Principles for Board Governance of Cyber Risk
Case Study: SWIFT

MAY 2021

WORLD ECONOMIC FORUM

This case study offers one example of how boards can encourage systemic resilience and collaboration as recommended in the 2021 report Principles for Board Governance of Cyber Risk

Working to facilitate strong system-wide cybersecurity

After Bangladesh Bank became the victim of a cyberattack in February 2016, SWIFT rapidly launched its Customer Security Programme (CSP) to drive industry-wide collaboration in the battle against ongoing cyberthreats.

Customer Security Programme

Designed to support all types of customers, from central banks to commercial banks of all sizes, the CSP provides tools, information and a framework to help the community secure itself. The aim of CSP is simple – it seeks to raise the bar of cybersecurity hygiene across all of SWIFT's 11,000+ customers, reduce the risk of cyberattacks and minimize the financial impact of fraudulent transactions. It does this by focusing on three pillars:

- **Secure and protect** – The Customer Security Controls Framework (CSCF) establishes minimum and recommended cybersecurity requirements each SWIFT customer must have in place. These are reviewed and enhanced annually to meet the challenge of the ongoing threat.
- **Prevent and detect** – Tools such as Payment Controls, an intelligent in-network solution to combat fraudulent payments, help strengthen banks' existing security measures.
- **Share and prepare** – The Customer Security Intelligence (CSI) team investigates cyber incidents experienced by customers and shares vital threat intelligence across community information via the SWIFT ISAC portal.

Built on these overarching principles, the CSP works in partnership with the community and is designed to reinforce the cyber resilience of the global banking system. Given its breadth and depth and importance in the market, the CSP programme is subject to strong governance.

Governance process

SWIFT has strong and structured governance and oversight in place. SWIFT's board is composed of 25 independent directors, which reinforces the neutral, global character of its cooperative structure. Additional supervisory oversight is provided by the G20 central banks, which focus on the security, operational reliability, risk identification and resilience of SWIFT's infrastructure.

Role of governance during the CSP design phase

The SWIFT board and overseers were closely involved in the development of CSP and approved each major component of the programme. SWIFT also took into account customer feedback and perspective for major design decisions along the way.

Facilitating success

To ensure the long-term success of the CSP, SWIFT monitors and quality assures the effectiveness of the programme on an ongoing basis and provides regular updates to the SWIFT board and overseers. In addition, key metrics are tracked and shared regularly as part of the governance process.

Current status

At the end of 2020, institutions representing over 99% of all message traffic carried across the SWIFT network attested to their level of compliance against the CSP controls. The overall compliance level reported by customers for each individual mandatory control was between 93% and 99%.

The programme is delivering tangible results, showing its ability to recover the vast majority of funds targeted by attackers. While the CSP has reinforced security, this journey will never be over. The financial industry must continue to remain vigilant, work together, adapt processes and share information as a community to collectively strengthen its defences.