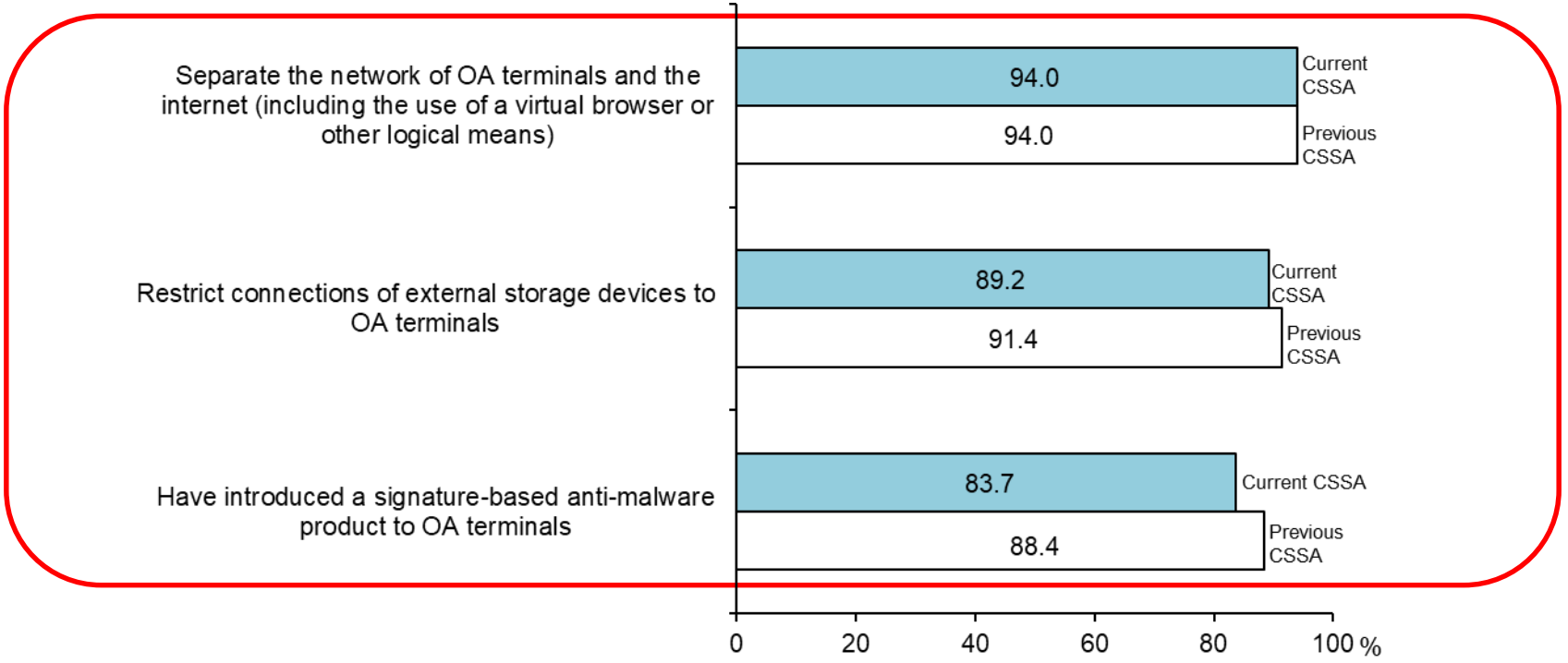


Summary of the Results 2. Measures against Risks (i)

■ Controls against cyberattacks taken for OA terminals

- ✓ 80% to 90% of the respondents answered that they conduct perimeter defense controls, such as the separation of networks from the Internet, restriction of connections of external storage devices, and introduction of signature-based anti-malware products.
- ✓ For further promoting digitalization, financial institutions need to strengthen their cybersecurity measures based on the zero trust security model.

▽ Controls against cyberattacks taken for OA terminals (Chart 15. in the report)



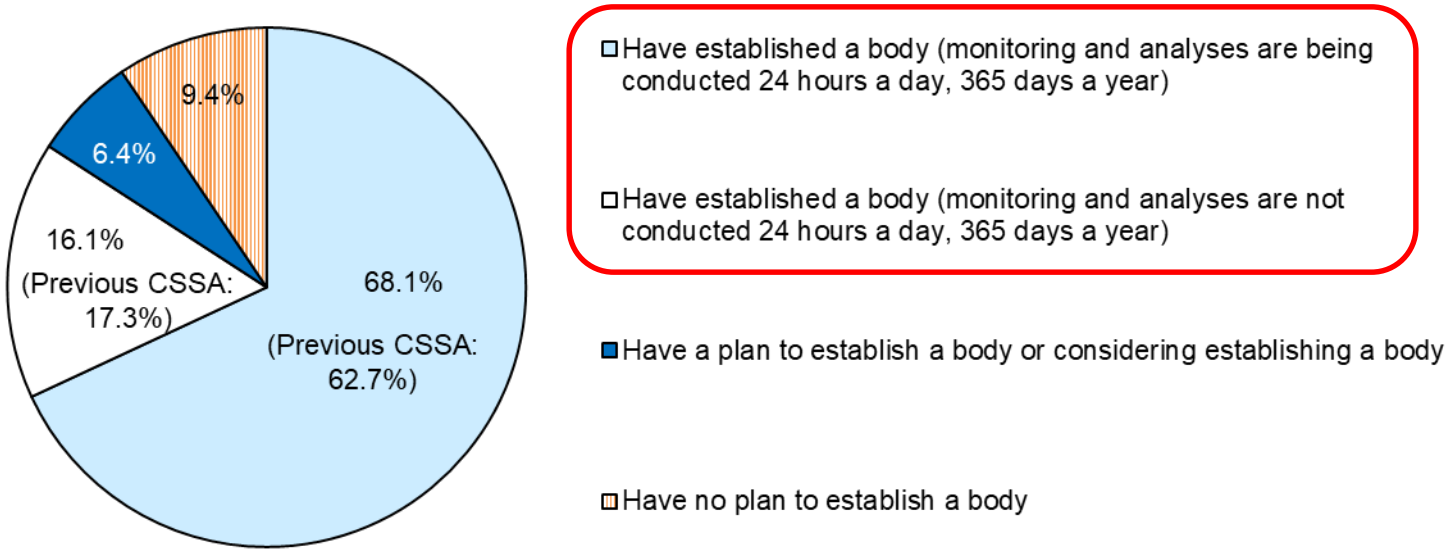
(Note) For the purpose of this CSSA, "OA terminals" are defined as "standard terminals that staff members normally use for preparing documents, etc."

Summary of the Results 2. Measures against Risks (ii)

■ Posture for monitoring and analyzing cyber incidents

✓ The respondents who answered that they have established a body that monitors and analyzes cybersecurity-related issues (SOC) accounted for over 80%, showing an increase compared with the results of the previous CSSA.

▽ Status of establishing a body that conducts monitoring and analyses of cybersecurity-related issues (including outsourcing) (Chart 16. in the report)



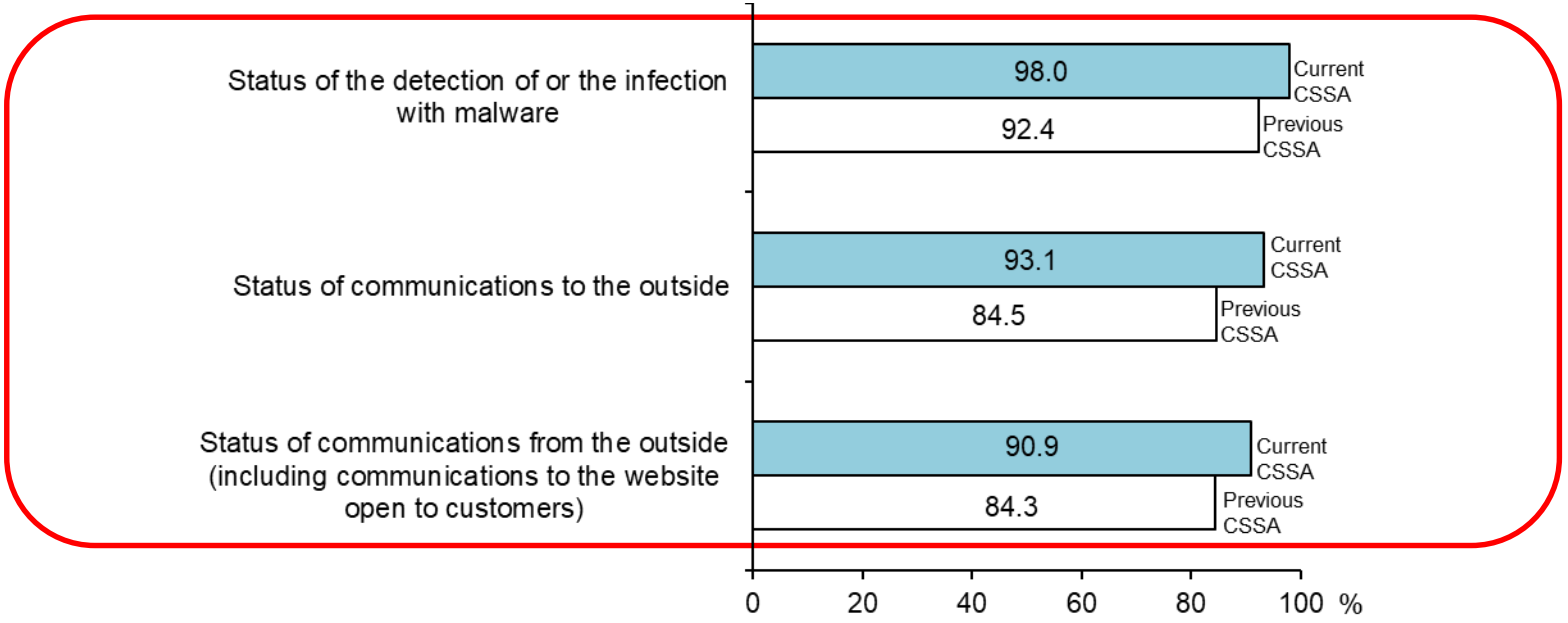
(Note) SOC is the abbreviation of Security Operation Center; A center to monitor and analyze cybersecurity-related situations, such as attacks to networks, servers, or firewalls, etc.

Summary of the Results 2. Measures against Risks (iii)

■ Posture for monitoring, and analyzing cyber incidents

- ✓ 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.
- ✓ If financial institutions intend to continue promoting digitalization, they are encouraged to monitor suspicious behavior on the assumption of the possibility of internal penetration and insider crime, thereby further strengthening posture for monitoring.

▽ Coverage of monitoring by an SOC or other department that monitors cybersecurity-related issues
(Chart 17. in the report)

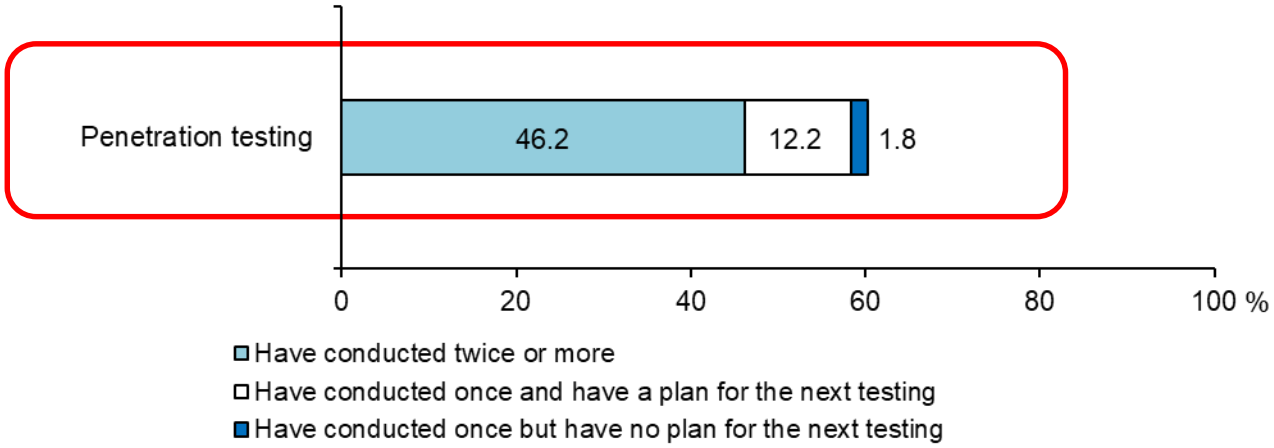


Summary of the Results 2. Measures against Risks (iv)

■ Confirmation of the effectiveness of posture for monitoring and analyses

- ✓ Looking at the status of confirming monitoring/analysis posture from an objective perspective, over 60% of the respondents answered that they have conducted penetration testing at least once.
- ✓ Financial institutions are encouraged to conduct penetration testing to find challenges regarding the effectiveness of their own posture for monitoring and analyses.

▽ Status of conducting penetration testing (Chart 19. in the report)



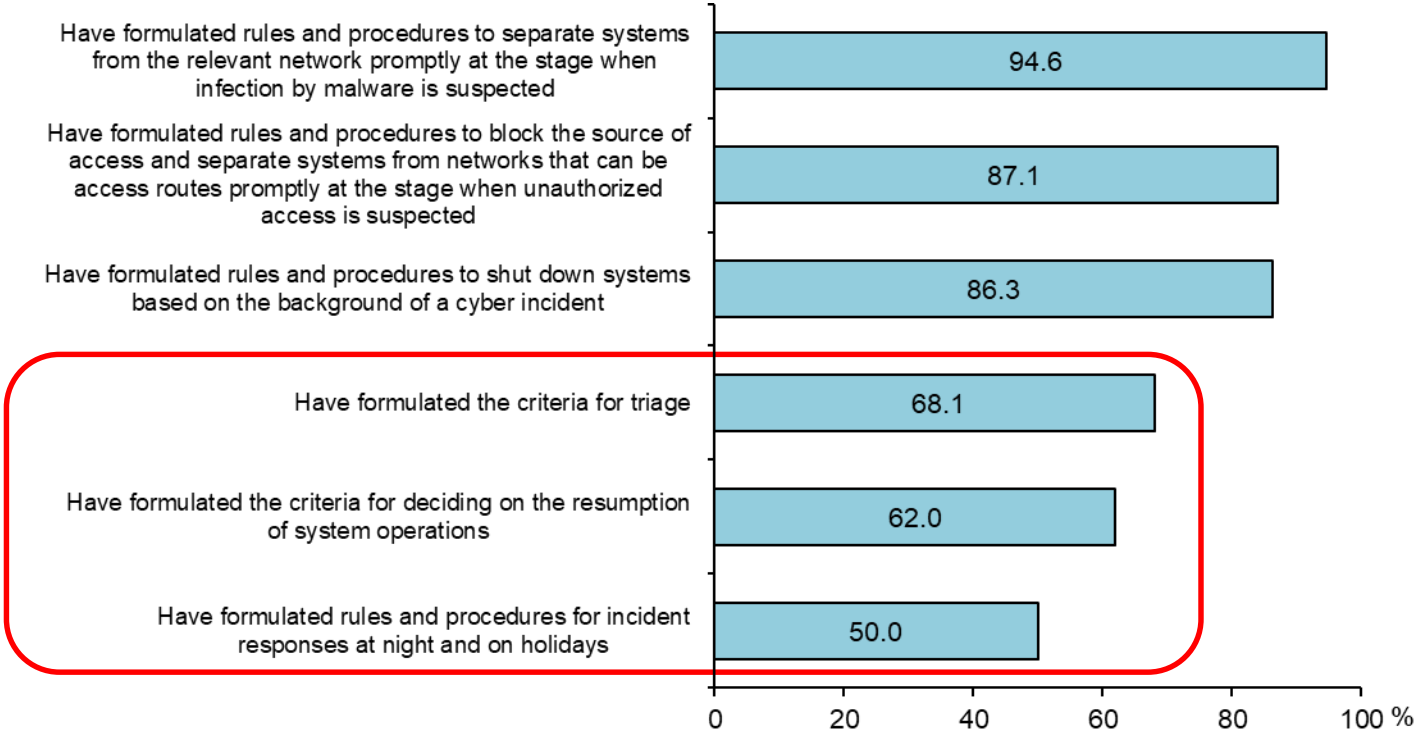
(Note) For the purpose of this CSSA, "penetration testing" is defined as a "test for checking whether penetration or falsification is possible and whether any attack can be detected and for verifying the promptness and appropriateness of responses by launching simulated attacks by such means as using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

Summary of the Results 3. Preparations for Contingencies (i)

■ Development of procedures for measures to prevent the spread of damage

✓ 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.

▽ Status of formulating rules and procedures to prevent the spread of damage
(Chart 20. in the report)

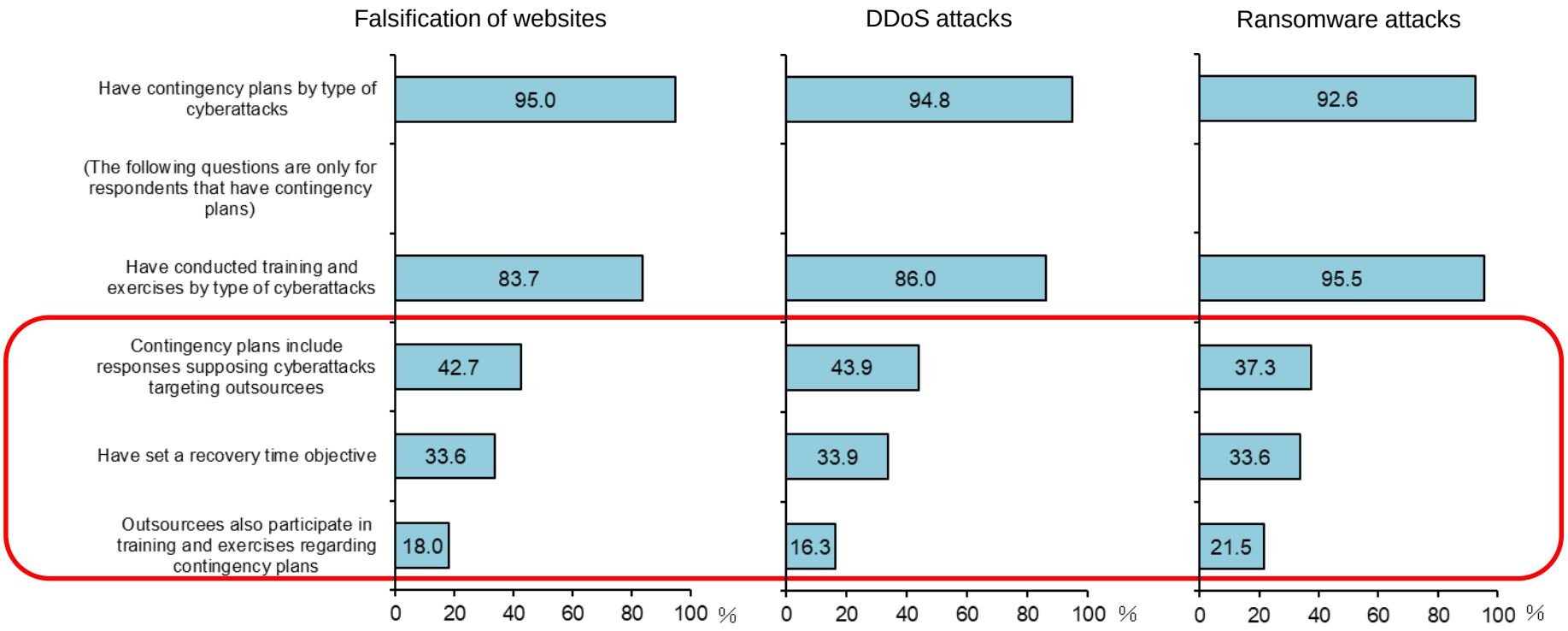


Summary of the Results 3. Preparations for Contingencies (ii)

■ Formulation of contingency plans and implementation of training and exercises

- ✓ Most of the respondents have formulated plans by type of cyberattacks and are conducting training and exercises.
- ✓ 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.

▽ Status of formulating contingency plans by type of cyberattacks and their content (Chart 21. in the report)

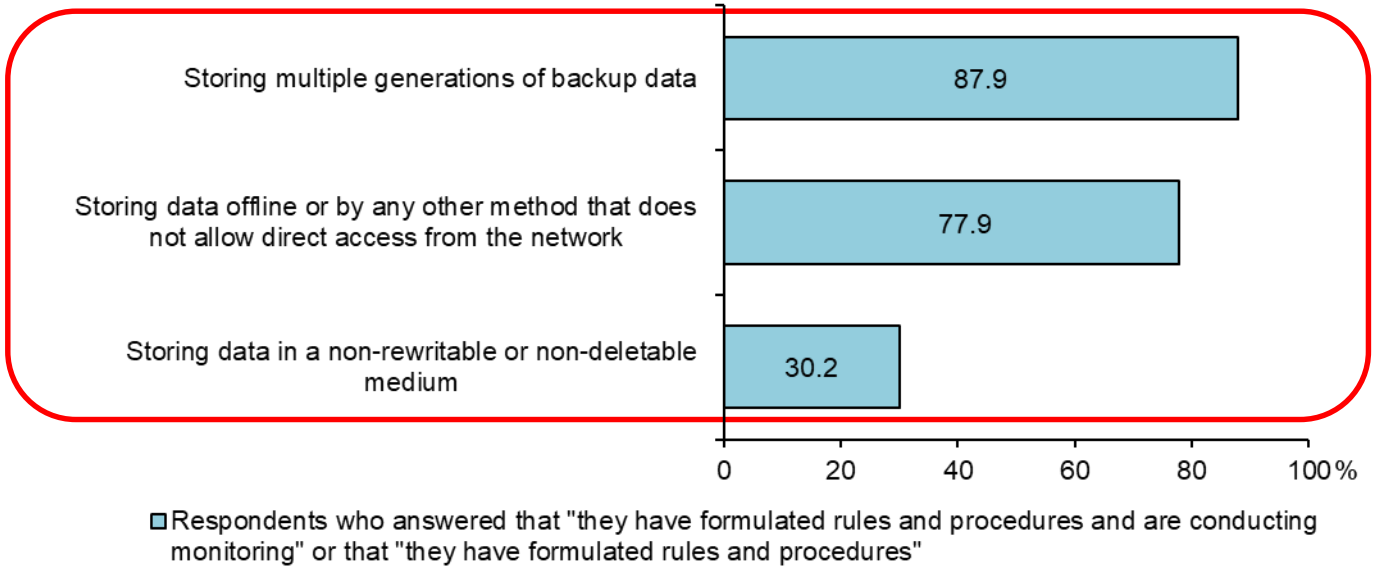


Summary of the Results 3. Preparations for Contingencies (iii)

■ Protection of backup data with the assumption of ransomware attacks

- ✓ Majority of the respondents are taking measures to protect backup 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.
- ✓ 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.

▽ Measures in consideration of the possibility of destruction or falsification of backup data in material systems (Chart 22. in the report)



Conclusion

- ✓ 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.
- ✓ It was 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, it was also found that they still have challenges in securing and fostering cybersecurity human resources and managing third-party risks.
- ✓ Considering such circumstances, the CSSA is envisaged to be conducted annually in and after fiscal 2024, while updating the questions in light of environmental changes.
- ✓ 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.