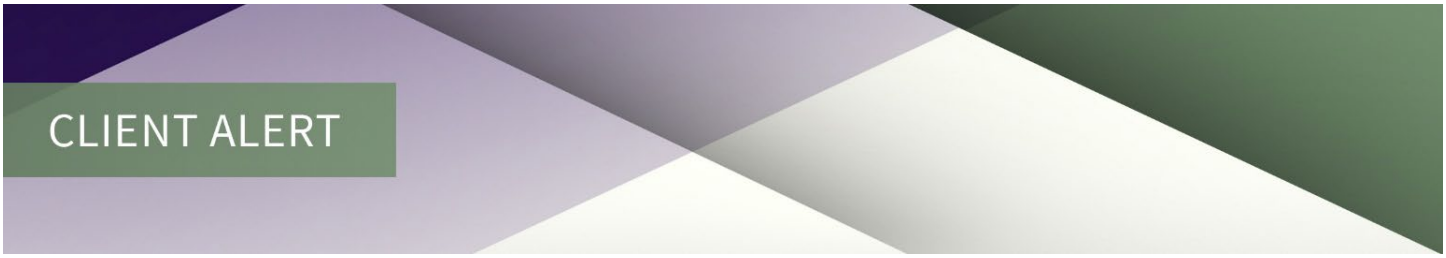

SEC Brings Cybersecurity Enforcement for Internal Controls Failures

June 28, 2024

AUTHORS

Adam S. Aderton | Daniel K. Alvarez | Laura E. Jehl | Michelle Bae Jahi Beal

On June 18, 2024, the Securities and Exchange Commission ("SEC") announced a $2.1 million civil penalty stemming from charges that disclosure and internal control deficiencies contributed to a failure to execute a timely and effective response to a ransomware attack at a public company in late 2021. In other words, this enforcement action suggests that (1) in some circumstances, the SEC may consider a public company's incident response plan as a key component of its accounting controls, and (2) the SEC may consider failure to have a carefully considered, resourced, and effective incident response plan in place a violation of SEC rules. This is the second time the SEC has publicly taken this stance, and the potential implications for public companies are significant.

What Happened?

According to the SEC,[1] R.R. Donnelley & Sons Company ("RRD") experienced a ransomware attack beginning on November 29, 2021. At the time, RRD's security incident response practices included an internal intrusion detection system, as well as a third-party managed security services provider ("MSSP") that was engaged to, among other things, review the alerts generated by the intrusion detection systems and escalate those alerts, as appropriate, to RRD's internal cybersecurity personnel. Despite having this system in place, and despite the system producing alerts triggered by the unauthorized activity on and after November 29, the SEC alleges that RRD did not take steps to prevent further compromise

[1] Press Release. *SEC Charges R.R. Donnelley & Sons Co. with Cybersecurity-Related Controls Violations*, U.S. SECURITIES AND EXCHANGE COMMISSION (June 18, 2024) available at https://www.sec.gov/news/press-release/2024-75; SEC Administrative Proceeding, *In the Matter of R.R. Donnelley & Sons Co.*, Release No. 100365, File No. 3-21969 U.S. SECURITIES AND EXCHANGE COMMISSION (June 18, 2024).

until December 23, 2021. Once RRD began actively responding to the attack, it took important steps to prevent expansion of the scope of the attack, such as shutting down affected servers. During the period before RRD acted, the threat actor was able to encrypt various RRD computers and exfiltrate 70 gigabytes of data, including data belonging to 29 of RRD's 22,000 clients. The SEC alleges that some of the data contained personal identification and financial information.

The SEC's Response

Although RRD maintained an internal intrusion detection system and engaged an MSSP to monitor and escalate issues, the SEC found that RRD's incident response plan was insufficient. Among other things, the SEC noted the RRD staff members who were tasked with reviewing and responding to the escalated alerts did not have sufficient time to respond to these alerts because they had significant other responsibilities. The SEC further found that RRD's internal policies governing incident response failed to establish clear workflows for alert review and incident response and reporting. Finally, the SEC found that RRD failed to maintain appropriate controls and procedures in the following areas:

- RRD's disclosure-related controls and procedures regarding cybersecurity incidents were not effectively designed to ensure all relevant information was reported to management to enable timely decision-making regarding disclosures or to ensure that guidance was provided to the personnel responsible for reporting to management;
- RRD's cybersecurity alert and incident response policies and procedures failed to adequately establish a prioritization scheme or to provide clear guidance to internal or MSSP personnel regarding response procedures; and
- RRD failed to design and maintain internal controls sufficient to provide reasonable assurances that access to RRD's assets—which includes its information technology systems and networks according to the Order—was permitted only with management's authorization, and that failure was exploited by hackers in the 2021 ransomware attack.[2]

Given all these issues, the SEC alleged that RRD's deficiencies amounted to a failure to manage its internal accounting controls for responding to a cyber incident in violation of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 ("Exchange Act"), which requires issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that … access to assets is permitted only in accordance with management's general or specific authorization." The SEC also alleged that RRD violated Rule 13a-15(a), which requires issuers to maintain disclosure controls and procedures.

[2] This is the SEC's second use of an internal controls charge in a cybersecurity matter. In the SEC's actions against SolarWinds, which is pending in the S.D.N.Y., the SEC alleged that shortcomings in SolarWinds cybersecurity controls constituted an internal controls failure. *SEC v. SolarWinds Corp.*, No. 1:23-cv-09518-PAE (Oct. 30, 2023 S.D.N.Y.).

Moving Forward

This is the second time that the SEC has applied Section 13(b)(2)(B) and Rule 13a-15(a) to public companies' cybersecurity practices, and represents a significant expansion of the conduct previously regulated by the SEC under these rules. That expansion did not go unnoticed by the two SEC Commissioners, Hester Peirce and Mark Uyeda, who issued a joint dissenting statement disagreeing with the majority's interpretation of Section 13(b)(2)(B), arguing that the expansive interpretation of what constitutes an "asset" under that provision exceeds the limits of the Exchange Act.[3] The Commissioners indicated concerns that the SEC's expansive interpretation of treating computer systems as an "asset" subject to the internal accounting controls provision does not establish proper limits of Section 13(b)(2)(B)'s requirements. They further argued that the SEC's broad interpretation gives it "a hook to regulate public companies' cybersecurity practices," and would allow the SEC to "stretch the law" to punish a company that had been the victim of a cyberattack.

Regardless of where one falls on the policy and legal questions, the dissenters are not wrong about potential implications for public companies moving forward. The settlement reaffirms the SEC's heightened focus on issuers' cybersecurity practices. The SEC's novel use of Section 13(b)(2)(B) to include incident response and cybersecurity management practices in its definition of internal accounting controls creates new uncertainties for issuers, even those that have implemented seemingly reasonable cybersecurity practices. The settlement leaves open the possibility that any public company could be subject to an SEC enforcement action if it becomes the victim of a cyberattack and the SEC later determines that the company's cybersecurity practices were inadequate. Basic cybersecurity controls and practices will not suffice — companies need to ensure that they have sufficiently robust teams in place, with appropriate policies, resources, lines of communication, and decision-making authority to act in the event of an incident.

[3] Statement of Commissioners Hester M. Peirce and Mark T. Uyeda. *Hey, Look, There's a Hoof Cleaner! Statement on R.R. Donnelley & Sons, Co.*, U.S. SECURITIES AND EXCHANGE COMMISSION (June 18, 2024) available at https://www.sec.gov/news/statement/peirce-uyeda-statement-rr-donnelley-061824?utm_medium=email&utm_source=govdelivery.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Adam S. Aderton
202 303 1224
aaderton@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Michelle Bae
202 303 1166
ebae@willkie.com

Jahi Beal
202 303 1002
bbeal@willkie.com