Milbank

Adam Fee and Matthew Laroche are partners and Marion Burke is an associate at Milbank LLP. Mr Fee can be contacted on +1 (212) 530 5101 or by email: afee@milbank.com. Mr Laroche can be contacted on +1 (212) 530 5514 or by email: mlaroche@milbank.com. Ms Burke can be contacted on +1 (212) 530 5065 or by email: mburke@milbank.com.

SPOTLIGHT ARTICLE REPRINT February 2023

Board responsibility for cyber security risk: guidance for navigating an evolving legal and regulatory environment

BY ADAM FEE, MATTHEW LAROCHE AND MARION BURKE

Last year saw a record-breaking number of cyber attacks, including escalating malware-based, phishing and denial of service attacks, to name a few. Some of the largest and most well-known companies in the world were victims of cyber incidents, including Apple, Cisco, Meta, Samsung, Twitter and Uber.

As an added challenge, cyber attacks have continued to become more sophisticated, often inflicting immense damage to businesses and governments across the globe. In May 2022, for instance, the Costa Rican government was forced to declare a state of emergency after a ransomware group breached systems of nearly 30 government institutions, stole highly valuable data, and demanded tens of millions of dollars to avoid it being leaked.

Companies suffer significant consequences not just from the breach itself but the litigation that often flows from it. Last year, T-Mobile settled a class action lawsuit following a data breach for $350m, and other data breach cases brought in the past decade have reached settlements well into the tens of millions of dollars.

Government and regulatory bodies also have taken notice, with companies facing pressure to effectively respond to cyber security incidents, and hefty fines when they arguably do not. More recently, boards are coming into the crosshairs and facing stockholder derivative claims in the US for the alleged breach of directors' cyber security oversight duties (referred to as *Caremark* claims under US law).

Under the US court decision *Caremark*, directors can face personal liability for failing to prevent harm under circumstances involving their knowing bad faith. Bad faith may be established based on allegations that the board either 'completely failed' to implement board-level reporting or control

systems, or failed to properly monitor or oversee the operation of those systems.

In two recent derivative suits before the Delaware Court of Chancery, plaintiffs asserted *Caremark* claims against directors for their alleged failure to oversee cyber security risk in the wake of cyber attacks that exposed customer data. Although both cases were dismissed at the pleading stage based on a failure to adequately allege bad faith, the cases highlight that cyber security is typically a 'mission critical' risk that must be effectively managed and monitored by companies and boards.

In *Construction Industry Laborers Pension Fund v. Bingle* (6 September 2022, *SolarWinds*), plaintiffs brought suit following a cyber attack of SolarWinds Corporation, a company in the business of developing software to manage technology infrastructure, which resulted in a massive leak of its customers' personal information. In dismissing the case, the court rejected allegations that the directors acted in bad faith by failing to follow Securities and Exchange Commission (SEC) guidance concerning cyber security because that guidance did "not establish positive law with respect to required cyber security procedures or how to manage cyber security risks".

As to allegations that directors consciously disregarded red flags, the court noted that the board's "oversight duties here appear in hindsight far from ideal" because, for example, they failed to receive a cyber security briefing in 26 months and ignored industry warnings about cyber attacks. Nevertheless, the court concluded that the allegations did not rise to an inference that the board acted in bad faith by showing an "utter failure" to monitor cyber security risk.

The Court of Chancery reached a similar conclusion in *Firemen's Retirement System of St. Louis v. Sorenson* (5 October 2021, *Sorenson*). There, plaintiffs brought suit following a data security breach discovered by Marriott International, Inc., which exposed the personal information of up to 500 million hotel guests. Plaintiffs failed to show bad faith because the allegations did not support that the directors "completely failed to undertake their oversight responsibilities, turned a blind eye to known compliance violations, or consciously failed to remediate cybersecurity failure".

Both *SolarWinds* and *Sorenson* reinforce that it is difficult to establish bad faith under *Caremark*. But they also highlight the need for companies and boards to remain vigilant with respect to cyber security risk. The decisions underscore certain 'bad practices' that boards should avoid, including the failure of committees with cyber security oversight responsibilities to regularly report to the board (*SolarWinds*), to adequately consider industry warnings (*SolarWinds*) and to conduct appropriate cyber security due diligence when acquiring a company (*Sorenson*).

Moreover, in both cases, plaintiffs alleged that the boards violated "positive law" by reference to industry standards promulgated by regulatory bodies. The courts rejected those arguments because the cited standards were not legal requirements but simply industry guidance. Nevertheless, it is well settled that violation of positive law heightens the risk of *Caremark* liability, which was a point underscored in the *SolarWinds* and *Sorenson* decisions.

As more companies become subject to laws and regulations governing cyber security practices, it is likely that plaintiffs will focus their allegations on noncompliance with those requirements. In this respect, new cyber security laws and regulations are proliferating. One significant regulatory development is the SEC's new proposed rules, announced on 9 March 2022, to enhance and standardise disclosure requirements for cyber security risks. Most notably, the rules would impose a rapid reporting requirement when covered companies face serious cyber attacks. Specifically, companies would have to report any "material cybersecurity incident" within four business days of its discovery.

The four-day clock begins to tick as soon as a company "determines that it has experienced" a significant incident, and there is no exception for delay in disclosure pending law enforcement investigations. Beyond the four-day reporting requirement, the proposed rules would impose other novel cyber security requirements on companies, including periodic reporting about: (i) a public company's policies and procedures to identify and manage cyber security risks; (ii) the board's cyber security expertise and oversight of cyber security risks; and (iii) management's role and expertise in assessing and managing cyber security risk and implementing cyber security policies and procedures.

The SEC's proposed rules are the tip of the iceberg. In 2022, 40 states introduced or considered more than 250 bills addressing cyber security. In March 2022, president Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act, which will expand cyber reporting obligation for a wide range of public and private entities. Governments around the globe are also redoubling efforts to protect data, and it is estimated that by 2023, over half of the world's population will have personal data covered under privacy regulations.

In light of the recent *Caremark* decisions and expected legal and regulatory developments, companies and boards should revisit their cyber security oversight roles and structures. At a high level, boards that have not delegated responsibility for overseeing cyber security to a specific board committee should consider doing so. Boards also need to assess whether the amount of time they spend addressing cyber security is appropriate and should consider receiving cyber security reports on at least a quarterly basis or more frequently as circumstances require. Companies also should consider the channels through which cyber security information is communicated to the board and evaluate whether those channels provide effective and timely communications.

Once boards have an effective oversight structure in place, they should ensure that the board or board committee with cyber security responsibilities is receiving appropriate management reports. Those reports should address, at a minimum: (i) external risks, such as updates on cyber security as it relates to supply chain, business partner relationships and business initiatives (e.g., acquisitions), management's plan for implementing

appropriate protections against cyber intrusions, and significant legal and regulatory developments; (ii) internal risks, such as explanations of mission-critical systems that the company uses, assessments of the company-wide cyber security programmes and cyber insurance coverage; and (iii) policies, procedures and training relating to cyber security.

Companies and boards also should ensure that the full board receives periodic reporting, at least on an annual basis, concerning cyber security. Those briefings should review procedures for responding to data breach incidents and communications with regulators and stakeholders, key cyber risks, including the main threat actors and potential business impact, and the sufficiency of cyber budgets and resources. The board also should consider having periodic reports from external cyber advisers with whom the company's cyber security management team has consulted.

If (and likely when) there is a cyber incident, the board and management should receive incident-specific reports whenever there is a basis to believe that the incident may materially impact the company's operations, reputation or financial performance. The board should also be briefed on the company's response to the incident and related impacts, the status of internal and external investigations, whether the company's response plan worked, and whether management recommends material changes to the response plan or the company's cyber security systems.

Finally, board and committee oversight activities should be appropriately documented in minutes and supporting materials. Stockholder inspection demands to review a company's books and records, including board and committee-level minutes, in preparation for litigation are becoming increasingly common.

Given the proliferation of sophisticated cyber attacks and the recent court opinions addressing a board's cyber security oversight duties, boards and companies need to remain focused on cyber security risk. By taking the steps outlined herein, boards will put themselves in the best position to appropriately monitor cyber security issues and limit associated legal and regulatory exposure. ■