Cyber resilience practices – Executive Summary

The financial sector faces significant exposure to cyber risk given that it is information technology-intensive and highly interconnected through payment systems. Therefore, it is important for financial firms to strengthen their cyber resilience, which is defined by the Financial Stability Board (FSB) as "the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents."[1]

Within the financial sector, banks typically have the most public-facing products and services. Bank systems have multiple points of contact with outside parties, which can mean significant vulnerability to cyberattacks, with those interfaces being used as entry points for attacks targeting other parts of the financial system. Bank supervisory authorities have established regulatory and supervisory frameworks to enhance banks' cyber resilience. In 2018, the Basel Committee on Banking Supervision (BCBS) issued a report entitled Cyber-resilience: Range of practices that describes and compares regulatory approaches and supervisory practices across BCBS member jurisdictions.

Regulation and supervision

Regulators expect banks to address cyber risk either in their risk management and/or information security frameworks or in their specific cybersecurity strategies. The latter includes requirements related to governance and oversight; risk ownership and accountability; information security; periodic evaluation and monitoring of cybersecurity controls; incident response; business continuity; and recovery planning.

Supervisors assess banks' cybersecurity controls and their monitoring and surveillance of emerging threats. These assessments are based on banks' adherence to existing industry standards.[2] Supervisory assessments also include challenges to bank approaches to testing controls and the remediation of issues identified. Challenges can include the review of control testing reports, which may be part of a more formal testing programme. Such a programme could employ various testing methodologies and practices, such as vulnerability assessment, penetration testing and red team testing.[3]

[1] Financial Stability Board, *Cyber Lexicon*, 2018.

[2] For example, the cybersecurity framework of the National Institute of Standards and Technology; the standards of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (in particular, the ISO/IEC 27000 series on information security management, ISO 22301 on security and resilience and/or ISO 31000 on risk management); and the Control Objectives for Information Technologies framework for information technology governance and management.

[3] See eg FSI Insights, no 21, Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions.

Cyber incident response and recovery

Regulators expect banks to establish a framework for incident response and recovery that may include cyber-specific business continuity and disaster recovery requirements. To help financial institutions enhance their practices in this area, the FSB in 2020 issued a report entitled Effective Practices for Cyber Incident Response and Recovery that provides a toolkit featuring 49 practices across the following seven components:

1. Governance
2. Planning and preparation
3. Analysis
4. Mitigation
5. Restoration and recovery
6. Coordination and communication
7. Improvement

Third-party dependencies

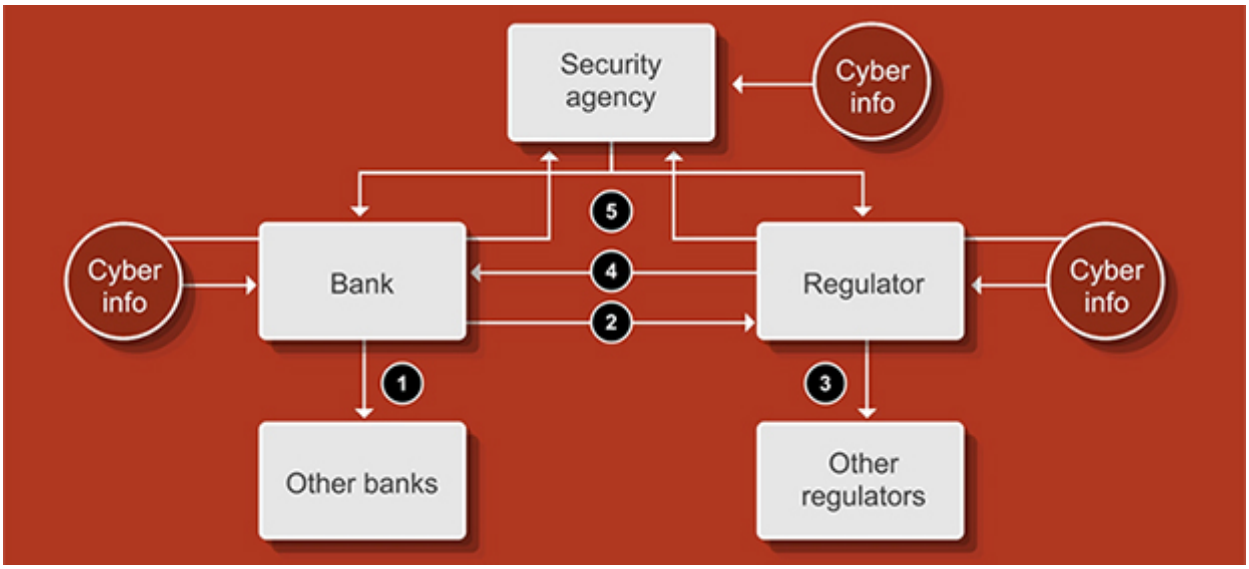
Regulators expect banks to account for business continuity and information confidentiality and integrity when dealing with third parties. Business continuity plans of critical third-party providers should align with the needs and policies of the bank. Confidentiality and integrity of information, on the other hand, are addressed in general data protection requirements and specific security requirements for safeguarding bank and customer information. Regulatory requirements for use of the cloud by banks may also apply. These include specific requirements on data location, data segregation, data use limitations, data security and treatment of data in the event of termination of a third-party arrangement.

Supervision of third-party dependencies relies on the ability of the authority to supervise these firms directly. When supervisors do not have oversight of third parties, one possible approach is to place the onus on banks to ensure that the third parties have the same security policies, procedures and controls that are expected of regulated firms. Another approach is to require service level agreements between banks and third parties to include a clause that allows supervisors to examine the latter's systems. In contrast, when supervisors have oversight of third parties, they may opt to assess for themselves the soundness of their cybersecurity, particularly for those that provide the most critical services.

Information-sharing arrangements

There are five types of cybersecurity information-sharing arrangement:

1. Sharing among banks
2. Sharing by banks with regulators
3. Sharing among regulators
4. Sharing by regulators with banks
5. Sharing with security agencies



The kind of information shared varies by type of information-sharing arrangement. For example, information related to cyber incidents is more widely observed in sharing by banks with regulators and with security agencies, whereas cyber threat-related information is the most common kind of information shared among banks.

Cyber resilience metrics

Supervisors are still developing metrics for measuring the quality of banks' cyber resilience. Early metrics have focused on using information from reported incidents, surveys, testing activities and on-site inspections. There is recognition of the need to develop more forward-looking cyber resilience metrics.

This Executive Summary and related tutorials are also available in FSI Connect, the online learning tool of the Bank for International Settlements.