Responses to SEC Proposed Rule RIN. 3235-AN08: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

Prepared by Nozomi Networks, the leader in OT & IoT Security

1. **Requirements to adopt and implement written cybersecurity policies:**

   It is more important than ever before for every organization to review cyber risks and established cybersecurity policies across their enterprise business, departments, and operations. Policies and procedures are in near-constant flux as the cyber threat landscape and regulatory requirements, guidance, and best practices continue to morph in parallel. The need for early detection and eradication of unauthorized access and prevention of damage or sabotage cannot be overstated, though the mechanisms for preventing poor security outcomes and cascading impacts remain nuanced.

   For many sectors that fall under critical infrastructure, there lacks a shared threshold for classifying an incident. In some security policies, unauthorized access is treated as a security event to triage, and if impacts or poor outcomes are avoided or prevented by other security controls these events are not considered "incidents" to report. Regulated entities require more guidance on what severity or impact result meets the definition or threshold for an incident to report on. They also must be directed or required to keep security log information related to critical assets and networks for root cause analysis and remediation. Reporting may overlap with other regulatory bodies, and the SEC should consider ways to collaborate with sector risk management agencies for critical infrastructure to alleviate redundant or burdensome reporting mandates.

   Furthermore, when creating an incident response program, it is essential to determine the scope of your operations, to include enterprise and IT assets, as well as operational technology or cyber-physical systems, transient devices, and sensor deployment and networks. Any scope for established, maintained, and enforced written cybersecurity policy should include all critical assets, technologies, and networks associated with an entity – not only cyber risks associated specifically with information systems alone.

   Collectively, a broader scope of requirements will help entities raise the baseline of cybersecurity across the nation and may serve to identify and prevent potential single points of failure or cascading impacts across investment portfolios. The new requirements may result in a need for entities to utilize security event management tools, and/or monitoring and detection capabilities to identify, detect, respond, and remediate events and incidents. These tools will also be important for documenting compliance and verifying policies and procedures are enforced. Raising the bar on security is extended by addressing data retention and disposal which continues to exacerbate cybersecurity risk if not properly regulated.

2. **Expansion of regulation systems compliance and integrity releases:**

There is sometimes a delay in applying cybersecurity to business continuity and disaster recovery preparedness. With the proposed expanded scope of SCI entities to include (1) registered security-based swap data repositories; (2) all clearing agencies that are exempt from registration; and (3) certain large broker-dealers, incident categorization, severity indicators, and reporting requirements should consider what constitutes a localized incident vs. a more widespread or global incident with potential cascading impacts in terms of affected assets, services, or entities.

Directing entities to develop categorized inventories with classification of all SCI systems and programs for lifecycle management, prevention of unauthorized access, and management and oversight is a key requirement for raising the baseline of cybersecurity across the nation. These activities can reveal legacy systems that are no longer supported by their original vendors, accessible technologies that require additional security controls, gaps in perimeter defenses, frivolous movement and unnecessary access and retention of data, and more.

Plans should be exercised to failure – in some cases manual alternatives to processes and operations – to fully vet the potential impacts and severity of an incident. Reflecting again on the many nuances of different entities, their assets and risk landscapes, it is vital to discern what else is critically important beyond information systems as classically defined. This broader awareness will impact which stakeholders are part of the incident planning and response teams, how incidents will be triaged and classified, and who and how notifications will happen after an incident is assessed for severity.