As Ransomware Attacks Increase, The SEC Takes Notice

September 10, 2020

2020 has seen a huge increase in ransomware attacks. According to CRN.com, victims of the 11 biggest ransomware attacks (as of June 30, 2020) spent at least $144.2 million on costs related to the attacks[1]. Moreover, the transition to a remote workforce as a result of the COVID-19 pandemic has increased the attack area while simultaneously limiting the effectiveness of cyber defenses. The Securities and Exchange Commission ("SEC") has taken notice of this increase in attacks and offered observations about what companies should be doing to address this risk.

What The SEC Expects From Companies

On July 10, 2020, the SEC Office of Compliance Inspections and Examinations (OCIE) issued a warning to advisors and broker-dealers to "immediately" review their cybersecurity controls to prevent and respond to an increase in phishing campaigns and ransomware attacks.[2] OCIE encouraged companies to monitor the cybersecurity alerts published by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), including the most recent alert published on June 30, 2020 relating to ransomware attacks. The warning also stated that OCIE encouraged registrants to share this information with their third-party service providers, particularly with those that maintain client assets and records for registrants.

The guidance broadly suggests the companies revisit their incident response procedures, including ensuring timely notification and a process for involving law enforcement. It emphasizes operational resiliency, including focusing on the capability to continue to operate critical applications in the event that a company's primary system is unavailable. The SEC also suggests that companies focus on employee awareness and training, while also ensuring that systems are set up so that only necessary employees have access to certain subsets of data.

Interestingly, the SEC provides only its "observations" of how companies are preparing for and reacting to ransomware attacks, stating

> Recognizing that there is no such thing as a "one-size fits all" approach, and that not all of these practices may be appropriate for every organization, we are also providing the following observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency to address ransomware attacks.

Therefore, while there is no requirement that companies implement each of these policies or procedures, companies should compare their current procedures with those outlined in the guidance and determine whether any of them are appropriate for their business. For example, a company that has access to or uses

1 https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-
2 https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf

a wide variety of consumer data may be more inclined to implement a greater number of these policies or procedures than a company with less data.

Disclosure Of Ransomware Attacks

An assessment of whether and how to disclose a ransomware attack or other cyber incident should begin with the SEC's most recent formal guidance for cybersecurity disclosures, which the SEC issued in February 2018[3]. Given that the July 2020 warning from the OCIE is simply a set of observations of what companies should be doing, a look at how companies have recently reported ransomware attacks is also instructive.

Companies differ greatly in their descriptions of ransomware attacks in their public filings. The SEC guidance requires a company that experiences a cyber incident to first determine whether the cyber incident was material enough to disclose. If the company does disclose, it must ensure that the language is not boilerplate and is tailored toward the issues specific to the company. In addition, the company must consider if the cyber incident requires the company to update or amend previous disclosures. Finally, the company must consider the timing of disclosures and whether that timing has any possible insider trading consequences.

Some companies are disclosing attempted ransomware attacks. SEC Guidance suggests that even if there is a failed attempted attack that does not result in monetary loss but does result in other consequences, such as a material increase in cybersecurity expenses or loss of data, disclosure is appropriate.

For example, 10x Genomics, Inc.'s 10-Q dated August 12, 2020 stated:

> In March 2020, we experienced an attempted ransomware attack in which cybercriminals were able to access our information technology systems. While we isolated the source of the attack and restored normal operations with no material day-to-day impact to us or our ability to access our data, we have reason to believe confidential information was stolen. We believe the attempted ransomware attack could lead to the disclosure of our trade secrets or other intellectual property, or could lead to the exposure of personal information of our employees. The release of any of this information could have a material adverse effect on our business, reputation, financial condition and results of operations.

Oftentimes, the company's disclosure of a cyber incident is the first time the incident is made public. In its August 17, 2020 8-K, Carnival Corporation revealed that it was the victim of a ransomware attack on August 15, 2020. It "detected a ransomware attack that accessed and encrypted a portion of one brand's information technology systems. The unauthorized access also included the download of certain of our data files." Carnival then went on to describe the immediate action it took, including launching an investigation, notifying law enforcement, engaging legal counsel, implementing containment and remediation efforts, and working with cybersecurity firms to defend its systems and respond to the threat. Many news sites and data privacy blogs are covering the incident and all cite to the SEC filing specifically.

For incidents that are made public ahead of any SEC filing, it is interesting how the language surrounding the attack differs. For example, Keurig Dr. Pepper, Inc. experienced a cyber incident in February 2019. On February 4, 2019, a news report said, "Keurig Dr Pepper is working to get all its systems back online after it was targeted by hackers. While the company isn't releasing many details, it says that it was impacted by a targeted malware incident, which interrupted some areas of its coffee business operations over the past few days. They say no

3 https://www.sec.gov/rules/interp/2018/33-10459.pdf

data was compromised. A spokesperson for the company says they have not yet resumed normal business operations, and appreciates the patience of partners and customers." Three weeks later, the company's 10-K said, "In February 2019, our business operation networks in the Coffee Systems segment were disrupted by an organized malware attack. We have taken actions to address this attack and to implement further safeguards against similar attacks. We continue to evaluate the impact on our business and are working to finalize the resolution of these actions." Interestingly, the news article provided more information than the SEC filing did, including that the company did not think any data was compromised.

Finally, some ransomware attacks are publicly known but are not disclosed in SEC filings. GoDaddy notified some of its customers that an unauthorized party used their web hosting account credentials to connect to their hosting account. While the incident took place on October 19, 2019, it was discovered on April 23, 2020, after the company's security team discovered an altered file in GoDaddy's hosting environment and suspicious activity on a subset of GoDaddy's servers. However, GoDaddy's August 6, 2020 10-Q does not discuss this event. It only states "In addition, there has been an increase in the number of malicious software attacks in the technology industry generally, including newer strains of malware, ransomware and cryptocurrency mining software."

Key Takeaways

The increase in remote work during the pandemic has made companies more vulnerable to ransomware attacks, which can have devastating financial, legal and reputational consequences. Companies should review their data security policies and incident response plans to ensure alignment with operations during the pandemic and for the "new normal" that is expected to come after it, and consider implementing new safeguards in light of new remote work arrangements. In light of the SEC's most recent observations and current trends in ransomware attack disclosures, even an attack this is believed to have failed should trigger a materiality assessment consistent with the SEC's 2018 guidance for cybersecurity disclosures.

Authors:

Travis P. Brennan
949.725.4271
tbrennan@sycr.com

Ryan C. Wilkins
949.725.4115
rwilkins@sycr.com

Katie Beaudin
949.725.4074
kbeaudin@sycr.com