Even before the proposal was issued, oversight of cybersecurity risk had become an increasing area of focus for boards. A survey by Deloitte and the Center for Audit Quality of 246 audit committee members published in January 2022 found that two-thirds of participants with oversight responsibility for cybersecurity expected to spend more time on the topic in the coming year.\(^1\) In addition, 62% identified cybersecurity as one of the company’s top risks to focus on in 2022.\(^2\)

An SEC proposal issued in March 2022 to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting has sparked increased discussions about cyber risk in many corporate boardrooms. At many companies, boards are asking questions about what measures they should consider taking that would help to enhance governance and improve risk management, which may also help prepare the company to meet likely new requirements.
If adopted as proposed, the SEC’s new rules would require prompt reporting of material cybersecurity incidents and disclosures in periodic filings focused on:

- Policies and procedures to identify and manage cybersecurity risks
- Management’s role in implementing cybersecurity policies and procedures
- Corporate directors’ cybersecurity expertise, if any, and the board’s oversight of cybersecurity risk
- Updates about previously reported material cybersecurity incidents

The SEC received nearly 150 comment letters on the proposal and is expected to issue final requirements later in 2022.

Leading up to the proposal, cyber incidents have increased in recent years, both in frequency and magnitude. Cyberthreats have become more complex as threat actors use more sophisticated techniques. At the onset of the pandemic, the cyberattack surface expanded significantly, and risk persists for many companies that are maintaining hybrid work arrangements. Companies face threats related to the theft of information, disruption of functions, ransomware demands, destruction of hardware and software, and corruption of data.

The financial risks that can stem from loss of confidentiality, integrity, critical business processes, and information assets can be substantial. In addition to direct costs, operational impacts such as an inability to produce goods and services, system downtime, missed opportunities, and an outsized focus on incident or breach management impacts can be significant. A company’s brand, one of its greatest assets, can be damaged significantly from the loss of customer trust that can occur with cyber incidents.

These and other impacts compound pressures within the cyberthreat landscape, making active board oversight essential to cyber risk management. These pressures can increase the need for more strategic dialogue among management and directors to help improve understanding of risk.

Revisit, intensify focus on governance

The importance of the board’s role in promoting a cyber-focused mindset and a cyber-conscious culture throughout the organization cannot be overstated. The board’s oversight role is a fundamental aspect of governance, which includes defined strategies, policies, and procedures to mitigate cyber risk. Many companies could benefit from an increased focus on cyber risk governance, with or without new disclosure requirements.

Boards can consider several measures to promote this increased focus, beginning with a cyber risk assessment, by business area, that includes the company’s readiness for a cyber incident, the response plan, and the recovery plan. Evaluation of the organization’s cyber incident response plan is also critical at the board level, with a focus on the controls surrounding business functions and what steps will be taken in the event of an incident.

4. Ibid.
The board can also set an expectation that the incident response plan has been practiced through scenario planning or wargaming exercises to improve the company’s ability to respond and recover in the event of an attack. The teams for such a review should include senior management from each line of business and corporate function.

In many organizations, budgets for security are typically given lower priority than budgets for other IT or business priorities, often rendering companies that take this approach unprepared to deal with risks and attacks. An annual review of cybersecurity budgets by the board or a designated committee, such as the audit committee or a technology committee, can promote an increased focus on the importance of adequately resourcing the business to manage and mitigate cyber risk.

The board can also review top-level policies on cyber risk to create a culture of awareness and accountability. Companies often enhance their security position when they promote a culture of cyber risk consciousness as part of the overall enterprise risk management structure.

External reviews of cyber risk programs, including the governance structure for cyber risk and the strategy and implementation of mitigation controls, can also give the board an improved understanding of the company’s level of resilience.

Boards can also request and review high-level reports on risk assessments at third parties—such as vendors and suppliers in cloud, mobile, hosting, and software-as-a-service arrangements—to confirm that those organizations are complying with the company’s cyber risk program and standards.

The National Association of Corporate Directors (NACD) suggests that boards consider five cybersecurity principles to improve their oversight of cyber risk. These principles are:

1. Boards should understand and approach cybersecurity as a risk management issue for the entire enterprise and not just a technology or IT issue. Cybersecurity may have begun as primarily a technology-centric risk, but it has evolved to become a multifaceted business issue. The ability to manage cyber risk is integral to every aspect of business operations.

2. Boards should understand the legal aspects of cyber risks that are relevant to the company’s own facts and circumstances. In addition to the business impacts of a breach, companies and directors may also face legal consequences that boards should consider as they set strategy and define risk appetite.

3. Boards should have appropriate access to cybersecurity expertise and discuss cyber risk management regularly in board meetings. Boards should expect cyber risks to be communicated to the board frequently, with adequate discussion about the company’s threat landscape and risk mitigation strategies. Boards can seek input from both internal and external experts.

4. Boards should set an expectation for management to establish an enterprise-wide risk management framework that is adequately resourced. The board can ask questions to confirm that the framework is implemented across the organization at all levels and that it had adequate staffing and budget.

5. Boards should discuss identified risks with management, including risk prioritization, appetite, and mitigation strategies. This discussion may include a review of options to transfer risks that cannot be practically mitigated using cyber risk insurance.

The benefits of a framework approach

Boards can evaluate the extent to which the organization’s cyber risk strategy aligns with a commonly accepted framework, such as the National Institute of Standards and Technology (NIST) cybersecurity framework. A framework approach guides how companies can assess and improve their ability to prevent, detect, and respond to cyber incidents.

A framework also provides a common language that enables companies—boards, management, and other critical stakeholders—to develop a shared understanding of cyber risks, and it enables a means for benchmarking the company’s approach against those of other companies. Under the NIST framework, the strategy would focus on five critical functions.

---

• **Identify.** An effective approach begins with identifying cybersecurity risk to systems, people, assets, data, and capabilities. This might include a focus on critical assets of the company and the degree of exposure in the environment, threats and threat actors, and possible business impacts. It could also include an understanding of regulatory requirements, governance, risk assessments (including risks arising from third parties), and risk management strategy.

• **Protect.** Appropriate safeguards to limit or contain potential impact of a cyber incident can be established to protect critical infrastructure. Here, the organization would focus on developing a cyber risk management framework with appropriate controls and asset management tactics that would be integrated into the overall ERM and crisis management programs to provide mobile and endpoint security.

• **Detect.** It’s not always immediately evident that a breach has occurred. Companies need to define how they will identify the occurrence of a cyber incident. Metrics for monitoring cyber key performance indicators and controls testing can help detect incidents. Security information and event management technologies as well as audits of third parties are also helpful.

• **Respond.** Companies need to define what actions they will take to effectively minimize the impact or negative effects of a cyber incident. Crisis response planning is critical, as is practicing the response through exercises such as scenario planning or wargaming, to promote resilience. Companies can also consider when and how to engage local, national, and global law enforcement resources.

• **Recover.** Timely recovery from a cyber incident and restoration of capabilities or services that were impaired is critical. Companies should understand leading practices at peer companies in their industry for activating crisis response plans and promoting technical resilience.

Leading practices for boards that are highly effective in overseeing cyber risk begin with driving cyber awareness with a strong tone at the top. Proactive boards often participate in organizational awareness programs and demonstrate due diligence, ownership, and effective governance of cyber risk.

These boards hold regular board and committee briefs to understand the threat landscape, the business-critical risks, and the metrics that describe the state of the control environment and mitigation efforts. Metrics can be developed with respect to many aspects of cyber risk management and mitigation, such as overdue security assessments, third-party incidents and recovery testing, overdue access reviews, deficient password requirements, asset threats, and many more.

Leading practices for highly effective boards also often include evaluation of the impact of an incident and the company’s existing cyber incident response plan with a focus on the controls surrounding business functions and what steps will be taken in the event of an incident. These boards often review policies and the company’s cyber risk framework to create a culture of awareness and accountability, and they meet with the CISO and CIO or other appropriate members of management to discuss cybersecurity risk, cyber talent, control activities, and improvement initiatives.

In addition, boards observing leading practices often conduct ongoing board education programs focused on enhancing the understanding of cyber risk and mitigation strategies. They request high-level reports on third-party risk assessments and ask questions about requirements for vendors and suppliers.

Like all risks that organizations face, cyber risk requires established and mature governance, oversight by the board, and inclusion into the overall enterprise risk management program. When the board works with management, each fulfilling its unique role, each can complement the other to drive an effective cyber-conscious culture, resulting in a high level of resilience to cyberthreats.
Authors

Mary Galligan  
Managing Director  
Deloitte & Touche LLP  
mgalligan@deloitte.com

Carey Oven  
National Managing Partner  
Center for Board Effectiveness  
Chief Talent Officer, Risk & Financial Advisory  
Deloitte & Touche LLP  
coven@deloitte.com

Maureen Bujno  
Managing Director and  
Audit & Assurance Governance Leader  
Center for Board Effectiveness  
Deloitte & Touche LLP  
mbujno@deloitte.com

Audrey Hitchings  
Managing Director  
Executive Networking  
Deloitte Services LP  
ahitchings@deloitte.com

Krista Parsons  
Managing Director  
Center for Board Effectiveness  
Deloitte & Touche LLP  
kparsons@deloitte.com

Caroline Schoenecker  
Experience Director  
Center for Board Effectiveness  
Deloitte LLP  
cschoenecker@deloitte.com

Bob Lamm  
Independent Senior Advisor  
Center for Board Effectiveness  
Deloitte LLP  
rlamm@deloitte.com

Maureen Bujno  
Managing Director and  
Audit & Assurance Governance Leader  
Center for Board Effectiveness  
Deloitte & Touche LLP  
mbujno@deloitte.com

Audrey Hitchings  
Managing Director  
Executive Networking  
Deloitte Services LP  
ahitchings@deloitte.com

Krista Parsons  
Managing Director  
Center for Board Effectiveness  
Deloitte & Touche LLP  
kparsons@deloitte.com

Caroline Schoenecker  
Experience Director  
Center for Board Effectiveness  
Deloitte LLP  
cschoenecker@deloitte.com

Bob Lamm  
Independent Senior Advisor  
Center for Board Effectiveness  
Deloitte LLP  
rlamm@deloitte.com

About DeLoitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more.

Copyright © 2022 Deloitte Development LLC. All rights reserved.