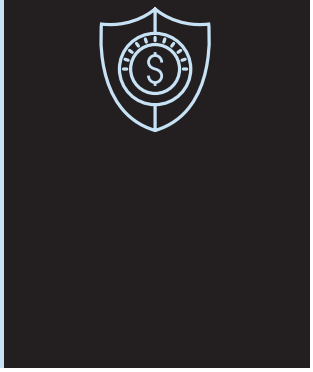
Cybersecurity: What Keeps Us Up at Night



Jonathan Kolodner
Partner
New York
jkolodner@cgsh.com

Rahul Mukhi
Partner
New York
rmukhi@cgsh.com

Megan Medeiros
Practice Development Lawyer
New York
mmedeiros@cgsh.com

According to a 2019 survey, Chief Legal Officers ranked data breaches as the most important issue keeping them "up at night."[1] Cybersecurity also remained top of mind for boards and other corporate stakeholders, particularly given the increasing reputational, regulatory and litigation consequences that often follow from a significant cybersecurity incident.

Major Data Breaches in 2019

Last year saw a continued steady stream of major cybersecurity incidents, including:

— The compromise of personal and financial information for approximately 100 million Capital One customers.

— The exposure of 885 million bank records from First American Corporation.

— Quest Diagnostics' disclosure that approximately 7.7 million patients' personal and financial data had been accessed through its external collection agency.

— The city of New Orleans declaring a state of emergency and shutting down its computers after being subject to a ransomware attack.

These are just some examples of a range of different kinds of cyberattacks that companies face, including system intrusions, business email compromise attacks (often through spearfishing) and ransomware. The continued prevalence of these attacks and their significant consequences underscore not only why companies and other organizations must devote sufficient resources to cybersecurity protection, but also why boards must be

[1] ACC Chief Legal Officers 2019 Survey, available here.

vigilant in exercising oversight of the preparation for, and response to, these incidents.

In assessing the lessons and trends reflected in these cyberattacks, companies continue to benefit from having well-developed and practiced incident response plans to ensure timely and appropriate reaction to an incident. The benefits of "segmented" data was another recurring theme. Certain companies were able to minimize the fallout from cyber incidents because they had segmented the data they stored, meaning that hackers were only able to obtain limited information and could not fully access customer personal identifying information and/or financial information. In addition, ransomware attacks on businesses are reportedly at an all-time high and becoming increasingly sophisticated. Board members should be aware of these developments and ask appropriate questions concerning management's policies and procedures around identifying and addressing these significant data security risks.

In assessing the lessons and trends reflected in these cyberattacks, companies continue to benefit from having well-developed and practiced incident response plans to ensure timely and appropriate reaction to an incident.

Regulatory Focus on Cybersecurity

In 2019, many regulators were active in bringing cybersecurity enforcement actions against companies that allegedly maintained inadequate cybersecurity protections or failed to comply with related obligations. In addition to the large financial penalties they are imposing, one significant trend is how US regulators imposed significant ongoing obligations on companies' business operations, boards of directors, corporate officers and compliance professionals. These obligations serve as an important signal of the developing (and increasingly onerous) cybersecurity expectations of regulators:

— ***Business Operations***. In settlements reached with Equifax involving the Federal Trade Commission and Attorneys General from 48 states, Equifax was not only ordered to pay a $700 million monetary penalty, but it was required to implement a robust and documented information security program that includes risk-based assessments, safeguards and qualified third-party evaluations, as well as specific security measures such as password encryption, multi-factor authentication and periodic penetration testing. The AG settlements further mandated that Equifax conduct biannual incident response exercises and weekly vulnerability scans of network systems, as well as begin remediating any "critical" security vulnerabilities within 24 hours.

— ***Compliance***. The FTC settlement with Equifax also required Equifax to designate the board of directors, a relevant committee thereof or a "senior officer" "responsible for [the] Information Security Program" to annually certify *under penalty of perjury* that Equifax has established the required information security program, is cooperating with the required third-party assessor evaluating the information security program and is not aware of any material non-compliance with the federal orders. Similarly, in connection with Facebook's settlement with the FTC related to Cambridge Analytica, CEO Mark Zuckerberg and Facebook compliance officers must personally certify quarterly that Facebook has established and maintained the privacy program required under the FTC settlement.

— ***Board Oversight***. In connection with Facebook's FTC settlement, the company was also required to create two new board committees: an Independent Privacy Committee and an Independent Nominating Committee. The Independent Privacy Committee is comprised of independent directors demonstrating certain minimum privacy and data protection capabilities and is responsible for meeting at least quarterly with other independent directors and a

third-party privacy assessor mandated by the order to discuss privacy issues, risks and compliance with the order, among other things. The committee must also approve any effort to remove or appoint an assessor. The Independent Nominating Committee, in turn, recommends and approves the appointment or removal of members of the Independent Privacy Committee, including determining whether members of that committee have the required privacy and data protection expertise.

Another important development is the increasing aggressiveness of European regulators in enforcing the General Data Protection Regulation (GDPR). In particular, the UK Information Commissioner's Office (ICO) announced headline-grabbing enforcement actions relating to alleged cybersecurity breaches and data protection violations in 2019:

— ***British Airways***. While not quite reaching the maximum fine permitted by the GDPR (up to the higher of €20 million or 4% of a company's global turnover), the ICO announced its intention to fine British Airways £183.4 million for a cybersecurity incident resulting in the misappropriation of the personal data of approximately 500,000 British Airways customers. The ICO has not disclosed how it determined the size of this fine, but it amounts to approximately 1.5% of British Airways global passenger turnover. The ICO noted that its investigation revealed that British Airways had "poor security arrangements" in relation to its customers' information.

— ***Marriott***. In July 2019, the ICO published its intention to fine Marriott £99.2 million for a cybersecurity incident affecting the Starwood guest reservation database starting as early as 2014—notably, before Marriott acquired Starwood in 2016—but not discovered until 2018. Records relating to about 30 million individuals in the European Economic Area were affected—7 million of which were related to individuals in the UK. Like the fine in British Airways, the ICO did not disclose how it calculated the fine, but it appears to amount to approximately 0.6% of Marriott's revenues in 2018.

One final regulatory note heading into 2020: More and more jurisdictions are imposing affirmative cybersecurity and data protection obligations on companies, beyond data breach notification obligations. Among other developments, in 2019, New York passed the SHIELD Act that, for the first time, affirmatively requires covered businesses to develop, implement and maintain "reasonable" data security safeguards, which include, among other things, conducting risk assessments and addressing identified risks. This will be a particular area to watch as regulators continue their focus on cybersecurity compliance in 2020.

Among other developments, in 2019, New York passed the SHIELD Act that, for the first time, affirmatively requires covered businesses to develop, implement and maintain "reasonable" data security safeguards, which include, among other things, conducting risk assessments and addressing identified risks.

Litigation Developments

2019 also saw a significant uptick in US shareholder litigation relating to data breaches. Until 2019, shareholder derivative cases against board members arising out of a data breach had resulted in either dismissals or settlements with relatively low monetary payments. However, in early 2019, *In re Yahoo! Inc. Shareholder Litigation* resulted in a significant monetary settlement by the defendants, potentially breathing new life into shareholder derivative claims following a significant data breach.

The complaints alleged, among other things, that Yahoo and its former and current executives and officers breached their fiduciary duties by failing to timely disclose and concealing two data breaches. The settlement reached by the board members and other defendants provided for a $29 million payment

to settle the derivative claims, by far the largest such settlement to date.

Shareholder securities fraud litigation also proceeded at a brisk pace, largely mirroring claims filed in prior years by claiming that public companies failed to adequately and/or timely disclose material cybersecurity incidents and risks. The success of these cases has turned on whether the company's public disclosures concerning cybersecurity risks and incidents were sufficiently robust to defeat claims that shareholders were misled.

Key Takeaways for Boards of Directors

— Data breach incidents continue to proliferate, with business email compromise and ransomware attacks against businesses on the rise in particular. Board members should focus on whether adequate resources are being dedicated by management to identify and address such risks, and whether management has a well-tested plan in place to execute in case of an attack.

— Regulators in the US and Europe continue their focus on cybersecurity. In addition to monetary penalties, certain regulators are also seeking to require companies to implement privacy and cybersecurity risk assessments, third-party monitoring, specified director and officer responsibilities and changes to board composition. If these promises are violated in the future, the company is subject to significant additional fines.

— Shareholders, regulators and courts will expect that boards, management and compliance personnel play increasingly active roles in privacy and cybersecurity oversight.

— The announced enforcement action against Marriott with respect to the Starwood breach, as well as related sprawling litigation, underscores that purchasers and investors should consider the necessary transactional due diligence with respect to material cybersecurity and privacy risks.

— US litigation risk following a data breach continues to be significant, with derivative actions against board members potentially on the rise following developments in 2019.