ISSUE 113

BOARD PERSPECTIVES: Risk Oversight

SHARPENING THE FOCUS ON CYBERSECURITY

Much has been written, and important insights shared, on cybersecurity. The threat landscape continues to evolve, and the topic remains significant in the boardroom. But is there anything new to talk about?

To gain fresh perspectives on cybersecurity, an important area of board oversight, Protiviti met with 20 active directors during a dinner roundtable at a December 2018 National Association of Corporate Directors (NACD) event to discuss their experiences. Here are some key takeaways from that discussion:

Don't let overinvesting in protection and detection lead to underinvesting in response and recovery. Effective cybersecurity begins with *protection*, followed by *detection*, *identification*, *response* and *recovery*. Using these five cybersecurity pillars, as defined in the NIST framework,[1] Protiviti sponsored and helped produce a global study in which executives were asked to rate their company's progress across these pillars.[2] The survey results indicated that most companies score highest on protection and detection and lowest on identification, response and recovery. As most cybersecurity investments address the protection pillar, the participating directors agreed their organisations need a balanced programme to detect and respond to the inevitable cyber attacks.

[1] The NIST Cybersecurity Framework offers computer security guidance for private sector organisations in the United States. It is available at www.nist.gov/cyberframework.

[2] *The Cybersecurity Imperative: Managing Cyber Risks in a World of Rapid Digital Change*, a joint effort of ESI ThoughtLab, WSJ Pro Cybersecurity, Protiviti and other organisations to conduct rigorous global research and analysis involving, amongst other things, a survey of 1,300 global executives across multiple industries and analytical benchmarking and performance assessment tools. The research is available at http://go.dowjones.com/cybersecurity-imperative.

protiviti®
Face the Future with Confidence

However, most board members report they only see an overall cybersecurity budget; the company's investments across the five NIST domains are not transparent to them.

One board member spoke of a maturity assessment using the NIST framework and of monitoring progress across the five domains to improve them to the desired maturity levels. Overall, it is important for organisations to move beyond the protection pillar when it comes to cybersecurity. The board should work with management to assess and monitor regularly the organisation's ability to identify, detect, respond to and recover from a cyber breach, as well as ensure that appropriate investment is supporting each pillar. One recommended and beneficial step is to conduct scenarios of cyber attacks that might occur and review the results. The outcomes can be enlightening when evaluating cybersecurity response and recovery capabilities.

Understand the paradox in breach detections between cyber "leaders" and "beginners." Protiviti's research finds that digital leaders report more cyber attacks than beginners. The roundtable discussion revealed several reasons, including the likelihood that digital leaders are better at monitoring security activity and have stronger detection measures. Also, they are more likely to have an expanded attack surface due to the new technologies and digitisation capabilities they employ. Organisations need to stay focused and keep cybersecurity a critical priority as they advance their digital maturity. To minimise their risks, companies should build cybersecurity into each step along their digital transformation process.

Manage the "cyber squeeze" on innovation funding. How does the board effectively address cyber risk without throttling innovation? This important question is a double-edged sword, as innovating creates more cyber risk because it almost always involves embracing new digital technologies. The roundtable discussion emphasised that innovation is about business strategy and should not be an IT or "innovation" budget item. Rather, it should be part of an overall budget for the enterprise's growth strategy. Also, risk and cybersecurity should be embedded into the design and developmental approaches — including Agile and DevOps — that innovation teams use, so that innovation is undertaken securely.

Mind the enemy within. According to Protiviti's research, nearly all firms (87 percent) see untrained general staff as the greatest cyber risk to their business because they may provide a conduit for outside attackers. As noted by several directors, there are solutions to help combat internal threats, but the board is typically not aware of how effective they are. Exposure to attacks by nation-states and sophisticated external attackers is compounded in that these groups often exploit untrained insiders. The directors agreed that boards need to turn up the volume on their inquiries of cyber management as to what is being done about insider risk, including exposure to third parties. One tried-and-true, not to mention low-cost, cybersecurity measure — at least for insiders — remains employee training and communication.

Know how much — quantify cyber risk to put a value on the "crown jewels." Quantification will help management and the board significantly as they work to understand the different types of data and information systems assets the organisation maintains and what needs to be protected most so they can oversee how asset protection is being prioritised. The FAIR methodology can assist with this analysis, as it employs risk quantification software to analyse risk using techniques such as the Monte Carlo method, which simulates risk scenarios. Conducting a quantitative risk analysis forces IT and security teams to set risk appetite thresholds, which enhances cybersecurity communications with the board. Cyber risk management, including risk-based decisions, is enhanced if risk is quantified in financial terms.

Increase the board's confidence in its cybersecurity oversight. Cyber threats represent a legitimate concern. A company's reputation established and nurtured for 100 years can suffer severe and lasting damage following just one high-profile cyber attack. As a result, it can be difficult for boards to feel fully confident in how they are monitoring cybersecurity risk, both within the organisation and amongst third parties. The roundtable discussion participants noted that, whilst directors must rely on management for this information, they should be proactive in refreshing the board's oversight capabilities, asking appropriate questions, receiving independent assurances, monitoring focused dashboards, and setting clear expectations regarding the need to preserve reputation and brand image.

Take stock of a changing landscape. Throughout the roundtable discussion, numerous comments were made regarding the changing cyber threat landscape and the importance of staying informed as it evolves (e.g., ransomware, expanding the value of data beyond credit cards, unapproved mobile devices, third-party threats and state-sponsored cyber attacks). The complexity of the evolving threat landscape is prompting a need for increased cooperation and information-sharing between the private and public sectors, an objective that remains elusive due to concerns over disclosing confidential and other sensitive information. The game has now changed. Virtually any organisation is susceptible to cyber attacks, even if it does not harbour customers' personal data or credit card information.

For a more complete look at the NACD roundtable, including key takeaways, read Protiviti's full summary of the event at www.protiviti.com/US-en/insights/active-directors-cybersecurity.

Questions for Boards

The following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Is the company a possible nation-state target based on what it represents, what it does or the value of its IP? If so, does the company have the advanced detection and response capabilities it needs? Given the increasing sophistication of threat actors, are simulations of likely attack activity performed periodically to ensure defences can detect a breach and respond in a timely manner?
- Does the board define its cybersecurity expectations for management and establish clear accountabilities for results? If the organisation has a risk appetite statement, are the board's expectations for cybersecurity incorporated therein?
- Is the board satisfied with the reporting and metrics used by management for cyber matters? Do the metrics provide supporting key performance and risk indicators as to how top-priority cyber risks are managed, and address areas that inform the board's oversight? Are the metrics refined over time to provide added insights as threats change?

For more questions for boards to consider, read Protiviti's full summary at www.protiviti.com/US-en/insights/active-directors-cybersecurity.

How Protiviti Can Help

Protiviti works with organisations to focus on foundational information security questions:

- Do we know what the most important data and information systems assets are (the "crown jewels") and where they are located? Concerning these assets, are we properly caring for them, who are we protecting them from, are our defences working as intended, to whom should we permit access, and how do we know?
- Can we recognise a new cyber threat and detect likely attack techniques on a timely basis? If so, are we able to align our protection measures to meet the threat?
- When incidents occur, are we able to keep them from happening again?

Protiviti provides a wide variety of security and privacy assessment, architecture, transformation, and management services to help organisations identify and address security and privacy exposures before they become problems. Working with companies in all industries, we evaluate the maturity of their information security programmes and the efficacy of their controls — and help them design and build improvements when needed. We have a demonstrated track record of helping companies react to security incidents with world-class incident response, establish proactive security programmes, deal with identity and access management, and handle industry-specific data security and privacy issues.

Is It Time for Your Board to Evaluate Its Risk Oversight Process?

The TBI Protiviti Board Risk Oversight Meter™ provides boards with an opportunity to refresh their risk oversight process to ensure it's focused sharply on the opportunities and risks that truly matter. Protiviti's commitment to facilitating continuous process improvement to enable companies to confidently face the future is why we collaborated with The Board Institute, Inc. (TBI) to offer the director community a flexible, cost-effective tool that assists boards in their periodic self-evaluation of the board's risk oversight and mirrors the way many directors prefer to conduct self-evaluations. Boards interested in using this evaluation tool should visit the TBI website at http://theboardinstitute.com/board-risk-meter/.

Learn more at
www.protiviti.com/boardriskoversightmeter

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti partners with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on https://blog.nacdonline.org/authors/42/. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* are consolidated into a printed booklet that is co-branded with NACD. Protiviti also posts these articles at protiviti.com.

protiviti®