Mitigating Cybersecurity Risks in Mergers and Acquisitions

The Importance of Due Diligence and Regulatory Compliance

By Karen Painter Randall, Joshua P. Previl, and Adam J. Salzer

With cybersecurity threats to both public and private companies becoming a daily occurrence, it has never been more important for venture capital, mergers and acquisitions (M&A) and private equity firms to conduct substantive due diligence on the organizational cybersecurity infrastructure of their target investments. Organizations of every size, across all industries, are constantly facing threats to their proprietary business data and the personal information of their investors, clients and employees through phishing emails, ransomware, spyware, and a myriad of other nefarious tactics. Despite employee cybersecurity training and the use of third-party specialists to manage company security and data systems, billions of dollars are lost each year due to data security breaches causing some enterprises to go out of business. This ever-evolving threat compels potential suitors to conduct extensive due diligence relevant to a target's security infrastructure, posture and culture during M&A to avoid having the acquiring firm inherit the security issues of its acquisition.

...[The] Securities and Exchange Commission (SEC) recently adopted new rules to enhance and standardize public companies' disclosures regarding cybersecurity, risk management, strategy, governance and incidents. Additionally, the Federal Trade Commission (FTC) recently approved amendments to the Standards for Safeguarding Customer Information Rule requiring non-banking financial institutions regulated by the FTC to report certain data breaches.

Government regulators have begun to take notice of the relentless threat landscape. Most notably, the Securities and Exchange Commission (SEC) recently adopted new rules to enhance and standardize public companies' disclosures regarding cybersecurity, risk management, strategy, governance and incidents. Additionally, the Federal Trade Commission (FTC) recently approved amendments to the Standards for Safeguarding Customer Information Rule requiring non-banking financial institutions regulated by the FTC to report certain data breaches. As recently as Dec. 18, 2023 (the effective date of the new SEC reporting requirements), VF Brands, a publicly traded company, filed an SEC report indicating that "attackers" stole personal data from the company, and that the incident would likely continue "to have a material impact on the Company's business operations..."[1]

In light of this high-risk environment and the new regulatory reporting standards, company executives are under increasing pressure to: (1) ensure that business, client and investor data is adequately protected, and (2) accurately and promptly disclose known cybersecurity risks and vulnerabilities. Failure to do so is a recipe for a crippling data breach, costly litigation and regulatory enforcement claims, and in the case of mergers and acquisitions, post-closing indemnity claims. The Oct. 30, 2023, complaint filed by the SEC in the Southern District of New York against SolarWinds, Inc., a publicly-traded software company, and its chief information security officer (CISO), Timothy Brown provides a cautionary tale.

The SEC's complaint charged SolarWinds with violations of the antifraud provisions of the Securities Act of 1933 and of the Securities Exchange Act of 1934 related to "misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened—and increasing—cybersecurity risks."[2] The SEC alleged that despite the company's known cybersecurity vulnerabilities, SolarWinds and Brown made false public statements and failed to disclose known risks related to the quality of its cybersecurity practices. Those vulnerabilities only came to light following the 2019 and 2020 SUNBURST cyberattack that exploited the vulnerabilities of SolarWinds' Orion product. By inserting a malicious code into the Orion product, the threat actor ultimately gained access to SolarWinds' customers data.

In December 2020, SolarWinds disclosed to the SEC that it was affected by the SUNBURST attack. Following its disclosure, SolarWinds' share price dropped 35% in approximately two weeks. At the same time, it came to light that numerous employees,

KAREN PAINTER RANDALL *chairs the Cybersecurity, Data Privacy, and Incident Response Group at Connell Foley LLP, where she counsels clients on cybersecurity, data rights, and privacy laws and regulations to safeguard their enterprise data. She guides businesses through the rapidly evolving cybersecurity and privacy space, mitigating risks and ensuring compliance with state and federal regulations.*

JOSHUA PREVIL *is an associate in Connell Foley's Corporate and Business Law Group. He assists public and private companies in a variety of engagements, including mergers and acquisitions, governance, and regulatory compliance.*

ADAM SALZER *is an associate in the Commercial Litigation, White-Collar Criminal Defense and Investigations, and Cybersecurity, Data Privacy, and Incident Response Groups at Connell Foley LLP. As a former assistant prosecutor, Adam has a unique perspective on digital security threats and criminal investigations while working with law enforcement agencies.*

including Brown, knew that the company had "serious cybersecurity deficiencies," as described in numerous internal statements. Those statements "dramatically contradict SolarWinds' public disclosures..."[3]

SolarWinds' failures to adequately address its cybersecurity policies, along with its materially false statements to the public and regulators regarding its cybersecurity practices, led to millions of dollars in investor losses and exposed SolarWinds to liability resulting from violations of a litany of regulatory issues and litigation. SolarWinds' counsel will move for dismissal of the SEC complaint.[4] They argue that the SEC's actions overstepped the agency's legislative authority since "the SEC is not a cybersecurity regulator."[5]

In an effort to promote accurate and complete cybersecurity disclosures and assist investors in making informed decisions, the SEC has adopted new rules that standardize the disclosure practices surrounding cybersecurity and hold boards of directors more accountable for the oversight of a registrant's cybersecurity protections. Effective December 2023, registrants are required to report on Item 1.05 of their Form 8-K the following information regarding a material cybersecurity incident:

1. When the incident was discovered and whether it is ongoing;
2. A brief description of the nature and scope of the incident;
3. Whether any data were stolen, altered, accessed, or used for any other unauthorized purpose;
4. The effect of the incident on the registrant's operations; and
5. Whether the registrant has remediated or is currently remediating the incident.[6]

With a limited exception for threats to national security or public safety, the Form 8-K detailing a cybersecurity incident must be filed within four (4) business days of the registrant's determination that the incident is considered material to the company. This determination does not necessarily coincide with the date of the incident.[7] The new rules maintain the current definition of "material" in securities law: An incident is material if "there is a substantial likelihood that a reasonable shareholder would consider it important."[8] Furthermore, the rules require foreign private investors to report similar incidents on a Form 6-K whenever they report such incidents in a foreign jurisdiction.

Already under a spotlight, the new SEC disclosure and governance rules will make a CISO's life even more complicated. Not only will the CISO be responsible for detecting and responding to a cybersecurity incident, but he will play an important role working with key stakeholders to determine whether the incident rises to the level of being material to the company's financial performance requiring regulatory notification. Legal and regulatory bodies have been proactive in this space including convicting the Uber Chief Security Officer in a federal court action, conducting a SEC civil investigation of the Solar Winds CFO and ordering Drizly's CEO to implement a data security program.

According to the new rules, registrants are also required to disclose on Item 106 of Form 10-K their current systems and policies for managing cybersecurity threats, including whether a third-party is engaged to manage such threats, procedures for identifying and addressing threats that are in place, and contingencies for recovering data after a breach. Registrants are also required to report on the company's cybersecurity practices to the board of directors' management and oversight committee.

The SEC's new disclosure rules will give investors the ability to gain more insight into a potential target's cyber risk and resiliency plan. In the context of M&A, this can provide investors with information that they may not have otherwise received or requested during the due diligence process. Although cybersecurity continues to be a minefield, investors request varying levels of detail from targets in this area. Some request high-level information on a target's information systems, while others have a team of specialists dedicated to gathering details about the target's cybersecurity posture. The new rules can also make investors aware of areas that might warrant follow-up or a deeper dive especially if the investor requests broader disclosures during the due diligence process than the target is required to report in its SEC filings. In today's data privacy landscape, it is crucial for investors to conduct a cybersecurity risk assessment to gain as much information about a target's security infrastructure as reasonably possible before deciding to consummate an acquisition. Without the proper vetting, gaps in data security can go undetected until post-acquisition. Without proper due diligence, an acquirer may find that it purchased the target without detecting an ongoing attack impacting its system. For example, just two years after it acquired Starwood Hotels & Resorts Worldwide, Inc. in 2016, Marriott Hotels & Resorts suffered a data breach caused by a Trojan malware placed on Starwood's servers.[9] Starwood's systems were not sufficiently secure, and it had suffered multiple data breaches even before it was acquired, including a successful attack in 2015.[10]

From the target's standpoint, the new rules reinforce the importance of conducting regular risk assessments and making sure that best practices are used across the enterprise using applicable frameworks as guidance. Ensuring that an incident response plan with different playbooks and tabletop exercises are practiced is crucial under the new rule. Cyber policies and procedures will need to be tested and updated as well to ensure

compliance with new laws and regulations. Security awareness training, third-party vendor management, patch management, multifactor authentication, endpoint detection and response (EDR) are just a few measures to be focused on in order to fortify an enterprise's cybersecurity. Companies should also keep abreast of changes in applicable privacy laws and update their privacy policies and practices accordingly. The new rules also put a spotlight on directors, emphasizing the importance of sufficient oversight of the inner workings of the company's data security.

Although the new rules seek to help investors to be more informed about their potential targets, attackers have found ways to use the new rules to their own benefit. On Nov. 7, 2023, ALPHV/Black Cat, a notorious ransomware-as-a-service operator, launched a successful ransomware attack on MeridianLink, Inc., a publicly-traded software company that provides digital solutions to financial institutions.[11] When MeridianLink refused to pay the ransom, Black Cat applied more pressure by filing a complaint with the SEC alleging that its victim failed to disclose the ransomware attack as required by the new rules. Although the new rules were not in effect at the time the complaint was filed, this tactic used by Black Cat serves as a warning for current registrants. In addition to enforcement actions by the SEC for failure to disclose material cybersecurity threats and processes, registrants may now face additional threats and pressure from groups like Black Cat. SolarWinds' counsel has also expressed its frustrations with the new rules, particularly the addition of Item 106 to Form 10-K. They argued that "it's unreasonable for the SEC to expect publicly available investor disclosures to spell out the specific vulnerabilities in a company's cybersecurity infrastructure, and in so doing, "giving a roadmap to fraudsters."[12]

The threat of a cyberattack may be increased during M&A transactions, especially as it pertains to publicly-traded companies. Due to the visibility associated with such a transaction, it is a prime opportunity for cybercriminals to launch ransomware attacks, phishing scams, and other data breaches. Cybercriminals can also play the long game by breaching the target company and waiting for it to be acquired by a larger entity, thereby circumventing the cyber protections established at the larger entity.[13] The creative tactics employed by cybercriminals require companies to conduct extensive diligence of their potential target. The SEC Commission Chair, Gary Gensler, has warned companies against "AI washing," the practice of overstating or misrepresenting the amount of AI or the level of sophistication of AI used in a company's operations.[14] Although companies may AI wash in an effort to assure investors that the company has the latest technology and cybersecurity protections, the deficiencies would be exposed if the company suffers a cybersecurity attack or data breach. With the increasing prevalence of cyber threats in a world dependent on information technology, companies' cyber protections will almost definitely be tested.

The new SEC rules aim to increase transparency between companies and their current and potential shareholders. The rules, along with the constant threat of cyberattacks, urge registrants to improve their cybersecurity processes and policies consistently. Making the required disclosures not only ensures compliance with the SEC, it also facilitates more seamless due diligence in M&A transactions.

Whether a company is selling or looking to acquire and expand, it is imperative that legal and security vendors work collaboratively with the client and counter-parties to ensure that sufficient, responsive information is disclosed during the due diligence process. Companies put themselves at risk when material information is concealed or omitted. Cybersecurity due diligence will continue to be a mainstay in M&A transactions. Investors and targets require proper counsel to guide them through this heavily regulated area to limit respective risks and liability. ■

Endnotes

1. sec.gov/Archives/edgar/data/103379/000095012323011228/d659095d8k.htm
2. sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
3. *Id.*
4. Scharf, Rachel, SolarWinds Tells Judge SEC Overstepped with Cyber Suit, Law360, December 14, 2023.
5. *Id.*
6. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038 (Mar. 9, 2022) at 12-13.
7. Registrants must determine the materiality of an incident without unreasonable delay following discovery.
8. *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976)
9. Fruhlinger, Josh, *Marriott data breach FAQ: How did it happen and what was the impact?*, CSO Online, June 20, 2019.
10. *Id.*
11. https://www.wiley.law/alert-Ransomware-Attacker-Files-SEC-Complaint-to-Increase-Pressure-on-Victim
12. *Supra* Note 4.
13. Mody, Sid et al., *Evaluating and Containing Cyber and Data Privacy Risks in Corporate Transactions*, 22 THE M&A JOURNAL 9.
14. Konnath, Hailey, SEC Chair Warns Businesses Against AI Washing: 'Don't Do It', Law360, December 5, 2023.