Initiatives to Strengthen Cybersecurity

Basic action guidelines

At a time when technological advances in generative AI and quantum computing, accompanied by an intensification of digitalization efforts, are raising expectations of increasingly severe threats of cyberattacks in the future, Nanto Bank has designated cybersecurity as a key management priority to protect its customers' safety and information assets. Under the active leadership of senior management, the Bank as a whole is working continuously to strengthen its ability to respond swiftly to cyberattacks.

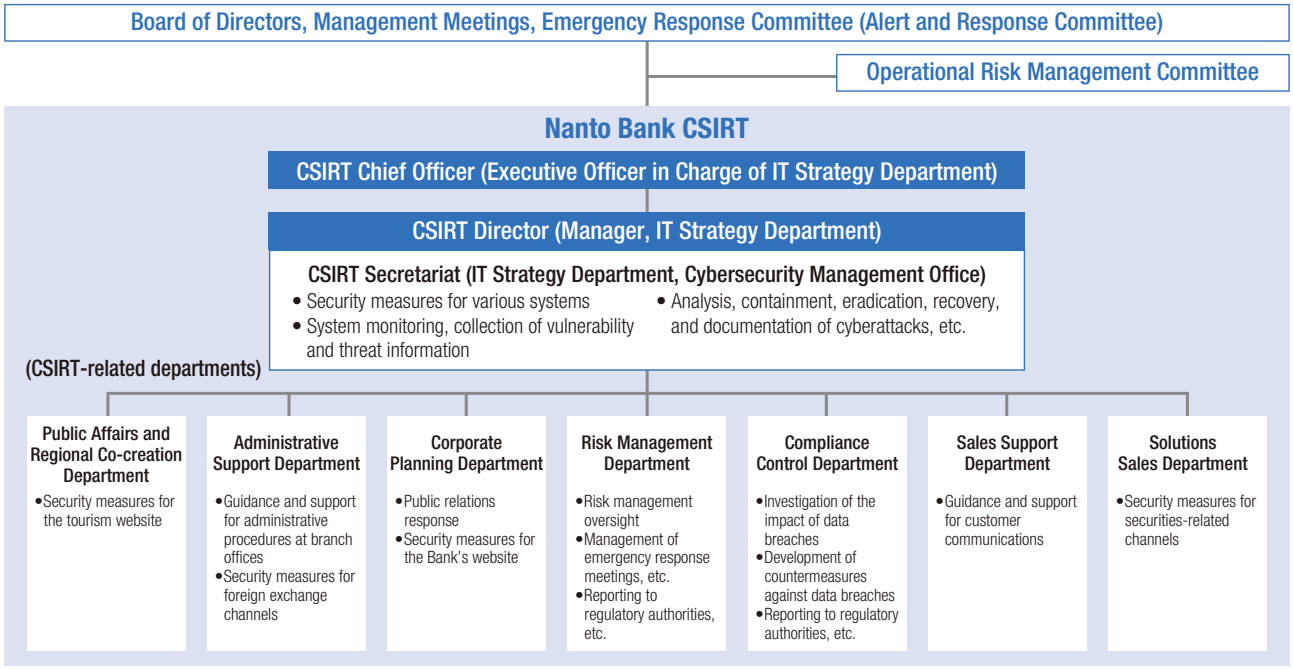
Cybersecurity management structure

Led by senior management and prompted by threats of increasingly sophisticated and complex cyberattacks, we established "Nanto Bank CSIRT*"—a cross-functional organization within the Bank that collects and analyzes intelligence concerning threats related to cyberattacks, investigates and responds to detected attacks, and implements security measures to defend against them.

In April 2026, with the aim of further strengthening various security measures and our response capabilities in the event of an incident, we established the Cybersecurity Management Office within the IT Strategy Department as a specialized unit dedicated to cybersecurity issues. We also added staff to reinforce our organizational structure.

*CSIRT (Computer Security Incident Response Team): An organization responsible for responding to computer security incidents.

■Nanto Bank CSIRT organization chart



Management involvement and governance reinforcement

The Bank's Information Asset Management Regulations stipulate that the Executive Officer in charge of the IT Strategy Department shall serve as CSIRT director. CSIRT meetings at the Bank center on items such as discussions of the progress on the medium-term roadmap and annual plans for cybersecurity, as well as the surrounding environment and challenges facing it. High-priority matters, such as changes in the Bank-wide security architecture, the results of self-assessments regarding the development of cybersecurity measures, and corresponding policies—are discussed and reported at Management Meetings.

Information on cyberattack incidents and internal and external trends is also reported to the CSIRT director and the Operational Risk Management Committee, ensuring that management takes the lead in strengthening cybersecurity measures, even during normal operations. With serious security incidents occurring more frequently even in Japan, we are increasing the frequency of our information-sharing with the CSIRT director—through weekly reporting and other means—to ensure more timely sharing of current internal and external conditions. Going forward, we plan to enhance our management-level engagement further and hold regular discussions at Board of Directors' meetings regarding the status of our initiatives and our cybersecurity posture.

As regards the "Guidelines on Cybersecurity in the Financial Sector" published by the Financial Services Agency in 2024, meanwhile, we are using these guidelines as a roadmap for strengthening our cybersecurity posture. We have conducted a self-assessment of our current status and formulated an action plan to address the guidelines. We are employing third-party evaluations conducted by consulting firms, moreover, to ensure the objectivity of our self-assessments and action plan and to further enhance our cybersecurity posture.

Cybersecurity measures

Ensuring convenience and security

The Bank is committed to maintaining a system infrastructure that balances convenience and security. As part of our 2025 system upgrade, we implemented state-of-the-art security measures that incorporate elements of the "Zero Trust Model," which does not rely on traditional perimeter-based security. By implementing such technologies as "endpoint detection and response (EDR)" and "microsegmentation," we have created an environment that enables employees to use the internet and cloud services safely and conveniently. This equips us to protect our customers' information assets securely while providing them with even greater value.

Emergency measures

Besides introducing various security measures to enhance our defenses due to the recent intensification of cyberattacks and incidents at other companies, we are also preparing for the possibility of large-scale ransomware infections. To this end, we are reinforcing our data backups to enable rapid recovery and developing BCP in preparation for prolonged outages of critical systems.

Third-party and outsourced vendor management

When accessing cloud services or outsourcing operations concerned with information systems, we evaluate the implementation status of their security measures based on the Bank's information system security standards. We proceed with implementation only if the standards are met, and we continue to conduct regular evaluations after implementation.
In light of the recent expansion of business stakeholders and the frequent occurrence of data breaches and system outages caused by cyberattacks originating from third parties, moreever, we are moving to strengthen our Bank-wide third-party management structures further and implement more rigorous management.

Education and training for executives and employees

In light of recent technological advancements, we conduct online training for all our executives and employees aimed at improving their IT and security literacy. We also carry out targeted email training that reflects current threat trends for all the executives, employees, and members of our Group. This includes monitoring their responses to suspicious emails and fostering a security-conscious mindset throughout the organization with awareness campaigns based on training results and recent threat trends. Drawing on examples of cybersecurity incidents at other companies, moreever, we are conducting cyber drills and BCP exercises that simulate potential incidents at our Bank.

Audit framework

The Audit Department conducts system audits every year to enhance the reliability of the Bank's operations by verifying its information system security.

To perform advanced audits that address recent trends in threats affecting financial institutions, moreover, the Audit Department collaborates with major consulting firms when conducting its cybersecurity audits. Based on guidelines such as the "Cybersecurity Management Guidelines" (Ministry of Economy, Trade and Industry) and "CIS Controls" (CIS, United States), we conduct audits of both organizational and technical aspects. The issues we identify are managed and addressed on an ongoing basis under the Nanto Bank CSIRT's annual plan, and the Audit Department monitors the progress of these initiatives. Through such efforts, we are making organization-wide efforts to strengthen our cybersecurity management framework.

When approaching cybersecurity, an ability to respond quickly and accurately to the rapidly changing threat landscape and assure secure executive-level involvement are critical capabilities. For this reason, I myself maintain a constant state of readiness to serve as a bridge between senior management and our front-line employees, while also working to accelerate decision-making and reporting.

Since cybersecurity risks can no longer be managed by any single department, we are reinforcing our cross-departmental framework by bringing together such departments as the Corporate Planning and Risk Management Departments, while working continuously to improve security literacy throughout the Bank.

This field is non-competitive, and while the Bank is already engaged in mutual assistance initiatives with participating banks in the "Chance" regional bank sharing system, we intend to expand these efforts to the local community in the future. We also plan to enter into agreements concerning cybersecurity and BCP with financial institutions in other regions to access the benefits from the mutual assistance this provides to help maintain our local customers' financial transactions and safeguard their information assets.



Manager, IT Strategy Department
Takayasu Sakagami