Akin®

SEC Cyber Enforcement Continues: More Scrutiny of Internal Controls

July 18, 2024

Reading Time : **4 min**

By: Natasha G. Kohne, Jesse Michael Brush, Garrett A. DeVries, Rosa A. Testani, John Patrick Clayton, Ryan Dowell, Joseph Hold

On June 18, 2024, the United States Securities and Exchange Commission (SEC) announced a settlement with R.R. Donnelley & Sons Company (RRD) for alleged internal control and disclosure failures following a ransomware attack in 2021. Without admitting or denying the SEC's findings, the business communications and marketing services provider agreed to pay a civil penalty of over $2.1 million to settle charges alleging violations of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 (Exchange Act) and Exchange Act Rule 13a-15(a).[1]

Background

RRD's relevant services involved storing and transmitting confidential client data on its network (from clients such as SEC-registered firms, healthcare organizations, publicly traded companies and financial institutions), including personal identifying information, financial information and business plans. According to the Order Instituting Cease-and-Desist Proceedings (SEC Order), RRD's wide variety of applications and network structure meant that its alert system for intrusion detection was very complex.[2] RRD used a third-party managed security services provider (MSSP) to conduct initial review and analysis of alerts before escalating to RRD's internal cybersecurity personnel.[3]

Per the SEC Order, a ransomware intrusion occurred between November 29 and December 23, 2021, during which time the MSSP escalated alerts to RRD's internal security personnel.[4] The SEC also alleged that RRD did not "reasonably manage" the MSSP's resource allocation for alert review.[5] Although RRD reviewed the alerts, they did not conduct their own

investigation, remove infected instances from the network or conduct any remedial steps, while the threat actor installed encryption software and exfiltrated client data.[6] RRD began responding on December 23, 2021, after another company that shared access to RRD's network alerted RRD's Chief Information Security Officer (CISO) about anomalous activity coming from the network.[7] This last alert led to a response operation by RRD's security personnel, which included shutting down servers and sending notices to clients and government agencies.

Disclosure and Internal Controls for Cyber Incidents

The SEC stated that protecting data confidentiality and integrity was critically important for RRD's business, therefore the company should have had effective disclosure controls and procedures to address cybersecurity incidents and to ensure information passed up the chain to decision-makers in a timely manner. The agency argued that RRD's cybersecurity practices violated the requirements of Exchange Act Section 13(b)(2)(B) to maintain sufficient internal accounting controls to prevent assets from being accessed without management authorization; and Exchange Act Rule 13a-15(a) to maintain internal disclosure controls necessary to ensure information is recorded, processed, summarized and reported within specified time periods.

Specifically, according to the SEC Order, RRD violated Exchange Act Section 13(b)(2)(B) and Exchange Act Rule 13a-15(a) by failing to:

- Design effective disclosure controls and procedures for escalating all relevant information related to cybersecurity alerts and incidents to decision-makers
- Respond to cybersecurity alerts and incidents in a timely manner
- Provide guidance for personnel responsible for reporting alerts and incidents to management
- Create a prioritization scheme and clear guidance to both internal and external personnel on incident response procedures
- Use sufficient internal controls to oversee third-party service provider review and escalation of cybersecurity alerts.[8]

Remedial Efforts

According to the SEC Order, RRD's cooperation with the agency and prompt remedial steps factored into the SEC's final decision to accept the offer. These steps included:

1. Reporting the 2021 ransomware event to the SEC prior to RRD's first EDGAR filing disclosing the event
2. Revising incident response policies and procedures voluntarily, with new cybersecurity technology and controls, updated employee training and increased cybersecurity personnel
3. Providing SEC staff with detailed explanations and summaries of specific factual issues throughout the investigation
4. Following up on SEC staff requests without requiring subpoenas, such as obtaining employee information, providing additional documents and explaining technical cybersecurity issues.[9]

Takeaways for Business

Cybersecurity remains a top priority for the SEC, and the agency is not shying away from using its full regulatory toolbox. The SEC has previously applied its power under Exchange Act Section 13(b)(2)(B) to alleged cybersecurity failures after a breach, notably enforcing such requirements against SolarWinds last October (see here for our article on that enforcement), which is still ongoing as of this writing. This latest enforcement is a signal for companies that the SEC's authority under Exchange Act Section 13 remains a significant consideration for their cyber policies and procedures as well as oversight of any third-party security service providers. Exchange Act Section 13(b)(2)(B) requires companies to maintain adequate "internal accounting controls," which will apply to cybersecurity-related controls after a cyberattack incident. Companies should not wait for an attack to test their practices and should proactively ensure those practices deliver critical information from their cybersecurity frontlines to decision-makers.

Please contact a member of Akin's cybersecurity, privacy and data protection team if you have any questions about this enforcement or how it may impact your company.

---

1 U.S. Securities & Exchange Commission, Press Release, *SEC Charges R.R. Donnelley & Sons Co. with Cybersecurity-Related Controls Violations* (June 18, 2024), available at https://www.sec.gov/news/press-release/2024-75.

2 *In the Matter of R.R. Donnelley & Sons Co.*, Release No. 100365 (June 18, 2024), available at https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf.

3 *Id.* at 2-3.

4 *Id.* at 3.

5 *Id.*

6 *Id.* at 4.

7 *Id.*

8 *Id.* at 4-5.

9 *Id.* at 5-6.

Categories

Cybersecurity, Privacy & Data Protection | Technology | Consumer Privacy | Consumer Data Protection | Privacy & Data Protection

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.