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." ■