

A Snapshot of Cyber Tsunamis

5 Observations from an analysis of the largest and most impactful multi-party cybersecurity events of the last 5 years



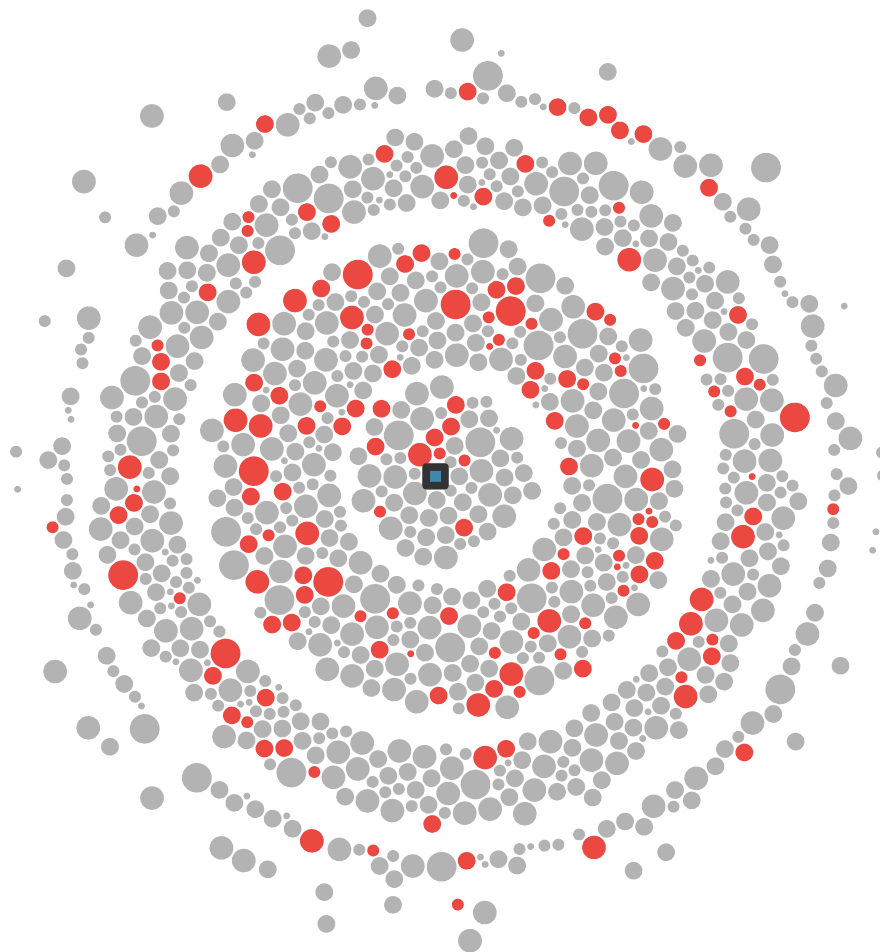
Cybersecurity

What's a ripple event? A tsunami?

A single cyber incident rarely stays contained to one organization. When a data breach, ransomware attack, or major outage at one company triggers cascading events and impacts across the supply chain, we call that a ripple event. And the biggest of those earn the “tsunami” moniker. RiskRecon and Cyentia have tracked these multi-party incidents together since 2019, publishing the [Ripples Across the Risk Surface](#) series and the 2021 [“Tsunami Edition”](#) of the Information Risk Insights Study (IRIS) that this report updates. This snapshot continues that lineage by analyzing the largest cyber tsunami events of the last five years.

This visualization, which is based on RiskRecon’s intel, demonstrates the context in which ripple and tsunami events form and propagate. The firm in the center hasn’t had a breach, but many of its third and Nth-tier parties have (indicated in red).

Not only that, but numerous 4th, 5th, 6th parties (the concentric rings) have known breaches. Any one of these can spawn ripple — or tsunami — events that propagate through direct and indirect relationships across the supply chain.



What Follows

The five sections that follow trace these events end to end: how large the losses run, whether disclosure or disruption does more damage, what triggers them, how the damage spreads downstream, and who ultimately absorbs it.

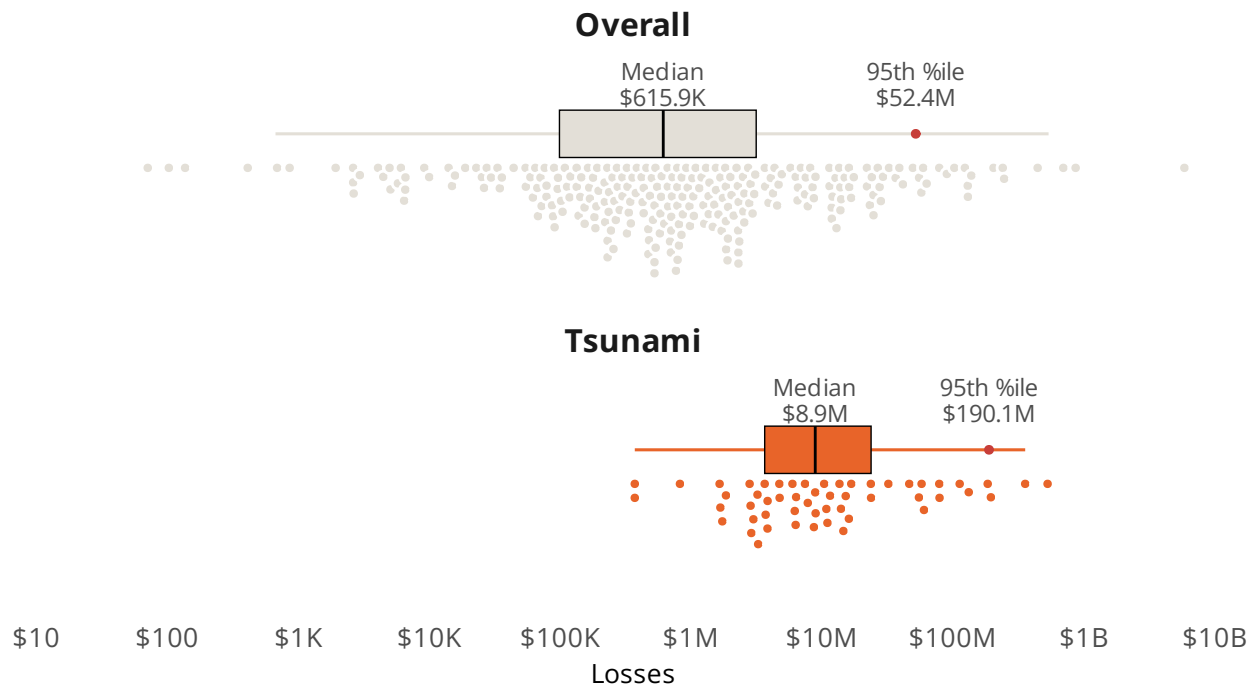
Analytical Approach

- This report analyzes the 100 largest ripple events of the past 5 years (through mid 2026).
- The sample is the union of the top 50 by reported financial losses, total data records affected, and the number of downstream organizations impacted.
- That’s double the scale of the original 2021 IRIS Tsunami, which applied the same three-criteria (albeit with a top-30 threshold) to identify 50 tsunami events. That suggests tsunami events are growing more common.
- Tsunami events run the full spectrum on each criterion. The costliest incidents aren’t always the ones that hit the most organizations or breached the most records.

How large are the losses?

Before examining the scale of financial losses from cyber tsunamis, let's establish the source. As with prior reports in the IRIS and Ripples series, all loss values are compiled from publicly available information (e.g., SEC disclosures, legal filings, company statements). That sourcing comes with an honest caveat that reported values tend to focus on "hard" rather than "soft" costs, and thus almost certainly understate the true toll on the organizations impacted. Nevertheless, it provides a ground truth lower bound estimate of losses from cyber events that inform risk assessments.

Losses depicted for tsunami events encompass the primary victim plus all downstream firms pulled into a tsunami event's wake. Given that, comparing losses between single-party and multi-party incidents isn't exactly "apples to apples." But it does enable us to make some important observations about the overall economic impact of tsunami events.



Key Facts & Figures

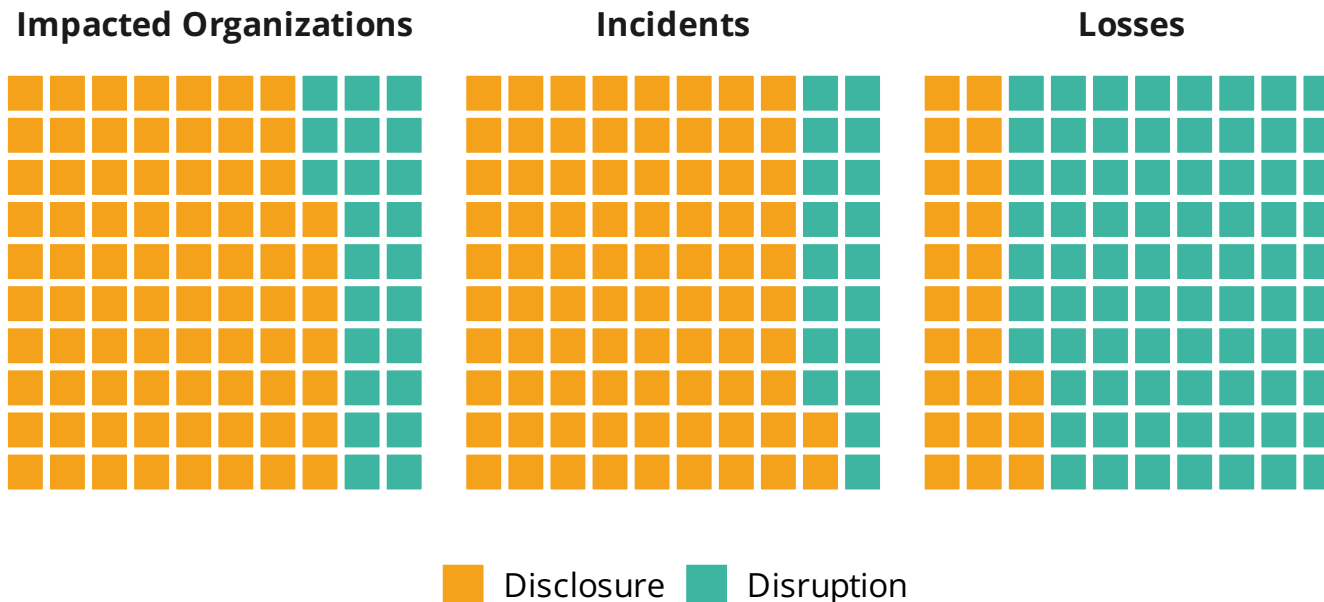
- Total losses for cyber tsunamis run 14X higher than for single-party incidents (median \$9M vs. \$616K).
- Even downstream firms suffer higher losses (median \$3.8M), meaning another organization's breach can hit harder than your own!
- Over a third (38%) of tsunamis cost more than 10% of affected firms' annual revenues. That's a much larger share than we see for the broader population of security incidents (10% to 15%).
- 98% of tsunami events carry known response costs; 94% involve data privacy liability; 36% involve business interruption.

So What?

Multi-party incidents — especially large ones — represent high risk. How are you managing that risk compared to single-party incidents?

What's riskier—disclosures or disruptions?

Not every tsunami event looks the same. We sort each into one of two broad patterns based on its primary character: a disclosure, where sensitive data was exposed, or a disruption, where the incident disabled or interrupted operations. In general, disclosures are more common among large multi-party incidents, but disruptions are more costly for the parties affected.



Key Facts & Figures

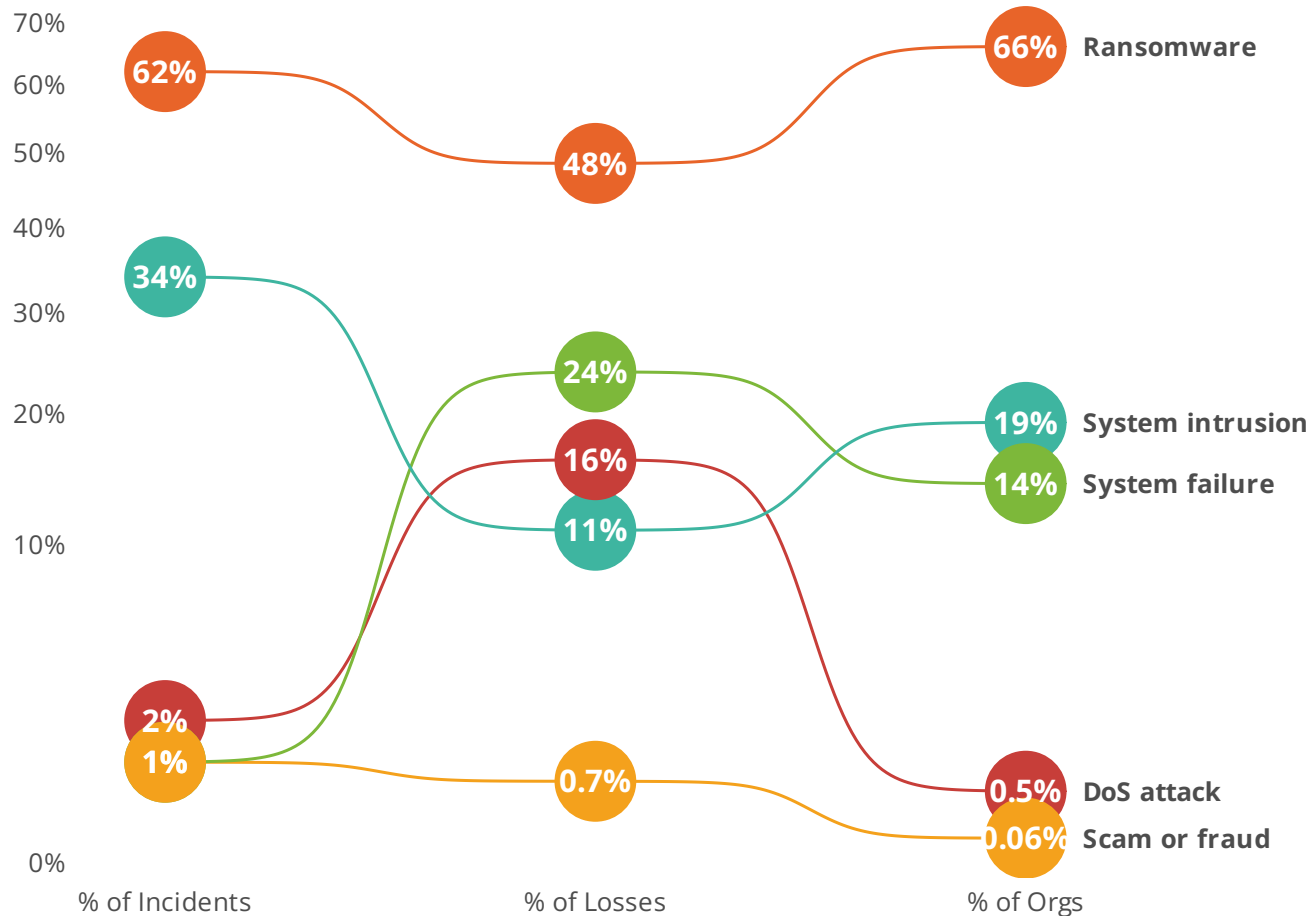
- Most (82%) tsunami events in this sample were caused by data disclosures rather than disruptions.
- Data disclosures were the initial incident for a strong majority of firms (77%) impacted by cyber tsunami.
- Yet disruptive events drive the lion's share of financial losses (77%) across all affected parties.
- Median losses from disruptions (\$61M) are ten times more than for disclosures (\$6.3M).
- Tail risk from disruptive events is also much higher, with a 95th percentile loss of \$411M vs. \$56M for disclosures.

So What?

When evaluating the risk of multi-party incidents, do you consider both data disclosures and service disruptions? They manifest risk in different ways and therefore require different mitigation strategies.

What triggers cyber tsunamis?

In the real world, tsunamis are caused by geological events such as earthquakes, landslides, and volcanic eruptions. The digital equivalents have triggering events too, and we've classified those in our sample using the incident patterns featured in the IRIS and Ripples series. In the grand scheme of all security incidents, system intrusions lead by a large margin across the board. But ransomware is the undisputed prime peril when it comes to triggering large multi-party cyber events.



Key Facts & Figures

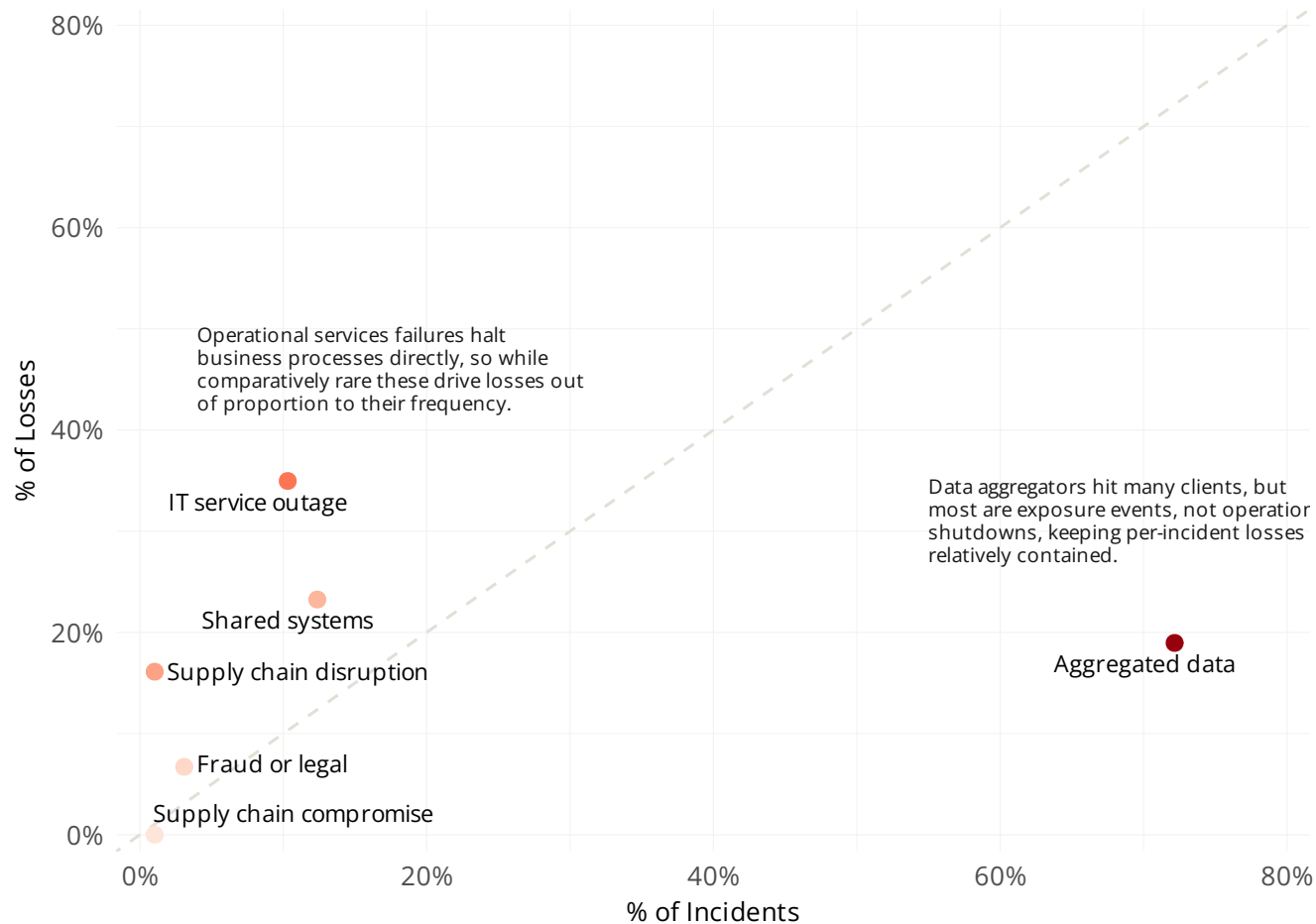
- Ransomware triggers 62% of cyber tsunamis — nearly twice the next most common cause combined — but accounts for just 48% of total losses.
- System intrusion is the second-most-common trigger (34% of events) and touches 19% of downstream organizations.
- System failures and DDoS attacks combine for barely 3% of events, yet drive more than a third of all losses — rare triggers, outsized damage.
- Ransomware also reaches the most downstream organizations (66% of them), underscoring its role as both the top trigger and the top propagator.

So What?

Ransomware and intrusions trigger the large majority of these massive ripples and impact the most downstream parties. BUT system failures and DDoS attacks generate the highest financial losses. Do you have a strategy for them all?

How do ripple events propagate?

You can do everything right and still take the hit for someone else's incident. This section maps the paths that damage actually travels: data a partner held on your behalf, systems you shared, software you both relied on, or the fraud and litigation a breach sets loose downstream. The chart below plots how often each path is the culprit against how expensive it turns out to be — because the most common way ripples spread isn't necessarily the most damaging one.



Key Facts & Figures

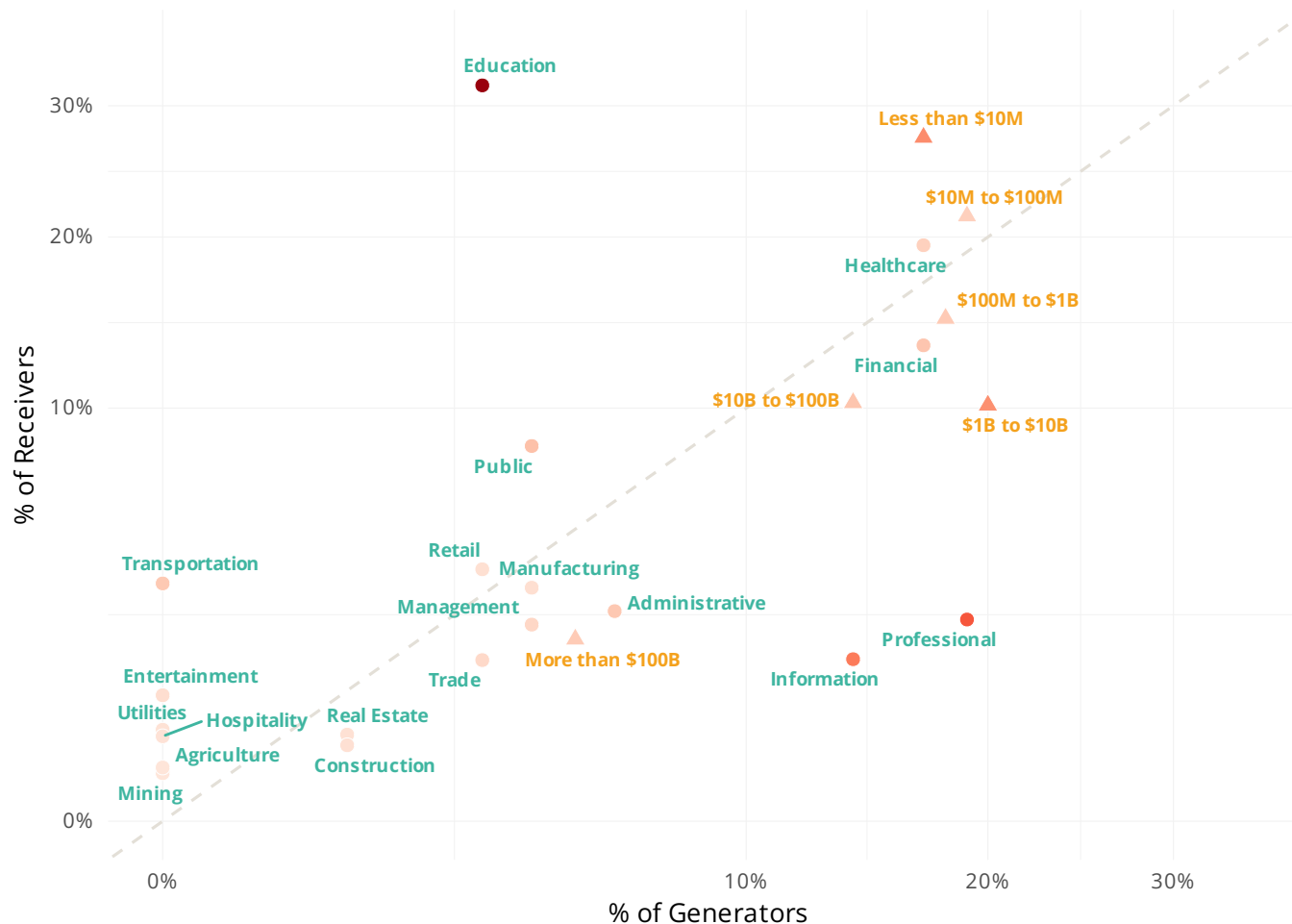
- Aggregated data — the generator holding data on behalf of parties it never directly breached — is the dominant propagation method by far, involved in the clear majority of tsunami events.
- Despite that volume, aggregated data events land toward the lower end on losses relative to their share of incidents.
- IT service outages are far less common but punch well above their weight on losses — when a shared tech or SaaS provider goes down, downstream costs pile up fast.
- Shared systems also skew toward higher losses relative to frequency; supply-chain compromise, fraud/legal, and supply-chain disruption remain comparatively rare in this sample.

So What?

Who's aggregating your data (or vice versa)? Whose services are you dependent on? How are you managing risk that originates upstream?

Who's impacted downstream?

Every tsunami event pulls other organizations into its wake — 5,915 of them, across our 100-event sample. But that pull isn't even across sectors. The chart below compares how often organizations in each sector cause a ripple (as the generator) against how often they get caught in someone else's (as a receiver) — the sectors that land farthest from the diagonal are the ones whose risk exposure looks nothing like their role in causing incidents.



Key Facts & Figures

- Education is an outlier. It rarely originates from tsunamis, yet accounts for the largest share (~30%) of downstream receivers.
- Professional services and Information/technology sit on the opposite side: meaningful generators of ripple events, but rarely receivers — consistent with sitting upstream in other organizations' supply chains.
- Healthcare and Financial are the only two sectors that rank high on both axes — heavily exposed as both generators and receivers of multi-party risk.
- Organizations under \$10M in revenue skew heavily toward receivers, while those north of \$1B skew toward generators — the smaller a partner is, the more likely they get pulled into your incident rather than cause one.

So What?

How does this align with your supply chain? How is your organization represented here?

Reducing the Risk of the Next Cyber Tsunami

The largest multi-party cyber events demonstrate that organizations cannot evaluate cyber risk solely within the boundaries of their own enterprise. Dependencies on third parties, technology providers, shared systems, data processors, and other critical suppliers create pathways through which a single incident can affect dozens—or even hundreds—of organizations.

The 100 cyber tsunamis analyzed in this study affected 5,915 downstream organizations. And while these events propagate in different ways, one cause stands above the rest: ransomware accounts for more than 60% of the major multi-party events analyzed and nearly half of their financial losses.

That finding reinforces an important lesson from Mastercard's Ransomware in the Supply Chain research: ransomware is no longer simply an enterprise security problem. It is a digital supply chain risk.

Organizations looking to reduce their exposure to the next major ripple event should consider three questions:

1. Where are your critical dependencies? Identify the suppliers, service providers, technology platforms, and other third parties whose disruption or compromise could materially affect your operations. Particular attention should be given to organizations that aggregate sensitive data, provide critical digital services, or support business processes that cannot easily be replaced.

2. Which organizations present the greatest potential for a ripple event? Not every supplier creates equal risk. Evaluate third parties based not only on their inherent importance to your business, but also on observable cybersecurity performance, exposure to ransomware and other threats, and the potential impact of a disruption or data compromise.

3. Are you managing risk continuously—or waiting for the incident? Point-in-time assessments provide only a snapshot. The conditions that contribute to ransomware and other disruptive events change continuously. Organizations need ongoing visibility into the cybersecurity posture of critical suppliers so emerging risks can be identified, prioritized, and addressed before they become pathways for widespread disruption.

From Ripple Risk to Action

The lesson from both studies is clear: your organization's cyber resilience increasingly depends on the resilience of the organizations around you.

Understanding those dependencies is the first step. The next is identifying where preventable cybersecurity weaknesses exist across your digital supply chain and focusing remediation efforts where they can have the greatest impact.

