Information security risks and cybersecurity measures

SuMi TRUST Group considers information assets to be one of the most important management resources, and has set the protection of personal information and client data as one of the materiality themes. In addition, the Group also identifies information security risk as "Risk that the Group may incur losses due to the improper management or maintenance of information assets, including through information leaks, information errors and misuse of information, as well as an inability to use the information system," and positions it as one of the risk sub-categories under operational risk. It has assigned an officer in charge and established a control department to properly manage client information and implement cybersecurity measures.

In addition, we have established and announced our Declaration for the Protection of Personal Information, which is a set of policies designed to ensure the protection of the personal information of our clients and shareholders, and have declared to abide by them.

We established internal rules regarding the management framework and handling of information in accordance with the Personal Information Protection Act, related laws and regulations, and "Guidelines for Personal Information Protection in the Financial Field" established by the Financial Services Agency. We also hold regular training sessions for all employees twice a year to ensure that they are fully acquainted with the points of concern regarding the handling of information in their daily operations and to promote a principles-based understanding of information security.

(1) Organizational structure

Matters related to information security risk, as a risk sub-category within operational risk, are deliberated on comprehensively by the Risk Management Committee at SuMi TRUST Holdings and by the Operational Risk Management Committee at SuMi TRUST Bank, covering a series of processes such as the development of a management framework, formulation of plans, and the identification, evaluation, monitoring and control of risks. In addition, policies and plans are decided by the Board of Directors after deliberation by the Executive Committee.

Based on the rules regarding authority, the series of processes are executed by the Business Process Planning Department, the IT System Planning and Management Department, and other control departments responsible for information security risk management. The officer in charge of the Business Process Planning Department and the officer in charge of the IT System Planning and Management Department are responsible for overall information security risk management.

(2) Cybersecurity management system

The Group has designated addressing cyberattacks as one of materiality themes as well as a top risk, and we are planning and promoting our cyber security measures at the initiative of management through the formulation of "Cyber Security Management Declaration."

- We have established SuMiTRUST-CSIRT*1 as a specialized organization for cybersecurity measures, and have built a management framework that collects and analyzes threat and vulnerability information from within and outside the Group, plans and implements security measures, and reports to management. We are also promoting the upgrading of security measures through security review meetings and our IT Council, as well as by utilizing outside expertise.
- The Group has established internal rules and regulations based on U.S. security standards, and has developed processes for responding to cyberattacks both in normal times and in emergency situations.
- In addition to conducting cybersecurity risk assessments and system vulnerability assessments on a regular basis for SuMi TRUST Group, including its subsidiaries and affiliates, we are promoting the standardization of cybersecurity rules and regulations to enhance and standardize the cybersecurity framework for the Group as a whole.

(3) Monitoring system

The Group has built a common infrastructure for internet communications, and Security Operation Center (SOC) monitors the common infrastructure network 24 hours a day, 365 days a year and detects threats by conducting correlation analysis of various types of data. This information is consolidated in SuMiTRUST-CSIRT, and we have established a monitoring system centered on the CSIRT.

(4) Enhancing cybersecurity measures

We have established perimeter defense measures (multi-layered defense consisting of entry, exit and internal measures) as a technical countermeasure against cyberattacks, and are working to reduce risk by implementing various measures to counter DDoS attacks, detect and block phishing websites, and handle other threats.

(5) Security personnel development

To develop personnel with advanced expertise in cybersecurity, CSIRT collaborates with external experts in internal review meetings, participates in external communities such as Financial ISAC*2 and FS-ISAC*3, provides external training and certification support and sends employees to graduate schools.

*1 CSIRT (Computer Security Incident Response Team):
In-house organization that collects, analyzes, and responds to early warning information about attacks
*2 Financial ISAC (Information Sharing and Analysis Center):
Information sharing organization for Japanese financial institutions
*3 FS-ISAC (Financial Services Information Sharing and Analysis Center):
Information sharing organization for financial institutions, mainly in the United States