ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Boards Under Fire

Compliance and Ethics

Information Governance

Technology, Privacy, and eCommerce

Corporate, Securities, and Governance

Banner artwork by *bussolati.com*

Cheat Sheet

- **Cybersecurity is top of mind.** Public company boards need to be especially careful as they have been increasingly targeted by shareholder suits.
- **Working remotely is part of the issue.** Whether work is completely or partly remote, companies are still responsible for cybersecurity.
- **Cybersecurity and compliance are separate but related.** Boards need to pay attention to both.
- **In-house counsel need to be knowledgeable.** You need to understand and, as needed, seek expert advice to protect your company — and board.

As businesses continue to expand the amount of data they produce and consume while simultaneously managing remote or hybrid work forces, cybersecurity remains on the radar of federal regulators, litigators — and criminals.

And as cyberattacks increase in frequency and cost, the US Securities and Exchange Commission

(SEC) has proposed amendments to its rules to “enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting.”

In the meantime, the SEC recently levied record fines against a handful of the world’s largest financial services firms for lax data governance practices involving communication tools. Additionally, public company boards continue to face shareholder scrutiny and litigation related to *Caremark* liability in the Delaware courts over security breaches and other alleged failures to adequately supervise their companies — some of which is beginning to gain traction in ways it had not previously.

The SEC has issued penalties and fines to many financial services firms due to non-compliance and lax data governance. Andrii Yalanskyi / *Shutterstock.com*

All this may seem to amount to a perfect storm of pressure on boards to step up their participation in and oversight of cybersecurity and data privacy practices, but it’s unlikely that the proposed SEC rules, in isolation, would actually end up making public companies — or the public — safer. What exactly will? That remains to be seen.

> It’s unlikely that the proposed SEC rules, in isolation, would actually end up making public companies — or the public — safer.

Proposed SEC rules

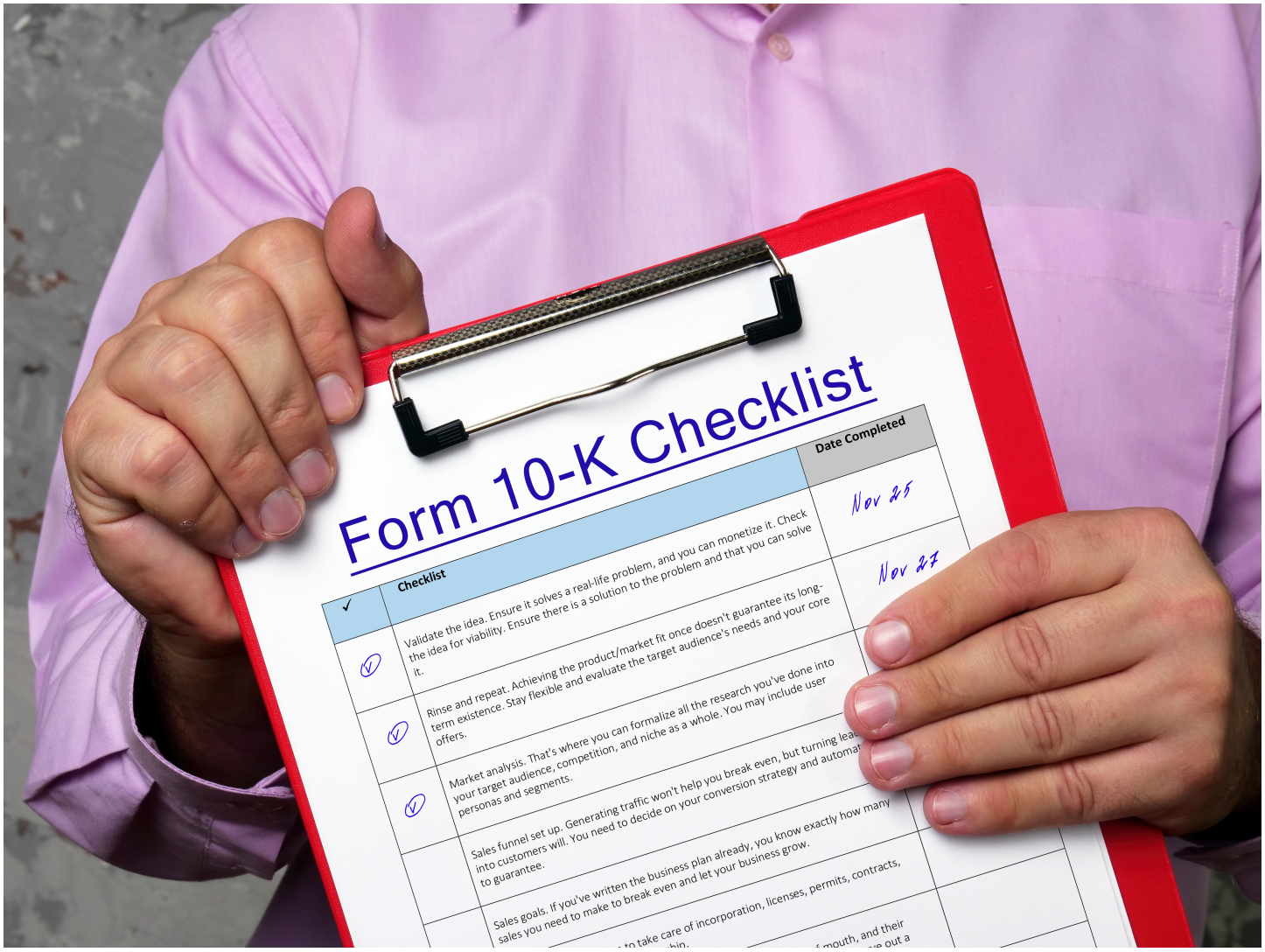
On the surface, the new SEC rules appear to be directed squarely at requiring boards to understand and actively manage cyber risk. The proposed amendments require public companies to report material cybersecurity incidents, and to periodically provide updates on previous incidents and information on the company’s policies and procedures to identify and manage cyber risks. The 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 it.

By requiring current and periodic reporting via Forms 10-K, 10-Q, or 8-K, as well as disclosure in proxy statements, the SEC is making plain its desire for the leadership of public companies to not only understand these risks but, perhaps more relevantly, to inform their investors and prospective investors about such risks.

> The SEC is making plain its desire for the leadership of public companies to not only understand these risks but, perhaps more relevantly, to inform their investors and prospective investors about such risks.

When a company realizes it has experienced a material cybersecurity event, it will have four business days to file a Form 8-K describing the incident. The Form 8-K must also report when the incident was discovered and if it was resolved, describe the nature and breadth of the incident, detail whether data has been compromised, and explain how it will impact the company's operations.

The proposed rules would require public companies to describe cybersecurity programs in some detail in their 10-K, including descriptions of their protocols, the names and expertise of board members who are responsible for cybersecurity oversight, and to report previous incidents and how they responded to them. They will also need to describe what they see as cyber risks they are currently facing and how they plan to respond to incidents in the future.



The proposed rules would require public companies to describe cybersecurity programs in some detail on their 10-K. Yuriy K / *Shutterstock.com*

Under these requirements, companies may end up not only disclosing information that may be of concern to investors as they look for possible regulatory violations and disruption to operations, but also exposing technical vulnerabilities and inadvertently putting a company at risk for further attacks.

Technical vulnerabilities and inadvertently putting a company at risk for further attacks.

Are the rules too prescriptive or too broad?

Whether or not all these rules will actually make companies — and, therefore, their customers — safer is a matter of debate. The sole commissioner to vote against the proposed rules wrote in her dissenting statement that the rules "look … 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."

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 policy or program. For instance, the proposed changes 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.

The form further requires reporting on management's expertise in assessing and managing cyber risk but does not specify what level or manner of expertise management should have. It could be argued that, by requiring a company to report on things like this "expertise," the SEC is expecting that investors will demand more companies have some reasonable measure of it in place — but this is clearly far from the imposition of a substantive standard.

Further, the SEC is concerned with investors, not with technology *per se* in that the threshold for material disclosure in cybersecurity incidents would be the US Supreme Court's definition of "materiality" in a series of disclosure-related cases, beginning with *Industries, Inc. v. Northway, Inc.*, as "a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision.

It is unclear if the average shareholder — or even a sophisticated shareholder — has a grasp of what constitutes an important cybersecurity issue for today's modern, global business enterprises. And, the technological threats, as well as the best means of safeguarding 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. Meanwhile, boards are already incentivized by market pressures to minimize or not report events that may be on the threshold of materiality since the reputational risks of a major cybersecurity event can be significant.

Litigation threats to boards

Separately from the SEC's proposed rules, a board's duty to understand and manage cyber risk has

been articulated in the now-famous Caremark standard. The Delaware Court of Chancery, in its landmark 1996 decision *In Re Caremark*, said for a board to avoid liability directors must act in good faith and be "reasonably informed" about the corporation.

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. To fail this test, however, a very high (or perhaps, very low) bar must be met: 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 tough standard. Until 2019 there were no cases brought in Delaware alleging a failure of its standard that survived beyond a motion to dismiss. Since Marchand v. Barnhill, however, Delaware courts have seemed more inclined to allow such claims to proceed, and cybersecurity issues have become a more prominent part of them. *Marchand* concerned a listeria outbreak at an ice-cream manufacturer and the Court held that the board's failure to implement a system to monitor food safety was a failure of the *Caremark* standard, especially since the defendant's sole business was food production. Notably, it also held that mere compliance with US Food and Drug Administration (FDA) standards was insufficient evidence of the necessary level of oversight.

> Mere compliance with US Food and Drug Administration (FDA) standards was insufficient evidence of the necessary level of oversight.

In Firemen's Ret*irement* Sy*stem* of St. Louis v. Sorenson, 2021, 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. 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." The court, however, found that the Marriott board had 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. The case settled out of court, but not until after the court had denied the motion to dismiss the *Caremark* claim.

The court in Sorenson*,* interestingly, 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 all sectors," and further stating that "as the legal and regulatory risks become manifest, corporate governance must evolve to address them. The … harms present by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place.

It seems likely that, at some point, someone will attempt to link compliance with the proposed SEC rules, if adopted, to the *Caremark* standard. *Marchand* may offer some guidance, such as where compliance with federal regulations was rejected as sufficient to pass the *Caremark* test. However, as discussed, previously, the proposed rules simply require boards to report on the existing programs and incidents, and having a "reasonable information and reporting system" would seem to be easy to report. The lack of detail on the substance of such programs, however, may render them significantly less potent at actually preventing cyberattacks.

> The lack of detail on the substance of such programs, however, may render them significantly less potent at actually preventing cyberattacks.

The SEC shows its teeth

Apart from, but adjacent to, cybersecurity, the SEC has recently shown it can take a hard line on compliance failures. In September 2022, it announced fines totaling more than US$1.1 billion against 11 financial services firms for "widespread and longstanding failures" to follow rules regarding the supervision and preservation of electronic communications. And they levied US$200 million against JPMorgan Chase & Co., the biggest US bank, for the same failures.

Part of the original US Securities and Exchange Act of 1934, firms have been required to monitor and preserve communications that relate to their "business as such." The SEC relies on these preserved communications, naturally, for the heart of any of its enforcement actions.

As the definition and scope of business communication has evolved from email to social media to unified communication tools like WebEx, Zoom, Slack, and Microsoft Teams that are the backbone of a distributed workforce, so have the ways in which financial institutions have complied (or failed to comply) with these rules. Email was the first massive shift; lately, however, mobile messaging, SMS, chat, and consumer applications like WhatsApp have become the source of the SEC's ire.

WhatsApp is an example of a mobile messaging app that is sometimes used for workplace communication, which presents preservation concerns to the SEC. PixieMe / *Shutterstock.com*

> Mobile messaging, SMS, chat, and consumer applications like WhatsApp have become the source of the SEC's ire.

The SEC stated in its press release that "from January 2018 through September 2021, the firms' employees routinely communicated about business matters using text message applications on their personal devices." As remote and hybrid work have accelerated the use of non-company supplied communications, and more and more employees — including senior management, as specifically called out by the SEC at some banks — use personal devices for work communication, the SEC's anxiety about the preservation of communication has clearly grown. While next-generation technological solutions to these problems exist in the marketplace, global financial institutions are not always able to stay at the cutting edge of adoption of such solutions, much like with technological cybersecurity safeguards.

Along with the SEC fines, the US Commodity Futures Trading Commission chimed in with just over US$700 million of its own fines, bringing the total to an eye-opening US$2 billion dollars. While not directed specifically at public company boards, these fines are without a doubt resonating at the highest levels of these institutions, both for their size and for their specificity in noting a failure at the highest levels to essentially enforce technological solutions to compliance issues.

What will actually make companies — and their customers — 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 entirely 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 (as in *Marchand*). 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.

> 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.

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.

There are, of course, other regulatory bodies which seek to force companies to improve their cybersecurity practices. The US 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. One recent proposed settlement even made headlines for singling out the CEO of a private company which had suffered a breach. The US Cybersecurity and Infrastructure Security Agency, which is a part of the US Department of Homeland Security, was established to better prepare the federal government and the United States against cyberthreats, but it does not have enforcement capabilities. Various US 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.

In-house counsel and compliance professionals will no doubt face questions from their managers and boards on how best to respond to the proposed rules and the increase in SEC fines for other data compliance issues. It's crucial that legal professionals understand what their compliance teams are worried about, and that both groups have as deep an understanding of the technological challenges and threats as possible.

> It's crucial that legal professionals understand what their compliance teams are worried about, and that both groups have as deep an understanding of the technological challenges and threats as possible.

Most public companies have a dedicated information security function at this point. In-house counsel need to make sure they meet regularly with their organization's information security leadership. It's also crucial to understand the difference between complying with data privacy regulations — which most lawyers today understand is crucial — and having truly good cybersecurity.

The latter may help with the former, but the two should not be conflated. Unfortunately, many outside

law firms lump the two together within practice groups (or tie cybersecurity to intellectual property or tech transactions practices). Some may have practitioners who are excellent at data privacy (and perhaps responding to security incidents after the fact) without being able to offer much counsel on the legal aspects of good cybersecurity.

Much more than a compliance issue, cybersecurity is also a critical risk-management issue for protecting companies from attacks and the associated fallout.

Legal departments need to be able to both guide their boards on the importance of cybersecurity compliance *and* support their information security teams on project prioritization across multiple levels of the company. They should also be savvy in their choice of outside counsel. Companies need expert advice on both data privacy and major commercial technology purchases, while also needing to understand privacy regulations, the SEC and other regulatory bodies, and the evolving technology landscape.

If the SEC's new rules are adopted, at some point 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 the SEC 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 the US 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.

The authors thank Madeline Maersk-Moller for contributing to this article. Maersk-Moller is a 2024 juris doctor candidate at the University of Colorado Law School.

J.D. Bridges

Senior Technology Counsel

Theta Lake

J. D. Bridges is senior technology counsel at Theta Lake, a startup focused on ensuring security and compliance for modern collaboration platforms using patented artificial intelligence (AI), machine learning, and natural language processing (NLP), and which is backed by investors such as Lightspeed Venture Partners, Battery Ventures, Cisco, Salesforce, and Zoom. Before joining Theta Lake, J. D. was an associate in the global corporate practice at Squire Patton Boggs, where he assisted in mergers and acquisitions, corporate governance matters, commercial technology transactions, and advised companies ranging from startups to Fortune 100 firms on matters of technology and cybersecurity. He has also served in-house at IT solutions and cybersecurity

providers.

Daniel G. Berick

Partner

Squire Patton Boggs

Daniel G. Berick is a partner in the Global Corporate Practice of Squire Patton Boggs and served for many years as its Americas Chair. He focuses his practice on mergers and acquisitions, securities law, corporate finance, and corporate transactional matters. He counsels public and privately held companies in cross-border and domestic mergers, acquisitions and dispositions; the issuance of equity and debt securities; securities law compliance; and general corporate matters. He regularly advises private equity and

venture capital firms and family offices in connection with portfolio company investments, acquisitions and dispositions, fund formation and structuring, and securities and corporate law matters.

Berick has been recognized by *Chambers USA*, *Legal 500,* and *Best Lawyers in America*, and has been listed in *IFLR1000* Elite Dealmakers. He received his juris doctor from University of Chicago and his bachelor’s degree from Columbia University.