

# The Informed Board

Fall 2024

At what point has a director served too long? What about term limits? A mandatory retirement age? When do a director's skills become stale?

These issues are addressed in this issue of *The Informed Board*, as well as why proxy advisory firms and institutional investors are questioning director independence after nine years of service, and how activists are leveraging this trend. Listen to our latest podcast episode to hear about best practices in assessing board skills and implementing an effective board refreshment policy.

We also look at the varied ways boards approach the oversight of cybersecurity issues, and what information directors need to know about cyber risks.

Finally, with a change in administration in the offing, we examine the prospect that national security AI regulations may change — or remain largely unchanged.

- 
- |   |  |
|---|--|
| 1 What Companies Can Do To Protect Against Cyberattacks ... and the Litigation That Often Follows | 10 A Director Discusses How the Roles of Public and Private Company Directors Differ |
| 6 Most AI National Security Regs Likely To Remain in Place Under the Next Administration          | 13 Recommended Reading: 'Multigenerational Boards'                                   |
|   | 14 Podcast: When and How To Replace a Director                                       |



# 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.

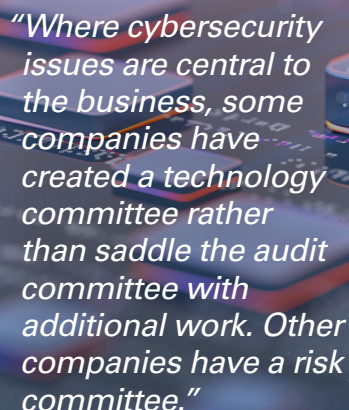
Other companies have a risk committee dedicated to identifying, assessing and mitigating risks, including cybersecurity risks, across the company. In short, there are many approaches to how a board may structure its cybersecurity oversight, yet it is ultimately the board's responsibility to determine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



## Most AI National Security Regs Likely To Remain in Place Under the Next Administration

- Rapid advances in artificial intelligence (AI), alongside the growing accessibility of AI platforms and tools, present unique national security risks and opportunities.
- U.S. regulators are implementing AI-related prohibitions, restrictions and reporting requirements across the AI supply chain with a focus on defense and cyber uses of AI, and a particular eye on China.
- While current restrictions and prohibitions regarding AI technology remain narrowly focused on defense and cyber-related capabilities, new requirements focused on monitoring and informing the U.S. government of the state of AI capabilities may lead to future scrutiny of AI, domestically and abroad.
- We do not expect the Trump administration to implement major changes to these regulatory initiatives.

With the rapid commercialization of artificial intelligence (AI) technology, the Biden administration has been grappling with its implications, including its potential impact on national security. Several departments have issued regulations to protect national interests against potential AI threats.

While President Trump said during the election campaign that he would roll back some of the restrictions that have been imposed on AI, we think it is unlikely that the provisions focused on national security — some of which target China, in particular — are likely to be significantly modified under the new administration.

Here is a summary of the major AI-related regulatory initiatives to date and what we believe is likely to remain largely in place.

### The Current State of US National Security AI Regulations

Over the past two years, the Biden administration pursued several initiatives to regulate the development of AI in the interest of U.S. national security. President Biden's October 2023 Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI Order) laid out both a broad approach and many policy details. With respect to national security, the AI Order directed the U.S. government to establish policies "for addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers — while navigating AI's opacity and complexity."

Several new regulatory initiatives address that concern, although some rules have yet not been finalized and could be changed or delayed by the new administration:

**Investments in Chinese AI companies:**

On October 28, 2024, the Treasury Department released a final rule restricting U.S. investments in Chinese companies engaged in developing AI systems, quantum technologies, and semiconductors and related computers, equipment and materials. The rule, which takes effect January 2, 2025, imposes additional diligence responsibilities as well as recordkeeping and notification requirements. It also adds restrictions on U.S. persons and their controlled foreign entities engaging in transactions with foreign persons in “countries of concern” (currently limited to China) that perform certain specified activities related to AI, semiconductors and microelectronics, or quantum information technologies.

While the rule attempts to focus on AI technologies that “pose a particularly acute national security threat to the United States,” the scope of coverage (e.g., for AI systems for “cybersecurity applications” or “the control of robotic systems”) is potentially broad.

**AI-related export controls:** Building on export controls implemented in the fall of 2022 and 2023, in September 2024 the Commerce Department’s Bureau of Industry and Security (BIS) issued an interim final rule tightening export controls on semiconductors and related items, including so-called “neural network” semiconductors that

may be used for machine learning of AI systems. This is the latest in a series of efforts by BIS to restrict the export to China of the types of hardware, software and technology powering advanced AI systems.

**Transfers of U.S. person data:** In February 2024, President Biden signed Executive Order 14117, which directs the Department of Justice (DOJ) to restrict the transfer of bulk U.S. individual or U.S. government-related personal data to countries of concern (i.e., China, Russia, Iran, North Korea, Cuba and Venezuela). Executive Order 14117 is inspired by AI-related concerns. It notes that U.S. adversaries can use AI “to analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations” and that bulk data sets can “fuel the creation and refinement of AI and other advanced technologies.”

On October 29, 2024, the DOJ published a proposed rule to implement these restrictions. We believe it is unlikely this rule will be finalized before the change in administrations.

**AI model reporting requirements:**

On September 11, 2024, BIS proposed a new rule that would require AI companies to report to the U.S. government on their development of dual-use AI foundation models, and related cybersecurity and safety measures. This rule, which would be issued pursuant to the Defense Production Act of 1950 (DPA), would impose periodic reporting requirements on AI companies similar to the initial disclosures that BIS has already required from several AI companies



*"Defense-related export and technology controls will remain an area of bipartisan focus, and we would expect continued development of U.S. export controls to address AI-related concerns."*

under the AI Order. BIS has the authority under the DPA to conduct industry surveys, and the proposed rule would amend BIS's existing industry survey regulations by mandating ongoing periodic reporting related to relevant AI models and clusters. This rule has not yet been finalized.

#### **Cloud services reporting**

**requirements:** In January 2024, BIS issued a proposed rule that would require U.S. cloud services providers to submit reports to BIS when foreign customers use U.S. cloud computing services to train large AI models for potential use in malicious cyber-enabled activity. The proposed rule, which imposes several national security-oriented obligations on U.S. cloud services providers, faced significant pushback from industry. Commerce has indicated that it expects to publish a final rule in December 2024, but this timing is subject to change.

#### **National Security AI Regulations in a Trump Administration**

During the presidential campaign, President Trump stated that he would "cancel" the AI Order on "day one." While a new Trump Administration may well carry through with this pledge, we do not expect significant softening of the national security-oriented regulatory initiatives outlined above.

- Congress generally supported, on a bipartisan basis, the Biden administration's initiative to create

restrictions on outbound investments in Chinese companies developing technologies of U.S. national security concern. It is possible that a new administration may impose further restrictions in this area.

- Defense-related export and technology controls will remain an area of bipartisan focus, and we would expect continued development of U.S. export controls to address AI-related concerns.
- While the incoming administration reportedly is considering a massive overhaul of the DOJ, the department's draft rule restricting transfers of data about U.S. persons to China does not seem to be a likely candidate for significant change.
- The draft BIS rules requiring reporting by U.S. AI companies and cloud services providers are perhaps the rules most likely to be changed or delayed, because of their ties to the AI Order (in the case of reporting by U.S. AI companies) and because of significant U.S. industry pushback (in the case of reporting by U.S. cloud services providers).

We also do not foresee changes in other AI-related national security regulations that rest on different legal grounds. For example, we expect continued close scrutiny by the Committee on Foreign Investment in the United States (CFIUS) of foreign investments in domestic AI capabilities and technology. We also expect BIS to implement AI-related U.S. supply

---

chain restrictions under the Information and Communications Technology and Services regulations — a regulatory program that was initially developed under the Trump Administration.

A Trump administration may also seek to accelerate national security-related AI innovation in the U.S. President Trump's advisers have reportedly worked on a new AI executive order that would seek to remove "unnecessary and burdensome regulations" that impede AI development in the interest of national security. President Biden's October 24, 2024 national security memorandum on "advancing the United States' leadership in Artificial

Intelligence" adopted some relatively modest measures in this direction — for example, by prioritizing the recruitment of non-U.S. "AI talent" under U.S. immigration laws. We would not be surprised if the new administration doubles down on these efforts.

---

#### **Authors**

*Brian J. Egan / Washington, D.C.*

*Michael E. Leiter / Washington, D.C.*

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

*Tatiana O. Sullivan / Washington, D.C.*

*Nicholas Kimbrell / Washington, D.C.*



## A Director Discusses How the Roles of Public and Private Company Directors Differ

Maggie Wilderotter is chairman of DocuSign and also serves on the boards of Costco, Sana Biotechnology, Fortinet, Sonoma Biotherapeutics and Tanium. She previously served on numerous boards, including Lyft, Hewlett Packard Enterprise and Procter and Gamble. Maggie was CEO and chairman of Frontier Communications and, before that, Wink Communications. Maggie also held senior executive positions at Microsoft and AT&T Wireless.

**Q: You've served on the boards of 36 different companies over the course of your career — some public, some private. How have you found board service to be different between the two?**

A: I've enjoyed serving on both for different reasons. On roughly half the public company boards on which I've served, I began service when the company was private and then it went public. Service on each can be an enriching experience, but each requires a fundamentally different approach.

For public company boards, the directors' core roles are to hire and fire the CEO, oversee risk — particularly financial risk — and set strategy for the company. The board performs these very core, and important, functions, but should not be in the weeds of running the company on a day-to-day basis; that is management's job.

Private company board service is very different. In most cases, management's expectation is that you'll be a real adviser and often act as a coach to the CEO and management team. Management affirmatively wants a board where directors can bring to bear a variety of different experiences and skill sets to help management in a variety of ways — whether that's making introductions, digging into product strategy or marketing, or whatever is most critical for the company to move forward at the time. There is more a sense of working side-by-side with management to achieve the collective objectives of the company, rather than a strictly oversight and monitoring role. Each role requires a different approach and skill set to be effective, but I find both rewarding.

**Q: You were CEO of Frontier Communications for over a decade before it was sold and before that a long-time, hands-on operational manager. Is it difficult to make the transition from sitting CEO to outside, independent public company board member?**

A: I don't think it is particularly difficult, at least for me, but it does require that you understand where the boundaries are, be mindful of what the core role of a public company independent director is and, occasionally, exercise some restraint.

Your role isn't to directly manage the company. You may have a great idea, a different way that you would do something, or you'd make a different choice on any one of a number of execution decisions that, ultimately, need to be management's to make. That doesn't mean that you can't raise questions, help management think through the issues or see a different perspective. You can and should do that, and it's a very valuable role to play. But it needs to be done with some humility and some cognizance that, as a board, you're hiring the CEO to make the call, ultimately, on many of these decisions once overall strategy is set.

Another major difference is that no individual director acts as the CEO's boss. The board as whole clearly does, but the board functions as a group. Even when I act as chair of a board, I recognize that, while I have a very important role to play — liaison between the independent directors

and the CEO, helping to set the agenda, occasionally acting as the voice of the independent directors to the investor community — I am just one member of the board. And it is important to try to achieve consensus as a board and to make decisions on a collaborative, constructive basis.

The CEO role is very different. While a good CEO will gather inputs from her senior management team and consider different points of view, in the vast majority of cases, the CEO's call is final and is hers alone to make.

**Q: Given the very different roles you see for directors of private versus public companies, and your experience serving on the boards of private companies that went public, how do you manage that transition? Can that be a difficult transition?**

A: It's really a key part of the IPO process. One of the key sets of issues for any private company board in that process is making sure you've got the right people in the right seats on the bus. And that applies equally to the senior management team and to the board. You have to make sure you've got the right people in all those positions.

It's not at all unusual to make senior management changes in connection with an IPO. The same is, and should be, true for boards as they transition from the adviser and coach role to one of oversight. Many times at the board level that's a relatively easy transition to execute. Many board

members do not want to continue to serve on a public company board — at least not beyond a transitional period. And many VCs will want to come off the board at some time fairly shortly following an IPO.

Other times, it will require a tough, or at least more delicate, conversation. Sometimes the answer might be to expand the board in the first instance to accommodate directors with different, public-company-oriented skill

sets, and then later shrink it down again to get to a more workable, manageable board size. That's often a good way to go as well in order to have some continuity as the board transitions along with the management team and company itself. The board itself needs to be clear-eyed and focused on how it can best position itself for life as a public company board when that day comes. And the IPO window is open once again!



Only 5% of S&P directors are under 50, but companies whose directors span a wide range of ages — at least 30 years between the youngest and oldest — generally outperform their peers in the same industry, according to a recent report from the corporate governance team at AllianceBernstein. ["The Case for Multigenerational Corporate Boards"](#) summarizes several studies and supplements those with the authors' own research.



**Listen to  
the podcast**

Boards need to have a robust refreshment program. Strategies change, directors' skills become stale and investors are skeptical about the independence of long-tenured directors. Skadden M&A partner Ann Beth Stebbins discusses best practices in board refreshment with her guests, Laurel McCarthy of Spencer Stuart and Elizabeth Gonzalez-Sussman, who heads Skadden's shareholder engagement and activism practice.

---

**Host**

*Ann Beth Stebbins / New York*

**Guests**

*Elizabeth Gonzalez-Sussman / New York*

*Laurel McCarthy / Spencer Stuart*

---

## Contacts

**Elizabeth R. Gonzalez-Sussman**

Partner / New York  
212.735.2366  
elizabeth.gonzalez-sussman@skadden.com

**Brian J. Egan**

Partner / Washington, D.C.  
202.371.7270  
brian.egan@skadden.com

**Michael E. Leiter**

Partner / Washington, D.C.  
202.371.7540  
michael.leiter@skadden.com

**Jenness E. Parker**

Partner / Wilmington  
302.651.3183  
jenness.parker@skadden.com

**William E. Ridgway**

Partner / Chicago  
312.407.0449  
william.ridgway@skadden.com

**David A. Simon**

Partner / Washington, D.C.  
202.371.7120  
david.simon@skadden.com

**Ann Beth Stebbins**

Partner / New York  
212.735.2660  
annbeth.stebbins@skadden.com

**Joshua Silverstein**

Counsel / Washington, D.C.  
202.371.7148  
joshua.silverstein@skadden.com

**Tatiana O. Sullivan**

Counsel / Washington, D.C.  
202.371.7063  
tatiana.sullivan@skadden.com

**Claire K. Atwood**

Associate / Wilmington  
302.651.3123  
claire.atwood@skadden.com

**Louis M. Davis**

Associate / New York  
212.735.2254  
louis.davis@skadden.com

**Nicholas Kimbrell**

Associate / Washington, D.C.  
202.371.7337  
nicholas.kimbrell@skadden.com

**Alexander J. Vargas**

Associate / Chicago  
212.735.3302  
alexander.vargas@skadden.com

**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