Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions

Guidance on cyber resilience for financial market infrastructures

June 2016

BANK FOR INTERNATIONAL SETTLEMENTS

OICU-IOSCO

Observance of CPSS-IOSCO Principles for Financial Market Infrastructures and Cyber Resilience of FMI

Guidance on Cyber Resilience for FMIs

Accra | 1 February 2024

Agnija Jekabsone
Monetary and Capital Markets Department (MCM)
Payments, Currencies and Infrastructure division (PI)

CPMI IOSCO Guidance on cyber resilience for FMIs

IMPORTANCE: If FMI risks are not properly managed, it can be source of financial shocks. Level of operational resilience – decisive factor in overall resilience

PURPOSE: provide guidance for FMIs to enhance their cyber resilience

Not intended to impose additional standards beyond PFMI.

Supplement to help enhance cyber resilience:

Principle 2: Governance
Principle 3: Framework for the comprehensive management of risks
Principle 8: Settlement finality
Principle 17: Operational risk
Principle 20: FMI links

Two important PFMI elements:

- Clear and certain Final settlement intraday or in real time, and
- Ability to resume critical operations within 2 hours from disruption

Cyber lexicon*

CYBER RISK - Combination of the probability of cyber incidents occurring and their impact

CYBER ATTACK - Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets.

CYBER INCIDENT - A cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not.

CYBER RESILIENCE- The ability of an organization 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

CYBER SECURITY - Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

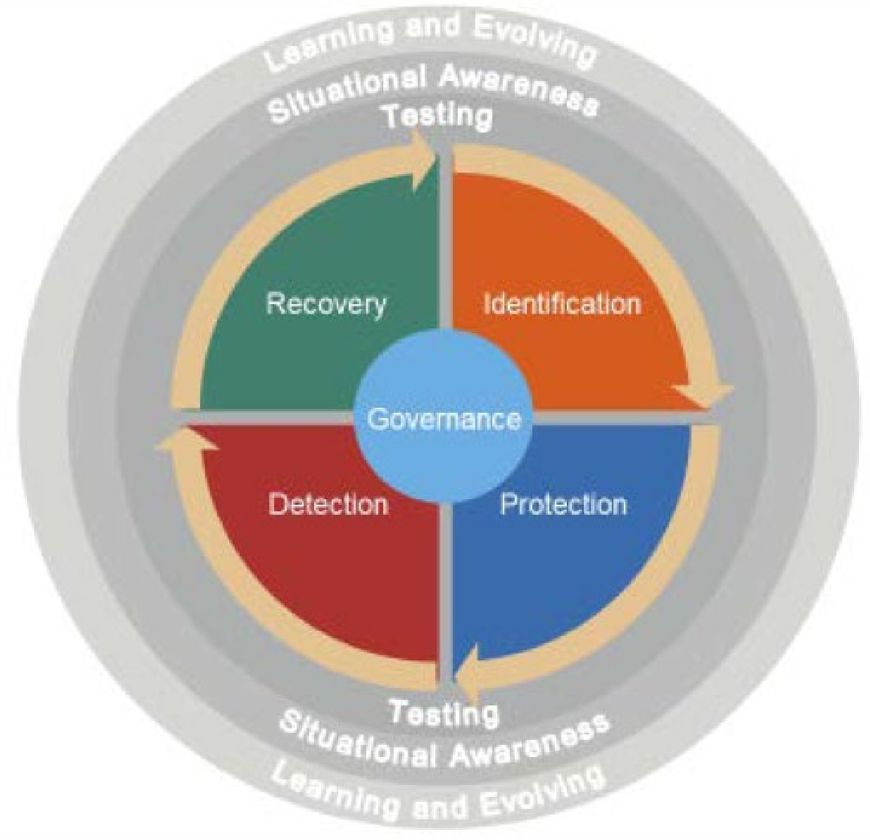
*Source: FSB

Uniqueness of cyber risks

1. Persistent nature, difficult to identify and breath of damage difficult to determine
2. Broad range of entry points: participants and linked FMIs, service providers, vendors and their products, FMI itself
3. Some risk management and business continuity arrangements – ineffective
4. Stealthy attacks propagating rapidly; exploiting vulnerabilities, weak links

Design of the Guidance

Five primary risk management categories and three overarching components



The risk management (RM) categories are:

- Governance
- Identification
- Protection
- Detection
- Response and recovery

The overarching components (OC) are:

- Testing
- Situational awareness
- Learning and evolving

Expected usage of the Guidance

- ✓ Directed at FMIs
- ✓ Reference for FMI’s board of directors, senior management and relevant staff
- ✓ For stakeholders – FMI’s participants, service providers, linked FMIs, and authorities
- ✓ Ongoing effort
- ✓ Risk-based approach in applying the Guidance, prioritize efforts
- ✓ Context of relevant legal framework; relevant for regulatory, supervisory and oversight authorities

RM1: Governance

Cyber resilience framework (CRF):

- How cyber resilience objectives and cyber risk tolerance is determined
- How identifies, mitigates and manage cyber risk
- Endorsed by the board
- Aligned with cyber resilience strategy;
- Cover people and processes.
- Reviewed and updated periodically
- Consistent with the enterprise operational risk management framework
- Takes an integrated and comprehensive view of FMI's ecosystem
- Aligned with leading international, industry level standards
- Clear roles and responsibilities.
- Assess effectiveness of CRF regularly through audits.

Roles of the board and senior management:

- FMI's board ultimately responsible for cyber risk management
- Cultivate appropriate culture
- Ensure appropriate skills and knowledge
- Ensure accountability

RM2: Identification

Identification and classification:

- Identify business functions and processes; understand importance and interdependencies; classify in terms of criticality.
- Identify and maintain inventory of information assets, system configurations as well as individual and system credentials; classify in terms of criticality.
- Facilitate regular review of critical business processes, functions, individual and system credentials and inventory of information assets.

Interconnections:

- Identify the cyber risks that FMI bears from and poses to entities in its ecosystem and coordinate.

RM3: Protection (1)

Protection of processes and assets:

- Implement controls in line with leading practice cyber resilience standards; proportionate to FMI’s threat landscape and role in financial system.
- Design cyber resilience from ground up; ensure rigorous testing; limit attack surfaces; adhere to common information security principles.
- Consistently maintain strong ICT control environment to protect information; ensure a comprehensive change management process; establish baseline system security configuration standards.
- Enable through FMI’s protective controls the monitoring and detection of anomalous activity across multiple layers of the FMI’s infrastructure.

Interconnections:

- Implement protective measures to mitigate risk arising from the entities within its ecosystem depending on risks and nature of relationship. Participation requirements should ensure support of cyber resilience framework. Cyber considerations should be integral part of vendor relationships and outsourced services.

RM3: Protection (2)

Insider threats:

- Implement measures to capture and analyze anomalous behavior by persons with system access
- Conduct background checks on new employees and all staff at regular intervals throughout employment; establish controls to mitigate risks of employment termination and change
- Permit physical and logical access to systems only for authorized individuals who are appropriately trained and monitored. Set controls to restrict access to those with a business need

Training:

- Ensure that all relevant staff receive training to develop and maintain appropriate awareness and competencies for detecting and addressing cyber-related risks.
- Provide to those with privileged system access or in sensitive business functions targeted information security training.

RM4: Detection

Detecting a cyber attack:

- Establish capabilities to continuously monitor and detect anomalous activities and events. Set up a “security operations center” (SOC)
- Monitor all relevant internal and external factors, including business lines, administrative functions and transactions. Detect vulnerabilities and misuse of access by service providers or other trusted agents, insider threats and other advanced threat activity.
- Set multi-layered detection controls covering people, processes and technology, with each layer serving as a safety net for preceding layers; apply approaches to delay or disrupt the attack; deploy an effective intrusion detection capability
- Ensure that detection capabilities facilitate incident response and information collection for forensic investigation.
- Implement measures to capture and analyze anomalous behavior.

RM5: Response and recovery (1)

Incident response, resumption and recovery:

- ➢ Perform a thorough investigation on nature, extent, and damage inflicted by cyber attack; contain the situation to prevent the damage.
- ➢ Notwithstanding the capability to resume critical operations within 2H, exercise judgment in effecting resumption not to escalate the risks to itself or ecosystem
- ➢ Plan for scenarios in which 2H RTO is not achieved, and for situations where critical people, processes or systems may be unavailable for significant periods.
- ➢ Develop and test response, resumption and recovery plans. Plans should be updated based on cyber threat intelligence, information-sharing, lessons learned and analysis of plausible scenarios; coordinate with stakeholders.

Design elements:

- ➢ Design systems and processes to limit the impact of cyber incident, resume critical operations within 2H, complete settlement by end of day, preserve transaction integrity. Integrate processes with crisis management, business continuity and disaster recovery planning.
- ➢ Have plans to identify the status of all transactions and member positions at the time of disruption; design and test the systems and processes to recover the data; include data recovery measures in the CRF.

RM5: Response and recovery (2)

Interconnections:

- Consider setting up in advance data-sharing agreements with relevant parties to obtain uncorrupted data once cyber attack has been identified.
- Work together with interconnected entities to enable resumption of operations when safe and practicable
- Plan for communications with participants, interdependent FMIs, authorities and others; develop communication plans; determine decision-making responsibilities for incident response in advance; implement clearly defined escalation and decision-making procedures; inform relevant oversight and regulatory authorities.
- Have policies and procedures to enable the responsible disclosure of potential vulnerabilities. Prioritize disclosures that could facilitate early response and risk mitigation by stakeholders.
- Have the capability to assist in or conduct forensic investigations of cyber incidents to facilitate the investigative process; establish relevant system logging policies.

OC1: Testing

Comprehensive Testing Program:

- Establish a comprehensive testing program to validate the effectiveness of CRF; employ cyber threat intelligence to inform testing methods; use results to improve cyber resilience; include internal and external stakeholders; involve board and senior management.
- Employ variety of testing methodologies and practices: Vulnerability assessment, Scenario-based testing, Penetration tests, Red team tests.

Coordination:

- Promote, design, organize and manage exercises to test response, resumption and recovery plans and processes; include participants, critical service providers and linked FMIs; include testing scenarios that cover breaches affecting multiple portions of ecosystem.

OC2: Situational awareness

Cyber threat intelligence:

- Identify cyber threats that could materially affect ability to provide services as expected, have significant impact or an effect on ecosystem; include threats which could trigger extreme but plausible cyber events; regularly review and update this analysis.
- Establish a process to gather and analyze relevant cyber threat information in conjunction with other sources of internal and external to provide business specific context turning the information into usable cyber threat intelligence.
- Include capability to gather information about cyber threats from participants, service providers and other FMIs and interpret it to allow to identify, assess and manage security threats and vulnerabilities to implement appropriate safeguards.
- Make available cyber threat intelligence to appropriate staff for mitigation of cyber risks.

Information sharing:

- Plan for information-sharing through trusted channels in the event of incident, collecting and exchanging timely information that can facilitate detection, response, resumption and recovery.
- Participate in information-sharing groups, including cross-industry, cross-government and cross-border groups to assess information on cyber practices, threats and early warning indicators; share information with trusted stakeholders.

OC3: Learning and evolving

Ongoing learning:

- Systematically identify and distil key lessons from cyber events within and outside the organization.
- Actively monitor technological developments and new cyber risk management processes to counter cyber attacks; consider acquiring technology and know-how.
- Aim towards achieving predictive capabilities, capture data from multiple internal and external sources.

Cyber Resilience Benchmarking:

- Analyze and correlate findings from audits, management reviews, incidents, near misses, tests and exercises as well as external and internal intelligence to benchmark against metrics and maturity models to identify gaps in FMI’s CRF

THANK YOU!