The new mindset in cyber security: The board lens

Has the cyber risk and security conversation in the boardroom kept pace with the business? Better yet, does the board have the assurance that operations, technology, and risk management are communicating on cyber expectations and priorities?

On the most recent KPMG/NACD Audit Committee Webcast, KPMG Global Cyber Security Co-Leader Greg Bell detailed the components of a cyber maturity framework that can help corporate directors assess the cyber capabilities of their companies.

"Cyber is much more about your company's business strategy and innovation plans than about technology architecture," said Bell. "When companies talk about cyber risk, that should be the lens."

"We're doing business differently. It's very rare that all of a company's business functions exist within their own walls," said Bell. "Supply chains, business partners, and outsourcing relationships are all handling the company's critical data, including customer data. How do we protect that information and ensure that we are providing due care?"

For example, Bell recounted separate meetings—held within hours of each other—in which executives at the same company detailed their respective approaches to the use of third-party brokers and agents to acquire new customers. The technology executive was preparing to overhaul the company's systems to defend against cyber hacks of customer information via the third party's technology infrastructure. Meanwhile, the business executive had already set plans in place to eliminate third parties altogether.

"The business was moving at such a fast pace that cyber capability just couldn't catch up," said Bell. "That's the risk we all face today." In fact, of the key cyber-related risks identified in a recent Audit Committee Institute survey, technology systems was only one of the top four challenges. The other three were business-focused: supply-chain vulnerability, people risk, and organizational awareness.

The Cyber Maturity Framework

Existing cyber security frameworks focus very little on governance and the role of the board, said Bell. Extending the reach of a company's existing cyber security framework to the board can both define and clarify how the board engages with management on cyber issues.

"The most important element is leadership and governance," said Bell. "How is the technology organization aligned with the business? Management really needs to make sure they can explain that to the board."

Bell discussed lines of inquiry across six areas of board oversight as well as related key performance indicators (KPIs) that can serve as a dashboard to help the board assess the cyber environment.

Board oversight	Lines of inquiry	How does the board gain comfort? (Example KPIs)
Leadership and governance	Understand governance structure and meet executive leadership team Review output of capability assessment Review and approve strategy and funding requests Participate in general board education Request periodic updates of program	Security spend as a percentage of overall IT budget Capability maturity review output Certifications within key leadership positions Number of board education sessions (frequency)
Human factors	Set the tone for the culture Review patterns/trends of personnel issues Understand training and awareness protocols	Percentage of employee/contractors attending training Trends related to cyber from whistleblower or ethics hotline
Information management	Understand risk management approach and linkage to enterprise risk Review and approve risk tolerance Understand third-party supplier program Review and question program metrics	Risk assessment output/linkage to ERM program Risk tolerance measures and metrics Number of high-risk third-party suppliers and review status Review metric output
Business continuity and crisis management	Understand current response capability Review status of overall plan maturity Meet with communications personnel Participate in table-top exercises	Number of mission critical business processes with plans in place Number of table top exercises (frequency) and results
Operations and technology	Understand current maturity of control structure Review relevancy of selected control framework Review relevant incident trend metrics Meet with CIO or equivalent to understand integration of cyber and information technology trends	Percentage of "crown-jewel" assets included in monitoring coverage Risk rating of security vulnerabilities (considering asset value) Cyber incident trends metrics
Legal and compliance	Understand regulatory landscape impacting the organization Clarify audit committee requirements for cyber Review litigating inventory trends Review and approve cyber insurance funding (if relevant)	Open regulatory and/or litigation matters Cyber insurance policy benchmarking with peer organizations

Insights for Directors

Directors need to stay vigilant, but it is more important to stay focused. This is an area that could take up a lot of energy and time. While it is clear that cyber risk is a fact of doing business today—it is going to continue to evolve and pose new challenges.

Boards should consider the following in their discussions with management:

Learn to live with cyber risk. Understand that it is an enterprise-wide challenge and opportunity.

— Cyber is a business issue that impacts the enterprise—strategy, operations, the supply chain, regulation, reputation and more.

— Regular reporting and communications to the board is critical, ideally with a dashboard and robust KPIs. Establish a rhythm, get to know the people, become better educated.

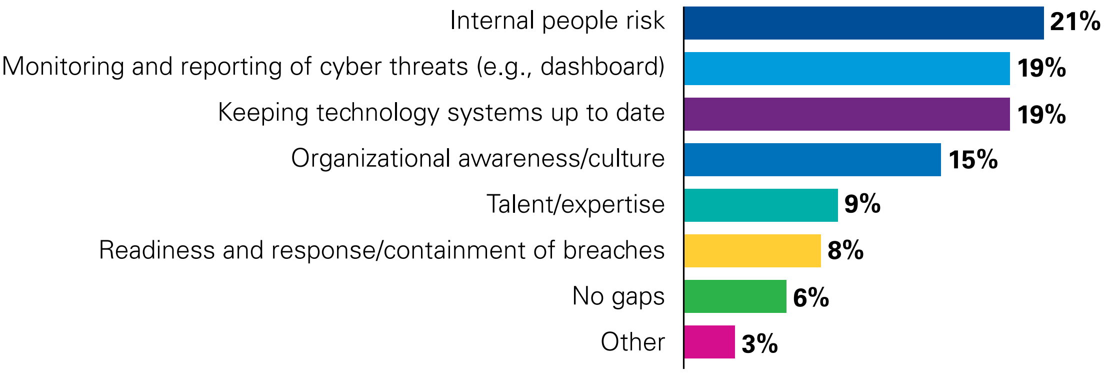
— It's about culture and tone at the top. Are the executives from the CEO on down making their voices heard about the importance of good cyber hygiene?

Stay abreast of industry practices and connect with law enforcement. How attuned is the board to industry trends and best practices? Is the company reaching out to law enforcement agencies proactively to understand trends in cyber risk and response?

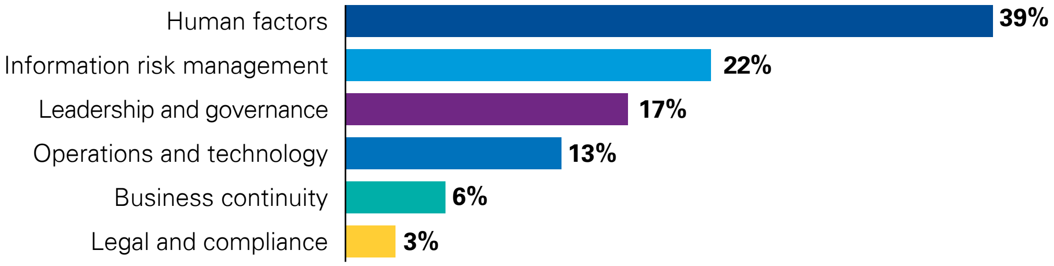
Have an incident readiness and response plan. Breaches will happen. Does the company have a clear "table-topped" response plan that has been reviewed and tested? Who leads the cyber incident response team? What about business continuity plans?

Webcast Survey Results

From a board perspective, what is the most significant gap in your company's ability to manage cyber risk?



From a board perspective, which aspect of this cyber maturity framework is the most challenging to monitor and assess?



Source: 310 directors and executives surveyed during the March 23 Webcast.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center champions outstanding governance to help drive long-term corporate value and enhance investor confidence. Through an array of programs and perspectives—including KPMG's Audit Committee Institute and Private Markets Group, the WomenCorporateDirectors Foundation, and more—the Center engages with directors and business leaders to help articulate their challenges and promote continuous improvement. Drawing on insights from KPMG professionals and governance experts worldwide, the Center delivers practical thought leadership—on risk and strategy, talent and technology, globalization and compliance, financial reporting and audit quality, and more—all through a board lens. Learn more at kpmg.com/blc.

Audit Committee Institute

Part of the Board Leadership Center, KPMG's Audit Committee Institute focuses on oversight of financial reporting and audit quality and other issues of interest to audit committee members, including risk oversight, internal controls, and compliance. Learn more at kpmg.com/aci.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.