A collaborative research project between

riskrecon by

Cyentia Institute

RIPPLES ACROSS THE RISK SURFACE 2025

A study of security incidents **impacting multiple parties**

INTRODUCTION

As our parents taught us, our actions impact the people around us. However, in the case of cybersecurity incidents, it is also the case that the things that happen to us also impact those around us. When one organization's security incident reaches out to impact third parties, we refer to these multi-party incidents as "ripple events." These ripple events have been the subject of several reports in our IRIS series over the years.

In the first ripple reports, we introduced our definition of multi-party ripple incidents and described their essential attributes. We covered their frequency and size, who is impacted by them, and the magnitude of those impacts. Later, we used the MITRE ATT&CK framework to dive deeper into the mechanics of ripple incidents. In this latest edition, we're revisiting some of these previous topics with more precision (and some models!) to provide more actionable insights on these types of incidents.

This edition examines more than 1,500 cybersecurity ripple incidents covering the time period from 2008 to 2024. This collection of incidents involved more than 1.2K unique generating firms and more than 12K[1] unique receiving firms. In this report, we aim to update our understanding of how these incidents occur and propagate to help your organization avoid being caught up in someone else's mess (or being the cause of someone else's mess, as our parents used to scold us). Feel free to review the terminology below before diving into the report.

[1] *Yes, that's a 10x difference between generating and receiving these events!*

2025 KEY FINDINGS

Less common but more costly. While single-party security incidents are more likely to occur, multi-party ripple events routinely trigger losses that are routinely 10 times higher for the organizations that generate them.

Downstream losses are rising. Historically, the primary victims (generators) of ripple events bore most of the costs, but losses for organizations impacted downstream (receivers) have risen steadily and now rival those of initial victims.

Larger firms face outsized risk. More smaller firms get swept up in ripple events, but larger organizations ($10B+ revenue) are twice as likely on a per-firm basis to both generate and receive multi-party incidents.

Exposure amplified in some sectors. Finance, Healthcare, and Education sectors are disproportionately affected as receivers, while Finance, Public, and Utilities are more likely to generate ripple effects.

Ripples cascade across tiers. Propagation tends to cluster among mid-to-large firms but often flows downstream from mid-sized organizations into their smaller suppliers and partners, magnifying systemic risk.

Threat profiles differ dramatically. Ripple incidents show markedly higher involvement from nation-states, hacktivists, and criminal actors compared to single-party events. System intrusions, DDoS attacks, and fraud schemes dominate multi-party incidents.

IMPORTANT TERMS

Security Incident: An incident that compromises the confidentiality, integrity, or availability of an information asset.

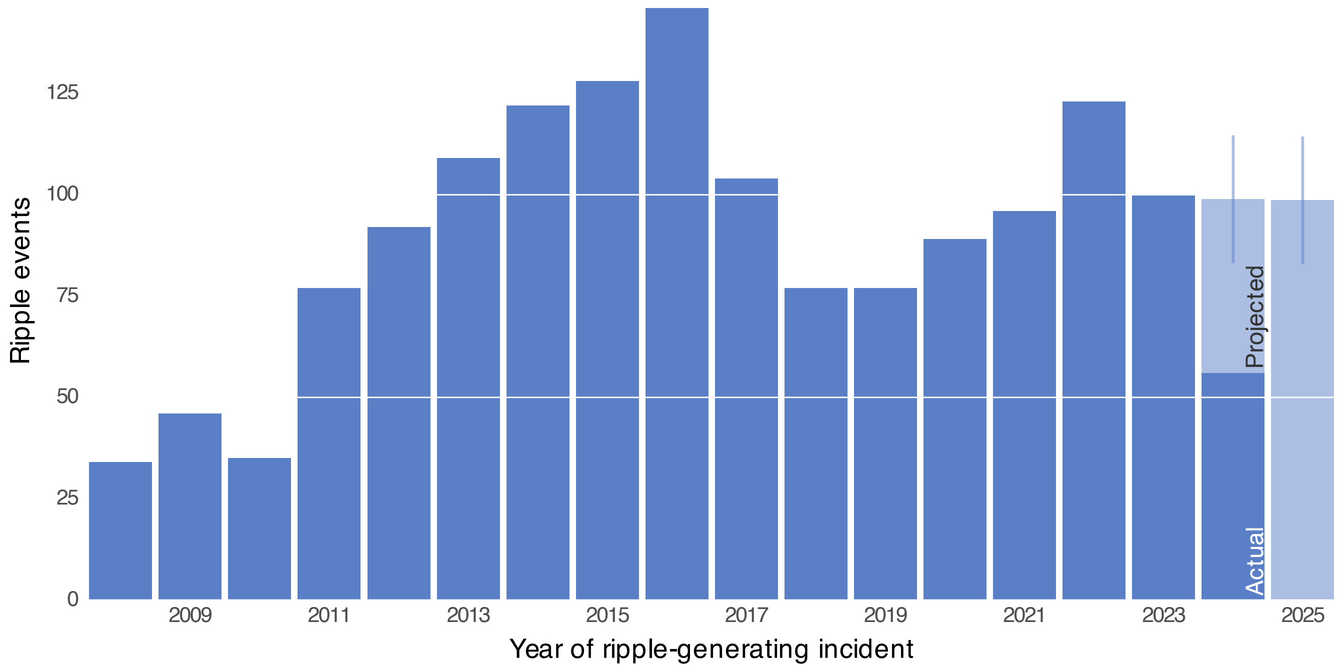
Multi-Party Incident (aka "Ripple events"): A cyber incident that affects multiple organizations. This usually involves a compromise to a central victim that generates downstream loss incidents for various third parties.

HOW COMMON ARE MULTI-PARTY (RIPPLE) INCIDENTS?

Figure 1 starts us off with a picture of how the frequency of ripple incidents has shifted over time. We've plotted counts of unique ripple events, using the date of the generating incident to place it in time. The frequency of ripple events grew steadily from 2008, peaking close to 150 each year during the 2010s before stabilizing at closer to 100 per year.

There is usually a reporting lag for cyber incidents in our incident data, so the count from 2024 is likely artificially low. We used a simple time series model[2] on the cumulative count of ripple incidents over time to extrapolate the likely totals for both 2024 and 2025, shown as "Projected" counts in Figure 1. The error bars represent the approximate range we can expect the projected counts to land in.

FIGURE 1: COUNTS OF MULTI PARTY (RIPPLE) INCIDENTS OVER TIME



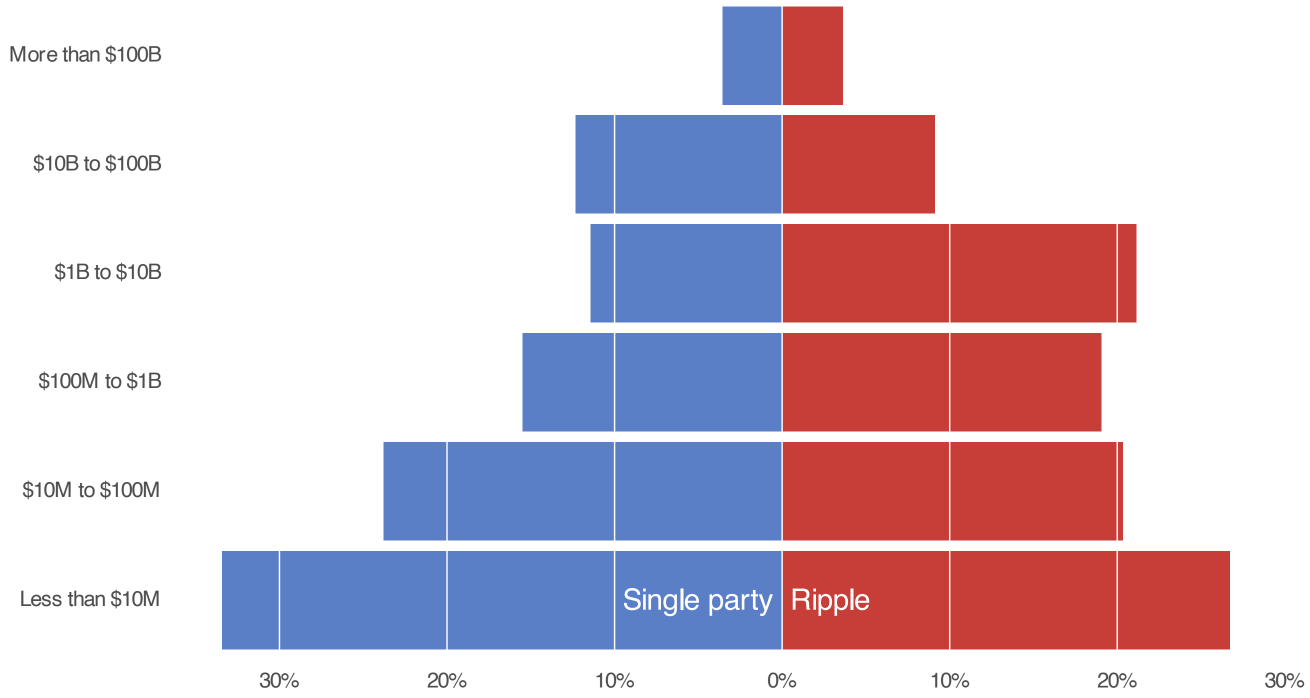
[2] "Simple", as in "it won't impress anyone at a statistics conference, but it probably works decently well."

HOW DO RIPPLE EVENTS DIFFER FROM SINGLE-PARTY INCIDENTS?

Now, when we were snarky teenagers[3] we might have sighed and said that single-party incidents involve a single firm and ripple incidents involve several, but we can do better than that. Also, we can dispense with one large difference immediately: single-party incidents are far more common than ripple incidents. To give a sense of scale to this claim, consider that the overall modeled likelihood of a single-party incident is ~8.4%[4] while the probability for ripple events is only ~0.7%. Keep that in mind as we progress through this section: in general, single-party incidents are much more likely to impact your firm.

With that out of the way, let's turn to some basic characteristics like firm size and sector, where we use the ripple generator to assign an incident to a revenue band or industry sector.

FIGURE 2: PROPORTION OF SINGLE VS. MULTI-PARTY INCIDENTS BY ANNUAL REVENUE



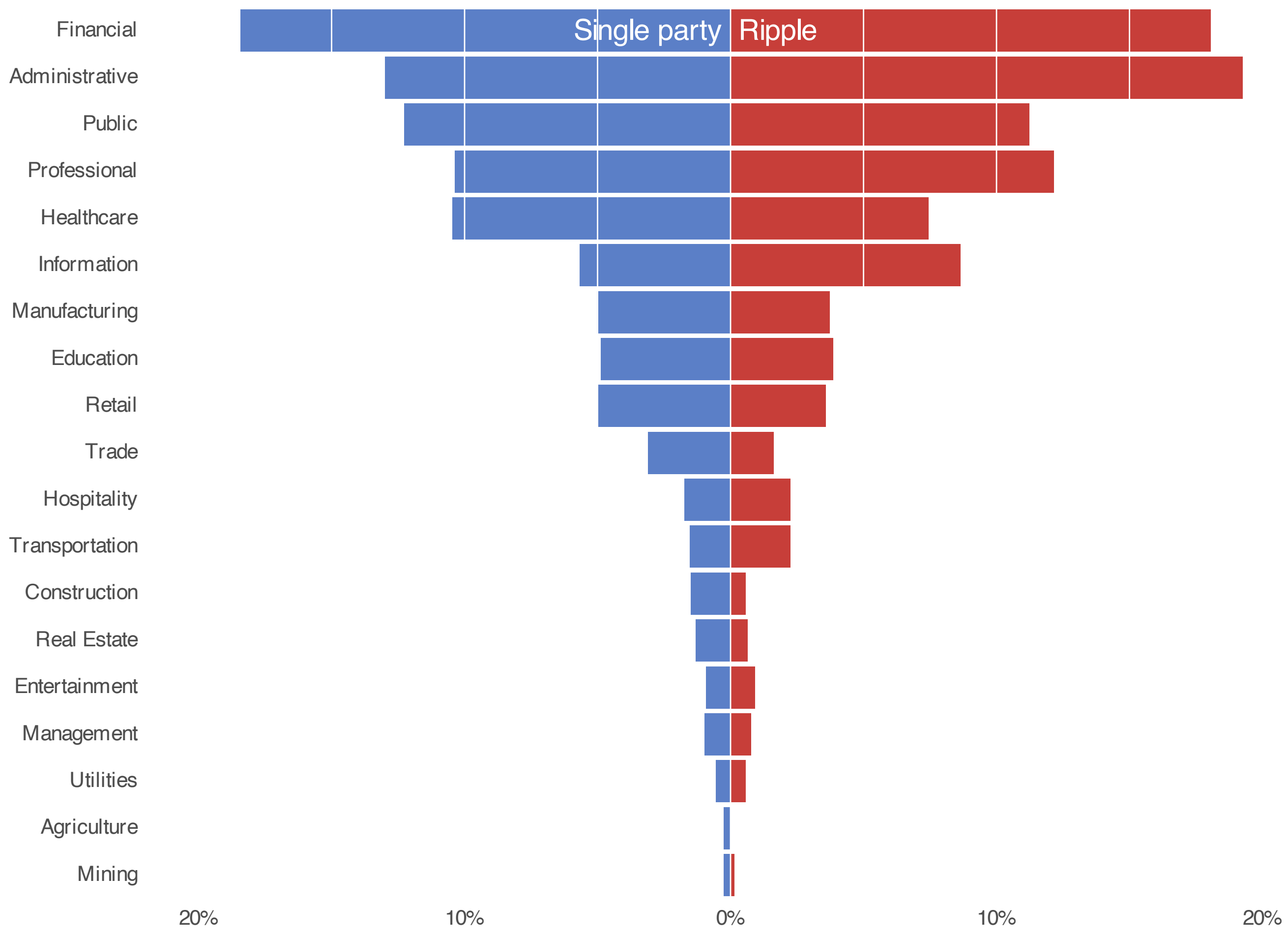
[3] Apologies to all of our parents. We may have been a wee bit insufferable.
[4] See our IRIS reports for this and more!

Figure 2 shows the proportion of single-party incidents and ripple incidents by firm revenue. There is some variation, but overall the distributions are roughly similar, with the smallest firms taking up the largest share and the proportions generally declining as the firms get larger.

In general, single and multi-party incidents follow similar patterns across firmographic dimensions—but notable exceptions exist.

Moving on to differences by sector in Figure 3, we see roughly similar distributions. While it may seem boring to highlight ways in which single-party and ripple incidents are roughly similar, it shows that these larger, multi-party incidents have the potential to impact firms of the same size and sector as single-party incidents do.

FIGURE 3: PROPORTION OF SINGLE VS. MULTI-PARTY INCIDENTS BY SECTOR



Like you, we are more interested in differences than similarities. To that end, Figure 4 shows comparisons of single-party and ripple events by incident pattern[5] and actor.

Focusing on pattern first, while system intrusion is fairly equally common, some other differences emerge. For example, accidental disclosures, physical threats, and insider misuse are considerably more prevalent among single-party incidents. On the other side of the ledger, DoS attacks, scam or fraud, and defacement incidents are all much more common among ripple incidents.

When it comes to who is responsible for these attacks, there are also some significant differences in the "actor" portion of Figure 4. Employees appear to be much more likely to be involved in single-party incidents, which aligns with the prevalence of accidental disclosures and insider misuse patterns.

On the other hand, ripple incidents see a much higher prevalence of hacktivists, nation states and criminal Individuals as the actors. While the latter two make some sense as actors looking to inflict as much damage as possible, the hacktivist difference may seem surprising at first.

We dug into the specific incidents in our data and discovered two large categories of attack. First, many involve hostile attacks against governments or nation-states for socio-political objectives. The other major grouping consists of attempts to embarrass the target into fixing a specific security vulnerability.

[5] *See Appendix A for definitions of incident patterns.*

WANT MORE RESEARCH ON RIPPLES?

The report you're reading now isn't our first Ripples Rodeo. It started way back in 2019 with the original Ripples Across the Risk Surface, with another edition in 2021. In late 2023, we took the series in a new direction with Ripples Across the ATT&CK Surface.

That study analyzed nearly 900 historical ripple events to identify the top MITRE ATT&CK techniques used to generate and propagate them. We also examined top mitigations for the most common techniques to help your organization from getting swept up in their wake.

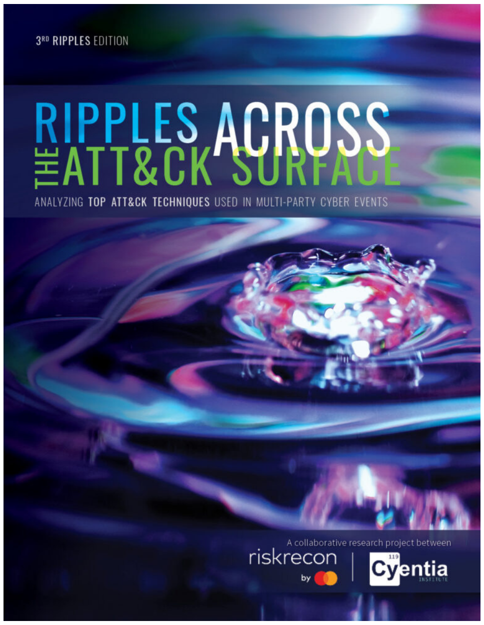
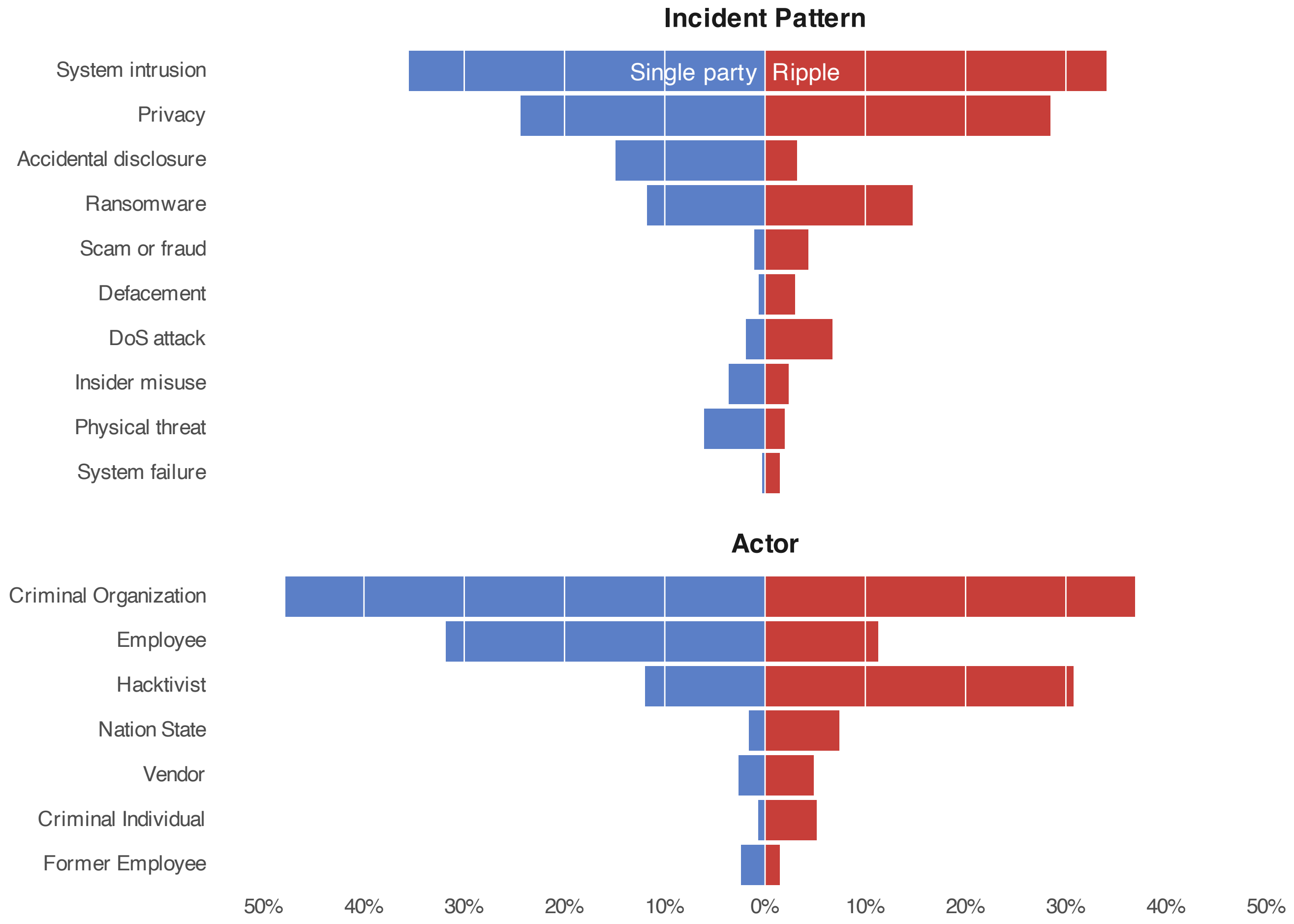

3RD RIPPLES EDITION
RIPPLES ACROSS THE ATT&CK SURFACE
ANALYZING TOP ATT&CK TECHNIQUES USED IN MULTI-PARTY CYBER EVENTS
A collaborative research project between
riskrecon by
Cyentia INSTITUTE

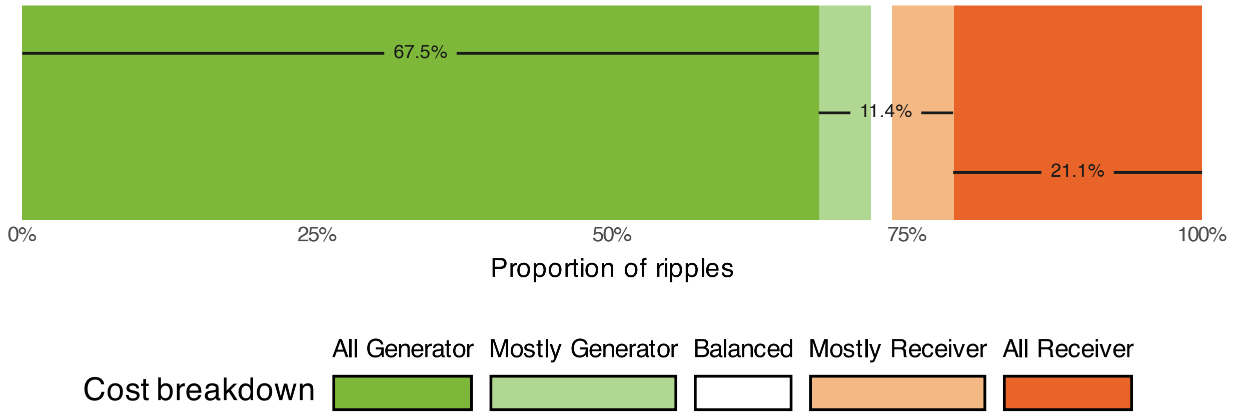
FIGURE 4: PROPORTION OF SINGLE VS. MULTI-PARTY INCIDENTS BY PATTERN AND ACTOR



WHO BEARS THE COSTS FROM RIPPLE INCIDENTS?

To answer this question, we first classified our ripple incidents based on the proportion of all associated losses that were borne by the generator firm versus the receiving firm(s). Figure 5 below shows the results indicating that overall, ripple generators bear the bulk of the total incident costs.

FIGURE 5: RELATIVE SHARE OF COSTS BORNE BY RIPPLE EVENT GENERATORS VS. RECEIVERS



Important Terms

Ripple Generator: The initial or primary victim of a ripple incident.

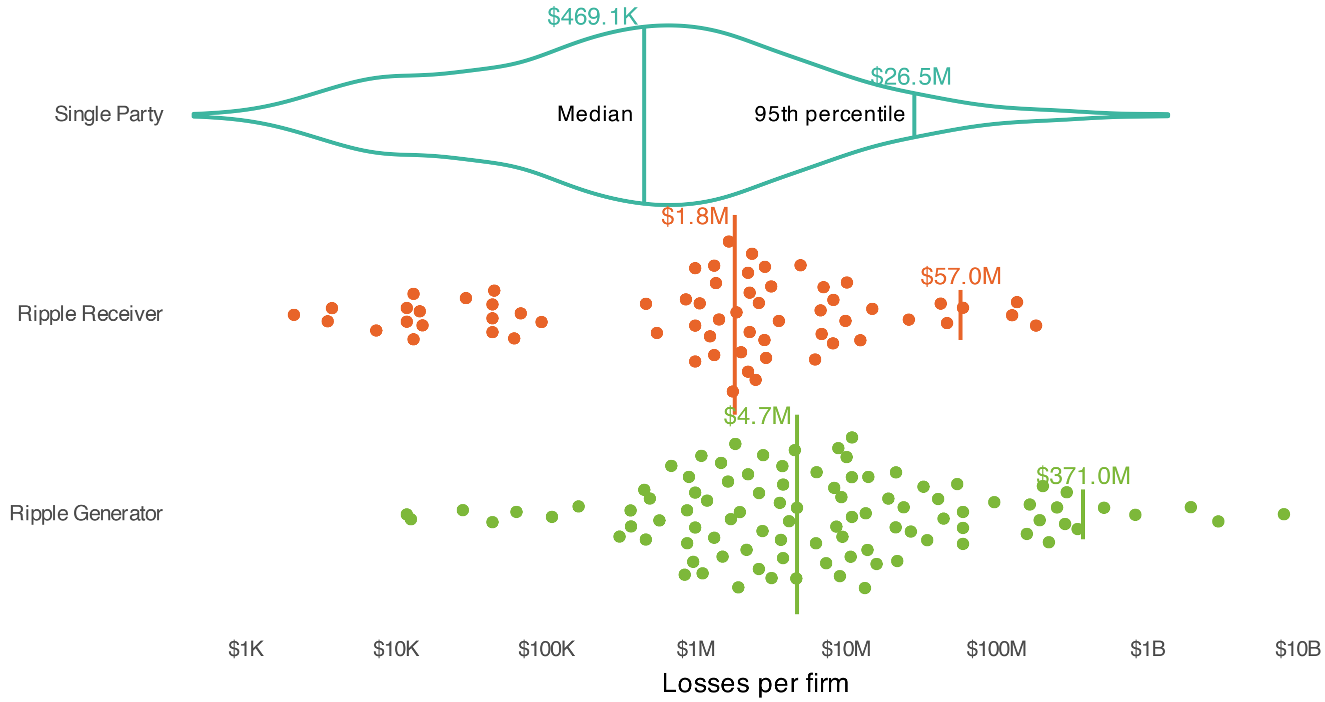
Ripple Receiver: Organizations affected by the generating event.

As a proportion of overall losses, the generators of multi-party incidents bear most of the cost.

Next, we wondered if this changed if instead of looking at the costs for an entire incident across all firms, we instead examined the costs incurred by each firm individually. The answer is shown in Figure 6, which displays the distribution of the per firm costs from single-party incident firms, ripple generator firms and ripple receiver firms.

Once again, per firm, generators tend to incur more losses than receivers, which in turn incur more losses per firm than those from single-party incidents. In fact, the typical (median) cost for generators is 2.6x higher for generator firms ($4.7M versus $1.8M). The difference in extreme losses is even greater, clocking in at 6.5x higher for generator firms ($371.0M versus $57.0M).

FIGURE 6: PER-FIRM LOSSES FOR SINGLE-PARTY INCIDENTS, RIPPLE EVENT GENERATORS, AND RECEIVERS

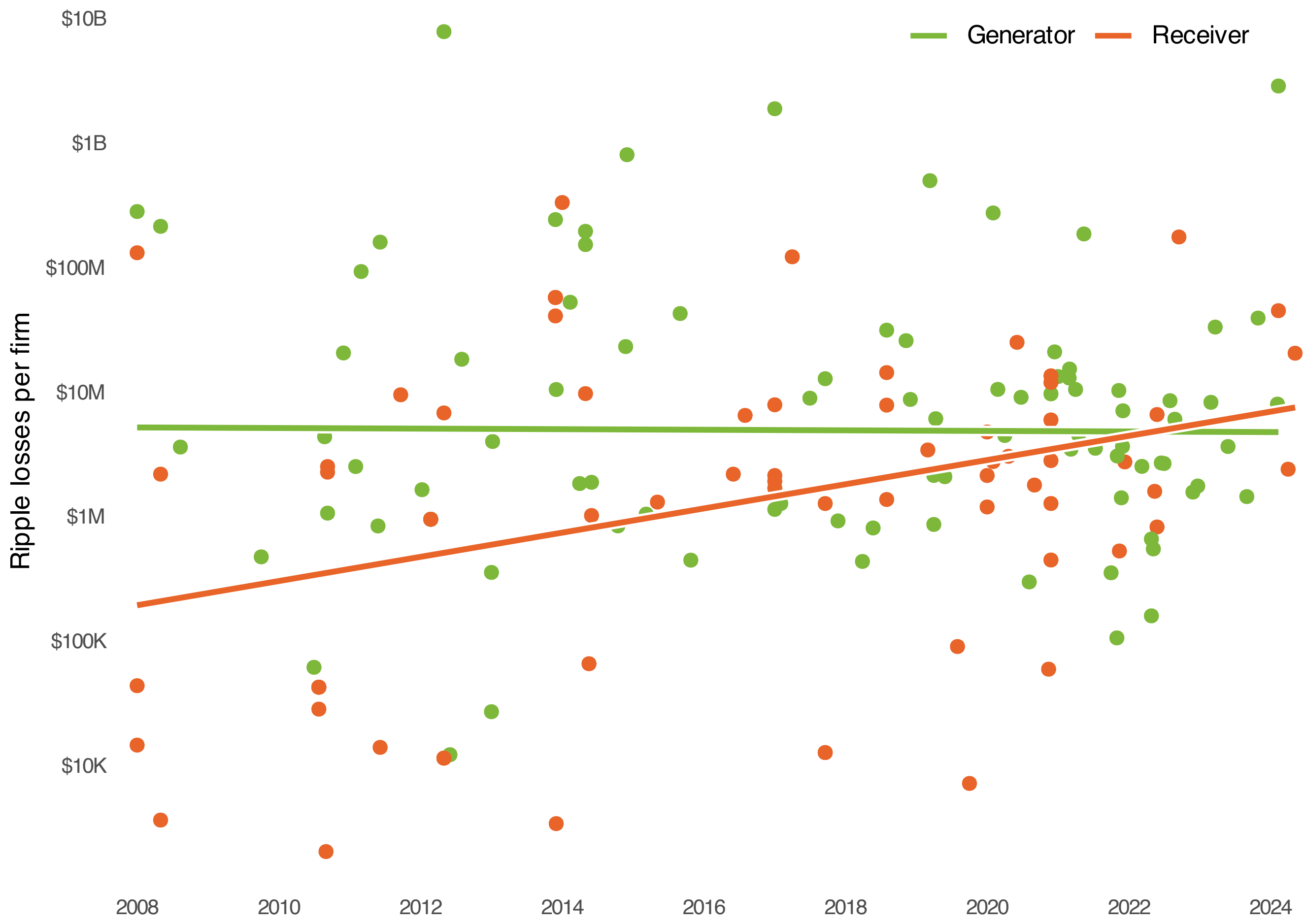


Ripple events are more costly to individual firms—even those impacted downstream—than single-party incidents.

These figures all make the per-firm costs for single-party events pale in comparison. Falling victim to a cyber incident that ends up being a multi-party ripple event can lead to typical losses 10x greater and extreme losses 14x greater than if the incident involves only your single firm.

However, this happy agreement between the overall and per-firm costs did not quite satisfy us, so we decided to check how the per-firm costs have shifted over time for generators and receivers, shown in Figure 7. Over time, the per-firm costs for ripple receivers have been increasing and now are roughly the same as the per-firm costs for generators. This highlights the increasing dangers faced by firms of being caught up in an incident involving another party.

FIGURE 7: PER-FIRM LOSSES OVER TIME FOR RIPPLE EVENT RECEIVERS AND GENERATORS



Losses from ripple events are trending such that they're now the same for generators and downstream receivers.

WHAT KINDS OF FIRMS GENERATE OR RECEIVE RIPPLE INCIDENTS?

In this section, we're going to peer inside multi-party ripple incidents to examine some of their internal characteristics. Specifically, we're going to revisit this note from our original 2019 Ripples report:

> "We considered including an alternative view that would scale the number of ripple events by the number of registered organizations in that sector. It's possible that Business Support and Finance are on top just because they have the most companies, rather than because they're more prone to spawning ripple events. If we make that simple adjustment to normalize for firms in each sector, the top five shift to Management, Public, Information, Business Support, and Utilities. That's different enough that we'll likely come back to this in future research to do it justice. For now, just keep it in mind."

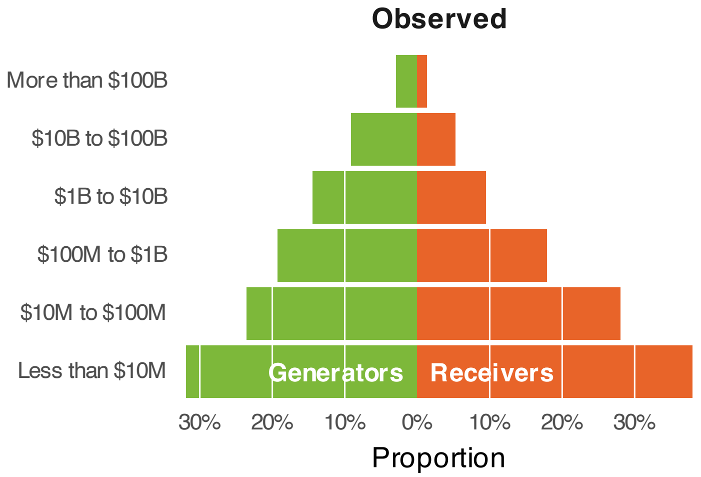
The point is that when we describe the prevalence of firms as generators or receivers from different industries or revenue bands, we should be accounting for how common firms are in those industries or revenue bands.

To achieve this, we employed a logistic regression model that counts each ripple generator or receiver firm as a positive case, and all other firms that experience only single-party events as negative cases. We then used this model to estimate the relative likelihood of firms being generators or receivers.

To make this concrete, let's begin by examining ripple generators and receivers by firm size, as measured by revenue. First consider Figure 8, which shows the proportions of firms comprising ripple generators or receivers. As we can see, the bars are large at the bottom and become progressively smaller as firm size increases.

But this may simply be because there are many more small firms than large ones! So let's turn to Figure 9, which shows the adjusted likelihoods of a firm in a particular revenue band being a ripple generator or receiver. The bars are shaded to highlight relative likelihoods greater than one.

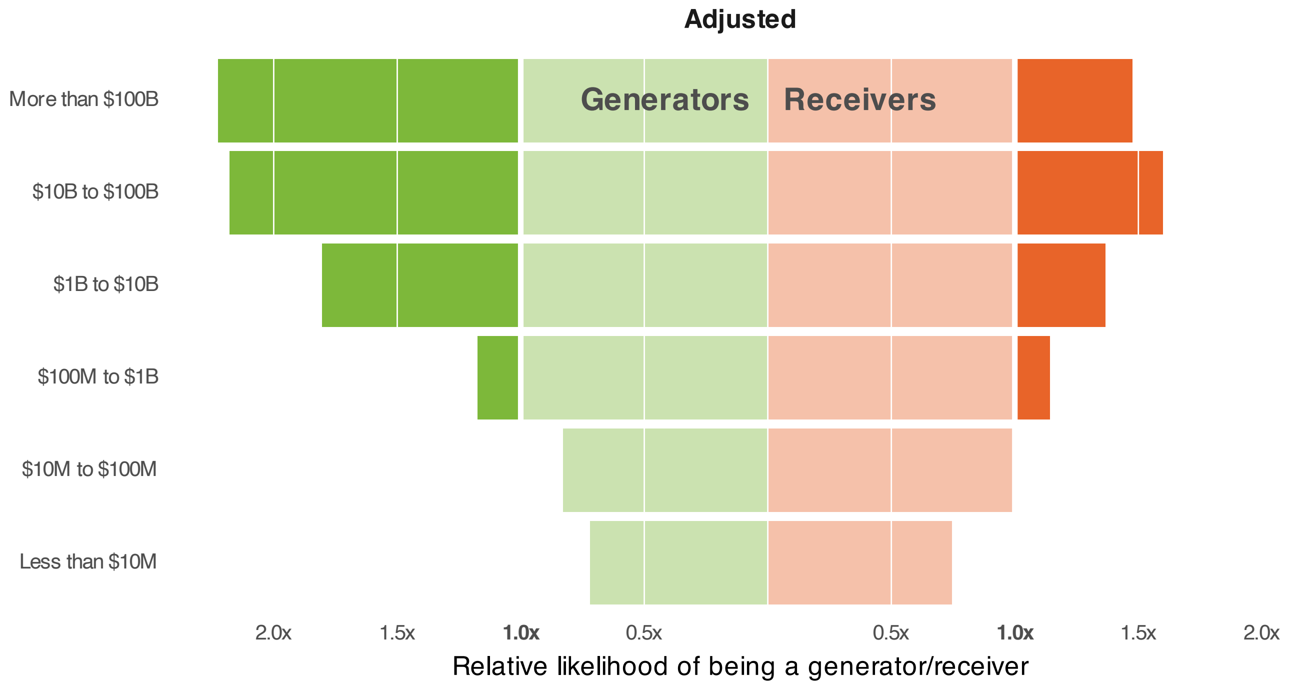
FIGURE 8: BREAKDOWN OF RIPPLE EVENT GENERATORS AND RECEIVERS BY REVENUE



Our adjustment has essentially reversed the picture entirely! While the largest firms comprise the smallest overall proportion of ripple generators and receivers (Figure 8), adjusting for the number of such firms that exist reveals that they are about twice as likely to be involved in multi-party incidents (Figure 9).

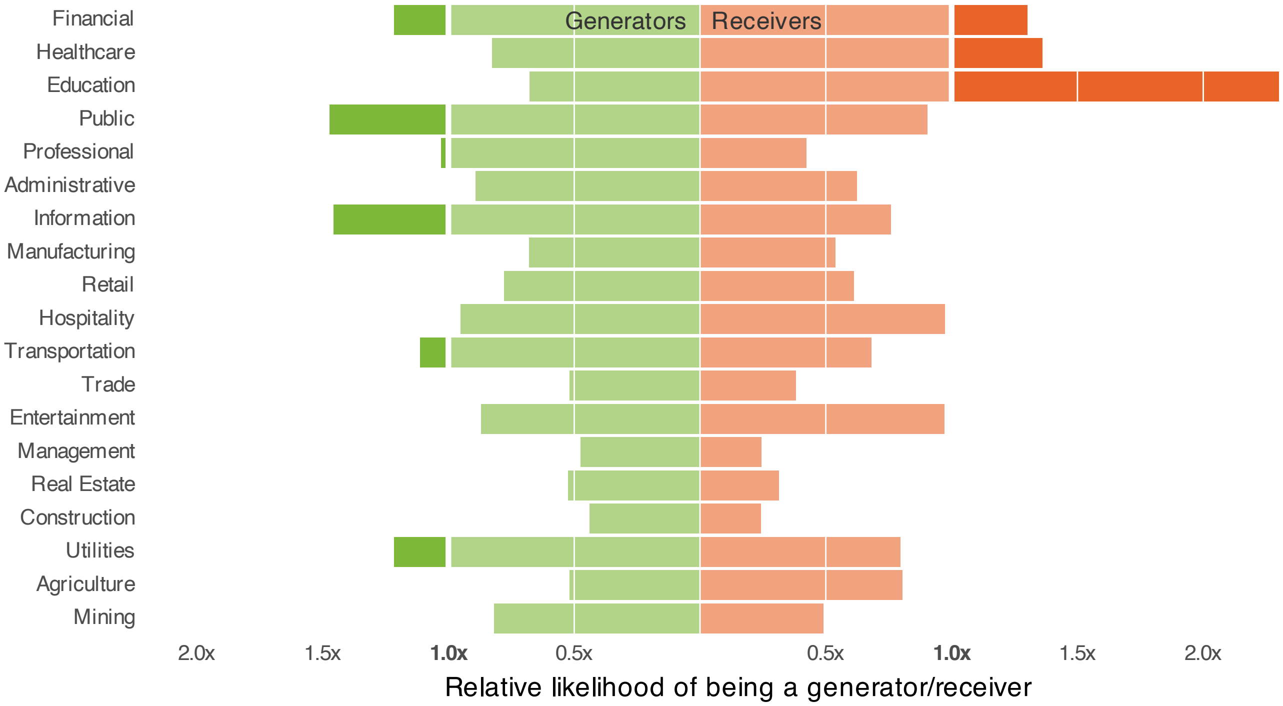
On a per-firm basis, larger organizations are far more likely to both generate and receive ripple events compared to SMBs.

FIGURE 9: MODELED RELATIVE LIKELIHOOD OF FIRMS GENERATING OR RECEIVING RIPPLE EVENTS BY REVENUE



If we apply the same adjustment at the sector level, we get Figure 10. Here, the Financial, Healthcare, and Education sectors receive more than their fair share of ripple effects. On the generator side, the adjusted likelihoods suggest that the Financial, Public, Information, Transportation, and Utilities sectors are more likely to experience incidents that spread across their third-party networks.

FIGURE 10: MODELED RELATIVE LIKELIHOOD OF FIRMS GENERATING OR RECEIVING RIPPLE EVENTS BY SECTOR

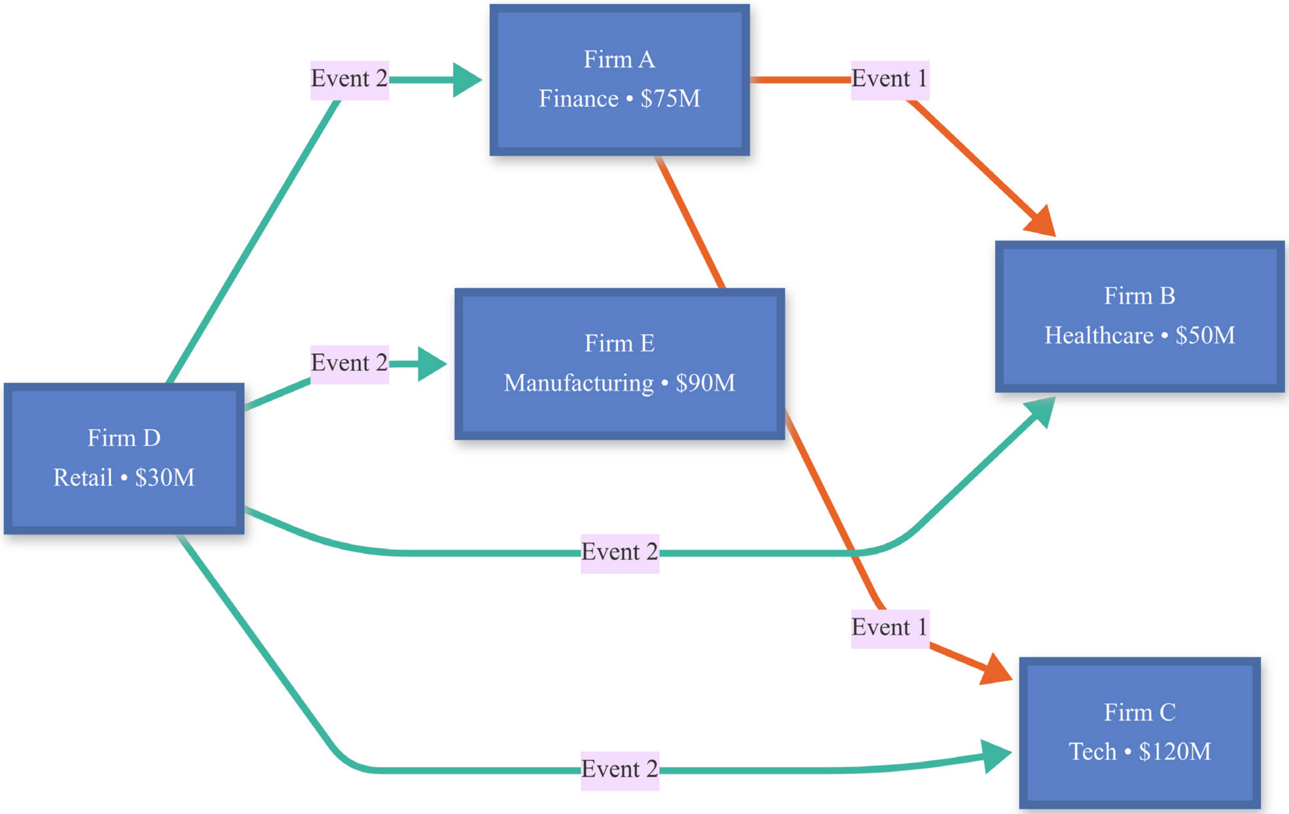


HOW DO RIPPLES FLOW BETWEEN SECTORS & REVENUE BANDS?

The previous section considered a static description of the firms that make up ripple incident generators and receivers, independent of how impacts flow between firms. We shift here to a more dynamic view that examines how ripple impacts connect generators and receivers. However, we still want to do so in a relative fashion that accounts for the overall populations of firms.

To do this, consider the hypothetical schematic in Figure 11, which shows two imaginary ripple events. Each box (node) is a firm, and the arrows between them (edges) define generator to receiver relationships. If we expand this diagram to include all firms and ripple events, we end up with a giant graph with thousands of nodes and edges.

FIGURE 11: ILLUSTRATION OF A HYPOTHETICAL GRAPH STRUCTURE BETWEEN FIRMS IN RIPPLE EVENTS.



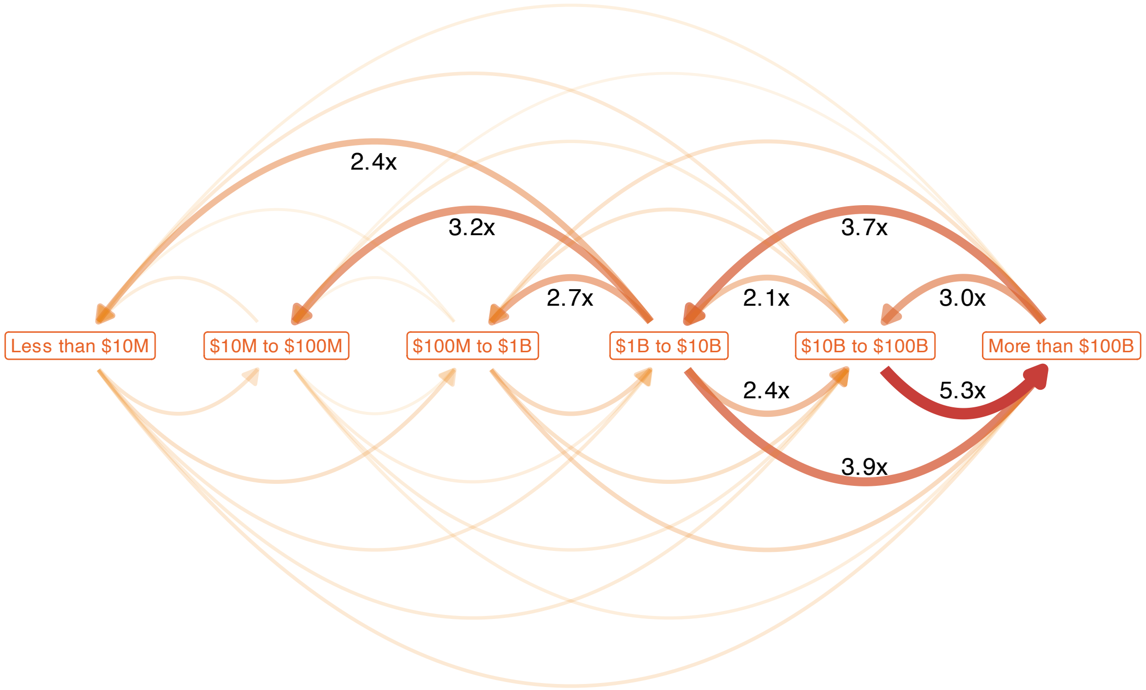
We can then use this graph to answer questions about how ripple events flow between groups of firms, such as by counting the number of edges flowing from large firms to small firms. However, since we want to adjust for the relative frequency of firms as we did in prior sections, we instead count edges relative to an equivalent graph but with all the edges randomly permuted between firms.

A concrete example will help ground this discussion, so consider Figure 12, which displays the relative degree of flow between firms of different sizes compared to a random assignment of connections. The heavier the arrow, the more flow there is between firms of those sizes than we'd expect if the connections were random. So, for example, there are 5.3x more generator-receiver pairs flowing from "$10B to $100B" firms up to "More than $100B" firms than we'd expect if those pairs were assigned randomly.

Two primary patterns appear. First, there is a significant amount of ripple impact within the mid-to-large firms ($1B to $10B and up), indicated by the heavier arrows running among those three revenue bands. Second, there is notable amount of ripple effects flowing downward from mid-size firms ($1B to $10B) to smaller firms.

A careful reader may have noted that there are no arrows positioned in "loops" running from a revenue band to itself. We wanted to focus on impacts between firms of different sizes, so we omitted those from the figure, but it is important to note that the flow within the same revenue band is also quite high for the mid-large firms as well.

FIGURE 12: RIPPLE INCIDENT GENERATOR TO RECEIVER FLOW BETWEEN FIRMS OF DIFFERENT REVENUE SIZES

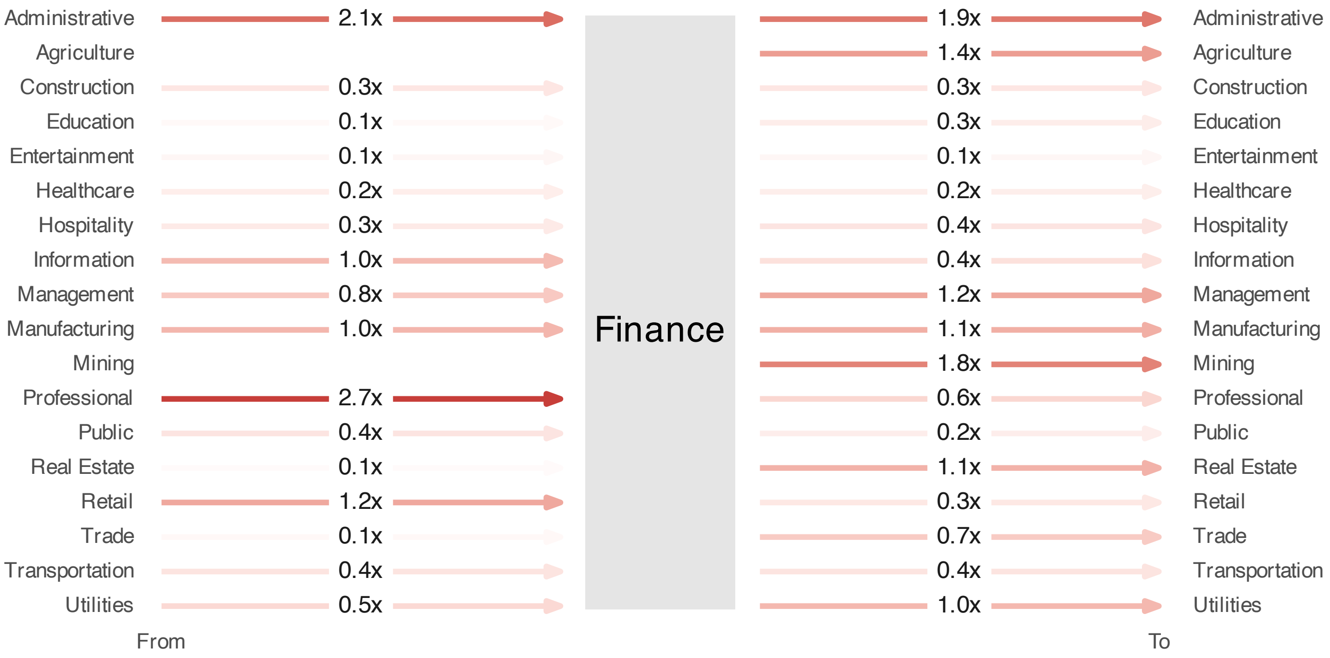


Ripples often propagate among larger firms, but there's also a tendency form them to flow from midsize to smaller firms.

An equivalent plot for industry sectors would be visually overwhelming, with arrows flying around between 20 different nodes[6]. Instead, we'll isolate a single sector and visualize the rate of ripple activity flowing into and out of that particular sector. We'll begin in Figure 13 focusing on the Finance sector. The arrows on the left denote ripple activity flowing into the Finance sector, while the arrows on the right denote ripple activity flowing from Finance into other sectors.

The sectors most likely to impact Finance firms are Professional, Administrative, and Retail, as those all appear more often than we'd expect if we assigned generator and receiver roles at random. For example, there are 2.7x as many ripple events generated by Professional firms impacting Finance firms than you'd expect if the relationships were totally random. Conversely, the sectors that Finance is most likely to impact include Administrative, Mining, and Agriculture.

FIGURE 13: RATES OF INFLOW & OUTFLOW FOR RIPPLE EVENTS SURROUNDING THE FINANCE SECTOR



[6] *Third-party relationships are more complicated than a late season episode of Lost!*

FIGURE 14: RATES OF INFLOW & OUTFLOW FOR RIPPLE EVENTS SURROUNDING THE RETAIL SECTOR

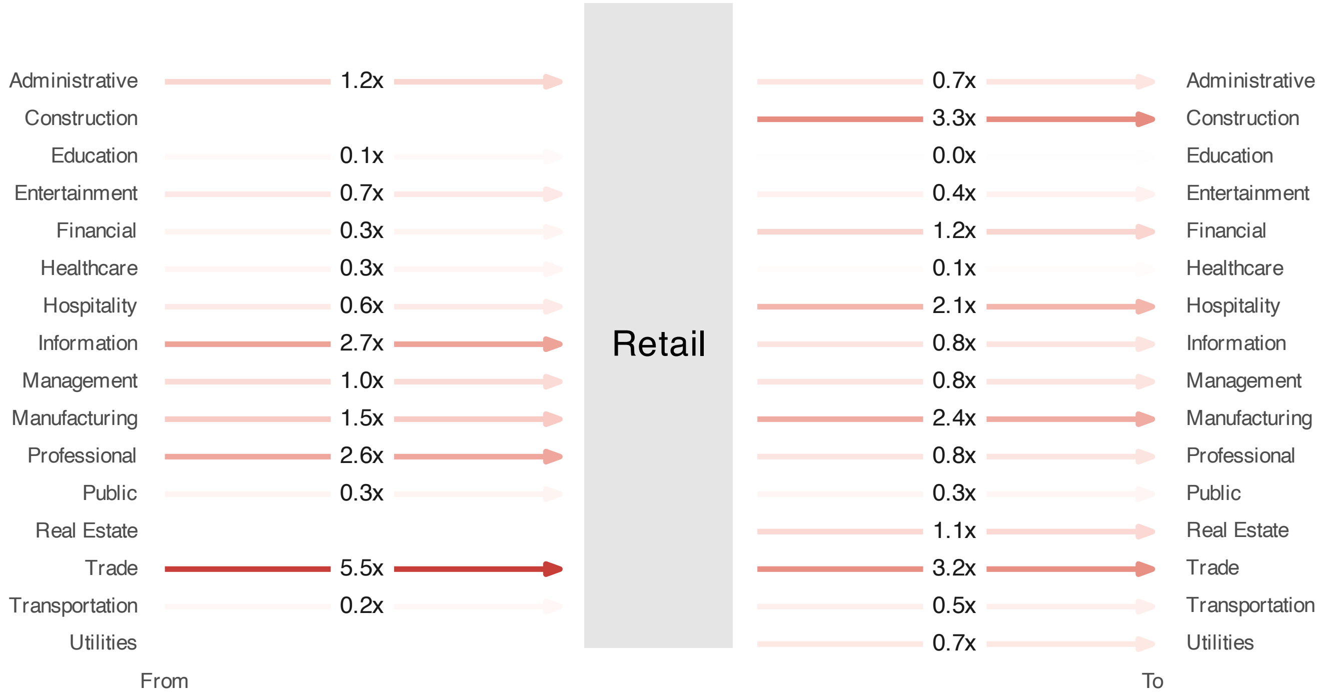


Figure 14 focuses on the Retail sector, highlighting that the Professional & Administrative sectors tend to send the most ripple activity in that direction and that multi-party ripples are most likely to flow out of the Retail sector into Administrative, Mining, and Agriculture.

CONCLUSION

As this year's Ripples Report clearly demonstrates, the fallout from cyber incidents rarely stops at the initial victim. Multi-party ripple events continue to amplify losses across interconnected ecosystems—impacting suppliers, partners, and customers alike. With downstream losses now rivaling those of primary victims, it's no longer enough to focus solely on your organization's internal defenses. True resilience demands a deep understanding of your digital supply chain.

Every connection introduces new risk. Larger firms are twice as likely to generate and receive ripple events, and industries such as Finance, Healthcare, and Education remain disproportionately exposed. As these relationships grow in complexity, the need for continuous visibility into the cybersecurity posture of your vendors has never been more urgent. Knowing who you're connected to—and how well they manage their own risks—is essential to preventing your organization from becoming the next ripple generator or downstream casualty.

The data is clear: ripple events magnify systemic risk, and strong cybersecurity hygiene across your vendor ecosystem is a decisive factor in limiting exposure. Organizations that can leverage insights to identify high-risk relationships early are far better positioned to mitigate the cascading impacts of a breach.

FREE OFFER

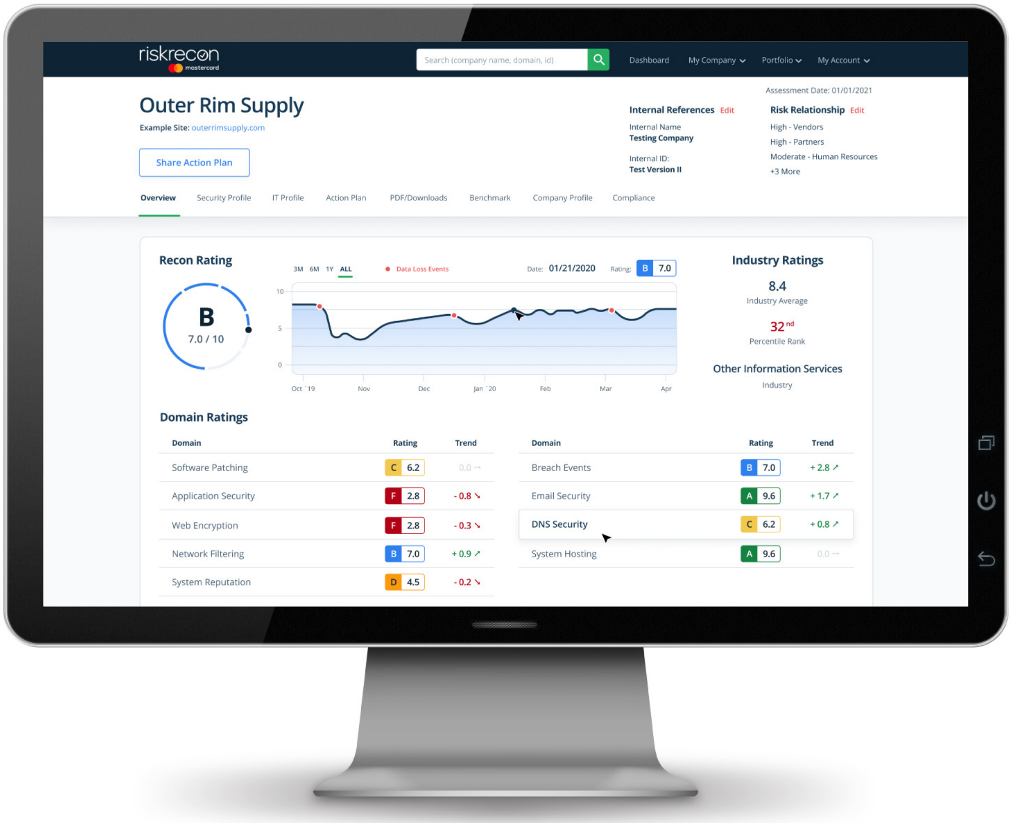
☑ Gain the clarity you need to protect your business from ripple effects.

☑ Start by assessing the cybersecurity hygiene of your most critical third parties.

☑ Get a free trial of RiskRecon by Mastercard and instantly understand the cyber risk ratings of up to 50 vendors in your ecosystem.

☑ Benchmark their security performance, uncover hidden risks, and take proactive steps to strengthen your digital supply chain.

☑ Start your free trial now. See where your risks lie—before they ripple across your business.



Outer Rim Supply

Example Site: outerrimsupply.com

Assessment Date: 01/01/2021

Internal References Edit

Internal Name
Testing Company

Internal ID:
Test Version II

Risk Relationship Edit

High - Vendors
High - Partners
Moderate - Human Resources
+3 More

Recon Rating

B
7.0 / 10

Date: 01/21/2020 Rating: B 7.0

Industry Ratings

8.4
Industry Average

32nd
Percentile Rank

Other Information Services
Industry

Domain Ratings

Domain	Rating	Trend
Software Patching	C 6.2	0.0 →
Application Security	F 2.8	- 0.8 ↘
Web Encryption	F 2.8	- 0.3 ↘
Network Filtering	B 7.0	+ 0.9 ↗
System Reputation	D 4.5	- 0.2 ↘

Domain	Rating	Trend
Breach Events	B 7.0	+ 2.8 ↗
Email Security	A 9.6	+ 1.7 ↗
DNS Security	C 6.2	+ 0.8 ↗
System Hosting	A 9.6	0.0 →