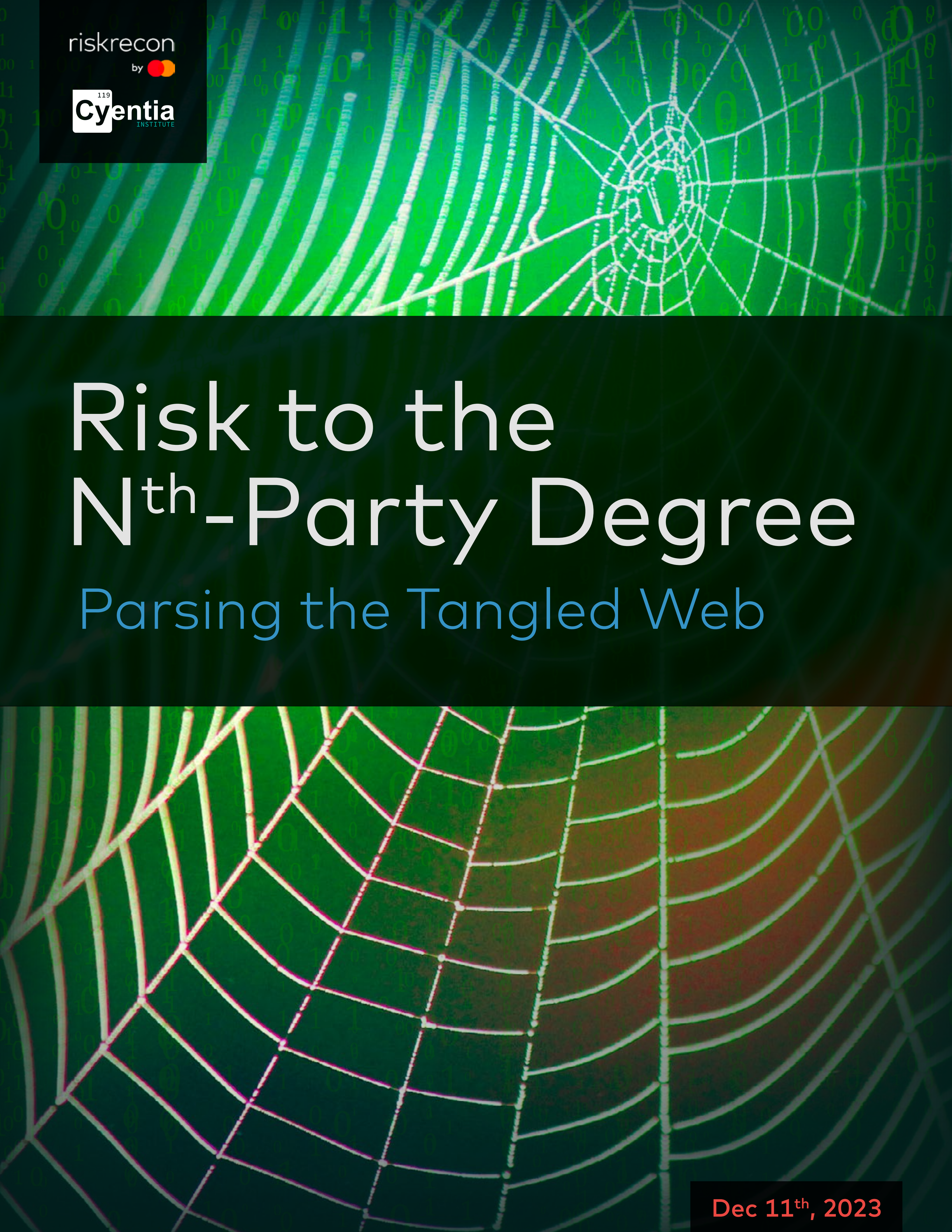
riskrecon by

Cyentia Institute



Risk to the Nth-Party Degree

Parsing the Tangled Web

Dec 11th, 2023

Introduction

> "The business of business is relationships" – Robin Sharma

Vendor risk is not just third-party risk: it's much more. Your business is complex, and relies on other businesses who in turn rely on still others. This branching network of dependencies means that your immediate business partners – your third parties – actually make up only a small portion of your business supply chain, and the risk it poses. In our last RiskRecon relationships report we dug into third-party risk and scratched the surface of fourth party, but we stopped short of exploring the whole web of relationships. This time we want to zoom out to see the whole tangled web.

What we have found is that while your third party relationships are closest and might prove the most tangible risks to your business, their business partners still pose a substantial threat to your enterprise, as well as the fourth parties' vendors (your fifth parties), their vendors (your sixth parties), and so on. While these orgs are at a larger degree of separation, you'll have less visibility into how they operate and the risks they pose. In vendor risk, as in life, it's the culprits you can't see who are most likely to cause you harm.

> Your business partners pose a substantial threat to your enterprise, as well as the 4th parties' vendors (your 5th parties), their vendors (your 6th parties), and so on.

How much harm?

Possibly, more than you think. The effects of an attack on a third, fourth, fifth, or higher party – commonly referred to as "nth party" – don't just ripple outward. They spread in multiple directions: inward, too, and upward, and sideways, usually affecting more than one organization at a time. Nth-party relationships aren't linear, but consist of numerous, multiple, repeating connections.

While we might think of them as a tree, with your company forming the trunk, your third-party partnerships the limbs, your fourth-party relationships the branches, et cetera, it's not that simple. Your third parties often rely on each other. A single 4th party is frequently relied upon by a large segment of your third parties. A business-to-business network can be highly interconnected. The result is an intricate network of relationships... and risk.

Suddenly, a single incident at a 4th party doesn't just affect one 3rd party you rely upon, but multiple. An outage at a 3rd party means many of your other 3rd parties might be affected. Nothing happens in isolation.

In this study, we'll try to unravel the implications of the complex network of interconnectedness. We'll examine where the bulk of your supply chain is (it's not third party), and how interconnected that supply chain is. We'll find that as your supply chain moves away from you, the businesses you deal with get more unlike your own, and more diverse. Then we'll dive directly into risk and show exactly how events might ripple out and affect your business, even when it seems like you should be insulated.

Key Findings

3RD PARTIES MAKE UP ONLY ABOUT **5% OF VENDOR RISKS.**

MOST BUSINESS RELATIONSHIPS **(75%) OCCUR AT THE 4TH- AND 5TH-PARTY LEVELS**.

3RD, 4TH, AND 5TH-PARTY ORGANIZATIONS TEND TO HAVE **HIGHER CYBERSECURITY POSTURE RATINGS**.

MORE THAN **80% OF ORGANIZATIONS HAVE RECURRENT 3RD-PARTY CONNECTIONS** – MEANING THAT THEIR 3RD PARTIES RELY ON OTHER 3RD PARTIES THAT THEY ALSO USE.

ON AVERAGE, **61% OF AN ORGANIZATION'S 4TH PARTIES** ARE RELIED ON BY MULTIPLE 3RD PARTIES.

21% OF 3RD PARTIES HAVE EXPERIENCED A SECURITY BREACH WITHIN THE LAST 3 YEARS.

87% OF ORGANIZATIONS' VENDOR RELATIONSHIPS **EXTEND TO THE 8TH PARTY**.

AS MANY AS **40% OF 3RD PARTIES ALL USE THE SAME OTHER 3RD PARTY**.

A BREACH AT THE 4TH-PARTY LEVEL TENDS TO AFFECT EVERY 3RD PARTY IN AN ORGANIZATION'S NETWORK – **AS MANY AS 10 TIMES** OVER 3 YEARS.

Can You Manage What You Can't See?

"Open your eyes. Look up to the skies, and see." – Queen

Understanding this complex web of risky relationships means decomposing our investigation into a number of parts. First we collected security assessments of more than 50,000 business-to-business relationships. Along with that data we collected information on the size and industry of those organizations as well as their security history. Then we dove right in and started to pick apart:

The size of an organization's relationships

How they connect and interconnect

The make-up of organizations' supply chains and different levels, including how the size and industry shift.

And how these factors coalesce to form a complex view of supply chain risk.

What we found was often alarming and sometimes counterintuitive – and always pointing back to this caveat: Effective risk management means vetting and monitoring not just your third-party risks but those associated with your business partners' business partners, and their partners, and so on, throughout the tangled nth-party web.

This is not a task for an individual, but having a partner equipped and ready to help you navigate these relationships (like RiskRecon) is key.

Quality risk management involves assessing and overseeing not only the risks posed by your third-party connections but also those linked to the business partners of your partners, and so forth, across the intricate web of nth-party relationships.

The Nearness of You:
Our Nth-Party Connections

> I know a guy, who knows a guy,
>
> who knows a guy, who knows a guy,
>
> who knows a guy, who knows… Kevin Bacon! – Weird Al Yankovic

The parlor game of "six degrees of separation from Kevin Bacon" goes like this: Name an actor and see if you can create a chain of films costaring successive actors until, eventually, one of those costars is Kevin Bacon. The goal is to find such a chain in less than 6 steps (or the minimum number of steps if you're ambitious). This game is based on the "small-world" concept popularized by Psychologist Stanley Milgram in the 1960s which found that personal connections were constructed in such a way that just about anyone could be reached in just a few steps. It turns out the phenomenon exists in your supply chain network, in particular the extent of your supply chain doesn't extend particularly far.

First a little bit of terminology because it can get a little confusing.

1ST PARTY	2ND PARTY	3RD PARTY	4TH PARTY	5TH PARTY	6TH PARTY
YOUR ORGANIZATION	CUSTOMERS	BUSINESSES THAT YOUR ORGANIZATION RELIES ON DIRECTLY	PARTIES ON WHICH YOUR 3RD PARTIES RELY	PARTIES ON WHICH YOUR 4TH PARTIES RELY	PARTIES ON WHICH YOUR 5TH PARTIES RELY

Throughout this report we'll use the term "first party" to refer to your organization. In common parlance, 2nd party is usually reserved for customers, and so won't enter into our vocabulary in this report. 3rd parties are those other businesses that your organization relies on directly. From here we proceed, sequentially: 4thparties are those that your 3rd parties rely upon, 5thparties are those that your 4thparties rely upon, and so on. This means 6 degrees of separation actually exists at your eighth party. So to answer how often supply chains actually extend that far, let's examine Figure 1.

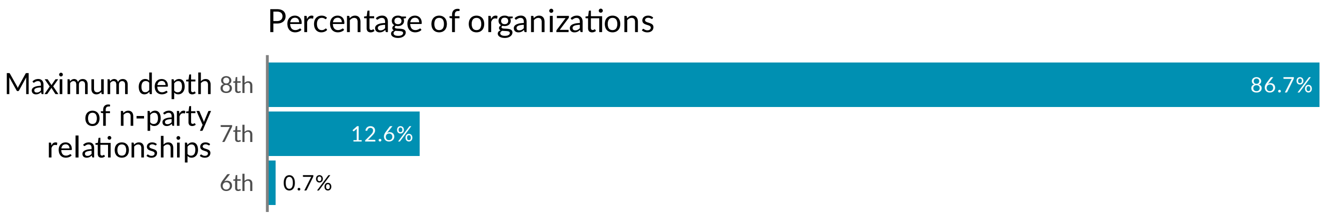


Figure 1 Maximum depth of an organization's supply chain in our data

Two things are interesting here. First, a large majority of organizations' supply chains do extend out to that maximum 8thparty (6 hops) of separation, but none of the orgs in our study go beyond that. Another interesting thing we see is that very few organizations' (13.3%) supply chains have shorter reach than that. Why this clustering around 6 degrees of separation? To answer that question we'll look at the size of an organization's supply chain at each distance in Figure 2.

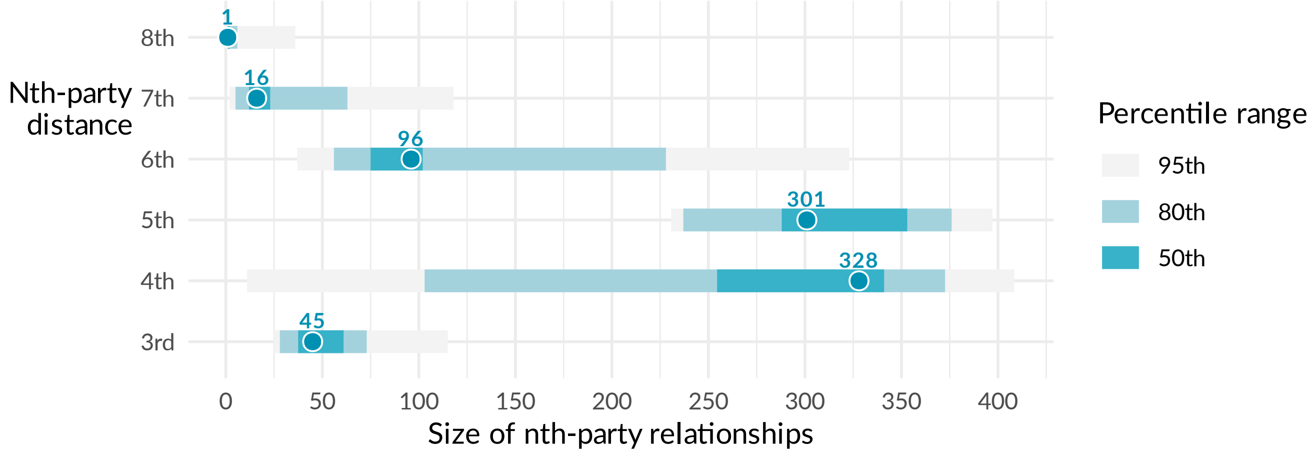


Figure 2 Number of partnerships at each level of an organization's supply chain. The dot in the middle is the median value with each filled rectangle representing the different range of values.

What's striking here is that we see the bulk of business relationships exist at the 4th and 5th party level. So while the median of 45 organizations you have direct contact with may pose the most immediate risk as far as impact, they are dwarfed by the nearly 14x more organizations that comprise your 4th and 5th parties. We can examine this on a percentage basis as well in Figure 3, and see the same result, but one in which it's easier to draw conclusions.

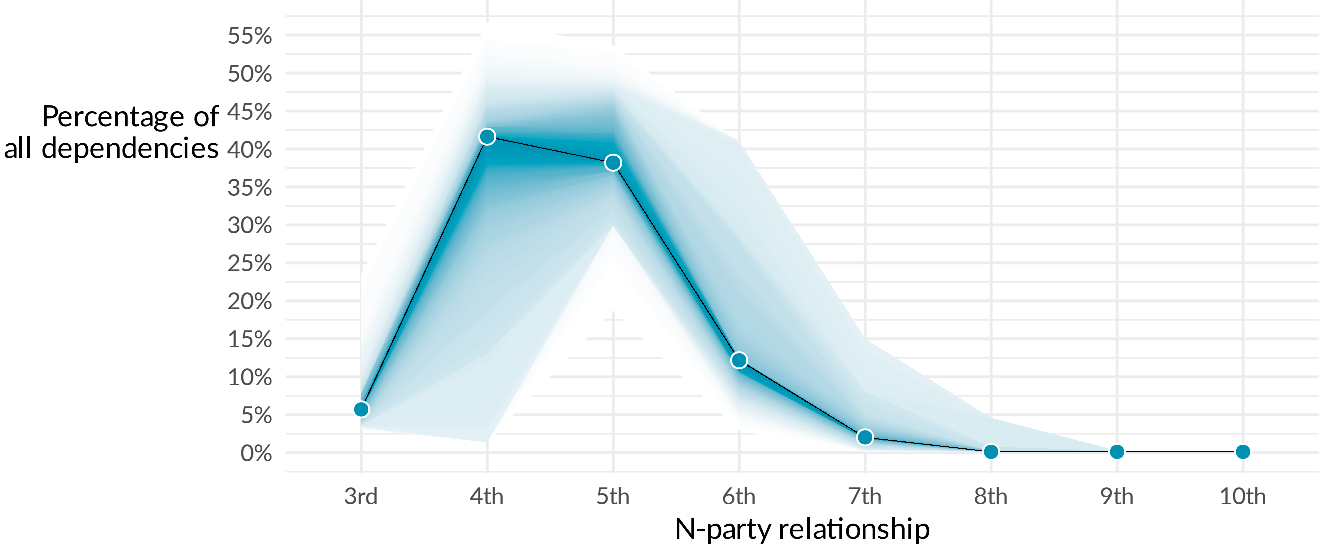


Figure 3 Percentage of supply chain at each level. Dots and lines represent the median value with the shading representing the relative density among organizations

In particular we see that for most organizations 40% of their supply chain is in their 4th party relationships with another ~40% in their 5th party relationships. The rapid dropoff starting at the 6th party level we saw in Figure 2 is mirrored here.

We also see the answer to the mystery raised in Figure 1, that is that the size of the network declines precipitously starting at the 6th party. Indeed, it's only a little more than a dozen firms typically at the 7th party level and most organizations only have a handful of 8th party relationships. So while most organization's networks expand out to that 8th party, that circle is incredibly small.

The takeaway: If you're managing your third-party-vendor risk (something many companies struggle with) but neglecting your fourth parties and beyond, you're barely scratching the topsoil of your threat landscape. 80% of most organizations' supply chain is located within the 4th and 5th party relationships.

Understanding nth-party connections and risk

"What you don't know sure can hurt you." – Twisted Sister

Before we move forward to try and understand exactly what types of organizations exist at each level of the supply chain and the risk they pose, it's useful to move from the summaries we've presented above to an illustrative example. To that end we imagine a theoretical organization with a nice round supply chain composed of 1,000 different suppliers. This is a convenient number because then each organization makes up exactly 0.1% of an organization's supply chain. Given the numbers we saw in Figure 2 this is a little on the high side of "median" for a supply chain.

This theoretical organization will serve as a foil as our analysis unfolds, and give us a better idea of how nth-party risk might affect the "typical" organization. We visualize this organization in Figure 4.

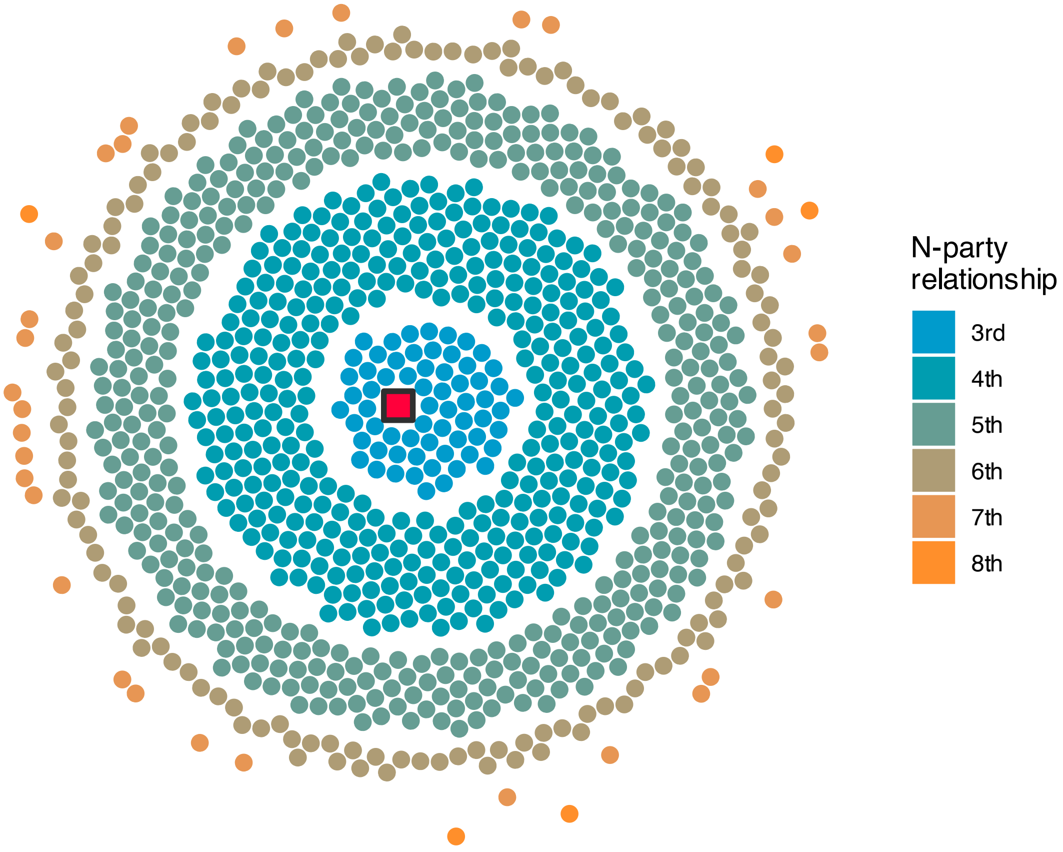


Figure 4 An example organization's supply chain.

Each dot in figure 4 represents a single node in our example organization's supply chain with the square in the middle the "1st party" – the organization itself. In Figure 4, all the dots are the same size and are colored simply by their distance from the 1st party, but as we explore further this example organization will evolve and we can uncover layers of complexity we hadn't seen before.

Recurrent Connections:
Doubling Down on Risk

"I'm my own grandpa" – Willie Nelson

Why does the number of dots in our chart decline so rapidly as they branch out from the primary organization? Third parties tend to be connected to each other. The answer is somewhat simple, many of your third parties rely on each other. What human-resources software do you use? Your other third parties may use it, too. Or perhaps a video-conferencing solution that your business partner uses – one that you don't use – also gets used by that company's third parties – your fourth parties – as well as by some of your third parties.

Recurring connections like these happen quite often, making nth-party networks quite dense, especially at the third, fourth, and fifth-party tiers. Enterprises connect again and again. Your third party may be your fourth or fifth party's third party, too, and vice-versa. Every connection and reconnection represents another risk to your organization. If, in the course of all these connections, a business whose services you use is digitally connected several times to other businesses, the jeopardy could double, triple, quadruple, or more. This can mean incidents or outages at one 3rd or 4th party can affect multiple others. To what extent this is the case we start to examine in Figure 5.

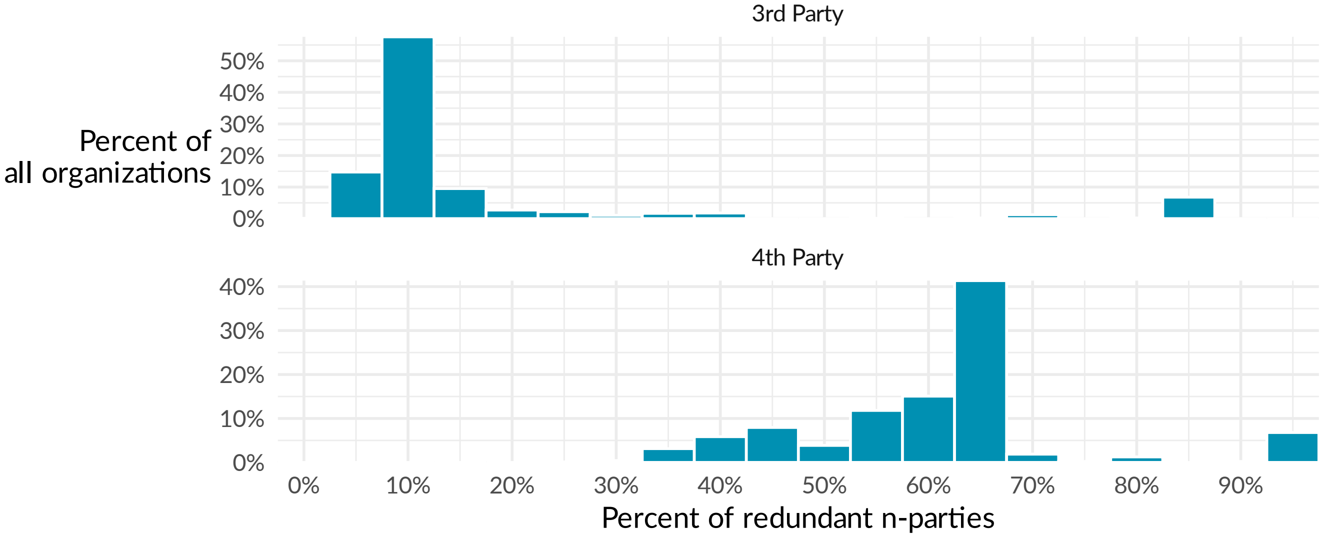


Figure 5 Percentage of an organization's 3rd and 4th party relationships that have relationships with other 3rd parties.

Some organizations have upwards of 80%+ of their 3rd parties having connections among themselves

Figure 5 indicates that for most organizations there are some (but not staggering) recurring relationships among an organization's 3rd parties. That is, typically among those 3rd parties 18% will be relied upon by other 3rd parties. There are some outliers however, with some organizations (around 5%) having upwards of 80% of or more of their 3rd parties having connections among themselves. However, when we move to 4th parties things get a little bit more dense.

On average, 61% of an organization's fourth parties are relied on by multiple third parties. This means an incident at one of those 4th parties is likely to affect multiple 3rd parties. This of course raises the question, exactly how many? To find the answer, we've isolated the interdependent nth parties from those that have no interconnections to see just how often these connections recur. How many companies in the network are using the same product or service providers and examined the distribution in Figure 6.

Interdependence is a fact, it's not an opinion. – Peter Coyote

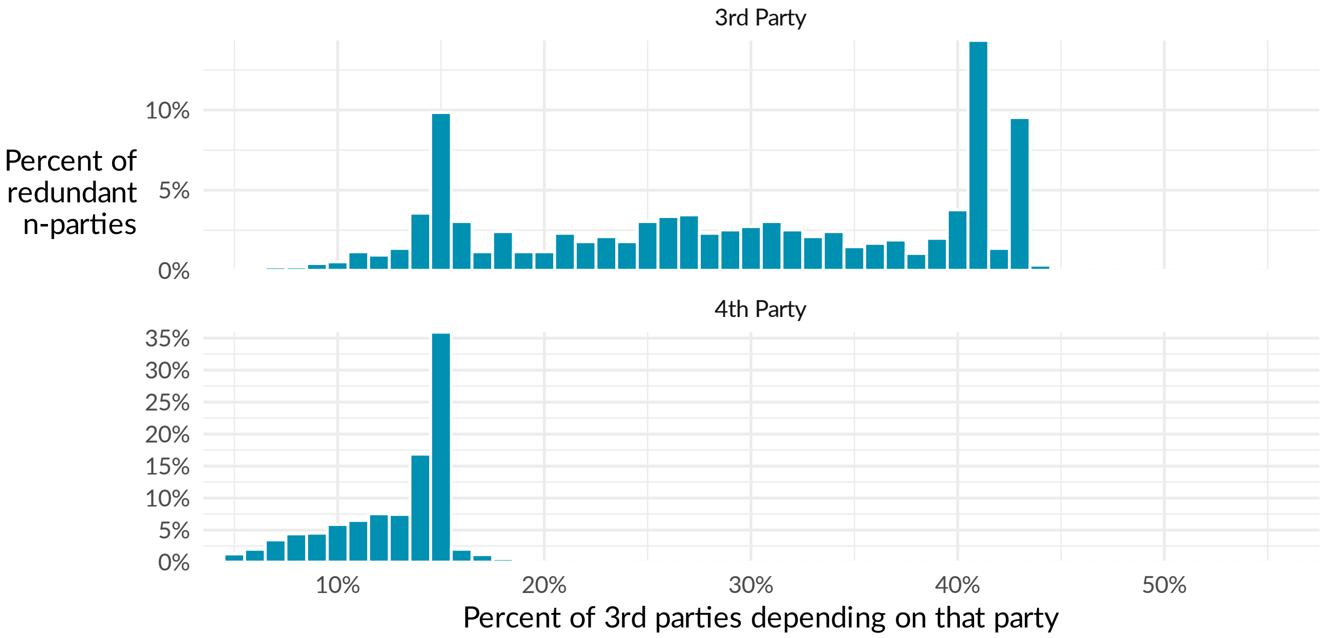


Figure 6 Degree of interdependence of recurring 3rd and 4th parties.

When a third party is relied on by multiple other 3rd parties, it is typically relied upon by nearly one-third – 29% – of those interconnected parties. Sometimes, as many as 40% of these third parties will all use the same other third party! If something goes wrong at that oft-used company, nearly half your business partners – and your company – could also suffer. The risk is less concentrated but more dispersed at the fourth-party level. When a fourth party is relied on by multiple third parties, typically it's used by 12.8% of them. But as we've seen, more fourth parties are frequented multiple times than are third parties.

The balance here is interesting and not necessarily a foregone conclusion. Third parties are less likely to be relied upon by other 3rd parties, but when they are, that reliance usually makes up a large percentage of your 3rd parties. This is likely due to the direct reliance on service providers or financial institutions. These big suppliers are likely to be relied upon by just about everyone making the extent of their connectivity vast. Let's look at what this means for our example organization in Figure 7.

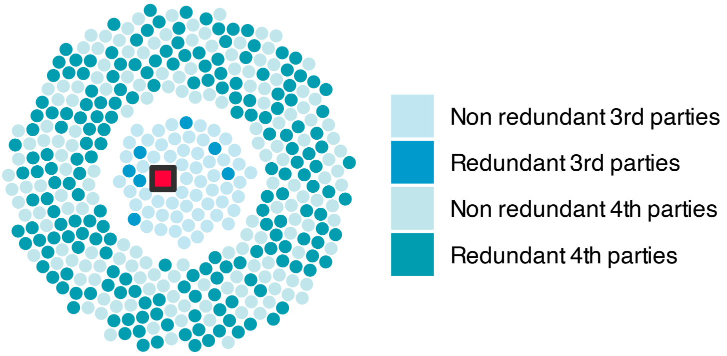


Figure 7 Example organization with redundant connections.

An attack or disruption at a single third or fourth party is likely to affect more than just your organization.

The orange square in the center is, again, our example org. The dots closest to it are all its third-party partners and those in the outer ring are its fourth parties.

The dark dots represent third or fourth parties that other third parties also use. As you can see, the number of third parties with multiple connections in the network is somewhat small but not insignificant. And it's very common for fourth-party organizations to be affiliated with more than one of your third-party partners.

To show the extent of that reliance, we've selected a single "sample partner" and colored it orange in the graph.

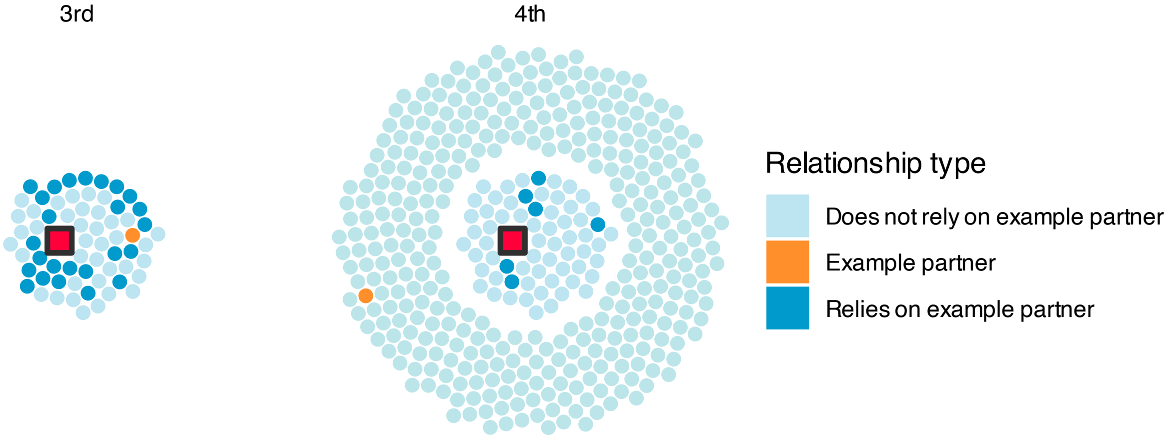


Figure 8 The extent of redundant connections for a single (orange) 3rd party (left) or 4th party (right).

If the sample partner is a third-party business partner of yours, it will more likely have connections with other third parties. If it's a fourth party, other third parties will still rely on it, but not as many. Nevertheless, an attack or disruption at a single third or fourth party is likely to affect more than just your organization.

Vive la Différence:
Nth-Party Risk by Sector and Size

Different strokes for different folks. – American proverb

No two companies are alike, but some are more different than others. Companies may find it more difficult to manage the risks associated with nth-party partners in a different industry, or of a different size, than their own organization. Risk managers at very large, mature enterprises, where processes including cybersecurity are spelled out in detail and meticulously followed, may find it challenging to understand and assess how a smaller, more ad-hoc, entity in a different sector approaches security. The risks would likely differ, as well.

In this section we'll examine how the distribution of different organizational types, particularly size and industry, varies as we move within the web of relationships within a supply chain. Figure 9 is a "worm chart" or "subway chart" where you can see that professional services and finance top the list of first-party organizations – those that rely on other companies to get work done.

The financial sector is particularly pronounced in 3rd and 4th-party relationships, suggesting that redundant connections are primarily constituted by these significant, large scale, financial institutions.

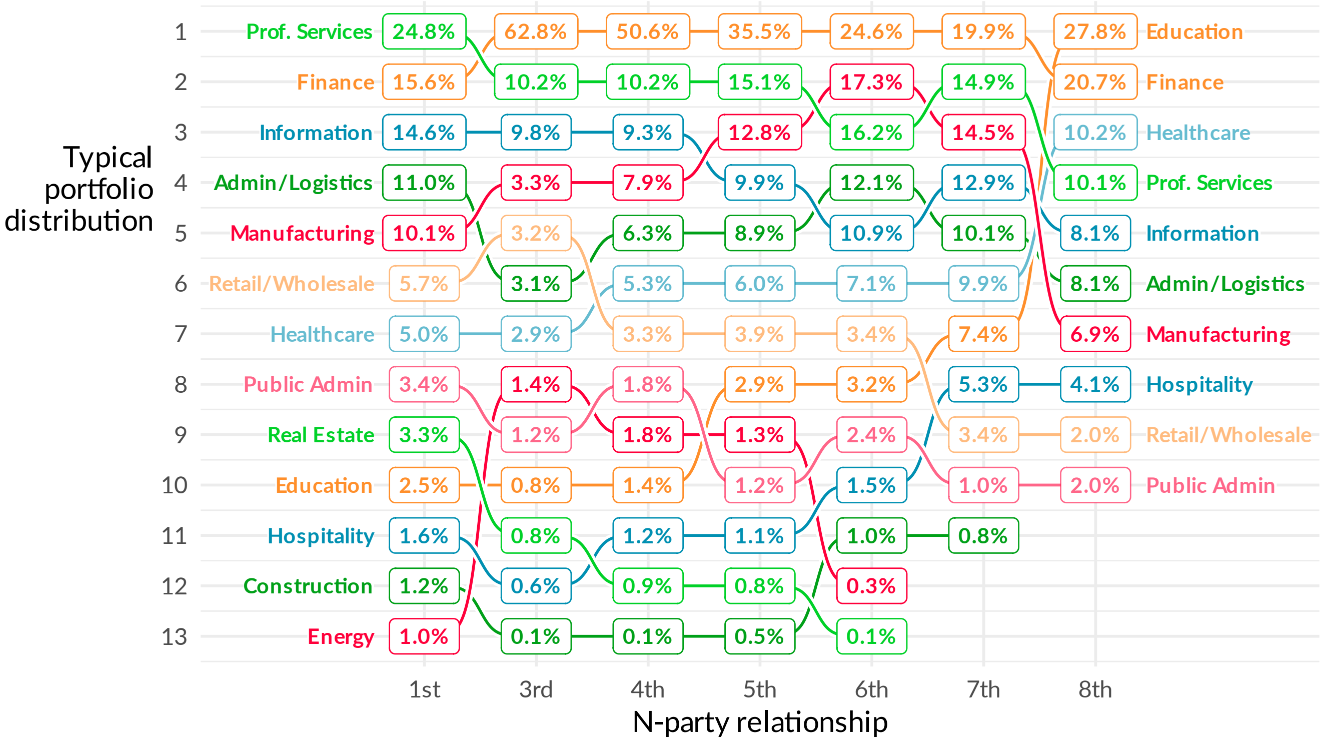


Figure 9 Typical distribution of different industries across an organizational supply chain.

In the third-party position, though, professional services drop to second. What dominates? Finance, which holds the top spot all the way through until the eighth party, when education finally takes the spotlight. This makes sense. Every kind of enterprise needs financial services, and everyone watches their bank's risk. Money makes the world go 'round, right?

Perhaps most striking here is the extent to which finance dominates 3rd and 4thparty relationships. Given that these institutions tend to be large, it appears that the redundant connections we saw above are in large part made up of those financial institutions.

> When one tugs at a single thing in nature, he finds it attached to the rest of the world – John Muir

To see this sector diversity in living color, here's our dot chart showing a typical organization's risk-management portfolio. Green – money-green finance – really dominates in the first couple of tiers, but other colors – gray-blue professional services, yellow information, dark blue administration and logistics – take up more space in the fifth-party tier and beyond.

Business risks tend to rise with every nth-party's difference from your own organization.

The typical nth-party risk portfolio contains a kaleidoscope of industries. Why does this matter? Business risks tend to rise with every nth-party's difference from your own organization. Those in other sectors – and of other sizes – may have business models, goals, and ways of operating that are unfamiliar to you, making managing the risks associated with them more challenging.

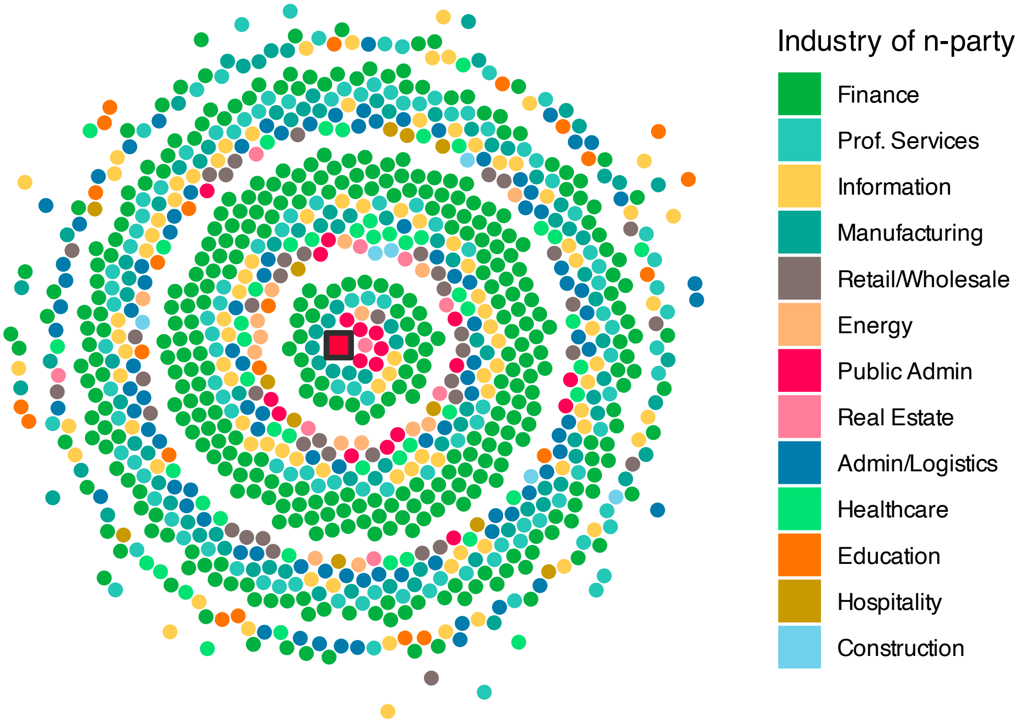
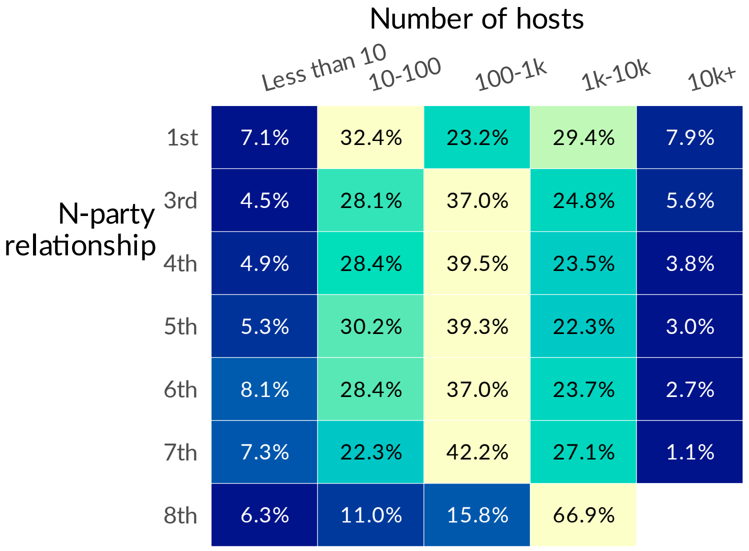


Figure 10 The typical distribution of industries for our example organization.

Trying Nth Parties on for Size

Industry is not the only way that we can examine how organizations are distributed about the supply chain. Do organizations rely on larger or smaller partners and at what level? Figure 11 has the answer.

This chart groups n-parties according to the number of hosts, or computers, their enterprise has. Most organizations in our study fell into the middle range, having between 100 and 1,000 hosts at every level except the eighth party. Larger enterprises with between 1,000 and 10,000 hosts were most likely to have an eighth-party relationship; very large businesses were an eighth party to none, recalling that that 8thparty circle is exceedingly small.

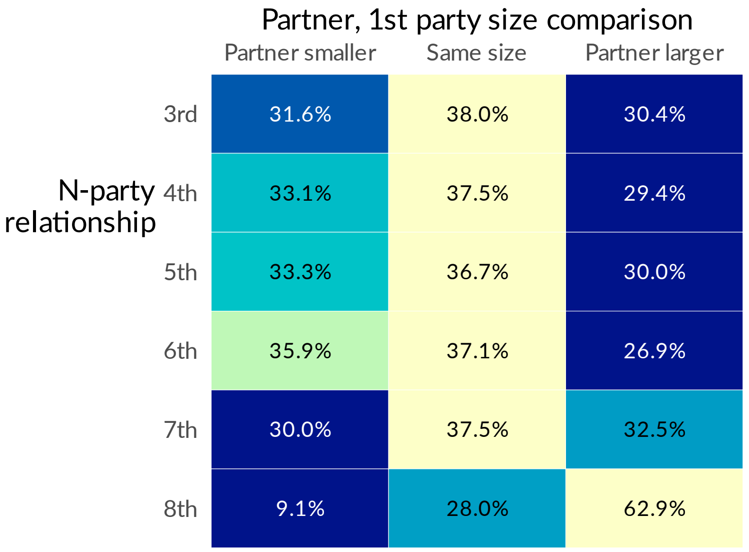


N-party relationship	Less than 10	10-100	100-1k	1k-10k	10k+
1st	7.1%	32.4%	23.2%	29.4%	7.9%
3rd	4.5%	28.1%	37.0%	24.8%	5.6%
4th	4.9%	28.4%	39.5%	23.5%	3.8%
5th	5.3%	30.2%	39.3%	22.3%	3.0%
6th	8.1%	28.4%	37.0%	23.7%	2.7%
7th	7.3%	22.3%	42.2%	27.1%	1.1%
8th	6.3%	11.0%	15.8%	66.9%	

Figure 11 Distribution of the size of partner organizations at each level of the supply chain.

But this only tells part of the story, what may be more instructive is whether the organizations in your supply chain are bigger or smaller than your own. This can have implications for the way they handle their security operations with larger organizations potentially being bigger targets but more equipped to handle attacks, Figure 12 makes the size comparison level by level.

We see here that at nearly every level, third-party to seventh, companies are somewhat more likely to monitor the risks of partnerships with businesses that are their own size.



N-party relationship	Partner smaller	Same size	Partner larger
3rd	31.6%	38.0%	30.4%
4th	33.1%	37.5%	29.4%
5th	33.3%	36.7%	30.0%
6th	35.9%	37.1%	26.9%
7th	30.0%	37.5%	32.5%
8th	9.1%	28.0%	62.9%

Figure 12 Size comparison of organizations at different levels of the supply chain.

This finding is seemingly at odds with the observations that financial organizations (who we expect might be large banks) are at the top of the 3rd and 4thparty lists by a longshot. Perhaps this is evidence that mid-sized organizations may like to partner with mid-sized financial institutions, trying to tailor their supply chain to organizations that look like themselves.

Mid-sized organizations may like to partner with mid-sized financial institutions, this tailors their supply chain to organizations resembling themselves.

Finally, let's take a look at how this size distribution is realized in our example organization. Given that size is a natural fit for the now familiar circle of circles, we can scale each organizational partner by that typical size distribution in Figure 13.

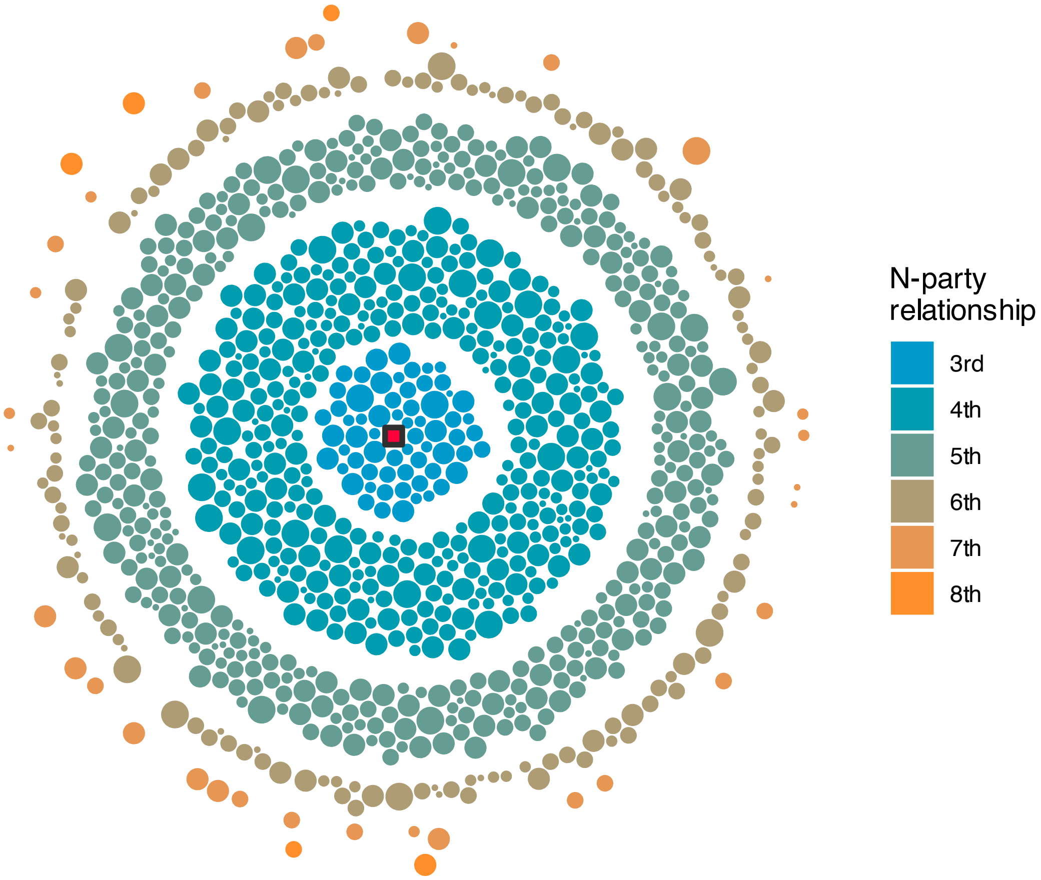


Figure 13 Example organization with supply chain partners scaled by typical size.

Diversity, Reconsidered

In the previous section we hypothesized that organizations are seeking out other organizations that are similar in size to partner with. A motivation may be that those partnerships are easier because organizations of similar size are going to have similar operational procedures, leading to a mutual understanding of day to day operations. It's worth considering how "different" the zoo of organizations at each level of the supply chain is at different levels.

To do this we borrow a quantity from ecology, namely "ecological diversity". This measures the diversity of an ecosystem by both the variety of species and their relative prevalence. Here an analogous "species" is a particular industry and organizational size combination. In ecology, having many species indicates that an ecosystem is in good health. More diverse natural ecosystems have more complex webs of dependencies, such as the food chain (which isn't really a chain at all, but more complex). These ecosystems can be both more fragile and more robust.

In cybersecurity, though, more diversity can equal greater risk. A diverse security ecosystem may mean that you're managing risks associated with organizations having a structure much different from yours. We examine diversity in Figure 14, below and will get back to how it relates to risk in the next section.

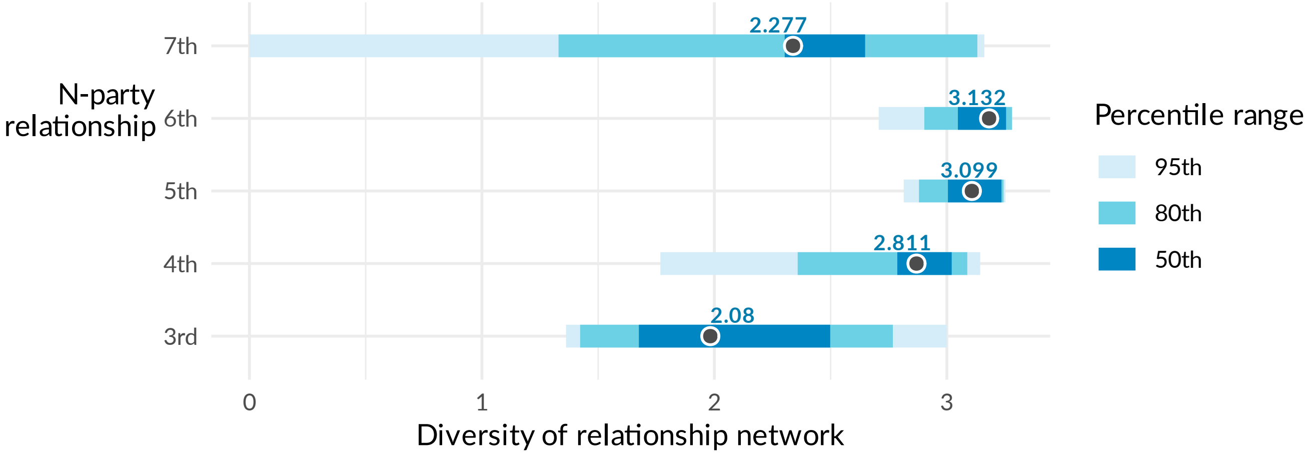


Figure 14 Diversity at different levels of the supply chain network.

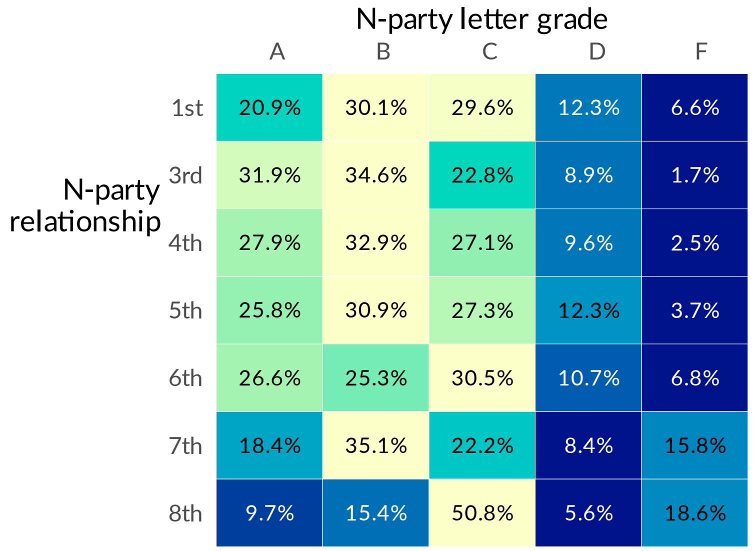
This chart shows diversity measurements based on both industry and size. We see the greatest diversity among organizations at the fifth- and sixth- party levels. Here's where you're most likely to be dealing with partners who operate well outside your expertise – which could raise your risk of breach exposure. Because organizations are trying to maintain supply chains similar to themselves it makes sense that the 3rd party has the lowest diversity, but as the rest of your supply chain decisions slip from your control things are going to become much different the further out you get. At 5thand 6thparty your supply chain likely covers just about every industry and organizational size.

Nth-Party Risk to the Letter

Now that we've examined the size and shape of the supply chain as it spreads outwards through webs of connections, we can finally examine the risk associated with those organizations caught in the web. We do this in two ways, first by examining the letter grade of these organizations and then their breach history.

A Web of Risk

Which nth-parties make the grade? In Figure 15, we find that third-, fourth-, and fifth-party organizations tend to have higher cybersecurity posture ratings – more As and Bs, in particular – than others. We also saw the most B ratings among seventh parties. And more than half of eighth-party organizations – which, remember, tend to be larger than their first-party partners – merit only a "C" grade.



N-party letter grade

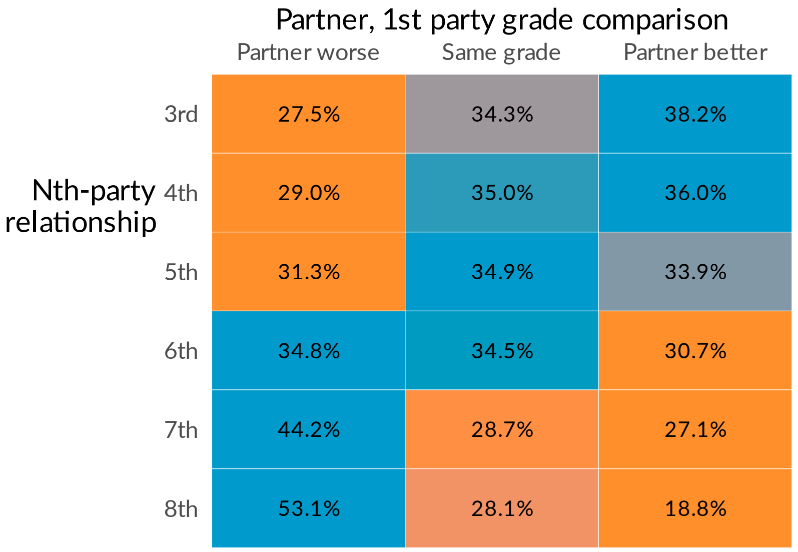
N-party relationship	A	B	C	D	F
1st	20.9%	30.1%	29.6%	12.3%	6.6%
3rd	31.9%	34.6%	22.8%	8.9%	1.7%
4th	27.9%	32.9%	27.1%	9.6%	2.5%
5th	25.8%	30.9%	27.3%	12.3%	3.7%
6th	26.6%	25.3%	30.5%	10.7%	6.8%
7th	18.4%	35.1%	22.2%	8.4%	15.8%
8th	9.7%	15.4%	50.8%	5.6%	18.6%

Figure 15 Letter grade distribution within the supply chain.

The poorest performers are also, generally, the farthest removed. The lion's share of Ds and Fs will most likely occur among seventh and eighth parties – again, predominantly larger entities than your own. Bigger doesn't always mean better, or more secure.

Neither does an "A" score necessarily spell perfection. Every company has vulnerabilities as well as cybercriminals working to find and exploit them. But a company's cyber risk rating can serve as an indicator of how secure it is, or isn't, with possible ramifications for all its nth-party partners.

Similar to how we examined size, and something we did in the previous 3rd party risk report, it's worth asking whether organizations' letter grades are higher or lower than those that rely on them? We looked at the propensity of companies to do business with parties with higher cyber-posture ratings than, the same as, or worse than their own in Figure 16.



Partner, 1st party grade comparison

Nth-party relationship	Partner worse	Same grade	Partner better
3rd	27.5%	34.3%	38.2%
4th	29.0%	35.0%	36.0%
5th	31.3%	34.9%	33.9%
6th	34.8%	34.5%	30.7%
7th	44.2%	28.7%	27.1%
8th	53.1%	28.1%	18.8%

Figure 16 Letter grade comparison across supply chain.

Risk rankings at the 7th and 8th-party tiers tends to be **worse** than that of the primary organization.

Interestingly, the distribution is fairly even until we reach the seventh- and eighth-party tiers. There, the risk ranking tends to be worse than that of the primary enterprise.

This trend first emerges at the sixth-party level, and worsens as we look outward – an indication that organizations pay less and less attention as their nth-parties become more and more further removed. These organizations at higher remove are likely to pose more of a risk than those closer, certainly better than the opposite.

Let's take a look at the distribution of cyber-risk ratings according to size in our example company's portfolio in Figure 17.

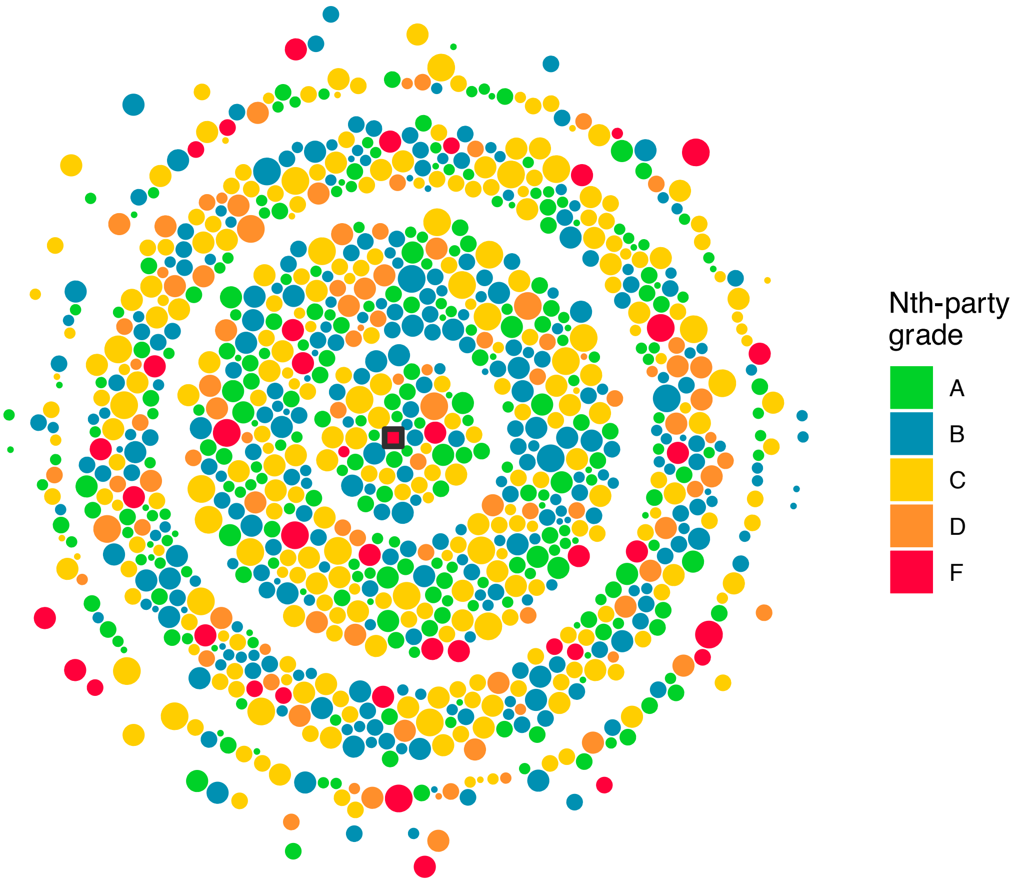


Figure 17 Example organization with the size of organizations and a typical distribution of letter grades.

Here you can really see in vivid color who makes the grade and who doesn't among our example company's nth-party business partners. Among the organizations closest to the example company, we see only one tiny red dot: just one small entity with an F rating. We also see only a few Ds. This is really a reflection of the distributions we see above, but the visualization here is powerful in that it lets us really see where the concentration of reds and oranges in the outer ring lies.

The Likelihood of N^{th}-Party Breaches

Breach Risk Along theN^{th}-Party Spectrum

Just as an "A" risk score doesn't necessarily equate to "no risk," however, neither does an "F" automatically mean a breach is impending. The proof is in the digital pudding: we can best see indicators of breach risk by looking at actual breaches.

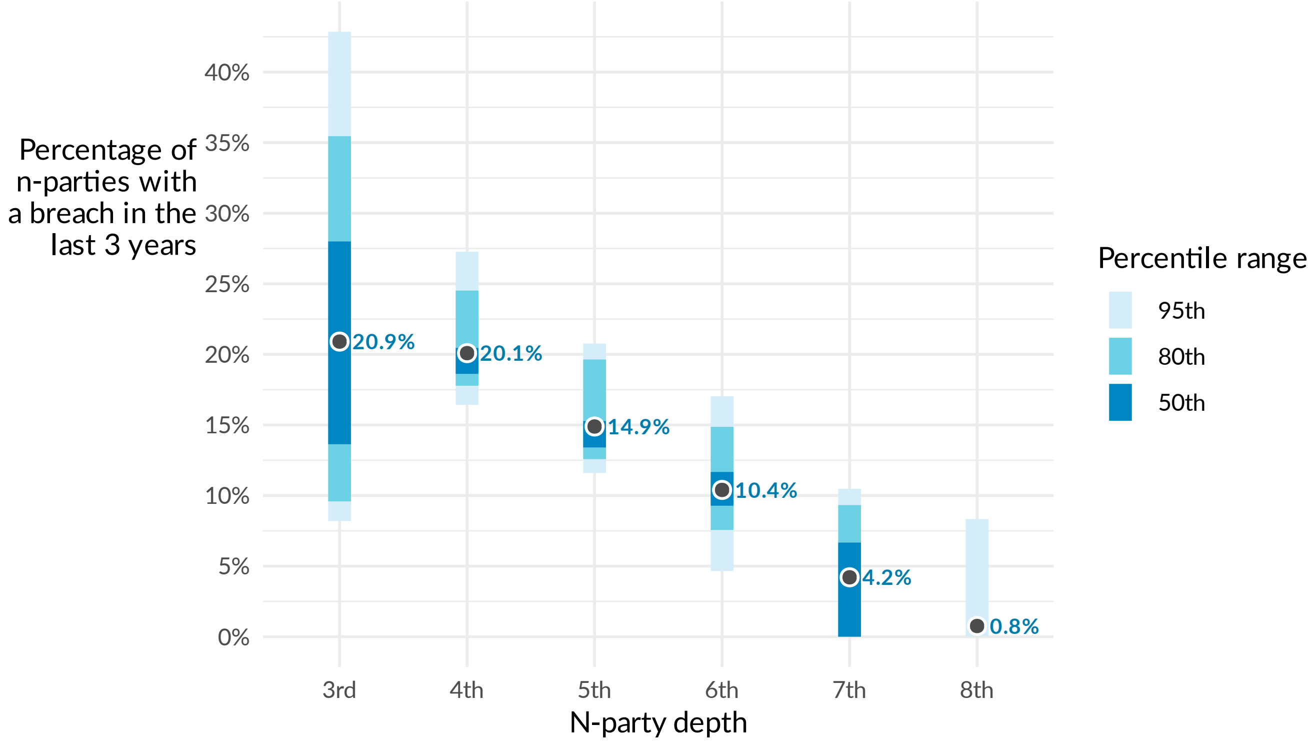


Figure 18 Breach probability among organizations at each level of the supply chain.

In the chart above, we see that more third and fourth parties have suffered a breach in recent years – about one-fifth of them – than those at subsequent levels of connection to the organizations in our study. The number of breaches dwindles to almost zero at the eighth-party level, where our sample gets smaller.

The discrepancy between risk score and breach history may be due to a lag in reporting. Or, as we've said, a high score doesn't always mean "breach safe." And some that have had breaches in the past may have improved their security in the time since, lifting their grades. By the same token, poorly-rated companies may have warded off or avoided attacks, or perhaps they've simply been lucky.

The occurrence of incidents within an organization's supply chain can exhibit an **unpredictable complexity that is not necessarily determined by size or industry.**

In Figure 19, we once again examine how these breaches might be distributed to our example organization. This shows, in stark relief, that incidents can be spread throughout an organization's supply chain in a way that is complex, and not necessarily predictable based on size (or industry). Next we'll examine how diversity relates to this breach likelihood and finish with how the effect of those ominous red dots might propagate throughout the supply chain network

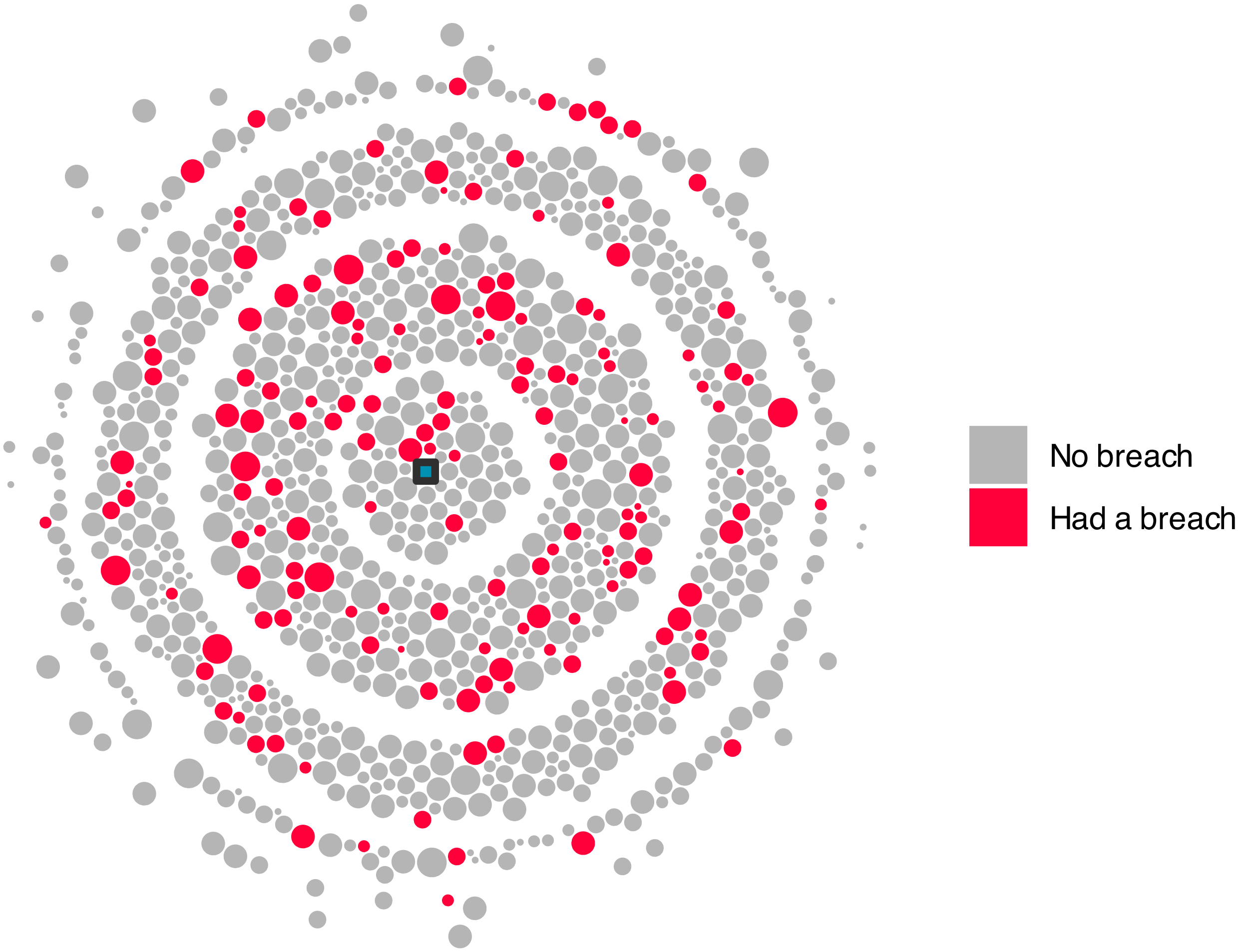


Figure 19 A hypothetical number of breaches for our example organization.

Diversity and Breach Risk

Having established that there is a wide variety of diversity among organizations at several levels of the supply chain, and that breach probability varies at each level of the supply chain it's worth asking whether there is a correlation between the two. In particular, are organizations whose supply chain is more diverse also more likely to have breaches in any particular level in that supply chain. The scatter plot in Figure 20 investigates.

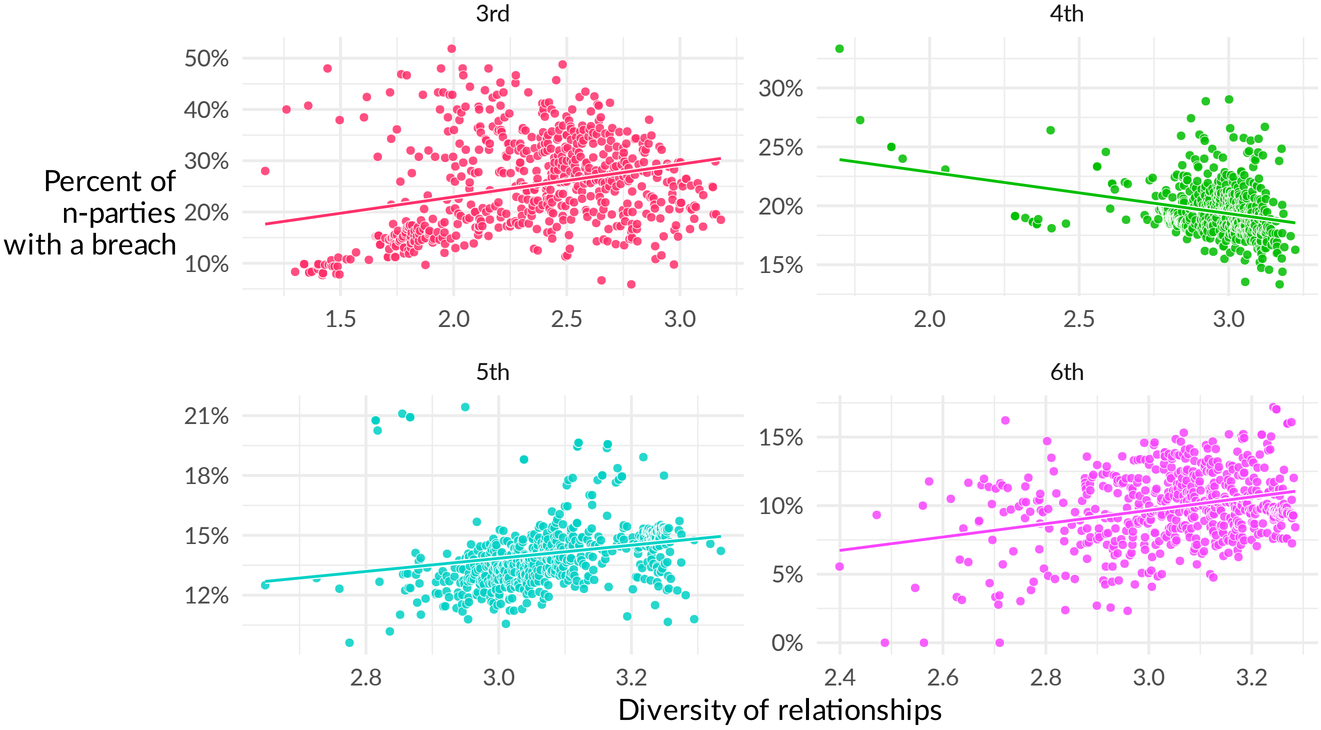


Figure 20 Diversity and breach probability at different levels of the organizational supply chain. Each point is an organization, with the diversity (based on size and industry) at that level of the supply chain on the horizontal axis, with the vertical axis the percentage of organizations in that level that have had a breach.

> Increased supply chain diversity correlates with **higher breach percentages in 3rd, 5th, and 6th party relationships**, except for a negative correlation in 4th party relationships.

What we can see is that for 3rd, 5th and 6th party relationships an increase in diversity in the supply chain results in a higher percentage of organizations with a breach. This trend is bucked with the 4th party where the correlation is negative. The result for the 3rd party is interesting, noting that there is likely a tension between organizations looking for secure partners, but also looking for those that are similar to themselves.

Going Viral:

How Nth-Party Breaches Spread

As we've seen, a company's third parties often rely on one another to a large extent. A breach at one of these companies would seem likely to affect the others.

In fact, that's just what we saw. A fourth-party breach is more likely to affect multiple third parties, but that multiplicity tends to be lower. Let's see how this might play out in our example organization.

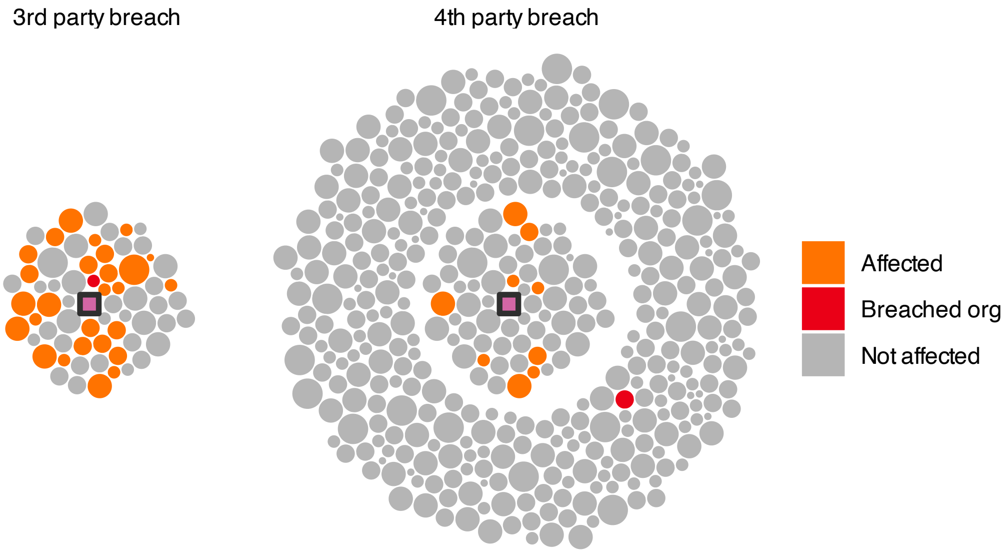


Figure 21 Breach spreading among 3rd and 4thparties.

In Figure 21, we examine a breach at a third party (left) and 4thparty (right) marked in red. Then, using data we calculated, we simulate a scenario where other 3rd or 4thparties might be affected. As can be seen a breach at a single 3rd party can affect a wide swath of other 3rd parties, potentially making for a wider ranging impact than just the one obvious relationship. The extent is lower on the right with the single 4thparty only affecting 9 of the third parties.

A 4th-party breach is more likely to affect multiple 3rd parties, but that multiplicity tends to be lower.

There is not just one single breach that spreads but many, with little escape for the cascade of parties.

But Figure 19 indicated that there is not just one single breach that spreads but many. If we fill in all the breaches we simulated in Figure 19 things get worse. In Figure 22, we mark orgs that have been breached in red, and the number of times they are affected by a breach in an increasingly alarming gradient of colors, with the light purple square is our example organization

"We are like islands in the sea, separate on the surface but connected in the deep." – William James

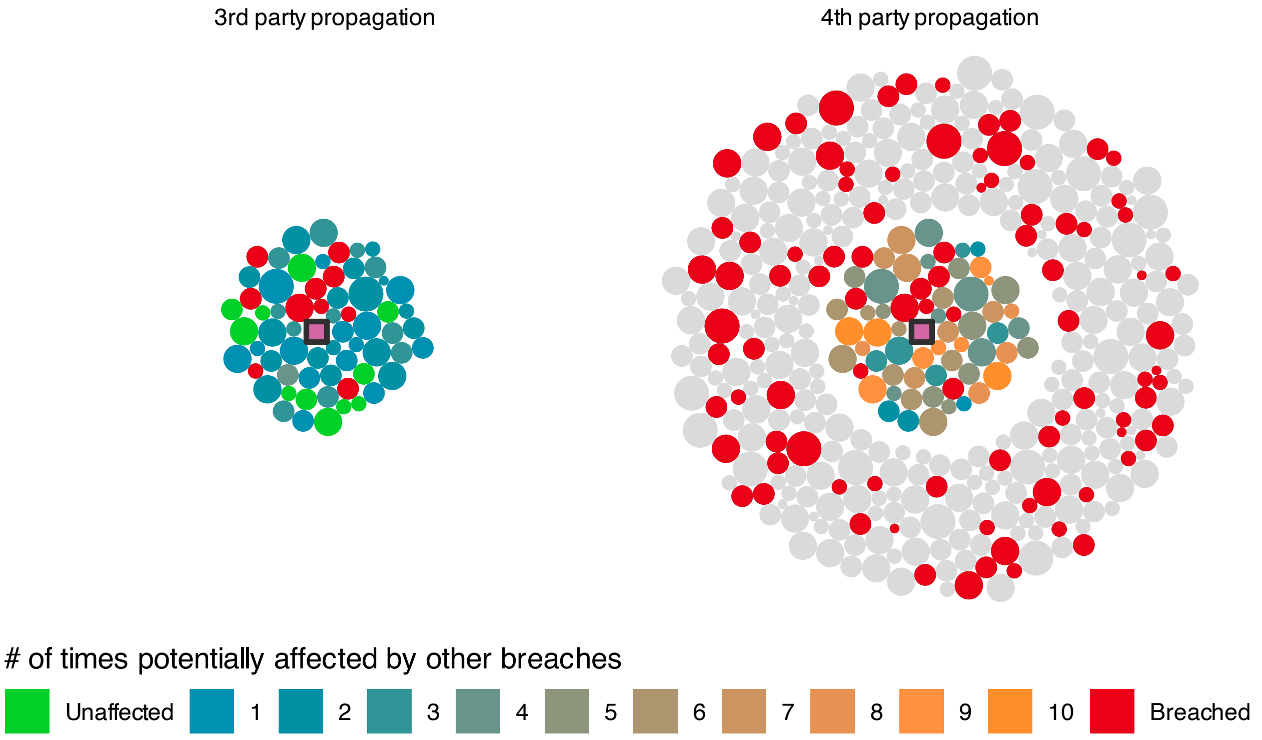


Figure 22 Multiple breach occurrences among 3rd and 4th parties.

The impact is stark, among 3rd parties only a handful are able to escape being affected by another 3rd party breach. For 4thparty breaches, there is no such escape. Every org is connected to numerous 4thparties that experience a breach, with some occurring up to 10 times. Certainly this interconnectedness, makes for a nearly inescapable likelihood of a breach

Conclusion

As we've seen throughout this report, your supply chain is a complex beast. It's not just a tree that spans outward with organizations further and further removed from your purview, but a complicated web of relationships. While no one is ever that far removed (only at most 6 degrees of separation, that web grows to vast proportions, typically multiple hundreds of organizations for 4th and 5th parties.

As that web grows, you are likely to see organizations that are both similar to and highly different from your own, possibly making their security practices somewhat alien to your own. Organizations will seek out similar partners and their closest partners will likely have higher security ratings than themselves. This isn't a guarantee of security, especially because as one gets to a 5th and 6th party things switch with organizations tending to have lower ratings.

Along with the lower ratings at the 5th and 6th party, comes higher likelihood of breaches. With diversity generally increasing the likelihood of an organization having a breach among your partners. One in which an incident at a single partner, can ripple outward to numerous others. In fact, it's highly unlikely that any of your partners have either not had a breach or not had a relationship with someone who had a breach.

What does this all mean for you? Supply chain risk management is not just about knowing who you depend on, but also knowing who they depend on. It's about building a picture of the web of dependencies and knowing where those critical spots in the web might be where incidents could ripple out. Doing this on your own is difficult, but partnering with a risk management partner who can make sense of this web at scale is critical.

This is where partnering with a specialized risk management solution, such as RiskRecon by Mastercard becomes indispensable. By leveraging advanced tools and analytics at scale, RiskRecon provides organizations with the capability to make sense of the intricate web of dependencies within their supply chain. It offers the expertise needed to assess and mitigate risks effectively, enabling organizations to navigate the challenges of supply chain intricacies with confidence. In an environment where proactive risk management is the key to resilience, aligning with a partner like RiskRecon ensures that your organization is well-equipped to tackle the evolving landscape of supply chain security.

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

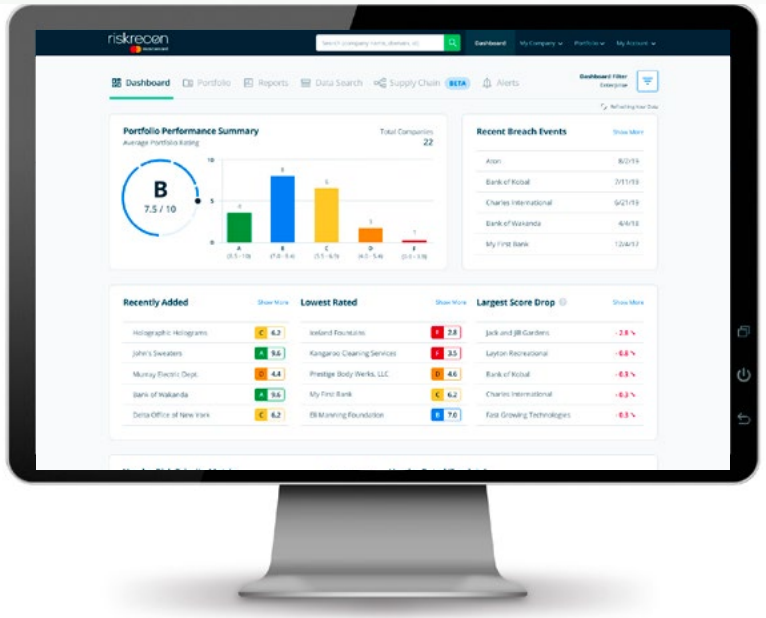
Security ratings and summary assessment of up to 50 vendors

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)

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



Portfolio Performance Summary
Average Portfolio Rating
Total Companies 22

Recent Breach Events

Acon	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

Holographic Holograms	C 6.2
John's Sweaters	A 9.6
Murray Electric Dept.	D 4.4
Bank of Wakanda	A 9.6
Delta Office of New York	C 6.2

Lowest Rated

Iceland Fountains	F 2.8
Kangaroo Cleaning Services	F 3.5
Prestige Body Werks, LLC	D 4.6
My First Bank	C 6.2
Eli Manning Foundation	B 7.0

Largest Score Drop

Jack and Jill Gardens	-2.8
Layton Recreational	-0.8
Bank of Kobal	-0.3
Charles International	-0.3
Fast Growing Technologies	-0.3

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