Shaping Your Board For Cybersecurity

by Jay W. Lorsch, John Howard and Antony Kim

Directors have heard plenty about company cybersecurity dangers and duties of late, but precious little on how to manage digital defense at the board level. Below, three noted names in governance legal duties lay out a blueprint for assessing your company's cyber exposures, and crafting a board committee structure that ensures solid oversight.

Cybersecurity is an embedded risk that represents an increasing and evolving threat to all businesses. Attackers range from well-financed, state-sponsored organizations, to criminal syndicates, to lone hackers working with little more than a laptop. Across industries and geographies, companies are besieged by the threats of these skilled and persistent threat actors. Experts at misdirection and obfuscation, attackers constantly shift tactics and tools to avoid detection and prolong their opportunities to exploit weakness.

This article offers insights into why the board of directors must "own" cybersecurity as a top enterprise risk management issue. We examine frameworks and information flows that can help the board understand cybersecurity programs, and suggest practical strategies to help boards structure themselves to address cybersecurity risk effectively.

While a new risk, cybersecurity falls squarely within traditional director oversight duties. Boards are expected to view cybersecurity as they do all other risks.

As a primary driver of business value, technology innovations have transformed almost every business strategy and process. However, the rewards technology brings also come with new risks. Cybersecurity risks can be hard to quantify because many companies have stitched together multiple information systems and data bases, making it difficult for companies themselves to understand the full extent of their vulnerabilities.

Compounding this problem, companies can be exposed to breaches within their own systems, both from external threats and malicious insiders, or through suppliers or vendors who fail to have appropriate information security safeguards. The stark reality is that unauthorized access to a network or database is, quite literally, a click away.

While a new risk, cybersecurity falls squarely within traditional director oversight duties. Board members generally have fiduciary duties to act in good faith, and with care and loyalty. Boards are expected to view cybersecurity risks as they do all other risks. Board members themselves do not manage risk by designing or executing mitigation programs. As with other potential threats or vulnerabilities, boards must engage in high-level *oversight* of systems, controls and management activities that assess and address risk.

Given the increasing expectations that boards will be both strategic advisors and monitors of management, and the time demands on corporate directors, not all "governance" must take place at the "full" board level. State corporate law generally permits boards to delegate broad powers and authorities to committees.

In complex or technical areas, including cybersecurity, directors do not have to be expert themselves. Instead, they may rely on external experts as long as the specialist was selected with reasonable care, and opines on matters within his or her competence. Directors may also rely in good faith on information, opinions, and reports presented by board committees and management.

Jay W. Lorsch *is a professor at Harvard Business School.* **John Howard** *is senior vice president and general counsel for W.W. Grainger, Inc.* **Antony Kim** *is a partner with Orrick, Herrington & Sutcliffe LLP.*

Boards may not abdicate key decision-making responsibilities to either an outside expert or management, but reasonable and appropriately documented reliance is protected under Delaware standards.

Directors should take some comfort that the Delaware liability standard in shareholder derivative actions is quite high. Yet state precedents, such as the *Caremark* and *Stone* decisions, make clear that directors cannot simply ignore their risk oversight responsibilities. Fulfilling these responsibilities is important particularly for cybersecurity due to the potential severity that breaches can have on the company's performance and value, including its brand and reputational assets.

Shareholders are increasingly focused on holding directors accountable for cybersecurity. The strong legal presumption in favor of directors has not deterred the plaintiffs' bar from bringing cybersecurity-related claims that seek to hold boards either directly or individually accountable for data breaches.

In lawsuits filed after large breaches announced by Target (2014), Wyndham Hotels (2014), Home Depot (2015), Wendy's (2016), Yahoo! (2017) and Equifax (2017), shareholders blamed directors for alleged cybersecurity failings.

The Home Depot cyber-breach settlement required the board itself to assume day-to-day digital oversight responsibilities for the company.

These lawsuits assert that board decisions were ill-advised, misinformed, and/or negligent, that directors failed to address reasonably known cyber threats, or that they made false and misleading statements in describing the breaches. Specific allegations include that the board failed to implement and monitor effective cybersecurity programs; the board recklessly ignored warnings and red flags; that there were inadequate controls and procedures to protect personal and financial information; and that the company did not give timely notice of the breach.

These cases have been resolved both through financial payments and agreements to improve cybersecurity programs. For example, the settlement agreement for the payment card breach in Home Depot included "corporate governance reforms," where the Home Depot board was required to:

- Monitor and assess key indicators that on the computer network could be compromised.
- Maintain a "dark web" mining service to search for confidential Home Depot information.
- Receive periodic reports from management regarding the amount of the company's IT budget and the percentage spent on cybersecurity measures.
- Maintain an Incident Response Team and an Incident Response Plan to address crises or disasters.
- Implement an executive-level "Data Security and Privacy Governance Committee."

What is remarkable in this settlement is who is responsible for executing the tasks. The settlement agreement required the Home Depot board itself to assume these responsibilities. Placing this day-to-day role squarely on the board goes beyond the traditional corporate oversight and governance responsibilities for directors.

Regulators are also expanding the board's accountability for cyber oversight. Securities and Exchange Commission guidance now makes explicit that the cyber-related roles and activities of the board are materially important to the market and investors. The SEC's new guidance underscores that cybersecurity risks and incidents can be material, nonpublic information. Further, the SEC's guidance also stresses the importance of disclosures regarding how the board addresses cybersecurity risk.

The inherent complexity and connectivity of information systems requires an enterprise-wide approach to cybersecurity. Throughout a company, this involves every department and discipline: technical players from IT and information security, risk mitigation experts, internal audit, legal, investor relations and communications, and operational professionals from engineering, customer service, business continuity, and human resources.

In companies that have mature approaches, management sets the strategy, and has clearly defined roles and responsibilities. Even so, boards ultimately

must understand the cybersecurity program, determine whether it is effective and ensure that it is implemented.

Given the expectation that boards play an active role in cybersecurity, directors must consider which governance structures would be effective within the unique contexts of their business and industry. Boards must organize themselves so that cybersecurity receives appropriately informed attention and oversight.

There is very little specific guidance on board cyber oversight. The board has significant flexibility in how it organizes and executes this function.

While the board itself retains final oversight responsibility, much of the initial work can and should be done by board committees. Given the fluidity of the technological and threat landscape, plus already packed board meeting agendas, a committee can be leveraged for more knowledgeable monitoring and informed oversight. The committee can support the full board with periodic information updates and periodic briefings.

There is very little specific guidance on this topic. The board has significant flexibility in how it organizes and executes its risk oversight functions. Currently, there are no regulatory mandates that require a board to create a separate cybersecurity committee, or to disclose whether one has been established.

When faced with this range of flexibility, many boards seek guidance by asking "what is everyone else doing." At present, there does not appear to be a single, best practice. We note, however, that forming a separate cybersecurity committee is not a widespread practice. In fact, the vast majority of public company boards discharge their cybersecurity oversight responsibilities through committees that have other responsibilities.

According to the 2017 Spencer Stuart U.S. board Index, which samples the practices of the S&P 500, most boards (69 percent) assign cybersecurity responsibility to a committee, with only 26 percent retaining oversight at the board level. Of those assigning cybersecurity responsibilities to a committee, audit committees had oversight in the majority of the respondents (57 percent), and risk or technology committees were sometimes mentioned (11 percent).

These results are generally consistent with other surveys. Based on our review of public filings over the last 12 months by S&P 500 companies, it appears that less than two percent of the S&P 500 has adopted a separate cybersecurity committee.

The absence of cybersecurity committees may be due to a variety of reasons. First, perhaps some companies are engaging in the wishful thinking that cybersecurity is just an issue *du jour* that will pass. Second, and more realistically, many other companies see cybersecurity as an extension of existing risk management programs. Since cybersecurity is a multi-disciplinary issue with cross-functional impacts, many companies find it easier to assign oversight to an existing committee with jurisdiction over the other various touch points. A third reason is equally pragmatic: the limits on a board's time. A new board committee would increase the burden on time, resources, and administration on an already crowded governance calendar.

A separate reason could be that many companies lack directors with deep understanding of cybersecurity systems, programs, and risks. According to PwC's *2017 Annual Corporate Director Survey*, only 16 percent of companies reported having enough cybersecurity expertise on their boards.

Indeed, "digital directors" with expertise in cybersecurity matters, technology, digital strategy, or digital or social media are a relatively small subset of corporate executives. As such, they are in high demand for board positions. Having tech-savvy directors can improve a board's ability to make more informed strategic decisions, as well as to understand and address cybersecurity risks.

Even when the board does not have a "digital director," there are several approaches for members to gain fluency in cybersecurity needed to effectively discharge their oversight function. Boards can retain outside experts not only to evaluate the company's cybersecurity programs, but also to increase their

understanding. Further, several organizations, like the National Association of Corporate Directors, provide board education programming intended to sharpen director skills in cybersecurity and other areas.

Appropriate board committee structure can only be determined with a full understanding of the company's cyber risks and systems.

There is no one-size-fits-all answer when it comes to the issue of "who" and "where" to lodge board oversight responsibility for cybersecurity. The question of appropriate board committee structure can only be answered when there is a full understanding of the company's risks and systems. Without this background, the committee's work, as well as the board's ability to fulfill its oversight responsibilities, is unlikely to be effective.

We suggest that boards begin with an ad hoc cybersecurity advisory committee assigned to determine a baseline of the company's cybersecurity policies and practices, and provide recommendations to the board on various topics. These include:

- Organizing principles for cybersecurity oversight.
- Selecting an appropriate risk management framework.
- Monitoring cyber risk management.
- Implementation/board oversight.

☐ ***Organizing principles for cybersecurity.*** The primary focus of a cybersecurity program should be to insure that cyber risks are identified so that they can be appropriately considered in formulating corporate strategy. This means recognizing the risks and then determining how they can be avoided, mitigated, transferred or shared, and, where appropriate, disclosed.

In developing organizing principles, it is important to establish a baseline of knowledge across the company's cybersecurity readiness so that management teams and boards have answers to key questions:

- What is the company trying to protect—what are its most critical assets? What cybersecurity risks are most like to be material to the company?
- What is the company's risk tolerance or appetite in cybersecurity matters? Is it appropriately aligned to the company's business, strategy and objectives?
- Is the company's current cybersecurity framework appropriate for our business?
- What is the company's current state of readiness—what are the company's most critical weaknesses?
- Does the company have the right people, process and technology to understand and effectively manage risks?
- Is the company allocating the right resources to cybersecurity risk management?
- How does the company compare to other public companies in its industry?
- Are the company's processes appropriately designed for timely identification, response and regulatory reporting?

A cybersecurity risk management program should be tied to a well-defined framework.

☐ ***Selecting an appropriate cybersecurity framework.*** Rather than treat cybersecurity solely as an IT issue, view it as part of a company's overall enterprise risk management (ERM) process. While each company will have to define for itself what cybersecurity risk means, one definition might be:

> *"A breach to the confidentiality, integrity and availability of systems and data that can impact the company's ability to conduct business or create an environment of decreased trust or compliance."*

To help gauge relative effectiveness, a cybersecurity risk management program should be tied to a well-defined framework. One commonly used risk management framework is the U.S. Department of Commerce's National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* (NIST). While initially targeted at entities vital to national and economic security, the framework has proven flexible enough for application across diverse industries and sectors.

The NIST framework is divided into five critical functions:

▫ *Identify.* Understanding the business context and critical functions, and the related cybersecurity risks so that the organization can focus and prioritize its risk efforts.

▫ *Protect.* Safeguards to ensure delivery of critical services to limit or contain the impact of a potential cybersecurity event.

▫ *Detect.* Identify whether or when there has been a cybersecurity event.

▫ *Respond.* Actions taken to address a detected cybersecurity incident.

▫ *Recover.* Maintain a plan to restore capabilities or services that were impaired due to a cybersecurity incident.

While other frameworks and standards might be more suitable for a company, depending on its industry or regulatory regimes, NIST is widely recognized as a useful tool for assessing a company's cybersecurity program and enabling a risk-based approach to improving maturity and effectiveness.

The NIST framework also has the added benefit of broad acceptance by regulators. For example, the SEC has embraced NIST as among best practices for publicly traded companies and the Federal Trade Commission has publicly stated that NIST aligns with the agency's approach in enforcement.

☐ ***Monitoring of cyber risk management.*** The ad hoc cybersecurity advisory committee can help make sure that the board has the information it needs to assess and monitor the company's cybersecurity program. Obviously, it is very important that management play an initial role in identifying appropriate metrics. Equally obvious is that this information must be provided in context to the board in an understandable form that quickly conveys areas of focus and status.

Some key elements of a "cybersecurity information package" for the board include:

▫ *New threats and developments.* Provides a quarterly snapshot of the landscape, including new or newly emerging threats and other developments, including new laws or regulations.

▫ *Actions and incidents.* Identifies significant events that have required action, provide a remediation plan and status, and quantify the business impact.

▫ *Current cyber program assessments and actions.* Compiles assessments, reviews and audits (both internal and external) that have been conducted on the company's cybersecurity systems, including timeline for completion.

▫ *IT control status.* Identifies any control gaps and the company's remediation efforts by business unit and type of assessment.

▫ *Risk profile.* Lists the top cyber information risks identified by management.

▫ *Planned projects and budgets.* Describe efforts and initiatives on the horizon, timelines and milestones, and resource allocation needs.

▫ *Cyber dashboard.* Presents a high-level roll-up of metrics showing the company's ongoing cybersecurity efforts segmented consistent with the company's cybersecurity framework.

The ad hoc cybersecurity advisory committee should also recommend a reporting cadence appropriate for the company's exposures and risk appetite.

☐ ***Board oversight.*** It bears repeating that as it relates to cybersecurity, there are no legal requirements for any particular governance structure. Boards have inherent and broad flexibility in deciding whether a committee would be useful. As a board begins its analysis, it should be mindful that cybersecurity, while involving complex issues of technology, is ultimately a risk management issue. This "risk lens" can be helpful in determining governance structures, particularly in weighing cybersecurity risks against other risks and issues.

An appropriate governance structure is a function of the company and industry risk, risk tolerance/appetite, the degree of specific threats, the company's maturity in addressing risks (including cybersecurity), and board resources, including director expertise and time.

Answering the questions in the box on the following page will help shape your structure. The more "Yes" answers, the greater the likelihood that the company may benefit from a board committee focused on cybersecurity issues.

No matter where cybersecurity is assigned, directors need accurate, complete, timely, and contextual information on the company's cyber risk. To enable the

How To Structure Cyber Oversight?
Begin With These Questions

Question	Yes	No
1. Does the company operate in a high risk industry?		
2. Does the company have a high public profile?		
3. Is the company highly regulated or does it deal with highly-regulated customers or business partners?		
4. Has the company suffered a major cyber-attack or data breach that significantly affected the company's brand/reputation, stock price, or operations?		
5. Do the company's existing board committees lack the time, resources and expertise to address cybersecurity issues?		
6. Are the company's business and operations sufficiently complex that the critical role of an existing board committee would be significantly impacted should it be assigned cybersecurity responsibilities?		

board to understand the context of any cybersecurity threats and risks, and to assess the company's efforts to address them, management should routinely provide an "information package" that clearly and succinctly communicates relevant material.

Effective cybersecurity risk reports communicate in a meaningful and explicit manner whether the right investments are being made.

There needs to be agreement between the board and management on what information is included. It is very easy to provide a multitude of technical metrics and measures, all of which may still fail to give the board a complete or accurate view. Effective cybersecurity risk reports communicate in a meaningful and explicit manner whether the right investments are being made, and the status of their implementation.

Boards and management teams undoubtedly will want to include metrics and other information tailored for their individual companies. Both accuracy and efficiency will be improved if the material is derived from the reports that management actually uses to administer the company's cybersecurity program. This will keep the information provided to the board germane to how the company manages cyber security on a day-to-day basis.

Of all the risks confronting companies today, cybersecurity is certainly the most technical and rapidly-evolving. The opportunity and challenge in organizing a board to effectively discharge its cybersecurity oversight lies in the absence of a single "right way" to do it.

Thankfully, the board's role is not to decipher the mysteries of the dark web or explain the coding behind encryption technology. Rather, the board's responsibility is to understand the cyber risks facing the company, ensure that management has an appropriate cybersecurity program, and evaluate whether the program is functioning effectively.

Cybersecurity risk is here to stay. With the proper framework, structure, cadence, and reporting, boards can do more than discharge their fiduciary responsibilities for cybersecurity oversight. They can also serve as a strategic asset and create a competitive advantage by the integrity of their information systems and reputational certainty of "getting cybersecurity right." ■

paloalto NETWORKS®

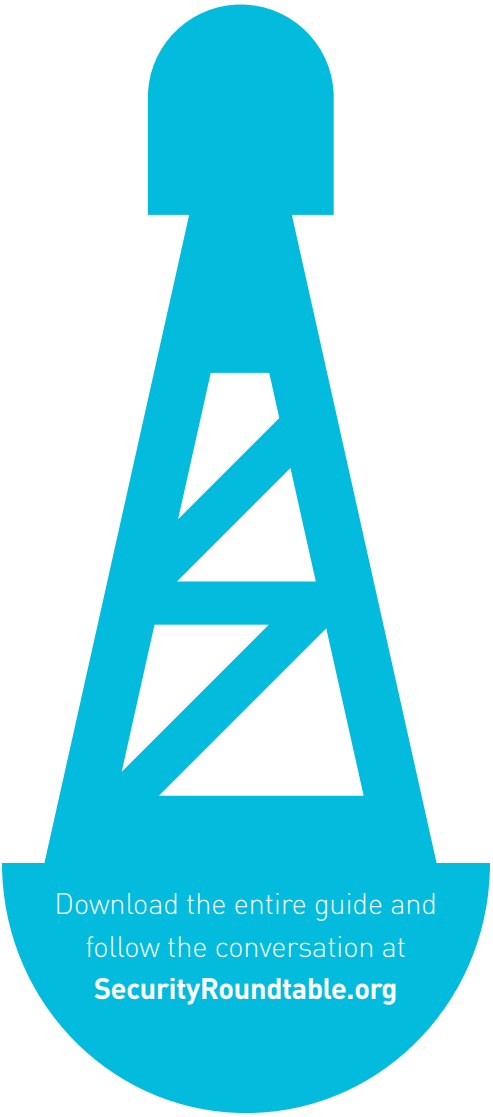
NYSE

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

Georgia Tech Institute for Information Security & Privacy

INTERNET SECURITY ALLIANCE


Download the entire guide and
follow the conversation at
SecurityRoundtable.org

8

The risks to boards of directors and board member obligations

Orrick, Herrington & Sutcliffe LLP – Antony Kim, Partner; Aravind Swaminathan, Partner; and Daniel Dunne, Partner

As cyberattacks and data breaches continue to accelerate in number and frequency, boards of directors are focusing increasingly on the oversight and management of corporate cybersecurity risks. Directors are not the only ones. An array of federal and state enforcement agencies and regulators, most notably the Department of Justice (DOJ), Department of Homeland Security (DHS), Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), and state Attorneys General, among others, identify board involvement in enterprise-wide cybersecurity risk management as a crucial factor in companies' ability to appropriately establish priorities, facilitate adequate resource allocation, and effectively respond to cyberthreats and incidents. As SEC Commissioner Luis A. Aguilar recently noted, "Boards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril."[1] Indeed, even apart from the regulators, aggressive plaintiffs' lawyers, and activist shareholders are similarly demanding that boards be held accountable for cybersecurity. Shareholder derivative actions and activist investor campaigns to oust directors are becoming the norm in high-profile security breaches.

Directors have clearly gotten the message. A survey by the NYSE Governance Services (in partnership with a leading cybersecurity firm) found that cybersecurity is discussed at 80% of all board meetings. However, the same survey revealed that only 34% of boards are confident about their respective companies' ability to defend themselves against a cyberattack. More troubling, a June 2015 study by the National Association of Corporate Directors found that only 11% of respondents believed their boards possessed a high level of understanding of the risks associated with cybersecurity.[2] This is a difficult position to be in: aware of the magnitude of the risks at hand but struggling

to understand and find solutions to address and mitigate them.

In this chapter, we explore the legal obligations of boards of directors, the risks that boards face in the current cybersecurity landscape, and strategies that boards may consider in mitigating that risk to strengthen the corporation and their standing as dutiful directors.

I. Obligations of Board Members

The term "cybersecurity" generally refers to the technical, physical, administrative, and organizational safeguards that a corporation implements to protect, among other things, "personal information,"[3] trade secrets and other intellectual property, the network and associated assets, or as applicable, "critical infrastructure."[4] This definition alone should leave no doubt that a board of directors' role in protecting the corporation's "crown jewels" is essential to maximizing the interests of the corporation's shareholders.

Generally, directors owe their corporation fiduciary duties of good faith, care, and loyalty, as well as a duty to avoid corporate waste.[3] The specific contours of these duties are controlled by the laws of the state in which the company is incorporated, but the basic principles apply broadly across most jurisdictions (with Delaware corporations law often leading the way). More specifically, directors are obligated to discharge their duties in good faith, with the care an ordinarily prudent person would exercise in the conduct of his or her own business under similar circumstances, and in a manner that the director reasonably believes to be in the best interests of the corporation. To encourage individuals to serve as directors and to free corporate decision making from judicial second-guessing, courts apply the "business judgment rule." In short, courts presume that directors have acted in good faith and with reasonable care after obtaining all material information, unless proved otherwise; a powerful presumption that is difficult for plaintiffs to overcome, and has led to dismissal of many legal challenges to board action or inaction. To maximize their personal protection, directors must ensure that, if the unthinkable happens and their corporation falls victim to a cybersecurity disaster, they have already taken the steps necessary to preserve this critical defense to personal liability.

In the realm of cybersecurity, the board of directors has "risk oversight" responsibility: the board does not itself *manage* cybersecurity risks; instead, the board oversees the corporate systems that ensure that management is doing so effectively. Generally, directors will be protected by the business judgment rule and will not be liable for a failure of oversight unless there is a "sustained or systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists." This is known as the *Caremark* test,[5] and there are two recognized ways to fall short: first, the directors intentionally and entirely fail to put *any* reporting and control system in place; or second, if there is a reporting and control system, the directors refuse to monitor it or fail to act on warnings they receive from the system.

The risk that directors will face personal liability is especially high where the board has not engaged in *any* oversight of their corporations' cybersecurity risk. This is a rare case, but other risks are more prevalent. For example, a director may fail to exercise due care if he or she makes a decision to discontinue funding an IT security project without getting any briefing about current cyberthreats the corporation is facing, or worse, after being advised that termination of the project may expose the company to serious threats. If an entirely uninformed or reckless decision to de-fund renders the corporation vulnerable to known or anticipated risks that lead to a breach, the members of the board of directors could be individually liable for breaching their *Caremark* duties.

II. The Personal Liability Risk to Directors

Boards of directors face increasing litigation risk in connection with their responsibilities

for cybersecurity oversight, particularly in the form of shareholder derivative litigation, where shareholders sue for breaches of directors' fiduciary duties to the corporation. The rise in shareholder derivative suits coincides with a 2013 Supreme Court decision limiting the viability of class actions that fail to allege a nonspeculative theory of consumer injury resulting from identity theft.[6] Because of a lack of success in consumer class actions, plaintiffs' lawyers have been pivoting to shareholder derivative litigation as another opportunity to profit from massive data breaches.

In the last five years, plaintiffs' lawyers have initiated shareholder derivative litigation against the directors of four corporations that suffered prominent data breaches: Target Corporation, Wyndham Worldwide Corporation, TJX Companies, Inc., and Heartland Payment Systems, Inc. Target, Heartland, and TJX each were the victims of significant cyberattacks that resulted in the theft of approximately 110, 130, and 45 million credit cards, respectively. The Wyndham matter, on the other hand, involved the theft of only approximately 600,000 customer records; however, unlike the other three companies, it was Wyndham's *third* data breach in approximately 24 months that got the company and its directors in hot water. The signs point to Home Depot, Inc., being next in line. A Home Depot shareholder recently brought suit in Delaware seeking to inspect certain corporate books and records. A "books and records demand" is a common predicate for a shareholder derivative action, and this particular shareholder has already indicated that the purpose of her request is to determine whether Home Depot's management breached fiduciary duties by failing to adequately secure payment information on its data systems, allegedly leading to the exposure of up to 56 million customers' payment card information.

Although there is some variation in the derivative claims brought to date, most have focused on two allegations: that the directors breached their fiduciary duties by making a decision that was ill-advised or negligent, or by failing to act in the face of a reasonably known cybersecurity threat. Recent cases have included allegations that directors:

- failed to implement and monitor an effective cybersecurity program;
- failed to protect company assets and business by recklessly disregarding cyberattack risks and ignoring red flags;
- failed to implement and maintain internal controls to protect customers' or employees' personal or financial information;
- failed to take reasonable steps to timely notify individuals that the company's information security system had been breached;
- caused or allowed the company to disseminate materially false and misleading statements to shareholders (in some instances, in company filings).

Board members may not be protected from liability by the exculpation clauses in their corporate charters. Although virtually all corporate charters exculpate board members from personal liability to the fullest extent of the law, Delaware law, for example, prohibits exculpation for breaches of the duty of loyalty, or breaches of the duty of good faith involving "intentional misconduct" or "knowing violations of law." As a result, because the Delaware Supreme Court has characterized a *Caremark* violation as a breach of the duty of loyalty,[7] exculpation of directors for *Caremark* breaches may be prohibited. In addition, with the myriad of federal and state laws that touch on privacy and security, directors may also lose their immunity based on "knowing violations of law." Given the nature of shareholder allegations in derivative litigation, these are important considerations, and importantly, vary depending on the state of incorporation.

Directors should also be mindful of standard securities fraud claims that can be brought against companies in the wake of a data breach. Securities laws generally prohibit public companies from making material

statements of fact that are false or misleading. As companies are being asked more and more questions about data collection and protection practices, directors (and officers) should be careful about statements that are made regarding the company's cybersecurity posture and should focus on tailoring cybersecurity-related risk disclosures in SEC filings to address the specific threats that the company faces.

Cybersecurity disclosures are of keen interest to the SEC, among others. Very recently, the SEC warned companies to use care in making disclosures about data security and breaches and has launched inquiries to examine companies' practices in these areas. The SEC also has begun to demand that directors (and boards) take a more active role in cybersecurity risk oversight.

Litigation is not the only risk that directors face. Activist shareholders—who are also customers/clients of corporations—and proxy advisors are challenging the re-election of directors when they perceive that the board did not do enough to protect the corporation from a cyberattack. The most prominent example took place in connection with Target's data breach. In May 2014, just weeks after Target released its CEO, Institutional Shareholder Services (ISS), a leading proxy advisory firm, urged Target shareholders to seek ouster of seven of Target's ten directors for "not doing enough to ensure Target's systems were fortified against security threats" and for "failure to provide sufficient risk oversight" over cybersecurity.

Thoughtful, well-planned director involvement in cybersecurity oversight, as explained below, is a critical part of a comprehensive program, including indemnification and insurance, to protect directors against personal liability for breaches. Moreover, it can also assist in creating a compelling narrative that is important in brand and reputation management (as well as litigation defense) that the corporation acted responsibly and reasonably (or even more so) in the face of cybersecurity threats.

III. Protecting Boards of Directors

From a litigation perspective, boards of directors can best protect themselves from shareholder derivative claims accusing them of breaching their fiduciary duties by diligently overseeing the company's cybersecurity program and thereby laying the foundation for invoking the business judgment rule. Business judgment rule protection is strengthened by ensuring that board members receive periodic briefings on cybersecurity risk and have access to cyber experts whose expertise and experience the board members can rely on in making decisions about what to do (or not to do) to address cybersecurity risks. Most importantly, directors cannot recklessly ignore the information they receive, but must ensure that management is acting reasonably in response to reported information the board receives about risks and vulnerabilities.

Operationally, a board can exercise its oversight in a number of ways, including by (a) devoting board meeting time to presentations from management responsible for cybersecurity and discussions on the subject, to help the board become better acquainted with the company's cybersecurity posture and risk landscape; (b) directing management to implement a cybersecurity plan that incentivizes management to comply and holds it accountable for violations or non-compliance; (c) monitoring the effectiveness of such plan through internal and/or external controls; and (d) allocating adequate resources to address and remediate identified risks. Boards should invest effort in these actions, on a repeated and consistent basis, and make sure that these actions are clearly documented in board and committee packets, minutes, and reports.

(a) **Awareness.** Boards should consider appointing a chief information security officer (CISO), or similar officer, and meet regularly with that individual and other experts to understand the company's risk landscape, threat actors, and strategies to address

that risk. Appointing a CISO has an additional benefit. Reports suggest that companies that have a dedicated CISO detected more security incidents and reported lower average financial losses per incident.[8]

Boards should also task a committee or subcommittee with responsibility for cybersecurity oversight, and devote time to getting updates and reports on cybersecurity from the CISO on a periodic basis. As with audit committees and accountants, boards can improve oversight by recruiting a board member with aptitude for the technical issues that cybersecurity presents, and placing that individual on the committee/subcommittee tasked with responsibility for cybersecurity oversight. Cybersecurity presentations, however, need not be overly technical. Management should use established analytical risk frameworks, such as the National Institute for Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity," (usually referred to as the "NIST Cybersecurity Framework") to assess and measure the corporation's current cybersecurity posture. These kinds of frameworks are critical tools that have an important role in bridging the communication and expertise gaps between directors and information security professionals and can also help translate cybersecurity program maturity into metrics and relative relationship models that directors are accustomed to using to make informed decisions about risk. It is principally through their use that directors can become sufficiently informed to exercise good business judgment.

(b) **Plan implementation and enforcement.** Boards should require that management implement an enterprise-wide cybersecurity risk management plan and align management's incentives to meet those goals. Although the details of any cybersecurity risk management plan should differ from company to company, the CISO and management should prepare a plan that includes proactive cybersecurity assessments of the company's network and systems, builds employee awareness of cybersecurity risk and requires periodic training, manages engagements with third parties that are granted access to the company's network and information, builds an incident response plan, and conducts simulations or "tabletop" exercises to practice and refine that plan. The board should further consider incentivizing the CISO and management for company compliance with cybersecurity policies and procedures (e.g., bonus allocations for meeting certain benchmarks) and create mechanisms for holding them responsible for noncompliance.

(c) **Monitor compliance.** With an enterprise-wide cybersecurity risk management plan firmly in place, boards of directors should direct that management create internal and external controls to ensure compliance and adherence to that plan. Similar to internal financial controls, boards should direct management to test and certify compliance with cybersecurity policies and procedures. For example, assuming that management establishes a policy that software patches be installed within 30 days of release, management would conduct a patch audit, confirm that all patches have been implemented, and have the CISO certify the results. Alternatively, boards can also retain independent cybersecurity firms that could be engaged by the board to conduct an audit, or validate compliance with cybersecurity policies and procedures, just as they would validate financial results in a financial audit.

(d) **Adequate resource allocation.** With information in hand about what the

company's cybersecurity risks are, and an analysis of its current posture, boards should allocate adequate resources to address those risks so that management is appropriately armed and funded to protect the company.

As criminals continue to escalate the cyber-war, boards of directors will increasingly find themselves on the frontlines of regulatory, class plaintiff, and shareholder scrutiny. Directors are well-advised to proactively fulfill their risk oversight functions by driving senior management toward a well-developed and resilient cybersecurity program. In so doing, board members will not only better protect themselves against claims that they failed to discharge their fiduciary duties, but will strengthen their respective organizations' ability to detect, respond, and recover from cybersecurity crises.

Endnotes

1. SEC Commissioner Luis A. Aguilar, Remarks at the N.Y. Stock Exchange, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014).
2. Press Release, Nat'l Assoc. of Corp. Dir., Only 11% of Corporate Directors Say Boards Have High Level of Cyber-Risk Understanding (June 22, 2015) https://www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=15879.
3. Personal information is defined under a variety of federal and state laws, as well as industry guidelines, but is generally understood to refer to data that may be used to identify a person. For example, state breach notification laws in the U.S. define personal information, in general, as including first name (or first initial) and last name, in combination with any of the following: (a) social security number; (b) driver's license number or other government-issued identification; (c) financial or credit/debit account number plus any security code necessary to access the account; or (d) health or medical information.
4. Critical infrastructure refers to systems, assets, or services that are so critical that a cyberattack could cause serious harm to our way of life. Presidential Policy Directive 21 (PPD-21) identifies the following 16 critical infrastructure sectors: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation, waste, and wastewater. *See* Critical Infrastructure Sectors, Department of Homeland Security, *available at* http://www.dhs.gov/critical-infrastructure-sector.
5. For Delaware corporations, directors' compliance with their oversight function is analyzed under the test set out in *In re Caremark Int'l, Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).
6. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). Consistent with *Clapper*, most data breach consumer class actions have been dismissed for lack of "standing": the requirement that a plaintiff has suffered a cognizable injury as a result of the defendant's conduct. That has proven challenging for plaintiffs because consumers are generally indemnified by banks against fraudulent charges on stolen credit cards, and many courts have rejected generalized claims of injury in the form of emotional distress or exposure to heighted risk of ID theft or fraud.
7. *Stone v. Ritter,* 911 A.2d 362, 370 (Del. 2006).
8. Ponemon Inst., 2015 Cost of Data Breach Study: Global Analysis (May 2015), http://www-03.ibm.com/security/data-breach/.

Orrick, Herrington & Sutcliffe LLP

51 West 52nd Street
New York, New York 10019-6142
Tel +1 212 506 5000

ANTONY KIM

Partner
Email akim@orrick.com

Antony Kim is a partner in the Washington, DC, office of Orrick, Herrington & Sutcliffe and serves as Global Co-Chair of its Cybersecurity and Data Privacy practice. Mr. Kim represents clients in federal and state regulatory investigations, private actions, and crisis-response engagements across an array of cybersecurity, data privacy, sales and marketing, and consumer protection matters, on behalf of private and public companies.

ARAVIND SWAMINATHAN

Partner
Email aswaminathan@orrick.com

Aravind Swaminathan is a partner the Seattle office of Orrick Herrington & Sutcliffe LLP and serves as the Global Co-Chair of its Cybersecurity and Data Privacy practice. Mr. Swaminathan advises clients in proactive assessment and management of internal and external cybersecurity risks, breach incident response planning, and corporate governance responsibilities related to cybersecurity and has directed dozens of data breach investigations and cybersecurity incident response efforts, including incidents with national security implications. A former Cybercrime Hacking and Intellectual Property Section federal prosecutor, Mr. Swaminathan also represents companies and organizations facing cybersecurity and privacy-oriented class action litigation that can often follow a breach.

DANIEL DUNNE

Partner
Email ddunne@orrick.com

Dan Dunne, a partner in the Seattle office of Orrick, Herrington & Sutcliffe LLP, represents corporations, financial institutions, accountants, directors, and officers in complex litigation in federal and state courts. Mr. Dunne defends directors and officers in shareholder derivative suits, securities class actions, SEC, and other state and federal regulatory matters.

orrick
Trust Anchor

SEC Commissioners Provide Guidance on Cybersecurity Disclosures After Wave of Record Incidents

Editorial Board (https://blogs.orrick.com/trustanchor/author/editorialboard/)

Much has been written about the SEC's **interpretive guidance on cybersecurity disclosures** (https://www.sec.gov/news/press-release/2018-22), issued in late February, including **Commissioner Stein's statement** (https://www.sec.gov/news/public-statement/statement-stein-2018-02-21)that it *under*-delivers for investors, public companies, and the capital markets. As many **observers have noted** (https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21), the Commission largely repackaged the Division of Corporation Finance's prior **October 2011 guidance** (https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm). Further, by issuing interpretive guidance, rather than engaging in formal rulemaking, the SEC's pronouncement does not have the force and effect of law and is not accorded such weight in the adjudicatory process.[1]

From an overview perspective, the Commission's guidance simply reminds us that digital technologies can create enterprise risk; that the securities laws mandate disclosures of material risk; that disclosure controls and procedures are critical and more effective when directors and officers are involved; and that trading on material nonpublic information is prohibited. These are hardly new concepts. Indeed, the general nature of these pronouncements is the source of frustration for those seeking more specific and potentially proscriptive direction.[2]

The Commission, however, chose its topics and words carefully; and close analysis reveals valuable details and insights. Thus, in addition to summarizing what the guidance "says," we offer a closer look at what the guidance "means" in terms of immediate action items for publicly traded entities and practitioners.

What Is in the New 2018 Guidance?

Duty to Disclose. The Guidance indicates that including risk of cybersecurity incidents within corporate disclosures of risk factors—a practice that became commonplace after the 2011 guidance—is not enough. Instead, "[c]ompanies must provide timely and ongoing information in [] periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations."

In essence, the SEC's position is that companies cannot stay silent and have a duty to disclose material nonpublic information relating to cybersecurity risks and incidents.[3] This position is broader than established Supreme Court precedent, which provides that disclosure is mandated only if a company is trading on the information, a statement or omission would render a prior statement materially misleading, or disclosure is expressly required.

In the context of the duty to update and correct prior disclosures, the Guidance provides that a company cannot rely on an ongoing internal or external investigation of a cybersecurity incident to withhold information as that "would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." Moreover, companies "may have a duty to correct [a] prior disclosure that the company determines was untrue . . . or a duty to update [a] disclosure that becomes materially inaccurate after it is made."

The materiality of cybersecurity risks or incidents "depend[s] upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations." The Guidance indicates that materiality analysis for cybersecurity should include (1) remediation costs; (2) increased cybersecurity protection costs; (3) lost revenues; (4) litigation and legal risks; (5) increased insurance premiums; and (6) reputational damage, including potential negative impact on the company's stock price.

Disclosure Controls and Procedures. The Guidance stresses the importance of adopting and maintaining disclosure controls and procedures that will ensure relevant information about cybersecurity risks and incidents is timely processed and reported to appropriate personnel all the way up to senior management. Before an incident, companies should assess whether their disclosure controls and procedures will enable them to (1) identify cybersecurity risks and incidents; (2) assess and analyze the impact of such risks and incidents on the company operations, including on each reportable segment; and (3) evaluate the potential materiality of such risks and incidents. Additionally, policies should provide for open communications between technical experts and disclosure advisors regarding such risks and incidents. In making Sarbanes-Oxley Act 302 certifications per Exchange Act Rules 13a-14 and 15d-14 for quarterly and annual reports regarding the design and effectiveness of disclosure control and procedures, a company's principal executive officer and principal financial officer should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents. If cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize and report information required to be disclosed in SEC filings, management should consider whether disclosure controls and procedures are effective.

Special Emphasis on Service Providers. In multiple places throughout the guidance, the Commission mentions third-party "suppliers," "service providers," and "vendors" as critical to, among other things, enterprise risk, cyber incidents, and response and remediation costs. Thus, the guidance admonishes companies to think long and hard about service providers in providing contextual disclosures (e.g., "Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure.").

Public research confirms that vendor-attributed data breaches are exceedingly common. In one oft-cited study, Soha Systems found that **63 percent of data breaches may be directly or indirectly related to third-party access** (https://static1.squarespace.com/static/56b3cadb59827ecd82b02b43/t/5906176a893fc052557a0646/1493571436523/Soha_Systems_Third_Party_Advisory_Group_2016_IT_Survey_Report.pdf) by contractors and suppliers. Widespread migration to cloud services, and outsourcing more generally, portends even greater potential for risk exposure—particularly for entities engaged in financial services, health care, and other sectors that have experienced serious data breaches in recent years.

The foregoing makes clear that companies should consider how their disclosures might be affected by operational connectivity (and sometimes, integration) with various third parties. Where companies rely on third parties not only for operational support but also for security controls, careful thought should be given as to how risk is disclosed. Specifically, risk disclosures may need to account for the fact that failures in a critical vendor's security measures to protect against, identify, detect, or respond to major cyber events could materially impact the company itself.

Insider Trading Policies and Blackout Periods. The Guidance encourages companies to review their code of ethics and insider trading policies to assess whether they take into account cybersecurity incidents. Additionally, the Guidance indicates that it may be appropriate to implement a trading blackout period while the company investigates and assesses the significance of a cybersecurity incident. Implementing a blackout period following an incident and prior to disclosure could protect against insider trading and avoid the appearance of improper trading during this period.

Regulation FD and Selective Disclosure. The Guidance reminds companies that persons acting on behalf of a company should not selectively disclose material nonpublic information relating to cybersecurity risks and incidents to brokers, dealers, investment advisors, and other persons enumerated in Regulation FD before disclosing the same information to the public. Companies should adopt policies and procedures to avoid selective disclosure prohibited by Regulation FD, or ensure a Form 8-K disclosure is made where such information is provided to Regulation FD enumerated persons, which may occur when a company is required to provide notification to individuals under state data breach notification requirements or other regulatory requirements.

Risk Committee and Board Oversight. Disclosure in annual reports or proxy statements of the board of directors' role in risk oversight of a company pursuant to Item 407(h) of Regulation S-K should include a discussion of the nature of the board's role in overseeing the management of cybersecurity risks that are material to a company's business. In addition, disclosures on how the board engages with management on cybersecurity issues will allow investors to assess how a board of directors is discharging its risk oversight responsibility in cybersecurity matters.

What Should Companies Do to Comply With the New Guidance?

In light of the SEC's new Guidance on cybersecurity, companies should consider the following:

- Identify and scrutinize all prior disclosures about cybersecurity and consider whether previous disclosures need to be revisited, updated or corrected, including during the process of investigating

a cybersecurity incident (which should be specifically articulated in the company's incident response plan).

- Review disclosure controls and procedures to determine if incidents and breaches are, or can be, timely escalated to senior management and legal department for disclosure analysis and certifications.
- Assess whether disclosure controls and procedures provide a method to determine the impacts of cybersecurity risks and incidents on the company and a protocol to assess the potential materiality of such risks and incidents.
- Review disclosure controls and procedures to assess whether procedures are in place to determine whether implementing a blackout period while the company investigates and assesses the significance of a cybersecurity incident is appropriate, and review insider trading policies to ensure they prohibit insiders from trading in company securities when in possession of material nonpublic information relating to cybersecurity risks and incidents.
- Review the company's incident response plan to determine if the appropriate level of coordination between information security, communications, legal, and management is included and that policies, procedures, and structures are in place for open communication between technical experts and disclosure advisors when an incident has occurred to protect against misstatements.
- Assess the company's Regulation FD policy to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively, and that Form 8-K disclosure is made simultaneously if material nonpublic information is provided to those persons enumerated in Regulation FD in connection with state data breach notification requirements.
- In preparing annual and quarterly reports and registration statements,
    - Avoid generic risk factors relating to cybersecurity and instead tailor them to the company's actual threat landscape, which could include some or all of the eight factors contained in the Guidance;
    - When crafting MD&A disclosure regarding events, trends, and uncertainties that are reasonably likely to have a material effect on results of operations, liquidity, or financial condition, consider the costs of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents, including the impact on reportable segments, and the risks of potential cybersecurity incidents; and
    - Make sure the range and magnitude of financial impacts of a cybersecurity incident, as they become available, are incorporated into financial statements on a timely basis.

---

[1] The SEC initially indicated that it was poised to tackle the issue by issuing a Sunshine Act Meeting notice on February 14, 2018, for a meeting on February 21, 2018. The purpose of the meeting was to discuss cybersecurity, and specifically "whether to approve the issuance of an interpretive release to provide guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents." However, the meeting was unceremoniously cancelled the day before it was to occur. Instead, the SEC issued its cybersecurity guidance via seriatim.

[2] As Commissioner Stein noted in her statement about the new guidance: "To be sure, these are all valuable reminders and raising them to the Commission level indicates a level of significance the staff guidance from seven years ago simply does not. The problem, however, is that many of these reminders were offered by the staff back in 2011. . . . The more significant question is whether this rebranded guidance will actually help companies provide investors with comprehensive, particularized, and meaningful disclosure about cybersecurity risks and incidents. I fear it will not."

[3] Although the SEC acknowledged that none of its regulations "specifically refer[s] to cybersecurity risks and incidents," it insists that "an obligation to disclose such risks and incidents" is imposed by a "number of requirements," such as periodic reporting requirements or Securities Act and Exchange Act requirements. What is required will "depend[] on the company's particular circumstances." For example, "companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussion of [cybersecurity] risks in the appropriate context." The suggestion that "[t]his type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors" was foreshadowed by the SEC in its **amicus brief** (http://www.scotusblog.com/wp-content/uploads/2017/09/16-581-bsac-unitedstates.pdf) to the Supreme Court in *Leidos, Inc. v. Indiana Public Retirement System*, relating to Item 303 statements.