Policies for Strengthening Cybersecurity in the Financial Sector

October 2018

Financial Services Agency

[Table of Contents]

1. Update to "The Policy Approaches to Strengthen Cybersecurity in the Financial Sector"

(1) Background to update

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.

Digitalization has been accelerating, and the financial industry is undergoing innovation with the entry of new players into the financial sector and the ever-growing application of data. While it is possible that such developments will dramatically improve user convenience and boost the productivity of the Japanese economy, there are concerns that the digitalization of all financial-related businesses and operations as well as the connection of all systems to networks will further increase cybersecurity risks. In a society characterized by growing reliance on digitalization, cybersecurity will be more important than ever to ensure the security of financial service users and the stability of Japan's financial system while improving user convenience and enhance productivity in the financial industry.

Cybersecurity risks have risen even higher in recent years due to the growing sophistication and complexity of cyberattacks both inside and outside Japan. The threat of cyberattacks has become more serious globally, as seen in the heist via fraudulent instruction of the SWIFT international remittance system at central banks overseas in 2016[1], and a large-scale ransomware[2] infection of PCs in numerous countries in 2017[3]. In light of such circumstances, cybersecurity has become an important topic internationally as well, and international discussions on cybersecurity in the financial sector are taking place in such forums as the G7 Finance Ministers and Central Bank Governors Meeting. It is needed for Japan to actively contribute and respond to such international discussions.

The reach of cyberattacks in Japan's financial sector has extended beyond major financial institutions to even small and medium-sized financial institutions as well as crypto-asset trading platforms, and a diversity of modus operandi have been employed, including distributed denial-of-service attacks (DDoS attacks), targeted attacks, and unauthorized access by penetrating server vulnerabilities. With the 2020 Tokyo Olympic & Paralympic

[1] An international remittance system (SWIFT) terminal at Bangladesh's central bank infected with malware was used to make an unauthorized remittance of a very large sum (approximately 81 million US dollars) (similar incidents have also occurred in Taiwan, Nepal, etc.).

[2] A neologism combining "ransom" and "software", this is a general term for malicious programs that encrypt the data of infected PCs to make it inaccessible, after which a ransom is demanded in exchange for restoring the PC to its former state.

[3] In May 2017, PCs and servers using WindowsOS in more than 150 countries worldwide were infected with ransomware called "WannaCrypt". In June of the same year, PCs in Europe, the US and other countries worldwide were infected by the "Petya" ransomware.

Games due to be held in Japan, it has been pointed out[4] that critical infrastructure in Japan, including the financial sector, could be targeted by cyberattacks, and the public and private sectors need to work closely to construct a crisis management system to prepare against large-scale incidents. The "Cybersecurity Strategy" that lays out the government's basic policies on cybersecurity was revised[5] in July of this year, and this updated strategy calls on government organizations to work together for ensuring cybersecurity measures for critical infrastructure, including the financial sector, with an eye to the 2020 Tokyo Olympic & Paralympic Games.

With circumstances surrounding cybersecurity in the financial sector changing greatly, the FSA recently clarified its policies for dealing with new challenges and its future approaches and policies in light of the progress and evaluation of its current "Policy Approaches" in building an effective cybersecurity management system, and decided to update the "Policy Approaches" to help financial institutions, financial service users, and related organizations come to a shared view of the challenges faced.

Major Cyberattacks in the Financial Sector in Recent Years

Motive	Target	Attack method	Overview of incidents
Political beliefs	Financial institutions	✓ Suspension of service on websites, etc., due to DDoS attack	◆ Harm incurred due to DDoS attacks against the websites of multiple organizations, including Japanese financial institutions and the Financial Services Agency. Impact also felt by financial institutions using the same Web hosting companies as the targeted organizations
Information theft		✓ Targeted attack by e-mail, etc. ✓ Unauthorized access of servers, etc.	◆ Unauthorized access was gained to the e-mail servers of Japanese financial institutions, and customer information (names, addresses, account numbers, etc.) was leaked (September 2016) ◆ Unauthorized access was gained to the websites of Japanese financial institutions, and customer information (IDs, names, addresses, birthdates, etc.) was leaked (July 2017) ◆ The website of a financial institution was tampered with through a server attack, and users who visited this website were re-directed to a malicious external website and had malware downloaded onto their computers
Monetary gain		✓ Illegal remittances via attack against the financial institution	◆ A PC at the Bangladeshi central bank connected to the SWIFT, international remittance system, was remotely operated to steal a large sum of money (February 2016) (similar incidents have occurred in Taiwan, Nepal, etc.) ◆ There were large-scale thefts of crypto-assets from crypto-asset trading platforms via unauthorized access from outside (January and September 2018)
		✓ DDoS attack for monetary gain	◆ Multiple financial institutions received an e-mail threatening DDoS attacks if they did not pay ransom in Bitcoin by a given deadline, and then suffered harm due to short-term DDoS attacks (June and September 2017)
	Customers	✓ Malware infection of customers' PCs	◆ Malware that steals the IDs and passwords of Internet banking users was uncovered. The presence of malware targeting the users of crypto-asset trading platform has also been confirmed lately

[Source] Prepared using publicly-available materials

[4] The "Cybersecurity Strategy" notes that there was a massive number of cyberattacks during the London Olympic & Paralympic Games, and there was a significant number of cyberattacks causing damages to the Rio de Janeiro Olympic & Paralympic Games and the Pyeongchang Olympic & Paralympic Games.

[5] The "Cybersecurity Strategy" incorporates such policies as ensuring preparedness for the 2020 Tokyo Olympic & Paralympic Games (developing the Cyber Security Response Coordination Center (Government Olympic/Paralympic CSIRT)), and promoting information sharing and collaboration between multi-stakeholders.

(2) Progress and evaluation of the current “Policy Approaches”

Since announcing the “Policy Approaches” in 2015, the FSA has endeavored to strengthen cybersecurity in the financial sector through public-private cooperation in line with the Policy Approaches. The progress and evaluation of each of the policies indicated in the current “Policy Approaches”[6] are discussed below.

① Constructive dialogue with financial institutions and assessment of their current condition regarding cybersecurity

Since the announcement of the “Policy Approaches” in 2015, the FSA has undertaken assessment of the current cybersecurity countermeasures at more than 200 financial institutions, primarily regional financial institutions but also including securities companies, insurance companies and a wide range of other institutions[7].

Financial institutions with advanced cybersecurity countermeasures tend to regard cybersecurity risk as a serious corporate risk and, under strong leadership from their senior executives, IT departments as well as other relevant in-house organizations (corporate planning, legal affairs, public relations, business divisions, etc.) are constructing frameworks for conducting risk assessments focused on cybersecurity, preparing response measures (organizational readiness, technical control), establishing contingency plans, continually participating in exercises, and conducting cybersecurity audits. These institutions will run through the PDCA (Plan - Do - Check - Act) cycle and periodically review risk assessments as new threats emerge and other external environments change.

On the other hand, financial institutions that see cybersecurity risk simply as a risk to be addressed by IT departments and other relevant organizations have not devoted sufficient attention to cybersecurity risk assessment, which forms the foundation for cybersecurity measures, leaving them unable to identify where cybersecurity-related risks exist within their own organizations. They also have a tendency to entrust technical responses entirely to the in-house organizations in charge or outside contractors, and have not established contingency plans to deal with cyber incidents.

Since this tendency is especially pronounced at small and medium-sized financial institutions, and improving the level of cybersecurity across the industry as a whole by

[6] The present “Policy Approaches” spell out five approaches: (1) constructive dialogue with financial institutions and assessment of their current condition regarding cybersecurity, (2) improvement of the information sharing framework among financial institutions, (3) continuous implementation of industry-wide exercises, (4) developing cybersecurity human resources in the financial sector, and (5) arrangements of cybersecurity initiatives in the FSA. With regard to (5) arrangements of cybersecurity initiatives in the FSA, the FSA already established a new division for cyber security “Cyber Security Measures Planning and Coordination Office”, which has the function to gather and analyze cyber threats and incident information from each bureau within the FSA and to plan and coordinate FSA’s cybersecurity policies. Thus, the progress and evaluation of (1) – (4) will be addressed here.

[7] The assessment at all Regional Banks and Regional Banks II were completed by program year 2016.

establishing fundamental cybersecurity management systems has become a major challenge. For that reason, in program year 2017, regarding Shinkin Banks and credit unions, with backing from the FSA, their respective cooperative central organizations and industry groups collaborated to publish risk assessment manuals and contingency plan templates and passed these on to their constituent financial institutions. It is needed for individual Shinkin Banks or credit unions, with suitable support from their respective cooperative central organizations and industry groups, to utilize these manuals and templates to accelerate cybersecurity readiness as best suits their own circumstances.

As for Regional Banks and Regional Banks II, they have made a certain degree of progress in constructing fundamental cybersecurity management systems, and the key will be shifted to ensuring the effectiveness of countermeasures against cyberattacks.

With regard to major financial institutions, discussions have been carried on continuously through regular dialogues, particularly with the three mega-groups, which form the core of Japan's financial system[8]. Considerable progress has been made by the three megabanks in taking their cybersecurity response capabilities to the next level, including their use of "Threat-Led Penetration Test"[9] as a more advanced assessment method.

In program year 2017, the FSA conducted studies and analyses, including on-site interviews, on the G-SIFIs' cybersecurity countermeasures and shared the view with the three megabanks of the need for more advanced countermeasures in reference to G-SIFIs' leading-edge efforts. Major financial institutions overseas have further upgraded their countermeasures as the threat of international cyberattacks has risen, and major financial institutions in Japan need to keep an eye on such efforts and step up their own countermeasures.

② Improvement of the information sharing framework among financial institutions

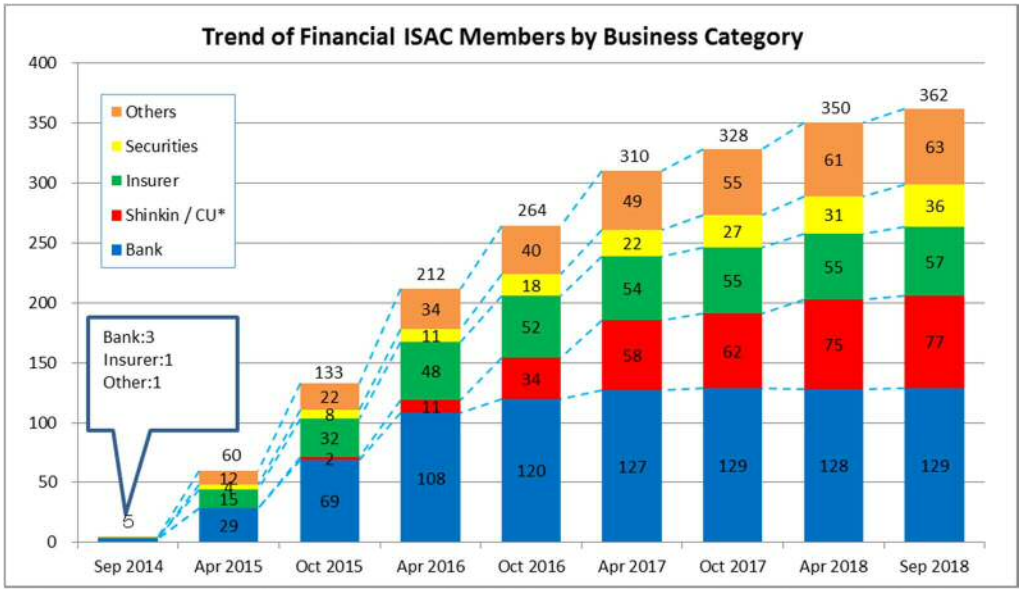
In improving the efforts of financial institutions and strengthening cybersecurity for the financial industry overall, the most effective approaches are to rely not only on the "self-help" efforts of financial institutions themselves and "public help" from the FSA and other authorities but also on "mutual help" in which information sharing and analysis are carried out among financial institutions. As part of these "mutual help" arrangements, membership in General Incorporated Association Financials ISAC Japan[10] (hereinafter,

[8] Since program year 2017, dialogues have been conducted periodically with major insurance companies on cybersecurity management readiness, human resource development and education, countermeasures at insurance agencies, and other matters.

[9] A practical penetration test of a financial institution based on an attack scenario prepared using an analysis of threat trends.

[10] The Information Sharing and Analysis Center was established by financial institutions in Japan as a general

"Financials ISAC") has steadily grown as a result of efforts in informing financial institutions of the significance of stepping up information sharing and cybersecurity countermeasures (e.g. promptly identifying vulnerabilities and implementing defensive technologies)by utilizing information sharing institutions such as Financials ISAC.



[Source: Processed using information from the Financials ISAC website (as of September 4, 2018)]

Financials ISAC engages in a variety of activities, sharing information as well as sharing resources through working group activities and holding local conferences, and its role has grown larger over time. Nevertheless, membership has stagnated among some business sectors[11], and continuing to promote the effectiveness of "mutual help" and endeavoring to establish a mutual help posture in the financial industry are challenges for the organization. Some small and medium-sized financial institutions have stated that joining Financials ISAC would be difficult for geographical, staff, or monetary reasons and, accordingly, consideration must be given to approaches such as intra-regional collaboration[12].

③ Continuous implementation of industry-wide exercises

The FSA has conducted annual financial industry-wide cybersecurity exercises (Delta Wall[13]) since 2016 to improve the ability of small and medium-sized financial institutions in particular to respond to incidents. A total of 77 financial institutions participated in the

incorporated association in August 2014 to ensure continued safety/security for users by sharing and analyzing information on cybersecurity, and by improving the security of financial systems.

[11] There are many Shinkin Banks/credit unions as well as small and medium-sized securities companies that have not yet become members.

[12] For example, there are such mutual help efforts as the "Niigata Prefecture Financial Institution Cybersecurity Countermeasure Liaison Conference" (established on February 22, 2018) and "Cybersecurity Day in Hiroshima – Let's All Safeguard Cyberspace" (held on April 10, 2018).

[13] Delta Wall: Delta (symbolic of the three cybersecurity keys of "self-help", "mutual help" and "public help") + Wall (indicating a defensive posture).

2016 exercise and 101 financial institutions in the 2017 exercise, and the aim has been to improve participants' ability to respond to incidents by preparing for and participating in the exercise as well as receiving feedback on the exercise outcomes[14]. To enable financial institutions not participating in the exercise to utilize the outcomes in their own efforts, information on trends and challenges faced in common is compiled and made available to the entire industry.

Though some financial institutions have good practices[15] that enable them to cope quickly and precisely with incidents, it has become apparent that most have a tendency to focus their attention solely on the specific attacks presented in the scenarios, highlighting the need to have them keep an eye out for the possibility of separate attacks carried out under cover of the attacks stipulated in the scenario through further monitoring and to have them otherwise address incidents from a broader perspective. To deal quickly and accurately with cyberattacks, it is crucial to identify in advance the actions anticipated, concretely manifest response procedures in their policies, and continually refine the response procedures by participating in external exercises, etc.

The outcomes of previous cybersecurity exercises must also be reviewed to devise more effective exercise methods and content, and the public and private sectors need to work closely to improve their responsiveness to incidents.

④ Developing cybersecurity human resources in the financial sector

The FSA has continually raised awareness of senior executives on the importance of cybersecurity countermeasures, taking opportunities of giving speeches to financial institutions and cybersecurity workshops[16] held by Local Finance (Branch) Bureaus in program year 2016. The Center for Financial Industry Information Systems (hereinafter, "FISC") has also been holding workshops primarily for small and medium-sized financial institutions across the country since program year 2017, and collaborating with the FSA to gain better understanding and skills on cybersecurity countermeasures and maintenance.

Although these efforts have to a certain degree been successful in improving the awareness and understanding of cybersecurity among financial institutions, the awareness and understanding of senior executives on the need for cybersecurity countermeasures, particularly at small and medium-sized financial institutions, are by

[14] At the end of October 2018, approximately 100 financial institutions are expected to participate in what will be the third exercise.

[15] For example, some financial institutions check with IT vendors to see if other financial institutions jointly using the system have suffered similar harm, and some monitor suspicious account activity to ensure that customers do not suffer secondary harm due to information leaks.

[16] In program year 2016, a total of 23 workshops were held by 10 Finance (Branch) Bureaus, with a total of about 500 financial institutions participating.

no means adequate. Additionally, it has been pointed out that Japan faces a shortage of cybersecurity human resources not just in the financial sector but across the country as a whole.

A change in the mindset of senior executives will be essential in strengthening the cybersecurity countermeasures of financial institutions. In conjunction, it will also be important to retain cybersecurity staff, improving their understanding of cybersecurity and enhancing their skills. This will require developing human resources for the industry as a whole in collaboration with Financials ISAC, FISC and others.

2. Approaches to strengthen cybersecurity in the financial sector

(1) Basic concept

As mentioned above, steps have been taken in keeping with the current “Policy Approaches” to strengthen cybersecurity countermeasures in the financial sector. With digitalization accelerating, the 2020 Olympic and Paralympic Games being hosted in Tokyo, and international discussions making headway, the circumstances surrounding cybersecurity in the financial sector have changed greatly since the “Policy Approaches” were formulated in 2015. The progress made in the current “Policy Approaches” and evaluations thereof must also be considered to make improvements.

Given this basic perspective, the public and private sectors will seek to work together closely in addressing the new challenges generated by changes in the environment surrounding cybersecurity in the financial sector as well as the challenges discussed below in order to leverage the progress and evaluation of efforts thus far to further buttress cybersecurity countermeasures in the financial sector. The FSA will strive to ensure that all relevant parties share the same recognition and achieve concrete improvements by actively presenting the cybersecurity challenges ascertained through these efforts to individual financial institutions and business sectors. The FSA will also promote stronger cybersecurity countermeasures for the financial sector overall by periodically compiling information on challenges to be shared in common by the financial sector and actively disseminating it.

Furthermore, these items will be reviewed when appropriate in recognition of the fact that technological advances and other factors require ongoing and significant changes in the approaches taken by the financial industry.

(2) Addressing new challenges

① Responding to accelerated digitalization

While Internet-centered operations and services have already achieved considerable

permeation throughout the financial sector, technological advances and innovations in cyberspace are expected to accelerate in the future. Such developments are causing fundamental changes to the business and operational approaches of the financial industry, as seen in the collaboration between existing financial institutions and FinTech companies in providing new financial services, the creation of new business models by non-financial players entering the financial industry, the increasing IT-driven operations and improved efficiency of operations through the application of IoT and AI by financial institutions and the spread of cloud-based services, and the appearance of new financial companies such as crypto-asset trading platforms and electronic settlement agents. At the same time, advancing digitalization could give rise to the following risks.

Expected risks from the accelerating digitalization (Hypotheses)

- A third-party (outsourcing) risk assumed as a result of collaboration with new players, outsourcing existing operations, etc.
- A risk of IT interruption having a direct impact on business continuity (a viewpoint on crisis management)
- A risk of an impact spreading to a wide range in chains from one single point of disruption due to the connection of all systems (the worst case might be the malfunctioning of settlement systems)
- A concentration risk due to rising dependency on specific business operators and technologies. (e.g., cloud computing)
- A risk of failure to detect or respond to new attack methods abusing technologies such as AI by existing measures

Consequently, the FSA is working to study and analyze suitable responses to such risks by determining the impact of advancing digitalization on the financial industry, the specific cybersecurity risks that could arise, and the impact such risks would have on financial institutions and the financial sector overall. The findings of this research and analysis will be used to encourage financial institutions to adopt new and effective measures to respond to such cybersecurity risks, and consideration will also be given to the way of monitoring approaches in response to such changes[17].

② Contributing and responding to international discussions

Cyberattacks easily transcend national borders, and concerns that their impact can reverberate throughout the entire financial system make cybersecurity an important

[17] A “Virtual Currency Monitoring Team” was organized inside the FSA in August 2017, since which time it has been screening the registration of, and monitoring, crypto-asset trading platforms and collecting/analyzing information on crypto-assets. In August of this year, the “Inspection and Monitoring of Virtual Currency: Interim Report” was published, covering problems identified through inspections and monitoring theretofore.

challenge internationally.

In light of this, the G7 Finance Ministers and Central Bank Governors Meeting set up a G7 Cyber Expert Group in 2015 to engage in discussions on cybersecurity[18]. Thus far, the “Fundamental Elements of Cybersecurity for the Financial Sector” (2016), outlining the fundamental principles for international cybersecurity countermeasures, and the “G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector” (2017) on assessing those countermeasures, have been formulated and published. In October of this year, the “G7 Fundamental Elements for Threat-Led Penetration Testing” and “G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector” to stipulate the fundamental principles for important topics in specific areas were compiled and published. A joint cross-border exercise for large-scale cyber incidents scheduled for 2019 is to be conducted in collaboration with authorities from the G7 countries.

Cyberattacks that readily cross national borders must be addressed not only by implementing cybersecurity countermeasures in each country but also by pursuing international cooperation. To that end, the FSA will work with various overseas authorities, and contribute and respond to discussions on international cooperation regarding cybersecurity on the G7 Finance Ministers and Central Bank Governors Meeting and other international conferences.

③ Preparing for the 2020 Tokyo Olympic & Paralympic Games, etc.[19]

In line with the policies for the government as a whole set forth in the “Cybersecurity Strategy” [20], the FSA will work in even closer collaboration with relevant ministries and agencies (National Information Security Center (NISC), etc.), the Bank of Japan, industry groups (CEPTOAR-Council[21]), Financials ISAC, FISC and other relevant groups to establish collaborative arrangements within, and a crisis management system for, the financial sector ahead of the 2020 Tokyo Olympic & Paralympic Games, and will make use of these arrangements as a framework for the financial sector’s crisis management system should a large-scale incident occur.

---

[18] In addition to the G7, cybersecurity is being discussed by the Financial Stability Board (FSB), the Senior Supervisors Group (SSG), the International Organization of Securities Commissions (IOSCO), and other organizations.

[19] Prior to the 2020 Tokyo Olympic & Paralympic Games, there are international events scheduled to take place in Japan in 2019, including the Rugby World Cup and the G20 Osaka Summit.

[20] The “Cybersecurity Strategy” states: “In addition to the sharing of information on cybersecurity threats among Olympic related organizations, such as the relevant ministries and governmental agencies, the Tokyo Organizing Committee of the Olympic and Paralympic Games, the Tokyo Metropolitan Government, local governments providing venues, and critical service providers, the government will promote the development of the Cyber Security Incident Response Coordination Center (Government Olympic/Paralympic CSIRT), the organization through which the government takes a role to coordinate the Olympic related organizations so that they can respond to cybersecurity incidents together when an incident occurs, and work to ensure the preparedness for close communication and coordination.”

[21] CEPTOAR: an acronym for Capability for Engineering of Protection, Technical Operation, Analysis and Response. This is the function for intelligence, sharing and analyzing information, by key infrastructure providers and the CEPTOAR-Council is the organization responsible for this function. In the financial sector, this covers four businesses: banks, securities companies, and life and non-life insurance companies (the secretariat comprises associations from each).

It is essential that the financial sector conduct threat intelligence on potential risks in a timely fashion and proactively address these to precisely counter cyberattacks. Given concerns that cyberattacks will become more sophisticated and complex and that their harm will extend beyond individual financial institutions to other financial institutions and throughout the entire financial system, the need for sharing such intelligence has steadily risen in recent years. There are particular concerns about an increase in cyberattacks, especially attacks and large-scale incidents that straddle various sectors, in connection with the 2020 Tokyo Olympic & Paralympic Games, making it necessary to collect not only information on incidents at financial institutions but also a broad range of information on critical infrastructure sectors such as the electric power grid and telecommunications sectors, third parties (outsourcing), developments overseas, etc.

Thus far, the FSA has actively used information provided[22] through industry groups (CEPTOAR-Council) as well as that disseminated by NISC to call the attention of financial institutions that could result in similar harm to incidents, and requested that they respond accordingly. In addition to this approach, the FSA has been preparing for the 2020 Tokyo Olympic & Paralympic Games by collaborating with NISC and others to conduct more effective threat intelligence than ever and, as necessary, to disseminate information to financial institutions and promote proactive responses[23].

(3) Promoting measures based on progress and evaluation thus far

In addition to addressing the new challenges mentioned above, it is important that the FSA utilize the progress and evaluation of measures under the current “Policy Approaches” in going through the PDCA cycle to further strengthen the financial sector’s cybersecurity countermeasures.

Cybersecurity risks differ by the business type and scale of financial institutions, their system configurations, business model features, etc., thus requiring cybersecurity countermeasures of varying complexity, but effective framework is required at all financial institutions. The FSA will look at the outstanding challenges based on the progress and evaluation of measures heretofore and, to accelerate financial sector’s cybersecurity countermeasures, will divide these into “cyber countermeasures as usual” (preparations against increasingly sophisticated and complex cyberattacks) and “incident responses” (suitable responses when incidents arise), tailoring responses to specific business type/scales/characteristics, etc.

[22] Implemented in accordance with the “Fourth Action Plan for Critical Infrastructure Protection” (approved by the Cybersecurity Strategy Headquarters on April 18, 2017; revised by the Cybersecurity Strategy Headquarters on July 25, 2018).

[23] The “Cybersecurity Strategy” stipulates: “Accordingly, the government must take the lead in sharing the information in its possession appropriately”.

With regard to audit firms, the FSA is encouraging more extensive and thorough use of IT-assisted audits, especially by major audit firms, as this is expected to produce in-depth audits that ensure greater effectiveness and efficiency. At the same time, there have been instances of audit firms overseas suffering harm as a consequence of being targeted by cyberattacks. Cybersecurity problems constitute managerial risks for audit firms, and cybersecurity needs to be steadily bolstered. The FSA will encourage audit firms to upgrade their readiness in line with the measures of financial institutions described below.

The FSA will seek to improve the effectiveness of information sharing frameworks and strengthen human resources development in the financial sector as industry-wide measures to ensure cybersecurity for the financial sector as a whole.

Furthermore, the FSA will review the methods by which it monitors the cybersecurity management systems of financial institutions in keeping with improvements made in financial institutions' cybersecurity management systems and changes in financial services driven by technological progress, and will select approaches effective for addressing specific cyber risks.

① Strengthening financial institutions' cybersecurity management systems

a Cyber countermeasures as usual

Given the risks anticipated in connection with the 2020 Tokyo Olympic & Paralympic Games, putting in place fundamental cybersecurity management systems and boosting their effectiveness have recently become major challenges for small and medium-sized financial institutions. For that reason, the FSA will pursue dialogue with cooperative central organizations and industry groups to promote the acceleration of preparedness, including implementation of cybersecurity risk assessments and contingency plans, to effectively raise the level of cybersecurity in the business sectors as a whole. Having ascertained the actual conditions and shared challenges of the industry overall through cybersecurity exercises, etc., the FSA will broadly familiarize industry members with the challenges to be addressed and then promote the necessary responses throughout the industry as a whole[24]. The FSA will also confirm the cybersecurity countermeasures of cooperative central organizations themselves and encourage them to implement necessary measures.

With regard to cybersecurity assessment of individual financial institutions and

[24] In program year 2018, the FSA will continue to encourage the financial institutions to underpin the fundamental cybersecurity management by utilizing the risk assessment manuals and contingency plan templates provided to the financial institutions as necessary. In addition, the FSA will verify the efforts being made to encourage the financial institutions to scan vulnerabilities and to implement the necessary security measures to manage these vulnerabilities.

dialogue with them, the FSA will verify the establishment of fundamental cybersecurity management systems (management team efforts, risk management frameworks, technical countermeasures and other controls, contingency plans, enhanced effectiveness through exercises, and cybersecurity audits), looking especially at security incident monitoring/analysis and vulnerability scan. In doing so, the FSA will determine the risk profiles of individual Shinkin Banks and credit unions, effectively assess their cybersecurity readiness by applying risk-based approach, and engage in dialogue. When financial institutions facing high cyber risks fall behind in their efforts and voluntary improvements cannot be expected, the FSA as necessary will conduct on-site inspections.

In this way, the FSA will be addressing the challenges of establishing fundamental cybersecurity management systems at small and medium-sized financial institutions and ensuring their effectiveness by effectively and efficiently linking up such methods as engaging in dialogue with cooperative central organizations and industry groups, assessing the cybersecurity readiness at individual financial institutions, and conducting on-site inspections.

The FSA will continue its dialogues with major financial institutions operating their businesses globally, keeping in mind the best practices of G-SIFIs and the developments in international discussions. The FSA will also conduct regular studies and analyses of the best practices of G-SIFIs and the developments in international discussions, bringing up outstanding efforts in the dialogues with major financial institutions and encouraging them to further upgrade their cybersecurity countermeasures.

b Incident responses

Even as cyberattacks become more sophisticated and complex, institutions are limited in their ability to quickly detect and defend against all cyberattacks, so post-attack responses will also be vital. An effective way to deal precisely with cyberattacks is to improve response capabilities while going through the PDCA cycle, e.g., trying out contingency plan-based responses during exercises to check whether the current response posture is sufficient.

The FSA has been holding financial industry-wide cybersecurity exercises (Delta Wall) annually to boost the level of cybersecurity countermeasures at small and medium-sized financial institutions in particular, and will continue to conduct such exercises as an important tool for improving the ability to respond to cyberattacks. In doing so, the FSA will be analyzing actual cyberattacks and utilizing the knowledge of outside experts to conduct these exercises with more practical content, envisioning the

cyberattacks posing the most likely threats in light of the characteristics of specific business. Additionally, the FSA will consider instances requiring responses by not just individual financial institutions but entire business sectors to, for example, broad-ranging attacks on shared infrastructure, to increase the sophistication of the exercise content. The business sectors participating in the exercises and the ex-post assessment criteria for the exercise outcomes will be reviewed as necessary.

Such exercises are being conducted not only by the FSA but also by NISC, Financials ISAC and others, and closer collaboration will be sought with these other parties to enable these exercises to offer a variety of options corresponding to the objectives and maturity of the financial institutions involved.

By supporting the participation of major financial institutions in joint exercises conducted by authorities in G7 countries, the FSA is looking to improve the ability of Japan's financial system as a whole to respond to large-scale, cross-border incidents. The FSA will also further boost responsiveness by promoting the utilization of high-level assessment methodologies such as threat-led penetration tests in light of the best practices of G-SIFIs and the developments of international discussions.

② Improving the effectiveness of information sharing frameworks

Ensuring cybersecurity is premised on "self-help" efforts [25] of identifying the cybersecurity risks that one's own organization faces and pursuing the cybersecurity countermeasures necessary in view of the information assets being used and the information technology possessed. In addition to such "self-help", the "mutual help" of financial institutions sharing and analyzing information among themselves has come to play an extremely large role as cyberattacks become more sophisticated and complex.

For that reason, the FSA is familiarizing financial institutions with the significance of "mutual help" utilizing Financials ISAC and other information sharing institutions and, given the difficulties faced by some small and medium-sized financial institutions in joining Financials ISAC in terms of geography, staff, or finance, collaborating with Financials ISAC, FISC and others to pursue intra-regional information sharing as a first step in "mutual help" efforts. More specifically, Financials ISAC and FISC are currently focusing their attention on regional activities, and the FSA will be working with Local Finance (Branch) Bureaus to provide active support so that these activities lead small and medium-sized financial institutions to participate in "mutual help" arrangements. In addition, FISC is striving to share information on cyber incidents with its members, and the FSA will provide backup support in this initiative.

[25] Efforts to develop human resources for the financial sector to promote "self-help" efforts are discussed in ③.

The “Cybersecurity Strategy” advocates the construction of an information sharing/collaboration structure transcending traditional frameworks and, with cybersecurity risk expanding, the FSA will pursue greater collaboration with financial industry groups other than critical infrastructure services (banks, security companies, life and non-life insurance companies) to promote “mutual help” efforts within the industry.

In connection with “public help” such as information provision from NISC and notices regarding incidents that have occurred at other financial institutions, the FSA will conduct threat intelligence more broadly than ever to rapidly uncover new cybersecurity risks stemming from advancing digitalization, and encourage financial institutions to take proactive responses by actively disseminating this information to the financial sector.

③ Strengthening the development of human resources in the financial sector

Active involvement by senior executives is extremely important in pursuing cybersecurity countermeasures, and the “Cybersecurity Strategy” calls for a “change in the thinking of senior executives”. To develop effective cybersecurity management systems, it is extremely important that financial institutions recognize the cybersecurity risks they face, e.g.,

- Responses by technical/IT departments → responses by management/ organization as a whole
- Front-line problems → management problems
- Scope of IT risks → scope of crisis/risk management

and then put in place countermeasures to business and corporate risks that require responses by their organizations as a whole; this will require a change in the thinking of senior executives. In its efforts thus far, the FSA has seen a major correlation between financial institutions pursuing cybersecurity countermeasures and the degree of involvement by the senior executives, and heightening awareness among senior executives is essential for boosting the level of cybersecurity in the financial sector.

Accordingly, the FSA will work with Local Finance (Branch) Bureaus to hold seminars for senior executives of financial institutions in various locales, will dispatch speakers to seminars and other events hosted by Financials ISAC, FISC and other relevant institutions to make senior executives more aware of cybersecurity and will continuously work to enhance human resources development in the financial sector.

The “Cybersecurity Strategy” also suggests establishing and fostering a strategic management level comprising personnel who serve as a bridge between senior executives and the operational/expert level. The FSA will promote the creation and

cultivation of this strategic management level at financial institutions by collecting information and providing feedback on good practices overseas and in other sectors[26].

Bolstering the knowledge of supervisory authorities, including Local Finance (Branch) Bureaus, is also essential for improving cybersecurity countermeasures at financial institutions. To help supervisory authorities develop human resources, the FSA will collaborate with relevant organizations to carry out specialized training for staff and will continue to send them to specialist graduate schools for outside training to strengthen its ability to conduct threat intelligence and monitor financial institutions.

[26] In the best practices of G-SIFIs, cybersecurity risk management is primarily the responsibility of the Chief Information Security Officer (CISO), and major financial institutions in Japan as well have begun establishing dedicated CISO positions.