[Summary]
Results of the Cybersecurity Self-Assessment for Securities Companies (FY2023)

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:	Developed a tool (a check sheet) for conducting a self-assessment of cybersecurity management posture, requested securities companies to assess their own cybersecurity frameworks, and fed back the overall results to them. This is the first time for securities companies
✓ Organizer:	The Bank of Japan (BOJ), the Securities and Exchange Surveillance Commission (SESC), and the Financial Services Agency (FSA)
✓ Subjects:	272 securities companies (members of the Japan Securities Dealers Association as of the end of June 2023)
✓ Period:	Self-assessments for securities companies were conducted in July to August 2023, and the overall results were returned in November 2023.

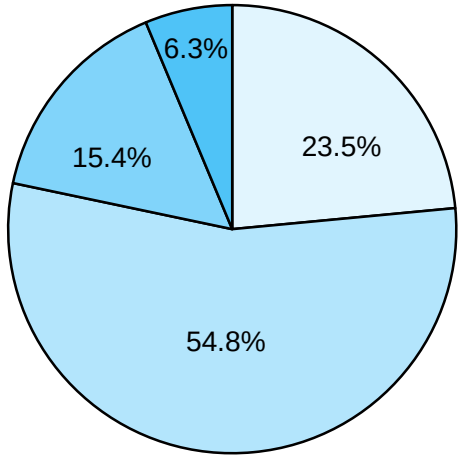
The status of securities companies' cybersecurity measures observed from the results of the CSSA is summarized below.

(Note) As values in the graphs are rounded to one decimal place, the percentages may not add up to 100.

Summary of the Results: Formulation of Management Policies and Management Plans

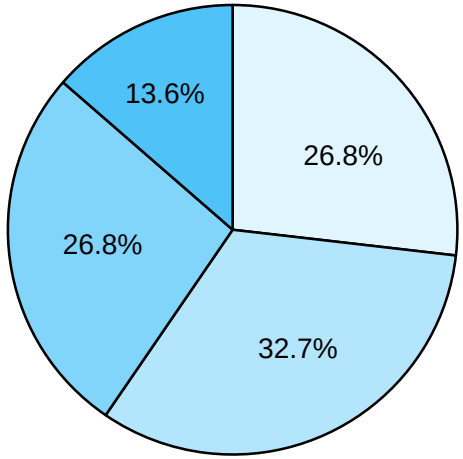
- ✓ In promoting a digitalization strategy to enhance customer services and promote operational reforms, it is necessary to concurrently develop cybersecurity management posture. With the involvement of the chief executive, it is important for securities companies to set up a management policy incorporating cybersecurity and formulate concrete plans. This includes how to allocate management resources in relation to cybersecurity, which is a precondition for a digitalization strategy. It is important to implement those plans as organization-wide efforts, instead of leaving them solely to the IT department.
- ✓ A certain number of the respondents have not set up a management policy incorporating cybersecurity, and/or have not formulated management plans (accounting to 20% and 40%, respectively) (Chart 1 and Chart 2).

Chart 1: Formulation of management policies concerning cybersecurity



- 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

Chart 2: Formulation of management plans concerning cybersecurity



- 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: Reporting to Personnel in Charge of Cybersecurity

- ✓ It is important to report the information on recent trends of cyber threats, including those of other companies' incidents, to executives* in fostering an organizational culture to facilitate checking of the status of the organization's measures.
- ✓ Many of the respondents answered that one of their executive officers is in charge of the cybersecurity of the organization (Chart 3). They periodically report cyber incidents that occurred within the organization to those in charge of cybersecurity. On the other hand, it was found that fewer respondents periodically report other companies' incidents (Chart 4).

Chart 3: Personnel in charge of cybersecurity

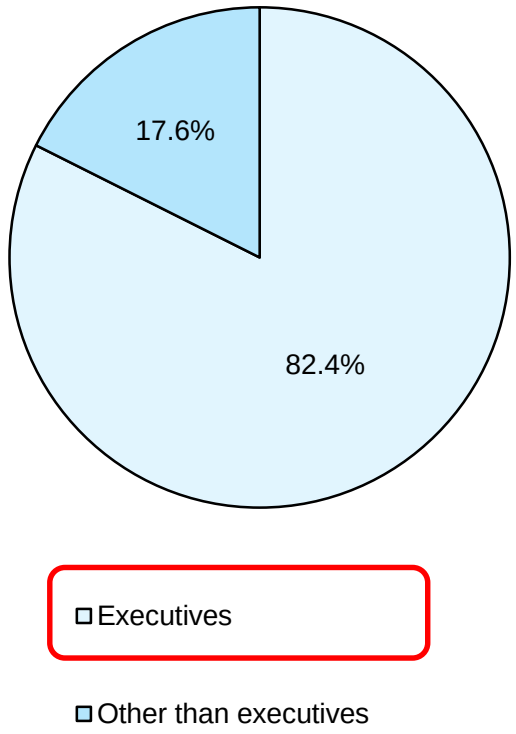
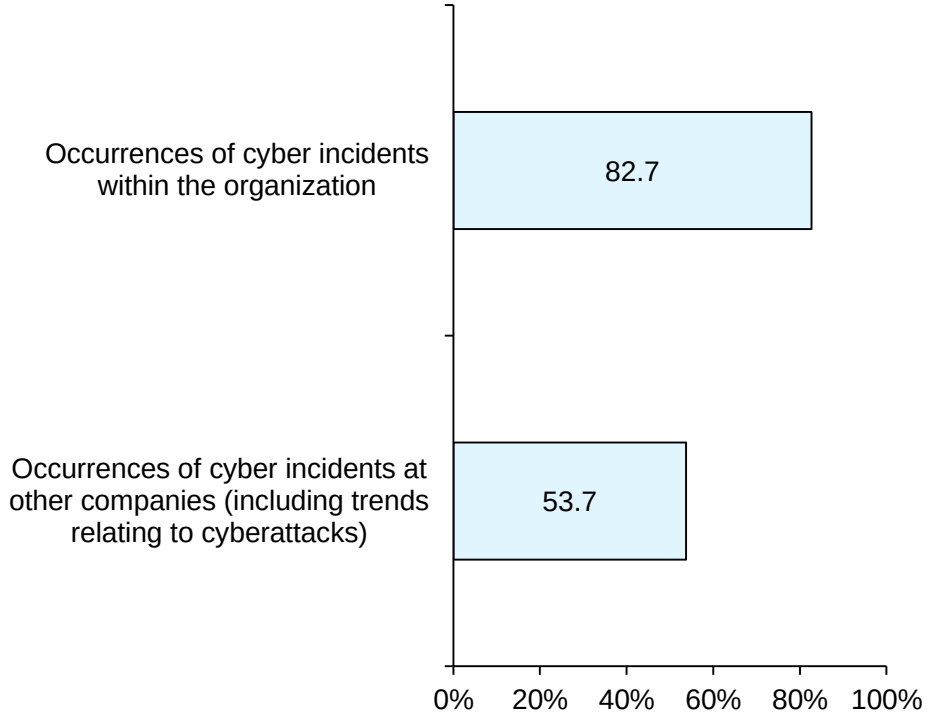


Chart 4: Contents periodically reported to the personnel in charge of cybersecurity



*An executive includes an executive officer whose position is non-statutory.

Summary of the Results: Risk Management and Involvement of Executives

- ✓ In order to properly respond to cyberattacks, it is important to assess cyber risks and take measures to mitigate those risks. Around 60% of the respondents conduct assessments of cyber risks of their material systems* regularly and when introducing a new system or conducting a large-scale renewal (Chart 5).
- ✓ Regarding risks that remain after assessing cyber risks and taking measures to mitigate them, countermeasures (including whether or not to accept those remaining risks) should be decided as judged by executives, depending on their significance. However, only around 30% of the respondents answered that policies for responding to remaining risks are decided based on the judgement of their executives (Chart 6).

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

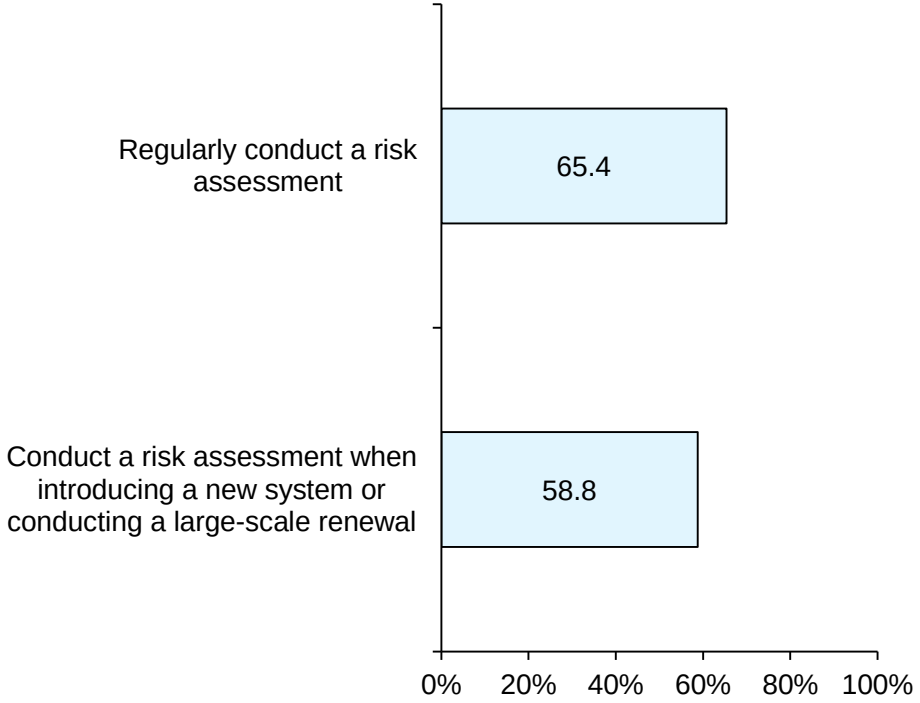
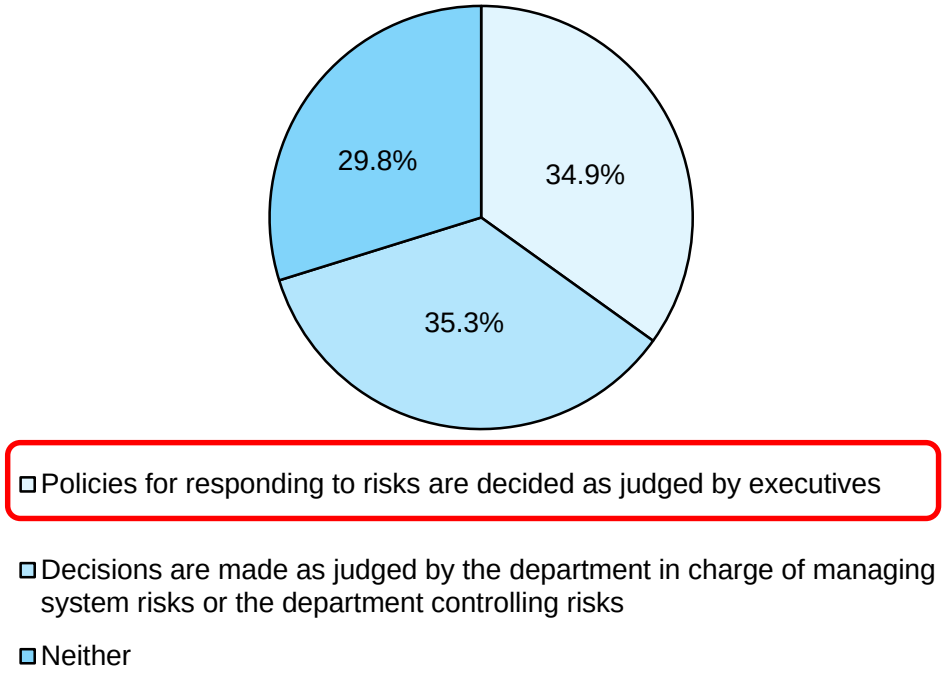


Chart 6: Decision maker for response policies based on risk assessments

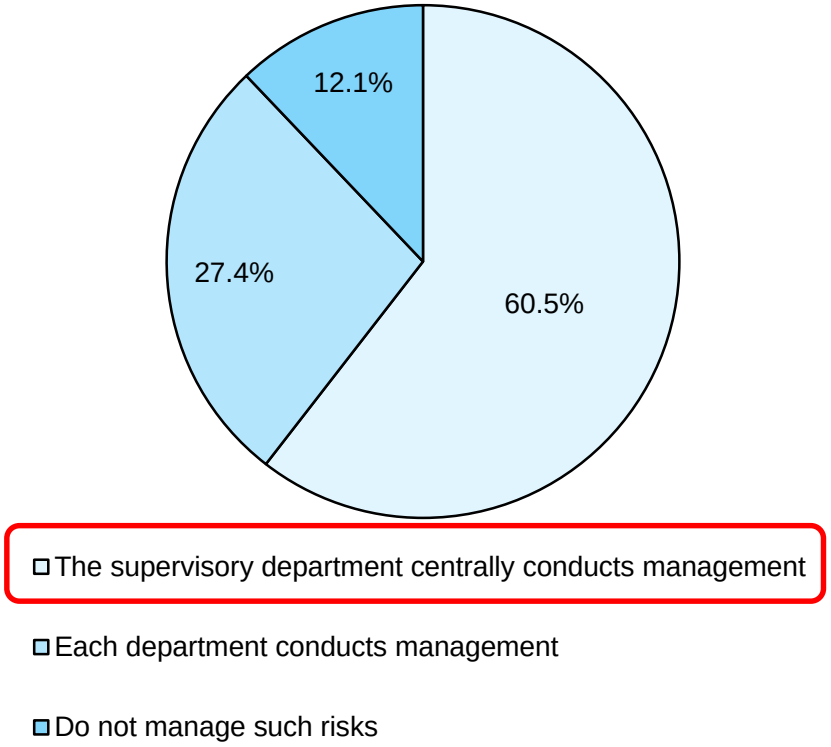


* For the purpose of this CSSA, "material systems" are defined as "accounting systems, systems handling customer information, or other systems that an organization recognizes as especially important in its business operations."

Summary of the Results: Controls against Third-Party Risks

- ✓ It is important to appropriately manage supply chains that support digital business as they become broader and increasingly complicated in recent years. In particular, it is important to develop posture for cross-organizational and centralized management of important third parties* to prevent the responsibility and the viewpoint for management from becoming blurred.
- ✓ Only around 60% of the respondents that have important third parties centrally manage them. A certain number of the respondents do not manage third party risks at all (Chart 7).

Chart 7: Status of managing cybersecurity risks for important third parties and services provided thereby

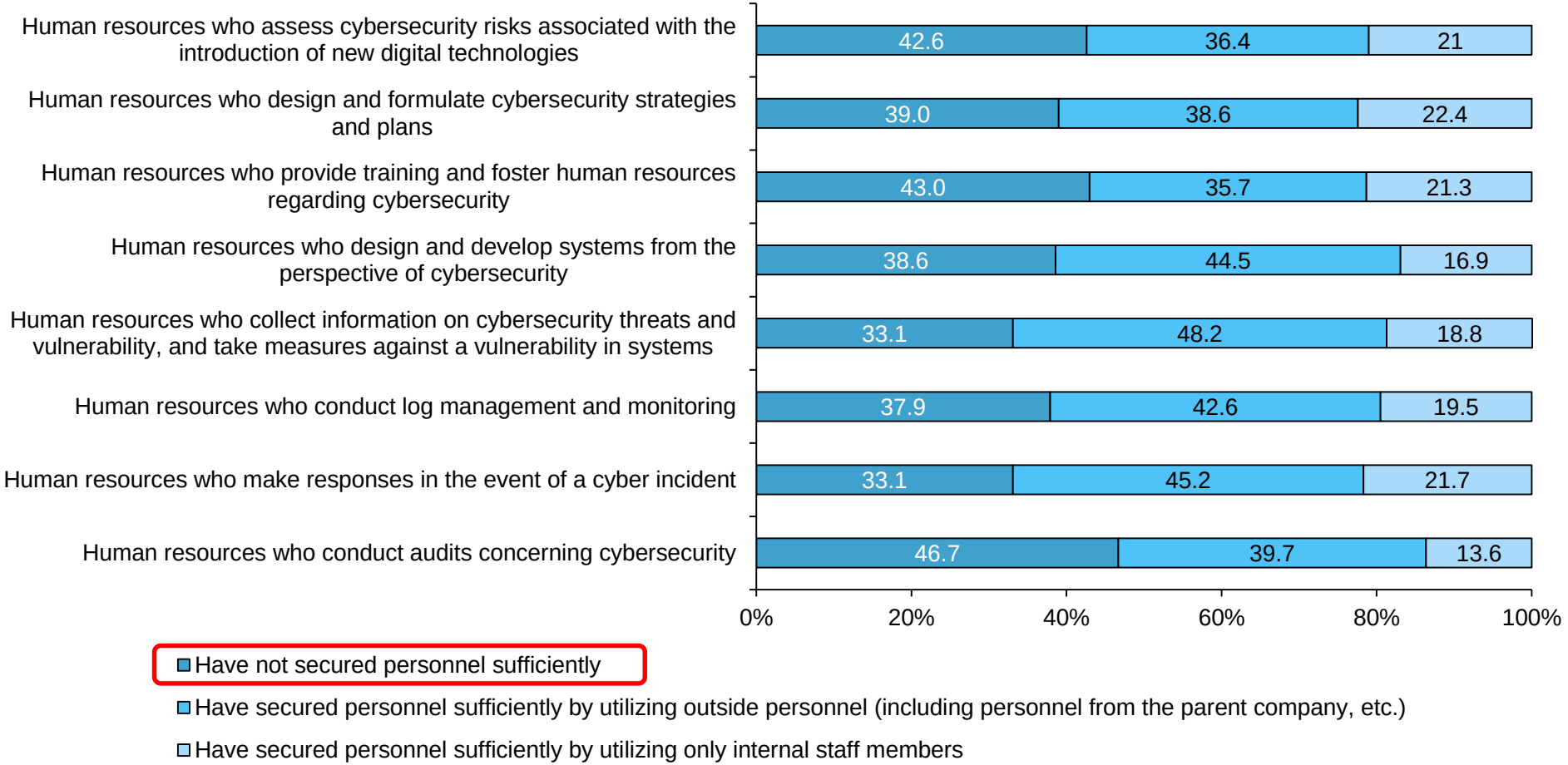


* For the purpose of this CSSA, an "important third party" is defined as a "third party which the organization recognizes as being important for its business operations." A "third party" is defined as "another organization with which the organization has a business relationship or has concluded an agreement, etc. for providing services" (e.g. an 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).

Summary of the Results: Securing Cybersecurity Human Resources

- ✓ It is necessary to secure cybersecurity human resources with knowledge in order to assess cybersecurity risks, respond to cybersecurity incidents, and conduct appropriate cybersecurity audits.
- ✓ As shown in Chart 8, certain percentages of the respondents are aware that they have failed to secure sufficient staff for all fields and functions.

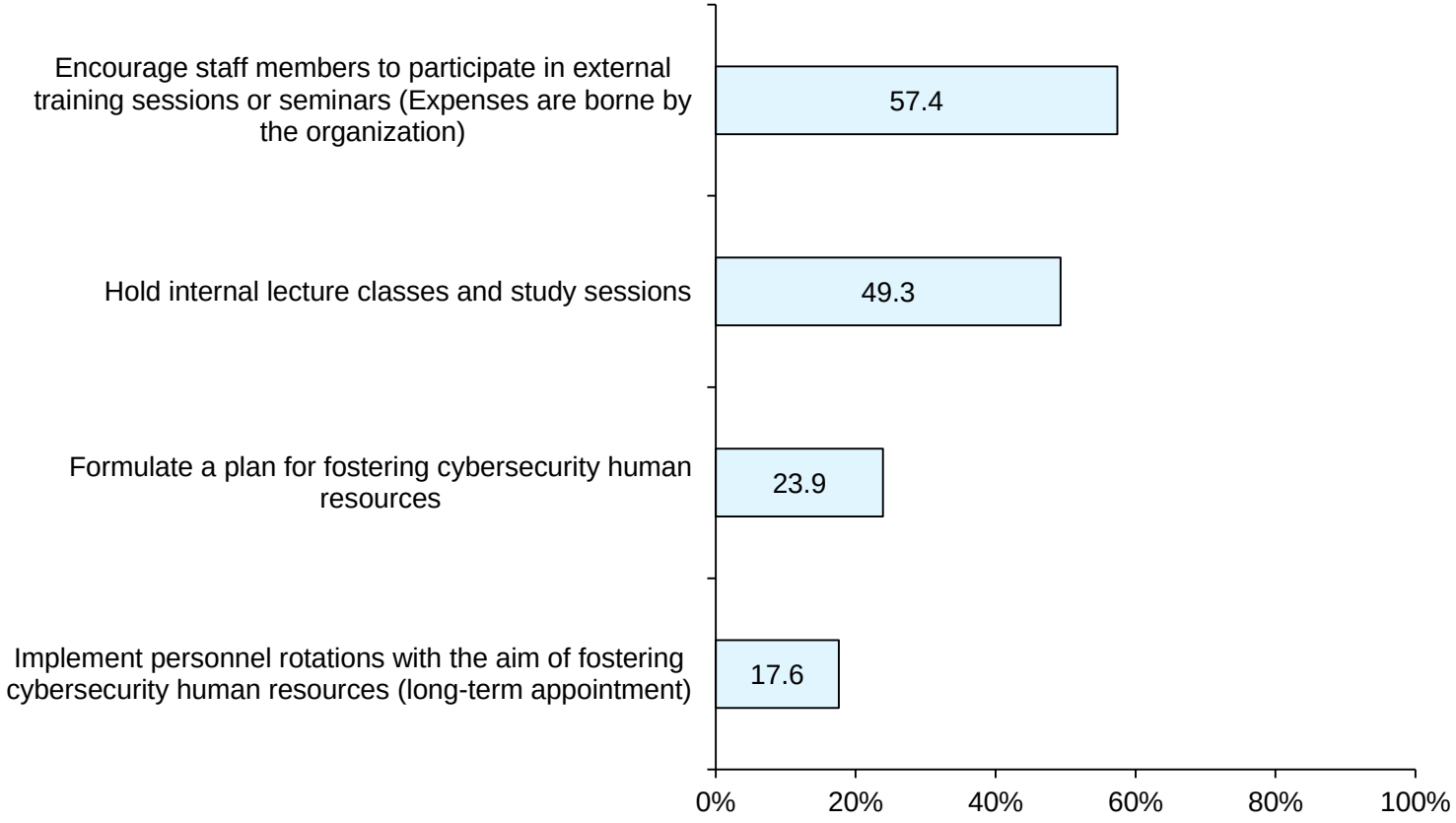
Chart 8: Status of securing cybersecurity human resources by function



Summary of the Results: Fostering Cybersecurity Human Resources

- ✓ As a shortage of cybersecurity human resources is expected to continue, it is important to foster cybersecurity human resources and bottom-up their abilities within the organization from a medium- to long-term perspective.
- ✓ Efforts for fostering human resources are centered on those from a short-term perspective, such as encouraging staff members to participate in external training sessions or seminars, or to obtain cybersecurity-related qualifications, or holding internal lecture classes and study sessions. The number of respondents that are making medium- to long-term efforts, such as formulating a human resources development plan, are limited.

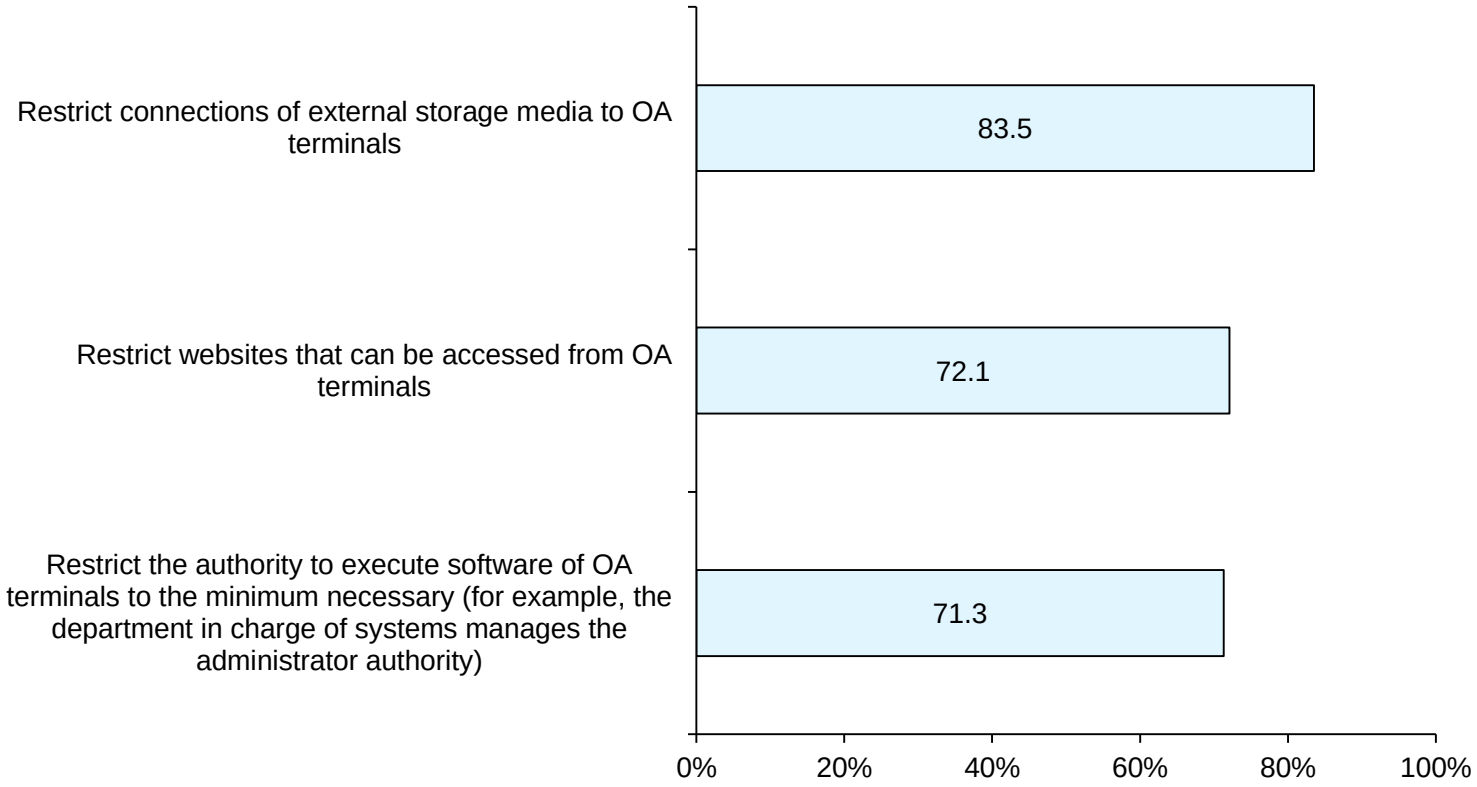
Chart 9: Efforts for fostering human resources



Summary of the Results: Controls against Cyberattacks Taken for OA Terminals

- ✓ Countermeasures against cyberattacks targeting OA terminals* should be put in place on the premise that the possibility of infection with unknown malware or penetration by attackers abusing a vulnerability in systems cannot be eliminated completely.
- ✓ Around 80% of the respondents restrict connections of external storage devices to OA terminals. Around 70% of the respondents restrict websites that can be accessed from OA terminals and the rights to run software of OA terminals.

Chart 10: Controls against cyberattacks taken for OA terminals



*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: Posture for Monitoring and Analyzing Cyber Incidents

✓ Around 70% of the respondents answered that they have established a body (i.e. SOC*) that conducts monitoring and analyses of cybersecurity-related issues (Chart 11). Around 90% of the respondents are monitoring the status of the detection of or the infection with malware. Around 70% of the respondents are monitoring communications to the outside (Chart 12). Securities companies are encouraged to further expand the scope of systems to be monitored and enhance the quality of their monitoring.

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

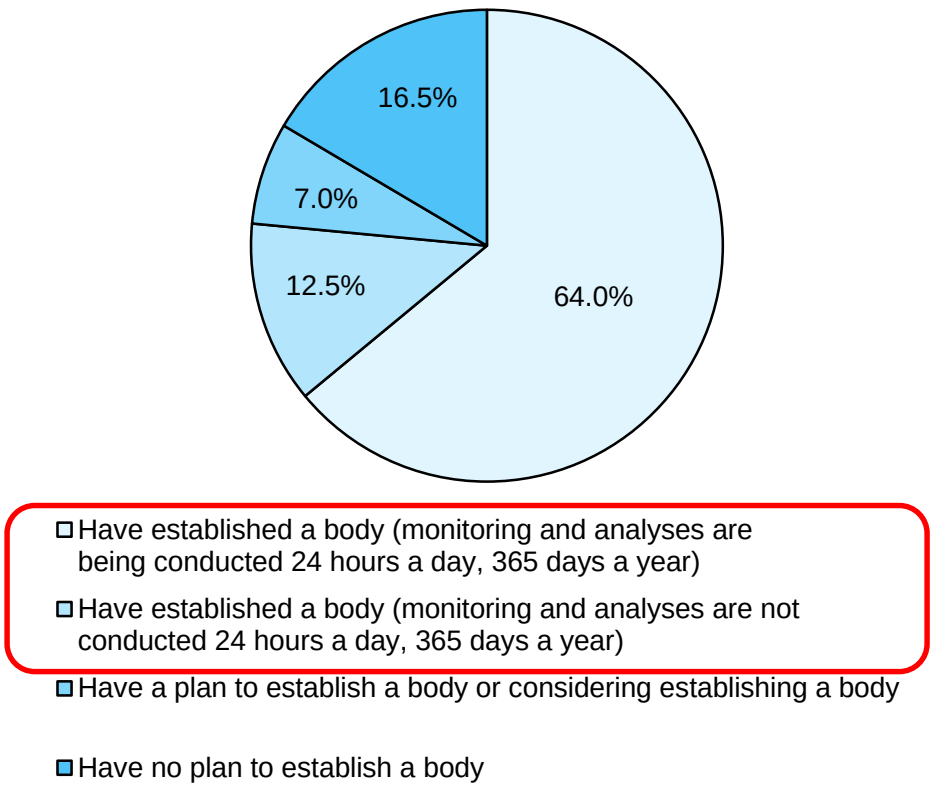
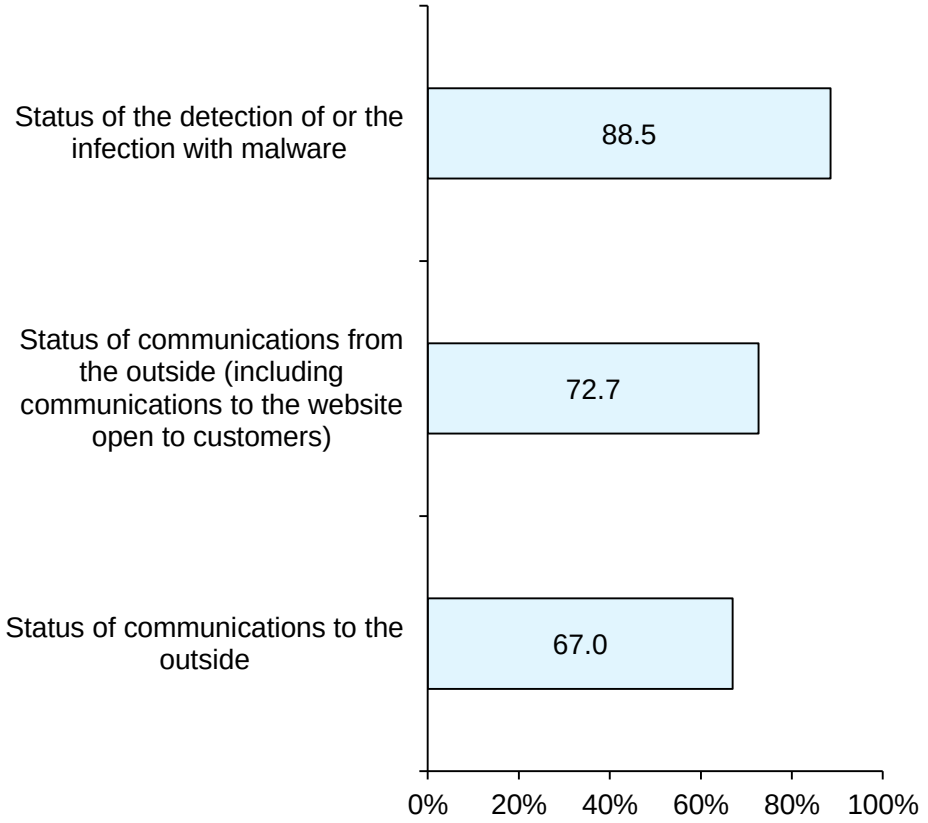


Chart 12: Coverage of monitoring by an SOC or other department that monitors cybersecurity-related issues

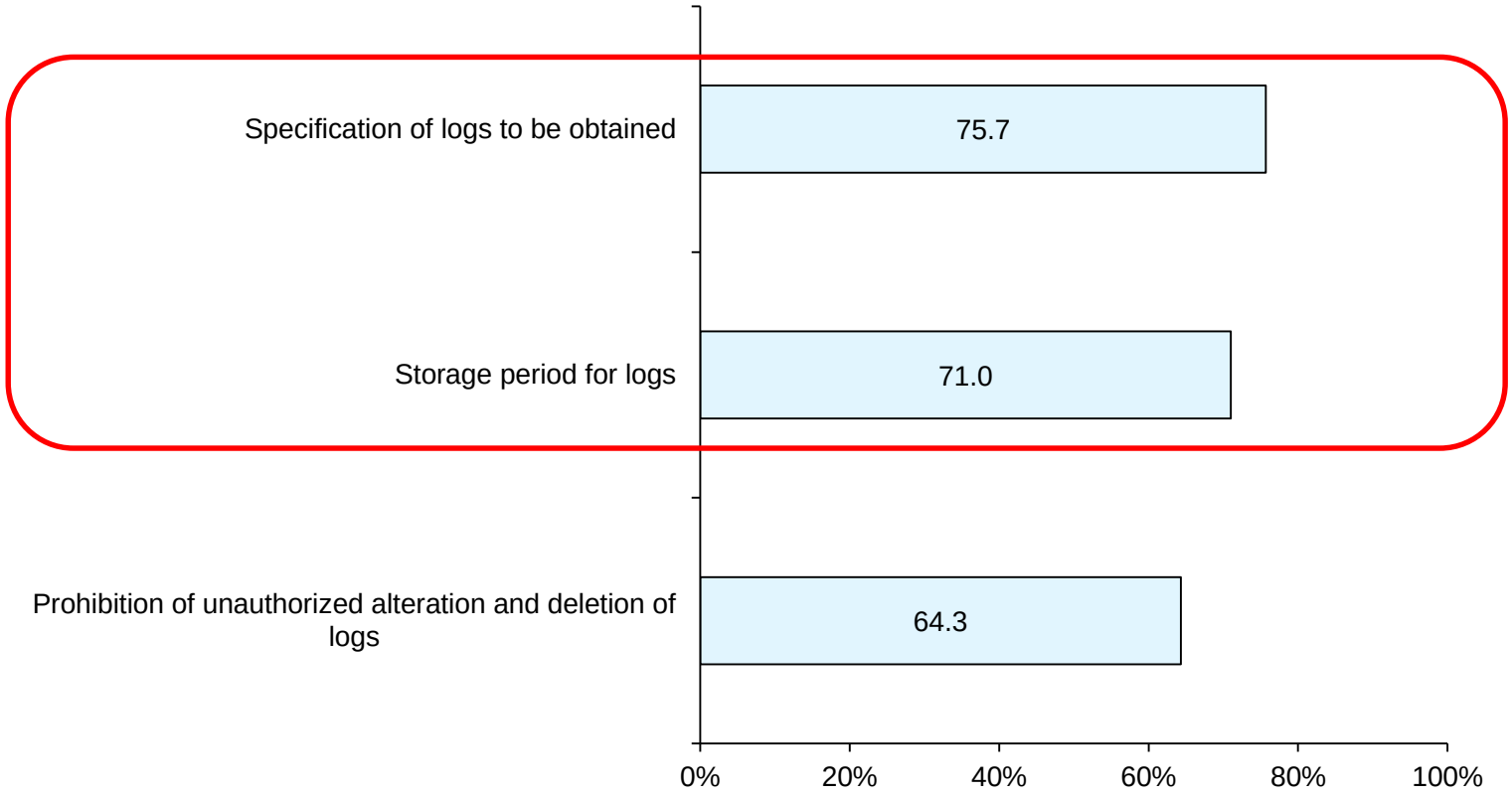


* Abbreviation of Security Operation Center; A center to monitor and analyze cybersecurity-related situations, such as attacks to networks, servers, or firewalls, etc.

Summary of the Results: Provisions Regarding System Logs

- ✓ It is important to ensure the accuracy and comprehensiveness of system logs because they are indispensable for detecting cyber incidents, examining the extent of the impact of cyber incidents, and considering measures for recovery.
- ✓ Around 70% of the respondents have formulated rules and procedures concerning specifications of logs to be obtained and a storage period of logs.

Chart 13: Matters prescribed regarding logs (audit trails) for material systems

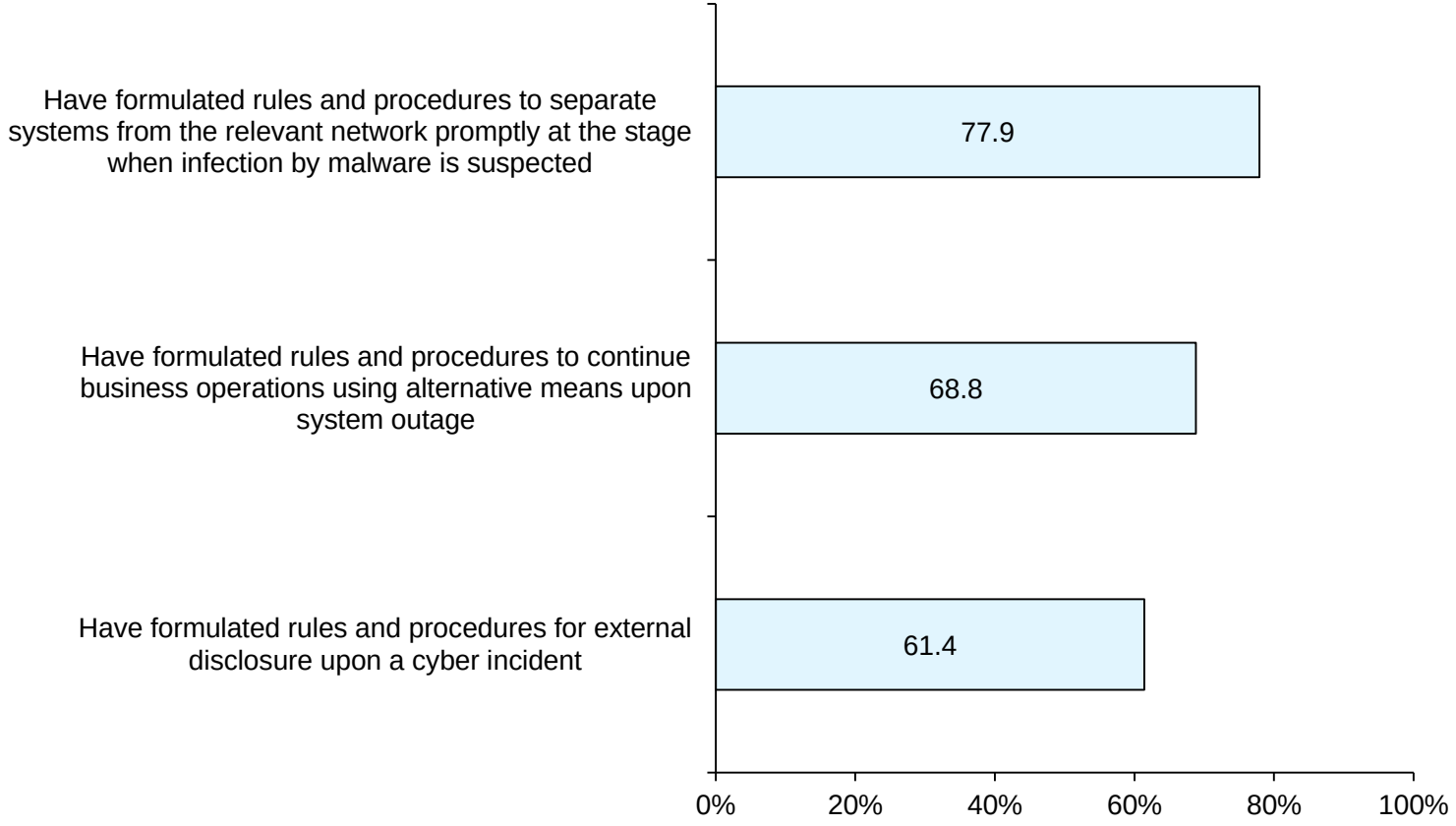


* Compiled the results for the respondents who chose "Have formulated rules and procedures and are conducting monitoring" and "Have formulated rules and procedures"

Summary of the Results: Development of Procedures for Measures to Prevent the Spread of Damage

- ✓ In the event of a cyber incident, it is important to endeavor to resume operations promptly, while taking measures to prevent the spread of damage. Securities companies need to develop posture for this.
- ✓ A certain number of the respondents have formulated rules and procedures for promptly separating systems from the relevant network at the stage when infection by malware is suspected, continuing business operations using alternative means, and externally disclosing information upon a cyber incident.

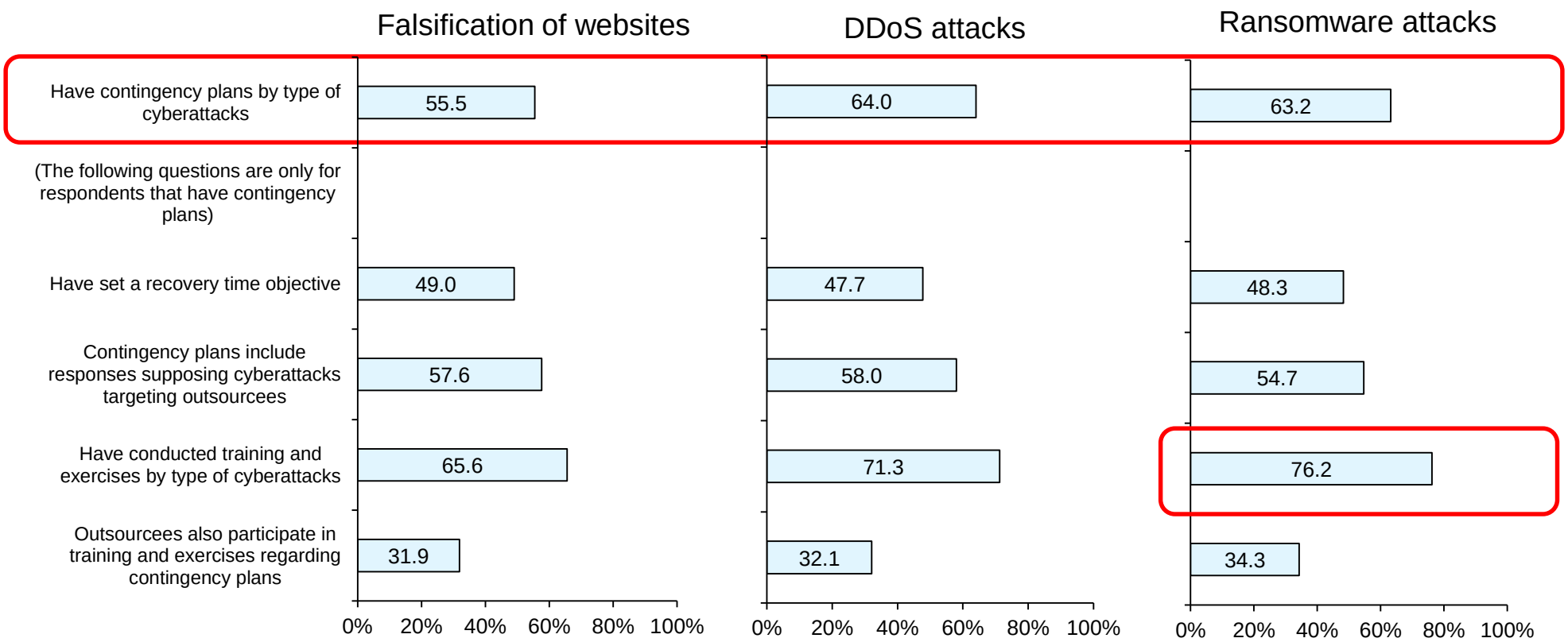
Chart 14: Status of formulating rules and procedures to prevent the spread of damage



Summary of the Results: Formulation of Contingency Plans and Implementation of Training and Exercises

- ✓ It is desirable for securities companies to formulate contingency plans by type of cyberattacks in advance so that they can make responses and recover business operations appropriately in the event of a cyberattack. As shown in Chart 15, a certain number of the respondents have not formulated contingency plans by type of cyberattacks.
- ✓ It is important to check the effectiveness of contingency plans through training and exercises. For ransomware attacks, nearly 80% of the respondents that have formulated contingency plans conduct training and exercises.
- ✓ It is of importance to formulate a practical contingency plan by envisaging the possibility that cyberattacks targeting outsourcees may exert influence on the organization and setting a realistic recovery time objective based on the organization's system environment.

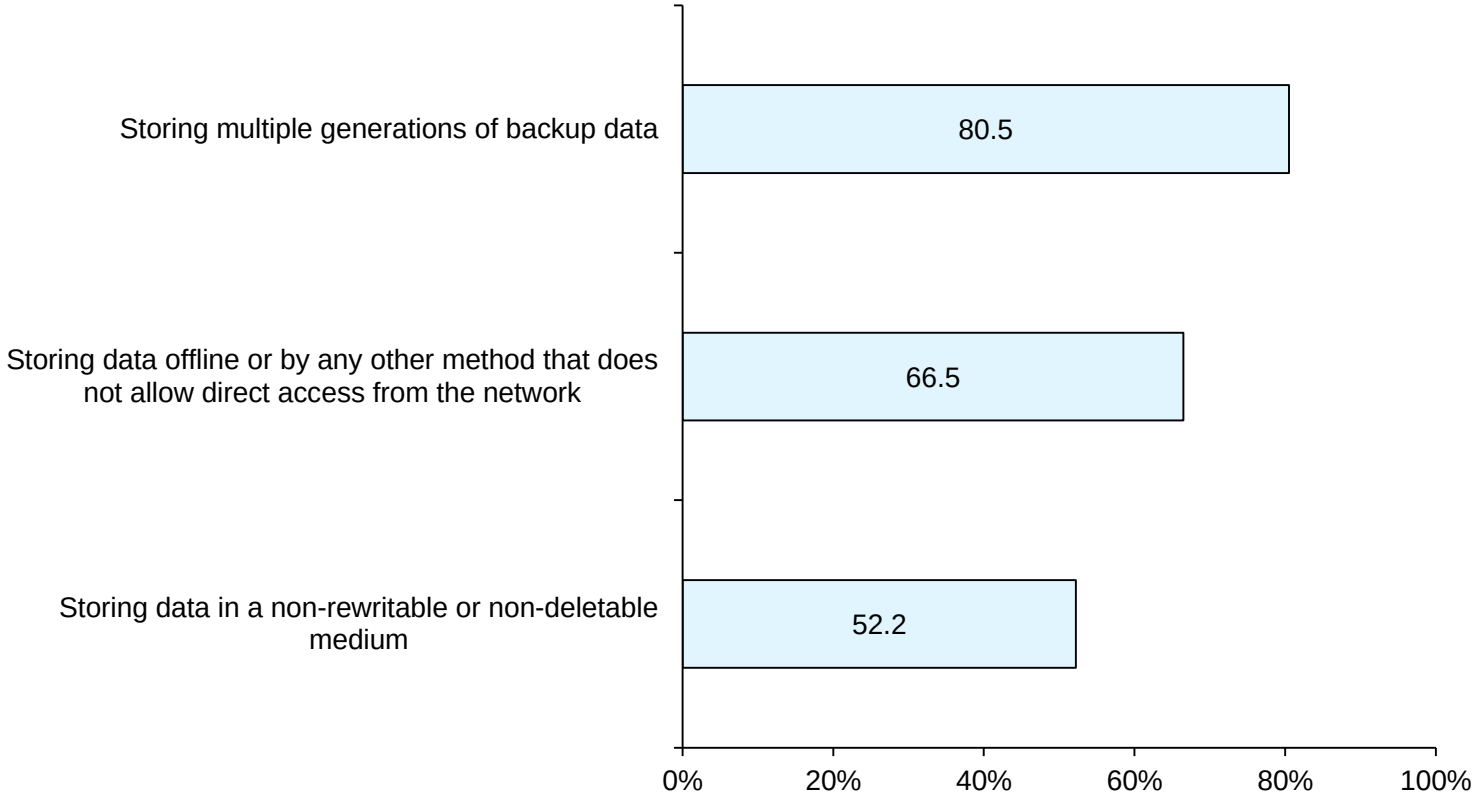
Chart 15: Contingency plans against cyberattacks (damage) and concrete measures



Summary of the Results: Protection of Backup Data

- ✓ It is important to put in place countermeasures against destruction of data in order to make it possible to recover systems by using backup data and achieve early resumption of business operations.
- ✓ Around 80% of the respondents store multiple generations of backup data. A certain number of the respondents answered that they store data by a method that does not allow direct access from the network or store data in a non-rewritable or non-deletable medium.

Chart 16: Measures in consideration of the possibility of destruction or falsification of backup data in material systems



* Compiled the results for the respondents who chose "Have formulated rules and procedures and are conducting monitoring" and "Have formulated rules and procedures"

Conclusion

- ✓ The threat of cyberattacks is becoming even larger as financial institutions are enhancing customer services and promoting operational reforms by utilizing digital technologies and hence are increasing their activities in cyberspace. It is therefore important for financial institutions to recognize the growing threat and continue efforts for developing better cybersecurity management posture and securing their effectiveness.

- ✓ Many of the securities companies 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, it was indicated that there is still room for improvement in their management of cybersecurity risks relating to important third parties, securing and fostering of cybersecurity human resources, and formulation of contingency plans.

- ✓ Considering such circumstancesthe CSSA is envisaged to be conducted annually in and after fiscal 2024, while updating the questions in light of environmental changes.

- ✓ The FSA expects that securities companies 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.