Are Boards the Weak Link?

Directors spend a lot more time thinking about cybersecurity. Perhaps they should look in the mirror.

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 act and to develop training tools to mitigate the effectiveness of such attacks.

Finally, one-on-one consulting, where cybersecurity 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, but directors need to be included in the security plans, too. If directors are expected to serve as the strategic cybersecurity guards of their companies, more needs to be done to guard the guards.

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