Published on *The National Law Review* https://natlawreview.com

Cyber Resilience Guidance for Financial Market Infrastructures

Article By:

Rahul Kapoor

A. Benjamin Klaber

Recent guidance on cyber resilience for *financial market infrastructures (FMIs)*, published by the ***Bank for International Settlements*** and the ***International Organization of Securities Commissions***, urges each FMI to develop an adaptive cyber resilience framework in line with certain principles and in collaboration with its ecosystem.

The guidance recognizes that FMIs are critical to financial stability and offers comprehensive insight into enhancing cyber resilience, some of which is particularly relevant to the financial industry and much of which is generally applicable.

We highlight a few key takeaways below:

- Given the extensive interconnections in the financial system and the stealthy and dynamic nature of cyberattacks, each FMI should collaborate with its participants, vendors, regulators, other FMIs, and other stakeholders within its ecosystem. Such coordinated efforts should be ongoing and should include
    - a strong cyber threat intelligence and information sharing program, encompassing (a) bilateral undertakings with trusted stakeholders to dovetail security measures and augment recovery of uncorrupted data, and (b) multilateral arrangements to facilitate cohesive and safe responses to sweeping incidents;
    - resilience solution design, strategy, and implementation;
    - scenario-based tests, penetration tests, and other testing exercises—periodically and as systems are updated and deployed; and
    - system logging policies, including retention, to facilitate forensic investigations of cyber incidents.
- To maintain a healthy financial system, FMIs must settle obligations when they are due (and

at least by the end of the day). Therefore, FMIs are expected to maintain systems and processes that can safely resume critical operations within two hours of a disruption, even under extreme scenarios. FMIs should exercise judgment in resuming operations after an incident, however, balancing the gravity of end-of-day settlement against the risk of escalation and propagation of a cyberattack and its fallout. Given the importance of on-time obligation settlement, FMIs should carefully consider the availability, interconnectedness, and response times and procedures of any related services or systems (including those managed by vendors or other third parties). Such procedures should address failure to achieve timing objectives, resource unavailability, data recovery, and critical transaction processing. FMIs should consider including express contractual rights to information related to cyber risks in agreements with service providers.

- Each FMI should identify and rank its critical business functions and supporting information assets. Each cyber resilience framework should prioritize risk mitigation efforts based on the categorized resources and perceived cyber risks, which risks may vary and may not be proportional to the size of the relationship between an FMI and a participant or vendor. Such identification efforts should inform network segmentation and other approaches to resilient design. In addition to adjusting for its unique risk profile, each FMI should account for applicable laws and regulations when implementing the guidance.

- Each FMI should cement a culture, incorporating staff and stakeholders at all levels, of cyber risk awareness, communication, and proactive improvement. Each FMI should adapt and improve its cyber resilience framework on an ongoing basis, especially when it contemplates any material changes to its services, policies, or practices. Each FMI should continuously monitor and detect anomalous activities and events, including signature monitoring for known vulnerabilities, behavioral-based detection tools, and security measures focused on potential insider threats.

- FMIs should recognize that cyber resilience requires more than just a strong information and communication technology environment and is part of a broader risk profile. For example, people, processes, and timely communication should be integrated into the cyber resilience framework, and the FMI's approach to cyber risk should be consistent with the FMI's enterprise operational risk management framework.

National Law Review, Volume VI, Number 188