TONE at the TOP®

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

Issue 125 | October 2024

The Board's Role in Cyber Resilience

Is your company prepared for the next cyberattack? Most organizations expect one in their future, with 73% of business and cybersecurity leaders predicting that a cyber incident will disrupt their business in the next 12 to 24 months, according to the **2024 Cisco Cybersecurity Readiness Index.**

There are many potential consequences of a cyberattack, including compromise of sensitive data, disruption of operations, and damage to third-party relationships and the company's reputation. In The IIA's **2025 Risk in Focus** report, internal audit leaders give cybersecurity the highest risk ratings by a wide margin. They also cite it as the area on which internal audit spends the most time and effort.

According to the report, cybersecurity remains the top risk the leaders expect their organizations will be facing three years from now, with digital disruption (including artificial intelligence (AI)), growing quickly from where it stood in past surveys to seize the number two spot. "AI is increasing cybersecurity and fraud risks around the world," the report says. Cybersecurity was rated as the top area in which AI would have the most negative impact.

In an environment where the question is not if but when an attack will occur, cyber resilience is critical in helping companies weather an incident. Companies can make robust efforts to protect themselves against cyberattacks, but they also must be prepared to respond to and recover from such attacks.

Cyber resiliency is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment." — National Institute of Standards and Technology.

New Expectations for Boards

Regulators and shareholders are examining the board's responsibility for cybersecurity and developing new expectations for directors' oversight of their organizations' vulnerabilities. Under a finalized rule, **Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure**, the U.S. Securities and Exchange Commission sets forth required disclosures for public companies, specifically addressing disclosure about material cybersecurity incidents and periodic disclosures on how registrants assess, identify, and manage these risks, as well as management's role in assessing and managing them. The final rules also require disclosures on boards' oversight of cybersecurity risks.

As part of their oversight role, boards should ensure executives and their teams set a high standard for cybersecurity, according to an article from McKinsey, **"Boards of Directors: The Final Cybersecurity Defense for Industrials."** They should then monitor cybersecurity efforts, determining whether goals are achieved and if teams are taking responsibility for cybersecurity. "The board is the last line of defense in ensuring such initiatives get planned and funded," the article notes.

A cyberattack is designed to make it difficult for organizations to continue with business as usual. Cyber resilience is about being informed and prepared, so options and priorities are clear when a crisis occurs. To ensure their organizations are well-prepared, boards should determine whether there are documented crisis management, incident response, and disaster recovery plans that management tests periodically in tabletop exercises, according to PwC's **Overseeing Cyber Risk: The Board's Role**. The exercises should focus on establishing clear roles and responsibilities to clarify management decision-making during a crisis.

Many boards receive a cyber scorecard or dashboard from management that highlights current risks and progress on cybersecurity goals. PwC points to several areas that might be part of a report to the board:

- *A multi-year strategic plan and current year business plan.*
- *Details on cybersecurity resource allocation broken down by funding and staffing.*
- *A maturity assessment measured against a recognized framework, such as the* **NIST Cybersecurity Framework.**
- *A regularly updated inventory of mission-critical systems.*
- *A summary of key cyber risks for the organization.*
- *A review of significant security incidents that the organization has experienced.*
- *Information on employee training and awareness efforts.*
- *Details on the organization's incident readiness framework, including information on the cyber insurance policy.*
- *Specifics on the third-party cyber-risk strategy.*
- *Information that benchmarks the organization's efforts against its peers.*
- *Details on key related legal and regulatory developments.*
- *Lessons to be learned from recent cyberattacks.*

While protecting the organization from attack is critical, boards should remember protection alone can only address issues that the organization already knows about. Unfortunately, armed with emerging technology tools that use AI, innovative cyber criminals continually develop new ways to cause damage. As a result, "to properly mitigate cyber risk, company leaders must have rock-solid plans in place to respond and recover quickly so that the company can continue to operate," reports the MIT News article, **"Now Corporate Boards Have Responsibility for Cybersecurity, Too."**

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 245,000 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 Audit: A Reliable Cybersecurity Partner

Boards should be aware of the value that internal audit functions can bring to cybersecurity efforts. Internal audit provides unique, objective, independent assurance and advisory services on cybersecurity strategy, governance, and controls. "Many companies leverage the internal auditors to review cyber processes and controls, including resilience and response," the PwC article notes.

Internal audit functions can contribute to cyber resiliency efforts in several ways, including through a cyber incident recovery and response audit. Last year's Risk in Focus report lays out some of the value internal auditors can add, and the list remains valid today:

- Assess the level of awareness, knowledge, and skills in key parts of the business, including the board, to ensure cyber defense responses are relevant and up to date.
- Evaluate the reporting lines between the chief information security officer, chief information officer, and the board to ensure clear communication of risks and recommendations and that they can be escalated to the highest level when necessary.
- Assess the frequency, timeliness, and effectiveness of simulated test phishing campaigns and other awareness-raising activities and the levels of staff engagement, as well as how well-integrated staff is with training and follow-up processes.
- Use scenario run-throughs to both educate the board on their governance responsibilities and to test that mitigation processes are complete and effective.
- Evaluate the effectiveness of the internal control environment and how well controls are embedded in the first and second lines according to The IIA's **Three Lines Model**, paying particular attention to practices staff find disruptive or intrusive and are likely to ignore, forget, or circumvent.
- Assess how well the organization's governance structure enables collaboration across the three lines.
- Determine how well the organization monitors global developments in cybersecurity and technology regulations and how readily internal controls can be changed to meet future requirements.

An Expanding and Evolving Risk

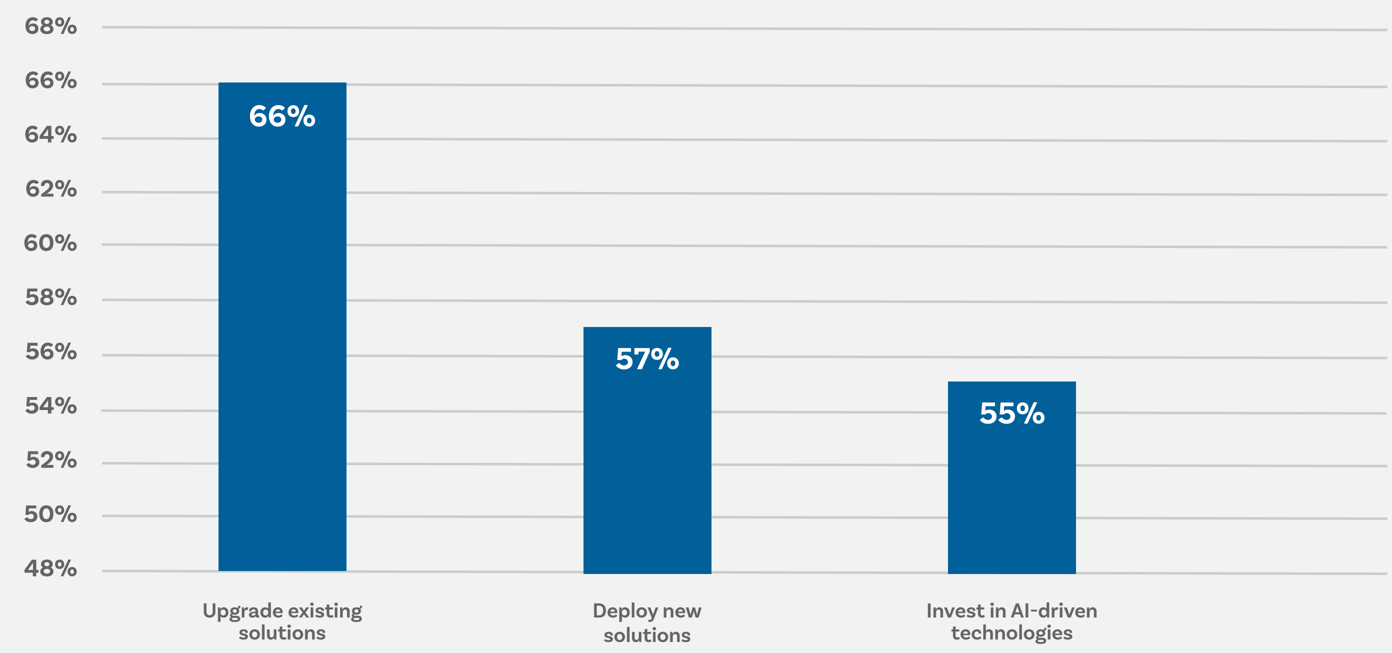
As new technologies rapidly evolve, many emerging tools are making cyberattacks even easier to carry out. Although AI and similar tools can enhance cybersecurity efforts, they also can simplify phishing and spam, blackmail and terrorism, and misinformation and election interference, according to Jen Easterly, head of the federal government's Cybersecurity and Infrastructure Security Agency. She also **notes,** generative AI is providing cyber attackers with new opportunities and allowing less sophisticated cybercriminals to wreak havoc.

Board members should turn to their internal audit teams for crucial information and advice on the best way to prevent cyberattacks and to assess the agility of their responses once they have occurred. Internal auditors can offer independent evaluations of the control environment and any identified risks that can help enable the organization to best recover from an attack.

QUESTIONS FOR BOARD MEMBERS

- How do we monitor new cyber threats, including how other organizations have responded to them?
- How does the organization measure and assess its own cyber resilience?
- How do we use this information to adapt our preparation for an attack and our potential responses?
- What are our disaster recovery plans? How well have they worked in the past? What have we learned from those experiences?
- What functions have direct responsibility for cyber resilience strategies?
- Do all employees understand the need for cyber resilience and the part they can play in it?

How are companies enhancing their cybersecurity?



Source: 2024 Cisco Cybersecurity Readiness Index.