KPMG

Top cyber security considerations in 2019

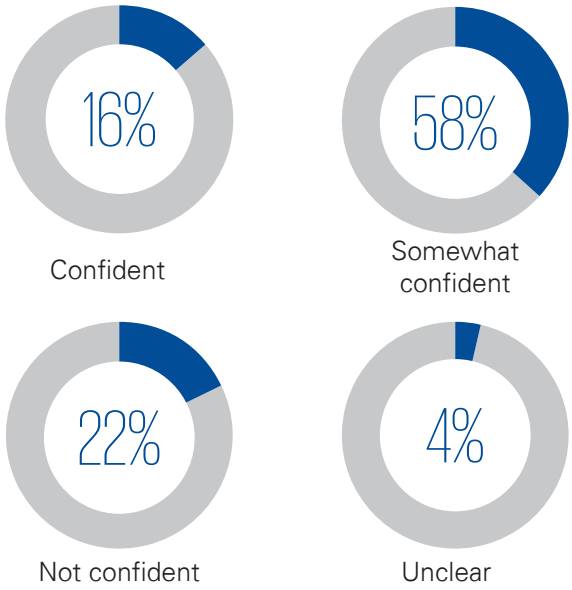
Cyber security efforts continue to evolve from keeping out the "bad guys" to making cyber security an integral part of the company's broader risk management effort.

"It's time for a change in how we look at cyber risk," said Charlie Jacco, principal, KPMG Cyber Security Services. Jacco joined Fred Rica, principal, KPMG Cyber Security Services, and Jose Rodriguez, leader of KPMG's Audit Committee Institute, to discuss the top cyber security issues for boards during KPMG's March Quarterly Audit Committee Webcast.

Several factors have propelled an increased focus on cyber security and information protection in recent years: rapid shifts in technology, the growing volume and sophistication of threats, the ongoing migration to automated and cloud-based services, the explosion of and focus on data, and more rigorous regulatory requirements. From a board perspective, there are six critical issues to consider, according to Jacco and Rica.

Skills shortage. "One of the biggest problems today is the absolute shortage of talent in the cyber space," said Rica. Of 605 directors and executives surveyed during the webcast, only 16 percent said they are confident that their company has the talent required to keep pace with cyber security risks. Rica noted that many internal audit departments are working to ramp up their skill sets to do robust and independent assessments of the cyber security program. The role of the chief information security officer (CISO) has also changed dramatically in the last two to three years. "The best CISOs are business savvy. They understand how to translate cyber security into business enablement," said Rica. "And they're helping to show how a good cyber program can improve a company's business results."

How confident are you that your company has the talent required to keep pace with cyber security risks?



Of 605 directors and executives surveyed during the March 21, 2019 KPMG Quarterly Webcast.

The dearth of adequately trained, appropriately skilled personnel to protect vital processes, intellectual property, and sensitive data is an issue across virtually every industry. Boards should pay attention to the company's cyber talent plan and ask management about efforts to automate tasks that are manual and time consuming and to reprioritize people to focus on more strategic activities instead of rote tasks.

Artificial intelligence (AI). AI has the ability to correlate numerous data sources to identify patterns or anomalies that might point to malicious activities. How are company leadership and cyber professionals thinking about AI and security in general in the context of the organization's longer-term platform strategy?

"Just like AI being used to attack the perimeter of an organization—or, once they're in, learn the patterns of where to put the bad malware—defense is working the same way," said Jacco. "Imagine a firewall being able to defend itself on the fly, based on a pattern it sees."

Still, it's important to remember that "technology alone has never solved the cyber security problem," said Rica. Forward-thinking organizations are focusing on the most important assets—the company's crown jewels—and applying controls appropriately against those crown jewels to make sure the most important data is the most protected, said Rica. "That's a philosophical shift that we've seen over the last two or three years in how organizations build their defenses."

Data privacy compliance. The board's view of data privacy sets the tone for the way privacy is addressed throughout the entire company. Full engagement across the organization is required as security professionals look to embed privacy into the DNA of business operations and customer engagement. A strategic approach to privacy and information governance can reduce the overall cost of compliance and enhance customer trust.

In light of new data privacy regulations such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act, "consumers are rightfully demanding more of an idea on how a given firm is protecting their information" and how they are using it, said Jacco. Companies need to know where all of their data is and understand what business processes are using it so they can give people in those jurisdictions the right to opt in or out. That exercise can be a significant challenge.

Fraud risk and cyber risk. Fraud and cyber should garner equal attention from a security perspective. New and improved strategies for collecting and leveraging client data, particularly authentication data, should be in the pipeline. Is the company doing enough to understand the customer's typical behavior, recognize anomalies, and, in turn, educate customers about the value of using personally identifiable information conscientiously to prevent fraudulent activity?

Authentication. Identity and access management is evolving from a security-driven initiative to a driver of business enablement. Directors should probe management about what the company is doing in the areas of advanced authentication, identity proofing, fraud, and analytics, including a move away from passwords to biometric-enabled apps.

"From a security perspective, the notion of opting in and opting out is going to become very important," said Rica. For example, companies that deploy 5G technology will need to help their customers make informed decisions about giving up their data and what they're giving it up in exchange for, whether it's convenience, flexibility, or ease of use.

Phishing. Despite the growing sophistication of today's attack methods, phishing remains one of the toughest threats to defend. A key differentiator will be internal analysts who are constantly engaged, tuning the networking as the business, and the threats, evolve. The cyber team must be out in front.

Key questions to drive robust boardroom discussions about cyber security

- How frequently is the maturity of the company's cyber security risk management framework evaluated?
- How is the company keeping up with regulatory changes and new legal requirements?
- Is the company staying abreast of industry practices and connecting with law enforcement?
- Does the company have an incident readiness and response plan that has been reviewed and tested?
- Is the board getting the information it needs (e.g., a cyber dashboard) to oversee cyber security efforts?
- Does the company have the talent it needs to keep pace with evolving cyber security threats?

"While the technologies to try to stop [phishing] will continually evolve…the best thing you can do to combat this is to have really good training and awareness programs around what to look for," said Jacco.

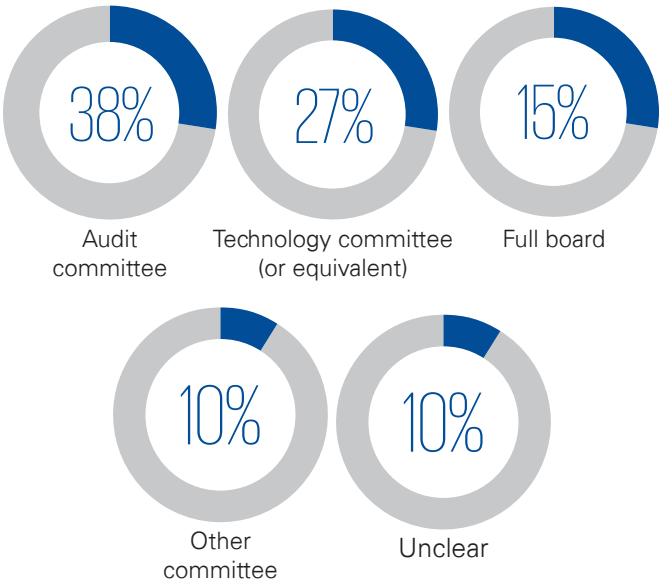
Rica concurred. "When clients ask me: if I have one more dollar to spend on security, where should I spend it? My answer has not changed in 30 years. Spend it on training and awareness. You get a huge return on that," he said.

Rica concluded, "When you think about a cyber program, whether you're an audit committee [member], board [member], or internal auditor, there are three questions you have to be comfortable answering: What are we doing? Is it enough? And how do we know?"

Watch the complete webcast replay at kpmg.com/us/aciwebcast.

Read What's next: Key cyber security considerations for 2019.

Which of the following devotes the most agenda time to cyber security issues?



Of 605 directors and executives surveyed during the March 21, 2019 KPMG Quarterly 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, the WomenCorporateDirectors Foundation, and more—the Center engages with directors and business leaders to help articulate their challenges and promote continuous improvement of public- and private-company governance. 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/us/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/us/aci*.

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

kpmg.com/socialmedia

Contact us

kpmg.com/us/blc
T: 1-800-808-5764
E: us-kpmgmktblc@kpmg.com