THREATREADY™
RESOURCES
Preparing Your People

Interview the Expert

An Interview With Rick Williams

Rick is a Partner with the Newport Board Group. He advises CEOs and boards at critical decision points – especially during important transactions or transitions. Rick was president of the Harvard Business School Assoc. of Boston and was a management consultant with Arthur D. Little. Rick.Williams@NewportBoardGroup.com / www.RickWilliams100.com

Interviewer - Geri Denterlein

Geri Denterlein is the founder and CEO of Denterlein*, a Boston based strategic communications firm. "Blue-chip" brands in education, health care, real estate development, finance, professional services, and energy are among the firm's clients. Denterlein strengthens clients' value by building their reputation and brand while also helping them weather complex crisis events including cyber breaches. She holds a Master of Public Administration from the Harvard Kennedy School of Government.*

Key Take Away

"As a board member, I am expected to ask the company leaders whether they have put in place policies and procedures that protect the company, its employees, its customers and its assets against cyber attack. But my real responsibility is to be sure these procedures actually work."

Denterlein

Rick, you have served as board member and board chair for a number of organizations. What do you see as the role of the board when addressing cyber security issues?

Williams

The CEO and senior leadership of the company have responsibility for day to day operations including IT and protecting all company assets. The role of the board of directors is to review and guide the work of the company leadership as they address cyber security issues. The board's primary responsibility is the long-term welfare of the company and its owners. The board is also responsible for assuring that the company is in compliance with state and federal laws and regulations.

Cyber security threats challenge the company in several dimensions - loss of IP, loss of reputation and brand value, loss of private customer information damaging the customers, loss of private employee data, possible violations of privacy obligations and others.

Something like 90% of the value of major US corporations comes from their IP and other intangibles. Yet a recent National Association of Corporate Director's report showed less than 10% of both public and private board members are very confident that their companies are secured against cyber attacks. This is a big issue for board members.

The board must be sure that the company leadership understands the profile of cyber risks specific to the company. *With that understanding, the board will ask whether the company has put in place appropriate policies and procedures designed to protect against these attacks and has developed responses in the event of an attack.* And the company must be current with proactive preventative measures as well as passive measures. Looking at the company as a whole and not just the IT department, is the combination of IT technology, employee awareness training, and insurance an appropriate and cost-effective response to the threat?

Denterlein

Do the threats posed by cyber attacks present unique challenges for boards to address?

Williams

The complex nature of cyber threats makes the job of the company's board unusually difficult. Bad actors can get access to the company's systems and assets through the company's online presence, employee emails, and connections to the internet, service contractors' links into the company and subcontractor components connected to the company's products or network. Building appropriate defenses is technically difficult and there are many not obvious pathways available to the bad actors.

The board must ask, "Does the company have defenses in place against cyber attack?" If the answer is a simple "Yes." That should be a red flag. There is no simple solution to the cyber challenge. Finding the proper balance of investment in cyber defenses against the risk of bad guy penetration is difficult. But most companies today are way under protected and don't understand their real vulnerabilities. Look at the list of brand name companies like Target and Sony that thought they were covered but got hacked and lost hundreds of millions of dollars.

Denterlein

What more can the board do?

Williams

Too often, topics like cyber are seen as specialized technical issues to be managed by the IT department. They may have only a passing mention at a board meeting.

As a board member, I am expected to ask the company leaders whether they have put in place policies and procedures that protect the company, its employees, its customers, and its assets against cyber attack. But my real responsibility is to be sure these procedures actually work. Cyber awareness requires a different approach than conventional training in order to bring about behavior change. For example, has the company developed a culture of cyber awareness? Do the ongoing training and awareness programs actually work? Is the company, in fact, developing and maintaining habits and practices from the CEO to shipping room that will keep the cyber criminals out of the company?

The board of directors is not directing the operations of the staff throughout the organization. But the board can challenge the CEO and other leaders to say the right things but also change behavior throughout the organization so the bad guys will have much more difficulty getting access to the assets of the company.

Denterlein

Are boards of directors exposed to liability risks if cyber attacks occur?

Williams

Boards and their members do have some liability exposure if they have not been reasonably diligent in their supervision of the policies and procedures put in place by the company. In cases where customer data has been stolen or the company valuation drops because of a breach, customer or shareholder groups can bring damage claims against the board among others.

I am not giving legal advice here, but my suggestion is that boards be purposeful about getting cyber security updates, providing thoughtful review and feedback to the company and recording these steps in board minutes. The board also needs to make sure that material breaches or liabilities from breaches are publicly disclosed.