GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

September 2021

With New Cybersecurity Enforcement, the SEC Puts Its Money Where Its Mouth Is

The past 12 months have seen an increase in cybersecurity attacks against major companies, placing data breaches on the front page of virtually every major newspaper. The U.S. government has taken notice. In May, the Biden administration issued an executive order requiring government agencies and certain government contractors to comply with cybersecurity requirements. In July, the U.S. Cybersecurity and Information Security Agency launched the Stop Ransomware website, to provide resources for companies addressing the recent increase in ransomware attacks. The Securities and Exchange Commission (SEC) similarly has ramped up its focus on cyber threats, identifying "Information Security and Operational Resiliency" as one of its 2021 Examination Priorities.

At the same time, the attack on SolarWinds' Orion network monitoring software discovered in December 2020 made the 18,000 organizations utilizing their affected security software products all too aware of the risks. Russian state-sponsored cyber attackers allegedly used a routine software update in March 2020 to slip malicious code into the software, enabling backdoor access to SolarWinds' customers who downloaded the affected products and had systems connected to the internet. While reports indicate that only a small fraction of the 18,000 companies and government agencies were successfully compromised, the message was clear: cyber attackers are often one step ahead of even the most sophisticated companies and governments.

Although the goal of the SolarWinds breach is believed to have been primarily intelligence gathering, ransomware attacks also have become big business. One security company study indicated that projected losses from cybercrime in 2020 reached a level equivalent to 1% of the world's GDP. Costs can include not only the ransom payment itself, if one is made, but also costs related to the inability to do business and reputational harm.

On June 11, 2021, the SEC's Office of Information and Regulatory Affairs released the Spring 2021 Unified Agenda of Regulatory and Deregulatory Actions. Included in the SEC's rulemaking list are rules regarding disclosure relating to cybersecurity risk. The SEC has indicated that the Division of Corporate Finance is considering recommending that the Commission propose rule amendments to enhance issuer disclosures regarding cybersecurity risk governance. The Notice of Proposed Rulemaking is expected in October 2021.

Given this context, it is not surprising to see the SEC ramp up its investigatory and enforcement activity over cybersecurity. The risks to publicly traded companies and companies otherwise regulated by the SEC (e.g., investment advisors, broker-dealers, etc.) include exposure of confidential information that could be used for insider trading purposes, disruption of supply chain leading to a domino effect if a vendor is attacked, inability to operate, and exposure of sensitive personal (customer) information, among other things.

The current reporting standard for publicly traded companies is whether the incident has a "material effect" on the company's finances, operations, or liquidity; or presents risks of litigation, regulatory investigations, harm to reputation, increased insurance costs, or potential harm to its products, services and customer and vendor relations. This standard obviously carries with it some significant gaps, particularly for extremely large companies for whom only a substantial "bet the company" hack would likely materially affect their finances. Indeed, recent enforcement actions have indicated that the SEC is increasing its focus on less tangible losses, like harm to reputation or harm to customer relationships.

The standard for breach reporting for companies that are not publicly traded but are nonetheless subject to the SEC's jurisdiction is less clear. While Regulation S-P to the Gramm Leach Bliley Act contains requirements around safeguarding customer information, the SEC notably did not sign onto the 2005 Intra-agency Guidance, which sets forth breach notification requirements for financial institutions regulated by various government agencies, including the FDIC and OCC. Accordingly, while these entities would still be subject to state data breach notification requirements, state laws only require reporting if certain types of sensitive personal information are accessed or acquired in a data breach.

Perhaps these gaps, combined with the near-miss nearly 18,000 organizations experienced as part of the SolarWinds Orion attack, are driving the SEC to take proactive steps. Specifically, beginning in June 2021, scores of companies began receiving correspondence from the SEC referencing "Certain Cybersecurity-Related Events," specifically, the SolarWinds Compromise. The requests ask for voluntary compliance with a series of questions about the attack, promising respondents something akin to amnesty from enforcement in return, subject to certain conditions. Four of the five questions on the voluntary response questionnaire directly relate to the SolarWinds Compromise.

The SEC goes a step further in question five, however, requesting that companies disclose "Other Compromises," defined as "any unauthorized access, other than the SolarWinds Compromise, to any computer (including any computer system, computer network, or data storage facility) owned or operated by You or on Your behalf occurring between October 1, 2019, and the present and lasting longer than one day [24 hour-period], including hacks, data breaches, or ransomware attacks." The SEC was clear in its FAQs, however, that the enforcement amnesty benefits do not extend to reports of "Other Compromises," which instead "would be considered self-reported conduct outside of the scope of the SolarWinds

[Compromise] and reviewed on a case-by-case basis," causing some degree of heartburn for respondents. The SEC also clarified that responses should not be limited "based on materiality or access to material non-public information." Those companies that were not impacted by SolarWinds, however, did not need to respond to question five.

What the SEC will do with respondents who answer affirmatively to question five remains to be seen, but it is quite possible that the Staff, having requested companies to disclose the existence of Other Compromises, will investigate them and initiate enforcement actions when they deem them appropriate. It is clear, however, that enforcement activity is already on the rise in 2021. In June 2021, the SEC charged First American Financial Corporation, a real estate settlement service provider, with failing to maintain disclosure controls and procedures designed to ensure that all available relevant information concerning cybersecurity vulnerabilities was properly analyzed for disclosure in company reports filed with the SEC. Specifically, the SEC alleged that the company was notified in late May 2019 that its document image sharing application had a vulnerability exposing 800 million title and escrow document images, including images with personally identifiable information such as social security numbers. However, senior executives had not been apprised that information security personnel had identified a vulnerability in a January 2019 penetration test of the application. Moreover, senior executives were not made aware that the company failed to remediate that identified vulnerability in accordance with its vulnerability remediation management policies. As a result, the SEC alleged that the company violated Exchange Act of 1934 Rule 13a-15(a) [17 C.F.R. § 240.13a-15]. Without admitting or denying the allegations, the company consented to the imposition of a cease and desist order and the payment of a $487,616 penalty.

Just two months later, the SEC announced another cybersecurity enforcement action targeting accurate and complete cyber disclosures. On Aug. 16, 2021, the SEC announced a settled enforcement action against Pearson plc, a London-based company that provides educational publishing and other services to schools and universities. According to the SEC, Pearson experienced a data breach in 2018 involving the theft of student data and administrator log-in credentials of 13,000 school, district, and university customer accounts. But in its semi-annual report filed in July 2019, it referred to a data privacy incident as a hypothetical risk despite knowing that the intrusion had already occurred. Further, in a July 2019 media statement, the company stated that the breach "may" include dates of births and email addresses when, again, it was aware the records were stolen. Finally, the SEC alleged that the company's disclosure controls and procedures were not designed to ensure that personnel responsible for making disclosure determinations were informed about relevant information regarding the breach. The SEC found that the company violated Securities Act of 1933 Sections 17(a)(2) and 17(a)(3) and Exchange Act of 1934 Section 13(a) and Rules 12b-20, 13a-15(a) and 13a-16 thereunder. Without admitting or denying the allegations, Pearson consented to the imposition of a cease and desist order and the payment of a $1 million penalty.

Most recently, on Aug. 30. 2021, the SEC announced three settled enforcement actions against registered broker-dealers and investment advisors concerning alleged deficient cybersecurity policies and procedures in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguard Rule"). The Safeguard Rule requires registered broker-dealers and investment advisors to adopt written policies and procedures reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial hardship or inconvenience to any customer. As alleged in the SEC's Orders Instituting Administrative and Cease-and Desist Proceedings, the email accounts of firm personnel and independent contractor representatives were taken over by unauthorized third parties, resulting in the exposure of thousands of customers' personally identifiable information

(PII) stored in compromised email accounts, known as a business email compromise. During the relevant periods, the firms allegedly either did not have or did not enable multi-factor authentication. The email account takeovers did not appear to have resulted in any unauthorized trades or transfers in customer accounts, but some emails containing customer PII were forwarded to unauthorized email addresses, and customers received phishing emails. The SEC deemed these deficiencies to violate the Safeguards Rule because the firms' policies and procedures were not reasonably designed to protect customer information and to prevent and respond to cybersecurity incidents. Of note, the SEC's press release announcing the settled administrative proceedings made reference to examination staff in addition to enforcement staff, making it clear that the examiners are actively involved in the SEC's cyber-initiatives. The firms settled, without admitting or denying the SEC's allegations, and consented to the imposition of cease and desist orders, censures and civil monetary penalties totaling $750,000.

Takeaways

Companies may consider taking the following steps given recent SEC enforcement actions:

- **Show Your Work**. Think ahead to what documents and information the SEC would request in connection with an investigation into cybersecurity practices and disclosures, including policies and procedures related to cybersecurity protection efforts, risks, and incidents. For example, companies should be able to show the following:
  - **Written Information Security Plan (WISP)**. Multiple laws, including those promulgated by the New York Department of Financial Services and several states, require that companies maintain WISPs. At minimum, a WISP should align with one of the recognized data security standards, like those issued by the National Institute of Standards and Technology (NIST) or International Organization for Standardization (ISO).
  - **Incident Response Plan (IRP)**. While most companies tend to think of IRPs as technical documents maintained by the IT or IS department, it is equally important to have an executive-level IRP outlining how a company would address the business, financial, and reputational risks posed by a cyberattack. The IRP should also identify members of an executive-level incident response team who would be called upon to make key decisions, including decisions concerning reporting and disclosure during a cyberattack.
  - **Test Your Procedures Through War Gaming**. Policies that gather dust on a shelf do little good. Further, testing your procedures for the first time during a live data breach can lead to costly errors. Increasingly, the expectation from regulators is that companies will conduct annual data breach training "war games." Also known as tabletops, a good war game will simulate a real-life attack, putting senior executives in the position of having to make tough decisions, including around disclosure and regulatory notification, in a safe environment.
  - **Board Oversight**. A company's board of directors must address cybersecurity risks as part of its oversight. Given the recent media attention paid to data breaches and ransomware attacks on major corporations, at minimum, a board should consider having a designated committee that provides appropriate oversight over management's handling of data security risks and incidents.
- **Disclose Possible Cyber Risks**. Every company faces cybersecurity risks, regardless of size or industry, and there truly is no excuse to ignore this risk in your public disclosures. But disclosing cybersecurity risks in periodic reports, including in a 10-K, is tricky. The SEC has advised that risk disclosures should be specific enough to identify risks investors might deem "material," while acknowledging that companies should not publicly disclose "specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such

detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident." In reality, there may be a fine line between the two. If the company previously experienced a significant cyber event that it did not publicly disclose, it should likely not frame such an event in future filings as a hypothetical risk. Ensure any financial reporting accurately discloses the costs associated with a cyberattack, including expenses and legal fees related to the investigation, loss of revenue, legal claims, or diminished cash flow.

- **Do Not Narrowly Evaluate the "Materiality" of a Breach**. The SEC has made it clear that an event that does not have substantial financial impact on a company (e.g., because the losses were covered by a cyber insurance policy) may nonetheless require disclosure, even in an 8-K report, which is required when publicly traded companies need to disclose a material risk promptly. The SEC has urged companies to consider the "range of harms that [cyber] incidents could cause" in evaluating disclosure obligations, including the importance of any compromised information and impact of the incident on the company's operations, impact on reputation, potential for regulatory investigations or lawsuits, and adverse impact on customer and vendor relationships, etc. In other words, consider more than financial impact when evaluating materiality.

Authors

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | valdeteroj@gtlaw.com
- Steven M. Malina | +1 312.476.5133 | malinas@gtlaw.com