AGENDA

# Opinion

## A Framework for Board Oversight of Digital Security

New method aims at helping boards become more resilient and adaptive

By Ann Cleaveland, Michael Mahoney, Phyllis Sumner | April 4, 2022


- **Ann Cleaveland**

  Ann Cleaveland is the executive director of the University of California, Berkeley, Center for Long-Term Cybersecurity

- **Michael Mahoney**

  Michael Mahoney is a partner with Tapestry Networks

- **Phyllis Sumner**

  Phyllis Sumner is partner and chief privacy officer at King & Spalding.


At this point, nearly every large company has made significant investments in cybersecurity. But even where internal management of cyber risk appears strong, a board may worry that its oversight of digital security is inadequate — or that it has no reliable way to assess its adequacy or to compare its capabilities with other firms'. Recently proposed SEC rules requiring disclosure about a board's cybersecurity expertise and oversight of cybersecurity risk make this an even more urgent concern.

Adding to the challenge, cyber risk is unlike almost any other risk, because the threats and their impact evolve quickly. Risks arise not only from distant actors, such as criminal gangs and hostile nation-states, but also from employees and third-party providers. Even full-time cybersecurity professionals are challenged to stay ahead; the majority of directors lack direct personal experience in dealing with cyber risk.

We developed a framework, called Cyber Oversight Effectiveness Development (COED), that addresses these gaps and aims at helping boards become more resilient and adaptive. Based on interviews and conversations with directors from a range of industries, this framework is predicated on the belief that cyber risk often requires different treatment than other risks, such as health and safety or fraud.

The first step is to ensure your board has a foundation of cybersecurity oversight in place. Baseline oversight is essential to meeting the requirements of regulators, obligations to investors and expectations of the public — ultimately reducing litigation and other risks to the company. Such

practices include determining your risk profile; establishing roles and responsibilities and enforcing accountability for digital security; and setting up protocols for monitoring and reporting on progress.

While this baseline may be sufficient for some firms, a variety of circumstances could motivate a board to extend its investment in cyber oversight — for example, if a firm has experienced a major cyberattack in the past, if digital operations are a major element of value creation, or if a digital security failure could prompt a cascading crisis (as with large banks or airlines, for example). We believe that the majority of Fortune 500 companies meet at least some of these criteria, and that more boards should go beyond the baseline than not.

This is where COED comes in: because cyber threats evolve continuously, the development of enhanced oversight capability must also be continuous. The COED framework provides a multi-step process to help gain a deeper understanding of their organizations' current capabilities, how they differ from those of others and where they need to aim. COED aims to help boards focus on three primary elements: staging, intervention and reflection.

Staging is the process of using diagnostic exercises to establish a snapshot of where the board is at a given moment. COED identifies five stages of board development, ranging from the "ad hoc stage," where technological knowledge is scattered and directors are taking cues from the company leadership, to the "resilient stage," when directors have a well-developed point of view on the future landscape and how risk is changing. As the technology, regulatory and threat landscapes co-evolve, boards will repeatedly traverse these stages.

Intervention entails a series of board actions — including education, reorganization, seeking out internal and external expertise, running war games, and engaging in scenario planning — that can accelerate learning and move the board toward greater cyber risk capability and confidence.

And in the reflection step, a board can look back at the original staging assessment, review the process and results of intervention and identify specific learnings. Third-party experts, including legal counsel, may be helpful as board and management engage in reflection on the progress they have made.

The approach repeats over time, ideally on a cadence determined by the board's view of the threat environment and its own needs. The key is to enhance the speed of the process so the board's management of each successive cyber threat creates greater confidence and results in greater speed in responding to future attacks.

Using the COED Framework will increase board members' individual and collective self-awareness, moving from an emergency "ad hoc" posture toward a stance that is both proactive and resilient. Getting the most out of the COED Framework will require time, resources and energy, but the payoff will be greater readiness for digital transformation and value creation that goes beyond the important goal of protecting the company from cyber criminals.

An Information Service of Money-Media, a Financial Times Company