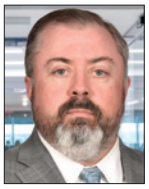
New York Law Journal
Corporate Update
WWW.NYLJ.COM
An ALM Publication
VOLUME 262—NO. 43
THURSDAY, AUGUST 29, 2019

CYBERSECURITY

More Than Ever, Cybersecurity Is a Board-Level Concern

By **Andrew T. Garbarino**



SHUTTERSTOCK

On June 18, 2019, Delaware's Supreme Court issued a decision in *Marchand v. Barnhill*, 2019 WL 2509617, reversing a Delaware Court of Chancery's dismissal of a shareholder derivative suit bringing claims under *In re Caremark*, 698 A.2d 959 (Del. Ch. 1996) stemming from a listeria outbreak that resulted in the deaths of three people who consumed Blue Bell ice cream and necessitated a disastrous total product recall.

Marchand seems a relatively straightforward interpretation of *Caremark*, underscoring a board's "bottom-line" requirement that it make a good faith effort to implement board-level compliance and monitoring systems. See *Marchand* at 12. The court found that even though board minutes reflected that the board was generally aware of the listeria issue, it failed to establish its own monitoring system. Id. at 14. The board should have instituted monitoring even though the company itself "nominally complied with [food safety] regulations," because *Caremark* "require[s] that a board attempt to formulate a reasonable system of monitoring and reporting about the corporation's central compliance risks." Id.

Where could be more of a central compliance risk than cybersecurity?

Cybersecurity has long been considered an IT concern. State-of-the-art hardware and cutting-edge software have traditionally been the tools used to address cybersecurity—even then somewhat passively. It used to be that breaches were rare events.

In 2012, then FBI Director Robert Mueller noted that, in the context of cybersecurity, there were two sorts of companies: those that have been hacked and those that would be. In the intervening years, his statement has proved prophetic.

Hacking scandals have been major news for years now. In 2018, Under Armour, Facebook and Panera Bread all suffered costly breaches. Before that, Target, Anthem, Equifax, Seagate, Ashley Madison—the list could fill pag-

ANDREW T. GARBARINO *is of counsel with Ruskin Moscou Faltischek, P.C. where he is a member of the health care, white-collar crime & investigations, not-for-profit and cybersecurity & data privacy groups.*

es—were all high-profile institutional victims of breaches. Banks and major law firms have suffered breaches. As of this writing, Capital One suffered the latest major breach; there can be no doubt that the next is just around the corner.

The prevalence of attacks (which may be better considered varying degrees of corporate failings for the purpose of this article), has created a minefield of issues that must be addressed at the board level, especially considering the *Marchand* ruling.

An Evolving Threat

Almost all boards must confront the ostensibly unbounding evolution of technology. The maelstrom of innovation (constantly improving technology creating different opportunities for hackers, which increases cybersecurity costs, heightened regulation and liabilities) carries the real chance of scuttling an organization as it attempts to remain on par with potential hackers.

The hackers seem increasingly sophisticated. Some are rogue individuals, seeking notoriety, revenge or personal gain. Some are corporate spies seeking to cause damage to competitors. Even nations like Russia, China and North Korea—all of which have been linked to cyber wrongdoing at a minimum, cyber terrorism at worst—have attempted to improve their economic standing on a potential trillion-dollar level. A terrorist organization may have even hacked the Town of Brookhaven on Long Island. See "Brookhaven Disables Town Website After Possible ISIS-Related Attack," *Newsday*, June 26, 2017.

Worse, cyber-attacks are becoming increasingly newsworthy. Much like the weather, cyber-attacks impact many millions of individuals at a time. As attacks become more newsworthy, authorities feel pressure to regulate and prosecute those involved in the attacks. From a public relations standpoint alone, the cost of a company's cybersecurity failing can be devastating and difficult to address.

Cyber-breaches are, and will likely continue to be, ubiquitous. As prophesized by Robert Mueller, no organization, be it publicly traded or not-for-profit, private or municipal, international or a small local shop, is immune from the dangers posed by a breach. As such, directors must affirmatively and proactively account for the adequacy of their company's cybersecurity or risk liability.

The prevalence of attacks … has created a minefield of issues that must be addressed at the board level, especially considering the 'Marchand' ruling.

Litigation: A Perilous Landscape

The abundance of litigation concerning recent breaches and the dollars involved are astounding. The Anthem class action settlement alone reached nine figures—$115 million—absent legal costs and the cost of investigating and remediating the issues leading to the breach, both of which were surely significant.

Organizations that suffer breaches have been sued by customers (Anthem and Target), shareholders in derivative lawsuits (Yahoo! and Wendy's) and employees (Sony—after being hacked by North Korea). In addition to those classes of potential plaintiffs, Home Depot was sued by a cadre of credit card companies that were impacted by a breach suffered by the company.

While the organizations listed above are large national and international companies, hacking targets include banks, law firms and health care organizations, whose data is especially valuable. See Caroline Hummer and Jim Finkle, "Your Medical Record Is Worth More to Hackers Than Your Credit Card," *Reuters* (Sept. 24, 2014). The not-for-profit sector is especially vulnerable, as those organizations often have donor information, private data of applicants and occasionally the aforementioned healthcare data, while lacking the resources available to large, for-profit entities.

Suits related to cyber concerns have been premised on theories ranging from breaches of fiduciary duty (for failing to effectively implement and oversee cybersecurity policies and protocol,) and failing to timely disclose cybersecurity breaches. The multiple theories of liability compounded by the multiple classes of plaintiff and the sheer number of potential victims of a breach shape a perilous landscape.

Litigations brought by various state attorneys-general, that uniformly seem to include forms of monitoring as requisites for settlement, can protract costs for a single breach over years or even decades. Once regulators take action, the company's board and officers often lose the ability to direct compliance protocol to government actors, who likely cannot understand

an organization's needs or appreciate the ongoing costs of court-approved codes of behavior. Even if a board does not face liability itself, a breach may cause government actors to require especially stringent compliance.

Compliance: Steeper Terrain

New and forthcoming government regulation and enforcement may prove more daunting. GDPR, California's CCPA and New York's SHIELD Act all seek to standardize data protection and have forced companies to consider their compliance needs. Many boards don't understand what data their company receives and retains in the course of business. Ignorance, in this arena, is potentially actionable, especially considering *Marchand*: How may one protect what one doesn't know exists?

It's no secret that the SEC has made cybersecurity a chief concern by announcing the creation of its own Cyber Unit. The SEC has recognized the danger hacking poses in the potential to obtain information that may aid in manipulating markets, insider trading (by outsiders in this context,) and other concerns. Combined with the SEC's continued pursuit of so-called "gatekeeper" failures which has focused on investigations and even charges against accounting firms (e.g., "Audit Firm Charged With Fraud Relating to Auditing of Penny Stock Companies" (Dec. 4, 2017), one is left to wonder how failings in cybersecurity may soon lead to similar regulatory intervention in the board room.

Director Responsibility

To avoid litigation, government intervention and public relations fiascos, a board must address cybersecurity on an ongoing basis. It is not enough to place faith in the company's IT group. Cybersecurity must be at the forefront of issues addressed on a regular basis. Directors may continue to be apathetic to cybersecurity at their own risk; it is essential to appreciate the risk of breaches, take affirmative steps to avoid them and mandate effective protocols should a breach occur.

One step should be the creation of a board committee to address cybersecurity. A smaller set of directors who are attuned to technology and data concerns can focus on necessary foundational steps, such as addressing the organization's technology and in-house IT talent, security (cybersecurity and physical security, such as access to hardware), audits and strategies accounting for innovation in hardware and software while keeping pace with sophisticated hacking. That committee would then be in a position to advise and educate the full board on facets of cybersecurity that may be hard for other board members to easily grasp. Frequent cybersecurity updates for the entire board should be a consistent agenda item. A board's compliance committee should also understand the organization's responsibilities from a regulatory standpoint and provide input on action plans.

Protocols must be followed when a notification under a policy is obligatory, focusing on mitigating the attack to lessen damage and investigate how the attack was accomplished. Once a threshold is crossed by a cyberattack, there must be no stopping the action steps required, and a board must adhere to that philosophy or risk civil, administrative or even criminal liability. Counsel should immediately be engaged to preserve privilege, consider and coordinate the involvement of law enforcement and potentially retain a public relations consultant to address potential investor and customer relations.

If disclosures concerning a particular cyber event are necessary, by law and regulation or by organizational guidelines, applicable deadlines should not only be understood, but affirmatively followed, lest accusations of an institutional cover-up be alleged.

The entirety of the board must be aware of data used and retained by their organization. In turn, the board should make clear to the rest of the organization, from the C-suite comprehensively downward, that data security is a chief concern and must be addressed on a daily basis.

Conclusion

There is no absolute defense against a data breach. A board can only do its best to ensure that its organization is as protected as possible and, under *Marchand* and applicable regulation, it must. Cyber predators prey upon those institutions unprepared or averse to addressing the concern. Failing to prepare for a cyberattack may only lead to ruin.