Financial Sector Cybersecurity Report

June 2019

Financial Services Agency

[Contents]

Introduction

Recognizing that cybersecurity in the financial sector is of utmost importance for the stability of the entire financial system, the Financial Services Agency (hereinafter, "FSA") formulated and published "The Policy Approaches to Strengthen Cybersecurity in the Financial Sector" (hereinafter, "Policy Approaches") in July 2015, and has since endeavored to strengthen cybersecurity in the financial sector through public-private cooperation.

In recent years, the environment surrounding finance has been undergoing huge changes as the traditional business models of financial institutions (hereinafter, "FIs") are transformed due to an acceleration in digitalization, non-financial players entering the sector, and so on. While it is possible that such developments will dramatically improve user convenience and boost productivity, the interconnectivity of all systems to networks has made it more important than ever before to ensure cybersecurity.

Furthermore, given that cyberattacks cross national borders with ease, international cooperation is vital, and it will be essential for Japan too to make an active contribution to the debate on this issue. Moreover, the 2020 Tokyo Olympic and Paralympic Games (hereinafter, "2020 Tokyo Olympics and Paralympics"), which are set to take place in 2020, will be an event that will attract a never-before-seen level of interest internationally, and it is said that not only organizations involved in the Games but also businesses that provide critical services could be targeted for cyberattacks. This means that it is crucial to further beef up cybersecurity in the financial sector in the run-up to the 2020 Tokyo Olympics and Paralympics.

The march of digitalization is making cyberattacks more complex and sophisticated, so to tackle them effectively, senior executives must be involved in building basic cybersecurity management systems, which direct the identification of and assessment of risks relating to the entity's own information assets, the establishment of a response framework, and the formulation of contingency plans to prepare for incidents. But this alone is not enough, as it will also be critical for entities to repeatedly monitor and analyze security incidents, scan vulnerabilities, conduct penetration tests, perform cyber-exercises, and so on to continuously enhance effectiveness.

In addition to the fact that the environment surrounding FIs is changing dramatically and cybersecurity needs to be substantially reinforced, the "Cybersecurity Strategy," which is the nationwide basic strategy , was revised in July last year, and in response to this we updated the Policy Approaches in October last year.

Based on the new Policy Approaches, this program year we have been proactively responding to significant changes in the financial environment, and have also been working to improve cybersecurity by strengthening cybersecurity management systems at FIs, enhancing the effectiveness of information-sharing frameworks, stepping up human resources development in the financial sector, and so on.

This Report summarizes the circumstances, common issues identified in the course of

conducting initiatives during this program year. The new Policy Approaches state that the FSA will also promote stronger cybersecurity countermeasures by actively disseminating information on challenges to be shared in common by the financial sector, and the purpose of the publication of this Report is to establish a shared awareness among the FSA, FIs and relevant organizations, which will lead to more robust cybersecurity in the financial sector.

1. Current situation with cybersecurity in the financial sector

(1) Threats in recent years

Although Japan has so far never experienced a large-scale cyber-incident sufficient to bring financial system functions to a halt, major cyberattacks aimed at stealing money have occurred overseas. According to media reports, for example, in April 2018 several Mexican banks using the local interbank settlement system operated by the Banco de Mexico were subjected to cyberattacks, and at least 400 million pesos (approximately 20 million U.S. dollars) was stolen by being illicitly transferred. Moreover, in August 2018 an Indian bank suffered losses amounting to 13.5 million U.S. dollars when ATMs and SWIFT[1] infrastructure in the country were hit by a cyberattack[2].

Last fiscal year, FIs in Japan were frequently subject to cyberattacks such as distributed denial-of-service (DDoS) attacks, targeted attacks, and unauthorized access through exploitation of server vulnerabilities. And the attacks no longer only affect large FIs. They have also spread to small and medium FIs and crypto-asset (virtual currency) exchange service providers. In fact, there were cases of the website of small and medium FIs being spoofed, with people being lured to the fake site. There were also incidents of crypto-assets (virtual currency) being stolen. Implementing effective cybersecurity measures is therefore an urgent task.

In addition, with attacks targeting cloud services expected to increase[3], the financial sector needs to continuously identify and analyze new threats, and take necessary measures against them.

(2) Action by the entire government

With knowledge/technology and services such as AI and Fintech penetrating society and cyberspace continuously expanding, ensuring cybersecurity is an important task for our society, not just for the financial sector but for all entities in every field. In line with this

[1] A network system whereby messages concerning international financial transactions among participating banks are transmitted via computers and telecommunications lines with the aim of promoting computerization, streamlining, and automation of international financial transactions among banks (definition from the Japanese Bankers Association website)
[2] Description based on information contained in "2. Trends with Cybersecurity in Critical Infrastructure Fields etc." *Cybersecurity 2019*, NISC (in Japanese)
[3] Based on information contained in "Cybersecurity in 2019 and Beyond," Annual Threat Report, FireEye.

basic view, the government revised its Cybersecurity Strategy in July last year.

Against this backdrop, this program year saw the government revise its "Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure[4]" in order to strengthen measures by operators of critical infrastructure, and the government has been taking steps to improve "crisis management" and "data management." Given that the "financial sector" is one of Japan's critical infrastructure fields, the FSA is also working with relevant organizations such as the Center for Financial Industry Information Systems (hereinafter, "FISC") to ensure that initiatives by the entire government are properly implemented.

Furthermore, in April this year the Basic Act on Cybersecurity was amended, and the "Cybersecurity Council" has been established to facilitate coordination involving a wide range of entities, including national government bodies, critical infrastructure operators, and cyberspace businesses, concerning the implementation of measures relating to cybersecurity. From the financial sector, entities such as the financial CEPTOAR[5] (banks etc., securities companies, life insurers, nonlife insurers) and the Financials ISAC Japan (hereinafter, "ISAC") [6] are participating in the Cybersecurity Council, and the FSA is also actively working to step up information sharing by the entire government.

2. Current initiatives to strengthen cybersecurity in the financial sector

In light of recent changes in the environment surrounding the financial sector, the new Policy Approaches define the following as key tasks: (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 FIs, (5) Improvement of the information sharing framework, (6) Strengthening of human resources development in the financial sector. Below we summarize progress with each of the measures, achievements and common issues during this program year.

(1) Responses to accelerating digitalization

Taking into account the impact that accelerating digitalization is having on financial

[4] Guidelines that organize and present information that should be prescribed in "safety principles," which serve as standards for the conduct of business by critical infrastructure operators etc. (determined by Cybersecurity Strategic Headquarters).

[5] Stands for "Capability for Engineering of Protection, Technical Operation, Analysis and Response." An organization for information sharing and analysis by critical infrastructure operators etc. and the administration of these functions. In the financial sector, there are four such organizations: for banks etc., securities companies, life insurers, and nonlife insurers (the industry associations for each of these sectors serve as the secretariats).

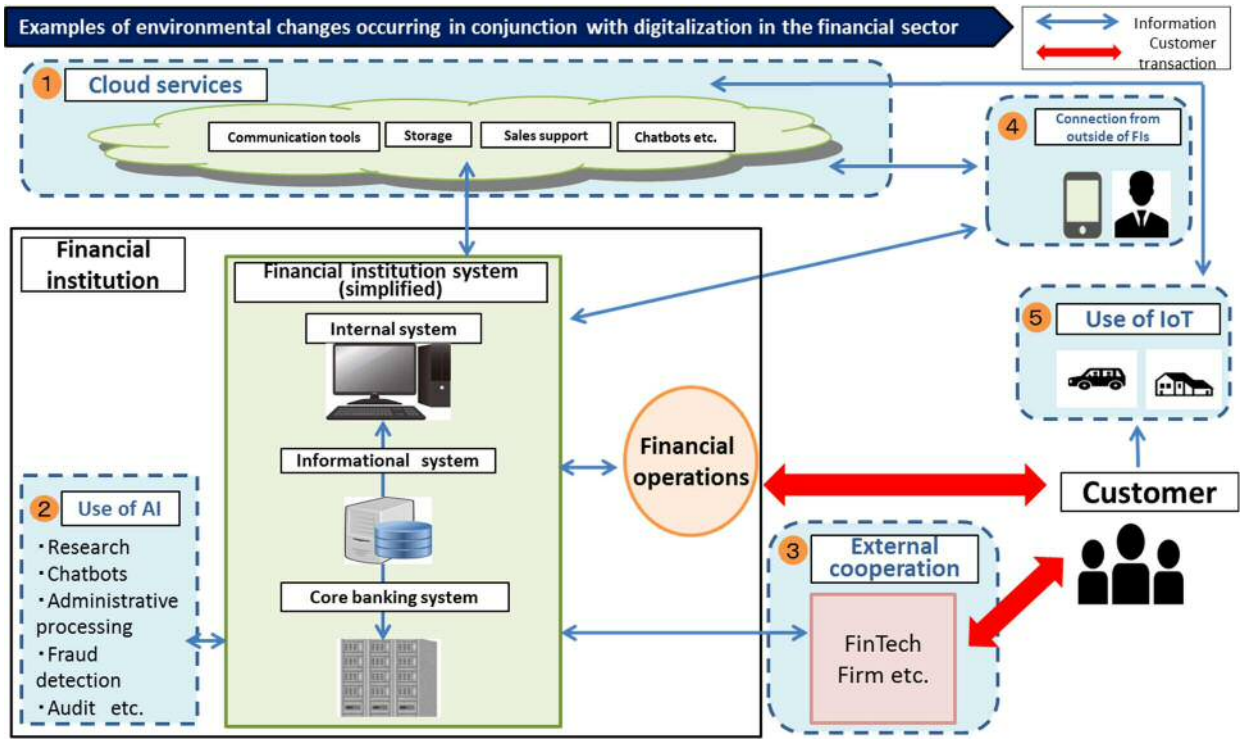
[6] ISAC stands for "Information Sharing and Analysis Center." A general incorporated association established in August 2014 for the purpose of ensuring peace of mind and safety among users by having financial institutions in Japan share and analyzes information relating to cybersecurity and promoting the increased stability within the financial system.

services, we endeavored to find out and analyze what sorts of cyber risks are emerging, how these risks are affecting FIs and the financial sector as a whole, and what action is being taken to address the risks.

Specifically, we started by gathering insights through interviews with outside experts such as IT vendors and consultants, after which we classified digitalization into five broad realms ahead of conducting dialogue with FIs. These five realms were (1) cloud services, (2) AI (RPA[7]), (3) external cooperation, (4) connection from outside of FIs, and (5) IoT[8].

Next we conducted interviews with large FIs to find out about and analyze the action that are taken to tackle issues and risks.

[Figure 1: Examples of environmental changes occurring in conjunction with digitalization in the financial sector (banks)]



Source: FSA

<1> Utilization of digital technology at large FIs

Regarding the utilization of digital technology, we found that large FIs have been moving fairly fast in realms such as cloud services and RPA.

With respect to cloud services, many large FIs have established dedicated cloud services teams[9], and are deploying such services in phases as they accumulate

[7] Robotic Process Automation
[8] Internet of Things
[9] Generally referred to as CCoEs (Cloud Centers of Excellence), these teams accumulate knowledge of cloud services, provide support with their use, etc. on a cross-organizational basis.

knowhow. Looking at the entire financial sector, we find that this has resulted in the concentration of cloud services at large vendors, and going forward such concentration could well increase as more knowledge is accumulated. On the other hand, large FIs remain cautious about shifting security and availability outside with regard to core systems and other important systems that are vital for business continuity, so they are excluding such systems from cloud services.

As for AI (RPA), large FIs are focusing in particular on the automation (RPA) of existing operations. Regarding the promotion of AI, many of them feel that it is important to ensure the reliability of data and output, and to be accountable to customers. Cases were therefore seen, even in areas in which AI is already in use, of human intervention at the conclusion stage, as a means of preventing the process through which the output is produced from becoming a black box.

Regarding external cooperation (outsourcing, partnerships, etc.), large FIs, regardless of the third party's sector or type, have formulated standards and/or checklists in accordance with the FSA Guidelines for Supervision and the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions and are confirming compliance through periodic assessments. They are also taking additional measures depending on the importance of the outsourced operations (service level agreements, business continuity plans, right to audit (right to conduct on-site investigations)).

As for the external environment (access from outside via mobile devices etc.), the FIs typically only allow the mobile devices provided to employees to be used, with only a few of them permitting employees to use their own personal devices.

Only a tiny fraction of FIs provide services that involve the use of IoT to gather data, and full-fledged utilization is not yet occurring at present.

<2> Cyber risks emerging in connection with digitalization

To properly manage risks, large FIs are pressing ahead with securing knowhow and specialist personnel. Specifically, they have been taking security measures in line with the existing cybersecurity frameworks[10]. However, with systems having becoming significantly more complex as a result of digitalization, it has become increasingly important to ensure the completeness of information assets and institute risk controls. As a result, some large FIs are taking steps such as deploying CASBs (Cloud Access Security Brokers) or conducting in-house monitoring and analysis of cloud-service logs.

[10] Refers to such frameworks as the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework and the U.S. Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT)

[Figure 2: Example initiatives at large FIs as gleaned from interviews]

Realm	Example initiatives
① Cloud	・Establishment of dedicated teams (CCoE). Accumulation of knowledge and human resources and development of cloud-related design guidelines and management standards ・Deployment of CASB (Cloud Access Security Broker) and in-house monitoring and analysis of logs of particularly critical cloud vendors ・In contracts with cloud vendors, demand for in-house management of secret keys and vendor's liability for damages associated with NDA (non-disclosure-agreement) breaches resulting from information leaks ・Given that the required knowledge differs from that required for on-premises systems, strengthening of development of specialist personnel
② AI (RPA)	・Formulation of guidelines for AI deployment and articulation of points to keep in mind to prevent unethical use, possession/assumption of rights and obligations relating to deliverables, and intellectual property rights relating to data for learning etc. ・Establishment of AI CoE (AI specialist team) comprising mainly experts from IT systems subsidiary
③ External cooperation	・Setting of number of actual cases of loss and number of cases of customer information leaks as KPIs/KRIs, and reporting of them to senior management ・Clarification of reporting deadlines in the case of suspected information leaks and compulsory reporting of cyber incidents ・Annual inventory of contracted services etc.
④ Connection from outside of FIs	・Security management involving deployment of tools such as MDM (mobile device management)
⑤ IoT	・Distributed storage of collected data on private clouds etc. so as to prevent identification of individuals

Source: FSA

Regarding cloud services, if understanding of not only security aspects but also service descriptions and scopes of responsibility is insufficient or the management of settings relating to the scopes of responsibility of users is inadequate, this could pose risks of incidents such as suspensions of service and information leaks and legal violations (compliance breaches). It will therefore be important to properly manage these risks while making use of cloud services. And as utilization increases going forward, the risk of overconcentration at certain vendors can be expected to rise, so the authorities will also need to perform fact-finding and analysis of how FIs are using cloud services.

In the realm of AI, all the FIs are cognizant of risks associated with fairness, transparency (blackboxing) and security, so it will be important to make usage criteria clearer by establishing guidelines as utilization is expanded.

Furthermore, with regard to outsourcing, the trend overseas is for emphasis to be placed on the supply chain (vendors and other product suppliers), so a task for FIs operating globally is to enhance the sophistication of the management of third parties and procurement.

As for access from the external environment and IoT, while use is limited at the present time, it will be important, before utilization is increased, to implement whatever security measures are required. These could include proper management of devices, access

controls, and distributed data storage.

Because digitalization is resulting in increasing dependence on external parties, there are huge risks to those on the outside of the security measures (including the supply chain) that the FIs have put in place. Appropriate steps will therefore need to be taken in accordance with the nature of the outsourced operations, and such steps will also need to cover the third parties.

However, it is difficult to defend against cyberattacks in advance, and there have already been cases of cloud services and third parties being attacked, so measures that are based on the assumption that incursions will occur are more important. 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, conduct BCP (Business Continuity Planning) that also involves important third parties, and enhance the effectiveness thereof through exercises and training. Taking international developments into account, the FSA will engage in monitoring to ensure that proper risk management is being performed with respect to cybersecurity in view of the extent of digitalization at FIs.

(2) Contribution and responses to international discussion

Because the financial system is globally interconnected, discussions aimed at ensuring cybersecurity through cooperation are taking place through international forums such as the G7 and G20. In 2015 the G7 Finance Ministers and Central Bank Governors Meeting set up the Cyber Expert Group, which has been engaged in discussions concerning cybersecurity. And in October 2018, 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." It will therefore be important for FIs that operate globally to take such international developments on board as they move forward with taking action to make their cybersecurity measures more sophisticated.

It will also be important to apply insights and lessons gained from participation in joint exercises, which are conducted on a crossborder basis by the G7 countries and simulate large-scale cyber-incidents, to develop future domestic and international initiatives.

(3) Responses to Tokyo Olympic and Paralympic Games in 2020

It is stated that ahead of the 2020 Tokyo Olympics and Paralympics, not only could organizations involved with the Games be subject to attacks, but there could also be cyberattacks targeting businesses that provide critical services in an effort to impede the administration of the Games and cause disruption among the public. In fact, at the London 2012 Olympics and Paralympics a tipoff was received that a cyberattack targeting the

electric power system was going to occur, resulting in operations being taken offline and performed manually. There was also a case where personal information was leaked from the website of a construction company that was doing work for the Rio 2016 Olympics and Paralympics[11]. Besides incidents like these, given that in recent years cyberattacks have become increasingly complex and sophisticated in addition to that the financial sector will be no exception, cybersecurity measures will need to be further strengthened. It is especially vital to adequately consider the possibility that an attack on a vulnerable financial institution could escalate and affect the entire sector.

Regarding the actions of the entire government ahead of the 2020 Tokyo Olympics and Paralympics, in April this year the "Cybersecurity Response Coordination Center" was established, putting in place a structure for information liaison between the public and private organizations. It is also important to establish a liaison structure for the financial sector, and closer cooperation will be necessary among relevant ministries/agencies (National center of Incident readiness and Strategy for Cybersecurity (NISC), etc.), the Bank of Japan, an industry groups (CEPTOAR), and other relevant organizations such as the ISAC and the FISC to work on establishing crisis management systems.

To that end, in June this year the "Liaison Council for Cybersecurity Stakeholders" was launched to enable information to be shared when cyber incidents, particularly major incidents, occur. Going forward, the Liaison Council will need to be utilized to share procedures for cooperation among relevant public and private organizations in the major incident ahead of or during the 2020 Tokyo Olympics and Paralympics, and the effectiveness of these procedures will need to be verified by conducting exercises.

(4) Strengthening of cyber security management systems of FIs

During this program year, we engaged in dialogue and conducted exercises with FIs based on risk and maturity the situation with each type of business, as understood through cybersecurity assessments and dialogue conducted up to now. These initiatives focused on two aspects of cybersecurity: countermeasures as usual and incident response.

① Cybersecurity countermeasures as usual

(a) Small and medium financial institutions

Until now, cybersecurity assessments and cybersecurity exercises have resulted in improvements across the board at small and medium FIs. Against this backdrop, and in light of anticipated risks relating to the 2020 Tokyo Olympics and Paralympics, major tasks for them are to improve their basic cybersecurity management systems

[11] Based on information contained in "Reflections on the 2016 Rio Olympic and Paralympic Games and Cybersecurity Measures for the 2020 Tokyo Olympic and Paralympic Games" (July 19, 2017, Takeshi Tachi, Manager, Technology Services Bureau, Tokyo Organising Committee of the Olympic and Paralympic Games) (in Japanese).

and take steps to make them more effective. Based on this basic understanding, we conducted cybersecurity assessments and engaged in dialogue with the sector.

During this program year, we not only verified their basic cybersecurity management systems[12] as usual, but also adopted a new approach, whereby we gathered facts by focusing on in-depth investigations of measures such as cyber-incident monitoring/analysis and vulnerability scan.

○ Regional banks

We have completed cybersecurity assessments at regional banks, during which we focused on those where the previous round of cybersecurity assessments had revealed insufficient in taking action[13]. Pursuant to the discussions we had at the time, the issues had been resolved on the whole, and in some cases senior executives were proactively getting involved in formulating action plans and moving voluntarily to beef up measures.

Furthermore, regarding the establishment of systems, something that is worthy of note is that so-called mutual-help systems, which involve multiple banks, are operating effectively. Banks are signing up to joint systems for sharing information, taking part in joint study sessions, and so on. One notable example of this is participation in the joint exercises run by the ISAC.

On the other hand, when we investigated, as part of our new approach, the status with vulnerability scan and penetration testing, we found that only a part of FIs were taking steps to perform them by outsourcing the task to security vendors. Furthermore, most had not formulated implementation standards, so there was inadequate awareness of the need for such measures. It will therefore be essential for them to accurately identify their potential vulnerabilities and fix them before the 2020 Tokyo Olympics and Paralympics.

Among regional banks, it is hoped that advanced ones will refer to leading examples from large FIs to further bolster their cybersecurity measures.

○ Credit associations/unions

Even though around three years has passed since the announcement of the Policy Approaches, even the top credit associations and unions were still in the process of establishing basic systems for risk assessment and incident response. Major factors behind this stalling across the sector are that senior executives has little sense of crisis toward cyber risks, and that a trial-and-error approach is being followed, with there being no specialist personnel on hand and no system of

[12] (1) Initiatives by senior executives, (2) risk-management framework, (3) implementation of technical measures etc., (4) assurance of effectiveness through establishment of contingency plans and the conduct of exercises, (5) cybersecurity audits.

[13] It is conducted follow-up at banks that had been found to be insufficient in taking action during the second round of cybersecurity assessments in the case of regional banks, or the previous round of cybersecurity assessments in the case of second-tier regional banks.

mutual help of the like seen with the regional banks. Furthermore, the credit associations/unions were even less aware of the need for vulnerability scan and penetration testing than the regional banks. They would leave everything to the third parties, and were unaware of the scope of vulnerability scan and penetration testing being performed or even whether they were being performed at all. So like regional banks, it will be essential for credit associations/unions to accurately identify their potential vulnerabilities and fix them before the 2020 Tokyo Olympics and Paralympics.

In light of this situation, and with the aim of ensuring that proper cybersecurity measures are instituted by the time of 2020 Tokyo Olympics and Paralympics, the authorities have formulated a three-pillar policy for strengthening cybersecurity at credit associations/unions. The three pillars are as follows: (1) raising awareness and sharing objectives among senior executives, (2) confirming and following up on action being taken, and (3) cybersecurity assessments covering more credit associations/unions considered high-risk.

Based on this policy, during this program year we worked with industry groups, through lectures and seminars for individual credit associations/unions, to share objectives for the 2020 Tokyo Olympics and Paralympics and to perform risk assessments and formulate contingency plans to serve as a foundation for cybersecurity measures by March of this year. Moreover, we confirmed the action being taken at each credit association/union using questionnaires, and are following up on those that have not completed risk assessments and contingency plans.

Furthermore, with the aim of improving cybersecurity at credit associations/unions, we employed questionnaires to gauge their risk profiles, and in the case of those that were being particularly insufficient in taking action, we directly urged them to step up their efforts through cybersecurity assessments that targeted more credit associations/unions considered high-risk.

As a result of these efforts, most credit associations/unions have performed risk assessments and formulated contingency plans. Going forward, ahead of the 2020 Tokyo Olympics and Paralympics, they will need to take whatever cybersecurity measures are necessary based on these risk assessments and ensure that these measures are effective through, for example, vulnerability scan.

○ Securities companies etc.

Among securities companies etc. that we had not yet conducted cybersecurity assessments at, we performed cybersecurity assessments at small/medium and regional securities companies, FX brokers, PTS[14] operators, asset managers, etc. While the number of FIs making progress is increasing, there remain numerous

[14] Proprietary Trading System

ones that have not taken any action or have made little progress.

At securities companies etc. where senior executives are highly cognizant of the risks, senior executives are becoming actively involved in the formulation of action plans and are moving independently to beef up cybersecurity. However, as is the case with credit associations/unions, most of them are still in the process of taking basic steps such as conducting risk assessments and formulating contingency plans. Furthermore, some of them misunderstand that it is enough for core systems to be separated from the network environment, and have stopped short of conducting cybersecurity risks assessments or addressing threats that the results of such assessments have turned up.

○ Crypto-asset (virtual currency) exchange service providers

In October last year we designated the Japan Virtual Currency Exchange Association (hereinafter, "JVCEA") as a certified association for payment service providers, and have been cooperating closely in the exchange of information. Based on rules and guidelines established voluntarily by the JVCEA, each service provider is establishing operational control systems that include cybersecurity measures. In addition, vulnerability scan and penetration test via third-party, which had only performed by a small number of service providers, have been conducted by each service provider, which come to recognize the need for them.

Furthermore, in light of the incidents of loss of huge sums of crypto-assets (virtual currencies) by illicit access, we interviewed all the service providers about how they control the wallets[15] used for keeping crypto-assets (virtual currencies) safe.

(b) Large financial institutions

Regarding large FIs, until now we have engaged in ongoing discussions through periodic dialogue, mainly with the three mega-banks that form the core of Japan's financial system.

During this program year we confirmed, through periodic dialogue, that the three mega-banks have been keeping an eye on the advanced initiatives being implemented by large U.S. banks and on global trends, and have responded by making their cyber measures even more sophisticated. In addition, with the aim of encouraging large FIs other than the three mega-banks (large securities companies, large insurers, Japan Post Bank) to further enhance their resilience, we conducted a comparative analysis both within and outside the sector.

The three mega-banks have formulated action plans for their own organizations that reflect the latest overseas trends, and are taking steps to enhance sophistication. On the other hand, given that cyberattacks are becoming increasingly complex and

[15] Place where secret keys are stored.

sophisticated, and in light of international developments, they are expected to further ramp up the sophistication of unified management structures for their corporate groups and global operations by, for example, strengthening the control tower functions of CISOs[16] and reinforcing access controls and vulnerability management.

As for large FIs other than the three mega-banks, although they are taking continuous action to beef up their cybersecurity systems based on their own risk assessments, depending on their size and global reach, some of them still had room to institute unified management structures for their corporate groups and global operations or improve their responses to vulnerabilities, so it is hoped that they will make improvements and increase sophistication on an ongoing basis by, for example, referring to examples from other FIs that are implementing more advanced initiatives and to deficiencies pointed out during assessments by external parties.

(c) Audit firms

In the case of audit firms, we confirm their cybersecurity measures and encourage them to improve their systems with reference to the initiatives seen at FIs.

During this program year, we conducted cybersecurity assessments at and engaged in dialogue with large-sized audit firms and second-tier audit firms. In the case of large-sized audit firms, they have appointed expert personnel and established dedicated departments, and are working with their global networks in the area of cybersecurity. Second-tier audit firms, on the other hand, were not making adequate progress with the implementation of cybersecurity initiatives.

② Incident response

(a) Small and medium financial institutions

With cyberattacks becoming more complex and sophisticated, there are limits to the ability to swiftly contain and defend against cyberattacks, so the response once an attack has occurred is important. Because of this, each year the FSA organizes a cybersecurity exercise called "Delta Wall" for the entire financial industry as a means of improving cybersecurity, particularly at small and medium FIs.

During this program year, we added new types of business operators, namely FX brokers and crypto-asset (virtual currency) exchange service providers, to the 105 companies (approximately 1,400 persons) on the list of participants in order to better reflect recent threat trends. The exercise emphasized ex-post assessment and, with the most of the participating FIs taking steps to revise their contingency plans and strengthen internal and external information sharing, has helped them improve their response systems. On the other hand, regarding industry-wide trends, a number of issues have been identified. These include the fact that many small and medium FIs

[16] Chief Information Security Officer.

have inadequate cooperation with third parties and communication with customers when responding to incidents, and the personnel needed to tackle incidents have not been secured. In light of these issues, FIs will need to continue following the PDCA cycle and to improve their response capabilities. And in the run-up to the 2020 Tokyo Olympics and Paralympics, we will need to improve the ability of the entire financial sector to respond to incidents by developing an exercise scenario that reflects risks that could materialize at the 2020 Tokyo Olympics and Paralympics and expanding the number of participating FIs

(b) Large financial institutions

Large FIs have been working to boost the capability of Japan's financial system as whole to deal with major incidents by, for example, taking part in joint exercises conducted by the authorities of the G7 jurisdictions. Furthermore, they have taken account of best practices at large overseas FIs as well as international trends to utilize and promote sophisticated assessment techniques such as TLPT[17], which is characterized by the employment of "threat intelligence," namely gathering information on threats facing the organization and investigating and analyzing modus operandi. Given this characteristic, this sort of testing is expected to become even more in depth.

Furthermore, in light of "G-7 Fundamental Elements for Threat-led Penetration Testing," which was published last year, the FISC is currently in the process of formulating the handbook for TLPT. The FSA will need to cooperate closely with such developments and work to ensure and promote the utilization of TLPT at each financial institution.

(5) Improvement of the information sharing framework

Until now, whenever we have had the opportunity to do so, we have informed FIs of the significance of "mutual help," namely the utilization of information-sharing organizations such as the ISAC, and this has led to a steady rise in the number of FIs that are members of the ISAC. Furthermore, a trial membership scheme, which ISAC was introduced last April, is resulting in many FIs becoming full members, so seems to be serving as a first step toward participation in "mutual help" schemes by small and medium FIs.

However, in light of the fact that some small and medium FIs feel that ISAC membership would be difficult due to geographical, personnel-related, and financial reasons, they will need to step up information sharing in their respective regions as a first step toward "mutual help." With that in mind, lecturers from the FSA, the ISAC, and the Japan Cybercrime Control Center (JC3) have been dispatched to "cybersecurity workshops" run by the FISC as a means of promoting local cooperation.

[17] Threat-Led Penetration Testing

In FY2018 FISC held workshops on 12 occasions at various locations nationwide and were attended by 241 companies (293 persons), and the number of credit associations/unions and regional securities companies was up compared with the previous year. This indicates that small and medium FIs are become increasingly interested in cybersecurity and in the concept of mutual help. Going forward, it is hoped that participation in these sorts of activities will act as an impetus for concrete action such as sharing information with other nearby FIs. Nevertheless, there were big gaps in awareness of "mutual help," as reflected in the fact that there are some regions with very few participants.

The role being played by "mutual help" in the financial sector has been growing substantially year by year, and the given the establishment of the Cybersecurity Council for the entire government as well as the Liaison Council for Cybersecurity Stakeholders for the financial sector, it will be essential for the authorities to continue to seize every opportunity to communicate the importance of "mutual help" that is founded on "self-help" by FIs.

(6) Strengthening of human resources development in the financial sector

If FIs are to establish effective cybersecurity risk management systems, it will be incredibly important for them to perceive and tackle cybersecurity-related risks not only as mere technology-related risks, but as business risks and corporate risks that need to be addressed by the entire organization. To that end, it will be essential for senior executives to raise their awareness.

We therefore worked, for example, with Local Finance (Branch) Bureaus to organize seminars for senior executives at FIs in order to encourage them at regional FIs to raise their awareness. And in some regions we teamed up with the ISAC and organized seminars in the form of workshops in which senior executives took part. In this way, we contributed to raising awareness among senior executives of FIs and mutual-help among FIs. Going forward, it will be important to keep an eye on the situations in the regions and expand these sorts of initiatives to other regions.

The FSA, meanwhile, took advantage of opportunities such as regular meetings with representatives of each industry and lectures at seminars hosted by relevant organizations such as the ISAC and the FISC, and monitoring by Local Finance (Branch) Bureaus to raise awareness of cybersecurity among senior executives. As a result, while awareness of cybersecurity seems to have increased to some extent, ahead of the 2020 Tokyo Olympics and Paralympics it will be important to further raise awareness and, under the leadership of senior executives, to move forward with initiatives that view cybersecurity-related risks as important business risks and corporate risks.

3. Future FSA initiatives

With the progress of digitalization, the environment surrounding the financial sector is undergoing rapid changes, with FIs revamping their business models, non-financial players referred to as "platformers" entering the sector. With cyberattacks becoming increasingly complex and sophisticated, and international events such as the upcoming 2020 Tokyo Olympics and Paralympics on the horizon, it has been said that providers of important services, including those in the financial sector, are at higher risk of cyberattack than before. The authorities will therefore focus on the following action in order to further strengthen cybersecurity across the entire financial sector:

○ Action in response to the advance of digitalization

We will utilize the results of the interviews conducted during this program year to find out about how digitalization is progressing at FIs, taking into account the sizes and characteristics of FIs. To keep up with the rapid digitalization in the financial sector, we will also be active in gathering information not only from FIs, but also from various other entities, including non-financial players, and proactively encourage the financial sector to take whatever steps are necessary to ensure cybersecurity.

○ Action ahead of the 2020 Tokyo Olympic and Paralympic Games

In the build-up to the 2020 Tokyo Olympics and Paralympics, we will take action to bolster cybersecurity at FIs through cybersecurity assessments, dialogue, etc. and to make cybersecurity more effective through the use of vulnerability scan, TLPT, exercises, etc. We will also actively contribute to the initiatives of the entire government relating to the 2020 Tokyo Olympics and Paralympics, and through organizations such as the recently launched Liaison Council for Cybersecurity Stakeholders, we will work with the ISAC, the FISC and other organizations to strengthen readiness, in the forms of "mutual help" and "public help," for large-scale incidents in the financial sector.