GLOBAL KNOWLEDGE BRIEF

Cybersecurity

Part 1: Staffing and Development for the Next Generation

AUDITBOARD

The Institute of Internal Auditors

Contents

About the Experts

Aneta Waberska, CISA

Aneta Waberska is Director of Information Security and Compliance Products at AuditBoard. She has more than 15 years of experience across IT audit and compliance domains and joined AuditBoard to focus on product development efforts serving IT risk and compliance users, leveraging her industry experience. Aneta started her career at KPMG and PwC, where she helped clients implement and assess frameworks such as SOC 1 and SOC 2. She has worked with companies of different sizes to implement and manage compliance programs of varying complexity, including managing company-wide policies and third-party risk management programs. Aneta has worked closely with management to implement controls to meet security framework requirements, as well as with executive management to ensure compliance supports the company's strategic objectives.

Uday Gulvadi, CIA, CPA, CAMS, CISA

Uday Gulvadi is a Managing Director in the Disputes, Compliance, and Investigations group at Stout, and co-leads its regulatory compliance and financial crimes practice nationally. Uday is a financial crimes, internal audit, information systems audit, and risk advisory practice leader with more than 20 years of experience. He specializes in advising boards, audit committees, and senior management on their most challenging financial crime compliance, IT, and cyber risk, governance and risk, and compliance matters, including enterprise risk management, AML and sanctions program governance, model validations, risk-based internal audits, information technology, and cybersecurity audit and controls. Uday's clients range from some of the world's largest banks and financial institutions to smaller financial services companies.

Introduction

Cybersecurity poses a significant threat for organizations of any size. Recent examples reflect how quickly things can go wrong. A cyberattack disrupted shipments from Ace Hardware Corporation to its dealers and forced it to temporarily disable customer online ordering. A ransomware attack at a major Chilean telecom company disrupted services, including data centers, internet access, and voice-over-IP. And, demonstrating that smaller entities can also be affected, public online access to land records and indexes of births, deaths, and marriages was interrupted by a cyberattack in Cabarrus County, N.C.

Internal audit is well-suited to play a key role in helping to manage cyber risks, but it must have the resources it needs to fulfill that role. It should have the knowledge and skills necessary to identify and advise on cyber threats facing the organization. In conducting a cybersecurity assessment, "It is critical to involve audit professionals with the appropriate depth of technical skills and knowledge of the current risk environment," according to Deloitte.[1]

This brief is the first in a three-part series on cybersecurity. Because internal audit leaders must understand the threats before they can staff up to meet them, it begins by examining cybersecurity challenges for internal auditors and their organizations. It also covers the options and strategies internal audit leaders can follow to ensure they have the talent they need to address ongoing cyber risks.

[1] "Cybersecurity and the Role of Internal Audit—An Urgent Call to Action," Deloitte Development LLC, 2017

A Clear Threat

Cybersecurity remains a top risk

Internal Audit's Cybersecurity Efforts Are Growing

"Internal auditors have to look at the entirety of the organization and take a risk-based approach," said Aneta Waberska, CISA, Director of Information Security and Compliance Products at AuditBoard. "Cyber risks are at the top of the list for most organizations."

Internal auditors appear to be well-aware of the threat that cyber risks pose. Cybersecurity was identified as the top risk going into 2024, according to a global survey of internal audit leaders by the Internal Audit Foundation. Cybersecurity, along with human capital and business continuity, were listed as the top three risks in the Risk in Focus 2024[2] survey of more than 4,200 chief audit executives (CAEs), with 73% of respondents listing cybersecurity as a top five risk.

In North America, 78% of internal audit leaders described cybersecurity as a high or very high risk in their organizations, according to The Institute of Internal Auditors' 2023 North American Pulse of Internal Audit.[3] The surveyed auditors were devoting 10% of their audit plans to cybersecurity, with IT concerns making up another 9%. In addition, almost 70% of functions reviewed high-risk areas that include cybersecurity and IT annually or continuously, according to the Pulse survey findings.

Some cybersecurity dangers to keep in mind include:

- Breaches that enable criminals to steal critical information or that expose customer or business partner data.
- Ransomware attacks that make it impossible for organizations to perform key functions or access necessary information without first paying a ransom to cyber criminals.
- Malware that can wreak havoc with a system.

Cyberattacks have consequences beyond the obvious, such as financial losses when business functions are impaired or if customers or business partners lose confidence in an organization and cease doing business with it. What's more, once a cyber incident is discovered, organizations must invest time and money in forensic investigations to understand what happened and when, undertake remediation to repair any damage, and determine whether fallout from such attacks are material from financial and operational perspectives in order to meet regulatory reporting requirements.

It's not surprising, then, that cybersecurity spending is expanding quickly. At the beginning of 2023, Canalys expected global cybersecurity spending to jump 13.2% during the year, with the potential to hit $224 billion.[4]

"Companies have come to realize that these threats carry very real business and financial consequences," said Uday Gulvadi, CIA, CPA, CAMS, CISA, Managing Director in the Disputes, Compliance and Investigations group at Stout. The threats are certainly all top of mind for audit committees, he said, and "internal audit is being asked to step up and provide assurance in these areas."

[2] "Risk in Focus 2024," The Internal Audit Foundation, 2023
[3] "2023 North American Pulse of Internal Audit," The Institute of Internal Auditors, 2023
[4] "Cybersecurity investment to grow by 13% in 2023", Canalys, Jan. 18, 2023, https://www.canalys.com/newsroom/cybersecurity-forecast-2023

The Challenges

Cybersecurity approach, maturity impact staffing

Clear-eyed Understanding of Cyber Environment Is Fundamental

To hire the right people to help internal audit support cyber risk management and offer them the appropriate development opportunities, it's important to fully understand the organization's unique cybersecurity circumstances and risks. Several factors and challenges should be considered.

A Manual Mindset

Many internal audit teams have traditionally been used to thinking about internal controls and various processes from a manual perspective, said Waberska. However, the ongoing digital transformation of business demands that teams be aware of how digital solutions can enhance and improve internal audits and other processes throughout the organization, including cybersecurity. At the same time, internal auditors should also understand the risks that digital transformation itself poses for organizations, as increasingly sophisticated cyber criminals exploit the vulnerabilities that digital environments can create.

If, for example, an organization operates in the cloud or uses or plans to use any advanced or emerging technology, it will need people who have worked with these tools. It's not necessary for team members to be experts in the technology, Waberska said, but exposure to the cloud environment or to other solutions will provide greater familiarity with the related risks. In addition to hiring for these skills, audit teams should also be sure to include new technologies in their training and development of existing staff.

Internal Controls

Internal auditors are trained to ensure that the organization has the proper controls to protect against the risks it faces. In regard to cyber risks, internal controls should work to ensure that an organization's information technology is not compromised and that business functions can remain operational.

To identify and advise on cybersecurity risks, internal audit teams will need to be familiar with IT security controls for the technologies used by their organization. In working with the cloud, for example, controls will differ from those used with in-house data centers, Waberska said. They will also need to understand which controls are appropriate considering the threat that cybercrime can pose to privacy and implications to audit plans of their organization's privacy program.

Disclosure Regulations and Data Protection

Organizations are now being called on to be more open about reporting on their cybersecurity efforts. Internal auditors will have to understand which rules affect their companies and be able to evaluate compliance needs. In one significant example, in August, the U.S. Securities and Exchange Commission issued a final rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, which requires public companies to provide greater transparency when they have experienced a cyberattack and to disclose specific information about their efforts to mitigate cyber risks. The IIA provided comments on the rule when it was in the proposal stage. It plans to continue to work with the SEC to develop implementation guidance, especially on determining the materiality of a cyber incident and better defining the term "cybersecurity."

Because of the increasingly multinational nature of doing business and the growing number of cybersecurity regulations around the world, internal auditors must become familiar with all data security and privacy laws that might affect their organizations, such as the European Union's General Data Protection Regulation. Indeed, according to the United Nations

Conference on Trade and Development, 137 out of 194 countries had put in place legislation to secure the protection of data and privacy.

IT Systems

Any organization with even basic technology is involved in some type of IT system, and all of them are vulnerable to cyber risk. Given the volume of systems and the potential weaknesses and threats involved, it's important for companies and internal audit to understand which systems are most important. "We will never be able to put the same level of controls around all systems," Waberska noted. Setting priorities will involve asking questions such as:

- Which systems are critical to the organization's functioning? It's possible to answer that question by considering whether – and for how long – the organization would be able to continue to conduct business or achieve key goals without them.
- Which ones process the most sensitive data? That might include confidential corporate information or personally identifiable information (PII).
- Which ones hold unique or hard-to-replace data?[5]

Third Parties

Even small and midsize organizations are involved with third parties that handle their data. It can happen through a cloud application or, for larger organizations, perhaps a processing center abroad. These vendors may handle important organizational data and customers' PII, and the data may be housed anywhere in the world, Gulvadi noted. For that reason, "It's extremely important to understand the whole landscape of IT assets," including where they are and whether the proper controls are in place around those assets, he said.

Organizations should evaluate third parties' cybersecurity processes before they share data with them and monitor those processes once the third parties begin using the data, in some cases retaining the right to audit the third parties. "If you share customer data with another party, you need to ensure they will protect them in the same manner that your company would," said Waberska. Companies should review a third party's attestation reports such as SOC 2, which evaluate their internal controls to see how well it addresses risk, or other types of attestations or certifications related to protecting relevant categories of data.

Ensuring Secure Access and Availability

There is a tradeoff between making sure the organization can protect data and systems while at the same time guaranteeing that information and systems are available for use as needed to achieve business objectives, noted Gulvadi. To maintain a balance, organizations will have to choose controls that safeguard data without making access to information that is necessary for customer service or other important business functions burdensome. This determination should be easier to make once the organization has considered which systems require the highest level of security. Some may need to be protected with multifactor authentication, encryption protocols, and data loss prevention software, while others won't require that level of granularity.

[5] "CISA Insights – Cyber, Secure High Value Assets (HVAs)," U.S. Department of Homeland Security, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf

Strengthening Internal Audit Resources

Cybersecurity staffing remains a top priority

Hiring and Developing Internal Audit's Cyber Talent

Given these risks, how can internal audit build and maintain a team that can address them? The specifics of the answer will vary by organization, but there are a few recommendations that apply to all.

Look for a Blend of Skills

To address cyber risk, internal audit teams need a deep understanding of the technical side of cybersecurity as well as the ability to comprehend the consequences that security issues may have for the business, Gulvadi said. In the past, IT auditors tended to be strong in the technical aspects of information security, but they often didn't focus on how related risks affected the organization's ability to fulfill its business objectives. The ability to articulate business impact can be particularly valuable if internal audit needs to gain management buy-in for needed investments in improved technology or controls or additional staffing.

Gulvadi is seeing more efforts to build teams that blend technical knowledge with an understanding of business objectives, processes, and value chains. In some cases, internal audit teams are finding professionals who have both skills, but in others, teams include professionals whose skills complement each other. The organization can consider offering training to give each type of professional a basic working knowledge of the other discipline.

Integrate Skills in Emerging Technologies

Many internal audit teams are adding professionals with expertise in data analytics, artificial intelligence (AI), and machine learning (ML) as they move away from sample-based testing. "You can use artificial intelligence to test the whole population and improve anomaly detection," Gulvadi said. This not only enhances efficiency and reliability, but it also helps internal auditors keep pace with cyber criminals, who are becoming increasingly sophisticated in their use of new technologies.

Investigate Outsourcing

Some internal audit teams bring in an outsourced team to enhance technical or business skills. Professionals with specialized expertise in cyber or IT security can be incorporated into the internal audit team on a project or longer-term basis as needed. When members of the internal audit team work alongside these experts, they can help the contractors enhance their knowledge and better navigate company processes and procedures. At the same time, exposure to outside experts can help expand team members' knowledge base. In evaluating an outsourcing option, Gulvadi recommends examining team members' certifications and prior experience to ensure they match or enhance current team skills.

Consider Collaboration

Sometimes the expertise that the internal audit team needs may be available in-house in areas such as IT, security, or compliance. A good partnership, while maintaining auditor independence, introduces internal audit team members to a range of new insights and knowledge about the organization's technology ecosystem and risks. It also sets the stage for fruitful audits in the future because other teams will know that internal audit shares their goal of protecting the organization from unnecessary risks and ensuring that it can achieve its objectives. Open communication can help other teams overcome any anxiety about internal audit objectives, as well. "IT and security teams are focused on fixing important problems and finding solutions," Waberska said. "They understand the risks and the need to mitigate them. Internal audit's ability to have a very risk-focused conversation with them explains why certain controls are necessary to make internal audit that much more effective."

Build Internal Relationships

All members of an internal audit team can benefit from building and maintaining relationships with other professionals on their organization's security, compliance, and IT teams to learn about their current work, even if they are not collaborating on a specific project. "Understanding what's happening in the company's environment is very important," Waberska said, and these relationships can ensure the team gets timely updates. Specific audits will reveal trends and threats, "But it's better to know what's changing as soon as possible," she said.

Make Use of Available Resources

"If internal audit teams carve out time to learn modern technologies at least at a high level and the risks that come with them, they will stay up to date on current and emerging risks," Waberska said. Options include The IIA's Cyber Resource Center, which includes a variety of cybersecurity guidance, research, certificate programs, and information about related conferences, such as The IIA's annual Cybersecurity Virtual Conference. AuditBoard provides a wide variety of cybersecurity resources as well, which are accessible through its resources page.

Risk in Focus 2024, from the Internal Audit Foundation, explores cybersecurity risk globally and provides unique regional perspectives on how cybersecurity and other top risks are viewed and managed around the world.

Conclusion

The 2023 IIA Pulse survey found that internal audit staff growth is increasing but that it had not yet returned to pre-COVID levels. Internal audit leaders should remember that the generations coming into the workforce are digitally savvy. It's smart to consider the best ways to use the knowledge they bring, Gulvadi noted. Internal audit shops will also set themselves apart in a competitive staffing environment by offering a new generation the chance to use emerging technologies like AI/ML to offer insights that will help solve critical business problems. As internal audit continues to rebuild teams or expand their expertise to take on new challenges, they should use the advice and insights in this brief in their planning.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 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 AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit AuditBoard.com.

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 2023

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