INSTITUTE OF INTERNATIONAL FINANCE

November 4, 2020

Overview of CIRR practices of global banks

Martin Boer, Director

Regulatory Affairs Department

Financial sector perspectives

- **Cyber Risk in Context**
- **IIF-McKinsey Cyber Resilience Report**
- **The FSB CIRR toolkit**
- **Dueling Definitions**
- **Incident Reporting in Practice**
- **Policy Measures and Industry Practices**

Cyber Risk in Context

- Addressing cyber risk is among the top priorities for the financial industry, as well as for the regulatory and supervisory community – interests here are **aligned**

- Enhancing cyber resilience is critical given the frequency, scope and increased sophistication of cyber-attacks, also evident during the COVID-19 pandemic
    - Cyberattacks on financial institutions increased 238% between 1 Feb and 30 April as COVID-19 spread across the globe, and ransomware attacks increased ninefold over the same period*

- While the financial industry is widely understood to be exposed to a larger number of cyber-attacks than other industries it is also often credited for suffering lower costs, on average, thanks to proportionality greater investment in IT security
    - There was an 80% increase in cyberattacks over the 12 months that ended April 2020, among surveyed financial institutions*

- Effective cyber incident response and recovery critical to building resilience

* = *VMware Carbon Black (May 2020)*

IIF-McKinsey Cyber Resilience

Topics of the 4 survey sections, and summary of findings

Section	Topic	Summary of findings
A Firm-level cyber resilience	Capabilities of each firm in developing and strengthening firm-level resilience across 7 Financial Services Sector Cybersecurity Profile (FSSCP) functions	— Firms with over $1 trillion in assets have better cyber resilience — Largest vulnerability could be supply chain/dependency mgmt. — Out-of-date infrastructures are at risk for hacking — 37% said it takes more than 3 months to remediate a vulnerability — Companies are willing to share information with peers
B Sector-level cyber resilience	Information on collaboration between financial sector firms and the public sector to enhance sector-wide cyber resilience	— Many are willing to work together to raise resilience for all (e.g., 40% would do joint 3rd party / vendor due diligence) — Many would also participate in public platforms or initiatives
C Costs and FTEs	Participants' cyber risk dedicated spend and FTE numbers, including their roles and responsibilities	— 58% self-reported underspending — The protect function gets the most resources, some others are lacking
D Next generation questions	Future topics and integration of next-generation technology, agile methodologies, and cyber insurance coverage	— Cyber insurance levels are insufficient — Key challenges include cloud adoption, digital innovation, talent gap — Cloud adoption is both a challenge and an opportunity — Automation and artificial intelligence will see continued adoption

Source: IIF/McKinsey Cyber Resilience Survey March 2020

IIF-McKinsey Cyber Resilience

Companies can draw on 6 sets of immediate actions to enhance their cyber security posture

1 Do the basics, patch your vulnerabilities!

- ☐ Assess your current vulnerability scan coverage and patch management practices
- ☐ Build metrics and a dashboard to report regularly on the identified vulnerabilities and patch releases to CISO and BISO
- ☐ Require leadership oversight and accountability for delayed patch releases and accepted vulnerabilities

2 Review your cloud architecture and security capabilities

- ☐ Understand what data you are putting in the cloud now and minimize the presence of sensitive information there
- ☐ Implement a holistic cloud security strategy, emphasizing access management, threat monitoring and incident response
- ☐ Conduct regular penetration and vulnerability testing; audit reviews to ensure your cloud environment is secure

3 Reduce your supply chain risk

- ☐ Define a supply chain cybersecurity policy, and classify vendors based on the risk exposure they create
- ☐ Enforce enterprise-wide controls and a risk-based approach on your vendor intake process
- ☐ Develop monitoring and a response plan for supply chain cyber disruptions

4 Practice your incident response and recovery capabilities

- ☐ Continuously assess and refresh your incident response and recovery program based on your business risks and emerging threats
- ☐ Host regular table-top exercises on emerging threats, and conduct comprehensive resilience exercises to test response and recovery capacities

5 Set aside a specific cybersecurity budget and prioritize it

- ☐ Evaluate cyber spending against key risks and its impact on them - is it proportional?
- ☐ Assess ROI for cyber investments based on risk reduction
- ☐ Assess your cyber insurance spend and whether it addresses the cyber risk exposure faced by your business

6 Build a skilled talent pool & optimize resources through automation

- ☐ Review your cyber and risk teams' RACI and the complexity of your solutions and environment to identify skillset gaps
- ☐ Provide continuous learning opportunities to help employees adapt to new tools and technologies
- ☐ Identify operational processes for automation transformation to reduce human overhead

Source: IIF/McKinsey Cyber Resilience Survey March 2020

The FSB CIRR toolkit

- Complements FSB Regulatory Stock-take and FSB Cyber Lexicon projects
- CIRR can help strengthen the overall resilience of the financial system, especially for less mature firms on a proportional basis
- Voluntary and principles-based, and applicable to wider financial ecosystem
- Aligns with leading global practices to help reduce fragmentation
- Encourage the FSB to play a role going forward in the active debate taking place around an “event” and an “incident”
- Clear definitions and thresholds would greatly benefit both authorities and industry to prioritize what should be reported

Dueling Definitions

- No universal definition of neither “cyber event” nor “cyber incident”
- Firms have adopted internationally accepted standards from US NIST, FSB Lexicon, ISO 27000, NYS DFS, EU NIS DIRECTIVE
- This creates fragmentation and there are material differences between jurisdictions of what is in scope and what is material
- Establishing a standard terminology for cyber incident reporting would improve the quality of information shared, improving the analysis and understanding, as well as communication between the various stakeholders
- Interest of public sector and industry aligned on common definitions

Incident Reporting in Practice

- Rules and regulations differ substantially around the world:
  - Reporting a single incident to multiple authorities, complying with different thresholds, data set, communication channels, perspectives (e.g. payment, critical infrastructure)
  - Different taxonomies
  - Different type and/or nature of a cyber incident
  - Deadlines for reporting cyber incidents differ from country to country
  - Multiple stakeholders to report to within jurisdictions
- Having the right cybersecurity incident management system in place is essential
- Firms would benefit from more feedback from regulators
- Close cooperation with regulators and supervisors is critical

Policy Measures, Industry Practices

- Harmonization of incident reporting framework, definitions, thresholds
- Greater standardization of incident reports templates
- Central reporting hub (or database) for “one stop” incident reporting
- A common taxonomy for regulatory notification of cyber security incidents
- Closer cooperation through public-private platforms
- Enhanced cross-border architecture for information sharing
- Greater information sharing between regulators and financial institutions
- Ensure (future) regulation is risk-based, supports innovation, tech agnostic