GLOBAL KNOWLEDGE BRIEF

Cybersecurity

Part 3: Cybersecurity Third-Party Risk Management

AUDITBOARD

The Institute of Internal Auditors

Contents

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.[1] 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.

1. 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)[2].

Figure 1

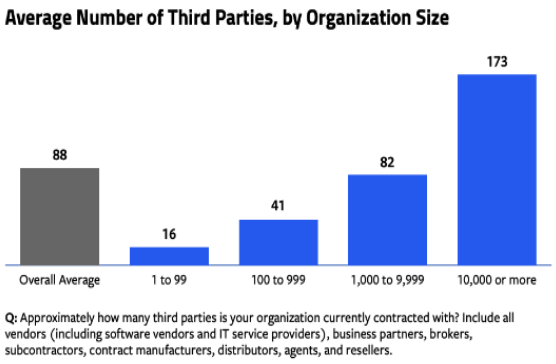
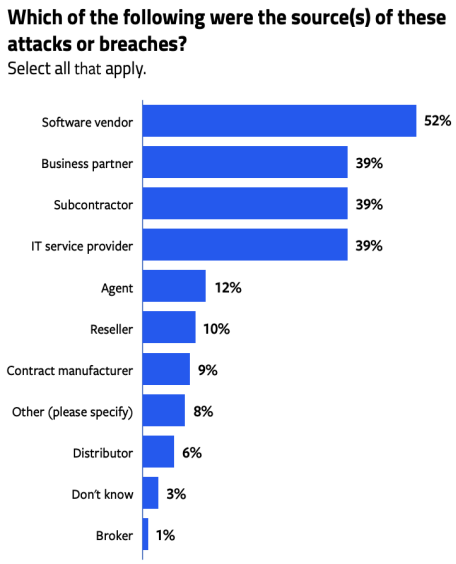


Figure 2



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.

2. "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 risk leaders in the U.S., 21% reported they did not perform qualitative or quantitative risk assessment when managing and monitoring third-party digital risk, and 56% are relying only on qualitative assessment approaches, which is limited compared to quantitative assessments.[3]

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."

3. "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/.

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.”

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.[4] 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.”

4. “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:[5]

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 in internal audit's 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

5. "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.[6] 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.

6. "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

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

December 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