Cybersecurity

Basic Approach

Amid accelerating digitalization and a changing environment for financial services, the posed by cyber threats is growing increasingly serious. To provide safer, more secure services to customers and achieve a society that is resistant to cyber threats, SMBC Group will further strengthen our cybersecurity.

Cybersecurity Management System

● Construction of management structure

Viewing cybersecurity risks as among the top risks faced by our management, we continuously engage in cybersecurity initiatives led by management under our "Declaration of Cybersecurity Management."

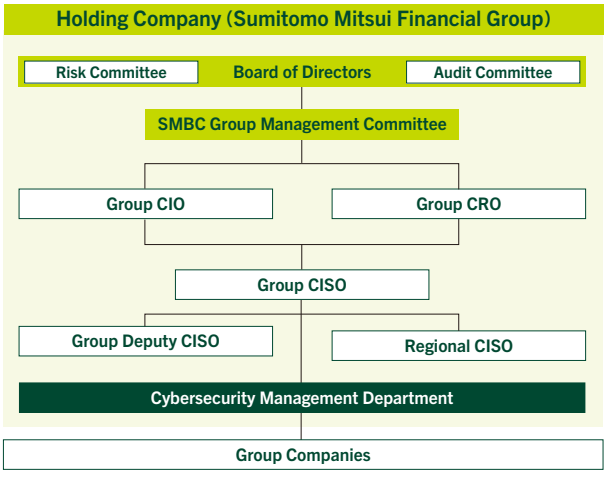
We manage cybersecurity risks within the framework of company-wide risk management. The Cybersecurity Management Department, a dedicated department for cybersecurity, leads the formulation of basic policy on cybersecurity management, based on the external environment, business strategy, and other factors.

The Group Management Committee regularly deliberates on cybersecurity management to further strengthen our system on the basis of the basic policy. In addition, the Board of Directors and internal committees such as the Risk Committee and the Audit Committee regularly deliberate cybersecurity management under the supervision of Directors.

To clarify the role of promoting effective security measures, we have put a Group CISO*1 in place under the Group CIO and CRO. As the party responsible for general oversight of cybersecurity, the Group CISO engages in supervision and guidance for the development of Group and global system and the promotion of measures at sites. Under the leadership of the Group CISO, we have appointed Group Deputy CISOs and regional CISOs, and have established a cybersecurity management structure encompassing over 600 people*2 on a Group and global basis.

*1 Chief Information Security Officer
*2 As of the end of March 2024

SMBC Group's Cybersecurity Management System



Identification of cybersecurity risks

We conduct identification of cyber threats through means including evaluations of cybersecurity-related structures.

Specifically, we undergo regular third-party evaluations of the degree of maturity of our security countermeasures, based on international standards.

We also make active use of threat intelligence to respond to the latest cyber threats. We collect and evaluate information on matters including geopolitical happenings, attack trends, and vulnerabilities, and apply this to our cybersecurity environment and to threat detection and defense.

We regularly conduct vulnerability diagnostics to deter damage caused by attacks on vulnerabilities, as well as threat-based penetration testing by which third parties penetrate actual systems to evaluate security measures. Based on the internal and external environment, we strive to identify cyber threats related to our Company and to further strengthen security measures.

Defense against and detection of cybersecurity risks

To prepare against unauthorized access, denial of service attacks, and other cyber attacks, we detect and block suspicious communications from the outside through varied security measure services and systems in a multi-layered defense structure.

We have also established a SOC*3, a dedicated organization for network monitoring and analysis, under a 24-hour, 365-day full-time monitoring system. Through ongoing close collaboration with SOCs established in Europe, the U.S., and Asia, we will further strengthen security surveillance on a Group and global basis.

*3 Security Operation Center

Response to and recovery from cybersecurity risks

We have established a CSIRT*4 in preparation for cyber incidents. By establishing a Cyber Fusion Center that integrates domestic security functions and human resources, we are working to enhance the efficiency of our management system and create an environment enabling quick response to incidents.

In preparation for cyber incidents, the CSIRT actively collects information on attack vectors and on vulnerabilities within and outside the Group, and shares this information as necessary with national authorities and bodies such as U.S.-based FS-ISAC*5 and Financials ISAC Japan.

In preparation against attacks, we are working to further strengthen our cyber resilience through regular participation in simulated attack exercises conducted by outside experts and cyberattack response exercises organized by the Financial Services Agency, Finances ISAC Japan, and other bodies.

*4 Computer Security Incident Response Team
*5 Financial Service Information Sharing and Analysis Center

Cybersecurity-Related Awareness-Raising Activities and Expert Human Resources

Awareness-raising activities

To foster a culture enabling conscious tackling of security measures, we conduct awareness-raising activities tailored to roles and responsibilities within the company.

For top management, we regularly hold study sessions on topics including management considerations in cybersecurity.

For executives and employees, we raise awareness of security through targeted attack email training and other actions, and use training to instill a “security by design” philosophy for IT system planning staff.

Expert human resources

We recognize that the development of expert human resources is a vital issue in maintaining a medium- to long-term cybersecurity management structure. We focus on the development of core human resources through the use of internal and external content, the introduction of a program that supports obtaining qualifications, dispatch of staff to graduate schools in Japan and abroad, and participation in external industry organizations.

We work to secure expert human resources through mid-career recruitment, and have set up a cybersecurity course for new graduate hires as a part of ongoing structural strengthening.