CRA | Business Intelligence
A CyberRisk Alliance Resource

Third-Party Risk:

More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations

JANUARY 2023

SPONSORED BY

AUDITBOARD

Contents

Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations

FINDINGS FROM A NOVEMBER 2022 CYBERRISK ALLIANCE BUSINESS INTELLIGENCE RESEARCH STUDY

Background

While data breaches are commonplace, occasionally there's an attack so audacious that its impact reverberates long after the initial jolt. Such was the case with the SolarWinds supply chain breach, in which a nation-state surreptitiously inserted eavesdropping malware into an Oklahoma software maker's IT performance management solution used by governments and major enterprises.

While IT security teams scrambled to determine and limit their own exposure, the SolarWinds breach had a detrimental downstream impact since the attackers also accessed users' customer data. Thus, organizations — from small businesses to huge government agencies — were reminded of how vulnerable they are to cyberattacks through service providers and software with privileged access.

It's no longer enough to secure internal assets; everyone must be doubly sure any sanctioned entity with network permissions does not become an unwitting conduit for malicious activity. Managing such threats remains a daunting task, according to new research from CyberRisk Alliance Business Intelligence, which gauged companies' understanding, interest and investments in managing third-party risk.

Research methodology

The data and insights in this report are based on an online survey conducted in November 2022 among 209 security and IT leaders and executives, security administrators, and compliance professionals in the U.S. from CRA's Business Intelligence research panel. The objective of this study was to reveal organizations' experience with cybersecurity attacks originating from third parties as well as their assessments of their supply chain visibility, and other issues related to managing third-party risk. The respondent profile is as follows:

Roles/titles:

- CISOs/CROs/CIOs/CTOs (9%)
- VPs/SVPs/EVPs in IT security/risk/compliance (8%)
- Directors of IT/IT security/audit, risk, and compliance (28%)
- Managers of IT/IT security/audit, risk, and compliance (30%)
- IT security admins (16%)
- Analysts/consultants (9%)

Organization sizes:

- Small (1 to 99 employees) (8%)
- Medium (100 to 999 employees) (29%)
- Large (1,000 to 9,999) (36%)
- Enterprise (10,000 or more) (27%)

Industries:

- Education (14%)
- High-tech, IT software and telecom (14%)
- Financial services (11%)
- Manufacturing (10%)
- Healthcare (10%)
- Professional services (consulting, legal, etc.) (8%)
- Retail, trade, eCommerce, and financial services (8%)
- Government (6%)
- Other (media/communications/advertising, transportation/warehousing, non-profit, energy, utilities, construction, hospitality, and real estate) (19%)

Executive summary

Respondents from CRA Business Intelligence's November 2022 Third-Party Risk Survey believe third parties are increasingly the cause of IT security incidents, while some think they have been the primary source of attacks in the past two years. As a result, organizations are now emphasizing third-party risk, and many are devoting more attention to risk management in this area. Respondents said their increased dependency on vendors and other partners such as manufacturers, suppliers, and sub-contractors, as well as increasingly complex supply chains, lack of visibility into third and fourth-party partners (i.e., their vendors' partners), and the vast scope of data accessible to them, have vastly increased their exposure to attacks. This trend, combined with a greater global presence, use of more diversified applications, programs, and cloud solutions, and the complexity and persistence of supply chain threats and threat actors are the catalysts for recognizing and addressing the risk exposure and potential liabilities from attacks and breaches originating from third parties.

> **"We don't have visibility into their day-to-day operations, so we don't know how vigilant they are."**

Additionally, the fear of severe consequences from a third-party-related attack or breach — including business disruption, financial losses, network and infrastructure disruptions, data loss, reputational damage, and regulatory compliance failure — have convinced more senior and board-level executives to increase their oversight of proactive third-party risk management, particularly as these types of breaches continue to make headlines. Customers, regulators, auditors, and cyber insurance providers are also leaning on organizations to demonstrate proper vetting and deeper management of their partners, according to multiple survey respondents.

Despite increased awareness and more demands to secure third parties, the growth of technology and connections to different tools, services, and vendors makes implementing an effective third-party risk management program an overwhelming challenge. Organizations face a variety of obstacles in auditing and managing third parties and coming up with policies to address the risks. Dedicating the funding, time, and qualified staff to this task is daunting, and impossible for many organizations as it often competes with other priorities. Respondents pointed out that simply getting the other party to get on board and implement good security controls can be a formidable challenge. And when a third-party breach did occur, potentially exposing their organizations' sensitive data to attackers, respondents remarked they didn't always receive timely notifications from their vendor or partner, limiting their ability to be proactive in notifying customers and other stakeholders.

> **"Any contractor with access to another company needs to have access secured in the same manner."**

Organizations recognize they must adopt a comprehensive risk appetite when they work with vendors and other partners while also accepting the potential culture shift in putting greater requirements on third parties, including getting third parties to respond to questionnaires and addressing any external-facing vulnerabilities detected in their systems. Going forward, some organizations said they plan to advance their third-party programs beyond the basics in the next 12 months and invest in human resources and technology to bolster their programs.

Key takeaways from the survey

- Most respondents said they are increasingly working with more third-party products and services. The overall average estimated number of third-party partners (including software vendors, IT service providers, business partners, brokers, subcontractors, contract manufacturers, distributors, agents, and resellers) among all respondents is 88. This estimate varies with organization size: large enterprises have roughly 173 third-party partners and are much more likely to have the most complex supply chains.
- More than half of all respondents (57%) reported they were victims of an IT security incident — either an attack or a breach — related to a third-party partner in the past 24 months. On average, organizations experienced two third-party-related security incidents (attacks or breaches) in the past two years. This number increases with organization size, with respondents from the largest organizations estimating they experienced an average of five incidents during this period.
- Among those whose organizations were afflicted, 52% reported the source of their attack was a software vendor. And for nearly 4 in 10 respondents (39%), a business partner, subcontractor, or IT service provider was responsible for the incident.
- About 8 in 10 respondents said they experienced one or more consequences from these attacks. The most common were network outages/downtime, reported by 31% and disruption in customer service (28%). Another 27% suffered a business disruption or shutdown, while 24% said their data was stolen/exfiltrated. One in five respondents also reported financial losses or supply chain disruptions.
- While organization size has no effect on the perceived importance of third-party risk management, the priority of these initiatives is highly correlated to the size of an organization. For example, about 6 out of 10 respondents (59%) from large enterprises specified third-party risk as either a critical or high priority at their organization whereas smaller organizations are less likely to have this at the top of their priority lists.
- Concerns about managing third-party risks centered around the lack of human resources, budgets, and technology solutions. Nearly half of all respondents (49%) rated the lack of qualified staff to implement a third-party management program as highly concerning (rating this a 5, 6, or 7 out of 7), while the lack of visibility into third-party risks (45%), insufficient budget (44%), and lack of an automated third-party

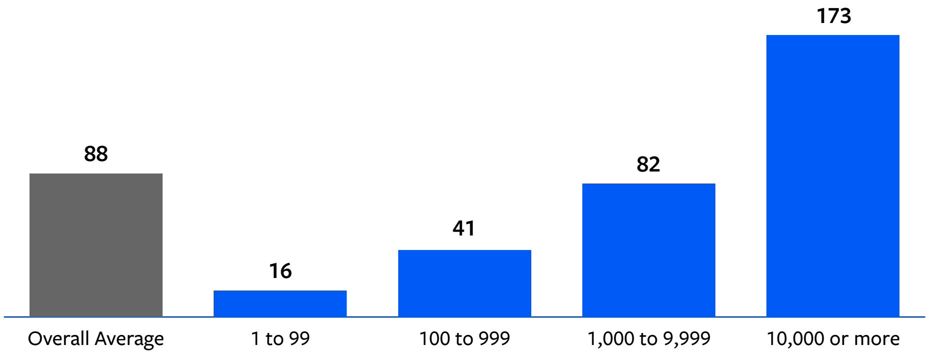
management technology solution (44%) were also similarly rated as highly concerning.

- Overall, employee training is the most common measure used to prevent or mitigate the risk of third-party attacks, as reported by nearly two out of three respondents. Additionally, annual risk assessments, third-party policies and standards, third-party attestation reports, and pre-contact processes and controls were also used by at least four out of 10 respondents. The largest organizations are more likely to use in-depth assessments of third parties (46%), third-party attestation reports (51%), third-party oversight or governance staff (40%), and automated third-party risk management tools or platforms (44%).
- The majority of respondents said they can assess the impact of a third-party partner or supply chain attack/breach in less than one week, with one in five indicating they can make an assessment within several hours. Another 20% said it takes a week or more to assess. Some attributed these longer assessment times to difficulties in getting their vendor or partner to take responsibility for the incident as well as vendor delays in notification or reporting.
- Overall, more than half (56%) said they expected “some investment” and 23% expected a “limited investment” in third-party risk management technology or resources in the next 12 months. While there were no respondents from small organizations (less than 100 employees) who said they expect a significant third-party risk management investment in 2023, 27% from the largest organizations anticipate significant investment in this area.

Third-party partnerships and supply chain complexity on the rise

Most respondents said they are increasingly working with more third-party products and services and have substantially increased their reliance on third-party partners. The overall average estimated number of third-party partners (including software vendors, IT service providers, business partners, brokers, subcontractors, contract manufacturers, distributors, agents, and resellers) among all respondents is 88. This estimate varies with organization size: the smallest organizations are partnered with an average of about 16 third parties, while large enterprises have roughly 173 third-party partners.

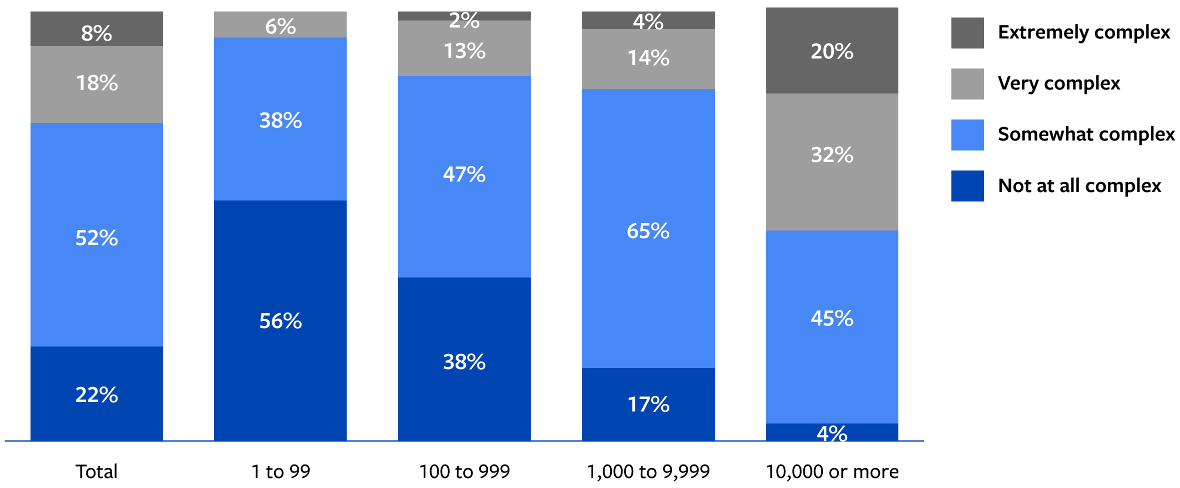
Average Number of Third Parties, by Organization Size



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.

Overall, nearly 8 out of 10 respondents (78%) reported some level of complexity in their supply chain. Of those, 26% categorized them as "very" or "extremely" complex. Unsurprisingly, the complexity of an organization's supply chain is associated with organization size in which the largest organizations (those with 10,000 or more employees) are much more likely to have the most complex supply chains: more than half of respondents (52%) in this segment indicated their supply chains are very or extremely complex.

Supply Chain Complexity, by Organization Size

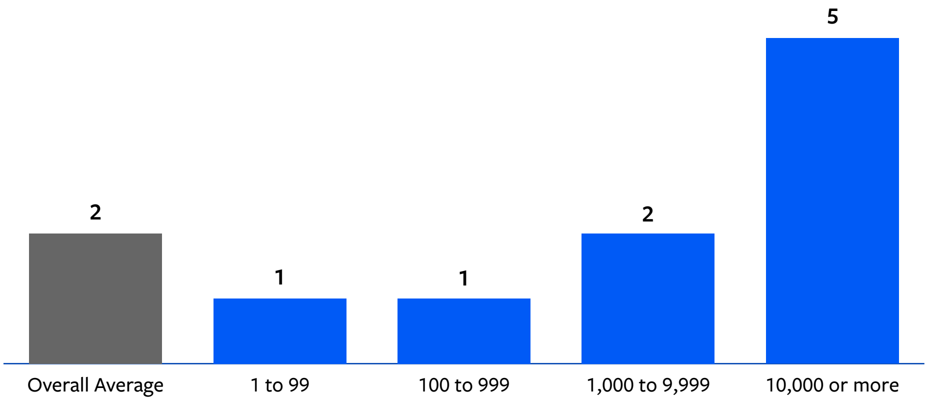


Q: How complex is your supply chain?

Business and custom service disruptions, data loss, and damaged reputation arising from third-party related incidents

More than half of all respondents (57%) reported they were victims of an IT security incident — either an attack or a breach — related to a third-party partner in the past 24 months. On average, organizations experienced two third-party-related security incidents (attacks or breaches) in the past two years. This number increases with organization size, with respondents from the largest organizations estimating they experienced an average of five incidents during this period.

Average Number of Third-Party Security Incidents, by Organization Size



Q: To the best of your knowledge, approximately how many IT security incidents (attacks or breaches) related to your third-party partners has your organization experienced in the past 24 months?

In recounting their experiences with attacks and breaches originating from third parties, respondents' descriptions ranged from minor incidents with little organizational impact, to major attacks and breaches in which their organization suffered serious consequences. Typically, organizations encountered business, customer service, and supply chain disruptions and delays, computing infrastructure failure or downtime, re-installations and re-implementations of software and business processes, stolen data/data leakage, and additional remediation resources and extra manual efforts as a result of a third-party incident. In some cases, organizations also faced reputational repercussions, legal actions, and even FBI investigations.

> **"Our supplier of PCs was hacked and it affected their supply chain, billing, AR/AP, and [caused] lots of frustrations between us."**

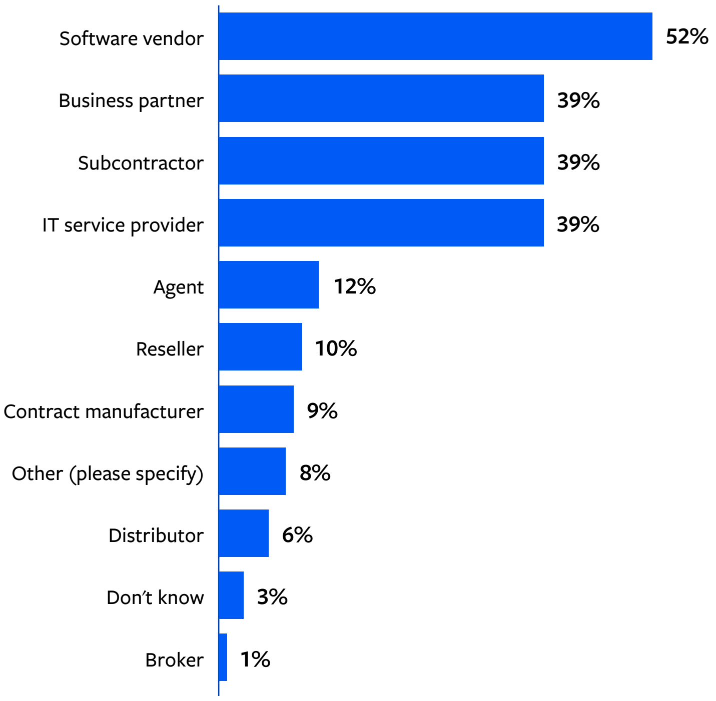
Respondents also revealed their accounts of frustrating vendor delays and even coverups in notifying or correcting the issues — several stating it took weeks, months, and even years to recover from a third-party-related attack. According to one respondent describing their experience following an attack, "It was difficult to determine and attribute" and "very difficult to get the vendor to take responsibility."

> **"A third-party data processor was compromised which exposed our data to the attackers. We were notified more than one month after the attack was discovered by the third party."**

Among those whose organizations were affected, 52% reported the source of their attack was a software vendor. And for at least nearly 4 in 10 respondents (39%), a business partner, subcontractor, or IT service provider was responsible for the incident.

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

Select all that apply.

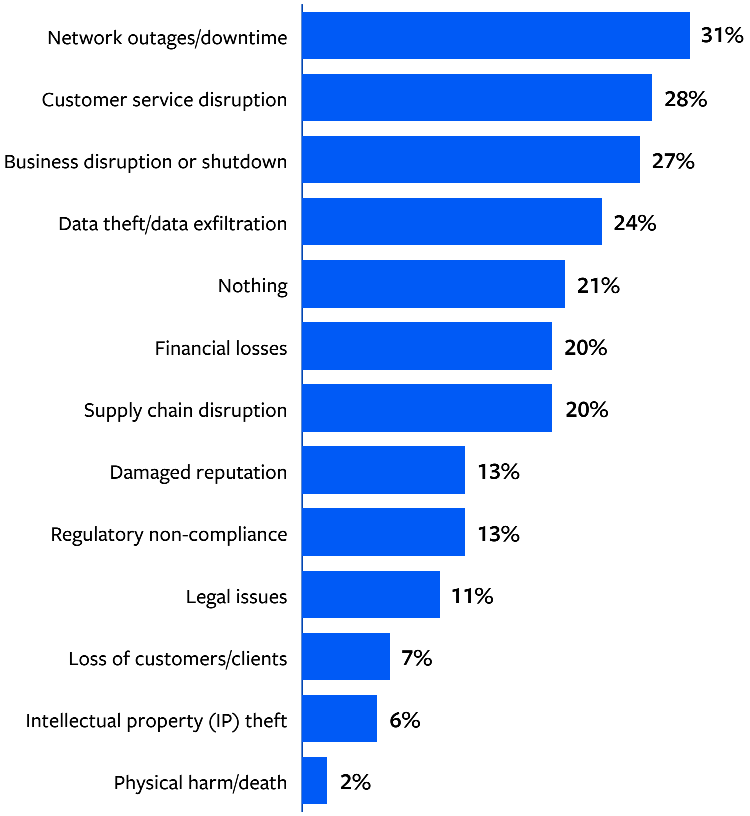


Overall, the consequences for organizations impacted by third-party attacks or breaches were serious, and in some cases, disastrous. About 9 in 10 respondents said they experienced one or more consequences from the attacks related to third parties. The most common were network outages/downtime, reported by 31% and disruption in customer service (28%). Another 27% suffered a business disruption or shutdown, while 24% said their data was stolen/exfiltrated. One in five respondents also reported financial losses or supply chain disruptions. Other impacts included damaged reputation (13%), regulatory non-compliance (13%), and legal issues (11%). Several respondents also reported physical harm/death as a result of their attack.

> **"An incorrectly configured AWS bucket was taken over, and customer data was stolen. Customer-facing sites were down, and calls and emails were arriving. A few weeks later, we had sporadic calls coming in from customers who were asking about their orders."**

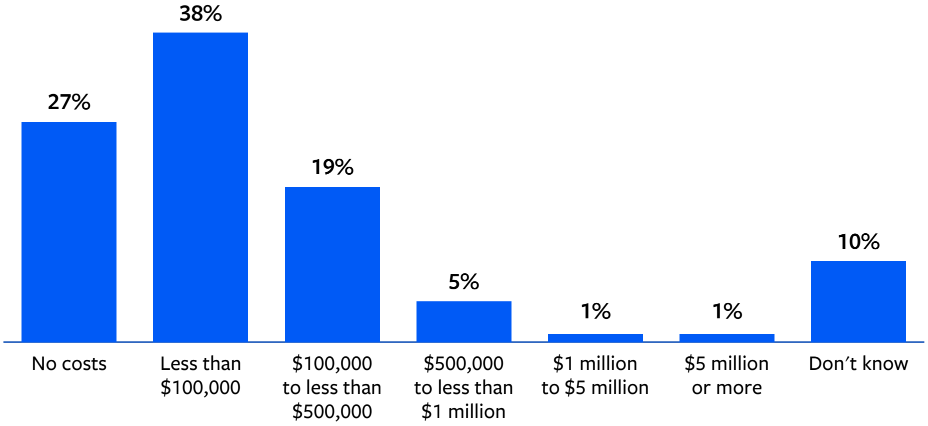
Which of the following did your organization experience as a result of any of these third-party partner attacks or breaches?

Select all that apply.



Nearly two out of three respondents (64%) also reported some level of imposed costs and fees associated with their attack/breach. While 38% estimated their cumulative direct and indirect losses and costs — including legal fees, downtime, and loss of customers and business — were less than $100,000, another 26% said these costs exceeded $100,000.

What were the estimated cumulative financial costs to your organization related to these third-party attacks or breaches?*



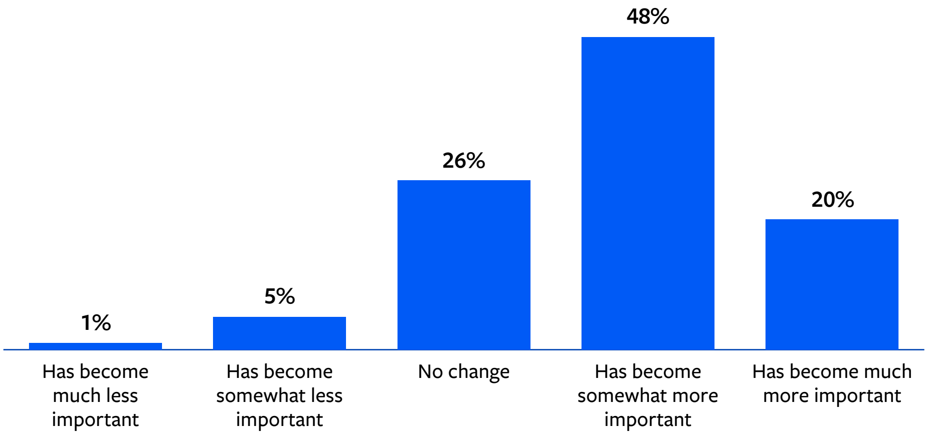
*Include all direct and indirect costs related to detection and notification, legal fees, system downtime, missed business, loss of customers, reduced shareholder value, etc.

> **"Partner had ransomware; shut down connections/services for our organization and impacted our supply chain and our patients."**

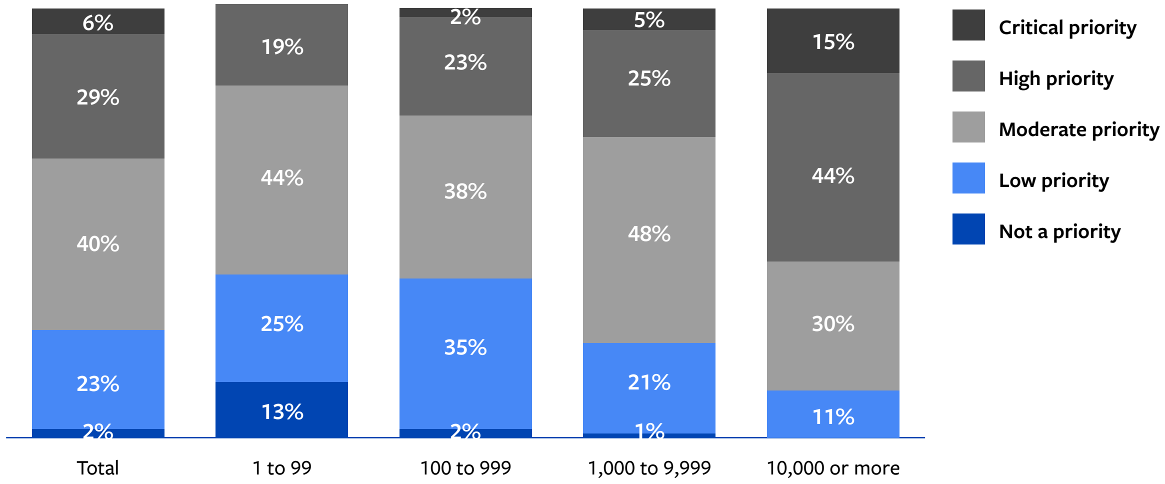
Large organizations more likely to prioritize third-party risk management

Compared to 2021, 68% of respondents said that third-party risk management has become either somewhat or much more important at their organization. However, nearly two-thirds (65%) have relegated the priority of managing third-party risk to no more than "moderate" at their organization. While organization size has no effect on the perceived importance of third-party risk management, the priority of these initiatives is highly correlated to the size of an organization. For example, about 6 out of 10 (59%) respondents from large enterprises specified it as either a critical or high priority at their organization whereas smaller organizations are less likely to have this at the top of their priority lists.

Compared to 2021, how has the importance of third-party risk management changed at your organization?



Priority of Managing Third-Party Risk, by Organization Size



Q: Overall, what is the priority of managing third-party risk at your organization?

In many cases, respondents attributed the increased importance of third-party risk to their heightened awareness of the issues. In describing the reasons for their deepened attention, many referred to their growing reliance and partnerships with third-party vendors, particularly since the onset of the COVID-19 pandemic and the shift to remote workforces. Their expanded use of diversified applications and programs, SaaS, and other cloud solutions were also factors in their greater focus on third-party risk. Others mentioned the publicity around high-profile, third-party attacks and that publicly disclosed vulnerabilities and breaches had raised their own awareness while also alerting senior management to the potential dire consequences if the vulnerabilities were not proactively addressed.

> **"We have so many third-party vendors and when data breaches show up on CNN, the C-suite and board perk up and expect something to be done proactively to protect our institution from lapses in security from our third-party vendors."**

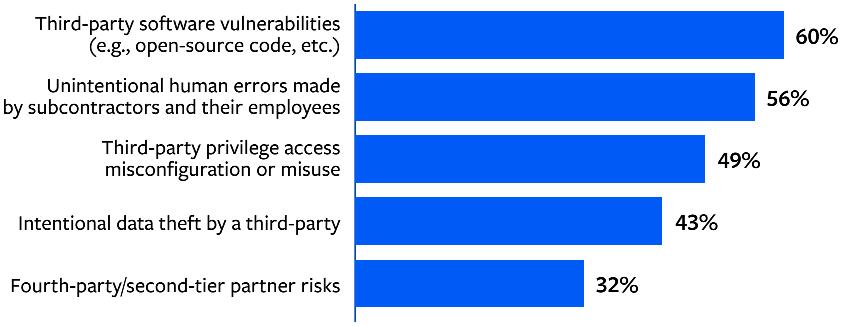
Respondents also stressed the increased complexities of their supply chains, while some explained they did not have a full "birds-eye view" into the security of their partners as well as their fourth-party vendors (i.e., their vendors' vendors), raising serious concerns about their vulnerabilities and the potential damage caused by the "unknowns" in their supply chain.

> **"We understand that the cybersecurity landscape is continuously evolving and that new threats are emerging on a daily basis. We cannot afford any business disruption from cybersecurity threats, especially if those disruptions were avoidable/ preventable."**

Respondents also commented that their customers, cybersecurity insurance providers, auditors, and/or regulators were putting more pressure on their organization to step up security and management of their vendors and partners.

In rating their perception about the risk levels of potential incidents caused by third parties, the largest proportion of respondents (60%) rated third-party software vulnerabilities a 5, 6, or 7 (rating out of 7 in which 7 is the highest risk). Nearly the same number of respondents (56%) provided these ratings for unintentional human errors made by subcontractors and their employees. Also, for almost half of all respondents, third-party privilege access misconfiguration or misuse (49%) as well as intentional data theft by a third party (43%) were considered high risks to their organization. However, less than one-third (32%) believe second-tier partners pose a high risk to their organization.

High-Risk Incidents (% rating 5, 6, or 7)

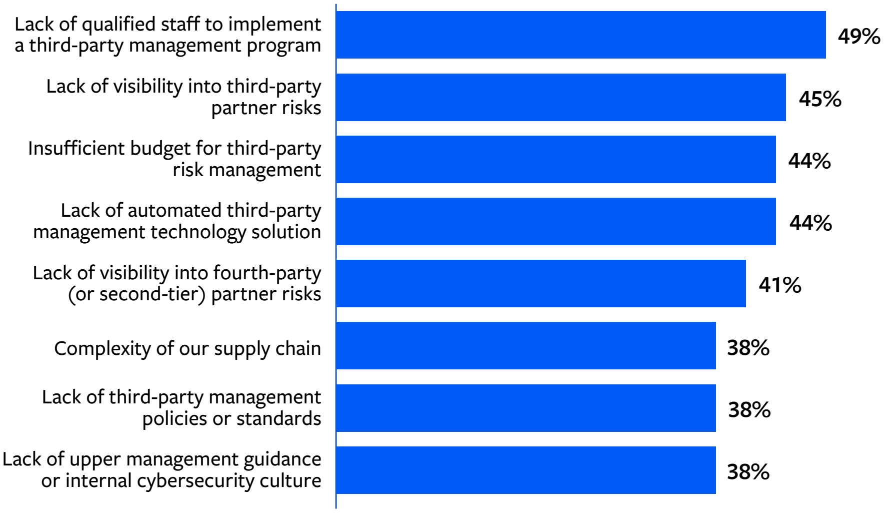


Q: How much of a risk does each of the following pose to your organization? Rate each on a scale of 1 to 7 where 1 is ″No risk at all″ and 7 is ″Extremely high risk.″

Concerns about managing third-party risks centered around the lack of human resources, budgets, and technology solutions. Nearly half of all respondents (49%) rated the lack of qualified staff to implement a third-party management program as highly concerning (rating this a 5, 6, or 7 out of 7), while the lack of visibility into third-party risks (45%), insufficient budget (44%), and lack of an automated third-party management technology solution (44%) were also similarly rated as highly concerning.

> **"There is increased reliance on SaaS vendors/services and less visibility into the downstream data processing in these third-party vendors."**

Level of Concern in Managing Third-Party Risk (% rating 5, 6, or 7)



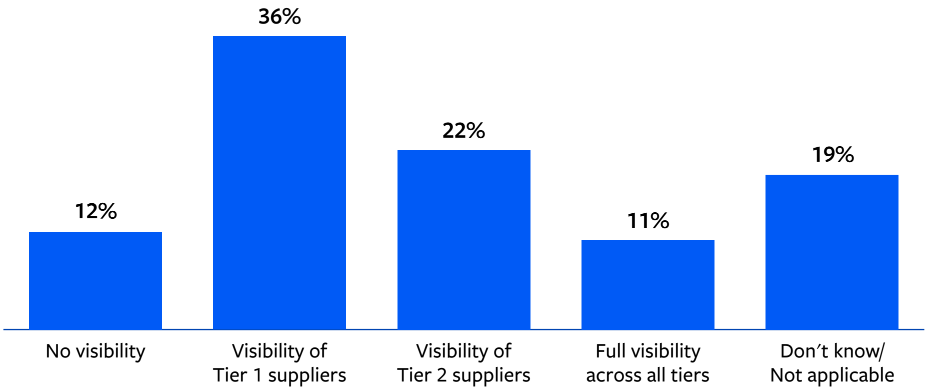
Q: How concerned are you about the following in managing third-party risk at your organization? Rate each on a scale of 1 to 7 where 1 is ″Not at all concerned″ and 7 is ″Extremely concerned.″

Murky visibility across the supply chain for most

As supply chains grow and become more complex, supply chain visibility, or the ability to track all tiers of the supply chain, becomes increasingly important. Among all respondents surveyed, visibility varied and was highly influenced by the complexity of their organizations' supply chains. The largest proportion of respondents (36%) reported they have visibility into only their tier one suppliers. Another 22% said they have visibility into their tier-two suppliers; these organizations are more likely to be larger organizations with highly complex supply chains. Only 11% said they have visibility across all tiers, regardless of their supply chain complexity. Another 12% said they have no visibility at all; these organizations are most likely to be the smallest organizations with the least complex supply chains.

> **"The third-party ecosystem has become complex, and the open-source software system has been attacked and is an easy target. Without having clear visibility into the remediation process, it poses a big risk."**

Which of the following best describes your organization's highest level of visibility into its supply chain tiers and their risks?



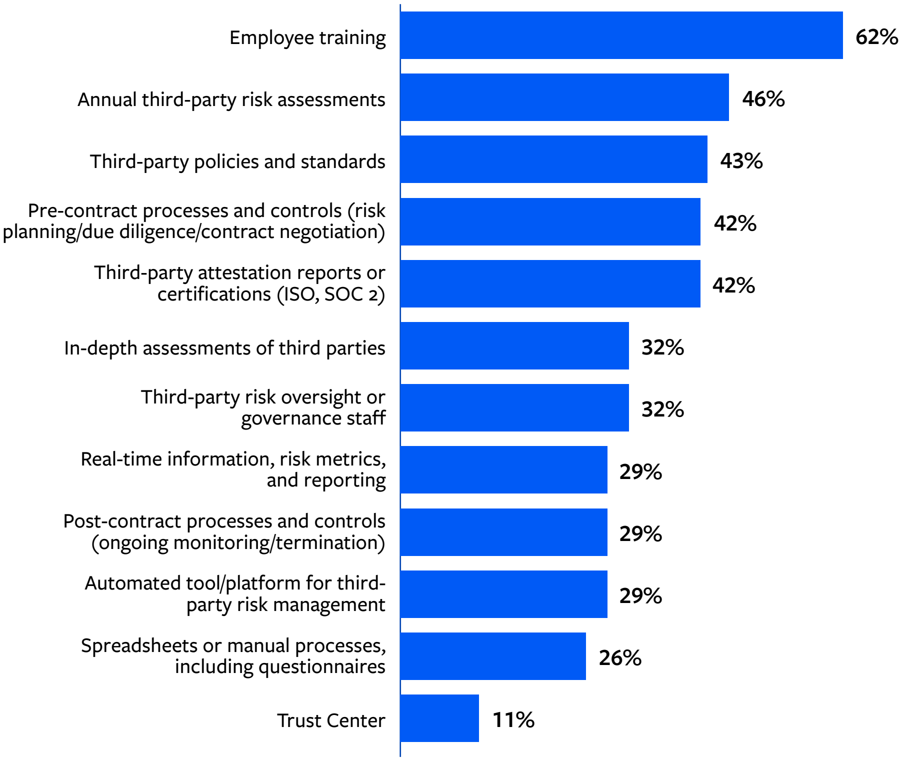
Third-party risk management: a resource-intensive process

Overall, employee training is the most common measure used to prevent or mitigate the risk of third-party attacks, as reported by nearly two out of three respondents. Additionally, annual risk assessments, third-party policies and standards, third-party attestation reports, and pre-contact processes and controls are also used by at least four out of 10 respondents. The largest organizations were more likely to use in-depth assessments of third parties (46%), third-party attestation reports (51%), third-party oversight or governance staff (40%), and automated third-party risk management tools or platforms (44%).

> **"We use more 3rd parties for services throughout the enterprise, and vulnerabilities for data, security and performance are even more visible and critical."**

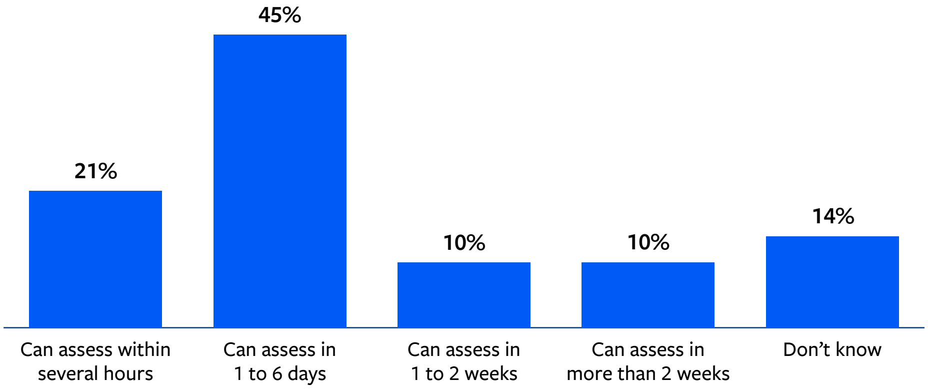
Which of the following does your organization use to prevent or mitigate third-party risk?

Select all that apply.



The majority of respondents said they can assess the impact of a third-party partner or supply chain attack/breach in less than one week, with one in five indicating they can make an assessment within several hours. Another 20% said it takes a week or more to assess. Some attributed these longer assessment times to difficulties in getting their vendor or partner to take responsibility for the incident as well as vendor delays in notification or reporting.

What are your organization's capabilities in assessing the impact of a third-party partner/supply chain attack?



Roadblocks in staffing, budgets, processes, and technology put organizations at higher risk

In weathering the third-party risk storm over the next 12 months, respondents said they face a multitude of challenges as the number of third-party vendors increases and their supply chains become more complex. Many indicated they are likely to struggle with the inability to find staff who are sufficiently trained in auditing and managing third party resources. Budget constraints also continue to persist as does the lack of buy-in from executive management in recognizing and proactively managing third-party risks. Respondents believe they will also continue to struggle with identifying third-party risks, creating internal policies, and ensuring that third parties are vetted and adhere to compliance requirements (e.g., ISO compliance, HIPPA, and PCI) wherever necessary.

Respondents noted that, in order to overcome some of their third-party challenges, they will need to address the limited visibility into their supply chains, identify critical vendors by risk tier, and establish a process for vetting and periodic reviewing of their third-party partners. They said they will also need better governance, stronger contracts, and more accountability on both sides.

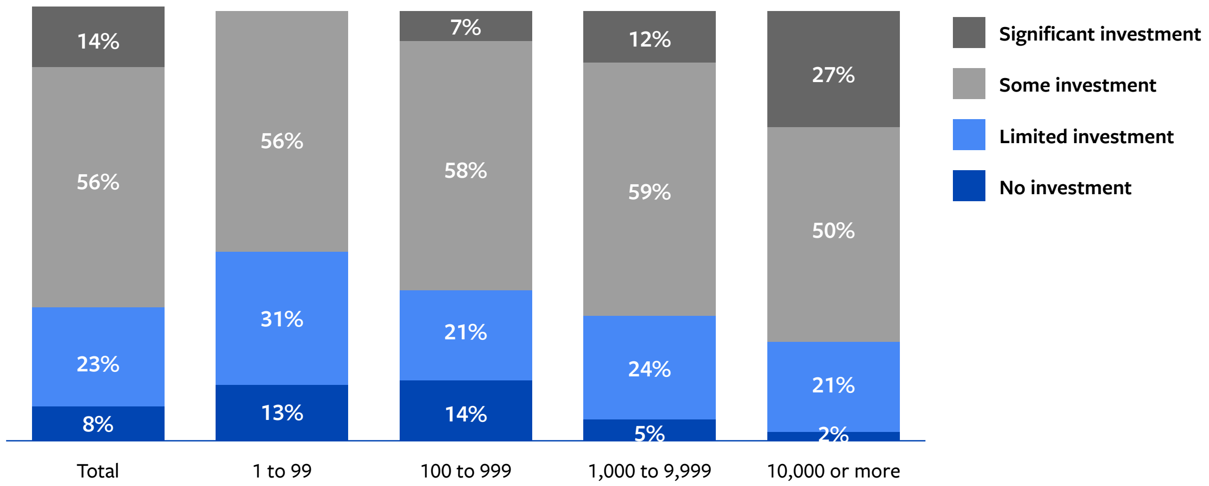
> **"The unknown risks that have not yet been encountered are the top challenges in managing third-party risk in the next 12 months."**

Without adequate human resources, adequate funding, "tone at the top" management oversight, security controls and processes, technology/automation for centralized vendor management, vendor assessment, risk analysis, and reporting, organizations will be at a disadvantage in fully securing their third parties.

> **"I think our top challenge is just to develop a process to manage third party risk that all parties can abide by and that works."**

Despite issues with reduced budgets and funding, many respondents said their organization is planning to invest in technology and staffing at some level to help mitigate third-party risk in the next 12 months. Overall, more than half (56%) said they expected "some investment" and 23% expected a "limited investment." Only 14% indicated their organization was planning a significant investment in resources and technology to manage third-party risks. The level of investment is, of course, associated with organization size: while there were no respondents from small organizations (less than 100 employees) who said they expect a significant third-party risk management investment in 2023, 27% from the largest organizations anticipate significant investments in this area.

2023 Investment in Third-Party Risk Management, by Organization Size



Q: To the best of your knowledge, what level of investment (for resources and/or technology) is your organization planning in the next 12 months to improve the effectiveness of its third-party risk management capabilities?

Conclusion

The need for greater transparency — from better visibility into who is a supplier or provider, to dashboards tracking trusted vendors with privileged access — is paramount to enterprises maintaining trust in third-party relationships. Given the potential financial, reputational, or legal fallout from a third-party breach, organizations recognize the need to proactively assess and monitor the increasing number of outside providers helping them do business. They also need to foster collaboration to ensure successful remediation when a security event does occur.

That commitment, however, doesn't always result in action. The study also showed that beyond recognizing the need to better manage third-party risks, organizations are torn on how to reduce these risks. Supply chain disruptions, IT complexities, and ongoing talent shortages have created the perfect storm for third-party risk, affecting organizations of all sizes and industries.

Related CRA Business Intelligence reports

- **Threat Intelligence: Critical in the Fight Against Cyber Attacks, But Tough to Master** (December 2022)
- **Ransomware Ready: Organizations Fight Back with More Aggressive Strategies and Technology** (November 2022)
- **The Harsh Realities of Cloud Security** (October 2022)
- **Zero Trust Adoption Faces Ongoing Headwinds** (October 2022)
- **Endpoint Security: Security Pros Concerned About the Proliferation of Non-Traditional Devices and Endpoints** (September 2022)
- **Organizations Adopt Aggressive, More Proactive Vulnerability Management Strategies in 2022** (August 2022)
- **Threat Intelligence: The Lifeblood of Threat Prevention** (July 2022)
- **CRA Study: Attackers on High Ground as Organizations Struggle with Email Security** (July 2022)
- **Security Teams Struggle Amid Rapid Shift to Cloud-Based Operations** (June 2022)
- **CRA Study: XDR Poised to Become a Force Multiplier for Threat Detection** (May 2022)
- **CRA Study: Zero trust Interest Surges, But Adoption Lags as Organizations Struggle with Concepts** (April 2022)
- **CRA Study: Managing Third-Party Risk in the Era of Zero trust** (March 2022)
- **CRA Ransomware Study: Invest Now or Pay Later** (February 2022)
- **CRA Research: A Turbulent Outlook on Third-Party Risk** (January 2022)

About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, SecurityWeekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. **Learn more**.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 35% 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**.