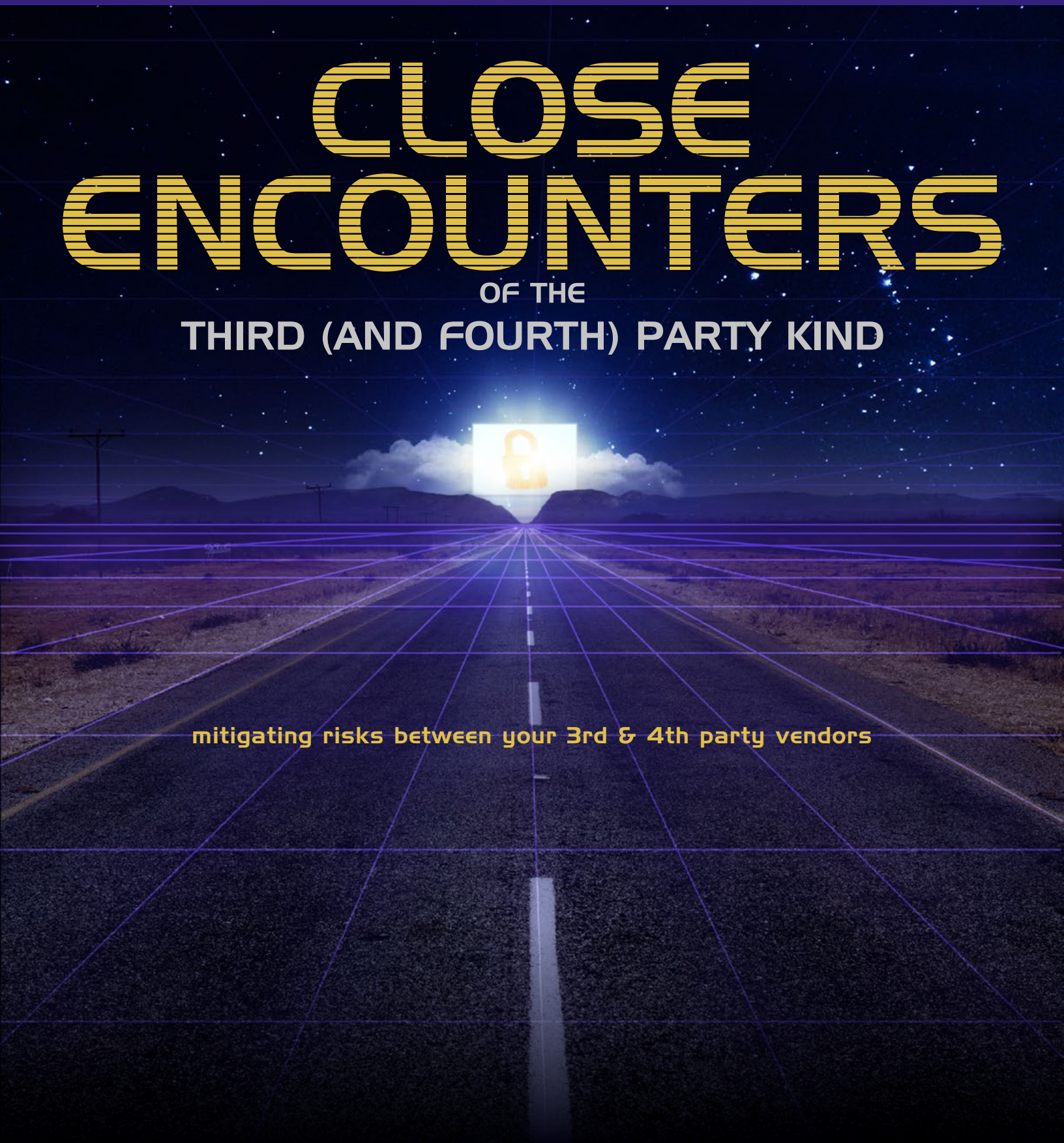
A COLLABORATIVE REPORT BETWEEN SecurityScorecard & Cyentia

CLOSE ENCOUNTERS

OF THE THIRD (AND FOURTH) PARTY KIND



mitigating risks between your 3rd & 4th party vendors

IMPROVING THE CYBER DEFENSES OF YOUR WEAKEST LINKS
SECURITYSCORECARD–GLOBAL LEADER IN CYBERSECURITY RATINGS
THE CYENTIA INSTITUTE–EXPANDING CYBERSECURITY KNOWLEDGE

Introduction

It's often said that cyber defenses are only as strong as the weakest link. For individual organizations, that saying is often (unfairly) directed towards insiders due to their ability to undermine security with the click of a button. The concept applies equally well, if not better, to managing cyber risk across multiple organizations in a supply chain.

This has not gone unnoticed by cyber threat actors. Exploiting inter-organizational trust relationships and targeting widespread vendor technologies have become go-to tactics in the adversary playbook. Breaches stemming from third (and fourth) parties routinely make headlines these days, so most cybersecurity practitioners are at least conceptually aware of the risks involved with these 'close encounters' with business partners.

This report offers an in-depth examination of the underlying condition that enables such incidents to take place—the widespread interdependence of modern digital supply chains. We analyze data from over 230,000 organizations to investigate the prevalence of security incidents among third parties. We then measure the extent of vendor relationships and explore the effects of that exposure. Finally, we compare the security posture of organizations to that of their third and fourth-parties to yield data-driven insights on how to identify risky vendors and better manage exposure.

CONTENTS

Key Findings.

98% of organizations have a relationship with at least one third party that has experienced a breach in the last 2 years.

The Information Services sector maintains 2.5 times the number of third parties than the overall average. Finance claims the lowest.

59% of organizations have vendors from 5 or fewer countries, and roughly 14% work with vendors spanning 10 or more countries.

For each third-party vendor in their supply chain, organizations typically have indirect relationships with 60x to 90x that number of fourth parties.

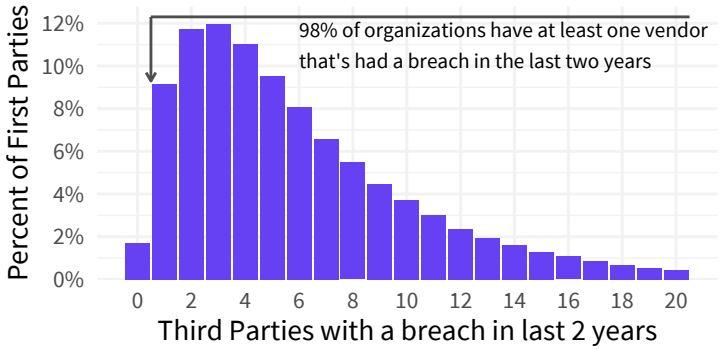
First parties are 2x more likely to achieve the highest security rating, while third parties are 5x more likely to exhibit poor security.

Organizations that exhibit poor security posture have twice the number of third-party vendors and 10x the number of fourth parties.

A Primer on Vendor Risk Exposure

Here's a statistic that hammers home the point about organizational interdependence and exposure to cyber risk: 98% of organizations have a relationship with at least one third party that has experienced a breach in the last 2 years. Another one that's equally jarring: Half of all organizations have indirect relationships with at least 200 fourth parties that have had breaches in the last two years.

98.3% OF ORGANIZATIONS HAVE A RELATIONSHIP WITH AT LEAST ONE THIRD PARTY THAT HAS EXPERIENCED A BREACH IN THE LAST 2 YEARS.



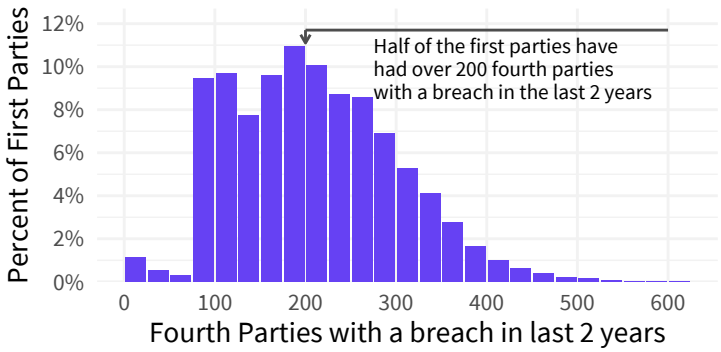


Figure I: Exposure to breaches via third (top) and fourth (bottom) party relationships.

This does not mean that those organizations were involved or impacted by those breaches. It doesn't even mean that the nature of the relationship between the victim and its third parties is such that the breach could propagate to them. But, it does mean that nearly every organization is at least indirectly exposed to risk from circumstances outside their control.

That's why we're keen to analyze the true extent of that exposure from third and fourth party relationships. Let's start digging into that topic through a short case study.

About the Data

SecurityScorecard continuously scans the internet to identify vulnerable and misconfigured digital assets. Additionally, SecurityScorecard monitors signals across the Internet, relying on a global network of sensors that spans the Americas, Asia, and Europe. The company operates one of the world's largest networks of sinkholes and honeypots to capture malicious signals and further enrich its data set by leveraging commercial and open- source intelligence sources. In total, SecurityScorecard continuously monitors the security posture of over 12 million organizations globally.

Specific to this report, the data on third and fourth party relationships comes from SecurityScorecard's Automatic Vendor Detection capability. Automatic Vendor Detection identifies vendors and products that make up the digital supply chain of modern organizations. This large sample of data centers on 235,000+ primary organizations and the 73,000+ vendors/products used by them directly (third parties) or used by their vendors (fourth parties). We refer to these connections between organizations and their third and fourth party vendors generally as "relationships."

A Case Study of Interconnectivity

> *Your organization may not run this company's code, but it's near certain that others in your supply chain do, representing some level of exposure to you.*

As we begin digging into this dataset, it might help to get a glimpse of the complex web of third and fourth party relationships for just one small company. The company we chose (which will remain unnamed) develops code that plugs into websites to determine what users are doing on their site. According to Automatic Vendor Detection, about 12,500 organizations have this code running on their sites. Not insignificant...but certainly not universal like you'll soon see for behemoths, like Google and Microsoft.

When we extend the aperture to fourth parties that share a relationship to those 12,500 organizations running our example company's code, "universal" does indeed become an apt description of the scope of potential exposure. A full 98.7% of the 232,000 organizations in our sample have an indirect, once-removed relationship to this company. In other words, your organization may not directly use them, but it's near certain that others in your supply chain do. Representing that if that code were compromised, or subverted, for nefarious purposes, you would experience some level of exposure.

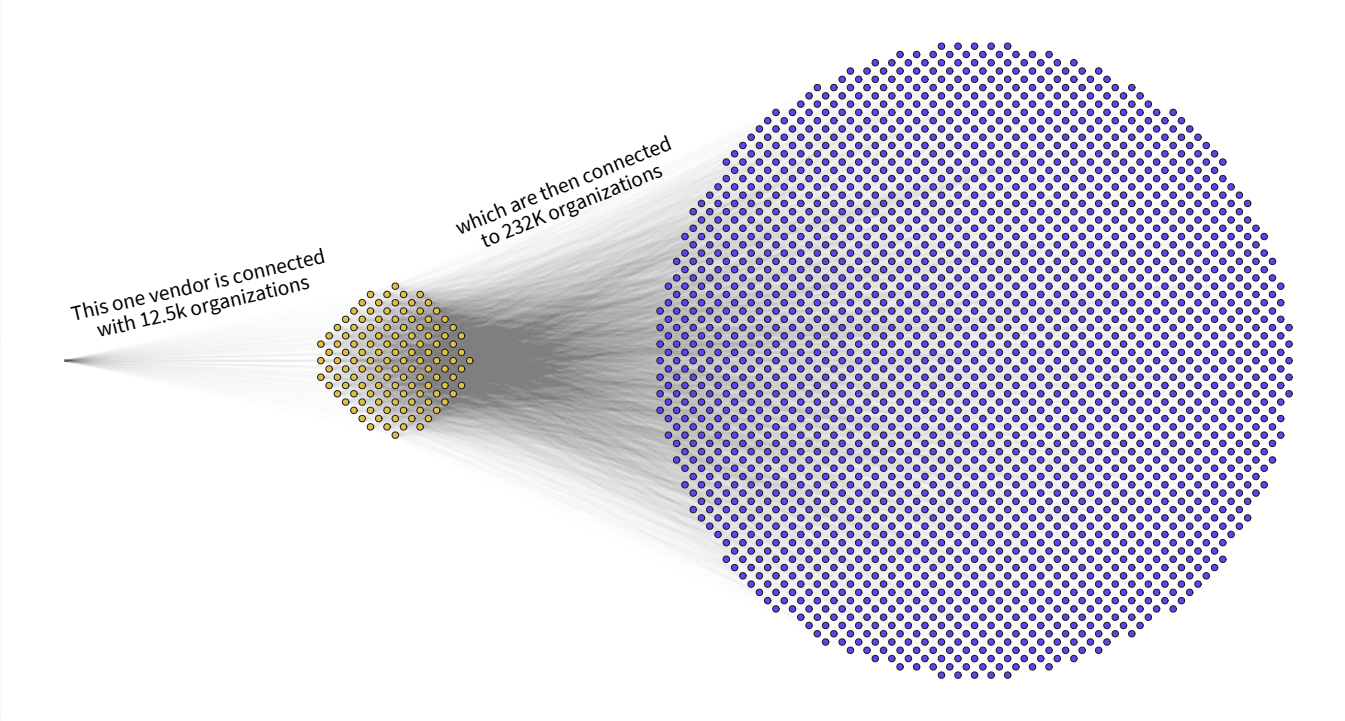


Figure 2: The escalating nature of third and fourth-party relationships of one small company.

Enumerating Third-Party Relationships

FOLLOWING THAT BRIEF EXCURSION INTO THIRD-PARTY RISK EXPOSURE, LET'S TAKE A MORE THOROUGH LOOK AT THIS TOPIC THROUGH THE LENS OF SECURITYSCORECARD'S AUTOMATIC VENDOR DETECTION DATA.

OUR OVERALL GOAL IS TO HELP YOU ANSWER THE QUESTION OF:

"HOW BIG OF A DEAL IS THIS FOR MY ORGANIZATION?"

How many third-party relationships do organizations maintain?

Let's start by counting the number of direct vendor relationships detected for each organization. Figure 3 presents that distribution and, even on a logarithmic scale, the data appears heavily skewed with a long tail to the right for hundreds of vendors. The typical number (peak density) of third-party relationships is about 10, and three-quarters of organizations have less than 30. Only the top 4% of firms exceed 100 direct vendor relationships—though that's still more than 10,000 organizations!

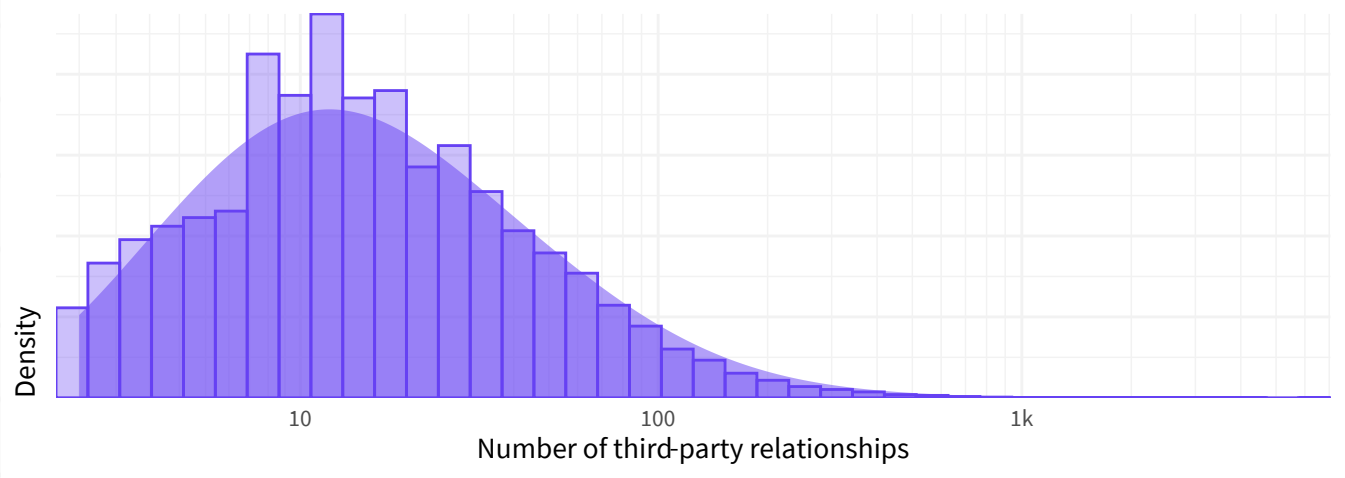


Figure 3: Number of third-party relationships detected per organization.

If those numbers seem small compared to other sources you may have seen enumerating third-party relationships, keep in mind the methodology behind this particular dataset. These are vendors that are visible from outside-in scanning of an organization's internet-facing infrastructure. We're not conducting an exhaustive inventory of upstream and downstream vendors of all types. The presence of a vendor's code running on your website will be detected, but we have no idea who carries your packages, or cleans the office.

WHY DO I CARE ABOUT THESE RELATIONSHIPS?

FAIR QUESTION AND ONE THAT WE'LL EXPLORE IN MORE DETAIL LATER. FOR NOW, THE MAIN POINT IS THAT EACH OF THESE RELATIONSHIPS REPRESENTS EXPOSURE TO RISK. PERHAPS THIRD-PARTY CODE IS COMPROMISED, IMPACTING CUSTOMER DATA PROCESSED ON YOUR WEBSITE. OR MAYBE USAGE OF AN INSECURE HOSTING PROVIDER LANDS YOUR COMPANY ON A BLOCKLIST OR TARNISHES YOUR REPUTATION FOR SECURITY DUE DILIGENCE.

Does the number of third-party relationships vary across sectors?

Above we looked at a wide range of third-party relationships among organizations. It seems logical that at least part of that disparity stems from different types of business activities. We obviously don't know all the business activities of the 235k organizations in our sample, but we can group them according to their primary industry. We've done that in Figure 4, and it's immediately clear that some sectors do indeed tend to maintain more third-party relationships than others.

CHART TIP: Figure 4 is essentially a more compact version of the distribution in Figure 3. The red point marks the "typical" value at the highest concentration of organizations. The thicker line covers 50% of organizations and the thinner line extends that to 90% coverage.

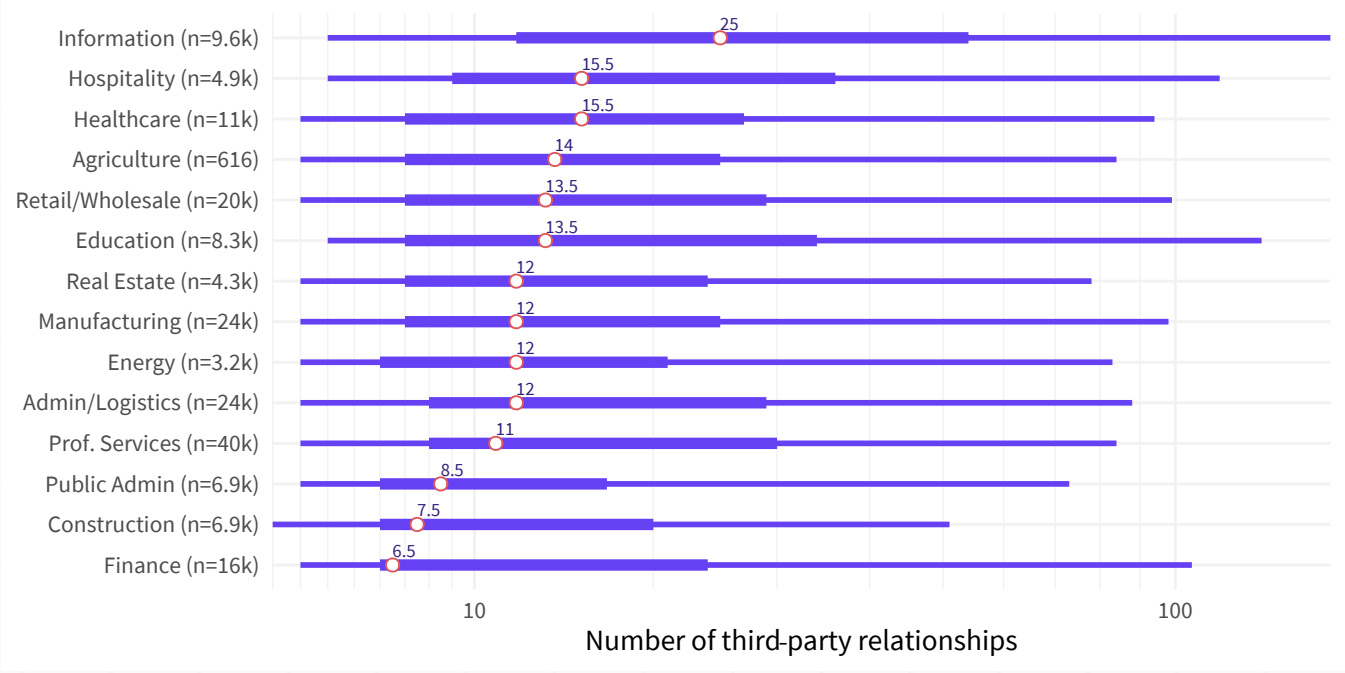


Figure 4: Number of third-party relationships detected per organization by sector.

The Information Services sector takes the cake with a typical number of third-party relationships (25) that's 2.5x the overall value of 10. That makes sense, because those firms tend to be more tech-heavy with vendors that are more readily detected from scanning external infrastructure. Hospitality, Healthcare, and Education also aren't surprising, as they depend upon service providers to do what they do.

Agriculture may seem an outlier among the top five, but that's probably a holdover memory from your grandpa's quaint farm. Modern farms have a huge number of technologies to remotely measure and manage everything under the sun (literally).

On the opposite end of the spectrum, Public Administration (government) and Finance rank among the sectors with the lowest median number of externally-detectable vendor relationships. Many things contribute to that outcome. Both are heavily regulated, which generally translates to higher due diligence and compliance requirements when it comes to third-party, tech-centric relationships. Also keep in mind that most organizations in the public sector aren't giant federal/central institutions; they're local and state-level agencies with smaller Internet footprints.

In addition to the typical number of vendors managed for a given organization within each sector, we're also interested in the proportion of all third-party relationships tied to each sector as a whole. In other words, which industries contain the most organizations that are vendors themselves?

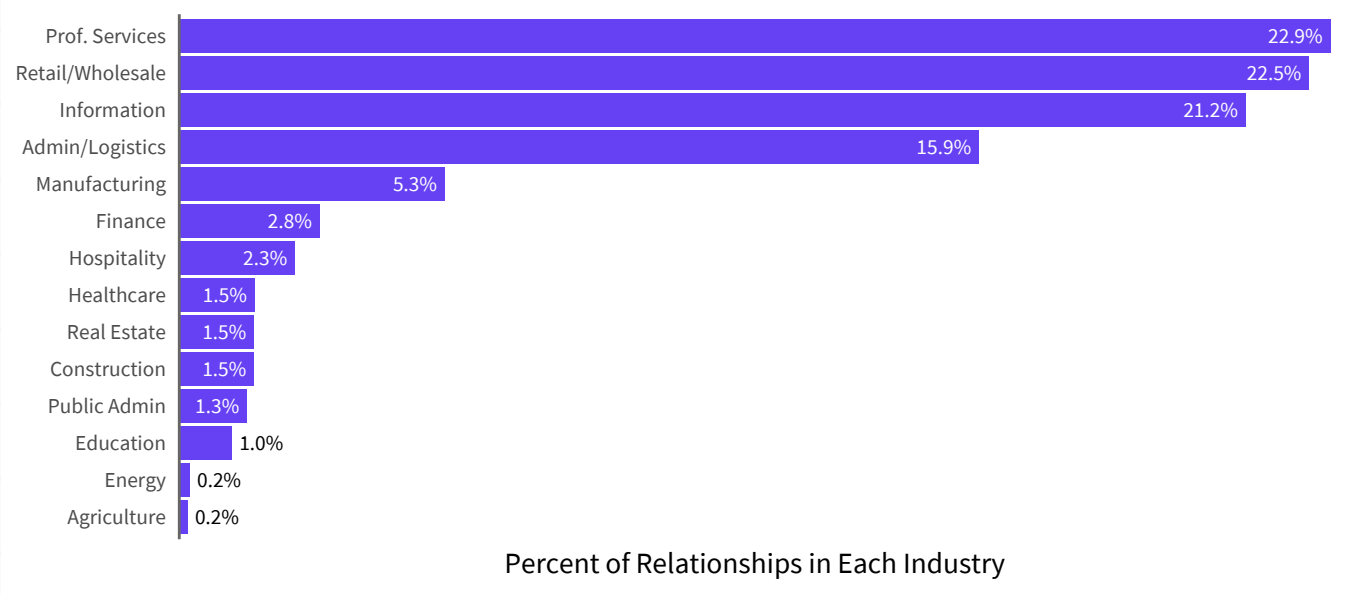


Figure 5: Proportion of third-party relationships associated with each sector.

The denominator in Figure 5 is all detected vendor relationships (185 million of them). So, 23% of all third-party connections are with professional services firms, 5% with manufacturers, sliding down to 0.1% for the Energy and Agriculture sectors.

These results are undoubtedly influenced by the size of the sectors listed (there are a ton of consultancies and retailers), but their propensity to play the role of vendor is a big factor as well. Comparing the positioning of industries in Figure 4 and Figure 5 yields some noticeable differences (i.e., Finance is last in Figure 4 but in the top half of Figure 5, indicating relatively few relationships per institution but substantial representation as a vendor of services).

How common are transnational third-party relationships?

We've examined industries common among third parties, and now we explore the regional dimension of those relationships. Doing business with a company in another country doesn't necessarily increase or decrease cyber risk. But, it does expose an organization to new laws, security requirements, and other geopolitical issues.

We tallied the number of unique countries represented across the network of third parties that we detected for each organization. Per Figure 6, 7% of firms have relationships with vendors in only their home country (no foreign ties). About 59% of organizations have connections to 5 or fewer countries, and roughly 14% have vendors spanning 10 or more countries.

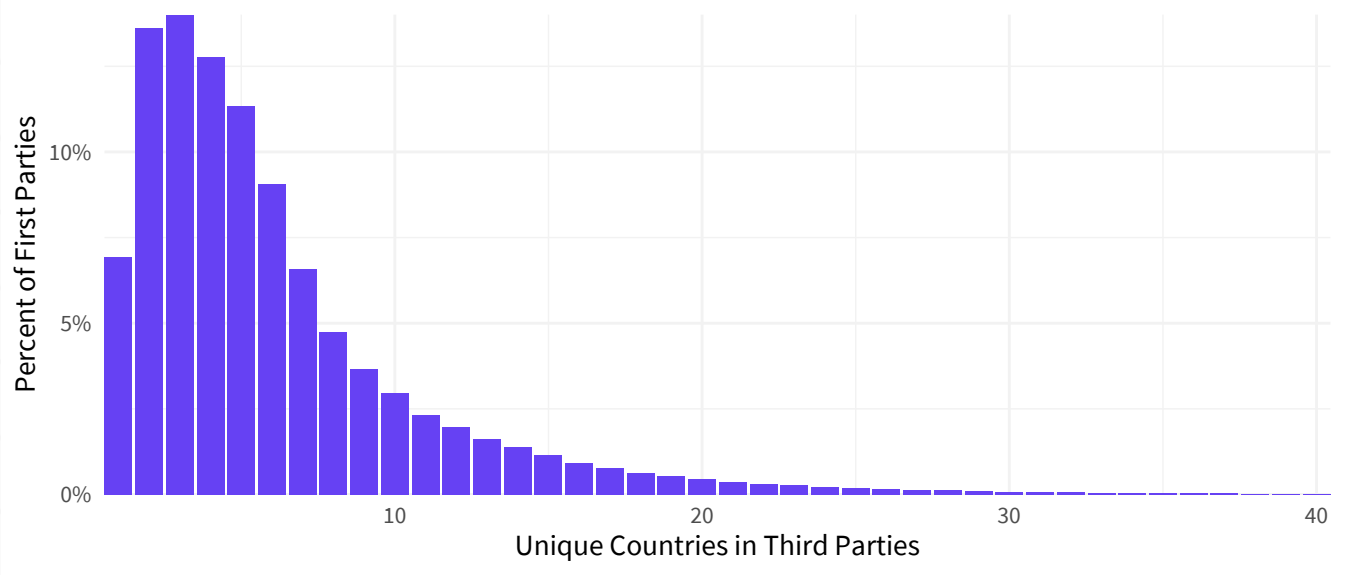


Figure 6: Number of countries represented among organizations` third-party relationships.

Another angle we can examine regarding transnational relationships is the degree of connectedness among regions. In other words, what world regions do detected vendors come from? Figure 7 shows that 99% of organizations have a relationship with companies in the United States and/or Canada. Southern Asia is next on the list with connections to 62% of firms and Northern Europe rounds out the top three regions.

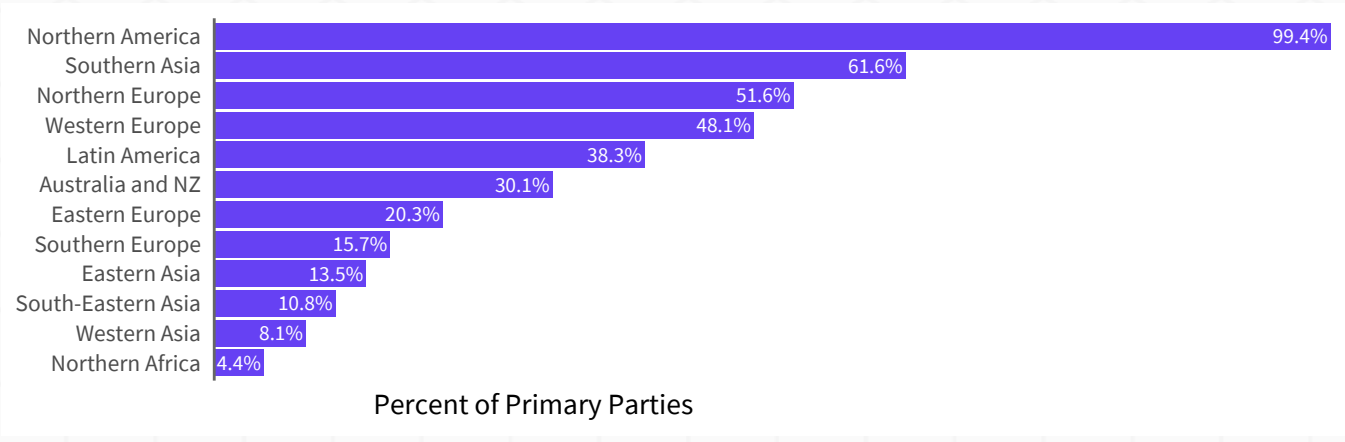


Figure 7: Percentage of organizations with third-party relationships in each region.

What technologies account for the most third-party relationships?

Another aspect of third-party risk that's top of mind for many organizations is the vendors and technologies that comprise their digital footprint. This collection of technologies is often referred to as "attack surface" and for good reason. It's constantly probed by adversaries seeking to exploit vulnerabilities and misconfigurations to gain illicit access to your systems, data, and users.

So, which vendors and technologies comprise that attack surface? Figure 8 has part of the answer to that question. We say "part of" the answer because this just shows the 50 most prevalent technologies indentified by Automatic Vendor Detection. For the most part, the list confirms what is already known or at least suspected. While most of us are using the likes of Google, Amazon, Microsoft, and Adobe, many of the other technologies round out our digital footprints or extended supply chains.

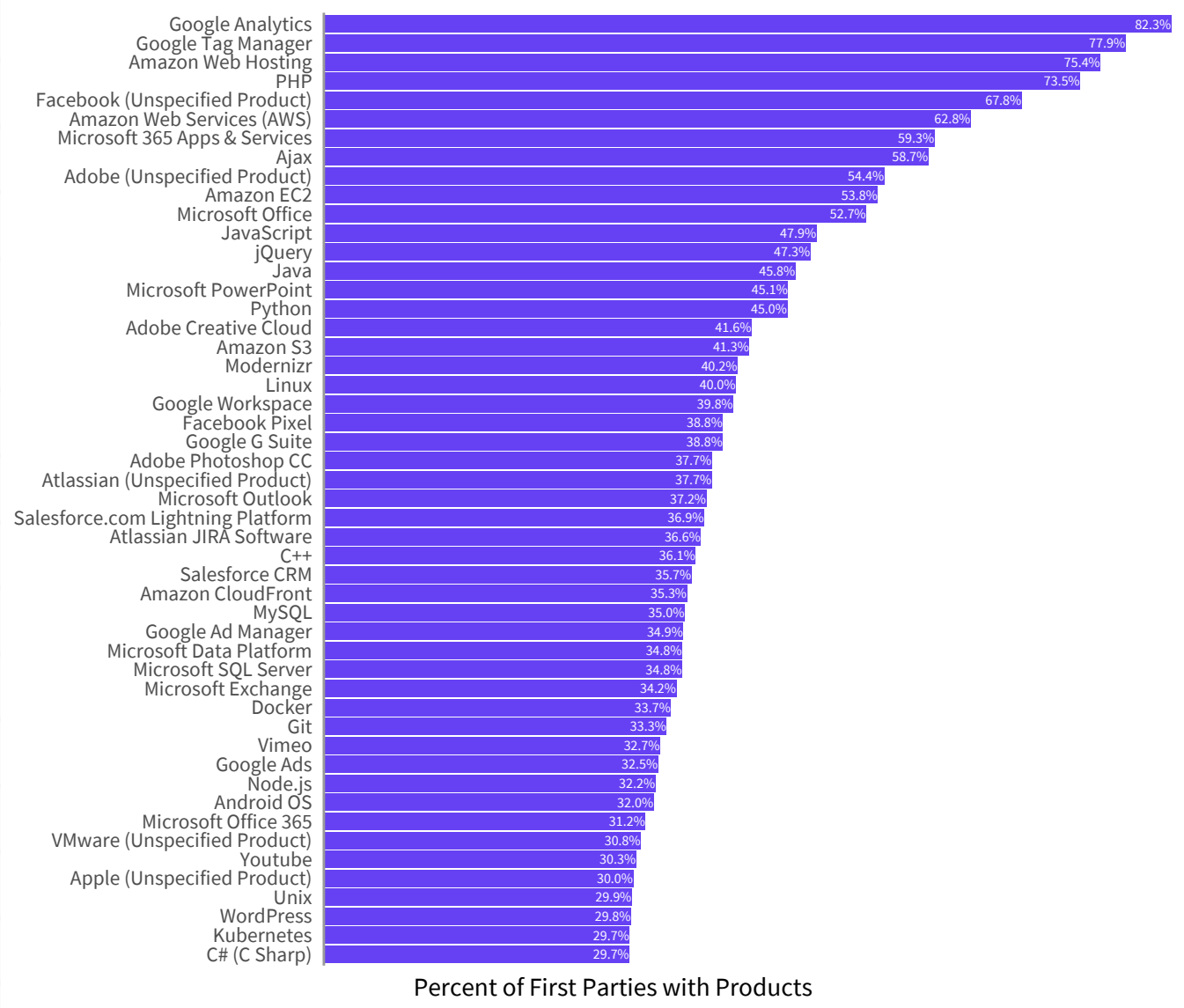


Figure 8: Most common technologies represented in third-party relationships

But, what about the less prevalent technologies that aren't shown in Figure 8? The iceberg metaphor is an apt one, because there are over 15,000 others that fall below the top 50 cutoff (imagine having to scroll through all those!). Managing the obvious vendors is certainly an important part of any third-party risk management program. But attention also must be given to technologies that lie below the surface to avoid the full range of potential hazards.

Enumerating Fourth Party Relationships

It would be easier if we lived in a world where we only had to worry about organizations that we have a direct business relationship with. But we don't. Modern firms are deeply interconnected, and many of those relationships span several degrees of separation (or degrees of Kevin Bacon, if you prefer). What's more, these indirect relationships introduce various forms of risk that are often outside your organization's control or even knowledge.

This section briefly examines the expansiveness of fourth-party relationships—organizations you share no direct relationship with but that are connected to your third parties. Discussions of fourth party relationships often bring up the topics of interdependencies and concentration risk. The ability to determine the fourth-party vendors in your extended digital supply chain can help organizations manage risks they might otherwise not be aware of or see coming.

What's the typical ratio of third to fourth parties?

It stands to reason that the more third parties a firm maintains, the amount of fourth-party relationships would be even greater. But how much more? Instead of direct relationships, this requires counting all the connections of connections, and the numbers blow up very quickly. We're not ones to let numerical challenges get in our way, so let's do this.

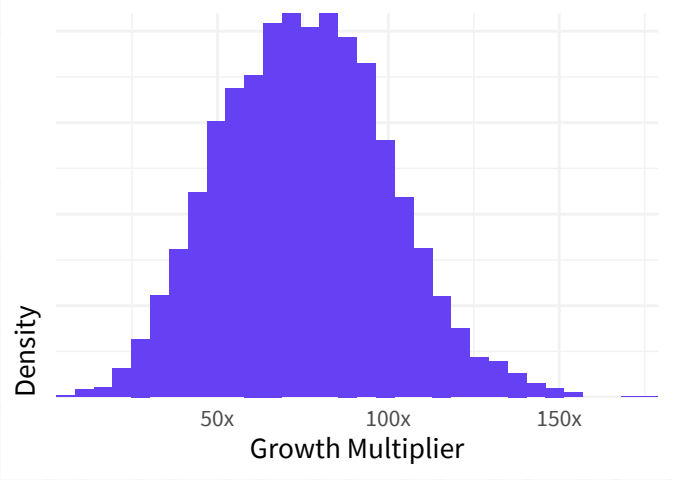


Figure 9: Growth multiplier for the number of fourth-party vs. third-party relationships

To measure this, we counted the number of third parties for each primary organization, and the total number of organizations each of those third parties were connected to (fourth parties). We then used those tallies to calculate a third-to-fourth-party growth multiplier for every organization. Figure 9 depicts how this growth multiplier plays out across all firms.

Given these third-parties that we can observe via Automatic Vendor Detection, the typical organization has indirect relationships with 60 to 90 times the number of fourth-parties. The fourth party growth multiplier for most organizations ranges between 15x and 150x. Depending on your perspective, that may seem remarkably compact or incredibly wide.Either way, it's an interesting point of comparison.

THE TYPICAL ORGANIZATION HAS INDIRECT RELATIONSHIPS WITH 60X TO 90X THE NUMBER OF FOURTH PARTIES.

What technologies account for the most fourth-party relationships?

Figure 8 reveals common third-party technologies used by the organizations in our sample. But, if we take what we just learned about fourth-party multiplication to heart, there's a realization that it's not enough to just know your direct vendors. You'll need to know who those vendors are connected with (and maybe even who *they are* connected with) to truly grasp the full extent of dependencies and exposure across your supply chain.

Let's move in that direction by investigating the most common "vendors of your vendors" identified in our sample. The x-axis of Figure 10 is basically a redo of what we showed in Figure 8—the most prevalent third-party technologies. It's easy to see that only a handful of vendors are used by more than 50% of organizations.

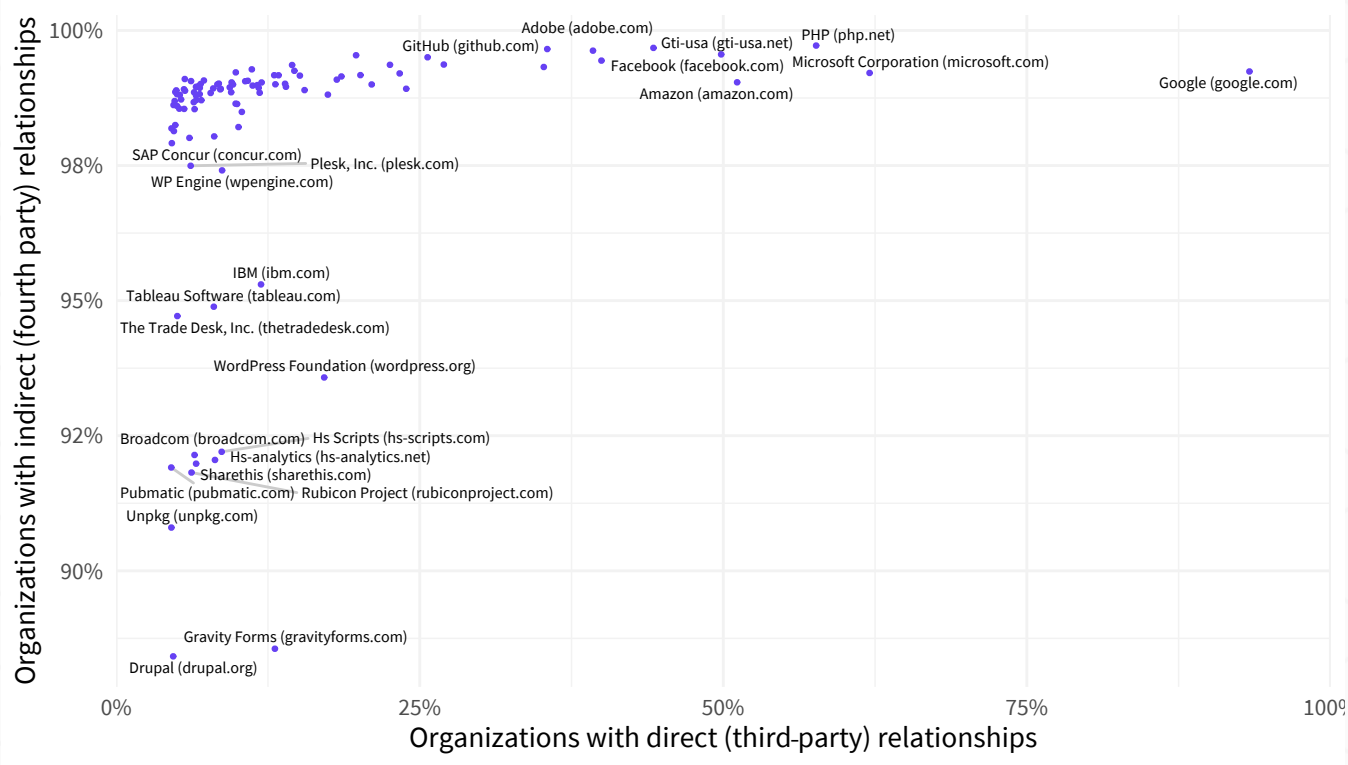


Figure 10: Prevalence of third and fourth-party relationships among top technologies

MOST ORGANIZATIONS ARE NO MORE THAN TWO STEPS REMOVED FROM EACH OF THE TOP 50 VENDORS.

Those numbers shift substantially for fourth-party relationships depicted on the y-axis. Rather than just a handful above the 50% mark, we now see that x-amount of vendors exceed 99% fourth-party saturation. Most organizations are no more than two steps removed from each of the top 50 vendors.

It bears repeating that this hyper interdependency doesn't by itself mean your supply chain is a stack of cards ready to crumble at the slightest nudge to any party. After all, many of the ubiquitous vendors listed in Figure 10 have a relatively good security track record. But, it's good to acknowledge an important fact: Even if your organization doesn't use a certain vendor or technology, there's a good chance that those you depend upon do. Because of that fact, you probably want to know how their security posture compares to that of your own.

WE EXPLORE THAT NEXT

Assessing Security of Third-party Relationships

It's now time to assess the relative security of third and fourth parties in a supply chain. Given the interdependencies we've observed thus far, it stands to reason that those dependencies have ramifications on cyber risk for both individual organizations and their broader supply chains. A firm that invests a great deal of effort in securing their own infrastructure could see those efforts undermined by vendors that don't maintain a similar level of security.

Are organizations more or less secure than their 3rd parties?

This is an important question for sure. While we can't answer it specific to your organization in this study[1], we can address it generally across the 235,000 organizations in our sample. We leverage ratings determined by SecurityScorecard as our measure of security posture for all first parties and vendors. Figure 10 compares the breakdown of scores for each group.

TWICE THE PROPORTION OF PRIMARY ORGANIZATIONS ACHIEVE THE HIGHEST SECURITY RATING OF A, WHILE THIRD PARTIES ARE NEARLY 5X MORE LIKELY TO RECEIVE AN F ON THEIR SCORECARD.

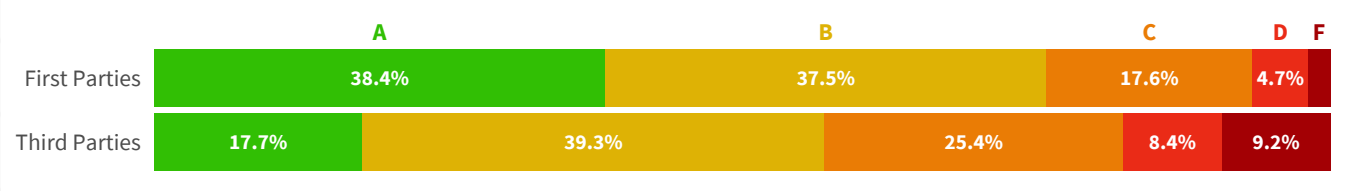


Figure II: Comparison of security posture rating for first and third parties

The results justify concern when it comes to the security posture of third-party vendors. Twice the proportion of primary organizations achieve the highest security rating of A, while third parties are nearly 5x more likely to receive an F on their scorecard. Not great news, but not entirely unexpected either for those familiar with third-party risk management.

At this point, you might be thinking something along the lines of "who cares about security grades—third-party breaches are what really matters to my organization!" Right you are. In fact, SecurityScorecard had the same question in mind when their analysts determined that firms with poor security ratings were up to 7.7 times more likely to experience a breach.[2]

[1] But you CAN begin answering this question for your organization with a free SecurityScorecard account.
[2] *Optimizing SecurityScorecard Ratings with Machine Learning*

Do less secure organizations also have less secure third parties?

The rather unfortunate answer, according to Figure 12, is "nope." About 10% of third-party vendors receive an F among organizations that earn an A for their own security posture. That proportion of failing vendors lessens along with the grade of first parties. Furthermore, the percentage of third parties with a strong security posture shows the opposite trend.

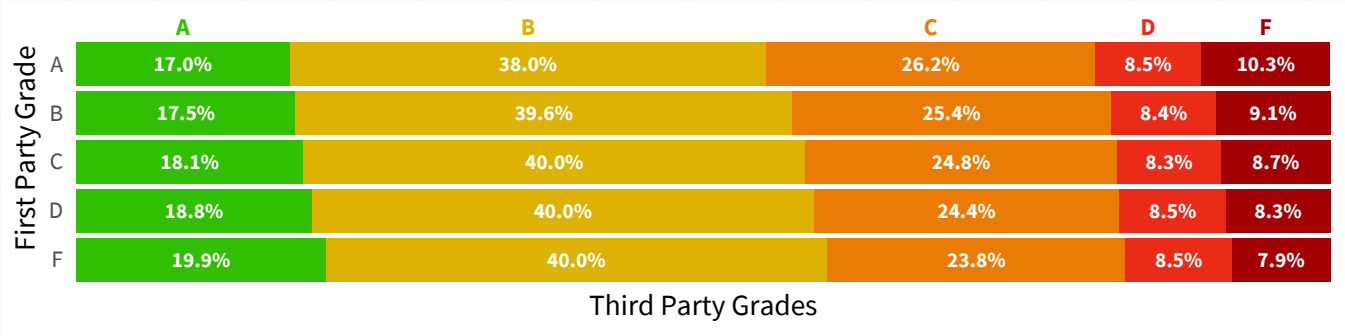


Figure 12: Third-party security ratings grouped by the rating of primary organizations

> *Many organizations are still unaware of the dependencies and exposures inherent to third-party relationships, and simply focus on managing their own security posture.*

This trend begs the question of "why?" Even though the ratios of third parties with poor and strong security don't differ dramatically based on first-party ratings, just the fact that there's not much difference seems worthy of consideration.

Many organizations are still unaware of the dependencies and exposures inherent to third-party relationships, and simply focus on managing their own security posture. Others are aware of those issues, but don't make vendor decisions based on security and/or require vendors to meet certain standards. Even firms that do establish third-party security requirements can struggle to continually monitor compliance and progress.

The good news is that the state of affairs may be changing.[3] According to Gartner, 60% of firms will use cyber risk as a significant determinant in conducting third-party transactions and business engagement. Our hope is that helps to make managing risk across supply chains more about creating a resilient ecosystem for all than pitting us vs. them.

Do less secure organizations have more vendor relationships?

The ecosystem analogy is actually more appropriate to third-party risk than you might initially think. Organisms in an ecosystem interact with and impact other members as well as their environment. In similar fashion, the security of organizations in a digital ecosystem can, and will, affect those around them.

One outworking of that can be seen in Figure 13, where we compare the number of third-party relationships identified by Automatic Vendor Detection for organizations of varying security ratings. In general, firms that achieve higher security ratings have fewer vendors (D/F's have >2x more than A's). Or perhaps it's vice versa: organizations with larger digital supply chains exhibit weaker security.

[3]2022 Gartner Market Guide for IT Vendor Risk Management Solutions

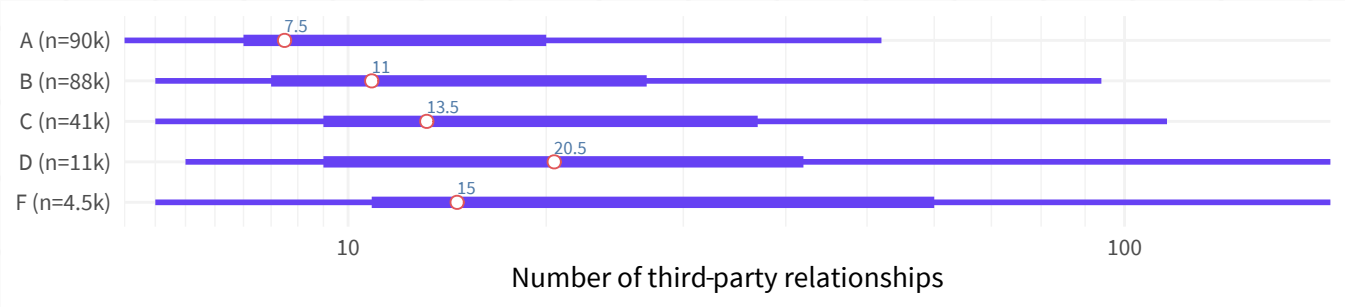


Figure 13: Number of third-party relationships based on first-party security rating

THE FOURTH-PARTY GROWTH MULTIPLIER OFORGANIZATIONS WITH A FAILING SECURITY GRADE IS 10X THAT OF THOSE RATED A.

We see the same trend when examining fourth-party relationships in Figure 14. The fourth-party growth multiplier of organizations with a failing security grade is 10x that of those rated A. Thus, we see an inverse correlation between expansive third and fourth party dependencies and strong security posture.

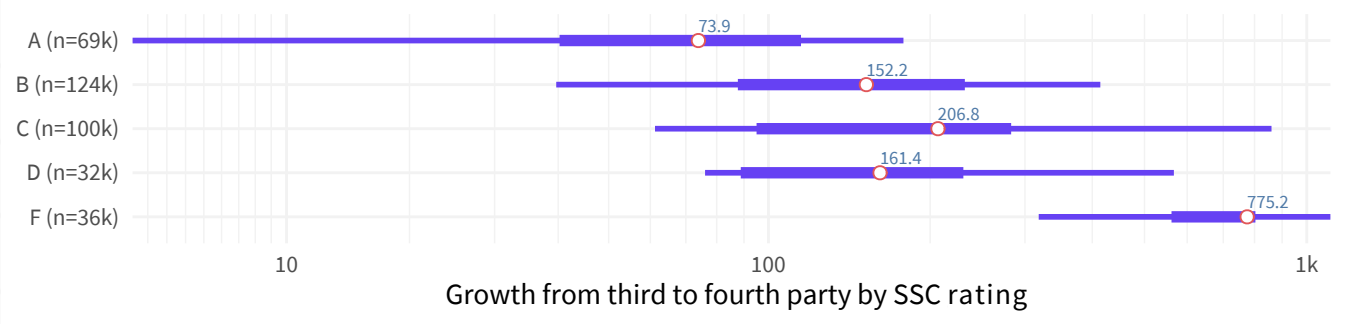


Figure 14: Fourth-party growth multiplier based on first-party security rating

We know what you're thinking—correlation isn't causation. And we agree. Any number of factors could be influencing what we see in Figures 13 and 14. It's certainly not as simple as "more vendors, less secure." But more vendors do add complexities, dependencies, and vulnerabilities that are increasingly difficult for your organization to monitor and manage.

Which technologies are more security organizations using?

Let's tackle one more question before closing out this report. While not our intention, we're conscious of the fact that some may interpret findings in the last section as justification for strict isolationist policies when it comes to vendor risk management. So, we thought we'd try to head that off by ending on a positive note: there are vendors and technologies that correlate with better security ratings.

More vendors do add complexities, dependencies, and vulnerabilities that are increasingly difficult for your organization to monitor and manage.

To be clear—the vendor landscape isn't divided into "bad" and "good" security. For the most part, organizations with ratings from A through F use many of the same technologies (they just manage them differently). But there do seem to be certain technologies that are significantly more likely to be used by organizations with strong security postures. Those with the highest variation in adoption rates between firms with A and F security ratings are shown in Figure 15.

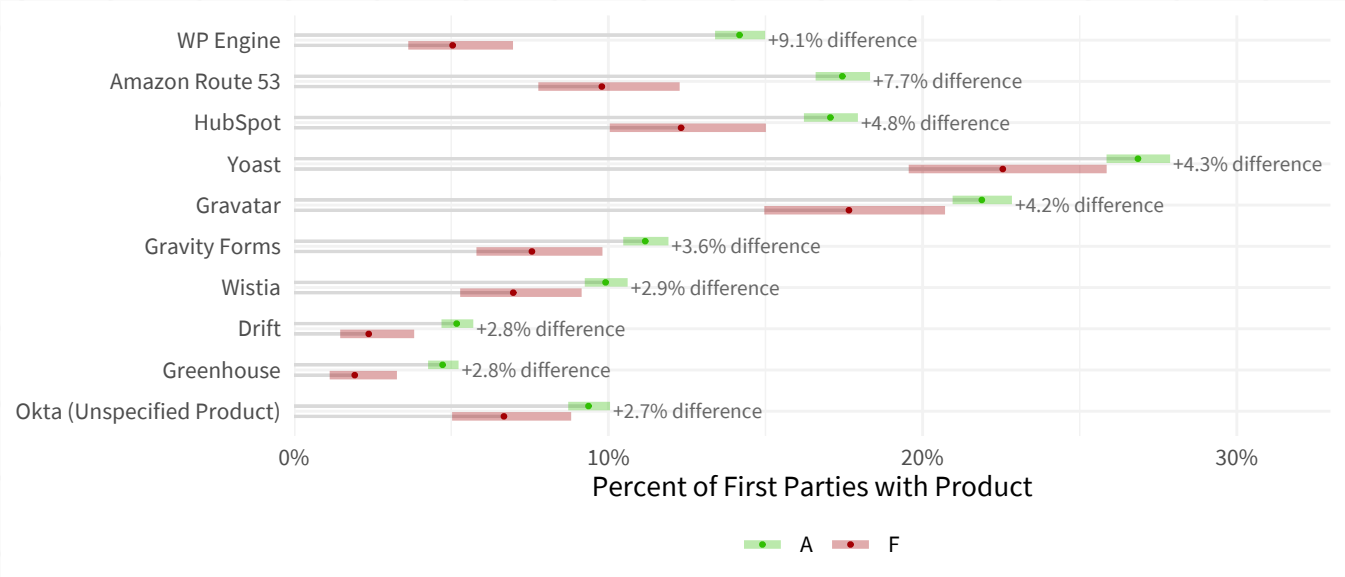


Figure 15: Technologies adopted by organizations with higher security ratings

We're not going to attempt to comment as to why these technologies have higher prevalence among firms with better ratings. We'll simply observe that several technologies featured in Figure 15 are major cloud providers, and enterprise-grade software solutions. Some may find it ironic that Okta makes the list, given their very public incident earlier in 2022. But, think of it this way: organizations using Okta almost certainly have an above average level of security awareness and maturity. Plus, it goes to show that there are no guarantees when it comes to managing cyber risk. That is, after all, why we call it "risk."

Final Reflections

As these findings indicate, almost all organizations work with third parties who have suffered some type of breach in the past two years. Managing cyber risk across your digital supply chain is more important than ever as cyber threat actors continue to find new ways to exploit any vulnerabilities a company may have. So what steps can your organization take to minimize any potential risk stemming from your third or fourth parties?

Understand Which Companies You Work With

Getting the entire picture of your vendor ecosystem is key to assessing risk and making informed decisions on your relationships with those vendors. Using tools that help you automate the vendor detection process can help you get that critical 360 degree view of your vendor ecosystem and potentially exposed companies you didn't even know your organization was working with.

Determine the Security Posture of Your Third and Fourth Parties

Once you've identified the companies you work with, knowing their cyber risk rating and any potential vulnerabilities an organization may have can help you make an informed decision about whether the associated risk is acceptable.

Collaborate with Vendors to Improve Your Own Security Posture

Work with your vendors to help improve any potential risks or vulnerabilities you discover about their security posture. This, in turn, improves your own cyber health.

Continuously Monitor Through Automation

Continuously monitoring your vendors' cyber risk and being alerted when there is a notable change to their security posture gives you the ability to collaborate with your partners, prioritize vulnerability remediation, and build a safer and more resilient digital ecosystem before a potential problem begins.

Your security posture is never just your security posture. It's a combination of yours, your vendors', and their vendors' that makes up your entire digital ecosystem. Getting ahead of potential risks and vulnerabilities associated with your third and fourth parties can help you not only manage risk, but also drive business results by saving your organization valuable time and money, and earning the trust of your employees, customers, and partners.

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, 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 30,000 organizations for enterprise risk management, third- party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

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. Gain continuous visibility into your digital footprint, vulnerabilities, and clear steps to remediate them with SecurityScorecard. Claim your free account and take control of your cybersecurity risk.

About The Cyentia Institute

The Cyentia Institute is a research and data science firm working to advance cybersecurity knowledge and practice. Cyentia pursues this goal through data-driven studies like this one and through a growing portfolio of analytic services. Learn more at www.cyentia.com.