Should your board of directors include a cybersecurity expert?

Credit: Thinkstock

The pros and cons of proposed legislation to identify a board's cybersecurity pro.

-  **By Stacy Collett**

Should companies have a cybersecurity expert on their board of directors? The federal government seems to think so, and increasingly so do security and risk professionals, although companies would prefer to make that decision without government involvement, according to a sampling of industry pros.

A disclosure bill introduced by the U.S. Senate in December would ask companies to disclose whether they have a "cyber security expert" or equivalent measure on its board of directors. While no action is required if no expert currently has a seat on the board, the company would need to provide an explanation for how it is approaching cybersecurity.

Many questions still need answered, such as what skills would qualify a board member as a cybersecurity expert.The SEC and the National Institute of Standards and Technology would be given a role in evaluating cybersecurity experts' qualifications, but it's not clear what those qualifications are. NIST would not comment on pending legislation.

Some industry professionals say government would be over-reaching by influencing the make-up of a company's board, while others believe it's a positive step toward making cybersecurity a companywide issue that is no longer relegated to IT.

"I'm not a big believer in a lot of legislative action because it drives a check-the-box mentality and doesn't solve the problem," says Malcolm Harkins, global CISO at Cylance. "On the positive side, it's driving the discussion and a dialog that I think is healthy and that should have been started 10 years ago."

"It's a simplistic answer to a complex issue,"says Michael Airdo, attorney and chair of the technology committee at the International Association of Defense Counsel. "Despite the fact that it's bipartisan legislation, there's a natural aversion to having the government dictating board composition."

Many industry watchers see benefits to the proposal. A cybersecurity expert could ensure there is adequate cybersecurity policy and help the board assess the company's risk in its plan to prevent a breach or respond to one, Airdo says. An expert could also make sure there are full board discussions on cybersecurity, not just committee meetings, and that the discussion is well documented. "If I'm going to represent a board member for breach of fiduciary duties, I'm going to want to establish that all these board meetings exercised due diligence through the minutes of the meeting. The cybersecurity expert will make sure the minutes reflect the discussion adequately."

Is there a potential that board members will turn on their fellow colleague and say, 'how did you let this happen?' I think there's a risk of that, but I don't think it's a defense.

Michael Airdo, attorney and chair of the technology committee at the International Association of Defense Counsel.

If history is an indicator, Yorgen Edholm believes that the disclosure bill could be beneficial to companies. Edholm, CEO of cloud solutions company Accellion, sat on the board of Hyperion Solutions after passage of the Sarbanes-Oxley Act of 2002. SOX mandated strict reforms to financial disclosures after the accounting scandals at Enron, Tyco and WorldCom shook investors' confidence in financial statements. "It was very interesting to see the resistance at first, but when people did the postmortem, they said that 'for all the complaining we did, this was actually very helpful. It gives us a better handle on what's going on in the business." Edholm now sits on the boards of Accellion and a business intelligence startup.

A growing need for cyber risk assessment

As technology permeates all aspects of life, Harkins says cybersecurity risk assessment has become critically important in the boardroom.

"Depending on what a company is doing with technology, the board needs to look at the risk and the consequences not only to their shareholders and the company, but also to customers and society," says Harkins, who is also an author and speaker on cybersecurity and the board.

He points to the example of an FDA-approved procedure that in 2015 helped a blind man regain his sight. The technology uses a visor with a video-processing unit that transmits signals to a retinal implant. The idea is to cure blindness, but sinister hackers may see it as an opportunity to extort money, he warns.

"If that technology is poorly designed, developed and implemented, and it has the potential for malicious code to execute, what's to prevent these individuals from being forced to pay Bitcoin to get their eyesight back?" Harkins says. Scary stuff, but it serves as a reminder that as opportunities grow, so does the company's responsibility to do it securely, he adds.

Another factor at play in the boardroom is a well-documented psychological phenomenon that more people perceive an opportunity– the so-called coolness factor – the more they start discounting the risks, Harkins explains. Similar to security pros who tend to focus on the risks and might over-characterize them,

board members must be wary of natural biases by decision-makers and technology creators, and the way they view risk.

Group think and scapegoats

Having a cybersecurity expert on the board also has its share of potential drawbacks. “It adds another layer of responsibility… relative to maintenance of proprietary information and systems,” says Elizabeth Ryan, attorney and vice chair of the technology committee of the IADC. The cybersecurity expert “is going to have to bear a significant portion of that responsibility.” The benefits could outweigh the burden, though, she adds. “Hopefully, it will help minimize potential leaks and hackings. I think it that could be an enormous benefit and save corporations millions of dollars in litigation fees” when a breach occurs.

A cybersecurity expert might also slow the board’s decision-making process, or run the risk of becoming its scapegoat, some industry professionals say. When boards are faced with topics they don’t understand, like cybersecurity, they usually concur with the presenter or pile on with a lone dissenter that makes a reasonable argument, Edholm says. Not doing so would grind board meetings to a halt. Having a cybersecurity expert on the board, could facilitate those discussions further, he says.

What’s more, easily deferring to the “expert” may encourage group think and even complacency among board members. If a breach occurs and questions arise about their fiduciary responsibility, they could just blame the expert. “Is there a potential that board members will turn on their fellow colleague and say, ‘how did you let this happen?’ I think there’s a risk of that, but I don’t think it’s a defense,” Airdo says.

Finding the right expert

With so much at stake, companies may be hard pressed to find qualified candidates for cybersecurity board positions. Finding people who have the right skillset that straddle business and security, and “who can parachute into boardrooms and provide guidance is quite difficult,” says Steve Durbin, managing director of the non-profit Information Security Forum. “The person must be a hybrid with strong communication skills, who understands how to operate at the board level, and have an understanding of the cyber space” – usually a chief privacy officer or chief risk officer with business experience from outside the company and

not security pros with only hardware or software experience, he adds.

Candidates will also want to do their homework before committing to a company's board."I can't believe that a person would be willing to sign up without commitment from the company that they're already doing an adequate job with their security. Otherwise, you're going to be the one thrown under the bus when something bad happens," Edholm says. "Even if you have the best software, you also have to have discipline in the ranks," when it comes security awareness, he adds.

Despite the challenges, there will be people ready to accept the risks of being a board's cybersecurity expert, especially if they're well-compensated, Edholm says. If they can stay current with the latest cyber threats, "this could be a security expert's wonderful retirement – sitting on a couple of boards."