Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY: pwc

Cybersecurity Trends for Boards of Directors

Posted by Patrick Fitzgerald & William Ridgway, Skadden, Arps, Slate, Meagher & Flom LLP, on Thursday, April 27, 2017

Editor's note: Patrick Fitzgerald is a partner and William Ridgway is counsel at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on a Skadden publication by Mr. Fitzgerald and Mr. Ridgway.

Cybersecurity has in recent years become an integral component of a board's role in risk oversight, but directors often find themselves in unfamiliar territory when it comes to formulating policies and oversight processes that address cybersecurity risk. It can be especially challenging for directors to identify upcoming risks and avoid focusing too much on yesterday's headlines. Prioritizing the following three areas based on impending cyberthreats and emerging regulatory developments will help corporate directors stay ahead of the curve.

1. Re-Examine the Company's Business Continuity Plans and Insurance in Light of New Cyberthreats

The fall of 2016 ushered in a new cyberthreat with the massive denial-of-service attack levied against internet infrastructure provider Dyn, which knocked many of the world's major websites offline. The attack harnessed an army of insecure internet-connected devices (i.e., the internet of things), such as cameras, webcams and digital video recorders, which were infected with malware and under the control of criminal actors. The exploitation of the internet of things was a game-changer for cybersecurity because it enables denial-of-service attacks of unprecedented strength. And criminals have already set their sights on the business community as targets, seeking ways to monetize their new weapons through extortion. Companies must think carefully about their internet-exposed infrastructure and that of their vendors—everything from a customer online portal to their building's heating, ventilation and air-conditioning system-and brace for heightened levels of disruption to operations if attacked.

A similar trend is taking shape with regard to ransomware, the malware that holds its victims' data hostage through encryption until a ransom is paid in Bitcoin. Ransomware became a dominant threat in 2016, generating over $1 billion in payments. These attacks will not subside anytime soon, but many hackers have moved on to targeted cyber extortions against businesses, armed with more sophisticated malware and demanding steeper payments. Some criminals have taken to stealing sensitive files and threatening their release rather than locking them down with encryption; others have been looking to hold hostage a business' internet-connected technologies and infrastructure, much like the tactics mentioned above.

As cyberattacks take a more destructive turn, corporate directors should evaluate cyber risk differently. Compared to more run-of-the-mill breach of customer data or theft of intellectual

property (which can still be harmful), destructive attacks call for unique defensive strategies and must be met with an effective business continuity plan to minimize operational downtime. Indeed, depending on one's industry, some destructive attacks may imperil the safety of employees or customers, a risk factor that has not traditionally been part of the cybersecurity calculus.

Almost all companies have a business continuity plan on the books, but many have not stress-tested their plans against these evolving threats. One method for doing so is to enlist employees or a cybersecurity firm to attempt to execute attacks through so-called "red teaming," which should help companies identify any shortcomings before an attack strikes. Certainly such an effort will signal that the board and management are paying attention to these risks.

The board also should determine whether the company's insurance covers these new risks. Cyber insurance has traditionally focused on privacy breaches, but companies now increasingly seek policies that cover business interruption coverage, including systems failure, cyber extortion and digital asset restoration, as well as contingent business interruption coverage, which covers business interruption caused by a third party such as a cloud provider. In light of these new threats, a company should consider readjusting its insurance coverage accordingly.

2. Scrutinize the Company's Cyber Risk and Incident Disclosures to the Securities and Exchange Commission

Cyber disclosure has long been on the Securities and Exchange Commission's (SEC) radar, but based on some signals from the SEC we may now see relevant enforcement actions. In the years since the SEC released its guidance on disclosing material cyber risks and incidents, publicly traded companies have rarely disclosed specific cyber incidents. Only about three dozen data breaches are disclosed every year, a figure that pales in comparison to the number of actual successful attacks (large or small). The conventional wisdom has been that data breaches seldom move the stock price and are therefore not material. But as we have recently witnessed more examples of significant stock price movement in the wake of a cyber incident, companies should assume that both regulators and plaintiffs' counsel will be more likely to challenge a nondisclosure. That increased risk should be weighed when making the difficult assessment of whether a cyber event rises to a level requiring disclosure.

Companies also should expect that cybersecurity whistleblowers will come to the fore with greater frequency in the years ahead. Because a failure to disclose cyber risks or cyber incidents is often difficult for a regulator to identify, it is not surprising that the SEC would try to draw on its successful whistleblower program to pursue its stated goal of incentivizing more robust disclosure. The whistleblower plaintiffs' bar no doubt noticed that the latest SEC enforcement cybersecurity fine against a financial institution in June 2016 met the threshold $1 million requirement for a whistleblower payout.

As such, the board should first ensure that the company has afforded opportunities for whistleblowers to report internally, and that management has trained information technology managers about what could form the basis for cybersecurity whistleblower complaints and how to properly receive and escalate any issues raised by internal reports to the appropriate level. The board also should ensure that management carefully considers its cyber risk and incident disclosure practice, mindful of the SEC's keen interest in this area and the prospect that whistleblowers may increasingly report perceived shortcomings to the SEC.

3. Reassess the Company's Cybersecurity Compliance

Over the past several years, regulators around the world have taken a keen interest in cybersecurity and data privacy, resulting in a patchwork of overlapping regulations. Last year, however, several regulators started taking a different tack and unveiled a series of prescriptive requirements, unlike the flexible "reasonableness" standards familiar to the security community.

California was the harbinger when the attorney general's office announced that a list of 20 security controls published by the prominent security nonprofit the Center for Internet Security "define[s] a minimum level of information security that all organizations that collect or maintain personal information should meet" and that a failure to do so "constitutes a lack of reasonable security." Some in the security community were taken aback that these best practices were turned into a regulatory floor.

A similar reception was given to the New York State Department of Financial Services' landmark cybersecurity regulations for banks, insurance companies and other third party service providers within its jurisdiction, which require an array of security measures, staffing requirements and senior-level annual certifications of compliance. Soon after these regulations were announced, the Federal Reserve Board and other banking regulators issued an advanced notice of proposed rulemaking, seeking comment on a new set of enhanced cybersecurity standards for certain institutions under their supervision.

These trends are happening overseas as well. China recently announced its first-ever law devoted to cybersecurity, which imposes a number of obligations on "network operators" regarding the protection of personal information and breach notification. A set of more demanding rules, such as data localization and data transfer restrictions, will be imposed on "critical information infrastructure operators," a potentially broad term covering entities in a wide range of sectors, including public communication and information services, energy, transportation, finance, utilities and e-commerce.

As these new cybersecurity and data privacy rules come into force across the globe, it is an opportune time for corporate directors to reassess how they exercise their governance responsibilities with regard to management's handling of cyber risk and compliance.