Five Topics to Follow in 2019: Cybersecurity

February 14, 2019

Vanessa Coiteux, Stéphane Rousseau

Cybersecurity is now well established as a focus for boards of directors worldwide. The pace of developments on the regulatory and litigation fronts in 2018 and early 2019 suggests that cyber-risk management will become an even more central preoccupation for corporate leaders in the months and years to come.

Introduction

In 2018, cyberattacks have continued to roil large publicly-traded corporations. The attacks have translated in major data breaches, business disruptions, as well as fraudulent appropriations of funds. While the range of cyberattack tools is ever expanding, classic techniques such as email spoofing remain common and widely used with some degree of success. Whatever its source, malicious cyber activity can inflict serious financial, operational and reputational harms to firms.

Looking ahead, cybersecurity risk shows no sign of abating.

Regulator Guidance

It is not surprising that cybersecurity has attracted the attention of securities regulators on both sides of the border. As we have previously discussed, the Canadian Securities Administrators (CSA)[1] and the Securities and Exchange Commission (SEC)[2] have published statements and guidance regarding the disclosure of cyber risks and incidents. Recently, after having investigated a number of U.S. public issuers that were victims of cyber fraud, the SEC published an investigative report where it emphasized the link between cybersecurity and enterprise risk management:

“[I]ssuers should be mindful of the risks that cyber-related frauds pose and consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks”.

Response from Boards of Directors

Boards of directors are well aware that cybersecurity is part of their risk management responsibility. Indeed, surveys of corporate directors indicate that cybersecurity is becoming a top boardroom priority.[3] Further, institutional investors are now engaging with corporations on governance issues related to cybersecurity, including incident preparedness and responsiveness.

In this context, corporate boards are taking a number of measures to address cyber risk, including:

- Revising disclosure policies and internal controls related to cybersecurity;
- Reviewing their technological infrastructures; and
- Assessing risks associated with third party suppliers and vendors.

The adoption of the EU General Data Protection Regulation and the new requirement for mandatory reporting of security breaches to the Privacy Commissioner of Canada add an additional layer of concern for directors regarding cybersecurity.

Cybersecurity in 2019: Early Indications of a Busy Year

In 2019, Cybersecurity will undoubtedly remain a key focus for boards of directors of publicly-traded corporations. Three developments already point in that direction.

The Yahoo shareholder derivative suit settlement

The first is the settlement, approved by a California court on January 4, 2019, of a derivative lawsuit launched by shareholders against the former officers and directors of Yahoo! Inc. concerning massive data breaches resulting from a series of cyberattacks. The allegations against the officers and directors focused on their alleged failure to:

1. Implement and enforce effective internal controls with respect to data security;
2. Disclose the effectiveness of a company's data security policies;
3. Disclose the scope of the data breach; and
4. Exercise oversight duties on how a security breach could adversely affect the company's business.

The $29M settlement is notable as the derivative lawsuit rested on allegations of breach of fiduciary duties regarding cybersecurity oversight, a claim that had been hitherto unsuccessful before the courts.

The Equifax class action

The second development relates to a securities class action lawsuit introduced by investors in the context of cybersecurity incidents that caused an important data breach at Equifax. The 2017 breach impacted 148 million U.S. customers. The plaintiffs argue that Equifax and some of its officers and directors made false or misleading statements and omissions about the sensitive personal information in Equifax's custody, the vulnerability of its internal systems to cyberattack, and its compliance with data protection laws and cybersecurity best practices.

At the end of January, the U.S. District Court for the Northern District of Georgia entered an order on a motion to dismiss the class action. The court rejected defendants' argument that plaintiffs had failed to sufficiently plead that Equifax's statements regarding its cybersecurity systems were false or misleading. However, the court granted the motion to dismiss with respect to the argument that defendants had a duty to disclose specifically the occurrence of the data breach. Though not determinative, the ruling underscores the disclosure issues raised by cybersecurity incidents and risks. It is particularly notable as securities class actions for data breaches have generally been unsuccessful.

OSFI's new incident reporting advisory

The last development concerns specifically federally-regulated financial institutions (FRFIs) that are regulated by Canada's Office of the Superintendent of Financial Institutions (OSFI). The OSFI advisory *Technology and Cyber Security Incident Reporting,* published in January 2019 and in force as of March 31, 2019, provides guidance to FRFIs with respect to the timely reporting of cybersecurity incidents to OSFI. We plan to publish a separate post on the OSFI advisory in the coming weeks.

Conclusion

In light of these developments, directors will be well-advised to continue adapting corporate governance to cyber risk by reflecting on board composition and education, the responsibility for cybersecurity issues in the boardroom, and the integration of cybersecurity in risk management oversight.