Cybersecurity Initiatives

Basic Policy on Cybersecurity

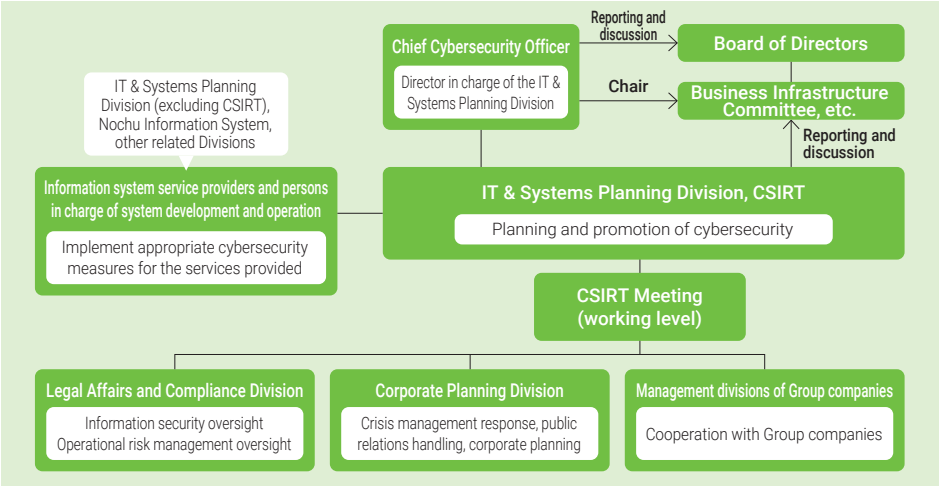
The Bank recognizes cybersecurity risk as one of its key management risks, with the potential to have a significant impact on business continuity and social trust. To minimize the risk of cyber incidents causing damage to the Bank's customers and/or disrupting the Bank's operations or the financial system as a whole, the Bank strives to maintain and enhance its level of cybersecurity.

Cybersecurity Structure

The Board of Directors has ultimate responsibility for cybersecurity. Under the leadership of the Chief Cybersecurity Officer, the IT & Systems Planning Division formulates the Bank's basic cybersecurity policies and promotes cybersecurity initiatives. The IT & Systems Planning Division also maintains a Computer Security Incident Response Team (CSIRT) to ensure readiness in normal times and a swift response when incidents occur.
The occurrence of cyber incidents, threat trends, and the status of cybersecurity measures are reported and shared regularly with the Board of Directors and the Business Infrastructure Committee established under the Board of Directors*. Based on this information, the Bank discusses and determines the direction of its cybersecurity policies and response measures.

* Reported to the Board of Directors twice a year and to the Business Infrastructure Committee at least four times a year.

Cybersecurity Structure



Cybersecurity Incident Response

The Bank maintains a 24/7/365 monitoring framework to detect signs of cyber incidents and is responsible for incident detection and analysis, damage containment, and recovery. During normal operations, it also monitors cyber threat trends and manages vulnerabilities to prevent incidents before they occur. In the event of a cyber incident, matters are escalated to the relevant parties according to the severity of the incident, enabling a Bank-wide response based on management's judgement. Where necessary, the Bank also works with external specialist organizations to prevent the spread of damage and support early recovery. In addition, the Bank has established incident response procedures and contingency plans for cyber incidents and conducts regular incident response exercises to confirm the roles and procedures of each division and enhance effectiveness.

Cybersecurity Management Process

To ensure the ongoing effectiveness of its cybersecurity measures, the Bank has established a cybersecurity management process comprising threat identification, risk assessment, implementation of countermeasures, operational monitoring and periodic review. Under this process, the Bank formulates a Cybersecurity Program and considers and implements the measures required in light of external threats, including changes in attack techniques, as well as internal vulnerabilities.
In FY2025, based on its assessment of the current state of its cybersecurity measures and external evaluations, the Bank formulated a cybersecurity action plan covering FY2026 to FY2028. Taking into account changes in threats and the system environment, the Bank regularly evaluates cybersecurity risks and the effectiveness of its countermeasures and improves and enhances cybersecurity measures based on the results.
In addition, the effectiveness of these cybersecurity management initiatives is verified through vulnerability assessments, penetration testing, and annual internal and external audits.

Education on Cybersecurity

The Bank provides ongoing cybersecurity education to all officers and employees to enhance cybersecurity awareness and literacy. This includes e-learning programs and phishing simulation exercises for all officers and employees. By providing training tailored to employees' roles and responsibilities, the Bank seeks to strengthen the cybersecurity capabilities required for their respective duties.

- E-learning for all employees to acquire basic knowledge of cybersecurity
- Newsletters to all officers and employees to enhance cybersecurity awareness
- Phishing email training for all officers and employees to raise awareness of, and readiness for, targeted phishing attacks
- Lectures by experts to improve officers' knowledge of cybersecurity
- Training by external experts to enhance CSIR's forensic capabilities