Incident Response Plans Are Now Accounting Controls? SEC Brings First-Ever Settled Cybersecurity Internal Controls Charges

June 20, 2024

In an unprecedented settlement, on June 18, 2024, the U.S. Securities & Exchange Commission (the "SEC") announced that communications and marketing provider R.R. Donnelley & Sons Co. ("RRD") agreed to pay approximately $2.1 million to resolve charges arising out of its response to a 2021 ransomware attack. According to the SEC, RRD's response to the attack revealed deficiencies in its cybersecurity policies and procedures and related disclosure controls. Specifically, in addition to asserting that RRD had failed to gather and review information about the incident for potential disclosure on a timely basis, the SEC alleged that RRD had failed to implement a "system of cybersecurity-related internal accounting controls" to provide reasonable assurances that access to the company's assets—namely, its information technology systems and networks—was permitted only with management's authorization. In particular, the SEC alleged that RRD failed to properly instruct the firm responsible for managing its cybersecurity alerts on how to prioritize such alerts, and then failed to act upon the incoming alerts from this firm.

The settlement marks a striking expansion of the SEC's view of its oversight authority relating to public company cybersecurity policies and procedures. In particular, the SEC Enforcement Division's "expansive interpretation" of Section 13(b)(2)(B)—the internal accounting controls provision added to the Securities Exchange Act of 1934 (the "Exchange Act") by the Foreign Corrupt Practices Act of 1977 (the "FCPA")—as covering incident response policies is in clear tension with the Director of the SEC's Division of Corporation Finance's ("Corp Fin") recent statement disclaiming any intent on the part of the Commission to prescribe particular cybersecurity risk management policies and procedures. The RRD settlement also troublingly suggests that, in the wake of a successful cyberattack, public companies can expect the Enforcement Division to pursue any substantial intrusion as evidence of an underlying per se internal controls violation.

The R.R. Donnelley & Sons Co. Settlement

According to the SEC's Order, RRD was the victim of a 2021 cyberattack in which a "threat actor was able to utilize deceptive hacking techniques to install encryption software on certain RRD computers (mostly virtual machines) and exfiltrated 70 Gigabytes of data, including data belonging to 29 of RRD's 22,000 clients, some of which contained personal identification and financial information." The SEC alleged that RRD did not detect the incident on its own. Instead, approximately four weeks into the incident, "a company with shared access to RRD's network alerted RRD's Chief Information Security Officer ["CISO"] about potential anomalous internet activity emanating from RRD's network." RRD's cybersecurity personnel only then conducted an extensive response, which included shutting down servers and notifying clients and government agencies. RRD's investigation found "no evidence that the threat actor accessed RRD's financial systems and corporate financial and accounting data."

While RRD maintained an intrusion detection system that issued alerts that were reviewed first by the company's third-party managed security services provider ("MSSP") and then escalated to RRD cybersecurity personnel, the SEC alleged that RRD did not adequately respond to the MSSP alerts, including by not timely taking infected machines off the network and not conducting its own investigation until it had been notified by the company with shared access. The SEC alleged that RRD did not reasonably lay out "a sufficient prioritization scheme and workflow for review and escalation of the alerts" in its agreement with the MSSP, did not have sufficient procedures to oversee the MSSP's escalation of alerts and did not allocate personnel with sufficient time to respond to the escalated alerts. The SEC also found that RRD's internal incident response policies did not sufficiently identify lines of responsibility, provide clear criteria for prioritizing alerts or establish clear workflows for incident response and reporting.

According to the Order, RRD's "failure to design and maintain internal controls sufficient to provide reasonable assurances that access to [its] assets was permitted only with management's authorization was exploited by hackers," who exfiltrated data belonging to 29 of its thousands of customers during the ransomware network intrusion.

To settle the SEC's charges, RRD agreed to pay a $2.1 million civil penalty and consented to a cease-and-desist order that found that it violated two provisions of the Exchange Act in connection with its cybersecurity practices between November 2021 and January 2022: Section 13(b)(2)(B) (the internal accounting controls provision), which in relevant part requires issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that . . . (iii) access to

assets is permitted only in accordance with management's general or specific authorization," and Rule 13a-15(a) ("Controls and procedures" relating to disclosure). First, the SEC found that RRD did not reasonably design and maintain internal accounting controls as required by Section 13(b)(2)(B) because its cybersecurity alert review and incident response policies and procedures did not adequately establish a prioritization scheme or provide clear guidance for responding to incidents, and did not establish sufficient internal controls to supervise the MSSP's review and escalation of cybersecurity alerts. Second, the SEC found that RRD failed to design effective disclosure controls around cybersecurity incidents to ensure that relevant information would be communicated to management for timely disclosure decisions. The Staff specifically noted that, because RRD's controls were not designed to ensure that relevant information was escalated and did not indicate who was responsible for reporting to management, RRD failed to adequately assess such information for potential disclosure.

RRD was credited with cooperating with the SEC's investigation and with promptly taking remedial actions, including revising its incident response policies and procedures, updating training for employees and increasing cybersecurity headcount.

The SEC's Aggressive Expansion of Section 13(b)(2)(B) Internal Accounting Controls

The SEC's application of Section 13(b)(2)(B)'s internal accounting controls provision to RRD's cybersecurity controls is the latest example of the SEC's recent reliance on that provision to bring charges outside the accounting context for which this statutory provision was arguably intended.[1] Indeed, SEC Commissioners Hester Peirce and Mark Uyeda issued a blistering dissenting statement to the RRD settlement, arguing that the SEC has in recent years inappropriately treated "Section 13(b)(2)(B)'s internal accounting controls provision as a Swiss Army Statute to compel issuers to adopt policies and procedures the Commission believes prudent." Reviewing the historical context of Section 13(b)(2)(B), Commissioners Peirce and Uyeda argued that accounting controls "are concerned with the safeguarding of assets and the reliability of financial records" and conclude that while the accessed IT systems and networks are a company "asset in a broad sense," they are "not an asset of the type covered by Section 13(b)(2)(B)'s internal accounting controls provisions." Commissioners Peirce and

[1] *See* Order, *In re Charter Communications, Inc.*, Securities Exchange Act Release No. 98923 (Nov. 14, 2023), https://www.sec.gov/files/litigation/admin/2023/34-98923.pdf (settling alleged internal accounting controls failures relating to stock repurchases made through trading plans designed to comply with Exchange Act Rule 10b5-1); Order, *In re Andeavor LLC*, Securities Exchange Act Release No. 90208 (Oct. 15, 2020), https://www.sec.gov/files/litigation/admin/2020/34-90208.pdf (settling alleged internal accounting controls failures relating to share repurchases pursuant to Rule 10b5-1 plan while in possession of material nonpublic information).

Uyeda argued that the SEC's interpretation of "assets" to include a public company's IT systems and networks improperly allows the SEC to wield the provision wherever it identifies a public company's "departure from what the Commission deems to be appropriate cybersecurity policies."

By doing so, the dissenting Commissioners asserted that "the Commission's assurances in connection with the recent cyber-disclosure rulemaking ring untrue if the Commission plans to dictate public company cybersecurity practices indirectly using its ever-flexible Section 13(b)(2)(B)." This assertion apparently references the December 2023 statement from Corp Fin Director Erik Gerding, who said that the Commission was not "seeking to prescribe particular cybersecurity defenses, practices, technologies, risk management, governance, or strategy" through its new issuer cybersecurity disclosure rule. In this statement, Director Gerding acknowledged that "companies will have diverse approaches to cybersecurity, based on their particular circumstances, and that not every company needs formal policies and procedures" and emphasized that "companies have the flexibility to decide how to address cybersecurity risks and threats based on their own particular facts and circumstances." Gerding's statement echoes the commentary in the Adopting Release for the issuer cybersecurity disclosure rule that the "the purpose of the rules is . . . to inform investors, not to influence whether and how companies manage their cybersecurity risk." *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 88 FR 51896, 51912 (Aug. 4, 2023). As the dissenting Commissioners note, these statements on the limits of the issuer cybersecurity disclosure rule are hard to reconcile with the Commission's allegations that RDD violated Section 13(b)(2)(B) by failing to implement allegedly appropriate cybersecurity alert review and incident response policies and procedures.

An Open Question on the Scope of Internal Accounting Controls

As Commissioners Peirce and Uyeda identify, a worrisome disconnect persists between Corp Fin's assurances that the Commission is not prescribing specific cybersecurity policies or procedures and the Enforcement Division's appetite for dictating public company cybersecurity practices through the investigative and enforcement process. The RRD settlement does not provide any limiting principle for the scope of Section 13(b)(2)(B) enforcement. In theory, any public company victim of a successful cyberattack could face liability for an internal accounting control violation if it experienced internal cybersecurity control failures that enabled a threat actor to access and exploit the company's information systems or network. Indeed, the reality is that in hindsight almost every cybersecurity incident can be traced back to a weakness or limitation with a control that could potentially have helped to prevent it. But the Commission has not provided any guidance on what it views as appropriate

cybersecurity-related internal accounting controls. As a result, public companies are left to hope that—in the aftermath of an attack—their controls pass muster with the Enforcement Division.

The SEC remains free to pursue cybersecurity-related internal accounting controls violations for the time being. However, a federal district court may provide guidance in the coming months in *SEC v. SolarWinds Corp.*, 23-cv-09518-PAE (S.D.N.Y), in which SolarWinds has moved to dismiss the SEC's claim that the company violated Section 13(b)(2)(B) by allegedly failing to limit access to its "crown jewel" assets. A decision on that motion is expected in Summer 2024.

Best Practices for Public Companies

Given this emerging area of public company cybersecurity enforcement risk, issuers may wish to consider several enhancements to their cybersecurity policies and procedures, which we have covered in our prior Debevoise Data Blog posts here and here. These include:

- Consider steps to align cybersecurity risk management processes with industry standards.
- Consider a cross-functional risk assessment that assesses both policies and procedures, as well as technical cybersecurity controls.
- Develop a disclosure analysis framework that incorporates both qualitative and quantitative factors, that accounts for the broadened definition of "cybersecurity incident," and does not disclose information that would impede incident response and remediation.
- Consider enhancing oversight of third-party service providers and management of cybersecurity risks presented by such third parties. Review policies provided to MSSPs and other cybersecurity vendors to ensure they provide clear processes in place for the review of alerts.
- Ensure that the cybersecurity team has the right processes and controls in place to ingest alerts, act upon the alerts, and document these actions. Adequate staffing can be a limitation in a company's ability to address alerts promptly and appropriately. Consider engaging vendors to augment cybersecurity capabilities, as appropriate.

- Ensure that incident response plans will support the timely escalation of incidents involving third parties and encompass procedures for documenting the handling of such incidents.

* * *

Please do not hesitate to contact us with any questions.

To subscribe to the Data Blog, please click here.

Andrew J. Ceresney
Partner, New York
+1 212 909 6947
aceresney@debevoise.com

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Benjamin R. Pedersen
Partner, New York
+1 212 909 6121
brpedersen@debevoise.com

Julie M. Riewe
Partner, Washington, D.C.
+1 202 383 8070
jriewe@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
amoody@debevoise.com

Andreas A. Glimenakis
Associate, Washington, D.C.
+1 202 383 8138
aaglimenakis@debevoise.com