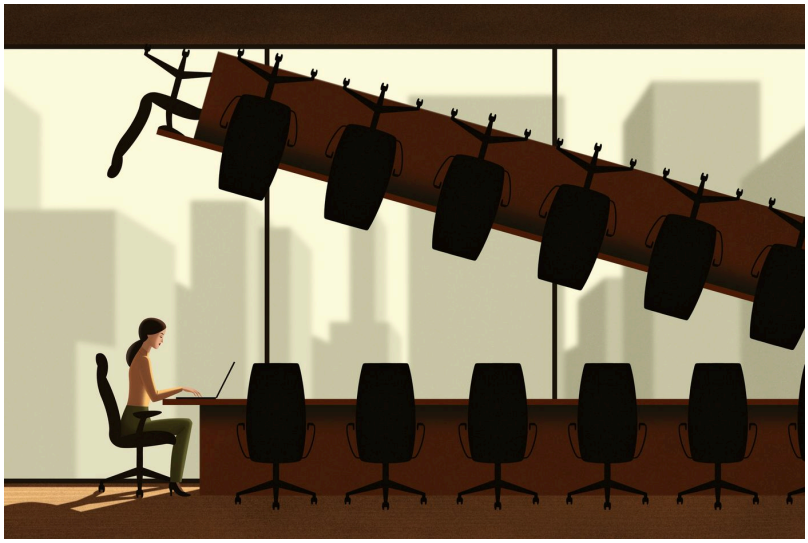
TECHNOLOGY | CYBERSECURITY

As Boards Focus More on Cybersecurity, Are They Missing One of the Biggest Threats?

The weak link inside organizations might be the very people responsible for making sure companies aren't vulnerable to attack

By Jeffrey Proudfoot and Keri Pearlson

March 13, 2024 10:00 am ET



Most companies don't seem to be preparing directors to anticipate, respond to or avoid cyberattacks on themselves. ILLUSTRATION: JON KRAUSE

Board members are taking on more responsibility for cybersecurity strategy at the companies they oversee. But they might be overlooking one of the organization's biggest vulnerabilities: themselves.

We uncovered this uncomfortable truth while conducting a series of interviews and surveys with dozens of directors across different companies and industries, part of our broader research into boards and cybersecurity issues.

Over the past decade, cybersecurity oversight has become an added board mandate, with directors becoming more accountable for ensuring that organizations have robust defenses in place against attacks. That means directors now have access to detailed tactical information about a company's cyber defenses, in addition to a lot of other sensitive data.

Despite that, directors haven't traditionally fallen within the scope of companies' cybersecurity efforts. Nor are most companies we surveyed preparing directors to anticipate, respond to or avoid cyberattacks.

The upshot: The board members themselves, the people responsible for making sure a company is well-protected, could well become the weak link in an organization's cyber defenses.

No preparation

Corporate executives have a number of ways to keep board members abreast of the company's cybersecurity preparedness, including presentations from technology executives, tabletop exercises that simulate hypothetical attacks, and reports on key cybersecurity metrics. However, none of these measures prepare directors to be resilient against potential attacks targeting them directly.

And there's no question that they are uniquely vulnerable. For example, based on research we have done, we know that many board members almost exclusively work remotely, meaning they share a lot of sensitive information electronically. In addition, directors usually aren't involved in, and thus don't benefit from, awareness programs, regular communications and informal water-cooler discussions that help keep cybersecurity on the minds of a company's employees. And since boards may receive cybersecurity status updates only periodically, it can take a while for directors to identify and fully understand emerging threats such as AI-driven cyberattacks and how they might be used to target them individually.

Several board members told us that some directors use public email accounts—rather than official or encrypted messaging systems or document-management platforms—to share board information and communications. One commented

that she thought the platform used by the board to share documents for meetings was secure, but she really didn't know for sure.

Other board members said that while they get limited briefings on things like the percentage of employees who fail phishing tests, they have never received training themselves on how to shore up their own personal defenses. Still others reported that, despite a growing focus on cybersecurity, many boards don't have a single director with a cyber background or with formal cybersecurity training who could help other board members prepare for, and respond to, targeted attacks.

What can be done?

In light of this risk, what can boards do?

First, the cybersecurity education-and-training programs aimed at rank-and-file employee could be customized for directors.

Second, customized tabletop exercises, in which board members are exposed to a hypothetical cyber incident and asked to respond, could be especially effective in terms of getting board members to recognize and prepare for direct attacks. The immersive nature of a tabletop exercise creates an emotional response that leads participants to become much more invested than they otherwise would in discussions about what to do during a real attack.

Third, organizations might want to include board members in phishing simulations, in which they send fake emails to employees to gauge how many will react and to develop training tools to mitigate the effectiveness of such attacks. The fake attacks and follow-up could be customized specifically for board members.

Finally, one-on-one consulting, where security experts are assigned to work with individual directors, might be the most effective training approach. This gives directors the tutoring they need at a time, and in a manner, most suited to them.

Virtually all cybersecurity assets and efforts are focused on protecting the organization itself—its employees, managers, executives, business processes, technologies and so on—but directors need to be included in the security plans, too. With the increasing mandate on boards to serve as the strategic

cybersecurity guards of their companies, more needs to be done to guard the guards themselves.

Jeffrey Proudfoot is an associate professor at Bentley University and a research affiliate at the Cybersecurity at MIT Sloan (CAMS) research consortium. **Keri Pearlson** is executive director of CAMS. **Stuart Madnick**, founding director of CAMS, also contributed to this research. The authors can be reached at reports@wsj.com.

Appeared in the March 18, 2024, print edition as 'Are Boards the Weak Link?'.

Next in Journal Reports: Technology