Debevoise & Plimpton | Data Blog

ARTIFICIAL INTELLIGENCE

The SEC's 2024 Examination Priorities: Continued Scrutiny of Cybersecurity Policies and Procedures

BY: CHARU CHANDRASEKHAR, LUKE DEMBOSKY, AVI GESSER, KRISTIN SNYDER, EREZ LIEBERMANN, MATT KELLY AND MENGYI XU - OCTOBER 18, 2023

On October 16, 2023, the SEC's Division of Examinations ("EXAMS") issued its 2024 Examination Priorities (the "2024 Priorities"). The 2024 Priorities reflect the Commission's continued scrutiny of information security and operational resiliency at registrants and the risks posed by third-party service providers, as well as new attention to artificial intelligence and other forms of so-called emerging financial technology.

1. **Information Security and Operational Resiliency**: EXAMS stated that "[o]perational disruption risks remain elevated due to the proliferation of cybersecurity attacks," among other factors. Accordingly, cybersecurity remains a "perennial focus area" for registrant examinations, and EXAMS will continue to review registrants' practices to protect "mission-critical" services and to protect investor

data and assets. The Division will additionally focus on registrants' policies and procedures, internal controls, oversight of third-party vendors, governance practices, and responses to cyber-related incidents, including those related to ransomware attacks.

2. **Reg S-ID Policies and Procedures**: In connection with such exams, EXAMS will consider staff training regarding Regulation S-ID (the Identity Theft Red Flags Rule) and the adequacy of policies and procedures to protect customer records and information.

3. **Firmwide Cybersecurity Across Branch Offices**:Because many registrants have a main office and multiple other offices, EXAMS will continue to look at practices to prevent account intrusions and safeguard customer records and information (such as personally identifiable information) across multiple offices.

4. **Vendor Risk Management**:EXAMS will continue to review vendor and third-party cybersecurity risk management, considering several different topics, including: the cybersecurity risks posed by third-party vendors; the security and integrity of vendor products and services; how registrants identify and assess vendor-related risks to essential business operations; and the unauthorized use of such providers. Consistent with its policy mandate, the Division will examine the concentration risk associated with third-party vendors, including how registrants are managing this risk and the potential U.S. securities marketplace impact.

5. **Artificial Intelligence**:In the context of crypto assets and emerging financial technology products ("fintech"), the Division will continue to examine new products and services and sales practices with an emphasis on technological compliance and marketing features for online accounts. In this context, the Division "remains focused on certain services, including automated investment tools, artificial intelligence, and trading algorithms or platforms, and the risks associated with the use of emerging technologies and alternative sources of data."

Takeaways

The continued focus in the 2024 Priorities on cybersecurity issues suggests that the Staff expects firms to continue demonstrating proactive efforts to reduce both the frequency and magnitude of cybersecurity incidents.

In previous posts regarding the SEC's cybersecurity priorities (including here and here), we identified multiple takeaways for firms based on SEC enforcement actions and guidance. These included: (1) Close Out Major Issues, (2) Prepare for the Need to Respond to and Recover from Ransomware, (3) Support and Document Senior-Level Engagement, (4) Perform Tabletop Exercises, (5) Provide Role-Based Employee Training, (6) Take Steps to Mitigate Risks from Credential Stuffing, (7) Enhance Programmatic Vendor Management, (8) Adhere to Cybersecurity Plans and Policies, (9) Revisit and Enhance Disclosure Controls, Where Necessary, and (10) Prepare for Supply-Chain and other Vendor Attacks.

The 2024 Priorities underscore the importance of these same measures, to the extent not already addressed, and they suggest firms should also consider the following:

1. **Revisit Business Continuity and Resiliency Preparations.** Firms should consider whether there are additional steps that they can and should take to prepare for, and minimize the impact of, business disruptions caused by cybersecurity incidents. Given the evolving tactics of threat actors, who often work to compromise the viability of recovery options in the course of executing an attack, various backup strategies may be less resilient and less helpful than anticipated in the event of a live incident. Steps to consider therefore include re-assessing the timeliness, security, and availability of backups, as well as the availability of fail-over systems that could be used to continue or restore operations, if needed.

2. **Reconsider Identity Theft Prevention Program Design and Implementation.** In light of the Staff's continued focus on firms' safeguarding and Reg S-ID obligations, firms should consider whether they have in place written policies and procedures reasonably designed to detect and address red flags of identity theft. They also should consider whether they conduct effective and appropriate training for employees to support the firm's compliance with obligations regarding customer accounts and information.

3. **Analyze Differences Between and Among Branches and Home Offices**. Firms should consider whether there are significant differences between the application of their cyber- and information-security policies, procedures, and controls between and among their various branches and offices. Any such differences should be examined carefully to ensure they are reasonable in light of the circumstances, and (if necessary) remediated.

4. **Vendor Risk Management.** Firms should consider the design and effectiveness of their third-party and vendor risk management programs. Among other risk areas to consider, firms should contemplate both (a) the risk of supply-chain and hub-and-spoke attack strategies, through which threat actors seek to compromise firm environments by taking advantage of third-party and vendor connectivity, and (b) the risk to sensitive or strategically important information held by third parties and vendors. Firms also may want to revisit the extent and prioritization of vendor diligence and oversight to test for compliance with cybersecurity-related terms and conditions, as well as the adequacy of documentation and records reflecting these efforts.

To subscribe to the Data Blog, please click here.

The Debevoise Artificial Intelligence Regulatory Tracker ("DART") is now available for clients to help them quickly assess and comply with their current and anticipated AI-related legal obligations, including municipal, state, federal, and international requirements.

The cover art used in this blog post was generated by DALL-E.

AI | AI COMPLIANCE | AI REGULATION | CYBERSECURITY | SEC

Charu Chandrasekhar

Charu A. Chandrasekhar is a litigation partner based in the New York office and a member of the firm's White Collar & Regulatory Defense and Data Strategy & Security Groups. Her practice focuses on securities enforcement and government investigations defense and cybersecurity regulatory counseling and defense.

Luke Dembosky

Luke Dembosky is a Debevoise litigation partner based in the firm's Washington, D.C. office. He is Co-Chair of the firm's Data Strategy & Security practice and a member of the White Collar & Regulatory Defense Group. His practice focuses on cybersecurity incident preparation and response, internal investigations, civil litigation and regulatory defense, as well as national security issues. He can be reached at ldembosky@debevoise.com.

Avi Gesser

Avi Gesser is Co-Chair of the Debevoise Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He can be reached at agesser@debevoise.com.

Kristin Snyder

Kristin Snyder is a litigation partner and member of the firm's White Collar & Regulatory Defense Group. Her practice focuses on securities-related regulatory and enforcement matters, particularly for private investment firms and other asset managers.

Erez Liebermann

Erez is a litigation partner and a member of the Debevoise Data Strategy & Security Group. His practice focuses on advising major businesses on a wide range of complex, high-impact cyber-incident response matters and on data-related regulatory requirements. Erez can be reached at eliebermann@debevoise.com

Matt Kelly

Matthew Kelly is a litigation counsel based in the firm's New York office and a member of the Data Strategy & Security Group. His practice focuses on advising the firm's growing number of clients on matters related to AI governance, compliance and risk management, and on data privacy. He can be reached at makelly@debevoise.com

Mengyi Xu

Mengyi Xu is an associate in Debevoise's Litigation Department and a Certified Information Privacy Professional (CIPP/US). As a member of the firm's interdisciplinary Data Strategy & Security practice, she helps clients navigate complex data-driven challenges, including issues related to cybersecurity, data privacy, and data and AI governance. Mengyi's cybersecurity and data privacy practice focuses on incident preparation and response, regulatory compliance, and risk management. She can be reached at mxu@debevoise.com.

Related Posts

Risk of AI Abuse by Corporate Insiders Presents Challenges for Compliance Departments

FEBRUARY 19, 2024

DOJ Announces Initiative to Combat AI-Assisted Crime

FEBRUARY 16, 2024

Webcast: NYDFS AI Requirements for Insurers Using AI or External Data

FEBRUARY 5, 2024

Top