AGENDA
A Financial Times Service

Opinion

Is the SEC Failing Investors on Cyber-Security Risk?

December 3, 2018

Doug Chia

Doug Chia *is the executive director of* ***The Conference Board Governance Center****.*

Bob Zukis

Bob Zukis is CEO of Digital Directors Network, a former PwC advisory partner, and a senior fellow at the Governance Center.

Hackers hack weakness. They are efficient at finding it and work relentlessly to exploit it. Now, new moves by the **SEC** are raising questions about whether the regulator is taking the right steps to protect America's capital markets and investors.

Warren Buffett recently declared at the 2018 **Berkshire Hathaway** annual meeting that cyber risk "is uncharted territory. It's going to get worse, not better."

The SEC recently released an investigative report on "spoofing." Under this common electronic communications fraud, a hacker sends a fraudulent e-mail seemingly from a company executive or vendor asking for funds to be sent to a bank account, which is actually under the hacker's control. The FBI has identified this type of fraud as having the highest out-of-pocket costs for any class of cyber crime, an amount reaching almost $6 billion since 2013.

The SEC investigation and report were focused on raising awareness of the fraud and the requirement under federal laws that companies maintain adequate internal accounting controls over their assets. The

SEC notes management's stewardship of a company's assets and its responsibility to establish an adequate control environment are long-standing, foundational principles in federal securities law.

While this type of cyber-security fraud is relatively new, the expectation that sufficient internal accounting controls be reviewed and updated as situations warrant is not. So, in other words, the SEC's stance on cyber security is: "It's on you, public issuers." While the SEC did not pursue enforcement actions against the nine companies it investigated, it put all public companies on notice that poor cyber-security risk management could lead to regulatory consequences in the future.

For every company, the cyber-security war is a nonstop series of battles fought on many fronts with sophisticated, creative and aggressive adversaries. Unlike other enterprise risks, cyber risk rapidly propagates and scales, with a complexity not seen before. It is also unique in that there are persistent and proactive adversaries — whether well-funded nation-states, organized crime or talented mischief-makers — constantly innovating their attack strategies and tactics.

In fact, SEC commissioner **Robert Jackson** is on record as saying that "cyber security is the single biggest risk in governance today."

In its October report, the SEC recognized both the unpredictable and fast-moving nature of cyber-security risk and the comparatively slow pace of maintaining an adaptive controls environment. Given that the cyber-security risk environment is unique, shouldn't the SEC take a different approach?

Indeed, according to public company intelligence firm **MyLogIQ**, almost 35% of the S&P 500 currently make no mention of cyber-security oversight in their public disclosure filings. That sends a strong signal to hackers: America's largest public companies may be ill-prepared for the war already being fought.

Possible Solutions

There are several ways that companies can address cyber risk, considering that the SEC is holding boards responsible for it by focusing on internal controls. Requiring boards to seat cyber-security experts would be a step not unlike what the SEC mandated with qualified financial experts in the wake of Enron with the Sarbanes-Oxley Act of 2002. Also having a board-level technology and cyber-security committee is a simple step to focus oversight and ensure that a structured approach is in place to govern digital risk.

America's companies are weak at cyber risk oversight and the war is escalating. This essentially ensures an ongoing and escalating loss of assets. That this is taking place in "uncharted territory" only raises the stakes.

There is nothing that should stop issuers from taking steps to strengthen cyber-security risk oversight themselves. But protecting investors requires a more proactive approach. Lawmakers and regulators can provide leadership by requiring companies to take the simplest of steps, such as disclosing if their boards have the necessary skills to adequately govern this issue.

The investing public deserves better than what America's companies are delivering in regard to cyber-security oversight. The weakest link gets hacked; it shouldn't be America's companies.

An Information Service of Money-Media, a Financial Times Company