5 insights you should know

Boards and stakeholders are asking more questions about cyber risks, including types of attacks, current cybersecurity capabilities, protection strategies, damage possibilities, and how to best evaluate the effectiveness of their organization’s cybersecurity program.

Board members and senior leaders want confidence in the security of their assets and a better understanding of how cyber events might disrupt the business—and they are increasingly looking to CAEs to provide this assurance.

Many CAEs are on the front lines providing credible, real-time risk-related advice and leading practices to management on strategic priorities such as product launches, new technology plays, and other digital transformations that could impact their company’s cyber risk posture.

Every organization’s pace of digital transformation (e.g., ERP, cloud-based systems) is unique and potentially introduces new cyber risks, but understanding digital transformation enables IA to anticipate emerging risks and deliver forward-looking cyber insights.

When examining current and future roles in addressing cyber threats, IA can help organizations accelerate change by focusing on organizational learning, management action, and remediation improvements with other potential solutions.

5 actions you can take

1. To be strategic and proactive, internal audit should prepare for and respond well to board questions about cybersecurity, current assessments, and necessary cyber resources to prioritize relevant cyber risk initiatives that elevate IA’s value and impact on the organization.

2. IA can leverage recognized frameworks such as the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO) to establish a baseline understanding of cyber program maturity and utilize leading security certification and third-party assurance efforts to highlight compliance with policies and practices.

3. Audit at the speed of risk by collaborating with the business and IT around strategic priorities, pivoting to emerging risks, recruiting new talent for specialized skills, and innovating to meet the challenges of a cyber risk landscape.

4. CAEs should shift to continuous, dynamic risk assessments flexible enough to incorporate new risk domains and sources of unstructured data that help IA anticipate and respond to the most significant risks—which often include cyber threats.

5. Accelerate improvements and solutions with innovative e-learning techniques such as virtual reality and gamification or by assembling a team to uncover root causes of cyber concerns and share new perspectives.
Internal Audit Opportunities:

- Performing risk-based cyber audits to identify emerging cyber risks and threats.
- Performing peer benchmarking to identify control areas that are secure, and exposed—and measuring against industry peers.
- Leading security certifications and third-party assurance efforts (e.g., ISO 27001).
- Delivering advice and recommendations related to system implementations and transformations.
- Performing assessment of cyber network endpoint security, compliance monitoring, and key configurations.
- Identifying business-critical activities, products and services, and reviewing programs with contingency plans for third-party risk management higher risk third parties.

For more information, or to explore insights visit: Internal Audit: Risks and Opportunities in 2022

Contact us:

Sarah Fedele
Internal Audit Managing Principal
Deloitte & Touche LLP
sarahfedele@deloitte.com

Pete Low
IT IA Managing Director
Deloitte & Touche LLP
plow@deloitte.com

Vipul Patel
Managing Director
Deloitte & Touche LLP
vbpatel@deloitte.com

Geoffrey Kovesdy
Principal
Deloitte & Touche LLP
gkovesdy@deloitte.com