CRA | Business Intelligence
A CyberRisk Alliance Resource

Managing Third-Party Risk in the Era of Zero Trust

FINDINGS FROM A Q4 2021 RESEARCH STUDY

Sponsored by

SecurityScorecard

Managing Third-Party Risk in the Era of Zero Trust

FINDINGS FROM A Q4 2021 RESEARCH STUDY

BACKGROUND

Look at the biggest data breaches of 2021 and you'll notice a connection between victims and vendors that unknowingly served as conduits of attack. One of the biggest attacks involved IT software provider Kaseya, whose vulnerable systems were exploited by a ransomware gang to insert malicious code into a routine software update. Among the hundreds of known victims locked out of their files and systems were schools, pharmacies, supermarkets, municipalities, and a national railway system.

Given this perceived weakness in vendor relations, more organizations are reevaluating who they work with and how they conduct business with partners outside network perimeters. In doing so, organizations are beginning to better understand the importance of Zero Trust and more restrictive access controls as part of third-party risk management.

Created a decade ago in response to an outdated assumption that everything inside an organization's network should be implicitly trusted, Zero Trust essentially eliminates that implicit trust and requires continuous validation at every stage of a digital interaction. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern environments and enable digital transformations by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular, "least access" policies.

"SecurityScorecard is proud to partner with the CyberRisk Alliance to uncover insights into how organizations of all sizes are managing third-party risks, which are often the primary vector for a malicious cyber attack. The report's findings highlight why organizations must have a comprehensive view of their cyber ecosystem not just to protect themselves, but also to know if their vendors are well protected. Every organization is only as strong as its most vulnerable third party."

–Aleksandr Yampolskiy, CEO and Co-founder of SecurityScorecard

RESEARCH METHODOLOGY

The data and insights in this report are based on an online survey conducted from October through mid-November 2021 by CyberRisk Alliance among 250 U.S.-based IT and cybersecurity decision-makers and influencers. Seventy-one percent worked at organizations with 1,000 or more employees, while the remaining 29% worked at smaller organizations. The vast majority of those surveyed worked in the private sector, with 49% representing financial services and another 16% in healthcare compared to 26% working for federal, state, and local governments or education. The remaining 9% represented other fields, such as retail. The study was underwritten by SecurityScorecard, the global leader in cybersecurity ratings.

Survey objectives were to gauge how well organizations understand and manage risks associated with third-party relationships. Study participants were asked about their own vendor relations, concerns, and challenges in managing certain risks, and the role of Zero Trust as a risk mitigation tool. Study participants provided their responses to structured survey questions and were encouraged to provide corresponding comments where applicable.

EXECUTIVE SUMMARY

Public and private sector organizations grant dozens, sometimes hundreds, of third parties' access to their private networks and sensitive databases as part of their ordinary course of business. Organizations rely on third parties for everything from expense reporting and email services to managing industrial control systems. More than a third of participants in this study had at least 100 third-party relationships, with

some sectors, such as healthcare and government, more likely to work with 500 or more vendors at any given time.

Each vendor creates additional vulnerabilities for organizations by expanding the number of entry points into an organization's digital footprint. Yet organizations lack the continuous visibility and knowledge of the security of these third-party networks that they have within their own networks.

Given such a large expansion of attack surface, it is no surprise that 91% of respondents had experienced a security incident during the past 12 months that tied back to one of those third parties. That ubiquitous threat is likely why respondents by and large expressed some level of concern with experiencing another breach or falling out of compliance due to a partner vulnerable to attacks.

Among the study's key findings:

- Ninety-five percent of respondents expressed some level of concern with IT security risks from third-party business relationships, with two-thirds of participants seeing a significant increase in third-party related security events at their organizations during the past year.
- Those working in the heavily regulated financial services sector were most apt to report a third party-related cyber event.
- The most popular mitigation strategies in managing third-party IT security risks involve a hybrid approach — that is, they do some, but not all, of the work in-house.
- Nearly one-third are very interested in adding technology solutions to their risk management programs, particularly to improve response/remediation times, risk assessments and regulatory compliance stances. However, priorities for managing third-party risk are contingent on the industry being served. For instance, regulatory compliance is a top priority for healthcare, while risk assessment is a priority for financial services. Insurers most wanted partner collaboration, while government organizations at the state, federal and local levels wanted to improve response/remediation times.
- While there are numerous options to reduce third-party risks, adoption of a zero-trust model appears to be growing in interest. A majority of those surveyed were at least considering — if not already incorporating — principles of zero trust to reorganize privileges and restrict third-party user and device access to their networks.

- The biggest performance gaps between expectations and results for a chosen mitigation path involved identifying high-risk third parties, risk assessment and ongoing monitoring capabilities.

LEANING IN TO PROTECT ENTERPRISES FROM THOSE THEY LEAN ON

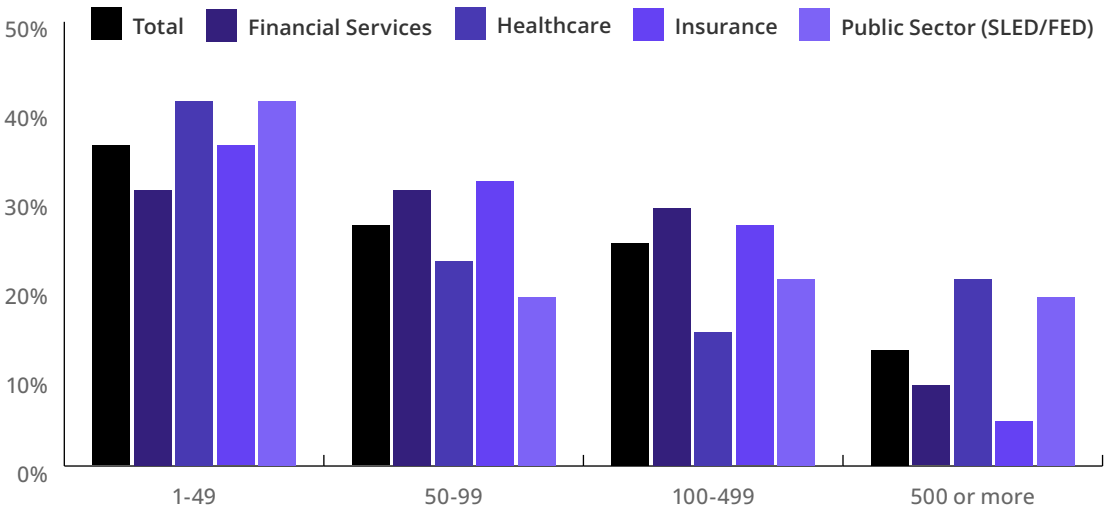
Enterprises typically engage with independent consultants, consulting firms, software vendors, and others when they don't have the means to perform a function in house, especially if a role or solution falls outside their core competencies. But such outsourcing involves a significant upfront investment, and a significant increase in risk exposure. In order to outsource business functions to a third-party, the enterprise must integrate that third-party with the internal processes, networks, and data that the business function requires.

Outsourcing requires a level of surety and "trust", which is much higher than a commodity supplier. These vendors with access to sensitive data and/or internal network assets are considered the enterprises' "trusted third-parties." These "trusted third-parties" are in effect acting on behalf of the enterprise, so they must follow all of the same rigorous regulatory standards for handling PII/PHI data and network security as the internal employees of the enterprise.

"It takes up to a year to onboard a third-party software provider, so we cannot build new capability very quickly, and our third parties tend to be unfamiliar with the rigors of banking regulatory compliance, so we need to educate them," said one survey respondent.

Despite onboarding challenges, the survey reveals that 38% of respondents currently contract with more than 100 "trusted third parties" and 13% currently contract with 500 or more such parties. Those in healthcare or public sector markets tended to have the highest number of trusted third parties under contract.

Number of Third-Party Partners, by Sector



Frustrations with how frequently third parties were introduced to operations were noted among respondents. A senior IT engineer in the insurance industry, for instance, worried about "staying ahead of the [third-party] risks as they are coming at us so quickly." A counterpart in healthcare noted, "Too many partners, not enough resources to manage."

Their concerns were warranted. Almost everyone (91%) reported their organization had experienced at least one IT security incident related to a third-party partner in the past year. Fifteen percent reported 20 or more partner-related incidents.

Those working in financial services were most likely to report a cyber incident involved a third-party breach. The financial services sector, a frequent target of cybercriminals is also heavily regulated and therefore required to report such incidents to authorities.

The pandemic accelerated a remote work movement that also presented additional security challenges. Employers suddenly had to provide employees secure access to networks and databases remotely, possibly over public Wi-Fi or unprotected home networks. Their vendors and contractors were challenged in the same way.

"As our endpoints increase with more employees working in a hybrid working environment, we increasingly need help from third-party partners on endpoint security management and support."

– IT Director, Financial Services

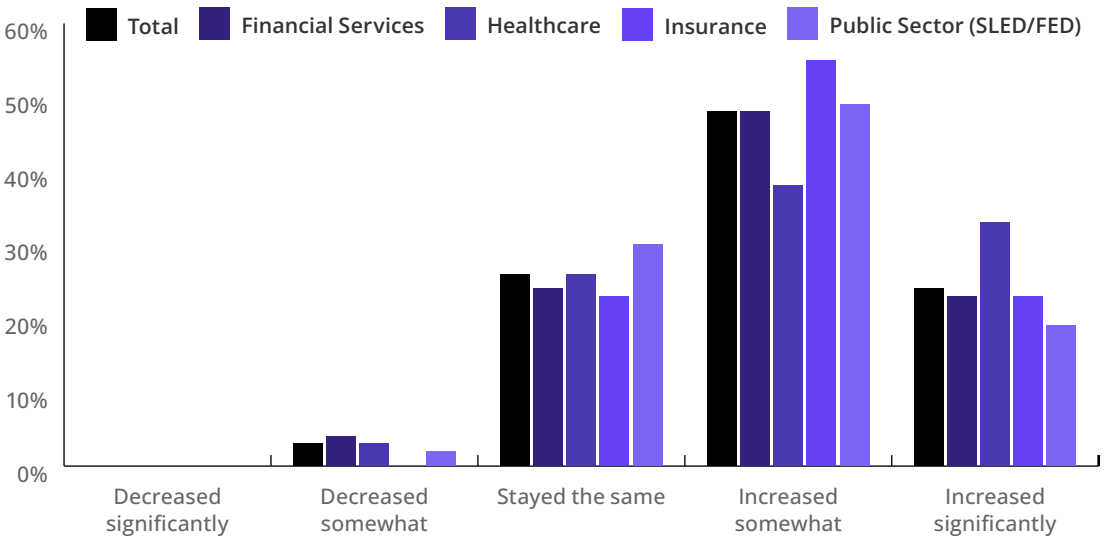
Given the past two years' evolving workforce configurations, it's easy to understand why two-thirds of respondents saw an uptick in third-party security incidents during the last 12 months. Motivations, however, differed significantly by industry. For instance, regulatory compliance was the top priority for healthcare, while those working in the public sector were most concerned with remediation times. Insurers were more likely to worry about partnerships and supply chains, and financial service providers ranked risk assessments and remote monitoring as the biggest concern.

CHALLENGES FROM INCREASED THIRD-PARTY RISK EXPOSURE

With cybersecurity incidents on the rise, it's no wonder everyone wants to reduce their risk exposure when it comes to vendors and contractors. And we mean everyone — virtually every survey participant registered some level of concern. Most were mildly (20%) or moderately (40%) concerned, while 27% were very concerned about the threat posed, particularly those working in healthcare. In that industry, 32% of respondents were seriously concerned about the third-party threats, which was higher than other sectors.

Again, stakes are higher in healthcare, where a compromised medical device can damage more than IT systems or a health system's reputation. Ransomware gangs have long placed regional hospitals in their crosshairs, knowing a disruption in service could be deadly. Not to mention pilfered patient records are more valuable than financial ones on the dark web, given someone's private health information cannot be replaced like a stolen credit card number.

Change in Concern about Third-Party IT Security Risks, by Sector



Such concern levels are inversely matched by confidence levels: Everyone is worried to some degree about their ability to prevent or mitigate IT security risks associated with their third-party relationships. This is especially disconcerting for those who partner with vendors that use subcontractors, creating tiers of risk that become difficult to monitor and manage.

This study also found those working for public entities had less faith in their organizations' ability to prevent third-party security threats — especially compared to their counterparts in the financial services sector. This makes sense given the different fiscal natures of private and public entities, the latter of which normally have less budget flexibility and fewer intermittent funding options.

What is more encouraging is the high number of organizations communicating third-party IT security risks or incidents to their boards of directors. Among those surveyed, 73% were keeping their board informed, and another 17% intended to start supplying such information in the coming year.

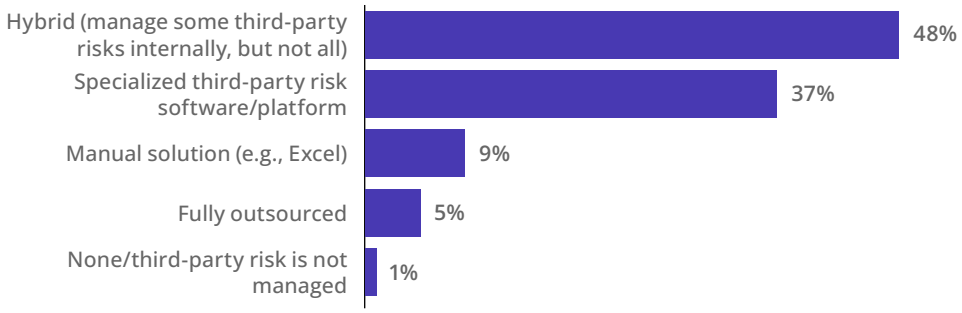
Such activity is encouraging, especially for organizations in industries that aren't heavily regulated and reflects the growing strategic and top-level support cybersecurity now commands.

A HYBRID APPROACH TO MANAGING THIRD-PARTY RISK

So how are organizations today managing third-party risk? Virtually all respondents identified at least one method they use to manage third-party risk. The top method, used by nearly half (48%) of all respondents, is a hybrid approach in which organizations manage some risks internally and turned to outside providers or technologies for the remainder. Another 37% use specialized third-party risk software or platforms, while 5% fully outsource to minimize IT security risks among their partners. While less popular than in past years, the manual/spreadsheet method is still in use by 9% of those surveyed.

Respondents in the financial services sector were most likely to use specialized risk software, while those in the insurance space were most likely to adopt a manual solution.

Primary Method for Managing Third-Party Risk



Respondents indicated broad interest in leveraging technology designed for greater third-party risk management, from rating vendors' cybersecurity posture to initial cyber risk assessments and ongoing monitoring in near-real-time. Almost all respondents expressed some level of interest in adopting these tools, with almost a third reporting they were "very interested."

Interest in technical solutions could stem from frustrations with the challenges of onboarding and retaining personnel to manage third-party risk and the intensive monitoring and managing of third-party access points required as their numbers grow.

"The top challenge is maintaining the personnel that can communicate, understand, and work with the third-party so that risk can be proactively addressed, not reactively."

– Computer Scientist, Federal Government

Financial services organizations were more likely to embrace technical solutions, given that industry's reputation for innovation and early adoption of emerging technologies. Meanwhile, the healthcare industry was among the most satisfied with the effectiveness of their chosen third-party solution, particularly a tools' ability to generate reports.

Along with enthusiasm for digital solutions, everyone surveyed most wanted a chosen third-party risk management system to assist with a number of challenges, including response/remediation time, risk assessments, and regulatory compliance.

Importance of Third-Party Risk Management Capabilities

Percentage of respondents indicating "Very important"

One participant in financial services was dubious of any software providing enough power to bring about better outcomes. "The top challenges include not getting the communication and reports needed to monitor and remediate security risks. They often leave out significant details regarding the situation," the project manager said.

Researchers also measured performance gaps between expectations and demonstrable effectiveness of current approaches or technologies in use. The results reflect areas where organizations are likely dissatisfied with current capabilities — such as flagging high-risk vendors and both evaluating and monitoring the risks those vendors pose.

THE GROWING ROLE OF ZERO TRUST IN THIRD-PARTY RISK MANAGEMENT

Technology is one solution to monitoring and minimizing third-party risks. Another assist is adopting a methodology or framework that denies access by default, a concept known as Zero Trust. The term and concept have existed for more than a decade, but it's only been in recent years that companies have independent consultants, consulting firms, software vendors, and others. As a policy and practice, the idea is to not trust anything inside or outside of established perimeters until verified.

Most corporate networks are designed to allow authenticated users on both sides of a cyber border to access applications, devices, and databases within an IT environment. Zero Trust requires that IT systems be rearchitected to block access to someone (or something) until high trust levels are established. When done properly, there is no negative impact on network performance or the user experience.

"The greatest benefit [of a Zero Trust model] would be to maintain the strictest level of regulatory compliance, equally important is maintaining the highest level of security as well," said an IT healthcare director.

The study found that 22% currently incorporate a Zero Trust model into their third-party risk management program. That percentage should grow, given nearly three in four (71%) believe the model is "very important" to managing third-party risk.

"Zero Trust would take care of some threats, not all. If you give access even momentarily, third parties may mismanage what they learn."

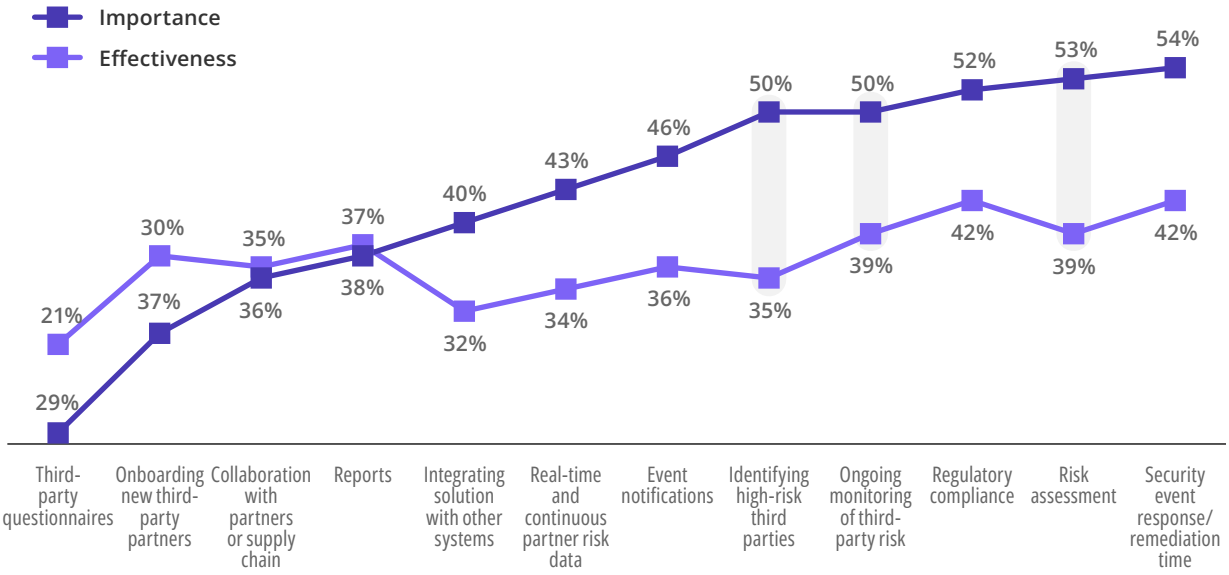
– System Manager, Education

There was a concern stated by several respondents that "trusted third-parties" can be compromised, and thereby compromise the Zero Trust model.

An emerging method of mitigating this risk/concern is to deploy a cyber ratings platform to continuously monitor "trusted third-parties" for breaches and/or any degradation of cyber security health.

Importance/Performance of Third-Party Risk Management Capabilities

Percentage indicating "Very important" and "Very Effective"



CONCLUSION

No matter the chosen methods to manage threats associated with third-party access to a network, sensitive data, devices, users, or applications, those with influence over decisions and purchases are willing to invest in models, methods, frameworks and technologies designed to reduce the risks of an IT security event due to a third-party exploit. That includes use of ratings platforms to help select trustworthy vendors and tools to provide a more layered approach to security — one that includes continuous monitoring of third parties.

Such vigilance, along with more stringent access policy making, will help an organization better evaluate where they and their vendors are vulnerable and, if required, remain regulatory-compliant. It also allows enterprises to respond more quickly to events triggered by a third-party threat. That includes recognizing both the promise and the potential problems associated with Zero Trust, which works only if a trusted user or device is not compromised after access is granted.

Technologies like those associated with security ratings can help narrow current performance gaps so that both partners can focus on market growth, not becoming the unwitting agent of mayhem.

A senior vice president in charge of technology, safety and strategic initiatives for an educational organization summed up what's needed to protect networks and assets while remaining accessible to those helping drive business. The statement also speaks to the holistic approach any organization must take to maintain needed oversight without compromising both business relationships and the business itself:

"In an era of many devices per person, coupled with peoples' reliance on those devices, the chances of a device bringing in an issue is high. Mitigating this with Zero Trust would add considerable protection and minimize risk. It is a complicated thing to do but the value is significant. One of the harder things is to ensure the organization is ready from a cultural standpoint."

– Sr. VP of Technology, Education

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, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. More information is available at ***http://cyberriskalliance.com/***.

ABOUT SECURITYSCORECARD

Funded by world-class investors including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, **SecurityScorecard** is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent **Instant SecurityScorecard** rating. For more information, visit ***securityscorecard.com*** or connect with us on **LinkedIn**.

