CRA | Business Intelligence

Third-Party Risk: *A Turbulent Outlook*

FINDINGS FROM A DECEMBER 2021 RESEARCH STUDY

January 2022

Sponsored by

TRAVA

Third-Party Risk: *A Turbulent Outlook*

FINDINGS FROM A DECEMBER 2021 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, which gauged companies' understanding, interest and investments in managing third-party risk. As one study participant put it: "Risk is the main cause of uncertainty in any organization. Thus, companies increasingly focus more on identifying risks and managing them before they even affect the business. The ability to manage risk will help companies act more confidently on future business decisions."

Getting to that level of assurance, however, is a challenge. Companies remain unclear on the best path forward now that they are keenly aware of the catastrophic impact from another's carelessness or compromised code.

> *"Having started my compliance career in third-party vendor management in 2003, I'm still surprised at the lack of visibility into the risk that third-party suppliers pose to organizations. This research confirms that third-party risk is a critical component of your overall risk management program, especially considering recent attacks. With increasing damages and outages, it's time for organizations to manage the risk of their third-party suppliers."*
>
> –Matt Alderman, SVP, Cyberrisk Alliance Business Intelligence Unit

RESEARCH METHODOLOGY

The data and insights in this report are based on an online survey conducted in late fall 2021 among 301 IT and cybersecurity decision-makers and influencers who stated their organization worked with third-party partners. All were in the United States except for 1% from Canada. Roles ranged from information security chief executives (35%) to IT security directors or managers (49%) to administrators, analysts, and consultants (16%). Roughly 64% worked at companies with less than 1,000 employees, while the remaining 36% worked at organizations with a larger workforce. The majority (86%) had security teams comprised of 20 or fewer full-time employees, while 14% had larger security operations centers. Here is a snapshot of responses by company size (number of employees):

- Small (1–99): **34%**
- Medium (100–999): **30%**
- Large (1,000–1,999): **23%**
- Enterprise (10,000 or more): **13%**

Study participants worked primarily in the following industries:

- Business or professional services: **16%**
- Manufacturing: **18%**
- Retail or ecommerce: **11%**

- High-tech/IT: **11%**
- Financial services and insurance: **9%**
- Other (healthcare, education, transportation, government, non-profits, media, energy and utilities): **35%**

Survey objectives were to gauge how well organizations understand and manage risks associated with third-party partnerships. Study participants were asked about their own vendor relations, concerns, and challenges in managing certain risks, and the impact of IT security incidents related to their third-party partners. They also provided responses to structured survey questions and were encouraged to provide corresponding comments where applicable. The survey was conducted by the Business Intelligence Unit of CyberRisk Alliance.

EXECUTIVE SUMMARY

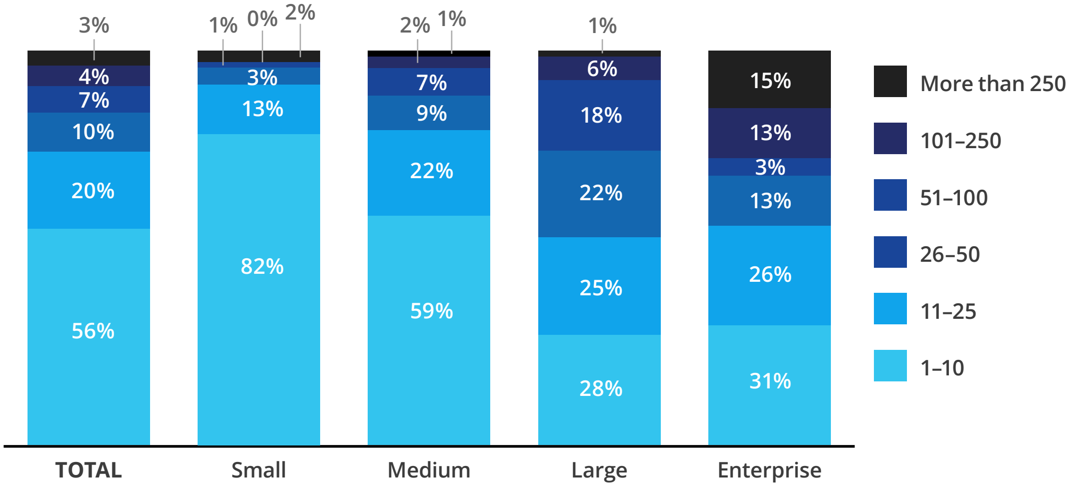
Third-party relationships continue to expand exponentially as companies seek outsourced services and software to perform optimally and to backfill talent and supply shortages during the ongoing pandemic. That expansion, however, is also broadening attack surfaces as threat actors target weaker vendors with strong market penetration to quietly surveil and paralyze systems. It can be months, even years, before the breach is detected — if at all. In the case of ransomware, companies can be shut down and extorted.

This elevated risk has not been lost on IT executives, decision-makers, and influencers, who appear to understand the need to better manage third-party cyber risks, but some aren't yet sure how best to go about it. Since the December 2020 discovery of suspicious code in a routine update to 18,000 SolarWinds customers, other victimized vendors and contractors have led to significant security events for their customers. Sometimes it's malicious code quietly inserted into a software update; other times, it's malware unleashed through phishing or contaminated external drives.

No man or woman is an island, and no organization now operates completely on its own. On average, the majority of respondents (76%) contract with up to 25 different vendors, business partners, brokers, contractors, distributors, agents, and resellers. Virtually all organizations (95%) indicated partnerships with IT software, platform, or service providers, suggesting a growing reliance on technology companies that historically secure code by default, not design, in a rush to market.

The largest organizations have the most partners: Fifty-six percent of large or enterprise organizations reported that they have more than 50 partners.

Number of Third-Party Partners, by Organization Size



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

Among the study's key findings:

- Sixty percent of respondents experienced an IT security incident in the past two years due to a third-party partner with access privileges and were most likely to have sensitive data stolen or suffered some type of business outage.
- While 52% of those who experienced third-party related attacks indicated they less lost less than $100,000 in damages, another 45% incurred higher costs, with a few paying $1 million or more.
- Victims impacted by the SolarWinds Orion SUNBURST supply chain attack suffered everything from day-long shutdowns to crucial data leakages.
- Perhaps because of real or perceived threats from SolarWinds and similar attacks, 70% of respondents ranked cyber the No. 1 or No. 2 risk among their third-party/supply chain partners.

- Supply chain visibility is more essential than prior to the pandemic. Almost everyone wanted this ability, with 72% believing that tracking components, sub-assemblies, and final products was very or critically important.
- More than three out of four (76%) IT leaders and influencers rated managing third-party risk as a high or critical priority at their organizations — for most respondents (74%) this priority has increased in importance since 2020, when the pandemic created major micro and macro business disruptions, including supply and workforce shortages.
- Nearly half of all respondents (45%) said they implement the guidelines within the NIST Cybersecurity Framework in their third-party vendors assessments.

Despite current challenges, organizations expect to improve their third-party risk management programs in the coming year. Budget spending is increasing for nearly half (49%) of all organizations, reflecting the growing importance of better third-party risk management to decrease the chance of a data breach or business disruption due to someone else's poor security posture.

A GATHERING STORM

To take center stage in a 2020 news cycle took some doing, given half the world was locked down at some point due to the discovery of a highly contagious, deadly virus. The mass work-from-home movement, rising death toll, civil unrest, supply shortages and contentious U.S. elections captured a bulk of news media attention.

In the cyber world, one of the biggest stories of the year broke when researchers at a security company announced they'd discovered backdoor malware coming from software used to monitor IT performance. Given the task at hand, the SolarWinds Orion platform required access to some 30,000 customers' log and systems performance data, with more than 18,000 known to have downloaded the update carrying malicious code by the time the breach was discovered — more than a year after it was said to have originally been planted.

Believed to be the work of Russian-government operatives using a malicious program called SUNBURST, the attack allowed threat actors to spy on the inner workings of government agencies, private companies, and other organizations without notice. It also exposed hundreds of thousands of victims' clients and customers data, making it one of the largest data breaches to date.

“Because we are connected to some software companies that use SolarWinds, it led to data losses both in our mailing system and supply chain,” noted one victim in the survey. Others reported system slowdowns, work disruptions and malware infections from downstream effects.

Other supply chain attacks followed the SolarWinds announcement, most notably the May 2021 ransomware attack on Colonial Pipeline, which disrupted fuel deliveries in the eastern United States, followed by an attack on JBS, which disrupted global meat production. Then came word that the Kaseya IT platform had been compromised to spread ransomware to customers that included many managed service providers, which expanded the damage exponentially to everything from railways to grocery chains. Even the open-source community wasn’t spared, with the late 2021 discovery of a zero-day vulnerability in the Log4j Java library popular with software developers.

With such an uptick in known supply chain attacks and well-publicized outcomes, organizations felt compelled to closely scrutinize their vendor relations, from those who physically have access to equipment to those providing software vital to business operations.

Just how they intended to vet vendors, however, remained an open question at a time when it was no longer business as usual.

NEW TECH TO NAVIGATE THE STORM

Organizations worldwide initially adjusted to the Covid-19 global public health crisis by asking non-essential employees to work from home, creating major IT headaches for those tasked with providing these workers secure remote access to do their jobs from different locations.

> *“Since the onset of Covid, our organization has a large percentage of employees working from home. It is critical that our third-party vendors provide transparency to our risk and/or exposure when doing business with them, particularly since remote workspaces may not have the same high-level cybersecurity as office or corporate facilities.”*
>
> –CIO, Education

By mid–2021, corporate America would be rocked by another labor movement — this time millions of employees monthly quitting their jobs in what's become known as The Great Resignation. This forced businesses to quickly downsize and/or hire contractors or automation software to fill labor shortages. Though some industries were hit harder than others, no sector appears to have been spared the mass exoduses due to a prolonged public health crisis. For those respondents who reported limited staffing due to the Covid crisis, third-party security became even more critical.

At the same time, everyone from sole proprietors to Fortune 100 companies felt the pinch of supply chain disruptions — some caused by labor, raw material, transportation, or manufacturing shortages; others from ransomware attacks that paralyzed computer systems and production schedules. These cyber threats had companies reexamining their dependency on outside providers whose cybersecurity posture remained unknown or proven unreliable.

> ***"With the pandemic and the changing conditions, there has been a significant change in reliance on third parties. There has been a larger need to procure and with that, a larger focus on getting the right person, right item, right price, right risk."***
>
> **– VP of IT, Financial Services**

When even a portion of an organization's IT functionality is in the hands of outside providers, it's crucial to know not only what vendor security controls are in place, but how to respond if they become vectors for cyber attacks, likely accounting for why 76% of those surveyed believed managing third-party risk was a high or critical priority.

It also could be because 60% said they had in recent years experienced an IT security incident due to a third-party partner breach that had led to stolen sensitive data or some type of business outage. While 52% suffered less than $100,000 in damages, about 45% incurred higher costs, with a few paying $1 million or more.

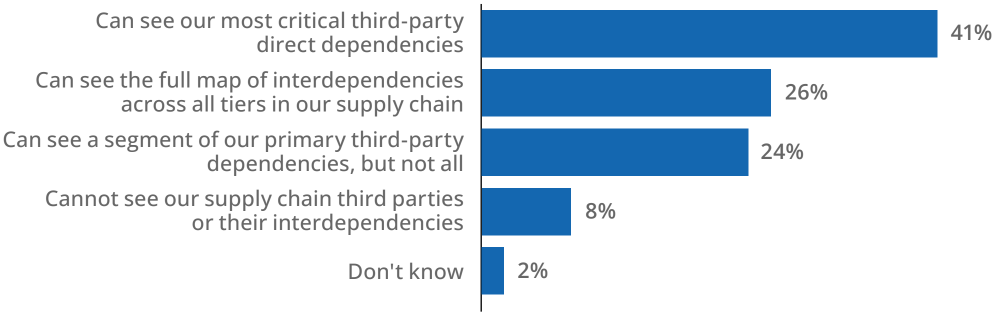
These events and the post–mortems that typically follow can serve as catalysts to changing cyber policies, procedures and even people to reduce organizational vulnerability. Especially when the weak link is within a supply chain.

SUPPLY CHAIN VISIBILITY: MANAGING WHAT YOU CAN SEE

To manage risk, a company must know who, how and where a third party operates within its networks and systems. After all, you can't manage what you don't know exists.

Yet, despite the vast majority (72%) finding supply chain visibility important, far fewer appear to have a firm grasp on the depth of third-party dependencies within their organizations — despite recognition that such visibility is more important than prior to the pandemic. In reporting their highest level of supply chain visibility, 41% had visibility only on their most critical third–party direct dependencies, while 26% could see the full map of interdependencies across all tiers in their supply chain.

Highest Level of Supply Chain Visibility



Q: Which of the following best describes your organization's highest level of supply chain visibility?

Among a minority that deprioritized third-party risk management, time, resources, costs and Covid were cited, as well as the need to look inward.

For organizations that prioritized third-party risk management, Covid came up frequently as a top driver due to its potential destructive and introspective powers. "I would say the primary role is Covid-19. It played into these criteria of supply chain. Managing our vendors individually and continuously to maintain our individual products has made us keep managing our third-party risk," commented one participant.

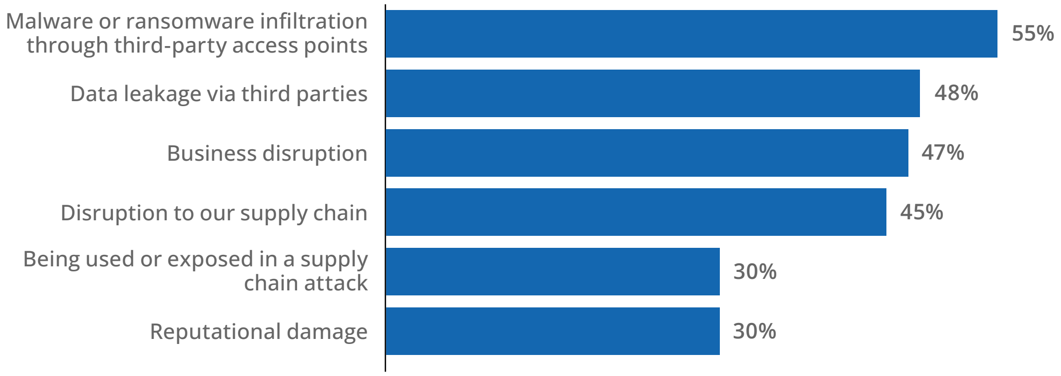
> *“Everything has changed since Covid began. Our once-stable world that seemed untouchable by something like a pandemic was really shattered. All business associations that have survived all the changes are priceless and must be maintained at much higher priorities.”*
>
> –Owner, High Tech Business

ASSESSING THE DAMAGE

In thinking about the top impacts of a potential third-party breach in the next 12 months, respondents were most concerned with malware or ransomware infiltration due to third-party access points, followed by data leakage and business and/or supply chain disruptions.

While most in the survey focused on actual or anticipated financial fallout from poorly managed third-party risk, others noted the potential collateral damage from being associated with those found to exploit or be exploited — reputational damage cited as a top concern for 30% of respondents.

Impacts of Potential Third-Party Breach



Q: Thinking about the impacts to your organization of a potential third-party breach in the next 12 months, which of the following would you say your organization is most concerned about? Please select up to 3.

The survey also asked security professionals to rank the importance of understanding the types of risks related to third-party partnerships. Cyber risks, by far, topped the list as the most important risk for 48% of respondents, outranking environment, financial, geopolitical, operational, and regulatory risks.

About a month following the survey, SC Media reported in a January 7, 2022 article that a third-party IT healthcare vendor had been hit with a class-action lawsuit after alerting regulators its solution was involved in a Kentucky health system's patient portal breach that compromised more than 300,000 electronic health records within the vendor's control.

"The lawsuit argues that the data exfiltration could have been prevented if QRS had adequately secured, monitored, and maintained the protected health information in its possession, according to the article. "The suit argues that QRS should have implemented federally recommended cybersecurity measures, which would have detected or prevented the hack."

Those allegations square with fears expressed by respondents in this study when it comes to collateral damage and legal liabilities from working with third parties found in violation of laws, regulations, or simply best practices.

> ***"If the pandemic customer acquisition and retention is vital, we must make sure all our suppliers are doing the right things, because if consumers see you are using some shady suppliers they may leave, and that's what we do not want to happen."***
>
> **–Director of Operations, Business/Professional Services**

From a cybersecurity standpoint, organizations cannot assume a business partner incorporates certain security controls or remains off threat actors' radar. This has put more pressure on companies to improve their due diligence before onboarding a new contractor, supplier, or software provider. They also should reevaluate the risk profiles of current partners and business relationships.

40% conduct ongoing or continuous risk reassessments after acquiring a third-party partner

In many instances, respondents who suffered a data breach said they were notified by the offending third party. Others were discovered through such incidents as:

- Catastrophic system failure
- Ransomware attacks
- Distributed denial-of-service attacks

- Customer complaints
- Business disruptions
- Credit card compromises

Many leaned into their own tools and techniques, from anti-malware alerts and firewall testing to employee reports, to prevent an outbreak or outage. In at least one instance, the victim bore the bad news. “Our own internal IT department discovered it through our auditing processes. It was concerning because we caught it before our third party did.” Others noted the importance of best practices, such as asset management, malware scans, and continuous monitoring in preventing attacks and other incidents.

45% Use the NIST Framework for guidance in managing third-party security

Aside from outsourcing risk assessments and/or ongoing management, respondents turned to expert guidance and methodologies to vet their vendor’s security posture. The most popular cited by study participants was the NIST Cybersecurity Framework. Others gathered information on shared assessments from special interest groups; ISO 27001 or ISO 27036; and NIST 800-161. About 8% said they didn’t bother with any standards frameworks.

THE MANY ROLES OF THIRD-PARTY SECURITY: WHO DOES WHAT?

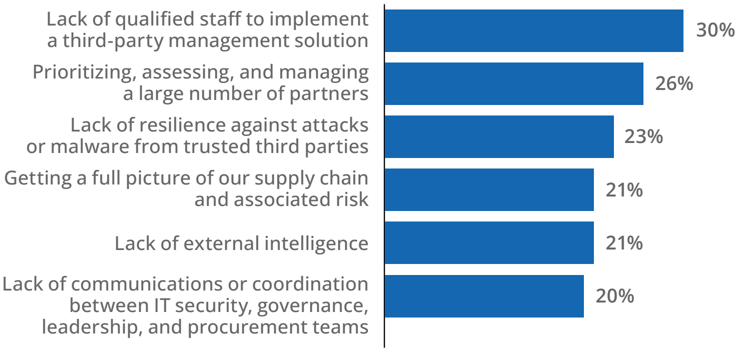
	Risk and Compliance	Procurement	IT Operation	IT Security	Individual Business Units
Vet and evaluate third-parties	33%	31%	17%	13%	6%
Assess third-parties	37%	29%	21%	8%	5%
Monitor third-parties	27%	13%	32%	27%	2%

WANTED: BETTER PROCESSES, MORE QUALIFIED PEOPLE

Among respondents' biggest challenges in gaining greater visibility were lack of qualified staff to implement a third-party management solution and prioritizing, assessing, and managing a large number of partners.

Challenges in Managing Third-Party Risk

Percentage of respondents indicating "Very challenging"



Q: How challenging is each off the following when managing third-party risk at your organization?

HOW DO ORGANIZATIONS EVALUATE THE RISK OF THEIR THIRD-PARTY PARTNERS?

54% Internal Partner Assessments

43% Outside Service for Third-Party Risk Intelligence

42% Partner References

36% Questionnaires

35% Partner Self-Attestation

A majority (54%) of proactive organizations relied on their third-party partners' assessments, while 43% hired an outside service. Others settled for questionnaires (36%) or their partners' preferences or attestations (35%). Only 2% acknowledged taking no steps to determine third-party risks levels.

Motivating those most likely to purchase third-party risk software or platforms in the coming year was a need to rank vendors based on external risks and gain visibility into the entire supply chain. Respondents also wanted automated vendor tracking and supply chain mapping, faster onboarding and deprovision as needed and an alternate to vet vendors whose assessments aren't available.

Most important within these purchases is the ability to report risk factors tied to specific environments. They also consider dashboards and scorecards to be valuable features.

From a budget standpoint, 46% of respondents intended to devote up to 10% to third-party risk management tools in the coming year, with another 3% willing to spend even more. Anticipated capabilities from these technologies include the need to do more with less to protect against attacks launched by insecure partners.

HOW TO MANAGE THIRD-PARTY RISK LIKE A CHAMPION

CRA Business Intelligence uncovered a segment of 214 respondents whose third-party risk management best practices and procedures distinguish them from other organizations. These "champions" are predominantly very large healthcare, financial services, and retail organizations, as well as mid-size and large manufacturers and high-tech/IT firms.

Likely driven by their large and complex supply chains and/or regulatory compliance mandates, champions can be role models in helping others secure their organizations against attacks originating from their external partners, vendors, suppliers, contractors, and service providers.

What do champions do to stay ahead of third-party risk?

- **Prioritize third-party risk management.** Virtually all champions indicate that third-party risk management is either a critical priority (42%) or a high priority (53%) at their organization, and nearly half of them (46%) say they have significantly increased their focus on third-party risk management since 2020.

- **Stay wary of third-party partner risk.** While champions rely on their external partners to do business, they have few illusions about the IT security risks their third parties potentially impose. Respondents in this segment are significantly more likely than their non-champion counterparts to be concerned about third-party breaches disrupting their supply chain — half of all champions consider this one of their top three concerns in the next 12 months.

- **Follow industry standards and guidelines.** On average, champions are twice as likely than non-champion organizations to follow industry standard frameworks in their third-party assessments. For example, 48% of champions say they use the NIST Cybersecurity Framework, 28% use ISO 27001, and 27% use ISO 27036.

- **Adopt multiple methods to vet third-party partners.** Champions use various methods to vet their partners. For example, 46% of champions (vs. 36% of non-champions) report using an outside service that provides third-party risk assessment or scoring. Champions are also more likely than non-champions to use questionnaires (41% vs. 24%, respectively). Additionally, many champions use partner references (43%) as well as their own partner assessment methods (55%).

- **Continually reassess third parties for risk.** Nearly half (45%) of all champions reported they conduct ongoing assessments of their third-party partners after acquiring them — almost twice as many as non-champion organizations (25%), who generally tend to check up on third parties once or twice per year (53%).

- **Strive for high supply chain visibility.** Champions are about five times more likely (94%) than non-champions (18%) to believe their ability to track individual components of their supply chain is either critical or very important. Indeed, a large majority of champions say they can either see their most critical third-party direct dependencies (47%) or see a full map of all interdependencies across all tiers in their supply chain (31%). Additionally, champions are much more likely than their non-champion counterparts (86% vs. 47%, respectively) to believe supply chain visibility has become somewhat more important or much more important compared to two years ago.

- **Adopt third-party risk technology.** More than half of all champions (56%) — and twice as many non-champions — use a third-party risk management software tool or platform as their primary method for tracking and monitoring third-party risk. Their top purchase criteria for these investments (rated as "very important") include reporting

and compliance dashboards (36%); standardized vendor assessments and scorecards (32%); risk-factor reporting for their specific environment (32%); and standardized, repeatable formulas for sharing assessment data (29%).

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, reputation, 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 convert into 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. "Would like no problem anywhere," one survey respondent said, "but I bet that wish won't come true."

Pandemic-related 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.

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 TRAVA

Trava was founded by Jim Goldman and Rob Beeler to protect small and medium-sized businesses from the potential damage of cyber threats. By integrating risk assessment, risk mitigation, and cyber insurance into one convenient, comprehensive, and integrated cyber risk management platform, Trava enables business owners and IT professionals to operate secure, productive businesses without fear of interruption or loss caused by cyber incidents. Trava is headquartered in Indianapolis, Indiana. To learn more, visit ***travasecurity.com*** or follow on social: **LinkedIn**, **Twitter**, **Instagram**, **Facebook**.