Cybersecurity and Data Privacy

Cybersecurity

KASIKORNBANK Public Company Limited ("the Bank") is committed to sustainable development encompassing environmental, social, governance, and economic dimensions, under its strategy to be a leader in digital banking in Thailand. The Bank recognizes the importance of cybersecurity and the protection of personal data in order to deliver secure, stable, and trustworthy services to its customers. This commitment extends to enhancing the cybersecurity of customers, business partners, counterparties, and companies within KASIKORNBANK FINANCIAL CONGLOMERATE, with the aim of ensuring the stability of the banking system and reinforcing the resilience of Thailand's financial information technology infrastructure both now and in the future.

In the past year, there were no significant cybersecurity incidents or data breaches within the Bank or KASIKORNBANK FINANCIAL CONGLOMERATE.

Cyber Risk Management Framework

The Bank has established a comprehensive cybersecurity risk management framework that encompasses governance, risk identification, prevention, monitoring and detection, incident response and recovery from threats, as well as the promotion of a cybersecurity-aware organizational culture. This framework aligns with the Cybersecurity Framework of the U.S. National Institute of Standards and Technology (NIST) and policies and best practice guidelines issued by regulatory agencies. In 2024, the Bank successfully enhanced its cybersecurity maturity to meet its target, achieving a level comparable to that of leading global banks, as assessed by a top-tier external consulting firm.

Information Security Management Approach

- The Bank has established an organizational structure to oversee the management of information technology and information security. This structure follows the Three Lines of Defense risk management model by clearly separating duties into the First Line of Defense, the Second Line of Defense and the Third Line of Defense. This structure ensures clear and independent responsibilities at all levels, including the Board of Directors and Sub-committees to operational units.

- The Bank has efficiently managed information technology and ensured the security of data and IT systems under three key principles: confidentiality, integrity, and availability.
- The Bank has established an IT Security Policy, which must be reviewed and updated at least once a year to ensure alignment with prevailing circumstances and potential risks. All employees, business partners, and external parties involved in the Bank's operations must strictly adhere to the prescribed guidelines. This policy applies to KBank and companies within the Financial Conglomerate and is aligned with ISO 27001. It encompasses security management measures in multiple areas, including:
    - Human resource security management
    - IT asset management
    - Information security
    - Access control to IT system
    - Use of portable computers and remote work practices
    - Security in IT system procurement and development
    - Encryption control and key management
    - Physical and environmental security
    - IT operational security
    - Communication network security
    - Third-party security management
    - Security incident management
    - AI security
    - Compliance with laws, regulations, and requirements

- The Bank has stepped up cyber risk control measures, including the prevention of sophisticated threats, improvements of cyber defense systems to guard against unknown attacks, enhancement of capabilities in monitoring and detection of threats, and timely and effective incident response in line with international standards.

- The Bank has improved incident response by establishing the Incident Response Team (IRT), which is responsible for centralized incident management. In addition, the Bank has developed comprehensive emergency plans covering various management aspects, including a Crisis Management Plan, Business Continuity Plan, and IT Disaster Recovery Plan. These plans are reviewed and cyber drills are conducted annually to ensure operational procedures and guidelines remain appropriate. Meanwhile, executives and staff are aware of and well-prepared to handle cyber threats effectively, ensuring business continuity under the prevailing circumstances.

- The Bank has continuously built a cyber hygiene culture across all levels, from the Board of Directors and executives to employees, through various knowledge-building initiatives, including basic cybersecurity e-learning courses and regular security newsletters on cyber threats. Additionally, simulated phishing drills have been conducted every quarter to ensure employees can properly identify, respond to, and prevent cyber threats. The Bank has also established clear incident reporting procedures, allowing employees to report potential cyber threats via email and a dedicated hotline.

- The Bank has raised awareness and prepared customers to deal with digital fraud through the SATI campaign, helping them stay informed about online threats and ward off current scams effectively. Such an initiative is achieved through the Bank's diverse communication channels, including websites, branches, and social media, ensuring a wide and comprehensive customer reach. Additionally, the Bank has educated its business partners and vendors about cyber threats and security standards, while regularly conducting joint cybersecurity drills to enhance preparedness.

- The Bank has enhanced risk management for its business partners and external parties to mitigate risks associated with service usage, connections, and data access. Such an initiative is achieved by establishing information security policies and standards, as well as implementing tools to assess the risks of business partners and external parties, starting from the onboarding preparation stage. Continuous risk monitoring is maintained throughout the business relationship, along with an alert system to notify of significant cyber anomalies when detected.

International Standard Certification

The Bank has continuously maintained ISO 27001 certification for information security management since 2014 and has been PCI DSS certified for credit card data security systems since 2019.