



## What Companies Can Do To Protect Against Cyberattacks ... and the Litigation That Often Follows

- Companies should critically assess the strength of their cybersecurity defenses against evolving threats, including third parties' vulnerabilities.
- Recent changes in regulatory expectations for cybersecurity have underscored the need for board oversight of this potential risk.
- Many boards are now revisiting whether and how to assign cybersecurity oversight to a board committee.
- A well-designed governance framework for managing cybersecurity risks can help minimize the legal risks companies and directors will face after an attack. Companies that implement policies and procedures for rapidly reporting, escalating and thoroughly documenting the board's oversight of cybersecurity issues will be well positioned to defend against post-attack litigation.

Cyber threats continue to grow as a result of increased digitization, widespread use of cloud computing, advanced connectivity and artificial intelligence (AI), requiring boards of directors across all sectors to focus more on overseeing cyber risks.

At the same time, the Securities and Exchange Commission (SEC) now requires public companies to disclose more information on the board's oversight of cybersecurity risk management and identify the board committee or subcommittee responsible for that oversight. See our Winter 2024 article "[Emerging Expectations: The Board's Role in Oversight of Cybersecurity Risks](#)" for a discussion of the SEC rules.

Together, these developments are prompting many boards to revisit their company's cybersecurity processes and oversight mechanisms. The

recent securities and derivative lawsuits against CrowdStrike following its computer outage in July 2024 showcase how stockholder litigation increasingly follows cyber incidents.

In general, a well-designed governance framework for managing cybersecurity risks will minimize the legal risks to a company if it is the victim of an attack. Documentation of the board's formal oversight role in cybersecurity, together with solid records of the board's role in implementing and monitoring cybersecurity controls, may provide a defense to allegations that the board did not fulfill its duties.

Below are some lessons gleaned from changes many companies are making in their governance relating to cybersecurity and from recent court decisions.

## Revisiting and Refining Governance

As corporate risk and regulatory frameworks evolve, so too must corporate governance. We have seen many boards reviewing their approach to cybersecurity oversight, prompted both by the evolving risks and the SEC's rules. Some are revising board committee charters to specifically assign oversight for cybersecurity issues to a particular committee, or reassign it if it had been specified, to reflect the growing importance of this potential risk.

While such a review is not expressly required by the SEC's rules, the requirement to disclose cybersecurity governance practices has led many boards to rethink their documentation and approach to managing this area of risk.

There is no one-size-fits-all approach. What is important is to be thoughtful about which body has the time available to assess these issues on an on-going basis and will be able to bring relevant expertise to the challenge. Responsibility could be given to the audit committee, since that body usually oversees controls of various sorts and general compliance with legal and regulatory requirements.

But, where cybersecurity issues are central to the business, some companies have created a technology committee rather than saddle the audit committee with additional work, since it typically already has a lot on its

plate. Such a technology committee is usually dedicated to overseeing the strategy, performance and compliance of all the company's technology, positioning this committee well to make cybersecurity governance decisions and address newly emerging challenges associated with other technology issues such as artificial intelligence deployment.

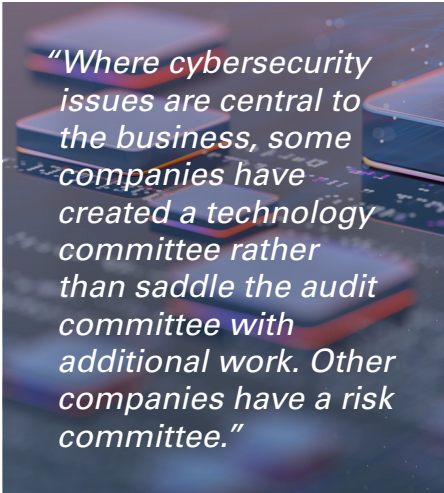
Other companies have a risk committee dedicated to identifying, assessing and mitigating risks, including cybersecurity risks, across the company. In short, there are many approaches to how a board may structure its cybersecurity oversight, yet it is ultimately the board's responsibility to determine which structure or body would best serve the company.

## A Refresher on the Duty of Oversight

Delaware law requires directors to implement and monitor oversight processes for business risks. This does not entail day-to-day management responsibilities, but the expectation is that directors will oversee management through established processes and rely in good faith on information provided by officers and advisers.

In practice, every company's approach to fulfill the duty of oversight will differ, but it should encompass several key cybersecurity risk areas.

*First*, in a world of expanding supply chain risks and "shadow IT," boards should oversee company processes to track technology assets and



*“Where cybersecurity issues are central to the business, some companies have created a technology committee rather than saddle the audit committee with additional work. Other companies have a risk committee.”*

understand associated threats. This could be satisfied, for example, via an IT asset mapping exercise, where the organization evaluates the location and interconnections among its various IT devices and networks to understand on what its IT systems depend and what is most critical. The board will want to ensure that management is aware of any technology blind spots, like unmanaged IT assets, and how the company addresses potential blind spots.

*Second*, regulators increasingly expect companies to adopt clear roles and responsibilities for cybersecurity and IT governance. The chain of command and authority should be clear and should ultimately route up to the board.

*Third*, boards need to understand to what extent their organization’s IT depends on other companies or specific pieces of technology. Several recent cases have highlighted the ways in which attacks on the software supply chain can have cascading effects far beyond the initial attack. In some sectors, such as financial services, regulators already expect boards to receive summaries or full reports of IT dependency that help pinpoint critical systems or third-party service providers.

If these three dimensions are not accounted for in a company’s governance procedures, officers and directors could face probing questions about the quality and sufficiency of their cybersecurity oversight.

In the oversight context, a breach of duty occurs only when directors act “in bad faith,” either because:

- a board “utterly failed to implement any reporting or information system or controls” (“the first prong”) or
- “having implemented such a system or controls, ... [it] consciously failed to monitor or oversee its operations, thus disabling themselves from being informed of risks or problems requiring their attention” (“the second prong”).

Suffering a cyberattack alone may not demonstrate bad faith. Delaware courts have acknowledged that “the directors’ good faith exercise of oversight may not invariably prevent employees from violating criminal laws, or from causing the corporation to incur significant financial liability, or both.” Instead, the legal question is “whether the board made a good faith effort to put in place a reasonable board-level system.”

Some lawsuits by stockholder plaintiffs have survived motions to dismiss where they alleged in some detail that a board acted in bad faith and violated its duty of oversight by failing to establish a committee or other system to monitor certain risks, including what could be a “mission critical” risks for a company, at the board level, thus violating the first prong of the breach test. That principle could apply to some companies whose business is particularly dependent on systems that could be subject to hacking or other cyberattacks.

Even where there were “red flags” that arguably should have prompted action by a board, a plaintiff must still show that the board “consciously overlooked or failed to address them.” And not every indication of a potential problem is a “red flag” worthy of a board-level reaction.

### **Oversight, Cybersecurity and Derivative Suits**

How does the legal framework apply to litigation where a board’s cybersecurity oversight is challenged?

So far, no cybersecurity oversight claim has survived a motion to dismiss in Delaware. And in two recent derivative suits, claims against directors following massive cybersecurity breaches were dismissed at the pleadings stage, before discovery.

These rulings offer lessons for boards weighing how best to oversee processes to minimize the risk of attack and how to ensure they have strong defenses if sued.

One case involved hotel operator Marriott International and the other involved SolarWinds, a software company. The rulings acknowledged the “increasing importance of cybersecurity.” But in both cases, the directors won motions to dismiss in part because the boards had taken good-faith efforts to monitor cybersecurity risks, and they had maintained records to demonstrate it. The rulings show that well-documented

oversight activity may aid in a defense before discovery gets underway, even if a court may criticize the board’s performance in monitoring that risk, as it did in the SolarWinds case.

### **Cybersecurity Oversight Considerations**

Based on these cases and the board deliberations we have seen concerning allocation of responsibility for cybersecurity oversight, here is some guidance for boards revisiting their cybersecurity defenses and oversight mechanisms:

- Consider delegating cybersecurity and data privacy oversight to a board committee and review that committee’s charter to consider specific cybersecurity language.
- Take steps to establish monitoring and compliance systems for cybersecurity issues and pay ongoing attention to them. This may include consulting legal counsel and other experts to identify where risks may arise and how best to monitor them.
- Directors should receive reports from management regarding internal and external cybersecurity events at whatever intervals make sense for a particular company.
- Coordinate with management and advisers regarding compliance with new cybersecurity disclosure rules and regulations.

- Given stockholders’ increasingly frequent demands to inspect corporate books and records as a prelude to litigation, boards should document their efforts and processes in sufficient detail to demonstrate the attention they have paid to understanding and overseeing risk and compliance systems and their responses to any cybersecurity issues that have arisen.

---

**Authors**

*William E. Ridgway / Chicago*

*David A. Simon / Washington, D.C.*

*Jenness E. Parker / Wilmington*

*Claire K. Atwood / Wilmington*

*Joshua Silverstein / Washington, D.C.*

---

**This article is from *The Informed Board*, Skadden’s quarterly newsletter for corporate directors.**

[View past issues of \*The Informed Board\*.](#)

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West / New York, NY 10001 / 212.735.3000