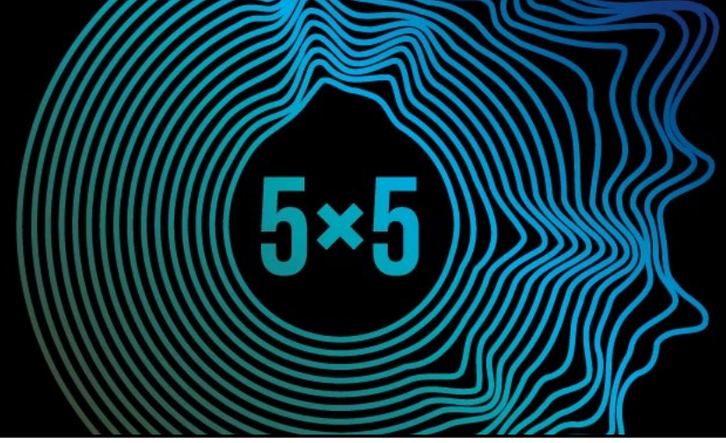
Deloitte.

Internal audit's role in cybersecurity

Internal audit megatrends | 5x5 series: Insights and actions



Today's internal audit (IA) teams and chief audit executives (CAEs) have a lot on their plate as they work to navigate the growing complexities within the cyber environment. Aside from rapidly growing systems, interconnected regulations, and increased risks—worldwide cybercrime costs are estimated to hit $10.5 trillion annually by 2025[1]. As organisations find difficulty in being able to keep pace with attacks, many are bolstering their defences, which go far beyond the chief information and security officer and their offices. CAEs are now relied upon to provide an independent and objective assessment of their organisation's cyber risk management practices and capabilities. In response, many are transforming their traditional audit and assurance role by further educating themselves and building more tech-savvy teams to join the cybersecurity fight. For organisations looking to introduce initiatives or boost efforts around cybercrime and cybersecurity, here are five insights to consider and five actions you can take.

[1] Why we need global rules to crack down on cybercrime accessed Jan 2, 2023.

5 insights you should know

1. 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 organisation's cybersecurity program.**

2. 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.**

3. 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.

4. Every organisation'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.**

5. When examining current and future roles in addressing cyber threats, IA can help organisations **accelerate change by focusing on organisational 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 prioritise relevant cyber risk initiatives that elevate IA's value and impact on the organisation.

2. IA **can leverage recognised frameworks such as the National Institute of Standards and Technology (NIST) or the International Organisation for Standardisation (ISO) to establish a baseline understanding of cyber program maturity** and utilise 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 specialised 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

5×5

Performing risk-based cyber audits to identify emerging cyber risks and threats.

Delivering advice and recommendations related to system implementations and transformations.

Performing peer benchmarking to identify control areas that are secure, and exposed—and measuring against industry peers.

Performing assessment of cyber network endpoint security, compliance monitoring, and key configurations.

Gap assessments against NIST, ISO or other relevant recognised frameworks

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:
2023 Global Future of Cyber Survey

Contact us:

Ian Coppini
Director Risk Advisory
Deloitte Advisory & Technology Ltd.
Phone:+356 2343 2444
Email: icoppini@deloitte.com.mt

Rafael Moreira
Manager Risk Advisory
Deloitte Advisory & Technology Ltd.
Phone: +356 2343 2328
Email: ramoreira@deloitte.com.mt