Summary of Financial Sector Cybersecurity Report (June 2020)

Background

- Based on "The Policy Approaches to Strengthen Cybersecurity in the Financial Sector" (updated in October 2018), the government and private sectors have worked in cooperation to strengthen cybersecurity in the financial sector.
- This Report publishes current status and common challenges identified in the course of conducting monitoring during PY(Program Year) 2019 based on the Policy Approaches.

1. Current situation with cybersecurity in the financial sector

(1) Threats in recent years

- Although FIs in Japan have not experienced any large-scale cyber incident that caused the entire financial system to break down, **customers have been invited to visit fake websites of FIs and others to heist cash or credit card information**.
- FIs overseas have experienced **large-scale cyber incidents leading to personal information leaks or service outage**.

(2) Cyber incidents at FIs in Japan

- Cyber incidents of **unauthorized logins through list-based attacks and DDoS attacks** were frequently reported from FIs. To prevent similar incidents from occurring at other FIs, the JFSA **issued warnings to FIs** in October 2019, asking them to take relevant measures.
- The JFSA need to **timely identify and analyze emerging threats and vulnerabilities** and encourage FIs to enhance cybersecurity management systems in the financial sector.

(3) Impacts of COVID-19 on cybersecurity

- **Many cyber attacks taking advantage of the COVID-19 pandemic and targeting telework environments are reported.**
- While FIs in Japan have faced no major problems, **FIs should pay attention to security measures as new workstyles using telework and the digitalization of financial services are expected to make further progress in the financial sector.**

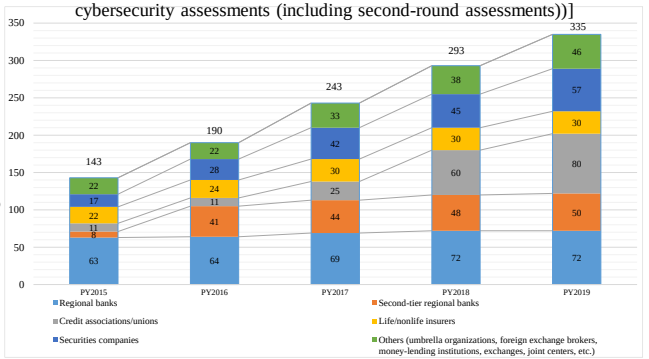
2. Current initiatives to strengthen cybersecurity in the financial sector (1/3)

(1) (i) Cybersecurity countermeasures as usual

(a) Small and medium financial institutions

- ✓ As for small and medium FIs, the FSA has so far verified the status of basic cybersecurity management system development through cybersecurity assessments (monitoring through dialogues).
- ✓ In PY2019, the JFSA sought to upgrade cybersecurity in the financial sector by conducting cybersecurity assessments mainly for small and medium FIs that are feared to delay the development of basic cybersecurity management systems.

[Trend of cybersecurity assessments by business type (total numbers of FIs subjected to cybersecurity assessments (including second-round assessments))]



Business type	Outline of initiatives
Regional banks and credit associations/unions	• While some of these FIs have voluntarily strengthened cybersecurity, others **still had challenges in developing basic cybersecurity management systems**. • The JFSA has encouraged FIs with challenges to **develop cybersecurity promotion arrangements under senior executives' leadership**.
Securities companies, etc.	• While a rising number of these FIs have made progress in cybersecurity efforts, some FIs have **not still made enough progress**. • The JFSA has encouraged FIs with challenges to **develop cybersecurity promotion arrangements under senior executives' leadership**.

(b) Large financial institutions

- ✓ The JFSA has so far discussed cybersecurity with large FIs through regular dialogue with global trends in mind.
- ✓ In PY2019, the JFSA focused on the advancement of group-wide and global cybersecurity management systems and the use of TLPT.
- ✓ The JFSA used questionnaire surveys for off-site monitoring of Trust banks, Internet banks and etc.

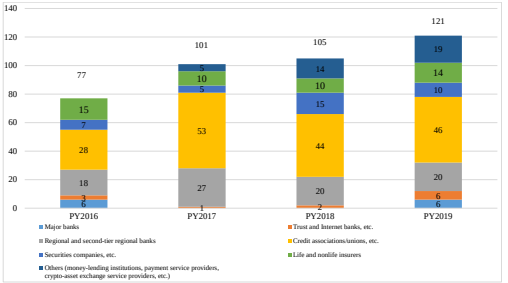
Business type	Outline of initiatives
Three mega-banks, etc.	• The three mega-banks and other large FIs are trying to **sophisticate unified group-wide and global cybersecurity management systems**. They are expected to **enhance cybersecurity management system by beefing up access control and cyber resilience**. • In a bid to make the TLPT more effective, they are expected to **continuously advance the assessment of incident response capabilities using various guidelines and international frameworks and to develop higher-level specialists**.
Trust banks and Internet banks, etc.	• Some of these FIs have been promoting initiatives to advance cybersecurity. As some banks **had room for improvement in cybersecurity measures and the recognition of risks under the leadership of senior executives**, the JFSA shared challenges with them and encouraged them to make improvement through dialogues.

2. Current initiatives to strengthen cybersecurity in the financial sector (2/3)

(1) (ii) Incident responses

- The JFSA implements an annual Financial Industry-wide Cybersecurity Exercise called "Delta Wall" to improve FIs' incident response capabilities.
- In PY2019, a total of 121 companies (about 2,000 individuals) participated in the exercise to improve cybersecurity in the entire financial industry in the run-up to the Tokyo 2020 Olympics and Paralympics, including small, medium and large FIs as well as fund transfer service providers and others.
- As well as the JFSA, other various organizations perform a diversity of cybersecurity exercises. It is **important for FIs to improve incident response capabilities through participation in such exercises**.

[Number of cybersecurity exercise participants by business type (by year)]



Business type	Outline of Delta Wall IV results
Large and regional banks	• Large and regional banks in general were found capable to respond to incidents. However, **challenges were seen at some FIs in regard to the restoration of IT systems and communications with customers.** • Those found fully prepared to **respond to incidents should deepen inhouse discussions to further advance their incident response capabilities**.
Others	• **Other FIs generally had room to improve triage decisions on priority responses, communications with customers and consider how to prevent similar incidents**. • They are required to further improve their incident response capabilities.

(1) (iii) Strengthening management systems in anticipation of Tokyo 2020 Olympics and Paralympics

- In anticipation of the Tokyo 2020 Olympics and Paralympics, the JFSA has endeavored to strengthen FIs' cybersecurity management systems.

(a) Improving effectiveness of basic cybersecurity management systems

Business type	Outline of initiatives
Regional banks and credit associations/unions	• The JFSA **requested these FIs 1) to conduct vulnerability scan, 2) to conduct exercises and training and 3) to straighten out the status of monitoring/analysis by the end of March 2020**. • Most of these **FIs met the abovementioned three requests**. However, some lagged behind in responding to the requests. **The JFSA followed them up in cooperation with industry groups**.
Others (Major banks, trust banks, other banks, fund transfer service providers, securities companies, life/nonlife insurers, money-lending institutions, etc.)	• The JFSA checked whether these FIs met the abovementioned three requests. • Although no particular challenges were found, the JFSA will examine and follow up their relevant initiatives as necessary.

(b) Practices and challenges for improving effectiveness identified through request responses and questionnaire surveys

Requests	Good practices and challenges
Vulnerability scan	• While some FIs systematically implemented such scan based on their risks, others failed to do so due to their insufficient risk awareness.
Exercises and training	• While some FIs revised contingency plans through exercises and training, others failed to review their participation in exercises.
Monitoring/analysis	• While some FIs were prepared to quickly detect and analyze incidents, others were not ready to check or analyze incident logs.

2. Current initiatives to strengthen cybersecurity in the financial sector (3/3)

(1) (iv) Responses to accelerating digitalization

- In PY2019, the JFSA interviewed FIs in Japan and overseas as well as IT vendors to find out about and analyze progress in digitalization.

(a) Overall cloud services
- ✓ Large FIs are trying to promptly adopt new services and continuously upgrade skills through **training, the establishment of targets for the number of qualified employees, orientation meetings on new services and other events**.

(b) Transition to new security models
- ✓ Large FIs are **seriously adopting security countermeasures, taking the Zero Trust Security Model into account**.

(2) (i) Improving effectiveness of information-sharing frameworks

- As the JFSA has taken every opportunity to promote FIs' understanding about the significance of their "mutual help", **the number of FIs participating in Financials ISAC Japan has steadily increased**.
- FIs are expected to deepen "mutual help", including the provision of cybersecurity countermeasures, by **expanding cooperation with industry groups further** to strengthen cybersecurity. The JFSA will continue to proactively support such initiatives for "mutual help".

(2) (ii) Cooperation in responding to large-scale incidents

- The JFSA has exploited the Liaison Council for Cybersecurity Stakeholders (launched in June 2019) to enhance the entire financial sector's **cooperation arrangements through the development of cooperation procedures and cyber exercises** regarding large-scale incidents in anticipation of the Tokyo 2020 Olympics and Paralympics.
- The JFSA will check **the effectiveness of information sharing between Liaison Council members using an information sharing platform through exercises**.

(2) (iii) International cooperation

- In June 2019, a joint exercise to tackle an assumed large-scale cyber incident took place to **check cross-border cooperation** mainly between G7 authorities.
- Recent international discussions have covered **third parties including cloud services and resilience concept such as restoration or recovery from cyber incidents**. It is important to accurately **assess and respond to international trends** including such discussions.

3. Future JFSA initiatives

- Cyber risks surrounding FIs have increased further due to external environment changes accompanying the expanding COVID-19 pandemic and the postponed Tokyo 2020 Olympics and Paralympics.
- The JFSA will promote primarily the following initiatives to further strengthen cybersecurity countermeasures in the financial sector:

Responses to financial sector environment changes

- While digitalization makes progress in the financial sector, a shift to online and remote services is accelerating in response to the COVID-19 pandemic, leading the financial sector environment to turn around. Cybersecurity has become an even more important challenge as the premise for such new financial services and infrastructure.
- The JFSA will **proactively collect information** on emerging security threats based on such environmental changes and **encourage FIs to take necessary responses, while tackling cybersecurity based on progress in digitalization**.

Initiatives to strengthen FIs' cybersecurity

- The JFSA will encourage small and medium FIs to **maintain and improve the effectiveness of their basic cybersecurity management systems through cooperation with their industry groups** and **upgrade their incident response capabilities through cyber exercises**. It will also collect practices through **dialogues with FIs making progress in cybersecurity countermeasures** and proactively recommend good practices to other small and medium FIs.
- With international discussions in mind, the JFSA will encourage large FIs to **upgrade risk management regarding group-wide and global cybersecurity and further advance cybersecurity countermeasures through increasing the effectiveness of the TLPT**. The JFSA will also discuss **cyber resilience initiatives** with FIs in consideration of the risk of malware failing to quickly be detected and continuing to work within networks over a long term.