PUBLICATION

SEC Issues Multiple Cybersecurity Rule Proposals

Authors: Matthew George White, Alexander Frank Koskey, III
March 28, 2023

The Securities and Exchange Commission (SEC) continued its focus on cybersecurity regulations this month by announcing three new proposed rules and re-opening the comment period on an additional proposed rule from last year.

Each of the proposed rules focuses on entities in the financial sector, including broker-dealers, investment advisers, investment companies, and other entities regulated by the SEC. The proposed rules would, among other things, require regulated entities to formally adopt policies and procedures for responding to cyber incidents, expand the scope of information subject to the rules to include information received from third-party financial institutions, and implement new requirements for reporting cyber incidents to both customers and regulators.

These proposed rules would impose significant new requirements on regulated entities. To prepare entities in the financial sector for these new requirements, this alert summarizes each of the proposals and provides best practices for designing your cybersecurity incident response plan.

Regulation S-P Amendments – The SEC's proposed amendments to Regulation S-P would require the following of broker-dealers, registered investment advisers, and investment companies.

- **Create an Incident Response Program:** Entities would be required to adopt written policies and procedures that address unauthorized access to, or use of, customer information, including procedures for notifying individuals affected by an incident. The proposed rule would also require regulated entities to notify affected individuals within 30 days after becoming aware that unauthorized access has occurred.

- **Expand Scope for New "Customer Information" Term:** The proposed rule would require regulated entities to apply safeguards to records containing "nonpublic personal information" that they collect, both about their own customers and that they receive from third-party financial institutions.

- **Records Disposal, Documentation, and Transfer Agents:** The proposal would also make several other amendments to Regulation S-P, including requiring enhanced procedures for disposing of consumer report information, extending the application of the safeguards provisions to transfer agents, and requiring covered entities to maintain written records documenting compliance with the proposed amended rules.

Additional Cyber-Related Policies and Procedures for Market Entities – Another proposal by the SEC would require these actions by entities including broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents (collectively, "Market Entities"):

- **Establish and Maintain Written Policies and Procedures:** Market Entities would be required to establish, maintain, and enforce written policies and procedures to address cybersecurity risks. This would include periodic assessments of cyber risks associated with information systems and maintaining written risk assessments.

- **Incident Response Procedures:** The proposed rule would also require Market Entities to implement measures and procedures to detect and respond to cybersecurity incidents, including written documentation of the response and recovery from an incident.

- **Reporting to the SEC and Public Disclosures:** Market Entities would have to report "significant cybersecurity incidents" to the SEC by filing a proposed Part I Form SCIR. If covered entities have reasonable grounds to believe that a significant cybersecurity incident has taken place or is in progress, they must instantly notify the Commission in writing. Furthermore, they must submit Part I of a new Form SCIR within 48 hours, which will be kept confidentially on EDGAR and contain thorough details about the incident. They must also continuously update this form if any substantial changes occur.

Expansion of Reg SCI – The third proposal would provide several updates to Regulation Systems Compliance and Integrity (SCI), including new specifications for required policies and procedures, as well as expanding the scope of covered entities. This includes the following, without limitation.

- **Expanded Scope of SCI Entities**: The proposed rule would expand the definition 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 – in particular, those that exceed a total assets threshold or a transaction activity threshold.

- **New Requirements for Policies and Procedures**: The proposal also includes additional provisions requiring that a covered entity's policies and procedures include a written inventory and classification of all SCI systems, and programs for life cycle management; prevention of unauthorized access to such systems, and management and oversight of certain third-party providers, including some cloud service providers.

- **Expansion of Notification Events and Other Requirements:** The proposed amendments would also expand the events that would trigger immediate notification to the SEC; update the rule's annual SCI review and its business continuity and disaster recovery testing requirements; and update certain of the regulation's recordkeeping provisions.

Additional Requirements for Registered Investment Advisers and Funds – Finally, the SEC announced that the comment period was reopened for a rule proposed last year relating to cybersecurity risk management and cybersecurity-related disclosures for registered investment advisers, registered investment companies, and business development companies. The proposed rule would, among other things, require adopting written cybersecurity policies, reporting cyber incidents to the SEC, and publicly disclosing significant incidents through brochures and registration statements.

Incident Response Planning and Best Practices

One of the primary areas of focus in all these rule proposals would be requirements for covered entities to respond to and report cybersecurity incidents. This also includes requirements that covered entities have written incident response plans. While having an incident response plan has been a "best practice" for some time, the SEC's proposals would potentially subject the contents of that plan to regulatory scrutiny.

It is, therefore, critically important for covered entities to focus on creating, developing, and refining their written incident response plans. This is not only an exercise of potential regulatory compliance, but also imperative to address the fluid landscape of cyber threats to protect the company and its customers. Covered entities must also include testing that plan through tabletop exercises and evaluating how to respond to wide-ranging incident variants. Covered entities must be proactive in taking steps to ensure they are prepared to respond to a cyber event.

The time to plan is *not* while under attack.

In evaluating your incident response plan, several critical considerations include:

- **Who is part of your response team?** Do you have representatives from the appropriate divisions? This should include not just your IT team, but also stakeholders from throughout the organization, including legal, public relations, human resources, operations, and representatives of the C-suite.

- **How will you classify the severity of an incident?** This will largely depend on how your most critical assets and operations are affected by an incident. How does your response differ depending on the severity of an incident?

- **Who has to be notified internally and when?** It its critically important to control information about an incident due to the effect it can have on liability and potential class-action lawsuits. Incident response plans have to include notification procedures for management, boards, and customer-facing personnel.

- **When do you need to notify regulators and/or law enforcement?** Cybersecurity reporting regulations and statutes are constantly changing and can vary significantly among geographic regions and sectors. That means incident response plans have to be updated regularly and reviewed by competent legal counsel to ensure compliance in the event of an incident.

- **What other third parties must be involved to contain and control the incident?** Vetting and retaining competent outside legal counsel, insurers, forensic vendors, e-discovery firms, and/or marketing/PR providers before any incident will allow for an efficient and timely response and recovery.

- **When do you need to notify customers?** All 50 states, various federal and industry-specific regulations, and international legal frameworks mandate individual notification requirements. Depending on the scope of the incident, each of these requirements may have to be taken into consideration and incorporated into your incident response plan.

These are some basic considerations to help you start thinking about how to create an incident response plan. Organizations must think through and address a host of considerations in developing their incident response plans. The time to develop these plans is *before* an incident occurs. Having a well-developed, current, and comprehensive response plan can make all the difference if and when an actual data incident occurs, and – if the proposed rules are passed – would also be a regulatory requirement.

If you have questions regarding any of the SEC's proposed regulations, need assistance in preparing or testing your incident response plan, or for any other cybersecurity- or data protection-related matters, please contact Matthew G. White, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, Alexander Koskey, CIPP/US, CIPP/E, PCIP, or any member of Baker Donelson's Financial Services Cybersecurity and Data Protection Team.