Global Knowledge Brief

Cybersecurity

Part 2: Ensuring Cyber Resiliency

The Institute of Internal Auditors

About the Experts

DC Chang, CPA, CDPSE, CISSP, CRISC, CISA

DC Chang is audit director, Digital Technology and Cybersecurity, at United Airlines in Dallas, Texas.

Michael Echols, CISSP

Michael Echols is CEO of Max Cybersecurity LLC in Washington, DC.

Justin Headley, CPA, CISSP, CISA, CRISC

Justin Headley is senior manager in Warren Averett's Risk Advisory & Assurance Services Group in Birmingham, Ala.

Even as organizations work to ensure they have adequate tools to prevent cyberattacks, it is almost guaranteed they will experience breaches or incursions of some form. With that in mind, businesses also must focus on their ability to respond to and recover quickly from a cyberattack. This brief discusses how best to understand and instill resilience to attacks and describes the internal auditor's role in strengthening an organization's response.

Setting the Stage for Recovery

At its best, cyber resilience is not just a reaction to a dire situation. It is a continuum of practices — planning, processes, analysis, training, critical services, and management — that ensure an organization can maintain operations, according to Michael Echols, CEO of Max Cybersecurity LLC. These practices make it possible to restore or maintain organizational functions after an attack, but they must be set in place long before a problem occurs.

For example, Echols worked with a law firm client that received all its referrals through its website. It typically received many referrals daily, but at one point, two to three days passed before the firm noticed it was not receiving any and ultimately realized it had been hacked. "The firm should have already had a process for continuous monitoring and for some type of notification" about an unusual drop in web referrals, as they were the firm's main source of business (a critical function), he says.

The problems to be identified — like a drop in web traffic — will be different for every business and there likely will be more than one. In many cases, organizations will want to be prepared for an incident that will affect their power supply, for example, with steps to deploy generators that are independent of the main business, so they are not affected by the attack, Echols says.

> 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."
>
> **— U.S. National Institute of Standards and Technology**

Preparing for what comes next requires putting the current cybersecurity environment in context, according to DC Chang, audit director, Digital Technology and Cybersecurity, at United Airlines. Twenty years ago, organizations had their own data centers, and cybersecurity was, to some extent, a matter of locking up the servers behind physical doors and windows. Today, data is stored in a virtual environment that can be vulnerable to bad actors around the world.

"There are thousands and thousands of windows and doors we need to keep track of now that we're digital, and they're being added and removed on a daily basis," Chang says. Organizations need to be aware of the pace and scope of digital acceleration to develop the resilience they will need in a crisis.

Governance and Culture

Governance has a key role in building cyber resilience, according to Justin Headley, senior manager in Warren Averett's Risk Advisory & Assurance Services Group. "We continually hear that employees are the weak point because they use a weak password or click on suspicious links," he says. "But if leaders are not bought in, you can't expect employees to do their part."

In many ways, cybersecurity is not entirely a technology issue, it is a culture concern. “If you change the minds of 90% of the people in the organization and one person opens a link in an email, it could sink the company,” Echols says. A cybersecurity-aware culture clarifies the organization’s expectations and reassures consumers and business partners. “Banks were one of the first groups to become cyber resilient,” he says, because they rely on the confidence of their stakeholders.

Headley recommends leaders foster a cybersecurity culture that goes beyond standard approaches such as quarterly emails containing cyber safety tips or rudimentary annual security training. Steps his organization take include sending out its own fake phishing emails to employees, then providing training to those who click on the embedded suspicious links. “You have to show how cyber governance works in action, not just in theory,” he says.

Leaders also can provide specific steps to take in an attack. “An organization can stop an attack and recover if there are practical, repeatable policies and procedures to follow in a breach,” according to Headley. If the leaders are involved when these steps are tested and take part in working out the kinks, they demonstrate their commitment to the effort, which can play a large role in making their cybersecurity strategy successful.

- 68% of breaches involved a non-malicious human element, such as someone falling for a social engineering attack or making an error.
- The median time for users to be taken in by phishing emails was less than 60 seconds.
- 15% of breaches involved a third party or supplier, including software supply chains, hosting partner infrastructures, or data custodians.

Source: Verizon Business 2024 Data Breach Investigations Report

The Impact of Regulation

Under the finalized rule, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, the U.S. Securities and Exchange Commission raised expectations for organizations by requiring public companies to disclose material cybersecurity incidents and make periodic disclosures on how they assess, identify, and manage cyber risks. The rule “highlights a major table stakes issue that every entity on the planet has to consider,” Chang says.

Among other requirements, the rule forces organizations to ensure their cyber practices are operational, Headley says. He notes that the IT function often operates within a silo, with implied trust from leaders who may not fully understand its workings. “That will have to change,” he says. There will have to be an organizationwide understanding of how to treat internal and customer data and address cyber concerns.

As is the case with many regulations, “it will all come down to transparency,” Echols says. “When there has been a material breach, the company must have a clear process for how it reacts to that breach.”

Adding AI to the Mix

Artificial intelligence (AI) can be an invaluable tool in enhancing prevention of cyber issues and resilience in the wake of an attack. Technology such as next-generation firewalls and point protection systems are making it easier to sort through the data traffic and find anomalies that should be investigated, Headley says. “The use of AI has been a game changer in the last several years, and it will continue to help companies get better at detecting and responding to attacks.”

AI also can be used as a weapon against organizations. “If you have vulnerabilities that have been ignored, AI will help hackers find them,” Echols says.

Among other considerations, organizations will have to balance the drive for greater efficiencies to be gained with new tools with the need to protect security and privacy, according to Headley. New technologies help organizations eliminate repeatable tasks, which often involves feeding the programs sensitive information. At the same time, "we continue to see targeted attacks on these technologies because the bad actors know that people do not fully understand the technology," which can make the sensitive data that programs contain especially vulnerable.

In building resilience, organizations will have to train their people in evolving technologies and ensure technology use matches the organization's risk appetite. "A company could have the best technologies and skills, but a user may still unknowingly or sometimes knowingly leak data through the front door using a GenAI tool," Headley says.

> "Stakeholders, primarily an organization's board and senior management, rely on independent, objective, and competent assurance services to verify whether cyber incident response and recovery controls are well designed and effectively and efficiently implemented. The internal audit function adds value to the organization when it provides such services in conformance with the Standards and with references to widely accepted control frameworks, particularly those expressly used by the organization's information technology and information security functions."
>
> **Source: Global Technology Audit Guide: Auditing Cyber Incident Response and Recovery, 2nd Edition, Global Practice Guide, The Institute of Internal Auditors, 2024**

Organizations should also be careful not to neglect traditional cyberattack approaches. Many cyber issues are caused by problems that are not new, such as misconfigurations or failure to follow an established practice, Echols says. Many breaches relate to known vulnerabilities that have never been fixed or patches that have not been installed, he says. As a result, educating end users about new and existing threats is particularly important. "Auditors must look under the hood and ask the right questions of clients to unearth hidden vulnerabilities created by apathy," he says.

How Internal Audit Can Help Enhance Resilience

In this environment, internal audit should be prepared to frame the outcomes of their audits to enhance resiliency and identify vulnerabilities in ways that help clients understand the potential consequences of lax cybersecurity, Echols says. While clients may assume the worst could never happen to them, internal auditors must be able to suspend disbelief, which will better enable them to imagine the unimaginable. For example, Echols had a client that had a best practice that prohibited use of corporate email addresses in social media accounts, but it was not an official policy. The error of that approach became clear when MGM suffered a significant data breach late last year. Investigation of the breach reportedly revealed that an employee was using their work email on a social media platform. The hackers found the employee's information on LinkedIn and impersonated the employee in a call to MGM's IT help desk, thereby obtaining credentials to access and infect MGM's systems. "Best practices are derived from the experiences of many and should be made policy when possible," Echols says.

Internal auditors must also understand that the compliance aspect of the audit is only the first step in helping build cyber resilience. "Compliance is not security," Echols says. Internal auditors should focus on translating their findings into greater insights that the client team can use to enhance security and in asking questions the team may not yet be able to answer.

“You should be able to instruct the client that not seeking and finding the answer to this question actually creates a vulnerability,” according to Echols.

Between audits, internal audit should keep the lines of communication open by scheduling times to check in and learn about teams’ challenges. “When internal auditors are able to position themselves as trusted advisors, it’s a complete game changer,” Headley says.

Transparency is crucial. Internal auditors should be clear on the scope and the planned testing procedures, as well as what issues have arisen. “Make sure to communicate early and often,” he says, “especially when it involves IT risk.” He advises that internal auditors avoid rushing to judgment immediately, but instead have an open conversation about the client team’s thought processes and encourage collaboration.

Headley notes that IT teams often get bogged down in meeting the demands of various lines of business, taking responsibility for everything from keeping apps up and running to dealing with day-to-day hardware glitches. As a result, cybersecurity may not always be a top priority. Internal auditors can promote awareness of these challenges and educate teams about opportunities to address them, thereby ensuring audits are a true value-add exercise.

“Internal auditors can be partners in helping to strengthen corporate resilience,” Headley says. Among other steps, they can help smooth out any disconnects between company leaders and IT teams, who often don’t speak the same language. Because internal auditors understand both business risk and IT risk, they can help bridge that gap.

Internal auditors can also shape the understanding of cyber risks and related problem-solving in a way that departs from past practice, Chang says. As organizations move away from traditional business continuity planning or business disaster recovery, internal auditors can help them adopt more multifaceted and nuanced approaches. They can enhance that effort by taking on a role as storytellers who process disconnected information and data points and put them together into a compelling narrative that drives better decision-making.

According to a survey of IT and security operations decision makers:

- Only 2% of respondents say they could recover their data and restore business processes within 24 hours of a cyberattack.
- 69% say their organization has paid a ransom in the last year, even though 77% say they have a defined policy or protocol against paying ransoms.
- 42% say their organizations could identify sensitive data and comply with applicable data privacy laws and regulations. Others do not have adequate IT and security capabilities to do both.

Source: Cohesity Global Cyber Resilience Report 2024

Evening the Odds

In the end, resilience means accepting the inevitability of attack and assuming that the organization’s outer walls are not impenetrable, Echols notes. As part of that effort, organizations must recognize they are in an unfair fight. While organizations strive to block 100% of the attacks they are facing, hackers only need to open one door to wreak havoc, Chang notes. “It’s a lot more difficult to be the defender than the perpetrator,” he says. Internal audit can provide the insights and information their companies need to improve their odds of cybersecurity success.

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.

Disclaimer

The IIA publishes this document for informational and educational purposes only. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as peer-informed thought leadership. It is not formal IIA Guidance. 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.

Global Knowledge Briefs are intended to address topics that are timely and relevant to a global internal audit audience, and each topic covered is vetted by members of The IIA's volunteer North American Content Advisory Committee. Subject-matter experts are primarily identified and selected from The IIA's list of Global Guidance Contributors.

To apply to be added to the Global Guidance Contributors list, email Standards@theiia.org. To suggest topics for future Global Knowledge Briefs, email Content@theiia.org.

Copyright

November 2024

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