BlackBerry ThreatVector Blog

Does my Board of Directors Need a Cybersecurity Board Member?

FEATURE / Thomas Bennett

Boards of Directors are more involved than ever before in discussions and strategy around their companies' cybersecurity and the solutions needed to prevent being the next big headline.

The questions they are asking are no longer as simple as "are we secure?" but more to the tune of "are we doing all we can to minimize or transfer risk, and what do we do in the case of a breach?"

Boards also want to know if there are score-cards that measure company security posture, whether the company is compliant with the most recent regulations, and if they have the security controls to demonstrate compliance.

This sea change also means Boards have new options: Do they act as change agents for cybersecurity? Do they get hands-on as decision makers? Is IT security so vital to the business that it should have direct representation on the board itself, as in a Security Director?

Many Boards have taken the first steps, for example requiring quarterly cybersecurity briefings - some being directly presented by the CISO or VP of Risk Management - rather than relying on the occasional or ad hoc updates. When it comes to actual board representation though, most companies subscribe to one of the following beliefs:

- "We don't need a cyber expert on our board - we have a CISO/CIO and that is plenty."
- "Cybersecurity is a reporting and risk management problem, so cyber belongs in the boardroom as an episodic reporting agenda item."
- "We definitely need a representational cyber domain expert, but we don't know what that person should look like, and/or don't know where to find and recruit one."

For many companies, the first two statements might be perfectly appropriate for now. In fact, most boards are opting to act as change agents, but only for risk transfer - recommending or requiring cybersecurity insurance for their organization.

But other companies have taken the leap. Sally Beauty Holdings, Huntington Bancshares, and others have specifically added board members with deep cyber backgrounds. What has changed that's driven that choice? Should all boards be considering doing the same?

The answer is both yes and no. But if you think it's a 'yes' for your company, or are on the fence, here's a framework crafting a recruitment strategy and making a more informed choice:

Candidate Profiles

First and foremost, the candidate has to be a fully functioning board member! Ideally, they would already have served on boards of similar companies and would have been active in one or more committees (but ideally risk or audit) and be effective across the same broad set of board functions as other members. This person will need to have all of the critical board inter-personal skills that support and define leadership: ethics, integrity, crisis management, and more committees (but ideally risk or audit) and be effective across the same broad set of board functions as other members. This person will need to have all of the critical board interpersonal skills that support and define leadership: ethics, integrity, crisis management, and more.

Ideally, any candidate should be required to not only have technical and cybersecurity expertise, but also financial, operational and executive level experience (C-Suite preferred).

Second, make sure the board member is a complement and a cultural fit with the executives in charge of executing cybersecurity (CIO, CISO, Risk Officer). The last thing you want to do is engage a Director who creates conflict or sends the wrong message to the existing officers and executives. Ensure that the boundaries set for the board member adequately deconflict any overlap.

Also, their cybersecurity domain expertise should be specific to the types of risk that would being the most damage to an organization. So, the board and the executive team need to do some technical diligence and soul-searching about which type of cyber risk is most important to your organization:

Does my Board of Directors Need a Cybersecurity Board Member?

FEATURE / Thomas Bennett

PROFILE 1: SUPER-CISO	PROFILE 2: RISK MITIGATOR	PROFILE 3: REG/LEG Expert
Desired Traits	Desired Traits	Desired Traits
Former Multi-Time CSO/CISO	Cyber Risk Transfer	Cyber Risk Transfer
Previous Board background	Data Privacy expert	Compliance/Regulation
Business Continuity Specialist	Breach Mitigation	Industry Influencer
Focus on Incident Response	Legal Experience	Hill Experience

- Brand damage of a massive customer data breach
- Losing millions of dollars in business downtime
- Loss of shareholder value and loss of customer trust
- Intellectual Property loss
- All of the above

Based on which type of cyber risk is most critical to your organization, you can next begin determining which type of cyber expert you need. Do you need someone who can be a proxy for the CISO? Someone who can be on Capitol Hill all the time who knows about policy? ASOC and APT guru who's defended against nation/state attacks? Or do you need a cybertraining HR specialist who increase workforce in security awareness?

How to Search for the Right Candidate

There are several ways your company can go about seeking out the right candidate for what your organizations requires.

- **Traditional board search firms.** Many of the large recruiters have a board search practice, but I personally recommend the small sharp-shooters who do nothing else (**Dora Vell**, George Fleck, Shelia Ronning among others).

- **Professional organizations and certification bodies.** Both the National Association of Corporate Directors and American College of Corporate Directors have excellent placement capability and are huge proponents of cyber in the board room.

- **Tapping industry influencers.** Some of the high profile cyberboard luminaries (like Johanne Bouchard) have a deep rolodex of seasoned executives and board directors who might prove to be good candidates.

Conclusion

Start your long-term search for this board member now, as it may take many months to find the candidate with the right qualifications, cultural fit, and of course the availability to take the spot. You can expect that there will be a great deal of competition in the marketplace for the top candidates, given that the prerequisite skills are in short supply.

A short list of action items in the meantime:

- Make sure you have consensus for the new board hire with your existing board and executive team. Don't make any assumptions!

- Craft a timeline with realistic milestones with dedicated roles and responsibilities for existing board members, executives and outside consultants as needed - a board search can take up to 12 months or even more, so be prepared!

- Determine early on whether you need a specialized recruiter to assist - the sooner this consultant is involved the better

- Do the internal needs audit and risk profile to identify the ideal candidate profile - make sure to include as many stakeholders as possible, including legal counsel, the CISO, the CSO, VP of HR, Compliance, etc.

- Scan sites like LinkedIn and make a shortlist of profile candidates (not necessarily actual candidates) to fine tune the profile.

Dora Vell is the CEO of Vell Executive Search, a premier retained technology executive search firm in Boston. Ms. Vell is an internationally recognized expert in recruiting technology executives including: CEOs, COOs, CTOs, CMOs, CROs, board members and others. She works with VC-backed, PE-backed private companies and public companies. She can be reached at dora@vell.com.