

Message

Message from the Chief Information Security Officer (CISO)



Manatomo Yoneyama
Senior Managing Executive Officer,
Executive Officer CISO
SuMi TRUST Group

As a financial institution that plays a critical role in national infrastructure, we place the highest priority on safeguarding our customers' diverse and sensitive information, including personal data. The cybersecurity landscape is evolving rapidly due to technological advancements in cyber threats and heightened geopolitical tensions. In addition, there has been a notable increase in attacks targeting the supply chains of Group affiliates and key business partners.

Cybersecurity threats are increasingly latent and complex, even within previously trusted perimeter-based defenses. As such, zero-trust security measures—which operate on the principle of “trust nothing” and verify all access—have become essential.

The SuMi TRUST Group has established a Chief Information Security Officer (CISO) and a dedicated CSIRT^{*1} (Computer Security Incident Response Team) to strengthen its cybersecurity posture not only through technical measures, but also through organizational and human resource initiatives. We are committed to continuously enhancing our cyber resilience so that customers can use our services with confidence and trust.

Topics

Enhancing Capabilities to Address Increasingly Sophisticated Cyber Threats

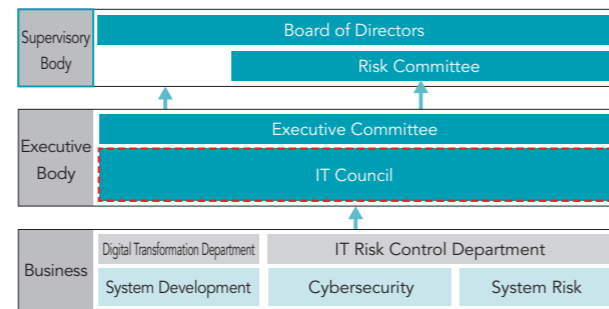
The SuMi TRUST Group has established a management framework within which the CSIRT collects and analyzes internal and external intelligence, formulates and implements countermeasures and introduces various countermeasures, and reports directly to senior management.

We proactively implement countermeasures against DDoS attacks and vulnerability exploitation, and continuously enhance multi-layered defenses, including phishing site detection and blocking.

In preparation for potential incidents, we conduct simulated cyberattack exercises with external experts and actively participate in security community initiatives, such as Financial ISAC², FS-ISAC³, and JC3⁴.

In April 2025, we established IT Risk Control Department,

which is responsible for IT-related risk management functions, and are enhancing our organizational framework and staffing, while advancing our capabilities to address increasingly sophisticated cyber threats.



1. Information Security Risks

Basic Policy on Initiatives and the Risk Management Framework

Based on recognition that information assets are among our most critical management resources, the Group has designated the protection of personal information and client data as a materiality theme. In addition, we have established executive officers and dedicated departments responsible for information security risk management, ensuring the appropriate governance of information assets.

Further, we have publicly issued our “Sumitomo Mitsui Trust Group Privacy Policy” as a statement of our commitment to safeguarding personal data.

We have also established internal rules and a management framework in accordance with relevant laws and regulations, including the “Guidelines for Personal Information Protection in the Financial Field” issued by the Financial Services Agency. In addition, we regularly conduct training sessions for all

employees to raise awareness of key considerations in daily information handling and to promote a principles-based understanding of data protection.

A series of processes, including the establishment of a risk management framework, the formulation of plans, and the identification, assessment, monitoring and control of risks, are comprehensively deliberated by the Risk Management Committee, and policies and plans are finalized by the Board of Directors following deliberation by the Executive Committee. These processes are executed by the Business Process Management Department, IT Risk Control Department, and other relevant departments in accordance with internal rules on authority. The overall risk management framework is overseen by the executive officers responsible for the Business Process Management Department and the IT Risk Control Department.

2. Cybersecurity Measures


(i) Basic policy and framework

The Group has designated cybersecurity as both a materiality theme and a top risk, and has formulated a Cybersecurity Management Declaration to guide the planning and promotion of cybersecurity measures under executive leadership.

Furthermore, through the Security Measures Review Committee and the IT Council, and by leveraging external expertise, we are advancing the enhancement and standardization of our cybersecurity framework. This includes the regular implementation of cybersecurity risk assessments and system vulnerability assessment, as well as the harmonization of related internal regulations across the Group.

IT Council

The IT Council serves as an advisory body to the Executive Committee, comprising the Chief Information Security Officer (CISO) as chair, executive officers and general managers from relevant corporate management departments, and external experts with specialized knowledge. It deliberates on critical matters related to system investments and technologies from a multifaceted perspective. From a risk management standpoint, the Council also discusses risks associated with system development, cybersecurity, and system operations, contributing to the enhancement of the Group's overall governance framework.



Cybersecurity Management Declaration
https://www.smtg.jp/english/-/media/tg/english/about_us/management/risk/pdf/CSMD.pdf

(ii) Cybersecurity

(1) Monitoring framework

The Group has established a shared internet communication infrastructure, and the Security Operation Center (SOC) conducts 24/7 monitoring of the network and detects threats through correlation analysis of various data sources. All relevant information is centralized within the CSIRT, which serves as the core of our cybersecurity monitoring framework.

(2) Technical measures

As technical measures against cyberattacks, the Group has implemented a multi-layered defense strategy, including perimeter (entry), outbound (exit), and internal controls. In addition, we continuously strive to collect and analyze threat intelligence, including information on attacker behavior, and to enhance our intelligence capabilities to support advanced vulnerability management across the Group.

(iii) System risk

To minimize the impact of large-scale system failures and natural disasters, and to ensure rapid recovery and business continuity, the Group has clarified its communication and response framework, developed contingency measures and recovery procedures, and conducts operational training and drills to strengthen overall resilience. In addition, for risks such as delays and cost overruns associated with large-scale system development projects, we monitor project progress and quality control, and report and consult with the IT

- Main measures
 - Detection and blocking of malicious communications
 - Prevention of virus and malware intrusions
 - Regulation of suspicious communications through behavioral analysis
 - Assessment and remediation of internet-facing vulnerabilities via vulnerability assessment
 - Detection of malware behavior at endpoints
 - Integrated analysis of communication logs from firewalls, proxy servers, and other sources to improve detection accuracy
 - Decryption and analysis of encrypted communications to expand detection coverage

(3) Human resource development

To cultivate personnel with advanced cybersecurity expertise, the CSIRT engages in collaborative discussions with external experts, participates in external security communities, and supports external training and professional certification programs. In addition, Sumitomo Mitsui Trust Bank, Limited continuously promotes employee education through information security training, phishing email simulation exercises, and cybersecurity drills conducted in collaboration with external organizations.

Council to ensure the appropriate governance of system development.

^{*1} CSIRT (Computer Security Incident Response Team): Internal team responsible for collecting, analyzing, and responding to early indicators of cyberattacks.
^{*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): Global information-sharing organization for financial institutions, primarily based in the United States.
^{*4} JC3 (Japan Cybercrime Control Center): A non-profit organization that facilitates cyber threat information sharing and analysis through collaboration among industry, academia, and government.