



## What CEOs need to know about Cyber Security today?

Kiran Mantha, Principal

Deloitte Cyber Risk Service

Email: [kmantha@deloitte.com](mailto:kmantha@deloitte.com) | Cell: 201 362 1236 | <http://deloitte.com/us/cyber>

**In the digital age, cyber is everywhere.** Which means cyber risk now permeates nearly every aspect of how we live and work. Increased use of technology and globalization are key drivers of cyber risk, but they are also key sources of competitive advantage. As the world becomes more connected, cyber threats are growing in number and complexity. Cyber is moving in new directions – beyond and organization’s walls and IT environments. Cyber today isn’t merely a technology issue. It’s a strategic business risk that will continue to affect every facet of every organization.

The ever-increasing attack surface, challenges related to legacy systems and technical debt, talent shortages, and visibility blind spots continue to compound the problem for organizations to effectively managing Cyber risk. Ransomware, supply chain security, business email compromise, and insider threat continue to dominate the news cycles.

Cyber risk is an imperative for everyone within the enterprise—but ultimate responsibility for overseeing risk rests with top leaders. Many board members and C-suite executives, however, are far removed from the day-to-day challenges of monitoring, detecting, and responding to evolving cyber risks. Effective cyber risk management starts with awareness at the board and C-suite level.

Realizing that at some point the organization will be breached, leaders should work to understand the most significant threats and how those threats can put mission-critical assets at risk. As the C-suite take a more active role in protecting their organizations, many will struggle to ensure that their efforts are effective. What are their

- 
1. Do we demonstrate due diligence, ownership, and effective management of cyber risk?
  2. Do we have the right leader and organizational talent?
  3. Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?
  4. Are we focused on, and investing in, the right things? And, if so, how do we evaluate and measure the results of our decisions?
  5. How do our cyber risk program and capabilities align to industry standards and peer organizations?
  6. Do we have a cyber-focused mindset and cyber-conscious culture organization wide?
  7. What have we done to protect the organization against third-party cyber risks?
  8. Can we rapidly contain damages and mobilize response resources when a cyber incident occurs?
  9. How do we evaluate the effectiveness of our organization's cyber risk program?
  10. Are we a strong and secure link in the highly connected ecosystems in which we operate?

responsibilities? Which competencies should they be cultivating? What are the right questions to ask? Faced with such questions and an evolving threat landscape, preparing for every possibility can prove daunting. So, planning for what’s probable—not just possible—offers a prudent path forward for leaders.

CEOs need to drive cyber awareness and organization wide “Tone at the Top” by participating in organizational awareness programs demonstrating due diligence, ownership, and effective governance of cyber risk. One way to accomplish this is by instituting a metrics driven conversation between the CEO/Board and IT and asking the right questions at the right time.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

Copyright © 2022 Deloitte Development LLC. All rights reserved.