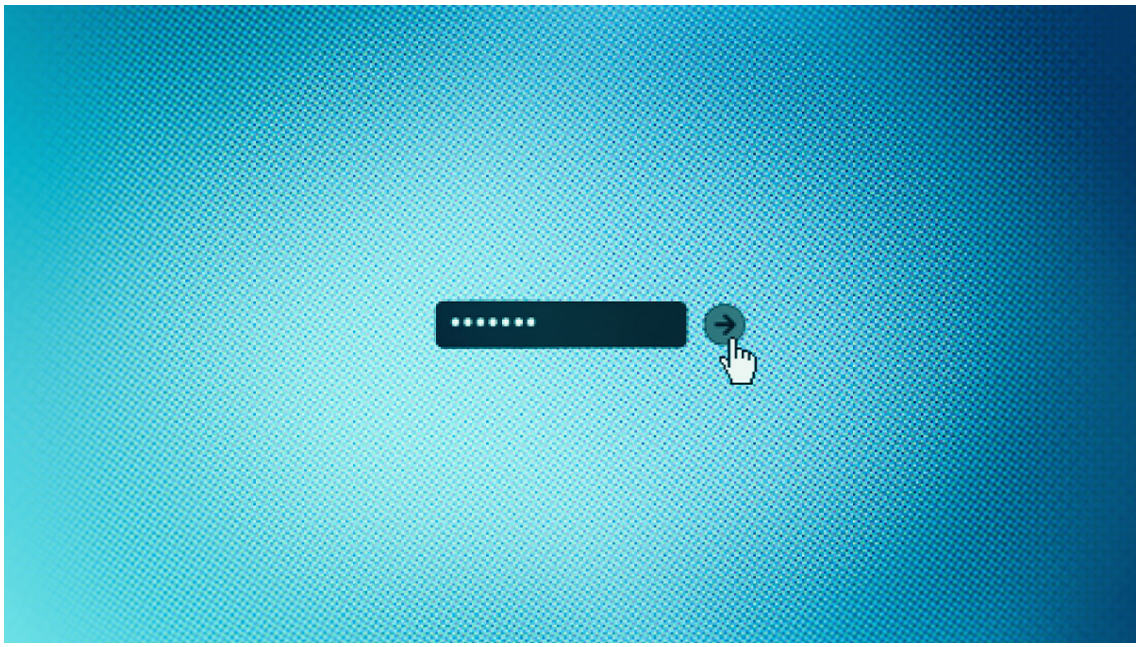
Harvard
Business
Review

Risk Management

The SEC Is Serious About Cybersecurity. Is Your Company?

by Stephen Riddick

September 08, 2021



Sean Gladwell/Getty Images

Summary. The SEC has signaled that it has started taking cyber vulnerabilities much more seriously than it has in the past. Two recent fines signal that the agency views lax cybersecurity as an existential threat to businesses and is willing to penalize companies who fall... **more**

This summer, the U.S. Securities and Exchange Commission (SEC) signaled a significant change in how it thinks about what constitutes a threat to companies: It now considers cyber vulnerabilities to be an existential business risk. This was evident in fines levied against two companies over inadequate disclosures of cybersecurity issues — British publishing company Pearson PLC and First American Financial Corp. In mid-August, the SEC announced that Pearson had agreed to pay $1 million to settle charges that it misled investors following a 2018 breach and theft of millions of student records. And in June, the SEC announced another settlement and $500,000 fine against real estate services company First American Financial for lack of disclosure controls following the discovery of a vulnerability in its system that exposed 800 million image files, including Social Security numbers and financial information.

These fines signal a major shift, and one that could profoundly change the way companies think about cybersecurity threats, communicate internally about these threats, and disclose breaches.

Businesses are required to properly disclose “risk factors” in SEC filings to inform the investing public about the risks that may come with the stocks they purchase. These risks can include competitive threats, natural disasters, supply-chain issues, economic downturns, political events, public-health issues, trade wars and cybersecurity incidents. Disclosures detail the operational risk investors face from the threats and detail their potential impacts on the company’s critical business operations, revenue, market share and reputation. While companies have to maintain proper controls for how they disclose the information to regulators, historically, there have been few regulatory repercussions from the SEC for companies that suffered cyberattacks.

This, of course, was never sustainable. The Securities and Exchange Act of 1934 was created to ensure transparency and fairness in the capital markets. While the act doesn’t specifically

require companies to disclose cybersecurity incidents, the SEC has been ramping up its warnings that it considers them a serious issue. In 2011, the agency clarified that significant cybersecurity-related risks and incidents need to be disclosed. And a 2018 update to guidance cited the "ongoing risks and threats to our capital markets" from cybersecurity incidents.

These updates — and their emphasis on the real risks that lax cybersecurity poses — reflect the state of the world right now. Just like natural disasters and supply-chain shortages of components like semiconductors, cybersecurity breaches can ultimately harm a company's financial condition and share price. In addition to the costs of remediation from a cyberattack and loss of customers, revenue and reputation, there could be shareholder lawsuits, customer lawsuits, increases in insurance premiums, and increased scrutiny from external auditors and the board of directors. There are indirect consequences as well: Cyberattacks can distract management, causing new problems; they can also trigger customer audits of a company's cybersecurity defenses, which can lead to the involvement of outside counsel and other third parties, and significant added expenses.

The First American Financial settlement is particularly notable because it inflicts operational consequences for a failure to properly disclose a cybersecurity issue that could have a material impact on the company, and thus its shareholders. The settlement signals a more forceful and direct approach from the SEC when it comes to how organizations communicate their cybersecurity risk posture and management — and companies should take notice.

So what should companies do to make sure they don't suffer a similar fate? There are fives steps corporate leaders can take to address this shift:

1. Create a disclosure committee composed of director and senior director level employees.

This committee should conduct surveys every quarter to ensure the company is aware of any material anomalies in the financial, legal, operational and cybersecurity realms that should be disclosed to senior executives, board of directors, external accountants and, potentially, the SEC.

This due-diligence process provides support for the certifications that the CEO and CFO make to the SEC every time 10Qs and 10Ks are filed and is designed to make sure the CEO and CFO have the information they need to avoid any potential disclosure-related liability. The committee should either have an infosec leader as a member or consult with infosec leaders before each meeting.

2. Don't wait too long to disclose.

Appropriate members of management, senior executives, the CEO, and the board of directors need to be informed about cybersecurity risks, incidents, and their business impacts in a timely manner — and if a public disclosure is necessary, it should be made promptly.

In the First American Financial case, six months passed between the InfoSec team becoming aware of the breach and the company's public disclosure of it. It seems the SEC is saying, at the very least, that six months is too long for a public company's disclosure controls and procedures to kick in and ultimately generate public disclosure of a breach. This is notable because the SEC has not seen fit to immerse itself in the internal affairs of public companies regarding cybersecurity before now.

Ultimately, the timing of disclosure depends on the facts of each case, such as whether the breach is material and the SEC's 8-K regulations, which generally impose a four-day disclosure requirement, are triggered, whether state or federal laws are implicated, and whether agreements with third parties are implicated.

3. Understand your risk by building visibility into your assets.

Use vulnerability management tools to assess the overall corporate and IT environment by taking an inventory to identify what assets are in your environment, their criticality to business operations and their overall exposure. This will help security teams prioritize which issues require immediate attention based on business risk, such as applying patches to critical systems.

4. Regularly conduct forensic assessments of the company's cybersecurity systems and all known and potential internal and external threats.

Once security leaders have analyzed the results and have recommendations, share the takeaways with the C-suite so they have a regular snapshot of the risk level.

5. Be prepared to disclose cybersecurity issues such as vulnerabilities, breaches and other cyber incidents before the full scope of the incident is understood.

Update disclosures as the details become more clear, financial consequences are quantified, and other repercussions emerge. Carefully determine what the impact is on the company of the incidents, how they could adversely affect operations and finances, and be prepared to divulge exactly when senior management and the board was informed.

In the end, both First American Financial and Pearson got off with relatively light penalties compared to the first case of breach disclosure issues. In 2018, Yahoo was fined $35 million for failing to reveal a 2014 data breach and its consequences in financial disclosures. However, First American Financial and Pearson are different from Yahoo in that they involve SEC action pertaining specifically to the breach and vulnerability, whereas Yahoo involved an SEC fine that came four years after the breach and which related solely to the charge of misleading investors. The new fines are proof positive from the SEC that the agency now considers cyber risk to be as significant as any other business risk that imperils the finances and future of the company and deprives the investing public of the information needed to make sound investment decisions.

Going forward, we will see greater scrutiny on how companies handle the disclosure of cybersecurity matters, in particular. The Biden administration has been laser-focused on creating greater transparency with cybersecurity in an attempt to improve our nation's defensive capabilities in the face of non-stop ransomware and other attacks. In strategic guidance provided in March, President Biden listed cybersecurity defenses as a top priority for our country's national security, the first time cybersecurity was designated as such.

Regulators will expect more transparency from public companies that experience cyberattacks and other incidents that can have material financial consequences. This is a good thing for companies and the industry as a whole. The more visibility companies have into their cyber risk the more effectively they can address it. With the right disclosure controls and best risk management practices in place, companies will be able to not just comply with SEC regulations but also better understand the risks and prevent future harm. This means less risk for their investors and a healthier marketplace.

Stephen Riddick is General Counsel at Tenable, a cyber exposure platform.