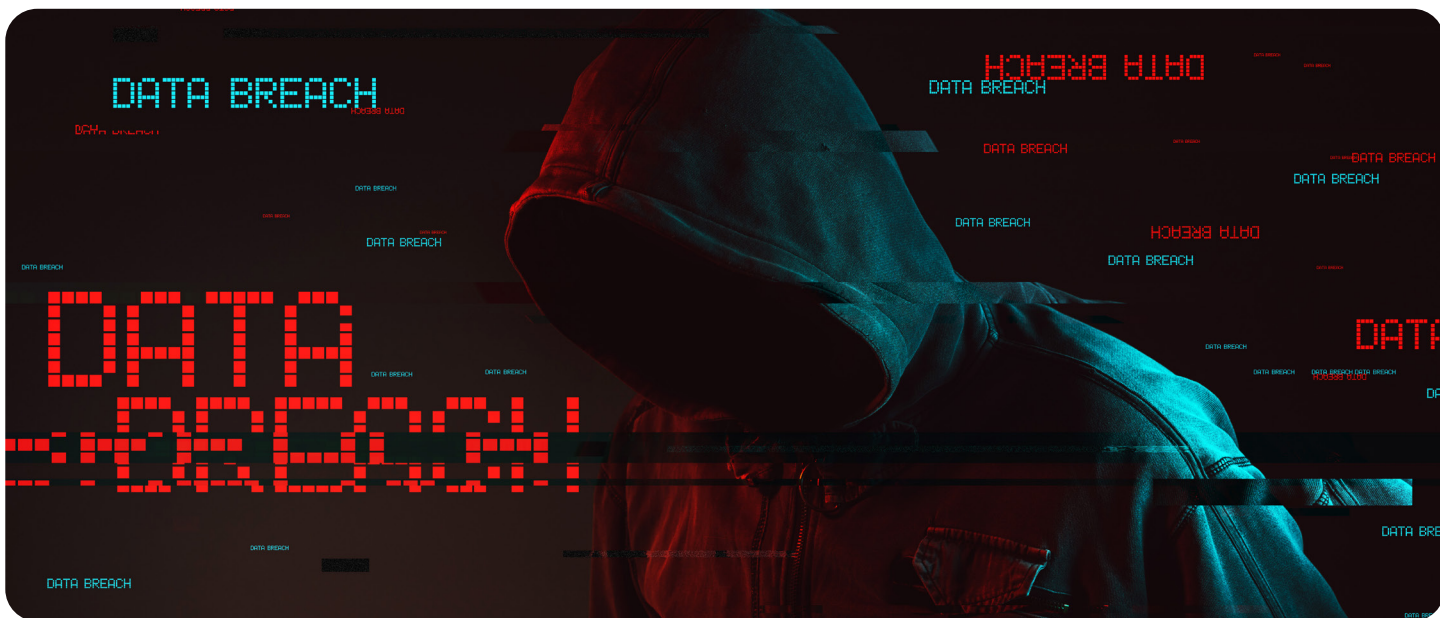


— TONE — at the — TOP[®]

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 137 | October 2026



From Breach to Boardroom: Strengthening Cybersecurity Oversight

In February 2024, a ransomware attack on Change Healthcare, a UnitedHealth Group subsidiary, halted claims and payment processing across much of the U.S. healthcare system. The damage: [\\$2.2 billion in direct response costs](#), another \$867 million in business disruption, and roughly 190 million people affected.

The entry point was a portal without multifactor authentication — a baseline security control, as CEO Andrew Witty [acknowledged](#) before the Senate Finance Committee. Chair Ron Wyden put the blame at the top, arguing in his [opening statement](#) that the company needed a genuine cybersecurity expert on its board.

That is no longer just a talking point. In a string of [2025 decisions](#), the Delaware Court of Chancery held that cybersecurity is a “mission critical” risk boards cannot simply delegate to management. Directors are now expected to receive regular briefings, and missing minutes on those discussions can itself suggest a failure of oversight.

This is not a risk going away any time soon. In The IIA’s [2026/2027 Risk in Focus Report](#), 80% of internal audit leaders selected cybersecurity as one of the top five risks facing their organization, up 7% from 2025 and 22% higher than the second most-selected risk, digital disruption (including AI).

Clearly, cybersecurity is a critical area that requires the utmost attention from the very top of the organization. Board members have an obligation to treat cyber-risk oversight as part of their duties and develop adequate expertise to carry them out.

This Tone at the Top examines potential gaps in organizations’ cybersecurity efforts, the expanding range of cybersecurity governance disclosures, and how internal auditors can help boards address their governance responsibilities in this area.

A Work in Progress

Cybersecurity has evolved from being a strictly technical concern into one of the central business risks facing modern enterprises. As CrowdStrike notes in its report, [Cybersecurity Risk Oversight: A Governance Guide for Board Directors](#), today's boards have seen cybersecurity shift "from a compliance exercise into a core governance mandate."

How organizations are treating cybersecurity disclosures provides a clear example of this shift. The U.S. Securities and Exchange Commission established [rules on cybersecurity disclosures](#) in 2023, but many organizations go further by voluntarily providing details on cybersecurity oversight and board expertise.

Indeed, as investors and stakeholders continue to demand more cybersecurity oversight information, [an analysis of large-cap companies](#) by EY found significant increases in disclosures in many areas over recent years. Key findings of EY's research include:

- Seventy-eight percent of companies say audit committees are responsible for cybersecurity oversight.
- Eighty-six percent say they disclose cybersecurity as an area of expertise a director has or that the board seeks — up from 53% in 2019.
- Seventy-three percent are aligning their cybersecurity efforts with an external framework, such as NIST CSF 2.0 or ISO 27001.

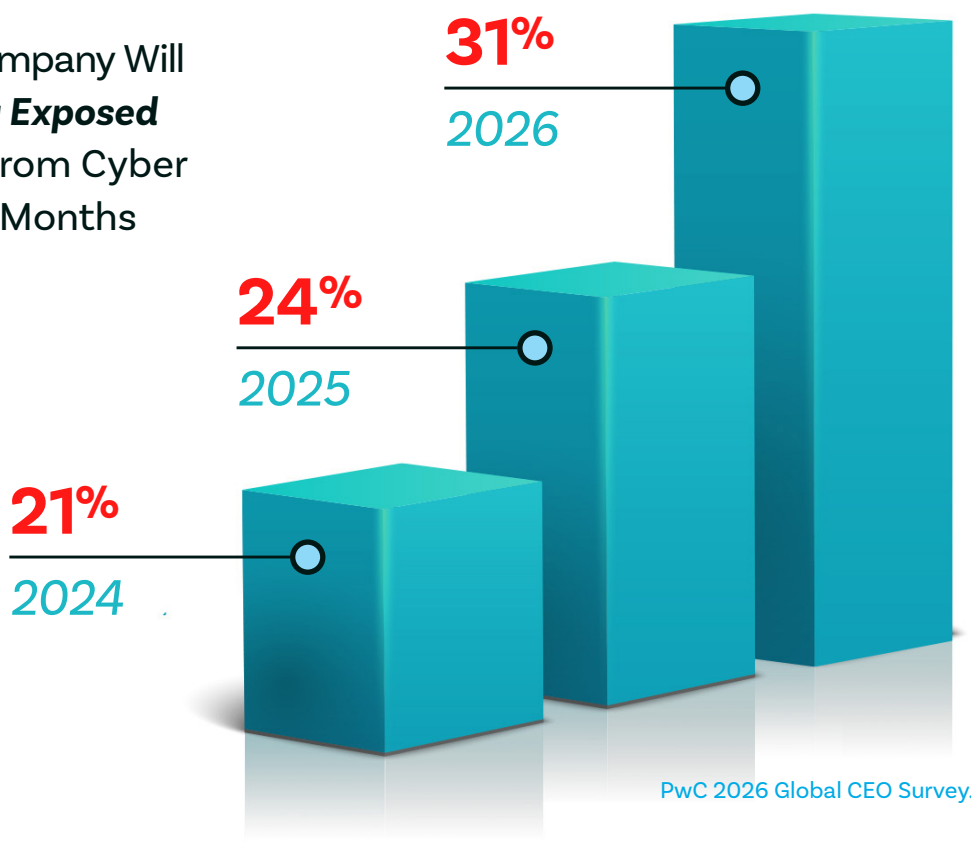
- Fifty-eight percent are performing cybersecurity preparedness activities, including simulations, tabletop exercises, or response readiness tests — an increase from 3% in 2019.

However, while organizations clearly are taking cyber risks seriously, significant gaps exist in their ability to keep pace with the speed of the risk. This can be seen, for example, in their use and understanding of AI, which remains a work in progress at best.

According to Workiva's [2026 Midyear Executive Benchmark Survey](#), 84% of executives say they are at least somewhat confident in the accuracy of AI output even with no human review involved. At the same time, 26% say that internal audits have detected AI errors that reached external audiences or board members. These results indicate a potential disconnect between executives' assumptions about AI and the reality of how it is functioning within their own organizations.

"As AI reshapes the enterprise at unprecedented speed, a new risk is emerging," says Workiva. "[T]ransformation could be outpacing the instincts of the leaders tasked with overseeing it."

CEOs Who Say Their Company Will
Be Highly or Extremely Exposed
to Significant Losses From Cyber
Threats in the Next 12 Months



About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

.....

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

.....

Complimentary Subscriptions

Visit theiia.org/Tone to sign up for your complimentary subscription.

.....

Reader Feedback

Send questions/comments to Tone@theiia.org.

.....



Internal Auditors' Place in the Cyber Discussion

The internal audit function is a valuable partner in organizational efforts to mitigate cybersecurity risks. The IIA's [Cybersecurity Topical Requirement and related User Guide](#) can be an essential resource that clearly illustrates what internal audit's role should be in the cybersecurity risk management plan – and what it must be to maintain conformance with the Global Internal Audit Standards.

The Requirement is designed to provide “a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management, and control processes.” To this end, internal audit has a duty to assess three key areas:

- Governance: Clearly defined basic cybersecurity objectives and strategies that support organizational goals, policies, and procedures.
- Risk Management: Processes to identify, analyze, manage, and monitor cyber threats, including a process to escalate cyber risks promptly.
- Controls: Management-established, periodically evaluated control processes to mitigate cyber risk.

Regarding cybersecurity governance, the Topical Requirement maps governance requirements to appropriate frameworks. An understanding of such frameworks should be a critical component of the audit committee's and board's knowledge base regarding the organization's cyber risk management plan. Additionally, the Requirement calls for internal audit to review how the governance processes are applied to cybersecurity objectives, including the existence of:

- Formalized plans and objectives.
- Policies, procedures, and other relevant documentation used to manage cybersecurity processes.
- Roles and responsibilities that support the achievement of cybersecurity objectives, and whether the cybersecurity function reports to a high-enough level in the organization to attain sufficient support and visibility.
- Evidence of engagement with relevant stakeholders within and outside the organization.

Taken together, these requirements should give boards and audit committees a clear picture of what to expect from internal audit on cybersecurity. Plus, because these requirements are mandatory for conformance with the Global Internal Audit Standards, board members can be confident that a conforming internal audit function is maximizing the value it can provide.

Growing Attention to Cyber Concerns

The telecommunications industry is one of many sectors grappling with cybersecurity risk, and recent advocacy advancements in this area provide a useful case study for helping boards understand how valuable internal audit can be in this space.

Hazards in the telecommunications industry include “machine-speed cyberattacks,” as well as generally slow responses from security operations to emerging threats, according to EY’s “How Telecoms Can Dial Up Cybersecurity in the Age of AI Attacks.”

Legislation recently enacted in Canada enhances the government’s ability to protect the country’s telecommunications system from such hazards. It requires operators of critical cyber systems in sectors regulated by the federal government to take necessary steps to protect their cyber infrastructure.

In its [comments](#) on what would become Canada’s [Critical Cyber Systems Protection Act](#), The IIA notes the need to develop effective processes to identify and mitigate potential cyber risks for organizations, as well as ensure the presence of appropriate internal controls and independent assurance procedures. The act calls for “an internal audit at a designated operator regulated pursuant to this legislation.”

Cyber regulations in other jurisdictions include:

- U.S.: [Cyber Incident Reporting for Critical Infrastructure Act of 2022](#).
- European Union: [NIS2 Directive](#).
- U.K.: [Network and Information Systems Regulations 2018](#).

Boards Need the Internal Audit Perspective

Cybersecurity is a vast and, at times, overwhelming subject for any organization to consider. With all the technical and evolving variables at play, boards will need to rely on sound governance and reporting structures to ensure they are given the clearest, most accurate, and most relevant information possible. To this end, there is no function better positioned to effectively contribute to the discussion than internal audit.

