Reinforcing Cyber Resilience of the Financial Ecosystem

PURPOSE

In the light of the recent cyber events, the SWIFT Oversight Forum has developed this document to express its common understanding of the importance of the cyber security arrangements of SWIFT's users in the overall cyber resilience of the financial system. Therefore, financial institutions accessing the network should adhere to the guidance provided by SWIFT and are encouraged to actively engage to explore opportunities to enhance the overall cyber resilience. Members of the SWIFT Oversight Forum are sharing this document with the banking and financial market infrastructure supervisors in their jurisdiction to form the basis for a dialogue, including with their supervised entities.

SWIFT overseers will be actively monitoring the developments and assessing opportunities that authorities may pursue to raise awareness and enhance supervisory expectations.

SWIFT OVERSIGHT

The goal of the cooperative oversight of SWIFT is to obtain assurance that appropriate governance arrangements, structures, processes, and risk management procedures and controls are put in place by SWIFT to effectively manage the potential risks it poses to the safety and soundness of financial institutions and, more broadly, global financial stability. This is accomplished through a framework that focuses on objectives for the security, operational reliability, business continuity, and resilience of the infrastructure.[1]

RECENT CYBER EVENTS IN THE FINANCIAL ECOSYSTEM

SWIFT has informed the Oversight Forum and customers that recent cyber-attacks against participants of its financial messaging network did not compromise SWIFT's network, messaging services, or connections to the SWIFT network. However, these attacks have demonstrated that hackers have the capability to:

- compromise a financial institution's payment origination environment, bypassing the institution's information security controls;
- obtain and use valid operator credentials with the authority to create, approve, and submit messages from the financial institution;
- use highly-customized malware to disable security logging and reporting and other operational controls to conceal and delay detection of fraudulent transactions; and
- transfer stolen funds across multiple jurisdictions quickly to avoid recovery.

A financial institution with weak cyber security controls is vulnerable to such attacks. Cyber attackers are now increasingly sophisticated and capable of circumventing the broad spectrum of an institution's internal controls and functions. Consequently, financial institutions may be subject to significant financial losses and serious legal, compliance, and reputational risks.

GOVERNANCE AND RISK MANAGEMENT

Financial institutions should adopt the same strategies, frameworks, and measures on the governance and risk management of cyber threats as they do for other forms of risk faced

[1] Annex F of CPMI-IOSCO's Principles for Financial Market Infrastructures (PFMIs) is based on these high level principles. http://www.bis.org/cpmi/info_pfmi.htm

by, and posed to, the financial institutions. Given the escalating cyber threat environment, it is important for financial institutions to recognise that effective risk management of cyber risk should include both technical security controls and sound governance arrangements. In particular, the framework should cover risk management practices and controls over information technology (IT) and financial messaging networks, including authentication, authorization, fraud detection and prevention, and response management systems and processes. It should also cover people and processes. Ongoing assessment of a financial institution's ability to mitigate risks related to information security and third-party service provider management is also crucial to responding to threats that are sophisticated, persistent, increasing in frequency, and able to adapt rapidly.

The SWIFT Oversight Forum has listed below several sources of cyber security guidance.

CYBER SECURITY GUIDANCE

Financial institutions, ultimately, remain responsible for their own IT environment and infrastructure. Financial institutions should use multiple layers of security controls to establish several lines of defence and ensure that their risk management processes also address the risks posed by compromised credentials. Additionally, where applicable, financial institutions should consult guidance provided by their third-party service providers and their banking regulators for specific security control recommendations.

Established guidance on cyber resilience for financial market infrastructures and other financial institutions emphasize a number of elements. These included, but are not limited to:

a) ongoing information security risk assessments;
b) security monitoring, prevention, and risk mitigation processes;
c) protective measures against unauthorized access;
d) implementation and regular testing of critical systems controls;
e) timely and comprehensive information security awareness and training programs;
f) information sharing processes; and
g) assessment and management of risks related to third party service providers.

The following resources provide examples may support the development and management of an organization's cyber resilience framework.

Guidance for financial market infrastructures

- CPMI-IOSCO, "Guidance on cyber resilience for financial market infrastructures", June 2016, https://www.bis.org/cpmi/publ/d146.htm
- CPMI-IOSCO "Principles for financial market infrastructures," Annex F: Oversight expectations applicable to critical service providers http://www.bis.org/cpmi/publ/d101a.pdf
- CPMI paper "Cyber resilience in financial market infrastructures", November 2014 http://www.bis.org/cpmi/publ/d122.pdf

While these sources of cyber security guidance are targeting financial market infrastructures, the practices they cover are equally valid for banks.

Most jurisdictions have developed their own guidance, for example:

- FFIEC Cybersecurity Awareness. http://www.ffiec.gov/cybersecurity.htm
- Federal Reserve Banks Operating Circular No. 5 Electronic Access, Effective June 30, 2016. https://frbservices.org/files/regulations/pdf/operating_circular_5_06302016.pdf

SWIFT has consolidated its guidance to users on cyber security. SWIFT's additional practical resources and security statements on https://www.swift.com/