Summary of Report on Cyber Security in the Financial Sector (June 2019)

1. Background

- With advances in digitalization accelerating, international discussions moving forward, and Tokyo Olympic and Paralympic Games in 2020 soon to take place, the environment surrounding financial institutions is changing, so in response to that we updated the Policy Approaches to Strengthen Cyber Security in the Financial Sector (October 2018)

  Key policy approaches: (1) Responses to accelerating digitalization, (2) Contribution and responses to international discussion, (3) Responses to Tokyo Olympic and Paralympic Games in 2020, (4) Strengthening of cyber security management systems of financial institutions, (5) Improvement of the information sharing framework, (6) Strengthening of human resources development in the financial sector

- With regard to initiatives being conducted in line with the Policy Approaches, we have published a report detailing circumstances identified and, common issues, etc.

2. Key Points

Item	Details of initiatives	Results (summary)
(1) Responses to accelerating digitalization	◆ Identify and analyze the impact of digitalization on financial sector, cyber-security-related risks and countermeasures, etc. through interviews with IT vendors, large financial institutions, etc.	✓ Large financial institutions are making increasing use of new technologies, particularly cloud services and RPA, and are acquiring knowhow and hiring experts to ensure proper risk management. They are also implementing security measures in accordance with the existing cyber-security framework. ✓ In light of the march of digitalization is resulting in increasing reliance on external vendors, it is vital to have proper measures in place that also encompass outsourcing. Furthermore, it is difficult to prevent all types of cyber attack in advance, so it is more important to take measures based on the assumption that incursions will occur. It is essential not only to identify information assets, including those held by third parties, perform risk assessments, and institute entry/internal/exit controls (multi-layered defenses), but also to strengthen surveillance and detection functions, establish BCP (Business Continuity Planning) that also involves important third parties, and enhance the effectiveness thereof through exercises and training.
(2) Contribution and responses to international discussion	◆ Contribute to and respond to international cyber-security-related initiatives devised by the Cyber Expert Group established by the G7 Finance Ministers and Central Bank Governors Meeting	✓ Formulated and published fundamental elements for “threat-led penetration testing (TLPT)” and “third-party cyber-risk management.” (October 2018) ✓ Participated in joint exercises, which are conducted on a cross border basis by the G7 countries. The insights and lessons gained from the exercise will need to be employed in future domestic and overseas initiatives
(3) Responses to Tokyo Olympic and Paralympic Games in 2020	◆ Work with industry groups in the financial sector to establish “Liaison Council for Cybersecurity Stakeholders” to enable information to be shared when cyber incidents, particularly major incidents, occur (June 2019)	✓ Regarding cooperation in the event of a major incident ahead of our during the 2020 Tokyo Games, it will be crucial, through the liaison council, for public and private organizations to share cooperation procedures and confirm their effectiveness through exercises.

Summary of Report on Cyber Security in the Financial Sector (June 2019)

Item	Details of initiatives	Results (summary)
(4) Strengthening of cyber security management systems of financial institutions	(1) Cybersecurity countermeasures as usual ➢ Small and medium financial institutions etc. ◆ Regarding regional banks, credit associations/unions, securities companies, etc., perform cybersecurity assessments to ascertain whether fundamental readiness have been established, whether vulnerability scan have been conducted . ◆ Demand that credit associations/unions complete risk assessments and contingency plans by March 2019, and confirm the results through questionnaire surveys. Perform risk-based cybersecurity assessments to in view of risk profiles ➢ Large financial institutions ◆ With an eye on global trends, engage in regular dialogue with the three mega-banks to confirm that their cyber-security measures are even more sophisticated ◆ As for other large financial institutions (securities companies, insurance companies, and Japan Post Bank), perform a comparative analysis within the sector and with other types of business to raise their capabilities to the next level (2) Incident response ➢ Small and medium financial institutions etc. ◆ Strengthen cyber-security measures by adding new types of business operator such as FX brokers and crypto-asset (virtual currency) exchange service providers to the list of participants in FSA exercises (DeltaWall III) (October 2018) ➢ Large financial institutions ◆ Participate in international joint exercises and promote the use of sophisticated assessment techniques such as TLPT	(1) Cybersecurity countermeasures as usual ➢ Small and medium financial institutions ✓ Regional banks have a been acting independently to beef up measures, with senior executives getting involved in the formulation of action plans. However, only a part of them are consciously taking steps such as vulnerability scan. Furthermore, implementation standards for vulnerability scan have not been established, and the need for them has not been fully recognized. ✓ Most credit associations/unions have completed risk assessments and the formulation of contingency plans. Going forward, it will be important for them to take measures based on the risk assessments. Steps such as vulnerability scan are even less likely to be being performed than at regional banks. ✓ As for securities companies etc., while the number of financial institutions that are making progress with their initiatives is on the rise, there remain many firms that haven't got started or where efforts have stalled. ➢ Large financial institutions ✓ The three mega-banks have formulated action plans for their own organizations in response to the latest trends overseas, and are moving forward with stepping up the level of sophistication. And in the face of international developments such as cyber attacks becoming increasingly complex and ingenious, they are expected to further ramp up the sophistication of unified governance structures for their corporate groups and global operations. ✓ Large financial institutions are working continuously to step up their cyber-security readiness based on risk assessments. Nevertheless, there is still scope for them to improve unified management structures for their corporate groups and global operations, so it is expected that they will make improvements and increase sophistication on an ongoing basis. (2) Incident response ➢ Small and medium financial institutions ✓ Most financial institutions have revamped their contingency plans and taken steps to improve information sharing both internally and externally, and have improved their readiness by conducting exercises. However, issues remain so that their cooperation with third parties and their communication with customers when responding to incidents is inadequate, and that they have not acquired the expert personnel they need to tackle incidents. So they need to bolster their capability to respond to incidents. ➢ Large financial institutions ✓ Through participation in joint exercises, the ability of the nation's financial system as a whole to respond to large incidents has been improved. However, the depth of TLPT needs to be further increased, such as through the application of "threat intelligence."

Item	Details of initiatives	Results (summary)
(5) Improvement of the information sharing framework	◆ Seize opportunities and raise awareness of the significance of "mutual help" involving information-sharing organizations such as the FS-ISAC and promote the sharing of information within the region ◆ Send FSA lecturers to cyber-security workshops run by the FISC	✓ The number of FS-ISAC member is increasing steadily. The recently introduced trial membership scheme, in particular, is serving as a first step toward "mutual help" participation by numerous financial institutions. ✓ Regarding the FISC-hosted workshops, interest in cyber security and awareness of "mutual help" is increasing to some extent as, for example, the number of credit associations/unions, and regional securities companies participating in them rises. On the other hand, there are regions in which participation is extremely low, so there is a lot of variation in awareness of "mutual help."
(6) Strengthening of human resources development in the financial sector	◆ Hold Regional Seminars for Senior Executives in cooperation with the Local Finance Bureaus.	✓ Local Finance Bureaus organized seminars and workshops, which served to raise awareness among senior executives. Going forward, it will be important to expand initiatives like this to other regions. ✓ In the run-up to the 2020 Tokyo Games, it will be important for senior executives to exercise leadership in regarding cyber-security-related risk as a material business risk and corporate risk, and to take action to tackle it.

3. Future FSA initiatives

➢ With the progress of digitalization, the environment surrounding the financial sector is undergoing rapid changes, with financial institutions revamping their business models, non-financial players referred to as "platformers" entering the sector, and so on. And with cyber attacks becoming increasingly complex and sophisticated, and in the run-up to international events such as the upcoming Tokyo Olympic and Paralympic Games in 2020, the FSA will focus on the following action in order to further strengthen cyber security across the entire financial sector:

➢ Action in response to the advance of digitalization
- We will take steps to find out about how digitalization is progressing at financial institutions, taking into account the sizes and characteristics of financial institutions. We will also be active in gathering information from various entities, including non-financial players, and proactively encourage the financial sector to take whatever steps are necessary to ensure cyber security.

➢ Action ahead of Tokyo Olympic and Paralympic Games in 2020
- In the build-up to Tokyo Olympic and Paralympic Games in 2020, we will take action to bolster cyber security at financial institutions through cybersecurity assessments, dialogue, etc. and to make cyber security more effective through the use of vulnerability scan , TLPT, exercises, etc.
- Through initiatives such as the Liaison Council for Cybersecurity Stakeholders, we will work with the FS-ISAC, FISC, etc. to strengthen readiness for large-scale incidents in the financial sector.