Financial System Report – Annex

[Summary]

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

Outline

- ✓ Objectives: To have financial institutions identify their own positions in comparison with other financial institutions and areas of their own challenges and to endeavor 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 frameworks, requested regional financial institutions to assess their own cybersecurity frameworks, and fed back the overall results to them. The first implementation is in fiscal 2022.

- ✓ Organizer: The BOJ and the FSA

- ✓ Subjects: 498 regional financial institutions (99 regional banks, 254 shinkin banks, and 145 shinkumi banks)

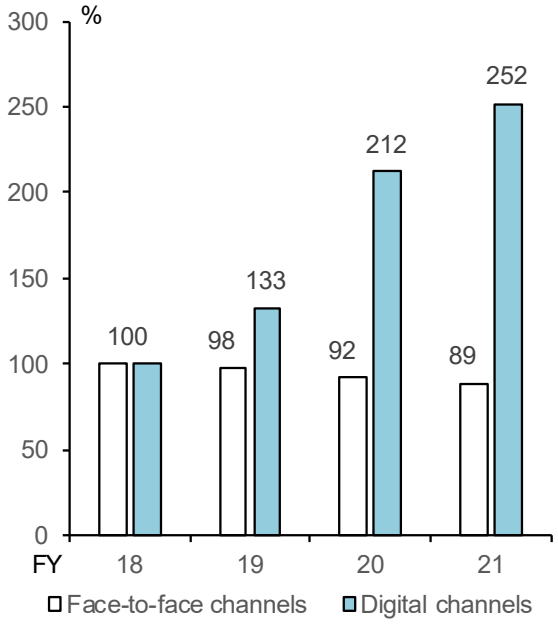
- ✓ Period: Self-assessments for financial institutions were conducted in July to August 2022, and the overall results were returned in November 2022.

Environment Surrounding Financial Institutions in Japan (i)

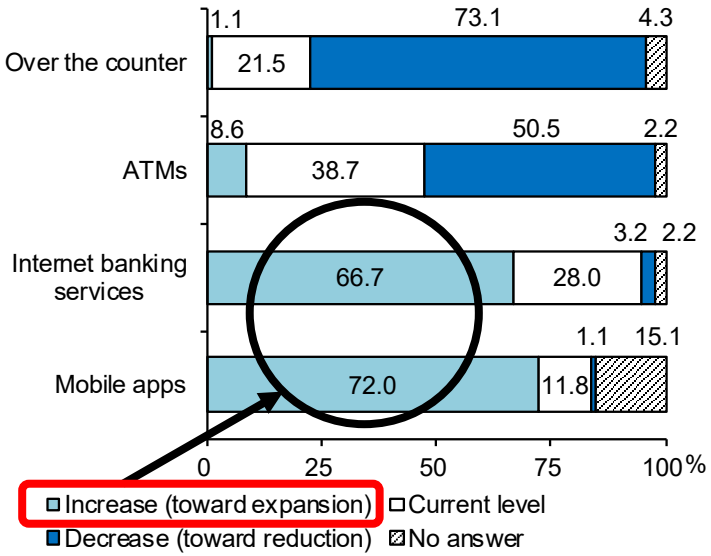
■ Progress in digitalization in channels for customer services (from external report)

✓ The amount of work handled through digital channels is increasing than that through face-to-face channels.

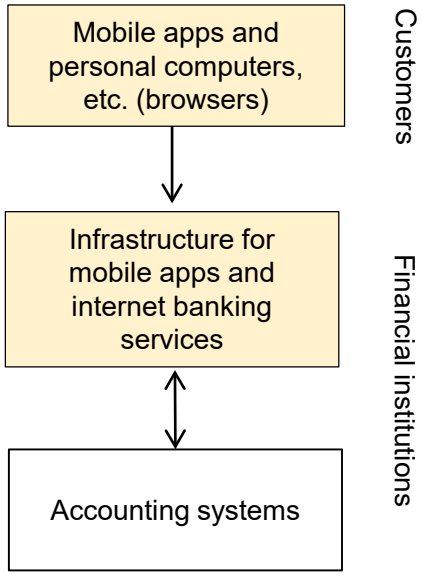
Changes in the amount of work handled



Outlook of the amount of work handled through each channel



Concept of digital channels



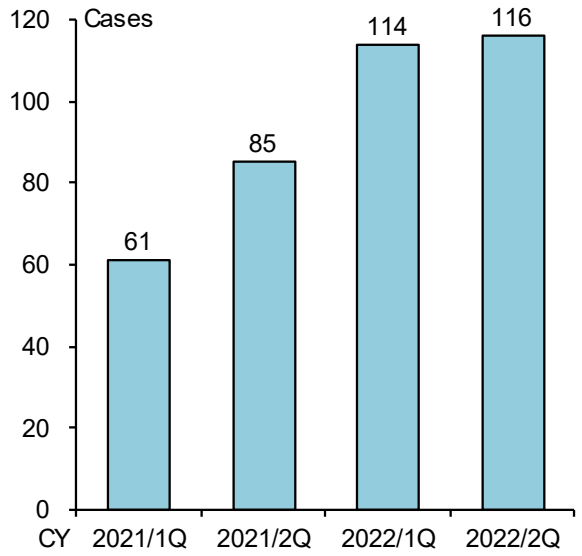
Source: Chart of "Changes in the amount of work handled" and “Outlook of the amount of work handled through each channel" are based on the "Status of Financial Institutions' Provision of Mobile Apps and Management frameworks Thereof – Results of the Questionnaire Survey –," Financial System Report Annex Series, November 2022 (available only in Japanese). https://www.boj.or.jp/research/brp/fsr/fsrb221115.htm

Environment Surrounding Financial Institutions in Japan (ii)

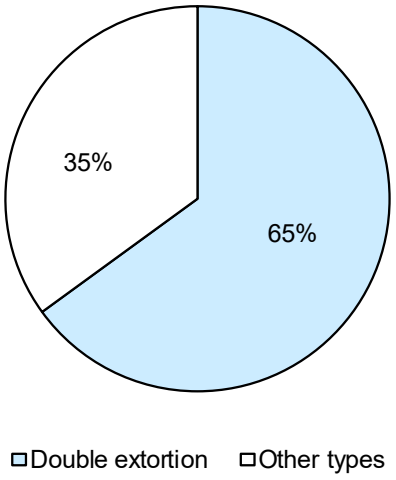
■ Trend of Cyber Threats Surrounding Financial Institutions (from external report)

✓ The number of ransomware attacks is increasing and the their tactics are becoming more sophisticated.

Number of damage caused by ransomware attacks



Tactics of ransomware attacks
(Cases for which tactics were identified: 182 cases <whole year of 2022>)



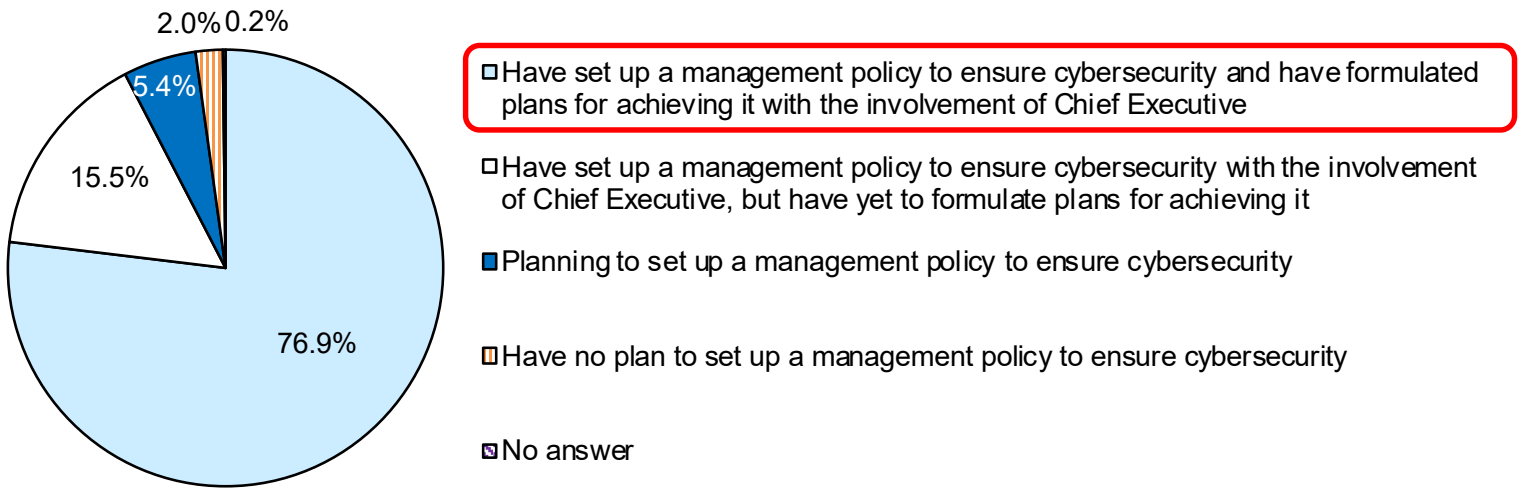
Source: "Threats in Cyberspace in 2022," the National Police Agency (available only in Japanese)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

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

■ Establishment of management policy and frameworks for its implementation

✓ Almost 80% of the respondents answered that they have formulated plans for ensuring cybersecurity with the involvement of Chief Executive.

Management policies and plans concerning cybersecurity (Chart 2. in the report)

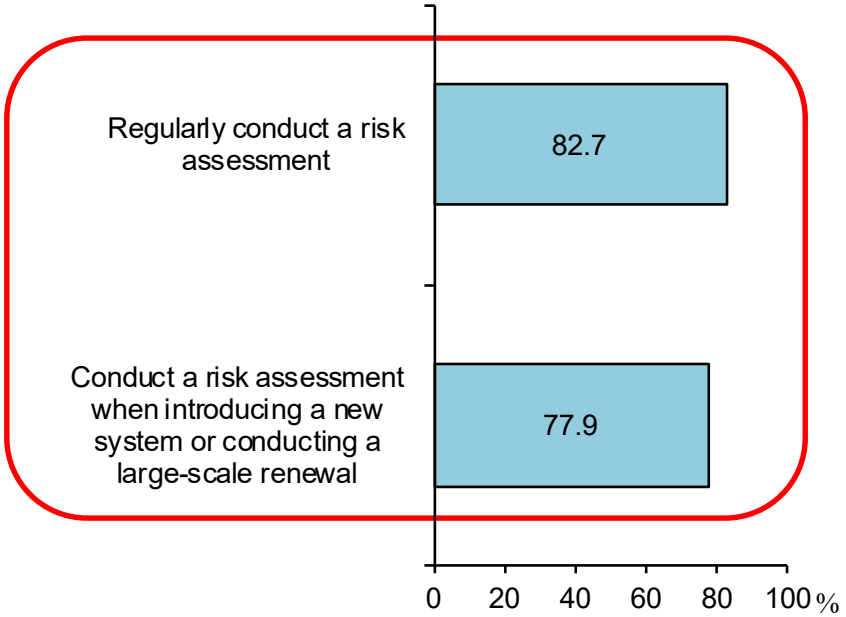


Summary of the Results　1. Involvement of Executives (ii)

■ Risk assessment concerning cybersecurity

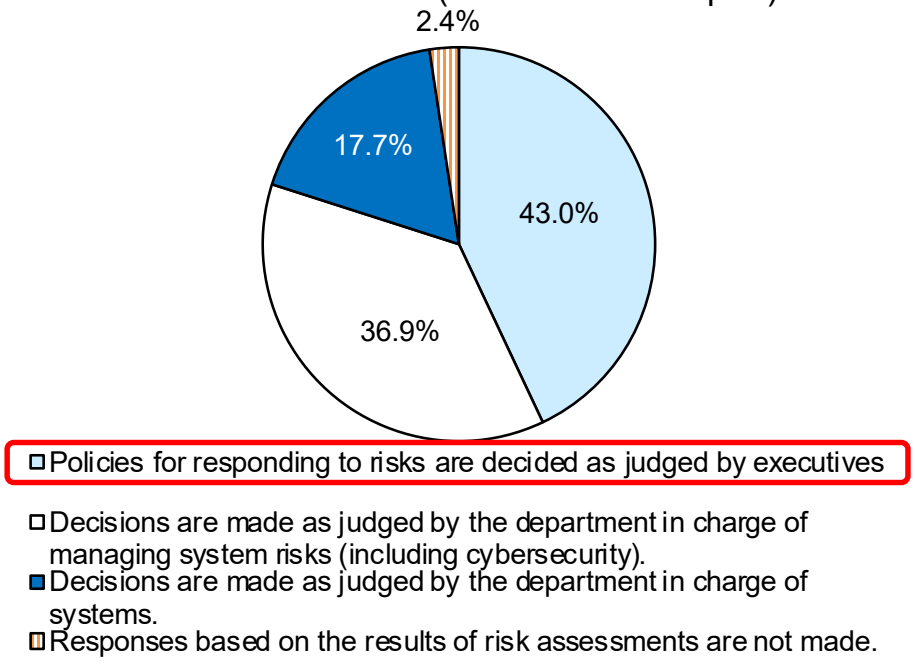
- ✓ Many of the respondents conduct risk assessments regularly and/or when introducing a new system.
- ✓ More than 40% of the respondents answered that executives make decisions.

Status of conducting risk assessments concerning cybersecurity of material systems (Chart 5. in the report)



Note: 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."

Decision maker for response policies based on risk assessments (Chart 6. in the report)

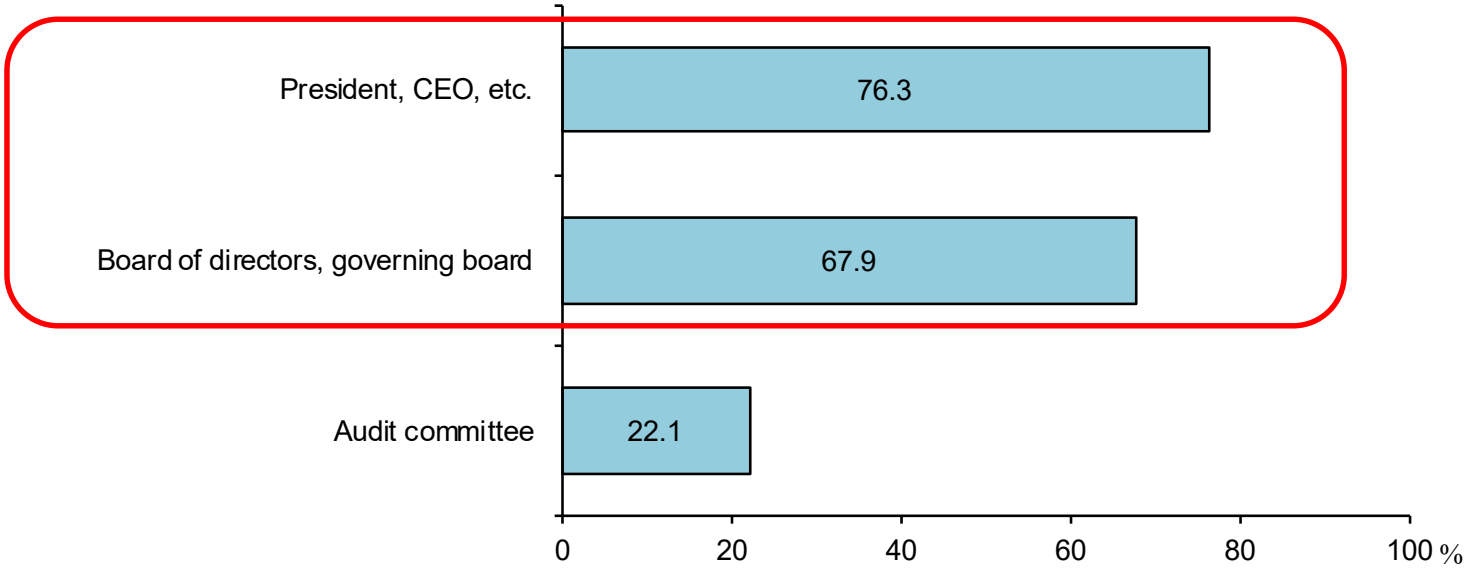


Summary of the Results　1. Involvement of Executives (iii)

■ Audit concerning cybersecurity

✓ The results of an audit concerning cybersecurity are mostly reported to executives.

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

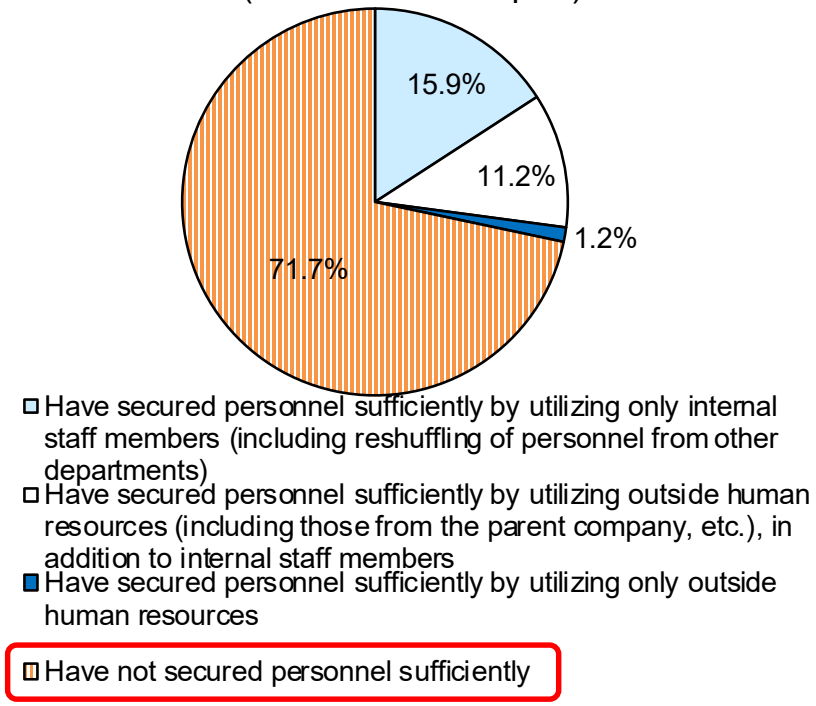


Summary of the Results　1. Involvement of Executives (iv)

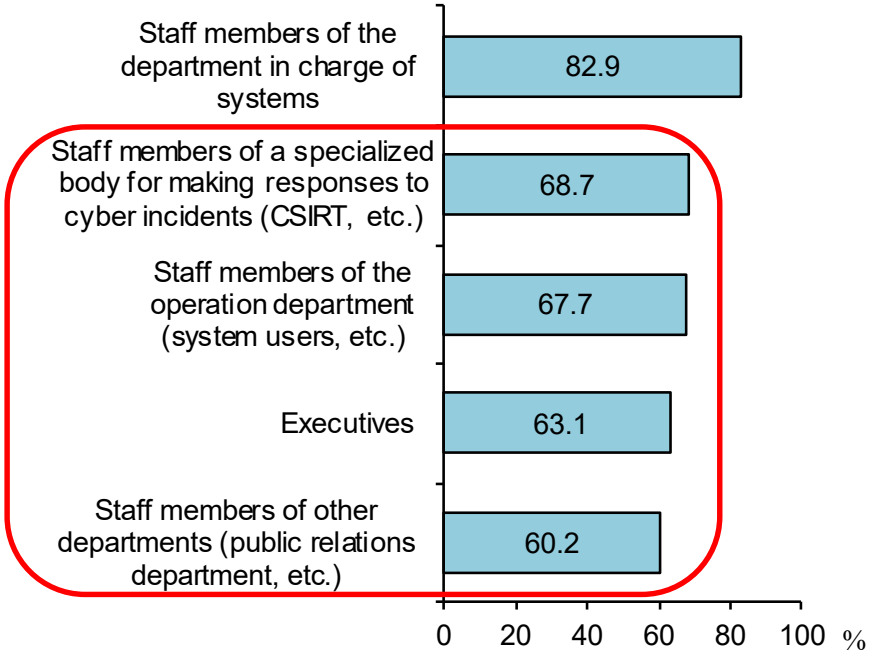
■ Frameworks for securing cybersecurity human resources

- ✓ Over 70% of the respondents answered that they have not sufficiently secured personnel who can assess cybersecurity risks that may arise on introducing new digital technologies.
- ✓ Regarding the staff targeted for e-learning for raising awareness concerning cybersecurity, which is one of the measures for fostering and strengthening human resources, over 80% of the respondents include staff of the department in charge of IT systems, but only around 60% to 70% of them target executives or other staff.

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



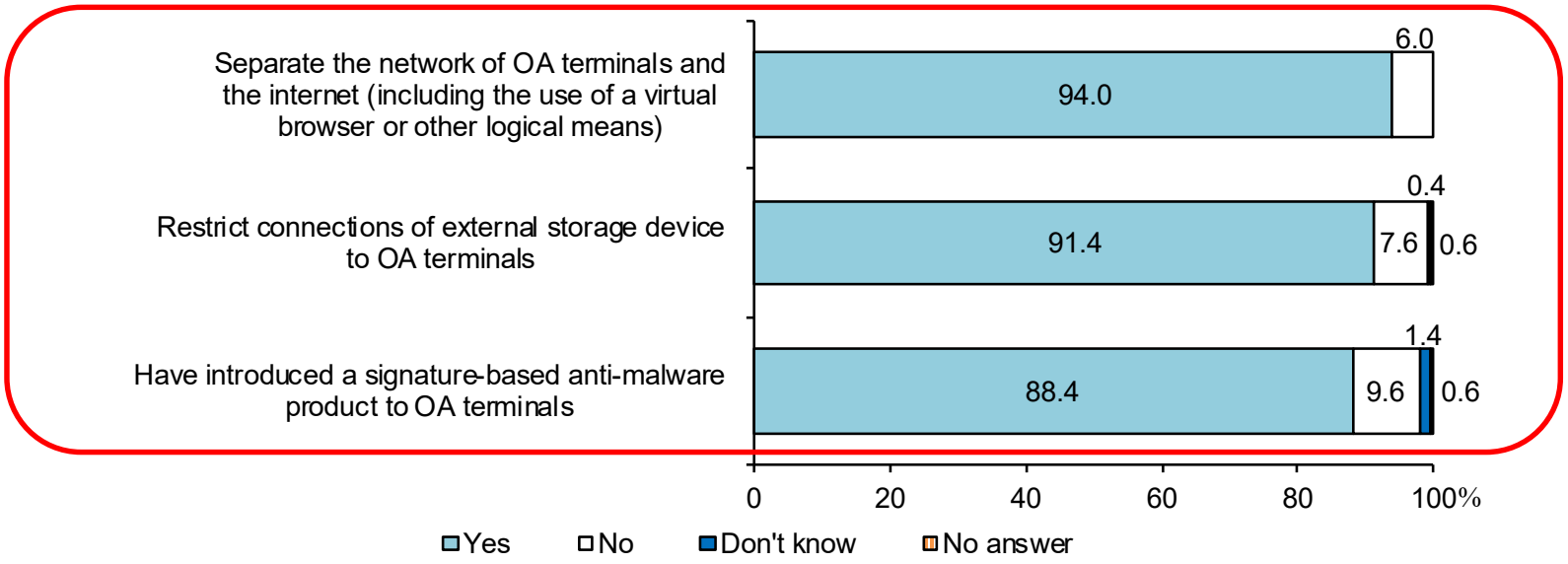
Staff targeted for e-learning (including learning using videos and documents, etc.) for awareness-raising (Chart 9. in the report)



■ Technical measures against cyberattacks

✓ As measures against cyberattacks taken for OA terminals, 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.

Measures against cyberattacks taken for OA terminal (Chart 10. in the report)

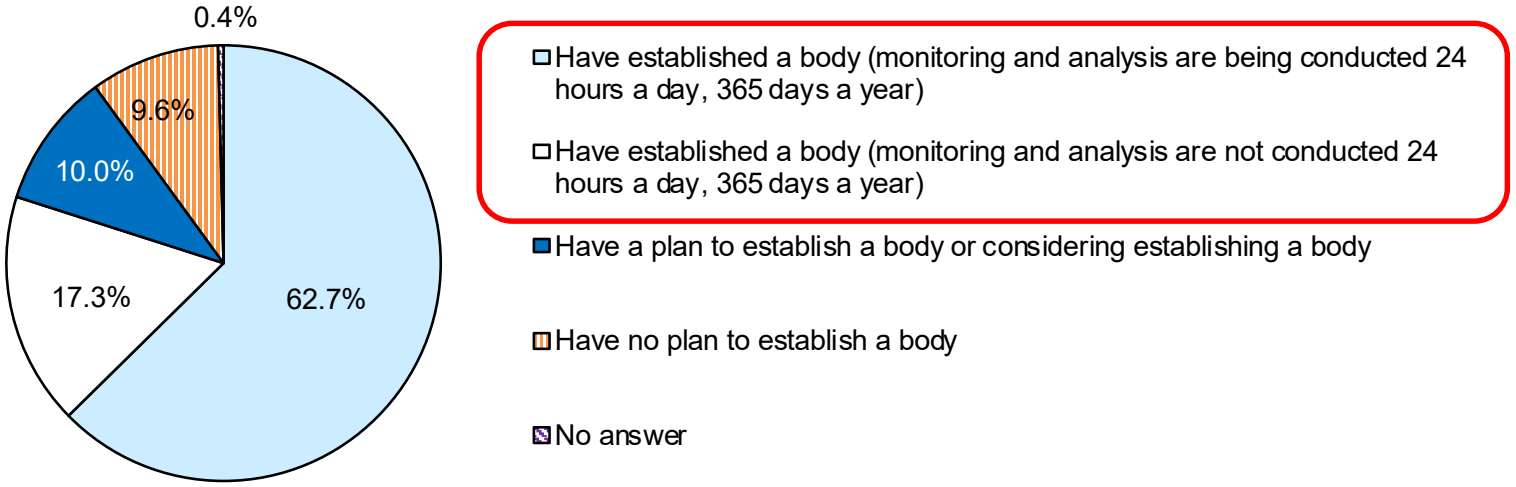


Note: For the current CSSA, "OA terminals" are defined as "standard terminals that staff members normally use for preparing documents, etc."

■ Structures for monitoring and analyzing cyber incidents

✓ Nearly 80% of the respondents answered that they have established a body that conducts monitoring and analysis of cybersecurity-related issues (SOC).

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

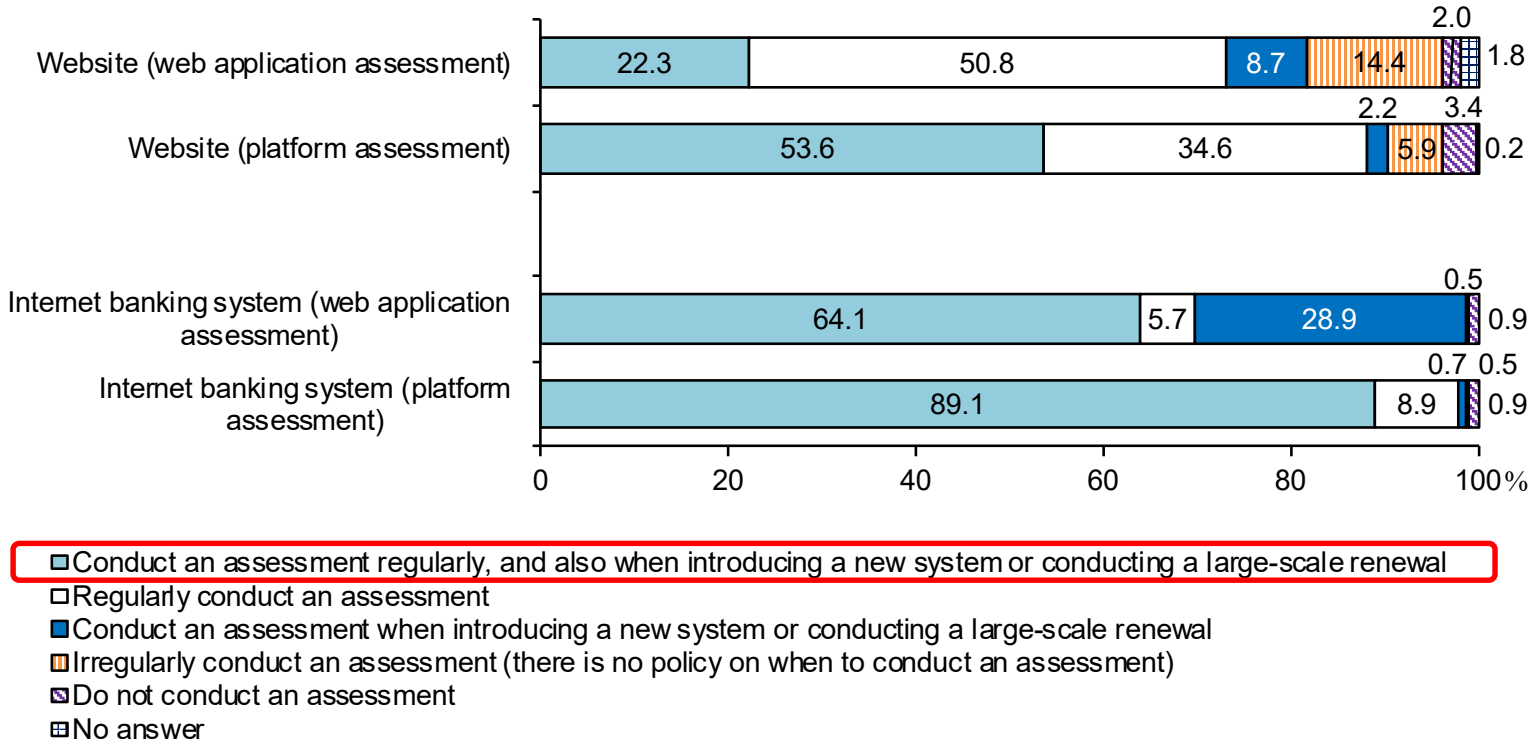


Note: SOC is the abbreviation of Security Operation Center. It is a body in charge of monitoring and analyzing cybersecurity-related issues, such as the status of attacks to the network or equipment, including a server and a firewall.

■ Management of system-related assets and measures against vulnerability

✓ Many of the respondents answered that they are conducting a vulnerability assessment regularly even after introducing a system.

Status of conducting vulnerability assessments, etc. (Chart 14. in the report)



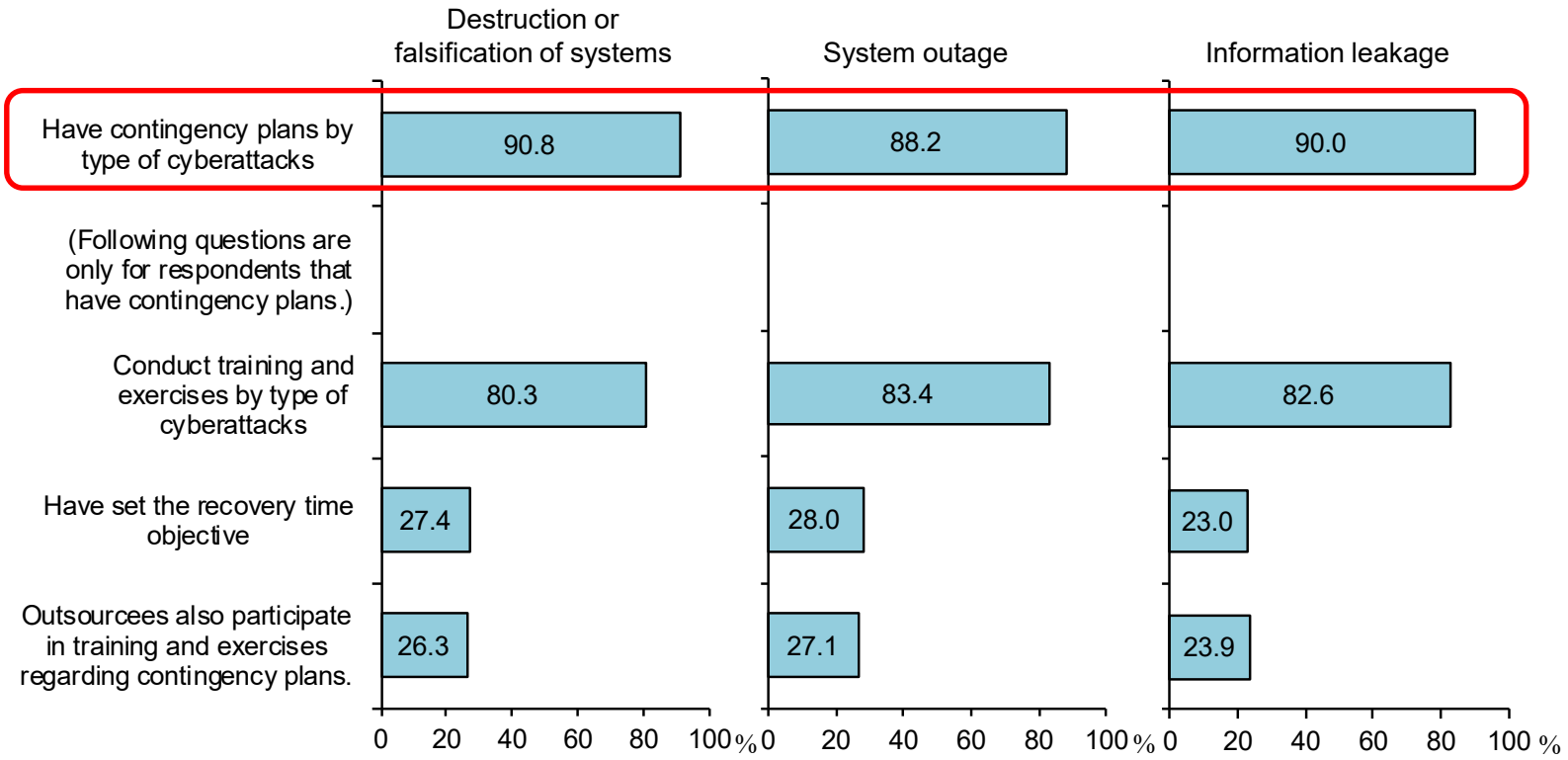
Note: Answers that they conduct an assessment, etc. include cases where they outsource system operations and check the outsourcees' implementation of an assessment, etc.

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

■ Formulation of contingency plans and implementation of training and exercises

✓ Most of the respondents have formulated plans by type of cyberattacks.

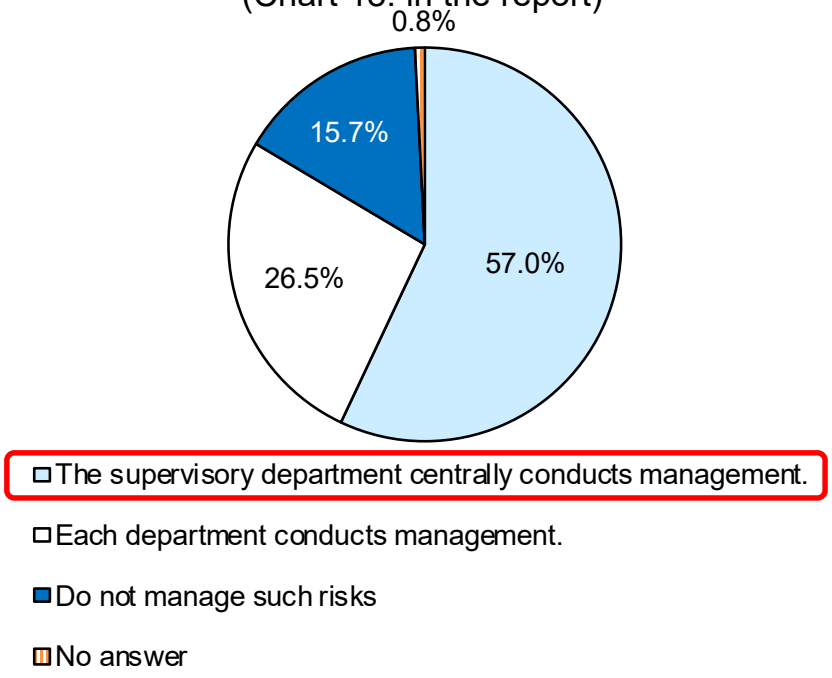
Contingency plans against cyberattacks (damage) and concrete measures (Chart 16. in the report)



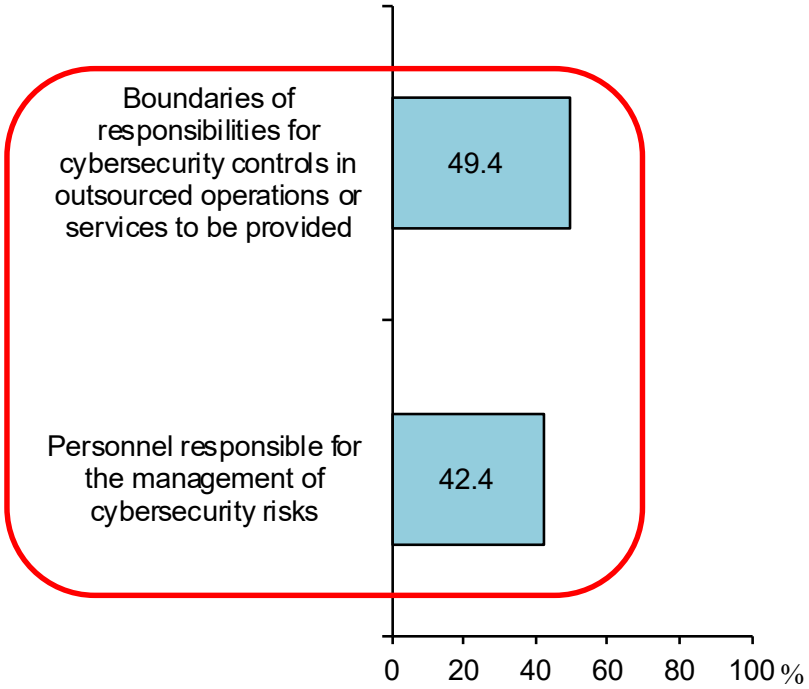
■ Measures against third-party risks

- ✓ Over 50% of the respondents answered that their supervisory department centrally manages cybersecurity risks relating to important third parties.
- ✓ More than a few respondents answered that they have not decided the boundaries of responsibilities for cybersecurity or that they have not appointed personnel responsible for the management of cybersecurity risks.

Status of managing cybersecurity risks for important third parties and services provided by them (Chart 18. in the report)



Matters decided in agreements, etc. with outsourcees (Chart 19. in the report)



Note: 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."

Conclusion

- ✓ While financial institutions are enhancing customer services and promoting operational reforms by utilizing digital technologies, the threat of cyberattacks is becoming even larger. 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 measures.
- ✓ 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. On the other hand, they also have challenges in securing and fostering cybersecurity human resources and managing third-party risks.
- ✓ 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.