GLOBAL PERSPECTIVES & INSIGHTS

Cybersecurity

PART I: Staffing and Development for the Next Generation

PART II: Artificial Intelligence – Cybersecurity Friend and Foe

PART III: Cybersecurity Third-Party Risk Management

AUDITBOARD

The Institute of Internal Auditors®

Contents

INTRODUCTION **5**

A Clear Threat **6**

Internal Audit's Cybersecurity Efforts Are Growing 6

The Challenges **7**

Clear-eyed Understanding of Cyber Environment Is Fundamental 7

Strengthening Internal Audit Resources **9**

Hiring and Developing Internal Audit's Cyber Talent 9

Conclusion **11**

Part 2: Artificial Intelligence – Cybersecurity Friend and Foe **12**

INTRODUCTION **14**

AI at Work **15**

Internal Audit Should Explore AI Uses and Threats 15

Risk Management Considerations **17**

Internal Audit Can Help Organizations Avoid AI Pitfalls 17

Protecting AI – and Protecting Against It **18**

Protecting Integrity of AI Systems, Access 18

Don't Forget the Human Element 18

Conclusion **19**

Part 3: Cybersecurity Third-Party Risk Management **20**

INTRODUCTION **22**

A Vast Challenge **23**

A risk on the rise 23

The Internal Audit Approach **25**

Establishing a culture of cyber action 25

A continuous monitoring approach based on risk level 25

Embrace Software Solutions 26

Focus on offboarding as well as onboarding 27

Conclusion **28**

Part 1: Staffing and Development for the Next Generation

About the Experts

Aneta Waberska, CISA

Aneta 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, third-party risk management programs, She has worked closely with management to implement controls to meet security framework requirements, and working with executive management to ensure compliance supports the company's strategic objectives.

Uday Gulvadi, CIA, CPA, CAMS, CISA

Uday 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 crimes compliance, IT, and cyber risks, 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 marriage 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 to 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 multi-national 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 the 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, and machine learning 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 teamwork 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 Cybersecurity 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 work force 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.

Part 2: Artificial Intelligence – Cybersecurity Friend and Foe

About the Experts

Aneta Waberska, CISA

Aneta 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, third-party risk management programs, She has worked closely with management to implement controls to meet security framework requirements, and working with executive management to ensure compliance supports the company's strategic objectives.

Terry Grafenstine, CIA, CPA, CISSP, CISA, CRISC, CGAP, CGEIT

Terry is the 2023–24 senior vice chair of the Global Board of Directors of The Institute of Internal Auditors (IIA) and chief audit executive with Pentagon Federal Credit Union (PenFed). She was recognized by The IIA as one of the "Top Ten Audit Thought Leaders of the Decade" for her contributions to the profession related to cyber and technology and was also inducted into The IIA’s Hall of Distinguished Audit Practitioners. She has held leadership roles at Citi and Deloitte and served as the appointed Inspector General of the US House of Representatives.

INTRODUCTION

Cybersecurity is the top risk consideration for internal auditors, and that will remain the case for the foreseeable future. Indeed, it is the singular risk consuming their greatest time and effort, according to Risk In Focus 2024. The report series, from The Institute of Internal Auditor's (IIA) Internal Audit Foundation, asked chief audit executives and directors from around the world about the top risks their organizations are facing, and how they expect the threat picture to change in the next three years.

The Risk in Focus 2024 findings demonstrate the complexity of cybersecurity as a risk and the added challenges stemming from near-constant changes in technology and how it can be used. This, too, was reflected in the report's findings. Internal audit leaders expected to see the threat of digital disruption jump from fifth place on the threat list today to second place in three years.

This brief, the second in a three-part series on cybersecurity, examines how artificial intelligence (AI) contributes to cybersecurity challenges and opportunities, and what internal auditors need to know about this emerging and evolving risk area as a cybersecurity consideration. AI holds great promise as a sophisticated tool to improve efficiency, productivity, and risk management in virtually any organization. However, it also presents new risk management challenges, including ethical considerations, the dangers of algorithmic bias, and over- or blind reliance on the use of AI. While it can be a valuable tool in the battle against cyberattacks, bad actors are also using it to perpetrate their crimes.

AI at Work

A Two-Edged Cyber Sword

Internal Audit Should Explore AI Uses and Threats

The term artificial intelligence refers to technology that can mimic human intelligence, such as learning, reasoning, and working to solve a difficult problem. It encompasses several types of technologies, including machine learning, or a system's ability to learn from data and apply that learning.

One way that AI and machine learning can significantly enhance cybersecurity efforts is in threat detection and data analysis, said Aneta Waberska, director of information security and compliance products at AuditBoard. Cybercriminals try to infiltrate an organization's network by seeking out weak spots and breaking down network defenses. In the past, organizations relied on system administrators to block these external threats. However, because of the advancement of automation and other technologies, the growing volume of entries from bad actors has overwhelmed the capacity for effective human review, she said. AI can address this problem. It can review large volumes of network entries and recognize patterns and learn from them over time, understanding if a particular event or cluster of events can pose a threat to an organization. "This is one of the most impactful uses of AI in this environment," she said.

In addition, more sophisticated malware detection tools have better capabilities, including the ability to block one of the top causes of security breaches and incidents—phishing. That can reduce or eliminate the potential for human errors—such as opening a link on a phishing email and exposing company networks to malware—because the tools filter them out before they get to someone's inbox, Waberska said. (See the sidebar for more information on some of the ways AI can improve cybersecurity defenses.)

AI can also quickly search for anomalies and identify problems already occurring within the organization's network, something that humans cannot do on such large-scale data. Unauthorized access to company systems is one example. A former employee could inadvertently make access available to a cybercriminal by sharing or writing down a password or may reenter the system with malicious intent themselves. In the past, an internal auditor checking for unauthorized access among former workers would have had to conduct a manual comparison of people with access and those who no longer should have it, then write an email to the IT team detailing any issues, noted Terry Grafenstine, chief audit executive with

Using AI as a Cybersecurity Tool

According to the IEEE Computer Society, some of the ways in which AI can enhance an organization's cybersecurity defenses include:

- Detecting malicious activities, by benchmarking acceptable activities and identifying anomalies and threats continuously and in real time.
- Supporting malware threat identification by examining file characteristics or code patterns to spot those that are unsafe.
- Improving a company's ability to deal with zero-day attacks or other unknown threats.
- Enhancing threat intelligence by pulling together security information from a range of sources, proactively hunting for threats, and assisting in threat management by easing the workload of company security analysts.[6]

[6] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society, September 6, 2023.

the Pentagon Federal Credit Union. AI, on the other hand, can search across multiple platforms, compare data in the payroll system and the access system, and generate an email to the appropriate teams about any anomalies.

Internal auditors should be aware that cybercriminals’ goals are often not simply to steal data, but to infiltrate and disrupt systems by changing data, Grafenstine said. On the largest level, nation-state bad actors can manipulate critical infrastructure, such as transportation, nuclear energy, banking, and many others, but the consequences can also be significant for organizations of any size.

Risk Management Considerations

Ethics, Bias and Over Reliance

Internal Audit Can Help Organizations Avoid AI Pitfalls

Along with its many benefits, AI does come with its own list of risk considerations. Some of the threats are internal ones but can be just as damaging as cyberattacks.

Ethics

Many of the concerns in this area relate to generative AI and large language models that can be used by internal auditors to create reports, write code, and sketch out recommendations and analysis, among other possibilities. However, these tools also raise security and ethical questions for organizations. “There is a risk that employees will look at these tools as a parlor game or a toy,” Grafenstine said.

Traditional cyber controls used on earlier technologies also apply to these systems, but “the repercussions of not doing it well are magnified,” she said. Among other things, as will be discussed in more detail, the systems can provide biased, inaccurate, or completely fabricated information, depending on how they are trained. Grafenstine also points to the costly and potentially embarrassing consequences for a company’s business and reputation if it uses a customer-facing chatbot that has been trained on poorly sourced internet data and the chatbot’s incorrect answers have a significant negative impact on the customers. For these reasons, there should be human review of anything produced by a generative AI system when the organization is not completely aware of the data it has been trained on. “The company has to own the answers,” Grafenstine said.

While the use of generative AI programs such as ChatGPT has exploded since they debuted in late 2022, posting information on publicly available generative AI can expose company or customer data and personal identifiable information, just as a hacking incident might do, and is a significant risk consideration. When employees post queries that include company information in public generative AI programs, the program will retain that information and potentially use it to respond to other queries outside the organization, exposing it to public view. Not only can this publicize confidential information, but bad actors can also use the details they discover in publicly available generative AI to engineer their way into the company systems, with phishing or other tools, Grafenstine warned.

Blind Overreliance on AI Output

Any professional is ultimately responsible for the tools they use and the information they generate. That’s particularly true of internal auditors, who could violate their own standards if they place too much reliance on unvalidated data or content. “Being reliable is what we do for a living,” Grafenstine said.

Algorithmic Bias

Machines are trained to learn based on specific algorithms and the information they produce can be influenced, intentionally or not, based on those algorithms. As an example, algorithms may filter out women’s résumés being used in a hiring decision if existing employees in a certain role are predominately male or they may favor mortgage applications from white buyers if most current mortgage holders are white.[7] “They are not intentionally trying to be malicious, but the biases are baked in,” Grafenstine said.

[7] “For minorities, biased AI algorithms can damage almost every part of life,” The Conversation, www.theconversation.com, August 24, 2023.

Protecting AI – and Protecting Against It

Internal Controls Are Critical

Protecting Integrity of AI Systems, Access

Security over AI itself and the ability to use it are other serious considerations for organizations and internal auditors. There should be controls over who can access AI resources, how the authority to change code is protected, and who is allowed to take information from a test area to production. As an internal auditor, "I want to make sure I can tell if an AI algorithm has been changed or if someone can disrupt it in the middle of a process and alter it," Grafenstine said. Internal auditors also need to be aware of the potential scope of the interference. "If I can access your company AI, it's not just one transaction that I can alter," she said. Instead, the bad actor can get to an organization's entire data lake or data warehouse, or whatever else the AI has access to.

> "Just because you have implemented a solution that leverages AI does not mean that you are now bulletproof,"
>
> Aneta Waberska
> AuditBoard

At the same time, it's important to be aware that AI is making it easier for cybercriminals to create malware rapidly, automate attacks, and improve the effectiveness of their scams or social engineering attacks by using tools such as deepfakes, which digitally alter videos or pictures, and AI voice generators to create false images or messages. "The cyber threat landscape is becoming more dangerous, and AI plays a big role in it," according to an IEEE Computer Society article.[8]

Internal auditors should see AI as an offensive and a defensive tool, said Waberska. "Just because you have implemented a solution that leverages AI does not mean that you are now bulletproof," she said. While past attacks were often launched by one hacker on a single organization, AI can carry out attacks on a much bigger scale, hitting multiple organizations. AI can enhance malware by learning from past programs and use that knowledge to generate stronger and better malware, doing so on its own with no developer needed. "If AI is trying to break into your organization, it may be much more powerful than your existing solution," Waberska said. Internal auditors can ensure that their organizations understand and are prepared to address those risks. The internal audit team can't implement solutions, but they can have an informed conversation with the security team to see if they are considering these threats and implementing solutions. "It will take time for organizations to adopt new solutions, but it is important to be aware of the threats and have a plan to defend yourself," Waberska said.

Don't Forget the Human Element

While organizations gear up to ward off external cyber threats, internal auditors should keep in mind the danger posed by inadvertent threats posed by their own people. Phishing attempts, for example, succeed because of human error in failing to recognize that a cybercriminal is trying to gain entry to the system or to an important password or other confidential data. "Internal auditors should look at how the organization is educating users about these threats," Waberska said. In particular, employees may not understand that phishing emails have evolved. While it was once easy to spot red flags such as misspellings or strange fonts, AI is being used to write phishing emails that are much more sophisticated and realistic. "They look very real, and it's much easier for bad actors to generate them," she said.

[8] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society Tech Trends, September 6, 2023.

Conclusion

The threat of cyberattacks is a permanent feature of doing business in the digital world, and AI and its evolving usage presents a new and provocative twist in the risk management battle against that threat. Internal auditors have an important role to play in:

- Ensuring that leadership and key teams are aware of the benefits and dangers related to AI.
- Determining and providing recommendations on how AI can enhance various cybersecurity efforts within the organization.
- Promoting awareness of the need to consider updated defenses against AI-powered cyberattack tools.
- Providing assurance on the company's understanding and use of AI technologies.

AI and related technologies can serve as valuable resources, but they are not a final answer. "Technology advancements can be great as long as you know how to use them in a way that is smart and safe," Waberska said. "You should always use professional judgment in considering what you get."

Remember, as well, that while being conservative is an asset for internal auditors, they should not be "the office of no," Grafenstine said. Internal auditors should provide good control and risk advice, including insights on the risk of failure to keep up with technology. "It's a massive risk to not embrace technology, but we need to do it in a thoughtful way," she said.

Part 3: Cybersecurity Third-Party Risk Management

About the Experts

Richard Marcus, CISA, CRISC, CISM, TPECS

Richard Marcus is VP, Information Security at AuditBoard, where he is focused on product, infrastructure, and corporate IT security, as well as leading the charge on AuditBoard's own internal compliance initiatives. In this capacity, he has become an AuditBoard product power user, leveraging the platform's robust feature set to satisfy compliance, risk assessment, and audit use cases.

John A. Wheeler

John A. Wheeler is the founder and CEO of Wheelhouse Advisors, a senior executive advisory firm that helps global businesses achieve greater risk visibility and understanding. He leverages his expertise in risk management, cybersecurity, digital business, operational risk, and integrated risk management to provide strategic guidance and technology solutions to his clients.

INTRODUCTION

The world is becoming increasingly interconnected, and industry is no exception. Today, nearly every major business sector in some capacity relies on third parties. In previous generations, this might have been primarily from a physical perspective, with one party relying on another for goods or services. While this is still true, now the connection between parties has become intertwined with the digital realm.

Naturally, while there are many benefits to be had with this trend — particularly regarding efficiency, productivity, and better meeting sustainability commitments — there are also risks that must be accounted for. According to Deloitte's 2022 Global Third-Party Risk Management Survey, 73% of respondents now have a moderate to high-level dependence on third-party cloud service providers, with that figure expected to rise to 88% in the coming years.[9] However, for such relationships to be successful, there must be an implicit trust between organizations that transferred data will be as secure as possible against cyberattacks, data breaches, or other related cyber incidents. To gain such trust, organizations should have a dedicated and extensive third-party risk management (TPRM) program in place that exercises due diligence when onboarding third-party vendors and continuously monitoring them through the lifecycle of the relationship.

The truth, however, is that too often companies assume trust without first doing adequate due diligence. "Any third party — vendor, provider of product components, partner, or customer — can present new cyber risks to your organization," said Richard Marcus, VP, Information Security at AuditBoard. "The need for robust third-party risk management has been growing over time, and many organizations are not keeping up."

As the final part of this three-part series on cybersecurity, this Global Knowledge Brief will highlight just how significant cyber risks associated with third parties have become and address where internal auditors can fit into third-party cyber risk management.

[9] 2022 Global Third-Party Risk Management Survey, Deloitte, 2022, https://www.deloitte.com\content\dam\Deloitte\us\Documents\TPRM_Survey_Report_Interactive.pdf.

A Vast Challenge

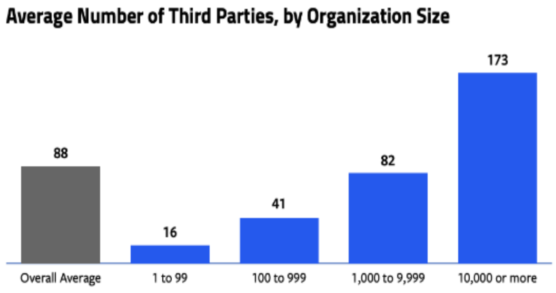
Cyber Risks Dominate Third-Party Risk Management Discussion

A risk on the rise

A recent report from CyberRisk Alliance, sponsored by AuditBoard, surveyed 209 U.S.-based security and IT leaders and executives, security administrators, and compliance professionals. It revealed just how vast the third-party cyber risk has become. Insights from the survey include:

- On average, companies use 88 third-party partners (including software vendors, IT service vendors, IT service partners, business partners, brokers, subcontractors, contract manufacturers, distributors, agents, and resellers). Numbers vary significantly based on organization size, with companies with 1-99 employees using 16 partners on average, while companies with 10,000 or more employees using 173 on average (see Figure 1).
- 57% of respondents reported they were victims of an IT security incident (either an attack or breach) in the past 24 months. Additionally, organizations on average experienced two third party-related security incidents in the past two years.
- Among those afflicted, 52% said the source of the attack was a software vendor, while 39% said a business partner, subcontractor, or IT service provider was responsible for the incident (See Figure 2)[10].

Figure 1

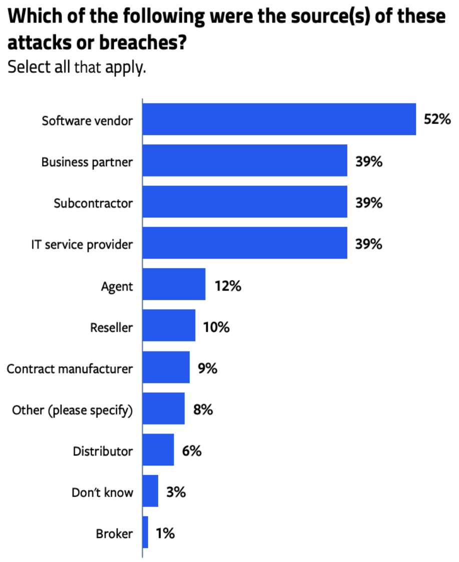


Average Number of Third Parties, by Organization Size

Q: Approximately how many third parties is your organization currently contracted with? Include all vendors (including software vendors and IT service providers), business partners, brokers, subcontractors, contract manufacturers, distributors, agents, and resellers.

Note: Graphs and data in Figure 1 and Figure 2 taken from "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," by CyberRisk Alliance and Auditboard. p. 9 and p. 18, January 2023.

Figure 2



Which of the following were the source(s) of these attacks or breaches?

Select all that apply.

[10] "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," CyberRisk Alliance and AuditBoard, January 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

Keeping Up With Change

The primary reasons for these issues are varied, but they arise from a combination of rapidly changing business models and an inability to update third-party risk management processes to match the change, according to John Wheeler, founder, and CEO of Wheelhouse Advisors. "In my experience," said Wheeler, "the biggest, most relevant risks are generated by major change. The growth challenge is driving major change by spurring companies to create new digital products and services."

On this point, Wheeler authored AuditBoard's "2023 Digital Risk Report: Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment." In a survey of more than 130 U.S. risk leaders, 21% reported they don't perform qualitative or quantitative risk assessment when managing and monitoring third-party digital risk, and 56% rely only on qualitative assessment approaches, which is limited compared to quantitative assessments.[11]

44%

THE PERCENTAGE OF ORGANIZATIONS RELYING ON MANUAL TECHNOLOGIES TO MANAGE THIRD-PARTY CYBER RISKS

AuditBoard 2023 Digital Risk Report
Pervasive Risk, Persistent Fragmentation,
and Accelerating Technology Investment

Equally concerning, said Wheeler, was that of the companies that do manage digital risks such as third-party cyber risks, an astounding 44% still rely on manual technologies (spreadsheets, email, shared drives, and Sharepoint) to do so. "It's a very time-consuming approach," he said. "The reality is that fragmented, inflexible, and compliance-driven legacy governance, GRC [governance, risk, and compliance] software simply cannot provide the connected risk capabilities needed to keep pace with digital risk — and as a result, most organizations are still relying on piecemeal manual processes."

This is particularly concerning regarding the changing attack patterns of bad actors, which grow more sophisticated by the day. "If you look at the root causes of how breaches have occurred the last few decades, most have occurred on the front door, at the application or infrastructure layers. So that's where security teams have invested their time and resources. But attackers are smart. They are going to be looking for the path of least resistance, and more often than not that is going to be through the back doors caused by gaps in third-party cybersecurity measures," said Marcus.

Regulatory Pressures

Also contributing to the pressure organizations are feeling around third-party cyber risks is the ever-changing regulatory landscape, which recently has picked up pace to match the speed of the risk. Such changes include the new mandates the U.S. federal government is placing on their supply chain partners, which has had trickle-down effects across multiple industries. "You might think that federal mandates for greater transparency regarding data security would only affect companies that do business with the federal government, but then there are third- and fourth-party requirements that flow down the supply chain and cascade through the hierarchy or service providers," said Marcus. "That creates a culture of accountability that permeates a lot of industries."

Regulatory bodies have also started taking more formal steps to address third-party cybersecurity risks. This would include the new rules recently enacted by the U.S. Securities and Exchange Commission (SEC) such as the new rules requiring registrants to disclose material cybersecurity incidents. "Even if your company isn't directly applicable to new rules or regulations, these rules permeate into the culture of cybersecurity," said Marcus. "It's a cultural change that is creating an expectation of transparency and accountability."

[11] "Digital Risk Report 2023: Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment," John A. Wheeler, Auditboard, July, 2023, https://www.auditboard.com/resources/ebook/digital-risk-report-2023/.

The Internal Audit Approach

Tips, Strategies, and Areas of Focus

Establishing a culture of cyber action

Organizations are not ignorant of these shortcomings. Indeed, most are aware of them in some capacity, even if that awareness does not always translate to organization-wide understanding and action. Although few internal audit functions can claim to have adequate cybersecurity knowledge to directly address the technicalities of third-party cybersecurity, what they can do is leverage their unique positions to unite the viewpoints of various stakeholders involved in the management of this risk (e.g., legal, procurement, IT, and the third parties themselves). Additionally, internal auditors can use their direct interaction with the audit committee and board to make sure this viewpoint is communicated regularly and accurately.

This viewpoint is extremely critical to CEOs and organizational leaders to spur appropriate action, said Wheeler, and it is something risk management functions should make an effort to understand enough to articulate. “CEOs need real-time insights from both inside and outside the organization, across the entire ecosystem of technology assets that are dynamically changing,” he said. “Through this process, they’ll have a better understanding of their digital products and services.”

Unity within the organization, however, is not enough. It must include stakeholders from outside the organization. “Each third-party relationship should have a designated owner or accountable person who is responsible for maintaining the vendor relationship, holding vendor contact information, and managing the terms of the contract,” said Marcus. “Third-party relationships differ from one vendor to the next — some may provide your organization with a designated customer support or success team that provides supplemental services, while others take an ‘off-the-shelf’ approach. Keeping lines of communication open and clear between your organization and its third parties is a major but often overlooked component of effective third-party risk management.”

Creating such a culture not only can spur preventive action; it can also increase the speed of reactions when a cyberattack or breach takes place. In the CyberRrisk Alliance report, 20% of respondents said it could take a week or more to assess an attack or breach, attributing the extended timetable to difficulties getting vendors or partners to report it or take responsibility for it.[12] Creating a positive, transparent cyber culture inside the organization and throughout its supply chain can reduce these times from week to hours, drastically decreasing losses in the process.

“The entire third-party risk management process,” said Marcus, “should be built around a culture of accountability in which everyone is aware of third-party risks.”

A continuous monitoring approach based on risk level

Beyond being a tone-setter, internal audit can and should act as a valuable resource in crafting the third-party risk management program as it pertains to cyber risks — and continuously evaluating it.

“I would say that the primary responsibility for internal audit, just like in most cases, is evaluating the effectiveness of TPRM program,” said Marcus. “This can include a complete inventory or picture of all of the third parties that are in use at the organization, understanding the risks those third parties can expose the organization to, and understanding how the organization is evaluating the strength of controls in those third party organizations.”

[12] “Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations,” CyberRisk Alliance and AuditBoard, February, 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

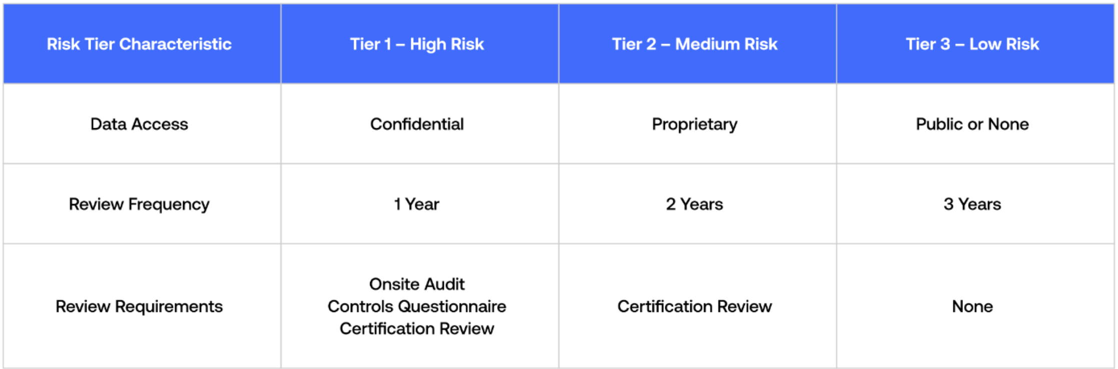
Again, while subject matter experts should be used for technical analysis, many of the risk management principles used by internal audit are applicable to this topic.

For example, internal audit should have a firm understanding of risk analysis, often visualized using heat maps or other tools. Such tactics can be used as a guide for stakeholders responsible for third-party onboarding and monitoring to grasp a better understanding of who and what to prioritize.

"The most important success factor for a TPRM program is to structure and formalize continuous monitoring activities based on risk level," said Marcus. "Higher-risk third parties should receive more attention more frequently, and lower-risk third parties should receive less attention less frequently." Of note, he continues, is that while the third party in question may not be a high risk within itself, the nature of the relationship — such as what kind of data is being transferred (e.g., confidential data, customer data, proprietary data) — could raise or lower risk categorization.

To help with this task, AuditBoard uses the following example (Figure 3) as a starting point for how to structure reviews related to the three following risk tier categories:[13]

Figure 3



Risk Tier Characteristic	Tier 1 – High Risk	Tier 2 – Medium Risk	Tier 3 – Low Risk
Data Access	Confidential	Proprietary	Public or None
Review Frequency	1 Year	2 Years	3 Years
Review Requirements	Onsite Audit Controls Questionnaire Certification Review	Certification Review	None

Note: Graphs and data in Figure 1 and Figure 2 taken from "Effective Third-Pary Risk Management: Key Tactics and Success Factors" by AuditBoard. p. 8, 2022.

Third-party vetting does not end at onboarding but should be continuously reviewed based on the perceived risk level. Ensuring stakeholders stay abreast of their own commitments to regular reviews, as well as the processes they use to conduct such reviews, should fall squarely within the internal audit risk universe. Ideas for such processes could include:

- Checking compliance certifications and reports such as SOC 2. Common frameworks to check compliance certifications include SOC 2, ISO 27001, and NIST SP 800-161.
- Use of standardized questionnaires. These could include the Standardized Information Gathering Questionnaire (SIG) or the CCM and CAIQ from the Cloud Security Alliance.
- Security controls questionnaires.

Embrace Software Solutions

[13] "Effective Third-Party Risk Management: Key Tactics and Success Factors," AuditBoard, January, 2022, https://www.auditboard.com/resources/ebook/effective-third-party-risk-management-key-tactics-and-success-factors/?utm_campaign=effective-third-party-risk-management-key-tactics-and-success-factors-0122022&utm_medium=download-image&utm_source=blog.

To keep so many variables together, internal audit as well as other risk management functions should also prioritize moving away from manual process in favor of software solutions. “Internal audit can be a champion for investment in technologies to make third-party risk management processes more efficient,” said Marcus. “In many situations, efficiencies of scale just require it. I remember one of the first organizations where I implemented third-party risk practices— we did risk assessments for five or six vendors and then considered expanding this process for all vendors. We were shocked to find out, however, that there were 17,000 vendors at this company. There's just no way to do that without some technology-enabled platform to facilitate scaling to the order of hundreds or thousands or tens of thousands of vendors.”

Additionally, such solutions also present an excellent opportunity for internal audit to collaborate more closely with other third-party risk functions. “Many of the barriers to collaboration involve data sharing and workflow issues,” said Marcus. “Having a technology platform where the two teams can evaluate the landscape of vendors together — using the same dashboard, the same database of vendors, etc. — allows them to work together a lot more efficiently and drive towards common outcomes.

Focus on offboarding as well as onboarding

Third-party relationships rarely last forever. However, just because a relationship formally ends does not always mean that data lines between parties close. As obvious as that may seem, these forgotten lines are responsible for some of the largest gaps found in organizations’ third-party cybersecurity systems, creating “digital backdoors” that are ripe to be exploited intentionally or unintentionally. When evaluating third-party review practices, this is something internal audit should not overlook.

“It’s essential to be detail-oriented in the offboarding phase,” said Marcus. “In today’s intertwined digital ecosystem, it’s easy to miss third-party accounts, services, or users that need to be removed or disabled. Access privileges need to be revoked, user accounts disabled, and any third-party issued software or applications removed. This is something internal audit absolutely should be looking at.”

Conclusion

The future of organizations is cyber. With each passing year, it is clear this trend is here to stay — and just because cybersecurity requires more specialized skill sets does not mean the business landscape is going to wait for stakeholders to educate themselves. Cybersecurity is a continuous journey of learning, and all parties involved in third-party relationships should consider it as such.

Thankfully, there are positive signs that organizations are accepting this reality. In the CyberRisk Alliance Business Intelligence report, nearly two out of three respondents said that the most common measure they used to prevent or mitigate the risk of third-party attacks was employee training.[14] While the risks associated with third parties will never end, policies and responses will mature to the point where they are as easily managed as any other established risk. That time is not today, but we are getting there, and effective internal audit risk-management assurance will help organizations arrive safely.

[14] "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," CyberRisk Alliance and AuditBoard, February, 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

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 fifth 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

January 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