SQUIRE PATTON BOGGS

THETALAKE

What's a Board To Do?

US – September 2022

Authors:
J.D. Bridges, Senior Technology Counsel, Theta Lake Inc.
Daniel G. Berick, Partner, Squire Patton Boggs

Proposed Securities and Exchange Commission (SEC) Cybersecurity Rules, *Caremark* and the Ongoing Risks to (and From) Public Companies

New SEC rules seek to give investors more insight into publicly traded companies' cybersecurity posture, but will not end up making those companies materially more prepared for a cyberattack or the public less vulnerable to the effects of such attacks.

Introduction

Earlier this spring, the SEC proposed amendments to its rules to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting."[1] The proposed rules require public companies to provide current reporting about "material" cybersecurity incidents, periodic reporting to provide updates on previous incidents, and information on the company's policies and procedures to identify and manage cyber-risks. The proposed rules would also require periodic reporting on the board of directors' oversight of cyber–risk, and management's role and expertise in assessing and managing cyber-risk.

The SEC appears to be squarely directing boards to understand and actively manage cyber-risk. By requiring current and periodic reporting via Forms 10-K, 10-Q or 8-K (or 20-F or 6-K, for foreign private issuers), as well as disclosure in proxy statements, it is making plain its desire for the leadership of public companies to not only understand and manage cyber–risks, but to inform their investors and prospective investors about such risks. Under the proposed rules, the SEC will require public companies to disclose not only whether they have a cybersecurity program, but will require them to describe their programs in some detail in their Form 10-K. Companies will have to describe their cybersecurity protocol, reveal the names and expertise of board members and managers who are responsible for cybersecurity, and report previous cybersecurity incidents and how they responded to them. They will also need to describe the cybersecurity risks they face and how they plan to respond to incidents in the future. If investors begin to weigh these additional disclosures in making their investment decisions, there may be considerable pressure on publicly traded companies to change their cybersecurity programs.

This pressure will be compounded by the SEC's proposed new reporting requirements surrounding material cybersecurity incidents. When a company realizes that it has experienced a material cybersecurity incident, it will have four business days to file a Form 8-K describing the incident. The Form 8-K must report when the incident was discovered and if it was resolved, describe the nature and the breadth of the incident, detail whether data has been compromised and explain how it will impact the company's operations. Companies will have to share information that will not only create concern for investors, but may expose their vulnerabilities and put them at further risk for additional cybersecurity attacks as well.

Caremark – What Boards Know Now

Separately from the SEC's proposed rules, a board's duty to understand and manage cyber risk has most recently been investigated in litigation in Delaware under the *Caremark* standard. The Delaware Court of Chancery, in its landmark 1996 decision *In Re Caremark*, articulated the now-famous standard for a board to avoid liability for failing to properly oversee a company – directors must act in good faith and be "reasonably informed" about the corporation.[2] In order to be reasonably informed, the court stated, the board must assure itself that management will inform it of relevant, appropriate information in a timely manner in the ordinary course of business. In order to fail this test, however, a very high bar (or very low bar, perhaps) must be met – in order for a claim to go forward, it must allege a "systematic failure of the board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists." A board could also fail the *Caremark* test by failing to monitor the risks reported by such a system or by instituting an obviously unreasonable or inadequate system.

Caremark is a high bar indeed – until 2019 there were virtually no cases brought in Delaware alleging a failure of its standard that survived beyond a motion to dismiss. Since *Marchand v. Barnhill* in 2019, however, Delaware courts have seemed more inclined to allow such claims to proceed, and cybersecurity issues have become a more prominent part of them.[3] In 2021's *Firemen's Ret. Sys. of St. Louis v. Sorenson*, the plaintiffs alleged that, soon after Marriott's acquisition of Starwood Hotels and Resorts Worldwide Inc. in 2016, Marriott suffered a massive data breach – exposing more than 500 million guest records – as a result of Starwood's antiquated reservation database.[4]

1 Cybersecurity Risk Management for Investment Advisors, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13523 (proposed Mar. 9, 2022) (to be codified at 17 C.F.R. pt. 229, 232, 239, 240, and 249).

2 *In re Caremark Int'l*, 698 A.2d 959, (Del. Ch.1996). *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

3 212 A.3d 805, 824 (Del. 2019).

4 No. 2019-0965-LWW, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021).

They further alleged that Marriott's board was liable under *Caremark* for its "conscious and bad faith decision not to remedy Starwood's severely deficient information protection systems."[5] In *Sorenson*, however, the court found that the Marriott board had in fact been regularly apprised of cyber-risks and had acted on those risks, including engaging outside consultants to help mitigate them, and denied the plaintiff's claim for *Caremark* relief.

Not all recent *Caremark* legislation has failed, however. In 2021's *In re Boeing Company Derivative Litigation*, the court sustained a claim that the Boeing board had ignored a mission-critical aspect of its business because it had not been regularly informed about aircraft safety – no board committee for safety existed, it did not discuss or monitor safety on a regular basis, it had no regular process for being updated about safety issues, it never received information on "red flags" related to safety from management, and had even made statements that it knew it should have had processes in place to be informed about safety information.[6] The case settled out of court, but not until after the court had denied the motion to dismiss the *Caremark* claim.

Interpretation of the Proposed Rules – Prescriptive or Broad?

Interestingly, the court in *Sorenson* made strong statements about the importance of cybersecurity programs (which have been widely quoted in discussion of the proposed SEC rules), stating that "cybersecurity has increasingly become a central compliance risk deserving of board level monitoring at companies across sectors," and asserting that "as the legal and regulatory risks become manifest, corporate governance must evolve to address them. The… harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."[7]

Whether or not the proposed rules will actually cause companies to put in place such "appropriate" systems is a matter of some debate – the rules do not specify what such a system might entail. The sole commissioner to vote against the proposed rules wrote in her dissenting statement that the rules "look more like a list of expectations about what issuers' cybersecurity programs should look like and how they should operate," and that they would "have the undeniable effect of incentivizing companies to take specific actions to avoid appearing as if they do not take cybersecurity as seriously as other companies."[8] The new rules, however, pertain largely to reporting – what happened and when, what the company's policies are, and the like – and not to the substance of any cybersecurity program or policy. For instance, the proposed amendments to Form 10-K require companies to disclose their policies and procedures, if any, for identifying and managing cybersecurity risks. It requires companies to disclose in annual reports and proxy statements whether any board members have expertise in cybersecurity. It further requires reporting on management's expertise in assessing and managing cybersecurity risk, but does not specify what level of expertise management should have. It could be argued that, by requiring a company report on things like this "expertise," the SEC is expecting that investors will demand that companies have some reasonable measure of it in place – and that may provide a roadmap to a *Caremark* claim, but is very different from the imposition of a substantive standard.

Further, the SEC is concerned with investors, and not with technology *per se* – the threshold for disclosure of "material," as applied to cybersecurity incidents, would be that which the Supreme Court has defined in a series of disclosure-related cases as "a substantial likelihood that a reasonable shareholder would consider it important"9 in making an investment decision. It is not clear that the average shareholder – or even, at present, a sophisticated shareholder – has a grasp of what constitutes an important cybersecurity issue for today's modern, global business enterprises. Furthermore, the technological threats, and the safeguards against those threats, are constantly changing. Boards will have a difficult enough time deciding for themselves what might have constituted a material incident to report, and such backward-looking reporting may have little effect on a company's preparedness against future cyberthreats. Boards are already incentivized by market pressures to minimize or not report events that may be on the threshold of materiality – and the reputational risks of a major cybersecurity event are not insignificant.

The Proposed Rules Do Not Make Companies Safer

There is no specific safe harbor for boards that follow the SEC rules as to any underlying cyber incident, of course – they are purely disclosure rules. Therefore, it seems possible that a company could comply with the SEC rules, if adopted, and still fail a *Caremark* challenge if its board exercised phenomenally bad judgment at some point. It remains to be seen what the final rules will look like, and, even more tellingly, how companies will choose to frame their public disclosures in order to comply with them. Law firms and consulting practices are, of course, urging public companies to review their cybersecurity and governance practices, and no doubt some will choose to improve those practices in anticipation of having to disclose more information about them. But, given the SEC's mandate to protect investors (rather than, say, consumers), it is likely that public companies will now be incentivized to structure their cybersecurity programs to comply with the rules first and protect against cybersecurity threats second. This proposed enhanced disclosure may lead to lower valuations for companies with spotty cyber histories, both in the public markets and in corporate transactions, but it is not likely to lead to fewer cyber incidents.

5 *Id at* 12.

6 No. 2019-0907-MTZ, 2021 WL 4059934, (Del. Ch. Sept. 7, 2021).

7 *Sorenson*, 2021 WL 4593777, at *12.

8 https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922

9 *See TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438 (1976); B*asic, Inc. v. Levinson*, 485 U.S. 224 (1988); and *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27 (2011).

There are, of course, other regulatory bodies which seek to force companies to improve their cybersecurity practices. The Federal Trade Commission, under its mandate to protect consumers from unfair, fraudulent and deceptive business practices, has traditionally been the agency which has been most active in reacting to cybersecurity incidents – it has issued fines and consent decrees to large public and private companies. The Cybersecurity and Infrastructure Security Agency, a part of the Department of Homeland Security, was established to better prepare the federal government and the US against cyberthreats, but it does not have enforcement capabilities. Various state agencies are beginning to propagate as well (largely in concert with the introduction of data privacy laws), such as the California Privacy Protection Agency, which is intended to enforce the California Privacy Rights Act. No agency, however, has the history and clout of the SEC when it comes to changing the behavior of corporate America and its flagship public companies.

At some point, if the SEC's new rules are adopted, someone will likely test the theory that compliance with them meets the *Caremark* standard all on its own, and compliance would and should carry some weight with Delaware courts. But it should not become a de facto safe harbor, and federal regulators in all sectors should continue to incentivize companies – both public and private – to improve their cybersecurity. Federal privacy legislation, along the lines of the California Privacy Rights Act or Europe's General Data Protection Regulation, would no doubt be a significant factor, but, until any such legislation actually makes it out of Congress with its teeth intact, the public should not assume that the proposed SEC rules will force companies to make significant improvements in their cybersecurity posture – and companies should not expect compliance to protect them from continuing litigation, both under Caremark and otherwise.

Contacts

Daniel G. Berick
Partner, Cleveland
T +1 216 479 8374
E daniel.berick@squirepb.com

Guest Author:

JD Bridges
Senior Technology Counsel, Theta Lake Inc.
T +1 650 514 5300
E jd@thetalake.com

With thanks to **Madeline Maersk-Moller**, 2022 Summer Associate and JD Candidate, University of Colorado Law School (Class of 2024), who contributed to this article.