Building Robust Cyber Resilience Framework for FMIs – Safeguarding Financial Stability

Jan/Feb 2024

Bank of Mauritius (BOM)

Contents

Cyber Risks to FMIs and the Imperative for Strong Defences – The key aspects

Safeguarding FMIs for Financial Stability

- Financial Market Infrastructures (FMIs) are the lifeblood of the global financial system, facilitating critical functions like payments, clearing, and settlement.

Data Flows and Cyber Vulnerabilities in FMIs

- The interconnected nature and high value of data make FMIs prime targets for cyberattacks, posing significant risks to financial stability and to systemic impact

Cyber Resilience is the Cornerstone of FMIs Safety

- Building strong cyber defences is no longer optional, but an essential pillar for FMI safety and the overall health of the financial system.

The Bank of Mauritius (BOM) Championing Cyber Resilience in FMIs

Risk-Based Approach

- BOM employs a dynamic risk assessment methodology aligned with the PFMIs
- Also ensures that these principles are observed within BOM and by its participants

Prevailing Acts*

- BOM imposed and enforced its Authority

Clear Roadmap - Setting Expectations and Guidelines *

- BOM established clear and comprehensive guidelines for cyber resilience

Sharing of Information and Incidence reporting

- BOM encourages transparency

Continuous Evolution Landscape

- Encourage Improvement and Adaptability

*

- **Bank of Mauritius Act 2004**
- **Guidlines on Mobile Banking and Mobile Payments - 2013**
- **National Payment Systems Act in 2018**
- **Guidelines on Cyber and Technology Risk Management – Last updated 2023**

BOM Committees – Locally (Participants) and internationally(SADC)

- Sharing Experiences - (We have also National Cyber Security Strategy)

Awareness

- Educating and training personnel on cyber hygiene and best practices is critical for preventing human error and phishing attacks

Enhancing Resilience

- Having robust plans and procedures to detect, contain, and recover from cyberattacks

CPMI-IOSCO Best Practices and BOM Collaboration for Effective Cyber Resilience in FMIs

CPMI-IOSCO Guidance on Cyber Resilience for FMIs

- Outlines best practices for FMIs to build and maintain effective cyber defences.

The NIST Cybersecurity Framework (CSF)

- Offers risk-based approach with actionable functions and categories. Widely recognized and adopted globally.

G-7 Cyber Resilience Framework

- Provides a high-level framework for national and international cooperation in strengthening cyber defences.
- Promotes international cooperation and collaboration in cyber defence

BIS research and policy discussions on cyber resilience in FMIs

- Provides symbiolising shield Initiatives with respect to a globe with interconnected nodes representing FMIs

PCI/DSS for the card payments systems

- Builds and Maintains a Secure Card Network and Systems

BOM “Guidelines on Cyber and Technology Risk Management”

Appointment of a CISO with Key Functions

Cyber and Technology Risk Management Framework

- Develop and implement the Cyber and Technology Risk management framework
- Regularly review and update the framework based on evolving threats and regulations.
- Conduct risk assessments to identify, analyse, and evaluate cyber and technology risks.
- Develop and implement risk mitigation strategies and controls.
- Monitor and measure the effectiveness of risk management controls.

Reporting and Governance

- Be independent of IT Operations
- Provide quarterly reports to the board or designated sub-committees
- Report on key performance metrics, training and awareness program results
- Report on the threat landscape developments, and findings from testing, audits, and reviews.
- Ensure alignment of cyber and technology risk management practices

BOM “Guidelines on Cyber and Technology Risk Management”

Incident Management and Response

- Develop and implement an incident response plan to address cyber security incidents effectively.
- Investigate and remediate cyber security incidents promptly and thoroughly.
- Communicate cyber security incidents to relevant stakeholders in a timely and transparent manner.
- Conduct lessons learned exercises to improve future incident response capabilities.
- Branches and subsidiaries of foreign banks may designate a senior officer to fulfill CISO responsibilities.
- This officer should report to the group/regional CISO and have access to necessary resources.
- The board must ensure all guideline requirements are met and provide adequate oversight.

Security Awareness and Training

- Develop and implement a security awareness and training program for all employees.
- Regularly update the program to address new threats and vulnerabilities.
- Measure the effectiveness of the program and make necessary adjustments.

BOM “Guidelines on Cyber and Technology Risk Management”

Other Responsibilities:

- Stay informed about evolving cyber threats and vulnerabilities.
- Participate in industry forums and collaborate with other CISOs.
- Promote a culture of cyber security within the institution.
- Ensure compliance with relevant cyber security regulations.

Oversight Functions (Key Benchmarks for BOM)

Governance and Risk Management

- Cybersecurity Policies and Procedures
- Cyber Resilience Framework
- Board and senior management involvement
- Risk identification and assessment – Gap Analysis
- Control environment – Audit trails

Technology and Infrastructure

- Robustness of Infrastructures including Network (recommend an Active-Active mode System)
- Security of systems and applications (CIA principles)
- Third-party dependencies
- Incident detection and response capabilities
- Data security and encryption
- Root Cause Analysis (RCA)
- Backup Policies (Backup Encryption)

Human Resources and Training

- Security awareness and training
- Phishing and social engineering awareness
- Physical Security – Limit Access to Critical Systems
- Authentication- Least privilege access/SPwd/Two/Multi Factor
- Incident reporting and escalation process

Oversight Functions (Cont.)

Testing and Exercises

- Penetration testing and vulnerability assessments
- Cybersecurity simulations and exercises
- Disaster Recover and Business Continuity
- Scenario Based testing
- Lessons learned and improvement

External Environment and Collaboration

- Third parties
- Sharing of threat intelligence
- Vulnerability disclosures
- Regulatory compliance

Real Case Cyber Attacks , Scenario and Tools

Real World Cyberattack

Account Take Over (ATO) - Phishing

- Hackers compromise user credentials through phishing and gain access to online banking accounts, transferring funds or stealing information.
  In 2020, attackers used ATO to steal £2.3 million from UK banking customers during the COVID-19 pandemic.

Bangladesh Central Bank Heist (2016) – Malware Attack

- Hackers breached the SWIFT messaging system of the Bangladesh central bank and sent fraudulent transfer orders, stealing $81 million.
- This attack exposed vulnerabilities in SWIFT and the need for better cyber hygiene practices.

Lessons Learned:

- Strengthening SWIFT security protocols and access controls
- Implementing multi-factor authentication for critical systems
- Conducting regular security assessments and vulnerability testing
- Continuously applying the releases (ISO Standard 20022)
- Mandatory Swift CSP Program
- Effective Communication is important

Denial-of-Service (DoS) Attacks: Overwhelming websites or servers with traffic, making them unavailable to legitimate users.

In 2021, major US banks like JPMorgan Chase and Bank of America faced DoS attacks, impacting online banking services.

- Impact: Service disruptions, customer inconvenience, potential financial losses.

Monetary Authority of Singapore (MAS) monitoring Cyber Threat Alerts Tool

Singapore Cyber Threat Intelligence Platform (STIP)

- Launched in 2021
- Collects Cyber Threat Intelligence (CTI) among all Stakeholders
  - Local and Global FIs, Government, Threat Intelligence providers

Key Features

  - STIP Agents are installed on the Interconnected Eco-System
  - Automated threat feeds: STIP automatically ingests and analyses CTI feeds from various sources.
  - Threat intelligence sharing: FIs can securely share specific threat information relevant to other participating institutions.
  - Alerting and notification: STIP sends real-time alerts to FIs about potential threats relevant to their specific operations.
  - Investigation and incident response: The platform supports collaboration between FIs and authorities for investigating and responding to cyber incidents.

- Benefits of STIP
  - Enhanced Situational Awareness, Improved Threat Detection and Prevention, Collaboration and information sharing
  - Strengthened Overall Cyber Resilience

Phishing Attack Scenario – Leading to Ransomware, Data Exploits or Back Door Threats

- Preparation
  - Target Selection – Identification of the Victims
  - Information Gathering – Credentials on the target Organisation
  - Crafting the Lure – Designing the Phishing Content
  - Delivery Channel – Selecting Channel – Email/SMS/Phone Calls)
- Attack Execution
  - Delivery - The Phishing content is sent to the target
  - Social Engineering Urgency – The message has a sense of urgency
  - Clicking and Interaction –Opening of the malicious link
- Payload Delivery
  - Redirection – By Clicking it redirects to a Fake Site or Download a Malware to your Device
  - Credential Harvesting - Fake websites attempt to steal login credentials
  - Malware Execution: Control of Device and capture data
- Post-Attack
  - Bring your System Down and look for Ransom
  - Exploit your Data
  - Open Back door – Execute fraudulous transactions

KnowBe4 – A security awareness training and simulated Phishing Tool

Objective

- Mitigate organisation Human Resources falling Victims into Social Engineering Attacks

Security Awareness Training

- Provides a variety of training modules for employees on topics like phishing identification,
  password hygiene, and social engineering tactics.
- Engaging content formats - Interactive simulations, microlearning modules, and gamified experiences.
- Tracks employee progress and identifies areas where additional training is needed.

Simulated Phishing

- Sends realistic phishing emails to employees
- Utilises various templates and attack methods
- Provides analytics and reports to track employee clicks

Benefits

- Reduces risk of cyber attacks
- Improves Security awareness
- Compliance Support
- Better Reporting

BOM Ongoing Challenges

Evolving Threats and Landscapes

- Emerging Technologies and Rapidly changing attack methods
- Globalized threat landscape

Balancing Security and Innovation

- Overly prescriptive regulations
- Lack of harmonised standards

Resource Constraints and Expertise

- Limited Resources and need for expertised resources
- Retention of resources

Data Sharing and Privacy Concerns

- Sharing threat intelligence
- Access to sensitive data
- Cross-border data sharing
- Building Trusts with private entities for information sharing

Despite these challenges, effectively overseeing FMI cyber resilience is essential for maintaining a stable and secure financial system

The 2023 assessment through a questionnaire meets a score of 70% achieved /observed on the average 30 % needs to review /partly or not observed/or needs improvement

Building a Collective Shield: Our Shared Responsibility for Cyber-Resilient FMIs

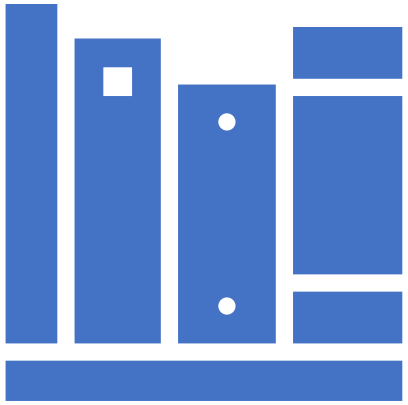
Cyber resilience is not a destination, but an ongoing journey

- Constant vigilance, adaptation, and collaboration are crucial for FMIs to stay ahead of cyber threats.

Building a secure financial future

- Strong internal cyber defences within FMIs
- Collaborative efforts between industry, authorities, and international organizations
- Continuous investment in education, awareness, and technological advancements.

By prioritising cyber resilience, we can safeguard the vital functions of FMIs and ensure the stability and prosperity of the global financial system.




End – Thank You - Q&A