Cybersecurity

Our Approach

The risk of cyber threats is growing ever more serious as a result of the accelerated digitization of financial services and changes to the surrounding environment.
We will further strengthen our security measures in order to achieve a society that is resilient to cyber threats and provide safer and more secure services to our customers.

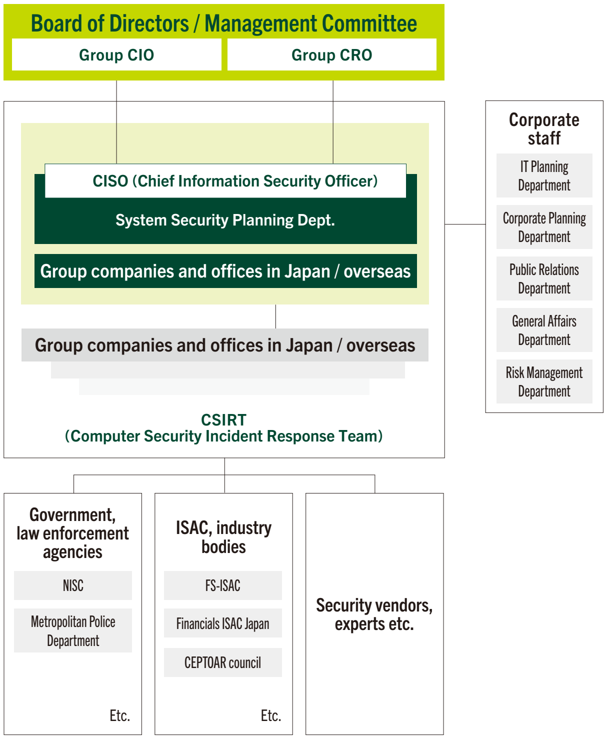
Cybersecurity Management System

Governance System

SMBC Group considers cyber threats to be one of the most important risks to its business, and is continuously promoting management-led cybersecurity initiatives under the “Declaration of Cybersecurity Management.”

In order to clarify the roles and responsibilities of promoting effective security measures, a specialist CISO*1 has been assigned under the Group CIO and CRO, and the Head of the System Security Planning Department is responsible for this role. The CISO promotes cybersecurity strategies in unison with management through discussions at meetings including the Management Committee meeting. Under the leadership of the CISO, the Company is creating a responsive posture to growing cyber threats on a group and global basis.

SMBC Group’s Cybersecurity Governance System


Board of Directors / Management Committee
Group CIO
Group CRO
CISO (Chief Information Security Officer)
System Security Planning Dept.
Group companies and offices in Japan / overseas
Group companies and offices in Japan / overseas
CSIRT
(Computer Security Incident Response Team)
Corporate staff
IT Planning Department
Corporate Planning Department
Public Relations Department
General Affairs Department
Risk Management Department
Government, law enforcement agencies
NISC
Metropolitan Police Department
Etc.
ISAC, industry bodies
FS-ISAC
Financials ISAC Japan
CEPTOAR council
Etc.
Security vendors, experts etc.

Incident Response System

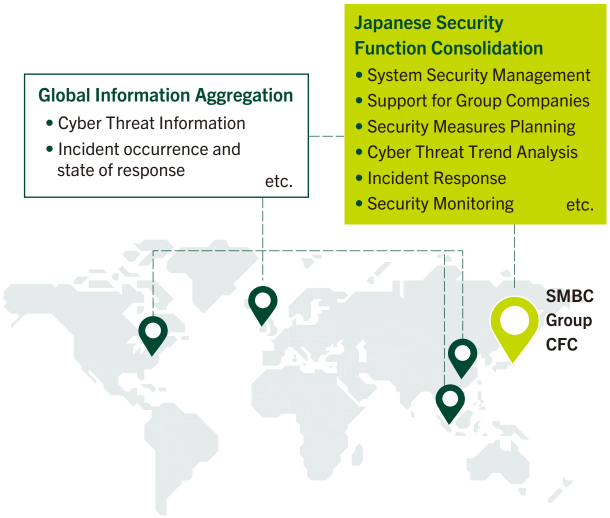
SMBC Group has established a Computer Security Incident Response Team (CSIRT)*2 and a Security Operation Center (SOC)*3 to create a response system with which to prepare for, and respond to, incidents.

The CSIRT is an organization in which the System Security Planning Department, responsible exclusively for cybersecurity, plays a central role. Working to ensure preparation for cyber incidents, the CSIRT actively gathers information on attackers’ methods and vulnerabilities from both within the Group and externally, and where necessary shares this information with national government agencies as well as with external institutions such as FS-ISAC*4 in the U.S. and ISAC in Japan.

The SOC is organized around the Japan Research Institute and has a 24-hour, 365-day monitoring system. We are also working to further strengthen security monitoring on a group and global basis in cooperation with SOCs established in Europe, the U.S., and Asia.

*1 Chief Information Security Officer

SMBC Group has also centralized its Japanese security functions at the Cyber Fusion Center (CFC) to ensure constant and close coordination between CSIRT and SOC.



Global Information Aggregation

- Cyber Threat Information
- Incident occurrence and state of response

etc.

Japanese Security Function Consolidation

- System Security Management
- Support for Group Companies
- Security Measures Planning
- Cyber Threat Trend Analysis
- Incident Response
- Security Monitoring

etc.

Key Measures related to Cybersecurity

Cybersecurity Measures

The Company possesses a multilayered defense system that includes detection and interception of suspicious communications from the outside, as well as operation and monitoring of various security services and systems, in preparation against various cyberattacks such as unauthorized and mass access attacks.

We also expect to further mature our intelligence functions, which collect and analyze information on attackers' latest tactics and trends.

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

Security Awareness and Professional Development

SMBC Group conducts ongoing awareness-raising activities through e-mail drills and study sessions to further foster a culture that encourages conscious efforts to address security measures.

In terms of professional personnel, we have actively recruited career professionals and established the Cybersecurity Course for new graduates recruited. We are also focusing on developing core personnel through further participation in external industry associations, sending staff to graduate schools in Japan and abroad, and supporting them in obtaining and maintaining professional certifications.

*2 Computer Security Incident Response Team

*3 Security Operation Center

*4 Financial Services Information Sharing and Analysis Center