Global Audit Committee Center

The Institute of Internal Auditors

AUDIT COMMITTEE BRIEFING SERIES: CYBERSECURITY

How Internal Audit Can Help Fight Cybercrime

November 2026

Practical boardroom-ready insights for audit committees.

Executive Summary

Cybersecurity—and the pervasive threat that it poses for organizations—is one of the most important risks that boards and audit committees must deal with today. Against this backdrop, every audit committee should be asking: **How confident are we in our cyber controls?**

Cybercrime continues to have a devastating effect on a broad range of organizations worldwide.

- A wave of highly disruptive cyberattacks targeting refrigeration systems at European supermarkets caused tens of millions of dollars in damage, leading to massive food spoilage, equipment failures, and isolated fires. Authorities have formally attributed the campaign to state-sponsored hackers.
- Organizations around the globe recently went into crisis mode after Amazon reported that it had suffered AI-driven cyberattacks by bad actors weaponizing security vulnerabilities in widely used internet software.
- Recently, Microsoft and partners dismantled three phishing kits associated with over 1 billion scam messages to over 75,000 organizations.
- Last year, the Bank of England attributed weaker-than-expected UK GDP growth at least in part to the fallout from a roughly £2 billion (about $2.7 billion) cyberattack at Jaguar Land Rover.

6 Questions Every Audit Committee or Board Should Ask Internal Audit

- Is cybersecurity incorporated into the audit plan? Does the plan translate current cyber risk assessment into auditable organizational impacts? Are there refresh points?
- Do the organization's cybersecurity efforts reflect current and expected risk, risk appetite, and shareholder expectations?
- Are the organization's controls over cybersecurity effective? If not, what changes are needed?
- Does the organization comply with the governance, risk management, and control process expectations in The IIA's Cybersecurity Topical Requirement?
- Does internal audit's cybersecurity coverage include areas such as AI, cloud, operational technology, software patching and updates, multi-factor authentication, employee awareness of phishing and cyber concerns, third party risks, resilience, recovery, communication, and fraud?
- What are the high-risk areas associated with the organization's AI use?

Internal audit is uniquely placed to provide independent assurance that cyber controls are strong and effective, as well as advisory services that can help strengthen boards and audit committees' cyber governance.

©2026 The Institute of Internal Auditors. All rights reserved. For individual use only.

A Business-Critical Governance Issue

89%	62%	$2.7bn
year-over-year increase in cyber-attacks by AI-enabled adversaries	of confirmed data breaches involved the unintentional human element	estimated cost of the Jaguar Land Rover cyber-attack

Chief audit executives and directors around the world consistently choose cybersecurity as the dominant business threat worldwide, according to Risk in Focus 2026/2027, The Internal Audit Foundation's annual examination of the most significant threats in the global business environment.

Digital disruption, including AI, was in second place this year, moving up 10 percentage points since 2025. While AI can be a valuable resource in fighting cybercrime, new technologies have also become a powerful weapon for bad actors. They use it to "accelerate, optimize, and troubleshoot their existing techniques," according to CrowdStrike's 2026 Global Threat Report. Last year, AI-enabled adversaries increased attacks by 89% year-over-year, the company said.

These developments create a new governance imperative. "Directors today must oversee cybersecurity in the same disciplined way they oversee financial, operational, and strategic risks," said Peter Gleason, NACD President and CEO. However, boards and audit committees often struggle to build strong cybersecurity governance, including gaining assurance over the effectiveness of cyber controls and risk management.

Internal audit is a critical resource in meeting cybersecurity responsibilities and harnessing new technologies. Among other things, "internal audit can be a key mechanism to help understand and assess whether the company's AI governance and related risk management programs are effective," according to a PwC article on the Harvard Law School Forum on Corporate Governance.

A Deeply Intertwined Global Risk Environment

The Risk in Focus findings illustrate the increasingly interconnected nature of organizational risk. The top three challenges—cybersecurity, digital disruption and geopolitical and macroeconomic uncertainty—have direct or indirect impacts on other key areas, such as fraud, human capital, regulatory obligations, and market competition.

> ***"The challenge for organizations is no longer simply identifying individual risks, but understanding how they interconnect, how quickly their impact can spread across the enterprise, and whether governance, internal audit and decision-making are keeping pace"***
>
> Anthony Pugliese, CIA, CPA, CGMA, CITP, President and CEO of The Institute of Internal Auditors

©2026 The Institute of Internal Auditors. All rights reserved. For individual use only.

One example of these interconnections is hostile actors' or nation states' use of cyberattacks to cause economic disruption. Another is supply-chain and third-, fourth- and fifth-party risk. Organizations typically outsource functions such as cloud infrastructure, software development, call centers, logistics, and even core finance or human resources processes. Internal audit can assess related financial, operational, compliance and reputational risks and audit the cyber defenses of critical suppliers. The IIA's Third-Party Topical Requirement provides them with valuable information in this effort.

To underscore the point, Stuart Machin, CEO of UK retailer Marks & Spencer (M&S), described the moment he learned the company had suffered a devastating cyberattack in 2025: "I went into shock. It's in the pit of your stomach, the anxiety." The consequences make the case for board attention. M&S said the attack, which it attributed to "human error," would cost around £300 million (about $400 million). Machin also explained that hackers failed to breach the company's systems directly and instead used social engineering to get in through a third party. Because of their holistic understanding of the organization, internal auditors are uniquely qualified to advise on this complex, evolving risk landscape.

Why Cybersecurity Is Different



A few factors combine to set cybersecurity apart from other challenges:

- It is a widespread risk and systemwide responsibility that impacts organizations across industries and around the world, potentially affecting virtually every part of the enterprise.
- It is a multifaceted threat, taking numerous forms that can include phishing, ransomware, malware, deep fakes, denial-of-service attacks, zero-day exploits, and many more.
- Cybercrime approaches are constantly improving and changing shape as new schemes or manipulations are created or updated.
- Despite their preventive measures, organizations of every size must expect to be victims. More than a potential risk, cyberattacks should be considered a fact of doing business.
- The human factor cannot be forgotten. According to the Verizon 2026 Data Breach Investigations Report, the unintentional human element was involved in 62% of all confirmed data breaches.

©2026 The Institute of Internal Auditors. All rights reserved. For individual use only.

Strengthening Cyber Resilience Through Internal Audit

With its independent, enterprise-wide point of view, internal audit gives boards objective assurance on the cyber risks that matter most. It goes beyond identifying vulnerabilities: internal audit anticipates how evolving threats — from AI-enabled attacks and social engineering to supplier breaches and state-sponsored activity — could disrupt the organization, and turns that foresight into timely, practical advice on cyber resilience.

Organizations should regularly revisit assumptions about cybersecurity overall and about specific risks as new technologies come online. To strengthen that effort, internal audit can examine governance, risk management and controls as mandated by The IIA Topical Requirement on Cybersecurity. Overall, internal auditors' work is governed by the Global Internal Audit Standards, including Domain III of the guidance on the governance of internal audit and its work on cybersecurity.



CAEs and the internal audit function can also make a difference by:

- Helping businesses clearly define and monitor strategic, emerging, and live cyber risks.
- Providing assurance that cyber controls are adequate to prevent unauthorized access to sensitive data.
- Facilitating cyber risk workshops that help risk owners and management anticipate emerging threats, test their incident response readiness, and make better-informed decisions on cyber investment and resilience.
- Reviewing cyber risk connections to ensure that there is a comprehensive approach to interconnected threats.
- Working with stakeholders within and outside the organization to define adequate coverage in areas such as cybersecurity and data governance and create a relevant risk-based audit plan.
- Ensuring collaboration across The Three Lines to improve the organization's ability to anticipate, and adapt to cyber disruption. Internal audit can also coordinate on assurance with second line and external providers.
- Advising on integrating cyber risk into the wider governance, risk, and compliance framework. It can offer information on compliance with established cyber governance frameworks, such as:
  - The NIST Cybersecurity Framework 2.0.

©2026 The Institute of Internal Auditors. All rights reserved. For individual use only.

- ISO/IEC 27001:2022.
- The EU Artificial Intelligence Act.
- The UK Cyber Governance Code.

- Determining if software patching and updating processes are effective.
- Helping audit committees ensure that the organization has a joined-up cybersecurity policy, rather than siloed approaches that are inconsistent, redundant, or contradictory. Internal audit can offer advice on gaps and overlaps to help build a strong, cohesive approach. At the same time, it can provide insights on customizing responses as necessary in specific functions or regions.

Exhibit 1: Examples of key cyber-related frameworks, standards and legislation



Internal audit advisory services reflect an organization's unique needs and are informed by a deep knowledge of the business. For example, an organization wanted to maximize resiliency by examining the concept of a "minimal viable company." The CAE provided a risk assessment of what systems it would need to recover in a blackout, including everything from software and buildings to personnel and furniture. In another case, a CAE facilitated risk management workshops for all new technology purchases, working with the risk owners and the CISO to identify and plan for potential problems.

Leaning into Governance

Without strong governance, companies may be left with a false sense of security, according to IIA President and CEO Pugliese. As a result, he says, "we've been advising our members to lean in and see how governance—whether it's an audit committee, special committee, or any number of functions across the organization—is keeping up with the actual speed of the technology evolution and implementation." As companies race ahead to harness new opportunities in an extremely complex and ever-changing technology environment, internal auditors are stepping up to help them understand all the risks and implications of their actions, he says. Internal audit can help boards and management understand the connections between urgent risks, assess preparedness, and anticipate where new pressures may emerge.

©2026 The Institute of Internal Auditors. All rights reserved. For individual use only.

Global Audit Committee Center

The Institute of Internal Auditors

About The Institute of Internal Auditors

The IIA is an international professional association that serves more than 265,000 global members and has awarded more than 220,000 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.

About the Global Audit Committee Center

The Global Audit Committee Center is dedicated to providing thought leadership, strategic insights, and resources to help boards and audit committees strengthen internal audit oversight and drive governance excellence. By fostering alignment between audit committees and internal audit, boards can enhance structure, support, and impact — driving governance quality and long-term value.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Volunteer

To learn more about contributing to Global Guidance, visit Volunteer Your Time | Get Involved with The IIA

Copyright

© 2026 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact copyright@theiia.org.

November 2026

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101