riskrecon by Mastercard

Cyentia Institute

Balancing Third-Party Risk

How Good Is the Company You Keep?

May 23rd, 2023

Introduction

> "Assumptions are the termites of relationships."
>
> -Henry Winkler

Organizations have a lot of assumptions about third-party risk. Many assume their vendors have terrible security posture and represent grave danger to their business. Others assume the opposite—that their partners are probably decent folks doing the best they can to work together securely. Sometimes annual questionnaires form what organizations believe about their vendors' security posture, but that only shows what they want you to know.

Thankfully, it's not necessary to make blind assumptions about third-party risk. We have data from security assessments of over 50,000 business-to-business (B2B) relationships. We'll use that data to investigate the equity of these relationships from a cybersecurity perspective. As we do, expect that some of your assumptions about third-party security will be shattered while others confirmed so they become true actual knowledge. Here's a sampling of findings that recalibrated our understanding of security imbalance in third-party relationships:

Key Findings

99.5% of organizations have at least one vendor in their third-party risk management program with a cyber **risk rating of D** or **F**.

86% of B2B relationships involve parties with **imbalanced breach histories** (one's had a breach, while the other hasn't).

20% of all third parties viewed **showed signs of experiencing a data breach** within the last three years.

Overall, just under **30%** of all third-party relationships involve a vendor with **worse security** than their primary sourcing firm.

Among organizations that have at least one vendor with inferior security ratings, **78%** of third parties had a significantly **higher density** of critical security findings

On average, high-risk vendors in our research had **4.5x higher** critical finding density than their sourcing firm. And some were **10x, 100x—even 1,000x—worse!**

Organizations that blindly choose 50 of the least secure vendors will have **30x the exposure** compared to those partnering with 50 firms with the highest finding density!

Sourcing firms are exposed to **3X as many** unique types of **security issues** from third parties than exist in their own infrastructure.

Source Data & Methodology

TL;DR methodology: We extracted a sample of ~1,000 organizations, each monitoring at least 25 third parties with RiskRecon. This spans 50,000 third-party relationships, which we examine in this report.

In our Internet Risk Surface Report, we explored implicit relationships between organizations and their third-party providers based on RiskRecon's external assessments. This report is different in that we're focusing on explicit relationships that are manually configured by organizations using RiskRecon's platform. In other words, we're examining curated portfolios of vendors and suppliers tracked as part of organizations' third-party risk management program.

Before moving forward, it's important to note that the data provided to Cyentia for this analysis uses anonymous IDs for all primary and third-party organizations. This allows us to study the relationships between organizations without identifying information other than basic firmographics.

We started with a dataset extracted from RiskRecon's platform consisting of over 100,000 primary organizations and more than 300,000 monitored third-party relationships. We're focusing on direct relationships in this report, but the data supports the analysis of indirect (fourth- to nth-party) relationships. We'll explore those nth-degree relationships in future research.

A large majority of organizations are monitoring a small number of third parties. Since we're mainly interested in insights relevant to more mature third-party risk management programs, we decided to construct our sample from firms tracking at least 25 third parties. To put that into perspective, our 2020 State of Third Party Risk Management survey found that 60% of respondents assessed 25 or more vendors each year.

Using that threshold, we extracted a sample of approximately 1,000 primary organizations spanning 50,000+ third-party relationships. We also leveraged RiskRecon's security assessment of the domains and internet-facing systems associated with both primary organizations and all third parties they monitor. This forms the basis of the security posture comparisons we make in this report.

Some terms we use in this report

First party: The organization monitoring another party using RiskRecon. We also refer to first parties as "primary" or "sourcing" organizations.

Third party: The organization being monitored by the first party.

Relationship: The one-to-one connection that exists between the first and third party. Organizations can be part of many relationships and be the first party in one and third party in another.

Third-Party Firmographics

This section provides information about the primary or first-party organizations in our sample and their third parties. We'll start with the number of third parties monitored and then touch on the industries, sizes, and regions represented.

We mentioned in the methodology section that we excluded organizations monitoring fewer than 25 vendors, so it seems a good starting point to measure what's typical among those in our sample. On average, each organization tracks about 50 vendors in their portfolio. The largest 5% of portfolios contain 100 or more third parties.

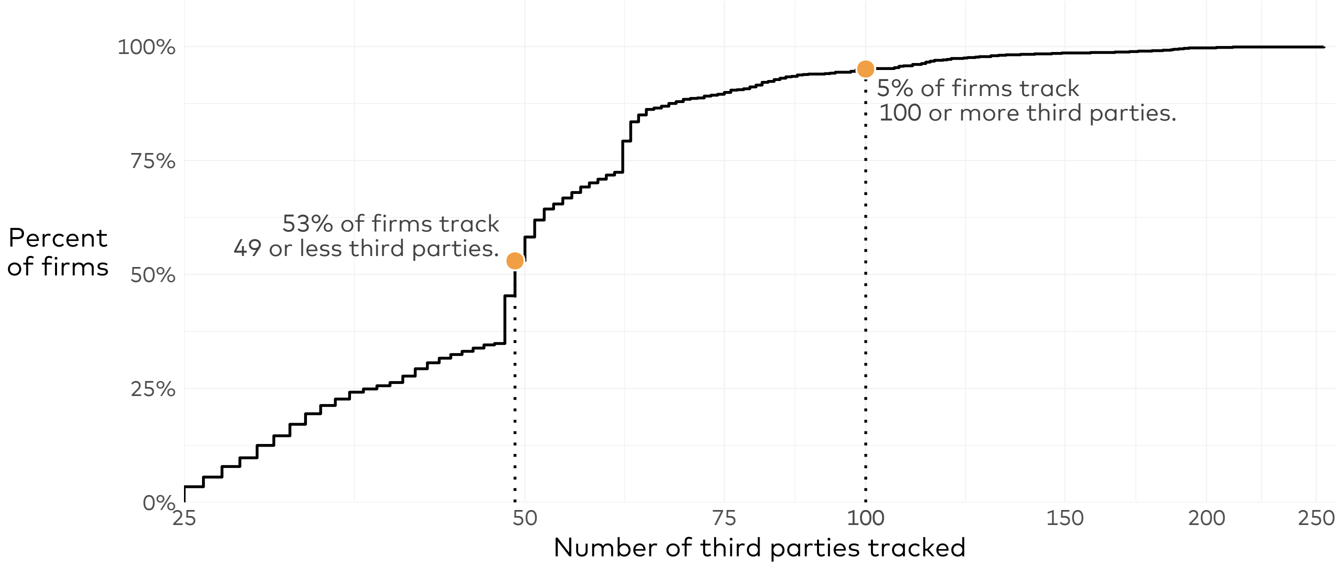


Figure 1: Number of third parties monitored by each primary organization

Next, let's look at an industry breakdown of primary and third-party firms. Per the leftmost column in Figure 2, Finance, Information, and Professional Services together comprise over 80% of primary organizations. Finance is still on top among all third parties in our sample (second column), but Manufacturing is placed in the top three, and Professional Services ranks at number 4.

The third column is a bit different. It shows the ratio each industry typically represents within primary organizations' third-party risk portfolio. So, financial firms typically represent nearly 70% of the vendors monitored by each organization, and no other industry claims more than 10% of the portfolio. "For where your treasure is, there will your heart oversight be also" seems an appropriate (adapted) quote.

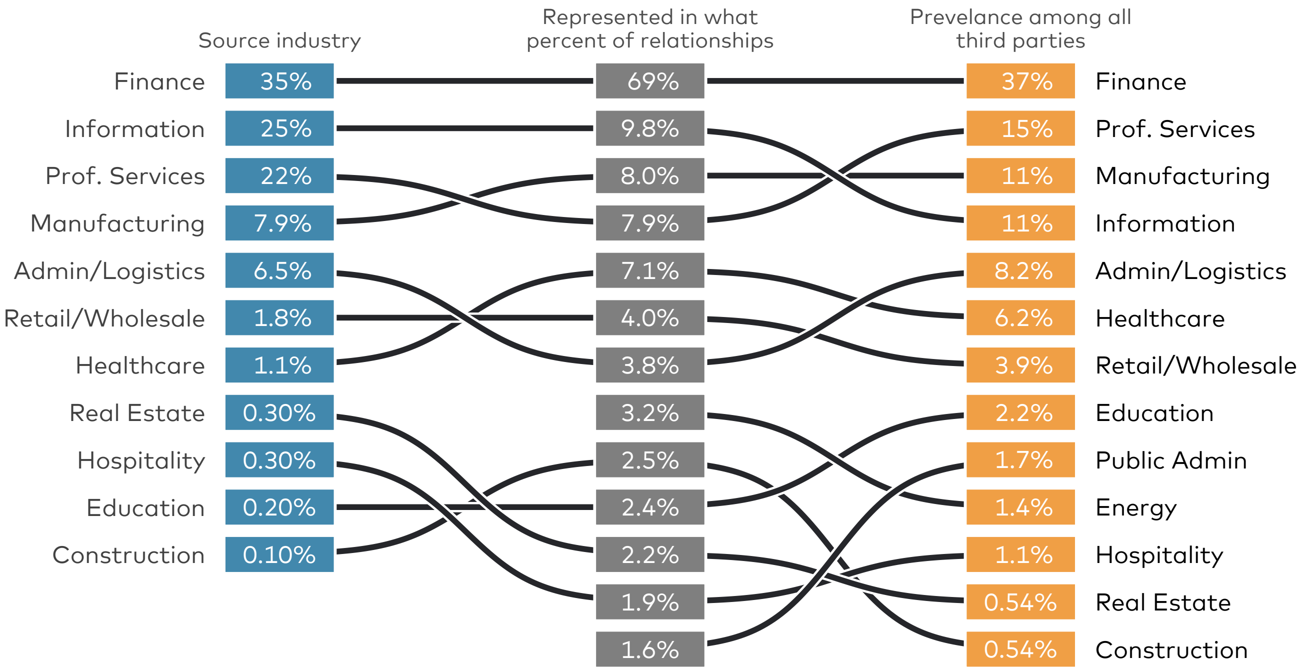


Figure 2: Industry representation among primary organizations and third parties

What about the relative size of first and third parties—who's the bigger player? We measured size in this case based on the number of internet-facing hosts for each organization. Figure 2 makes it plain that primary organizations are larger than their third parties in over half of the relationships we examined. Vendors are a larger party about 30% of the time, and the remaining ~20% of relationships are on equal footing.

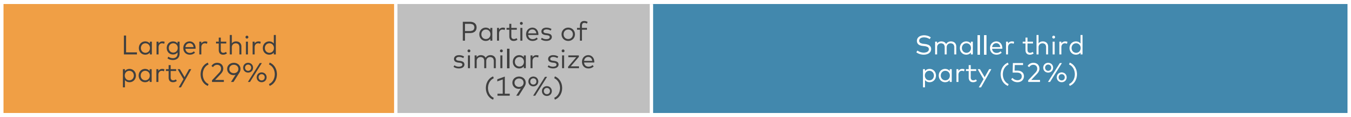


Figure 3: Relative size of primary organizations and third parties

We'll take a look at one last firmographic dimension before closing out this section—the geographic region of third parties. Since we measured size based on digital footprint, we'll stick with that approach here...with a twist. Many organizations have systems in multiple regions, so we've elected to assign the region based on where the majority of hosts are located.

The horizontal axis of Figure 4 shows the percentage of primary organizations monitoring third parties with a majority of hosts in each global region. Keep in mind that these are not mutually exclusive. Just about all organizations have at least one vendor with hosts in North America in their portfolio, followed by Europe (~90%) and Asia (~65%).

A little over **35% of relationships** involve a vendor in **North America**

On the vertical axis, we show the percentage of all relationships represented by third parties in each region. The ordering is mostly the same, but the percentages are lower. A little over 35% of relationships involve a vendor in North America, while less than 0.03% hail from Africa. The size of the dots is relative to the unique number of third parties in each region.

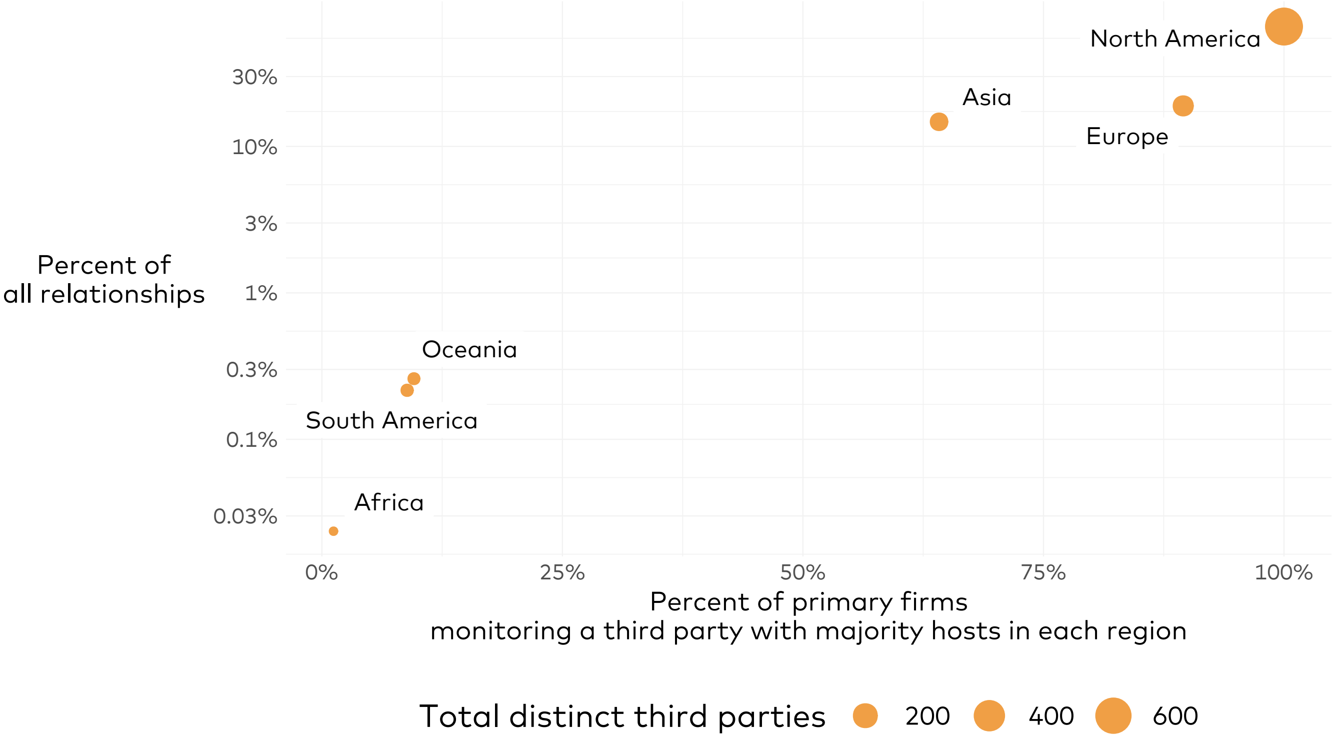


Figure 4: Regional representation of third parties based on majority of hosts

Calibrating the Balance of Risk

"Give me golf clubs, fresh air and a beautiful partner, and you can keep the clubs and the fresh air."

-Jack Benny

In this section, we compare the security posture of first and third parties. As you might suspect, these partnerships are not always productive. We leverage RiskRecon's continuous security assessments of organizations' internet-facing systems and related intelligence. Our main interest is to understand how balanced these business relationships are from a cyber risk perspective. We'll explore a few different ways of assessing security posture, including prior breaches, ratings, and the density and type of findings.

Breaches of Third Parties

Beyond continuously monitoring cybersecurity hygiene, RiskRecon analysts catalog breach events occurring in organizations around the world. Analysts source data loss events from channels such as public media, regulatory filings, and dark web monitoring. We published a study analyzing 10 years of incidents discovered through these methods, which provides in-depth information.

We'll leverage that breach signals intelligence here to examine the "nearness" of security incidents within third-party relationships. And just like your rearview mirror warns: breaches are closer than they may appear. Every primary organization in our sample has at least one vendor in their portfolio with a detected breach in the preceding 36 months.

That stat certainly has some shock value, but it doesn't do a lot to inform third-party risk management decisions. Knowing the proportion of vendors with breaches would be a lot more useful. So, let's do that.

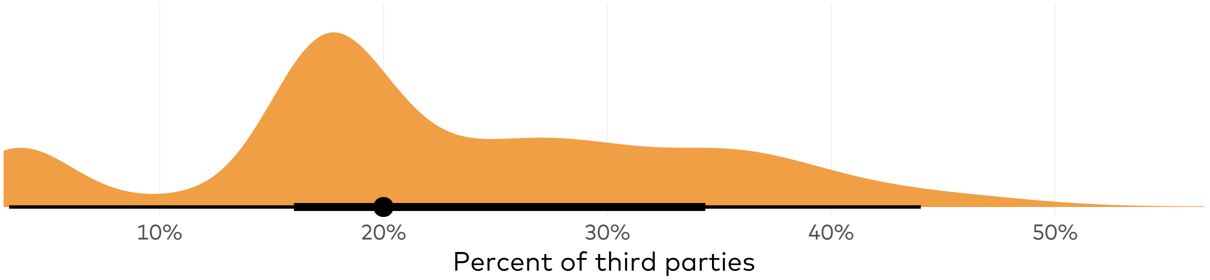


Figure 5: Percent of monitored third parties with probable breaches in the last 36 months

About 20% of the third parties in a typical organization's vendor portfolio showed signs of experiencing a breach in the preceding three years. As seen in Figure 5, there's quite a bit of variation among firms on that proportion, ranging from 5% to over 50%. Breaches of third parties under management doesn't mean the source organization was harmed in any way, of course. But there's presumably a risk-relevant reason those firms were being monitored through a platform like RiskRecon. Most third-party risk management teams would like to see that ratio as low as possible.

Since we're exploring the concept of security equity in B2B relationships, we found it prudent to widen the spotlight to cover not just third parties but also the first-party firms monitoring them. Which party is more prone to breaches? To answer this, we examined the historical breach information collected on both parties in each of the 50,000+ relationships.

In 14% of those relationships, we found evidence that both parties experienced a breach within the preceding 36 months. Third parties were the only side breached in 45% of partnerships, while first parties were the sole breached entity 41% of the time.

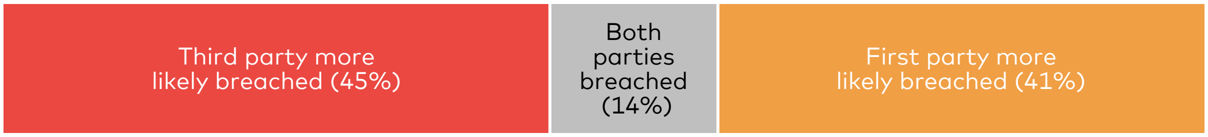


Figure 6: Comparison of historical breaches between between first and third parties

On the surface, that seems remarkably equitable. Though it probably doesn't feel that way if you're in a relationship where the other party has a bad track record, and yours is a clean slate. Looking at it from that perspective, 86% of B2B relationships involve parties with imbalanced breach histories (one's had a breach, while the other hasn't).

86% OF B2B RELATIONSHIPS involve parties with imbalanced breach histories

Security Posture of Third Parties

Breaches among third parties are certainly an indicator of security posture but not a direct measure of it. We turn to measuring this now, and we'll do this using two different methods. The first uses RiskRecon's cybersecurity risk rating for each vendor, and the second examines the density of security findings detected during those assessments.

Cyber Risk Ratings

RiskRecon's risk ratings are based on continuous assessments of the prevalence and severity of security issues affecting and the value at risk for the systems in which those issues exist. They provide a concise way to pinpoint concentrations of risk across the third-party ecosystem. Specific to this study, they offer a simple comparison of security posture among primary organizations and vendors in their risk management portfolios.

If we simply compare the breakdown of scores among first and third parties in Figure 7, the results aren't all that different and convey a false sense of relative equity among organizations. But that is often how statistics work. With so many organizations in each group, results inevitably trend toward the average.

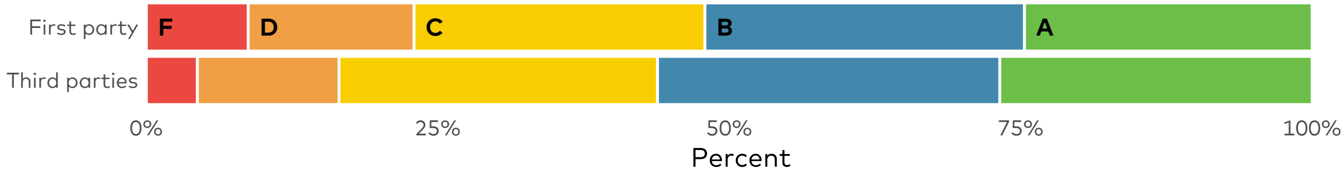


Figure 7: Overall comparison risk ratings between primary and third parties

Instead, we're more interested in comparisons made within the context of each organization's third-party ecosystem. Those results are more telling. We found that 99.5% of organizations have at least one vendor with an overall risk rating of D or F. Typically, though, less than 10% of the third parties monitored by each primary firm score Ds or Fs.

86% of Organizations have at least one third party with a risk rating worse than their own!

But keep in mind that first parties get D and F ratings too. For that reason, we think it more enlightening to compare the equity of risk ratings at the relationship level. Here, we learn that 86% of organizations have at least one third party with a risk rating worse than their own. If we extend the first-to-third-party rating comparisons across the entire vendor portfolio, we get Figure 8.

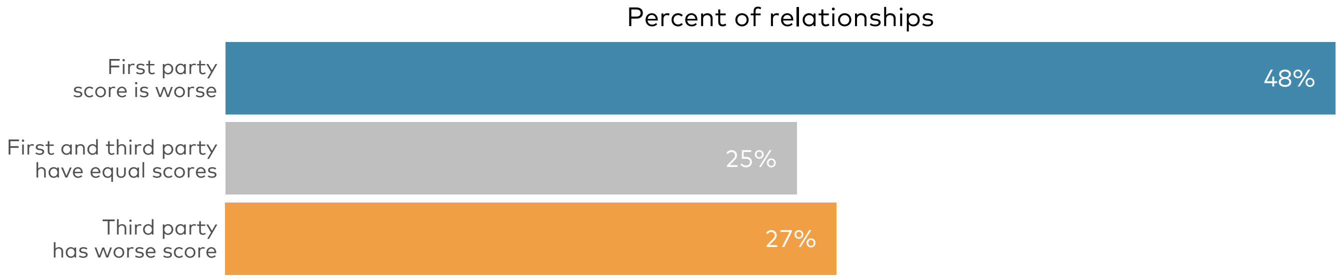


Figure 8: Relative comparison of risk ratings within third-party relationships

A quarter of B2B relationships are balanced in the sense that first and third parties have the same risk rating. In what is likely to be an eye-opening and uncomfortable finding for many, organizations have a worse security posture than their third parties in just under half of all relationships we assessed. We can't help but think of the adage, "Every time you point a finger in scorn, there are three fingers pointing back at you." But third-party risk management is mostly about that first finger, so let's keep our focus on that for now.

> "Every time you point a finger in scorn, there are three fingers pointing back at you."
>
> -Unknown

Per Figure 8, just under 3 in 10 of all B2B relationships involve a third party with a worse risk rating than their primary sourcing firm. That varies among portfolios, of course, which is why we include Figure 9 for additional insight. Here, we see that the majority of firms fall at or below that 27% overall mark for relatively less secure vendors. But we also see many organizations for which over half their third-party portfolio has worse risk ratings than their own.

Just under **3 in 10 of all B2B relationships** involve a third party with a worse risk rating than their primary sourcing firm

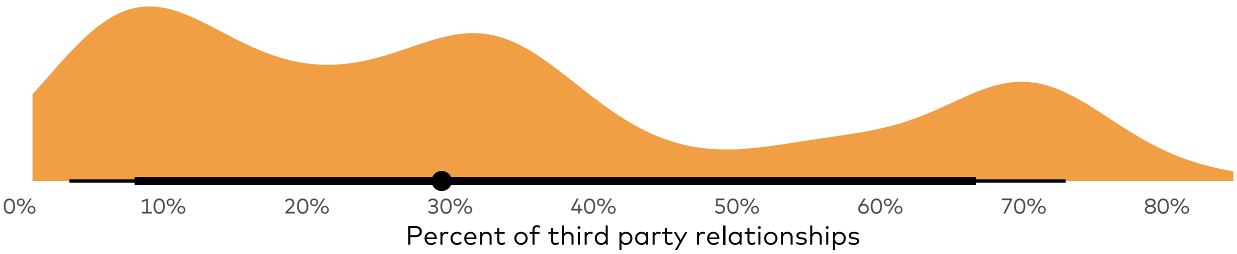


Figure 9: Proportion of relationships in which third parties rate worse than first parties

Before leaving the topic of relative risk ratings among parties, we'll note an interesting observation made in running these portfolio-level comparisons. Organizations with larger vendor portfolios tend to have a significantly lower proportion of worse-rated vendors. This may be due to more robust third-party risk management programs necessitated by larger supply chains. A muscle exercised is a muscle strengthened.

Density of Security Findings

Risk ratings provide a great overall assessment, but we're also interested in directly comparing the prevalence of findings within partnerships as well. In prior research, we used a metric termed high-risk finding density as a measurable proxy for organizational cybersecurity posture. It focuses on the worst security issues affecting the most critical assets, which is usually a fairly small subset of all findings. That's telling because if organizations aren't addressing those riskiest issues, they're probably not staying on top of other aspects of their security posture either.[1]

Now that it's defined, let's see if finding density can shed some additional light on the darker side of third-party relationships. We'll start simply—what proportion of relationships involve vendors with a higher density of risky findings than the organization they serve? Overall, about one-quarter of all third-party relationships fit that description and are thus risk-additive in nature. That's in line with the ratio we saw earlier for risk ratings.

[1] More information on the predictive value of high-risk finding density can be found in the joint RiskRecon and Cyentia Institute report: From Uncertainty to Understanding

Finding density allows us to measure precisely how much worse those risky vendors are compared to their sourcing organizations. This comparison gets to the heart of the notion of security equity in third-party relationships. The answer revealed in Figure 10 may surprise you.

Among organizations with at least one risk-additive relationship, the high-risk finding density of third parties in their portfolio is typically **4.5 times worse than their own**.

What's more, there's no shortage of vendors that **were 10x, 100x—even 1000x—worse!** We suspect not many would consider that a healthy, equitable business relationship.

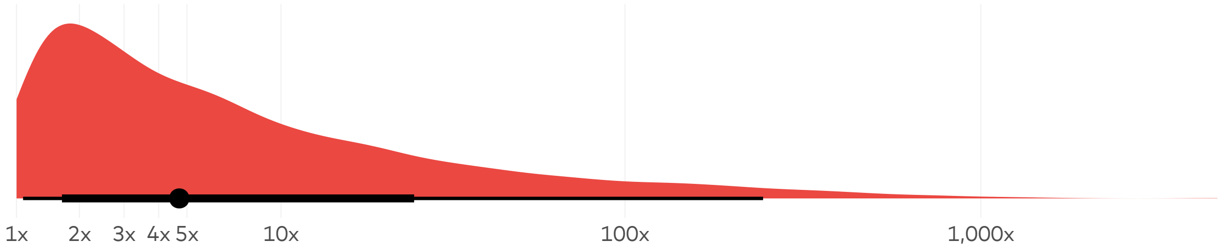


Figure 10: Relative density of high-risk security findings for third vs. first parties

One bad apple spoils the bushel

In analyzing finding density within third-party portfolios, we noticed that imbalanced partnerships tend to come in droves. If an organization has at least one vendor with a worse security posture than its own, there's a good chance that many others do too. Take a look at Figure 11, which illustrates this phenomenon.

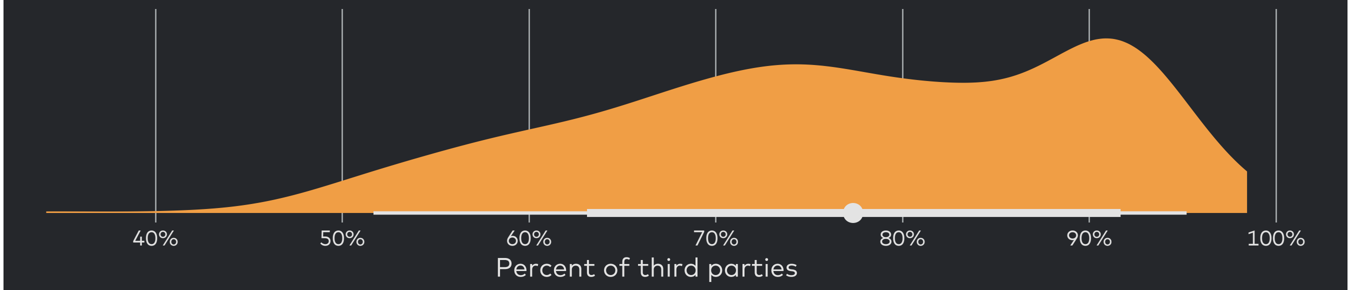


Figure 11: Proportion of third parties with worse density of high risk findings compared to first parties

Given there's at least one bad apple in the portfolio, we found that an average of 78% of all monitored third parties had a higher density of high-risk findings than the sourcing organization. Perhaps, like misery, insecurity loves company. Or, more likely, mature third-party risk management programs remove or reform bad apples before they spoil the whole bushel.

At this point, you may be thinking, "If one vendor has 5x our finding density, what happens when we're working with numerous less-secure partners?" That's the question on our minds, at least. So, we'll briefly weigh the effects of poor partnership choices to close out this section.

To do this, we sampled from the best 100 third parties with the lowest...." and "and the worst 100 with the highest density. Our interest is to contrast the effect of bad vs. good partnership choices on the security posture of the entirety of monitored third parties. Figure 12 tallies these mounting effects across vendor ecosystems of increasing size. Spoiler: they're **HUGE**!

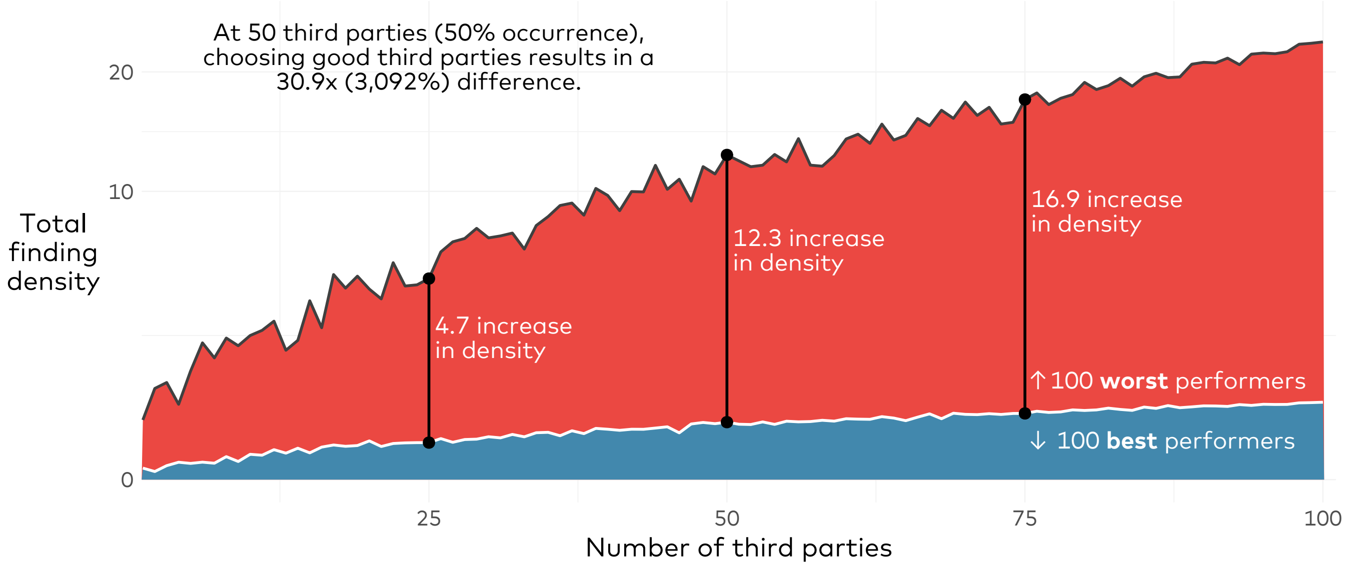


Figure 12: Compounding effect on overall exposure from partnering with insecure third-parties

> Organizations that blindly choose 50 of the least secure vendors will have **30x the exposure** of those partnering with 50 firms with the highest finding density!

Earlier, we noted that organizations in our sample are actively monitoring a median of 50 vendors. Organizations that blindly choose 50 of the least secure vendors will have 30x the exposure of those partnering with 50 firms with the highest finding density! The security impact of those poor partnership choices grows, of course, with the number of third parties under management.

It's true that this is an extreme and rather unrealistic example. It's unlikely that any organization would always choose the least secure partners. Yet the question it begs remains valid: How do you distinguish which vendors have security postures consonant with your own and which do not?

> ♫♪Oh, choose partners, skip to my Lou
> Lost my partner, What'll I do?
> I'll find another one better than you!
> Skip to my Lou, my darling!♫♪
>
> -Skip to my Lou, Unknown Origin

The Risk of Contagion

The last section made it quite clear that organizations can greatly increase their risk exposure through insecure third-party relationships. But what wasn't stated directly is that they also become exposed to a host of new security issues they're not used to dealing with through those partners. We'll illustrate that challenge in this short section.

RiskRecon groups security findings identified through its ongoing assessments into high-level domains and criteria. For instance, the most frequent issues detected for the primary organizations in our sample fell into the network filtering and software patching domains. Running unsafe network services is a common example of the former while failing to apply the latest updates to web servers exemplifies the latter.

Figure 13 demonstrates how things shift around in the context of third-party relationships: 83% of organizations have vendors in their portfolio flagged by intelligence sources for malicious scanning activity. That may not seem like a big deal until you realize those scans may uncover vulnerabilities in a partner's systems that enable attackers to propagate to yours.

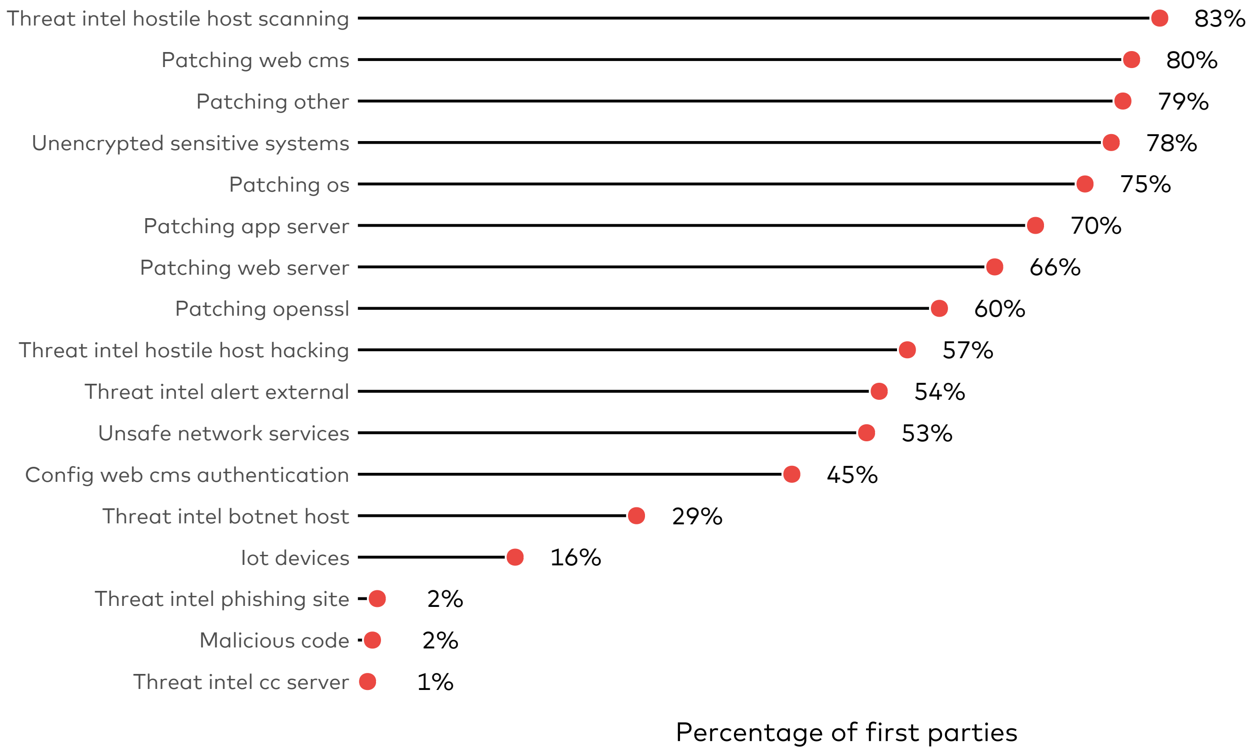


Figure 13: Types of security findings organizations become exposed to via third parties

Firms typically **"inherit" exposure to 3x as many unique types of security issues** from third parties than exist in their own infrastructure.

Speaking of exposure to vulnerabilities, poor patching of various types of infrastructure evidently plagues many third-party relationships. Intelligence reports of hacked systems and running unsafe services also affect the vendors of over half the organizations in our sample. All told, firms typically "inherit" exposure to three times as many unique types of security issues from third parties than exist in their own infrastructure. There's clearly a contagion aspect to third-party cyber risk that organizations must recognize and manage accordingly.

If contagion risk is an issue in direct vendor relationships like those we study here, you can imagine that it becomes a much bigger issue with nth-tier indirect partnerships. Since such indirect relationships tend to be amorphous for many third-party risk management teams, we include Figure 14 to provide a concrete example.

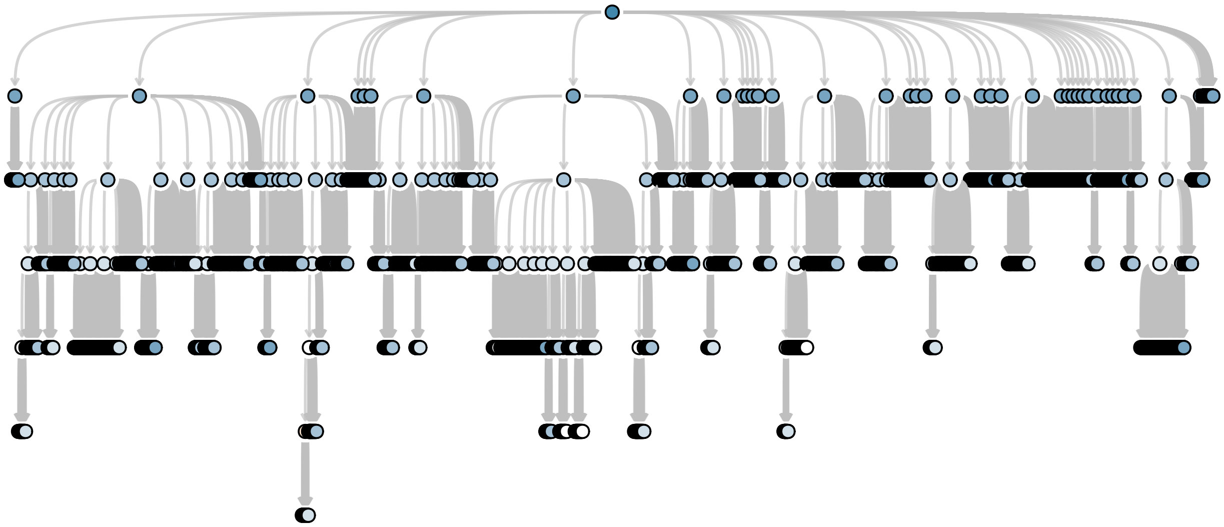


Figure 14: Example of multi-tier relationships for one organization

Figure 14 depicts the complex web of inter-relationships for a single organization. This report focuses exclusively on the first tier down (third parties). But it's clear there are many other parties in the mix, any of which potentially alters the balance of risk for those around them. We can't possibly dig into that topic at the end of this report…but we absolutely can—and will—do so in another. Until then, we hope this drives out those termites of assumptions from your third-party relationships.

Achieving the Perfect Balance

As illustrated throughout this report, the company (vendors) you keep or grant access into your organization's digital ecosystem can dramatically increase your risk exposure. How can you achieve a healthy balance between leveraging third-party provided technologies and tools to help fulfill your various business needs while still maintaining a secure cyber ecosystem?

Good risk management requires an accurate and complete understanding of your risk. Vendor attestation of security through annual questionnaires helps you understand the investments they have made to achieve good risk outcomes within a point-in-time, but that is only half of the information needed. Objective data helps you understand how well they implement and operate their program – this is the true benefit a real-time, continuous risk monitoring solution can provide.

Free Offer: Know Your Third Party Security Risk

As a busy third-party risk professional taking swift action with limited information is no easy feat. Fortunately, RiskRecon is offering complimentary enterprise access to assess and monitor the cybersecurity of your supply chain for 30 days.

For 30 days you can enjoy a detailed view of the risk up to 50 vendors pose to your organization. Plus, you'll learn how to use these scores to influence corrective action with risk prioritized data based on issue severity.

What's included in the offer?

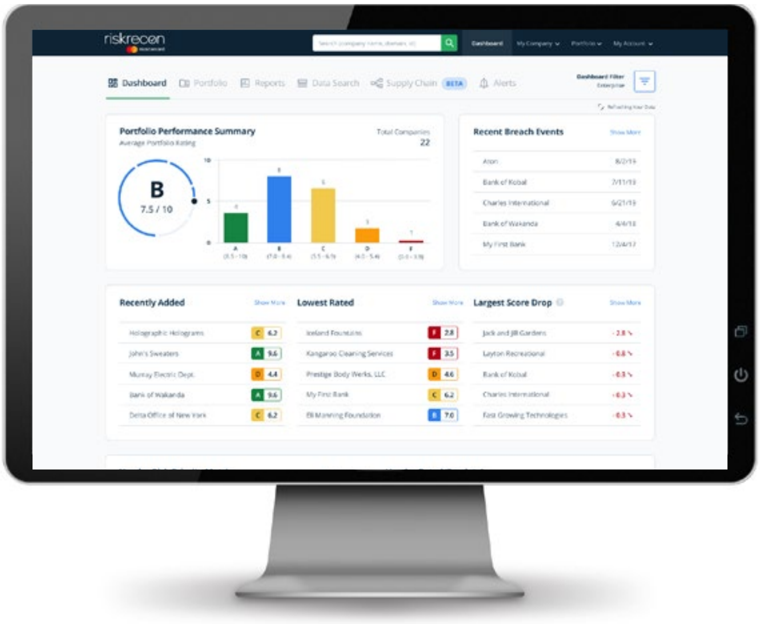
Detailed assessment of your own IT assets

Security ratings and summary assessment of up to 50 vendors

Full access to RiskRecon Technical Support

A risk-prioritized view into your vendor ecosystem with our vulnerability matrix

Superior data accuracy (over 99% - which drastically reduces false positives)



Recent Breach Events

Aton	8/2/19
Bank of Kobal	7/11/19
Charles International	6/21/19
Bank of Wakanda	4/4/18
My First Bank	12/4/17

Recently Added		Lowest Rated		Largest Score Drop	
Holographic Holograms	C 6.2	Iceland Fountains	F 2.8	Jack and Jill Gardens	-2.8
John's Sweaters	A 9.6	Kangaroo Cleaning Services	F 3.5	Layton Recreational	-0.8
Murray Electric Dept.	D 4.4	Prestige Body Werks, LLC	D 4.6	Bank of Kobal	-0.3
Bank of Wakanda	A 9.6	My First Bank	C 6.2	Charles International	-0.3
Delta Office of New York	C 6.2	Eli Manning Foundation	B 7.0	Fast Growing Technologies	-0.3

Register to get insights into your supply chain at: https://www.riskrecon.com/know-your-portfolio.

riskrecon

by

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

www.riskrecon.com

119 Cyentia INSTITUTE

The Cyentia Institute produces compelling, data-driven research with the aim of improving knowledge and practice in the cybersecurity industry.

www.cyentia.com