Cooley

SEC Settles Charges Against RR Donnelley Related to Cybersecurity Incident Disclosure and Internal Access Controls

July 17, 2024

On June 18, 2024, the Securities and Exchange Commission (SEC) announced that it had settled claims against RR Donnelley (RRD) related to a 2021 ransomware and cyber extortion attack. Despite RRD having discovered and reported the incident within 30 days (a relatively short time frame for investigating complex data breaches), the SEC alleged deficiencies in RRD's disclosure and access controls, as well as its internal controls. The incident happened before the SEC's 2023 cybersecurity incident reporting rule amending Form 8-K went into effect, meaning that no explicit cybersecurity incident reporting obligations or deadlines existed at the time.[1] The action against RRD reflects the SEC's continued expansive use of the internal accounting controls provision of Exchange Act Section 13(b)(2)(B) – now in the context of cybersecurity incidents – and has implications for security professionals and legal counsel concerning incident detection and escalation procedures, along with the steps necessary for the investigation and remediation of cybersecurity incidents (in this case, a ransomware attack). Below we summarize the RRD matter and provide our take and next steps and action items.

Background

The situation arose on November 29, 2021, after RRD's third-party managed security services provider (MSSP) escalated three security alerts to RRD's internal security team. The SEC contends that RRD reviewed the escalated alerts but, in partial reliance on its MSSP, did not take the infected instances off the network and otherwise failed to conduct its own investigation of the suspicious activity or take steps to prevent further compromise at that time. During the same time frame, the MSSP also reviewed, but did not escalate to RRD, at least 20 other alerts related to the same activity.

RRD began actively responding to the attack on December 23, 2021, after a company with shared access to RRD's network alerted RRD's Chief Information Security Officer (CISO) of potential anomalous internet activity emanating from RRD's network. RRD determined that the threat actor successfully installed encryption software on certain RRD computers and exfiltrated 70 gigabytes of data belonging to 29 of RRD's 22,000 clients, some of which contained personal identification and financial information. Beginning on December 27, 2021, RRD issued public statements regarding the incident, including in filings with the SEC.

RRD's share price dropped by one cent on the day of its 8-K filing and was down 10 cents two days later. By December 30, 2021, its share price had fully recovered and was up 50 cents a share.

The SEC's allegations and settlement with RRD

Based on the foregoing, the SEC alleged violations of two sections of the Exchange Act – Section 13a-15(a) (related to disclosure controls) and Section 13(b)(2)(B) (related to internal accounting controls to prevent unauthorized access to registrant assets),[2] as follows.

Failure to maintain adequate disclosure controls

The SEC focused on RRD's alleged failure to react to reported alerts from its intrusion system and the failure of the MSSP to report certain alerts to RRD. Specifically, the SEC alleged that:

- RRD's disclosure controls were not designed to ensure all relevant information relating to alerts and incidents was timely reported to RRD's disclosure decision-makers.
- RRD's disclosure controls did not provide guidance regarding the personnel responsible for reporting such information to management, including by failing to sufficiently identify lines of responsibility and authority or establish clear workflows for

alert review and incident response and reporting.

- RRD's incident response plan did not have a prioritization scheme to provide clear guidance to internal and external personnel for responding to incidents.
- RRD's staff members responsible for reviewing and responding to alerts did not have sufficient time to dedicate to the escalated alerts and general threat-hunting in RRD's environment.
- RRD failed to establish sufficient internal procedures to audit or oversee the MSSP's review and escalation of the alerts or otherwise manage the MSSP's allocation of resources to the task.

Failure to maintain internal controls to prevent unauthorized access to company 'assets'

The SEC also alleged that RRD failed to implement internal controls sufficient to provide reasonable assurances that access to RRD's assets was permitted only with management's general or specific authorization. On this point, the SEC focused on the lack of internal controls to enable RRD's external and internal security personnel to adequately investigate and remediate the incident in a timely manner, resulting in unauthorized access to an "asset" within the purview of internal controls – the overall IT environment. **This charge goes to the heart of incident investigation and remediation tactics, which are administrative controls deployed by nonmanagement security personnel.**

These allegations resulted in two claims by the SEC against RRD:

> [ ] As a result of the conduct described above, RRD also violated Exchange Act Rule 13a-15(a), which requires issuers of securities registered pursuant to Section 12 of the Exchange Act, such as RRD, to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms.
>
> [ ] As a result of the conduct described above, RRD violated Exchange Act Section 13(b)(2)(B), which requires issuers with a class of securities registered pursuant to Section 12 of the Exchange Act to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances, among other things, that access to company assets is permitted only in accordance with management's general or specific authorization.

Interestingly, two SEC commissioners (one appointed by President Joe Biden and one by former President Donald Trump) formally dissented to at least part of the SEC order. Echoing previous criticisms of the SEC's use of the internal accounting controls provisions, the commissioners stated that:

> The Commission's order faulting RRD's internal accounting controls breaks new ground with its expansive interpretation of what constitutes an asset under Section 13(b)(2)(B)(iii). By treating RRD's computer systems as an asset subject to the internal accounting controls provision, the Commission's Order ignores the distinction between internal accounting controls and broader administrative controls. This distinction, however, is essential to understanding and upholding the proper limits of Section 13(b)(2)(B)'s requirements.

These dissenting commissioners, however, did not criticize the SEC's allegation that RRD violated Exchange Act Rule 13a-15(a) based on inadequate disclosure controls.

Our take

The SEC continues to signal its regulatory priorities related to cybersecurity and, in particular, incident response and related disclosure requirements. The SEC clearly seeks to expand both its regulatory reach and the scope of registrants' incident response, investigation, remediation and disclosure measures. Our key takeaways are as follows:

The SEC keeps moving goalposts regarding disclosure controls and escalation to management.

One of the key questions facing security teams and legal departments in the wake of the recent SEC cyber rule is ***when*** reporting to management is necessary. The SEC (in)famously first moved the goalposts in its action against First American, where it took umbrage with the registrant's failure to escalate a yet-to-be-exploited **security vulnerability** (not an incident in the general meaning of the word) to management for reporting consideration.

In this case, the SEC took issue with RRD's failure to escalate various security alerts (not incidents) to management (including RRD's CISO). If missing a security alert is evidence of poor disclosure controls, then far more companies may have issues when they miss the needle in the haystack. Also, this runs counter to the current SEC cybersecurity disclosure rule, which focuses on 8-Ks for material incidents and escalating incidents to management for assessment. The SEC's review also is done with 20/20 hindsight, allowing the SEC to selectively target incidents and companies.

Is the SEC imposing (through enforcement) specific security investigation and remediation measures?
The SEC alleged that RRD failed to implement measures to ensure an adequate investigation and remediation of the RRD incident. As highlighted by the dissenting commissioners, this should be the concern of information security professionals and not securities regulators. This also runs counter to statements made by the director of the SEC's Division of Corporation Finance in December 2023 that the SEC was not **"seeking to prescribe particular cybersecurity defenses, practices, technologies, risk management, governance or strategy"** through the new SEC cyber rule.

How far does the SEC's concept of a 'disclosure control' extend?
In this case, RRD did have detection capabilities, but it allegedly did not respond to them appropriately. However, in hindsight, if a registrant does not have detection capabilities or does not have the right ones to detect a breach that has occurred, is that also a failure of disclosure or internal controls? And to enable detection and response capabilities, security teams segment their networks, erect firewalls, implement access controls, employ data classification and maintain other measures that are the foundation to detection capabilities. If these measures are on the spectrum of "disclosure controls" and "internal controls," the SEC is now starting to regulate information security in a much broader fashion than its impact on disclosure controls.

How far does the SEC's concept of an 'asset' extend?
As the dissenting commissioners noted, internal controls rules and regulations focus on assets that are the subject of corporate transactions, which would not traditionally cover information technology systems. The expanded use of internal controls didn't start with RRD either. In the *Charter Communications* order (stock buybacks not authorized by the board of directors) and *Andeavor* order (Rule 10b5-1 trading plans improperly authorized), the SEC found inadequate internal controls, among other things, with these companies through expansion of the term "asset" to include an increasing amount of corporate activity. The dissenting commissioners summarized the issue succinctly:

> [ ] the Commission in recent years has taken to treating Exchange Act 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. Identifying a link between the Commission's preferred policies and procedures and accounting controls seems a collateral concern, if it is a concern at all.

The SEC's broad interpretation of "assets" suggests that the SEC could scrutinize the finite details of a company's information security programs with the benefit of 20/20 hindsight after incidents have occurred.

Next steps and action items

1. Revisit and update your cybersecurity incident response measures.
While the SEC focused on RRD's alleged failures to respond to incident alerts, the *RRD* order focused on RRD's alleged lack of disclosure and internal controls with respect to cybersecurity incident review and escalation. As mentioned above, the SEC's focus on internal controls has become an increasingly common theme in recent SEC investigations, including in other areas (such as non-generally accepted accounting principles financial measures in the *DXC SEC* order and stock buyback programs in the Andeavor SEC order). Based on the RRD case, the SEC's 8-K cyber rule and the *First American* order, registrants should analyze their full incident response "stack" to determine if controls are in place to detect and escalate not only material cybersecurity incidents but also "security events," such as vulnerabilities and alerts that could indicate such an incident. As demonstrated in RRD and in *Solarwinds*, a registrant should consider how its detection capabilities enable it to "connect the dots" based on alerts and the cumulative effects of multiple security vulnerabilities (both of which were themes in the SEC's enforcement actions).

In particular, ascertain whether the plan sufficiently identifies lines of responsibility and authority, with actionable workflows rather than high-level concepts. Are the key definitions in the plan clear, properly scoped and understood? Does your incident response stack provide clear criteria – including a materiality assessment framework – for prioritizing incidents and escalating them internally to senior security professionals, management, and the registrant's disclosure or materiality assessment team? Given the SEC's expanded use of

internal controls, the SEC could investigate companies solely for potential deficiencies at the cybersecurity "front line," without looking at whether incidents were escalated to senior leadership and the board of directors (which is more within the purview of disclosure controls). For example, the SEC focused on RRD's lack of clear guidance to the personnel responsible for initially reviewing and responding to incidents.

Speaking of disclosure controls, consider whether the appropriate team members are involved in the "chain" of escalation. For example, if only a subset of the disclosure committee is involved with materiality assessments, consider whether additional team members from other functional areas may be relevant, including based on actual alerts to date. From experience, we are seeing many incident response plans drafted by security professionals over multiple years that are unclear and ambiguous as to many of these points.

2. Conduct 'executive tabletops' and break down silos.

While the trend has been to view incident response as a holistic and multidisciplinary team effort, silos still exist, and sometimes security events or incidents can get "stuck" in the IT or security departments. As such, testing the incident response stack through executive tabletops has become crucial. Not only does it allow a wider team to understand and improve a company's response and escalation capabilities, but it also enables a disparate group of stakeholders who don't always work together to understand respective concerns and views concerning incidents, and to collaborate to solve a problem that increasingly causes a companywide impact. Ultimately, while security incidents often implicate highly technical issues, response comes down to people, communication, and multidisciplinary cooperation during a crisis. Participants for these exercises should include not only the security team, but also legal (who is at the center of managing these events), financial management (who has a wider view of business impacts), communications (to help mitigate reputational harm), risk and insurance personnel (to access cyber insurance) and senior management (as necessary when materiality assessment is in play).

3. Consider information security resource capacity restraints.

The SEC also took issue with RRD's capacity for responding to alerts. This is, and likely always will be, a huge challenge for organizations. The irony around incident detection is that the more sophisticated and successful detection measures are, the more effort it takes to sift through the noise and connect the dots. In this case, registrants should consider whether their internal and external security teams (including MSSPs) have sufficient time to dedicate to reviewing and potentially escalating alerts, based on actual performance and response times to previous alerts. The SEC's ultimate finding with RRD's internal controls was that RRD did not give its response personnel clear guidance and sufficient resources. Significantly, some believe that AI will soon be available to make these tasks easier for overstretched security professionals.

4. Revisit and monitor relationships with MSSPs.

The SEC order specifically criticized RRD's internal procedures to audit or oversee the MSSP's review and escalation of alerts or otherwise manage MSSP's allocation of resources to the task. This implies a need for registrants to carefully vet their MSSP's capabilities before engaging. Once engaged, registrants should take steps to understand how the MSSP's alerts work, calibrate alerting, explore how seemingly independent alerts may be connected and develop clear escalation paths. The SEC references "audits" of MSSPs, which would likely include fine-tuning alerts, testing escalation procedures and integrating "lessons learned" during actual security events. Again, the hope is that the existence of reasonable procedures for monitoring MSSPs will provide some level of protection against SEC enforcement even if something is missed or those procedures do not work perfectly.

Notes

1. The SEC released guidance on the topic in 2011 and 2018.
2. Each of which also was referenced in the SEC's amended complaint against Solarwinds.

Key Contacts

Jon Avina Palo Alto	javina@cooley.com +1 650 843 5307
Milson Yu Palo Alto	myu@cooley.com +1 650 843 5296
Brad Goldberg New York	bgoldberg@cooley.com +1 212 479 6780