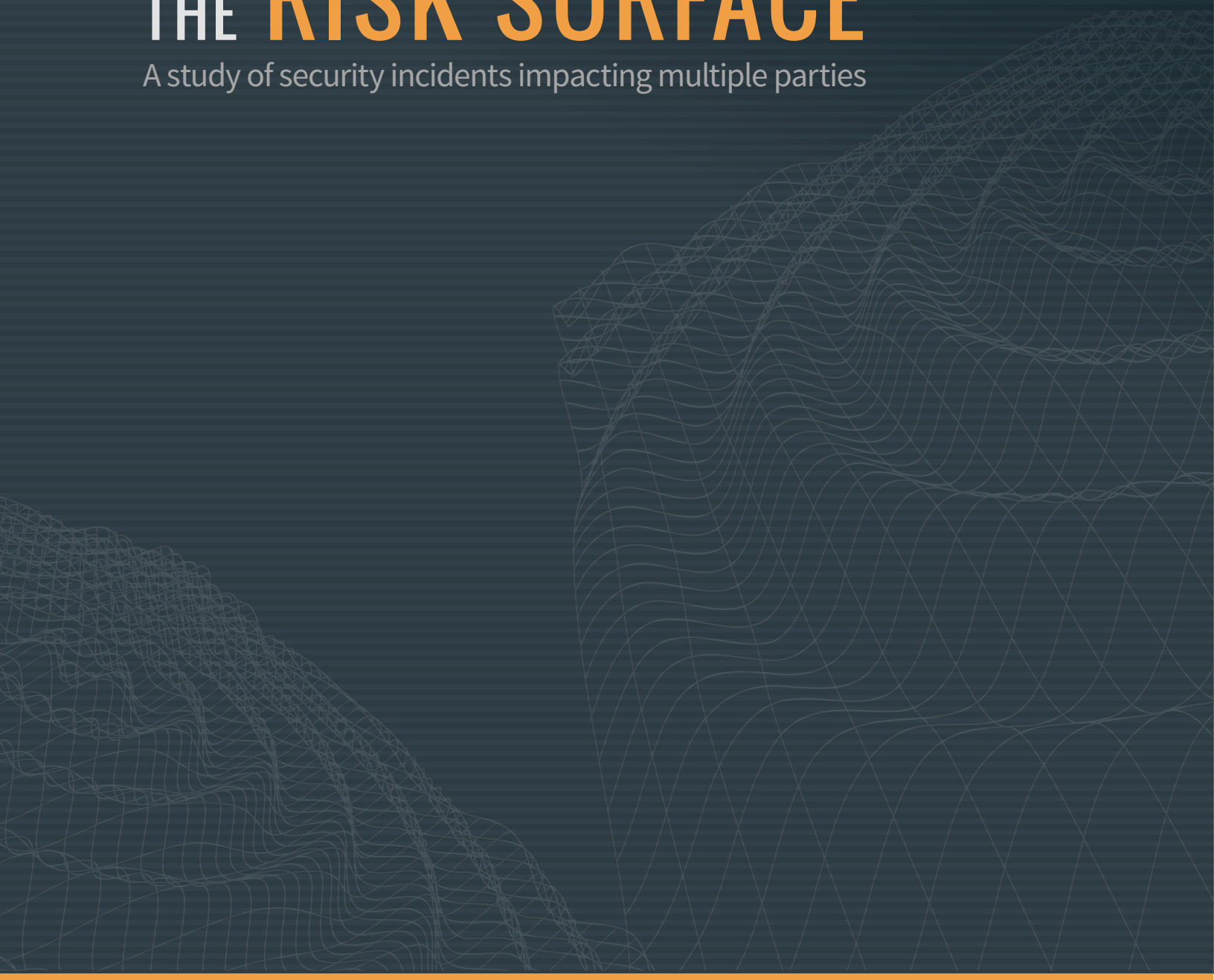
RIPPLES ACROSS THE RISK SURFACE

A study of security incidents impacting multiple parties



A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon™

Cyentia INSTITUTE

This research was commissioned by RiskRecon to study how security incidents affect third-party risk.

The Cyentia Institute obtained the primary data from an independent source (Advisen), conducted the analysis, and drafted this report.

Table of Contents

HAVE COMMENTS OR QUESTIONS ABOUT THIS REPORT?

We'd be glad to discuss them. No, really—we love this stuff! RiskRecon and the Cyentia Institute can be reached via the methods shown below.

RiskRecon: info@riskrecon.com or @riskrecon on Twitter

Cyentia: research@cyentia.com or @cyentiainst on Twitter

OVERVIEW

Introduction & Key Findings

This report analyzes independent data gathered on over 800 multi-party cyber incidents observed over the last decade. These so-called "ripple events" are different than traditional security breaches because they don't just impact a single organization, but spawned secondary loss events affecting thousands of organizations downstream in the supply chain. Multi-party loss events are in part enabled by the extensive network of third party dependencies and exposures explored in the Internet Risk Surface Report published earlier this year by Risk Recon and the Cyentia Institute. We demonstrate that multi-party losses are increasing in frequency and that losses incurred by these ripple events are much higher than single-party incidents. Here's a quick view of the key findings:

Key Findings

- The median financial loss from multi-party cyber incidents—events that impact not only the primary victim firm but multiple third parties as well—is 13x larger than losses from single-party incidents. Extreme losses (95th percentile) show an even larger discrepancy ($16M for single-party incidents vs. $417M for multi-party incidents).
- These multi-party incidents, which we also call "ripple events," are becoming more common over time. Their frequency has been increasing at an average annual growth rate of 20% since 2008. We can't help but see in this trend the influence of hyper interdependency among organizations in the modern era.
- We identified 813 multi-party incidents that generated a total of 5,437 downstream loss events. Adjusting for repeat victims, those entities impacted downstream outnumber primary victims by over 800%!
- While the average ripple event impacts fewer than 10 firms beyond the original victim, they can swell much wider than that. The largest we examined encompassed 131 organizations.
- Collection agencies, banks and lenders, credit bureaus, government offices, and IT firms account for half of organizations that generate ripple events. Along with hotels and hospitals, they're most often impacted by those events as well.
- SMBs are more likely to be on the receiving end of multi-party incidents originating from larger enterprises. Given that small firms already struggle with security, the fact that they suffer loss from a larger firm's incident adds insult to injury.
- Our analysis reveals little difference between losses reported by primary and secondary victim organizations of a cyber incident. This suggests that another firm's breach could impact your organization just as much (or worse) than a breach of your own systems.

PART 1

Defining Multi-Party Cyber Incidents

Studies of third party or multi-party cyber incidents are not new. For instance, Verizon's Data Breach Investigations Report (DBIR) has reported statistics on the involvement of third parties in breaches since it's beginning in 2008. The latest edition of the DBIR attributed 2% of the 2,000+ breaches examined to partners of the victim firm, a rate that stays fairly consistent over the last decade. The DBIR also reports that 5% of breaches involved multiple parties, but that percentage refers to multiple threat actors (e.g., an insider colluding with outsiders) rather than victim organizations. The report historically ties an even larger proportion of breaches to exploited third-party remote access services or credentials.

It's important to establish that the DBIR and other similar sources analyze breaches for which trusted partners play a causal or contributing role. They do not examine how cybersecurity incidents impact the numerous 3rd/4th/Nth parties that share some type of business relationship with the primary victim organization. We call these multi-party incidents and related downstream losses "ripple events," reflecting how the effects of an event spread outward from the central organization to disrupt ecosystems that are often not thought to be connected. Examining these ripple events and raising awareness of these deep connections among organizations is the goal of this report.

To accomplish that goal, we leverage Advisen's Cyber Loss Database, which contains over 90,000 cyber events collected from publicly verifiable sources. The database is widely used, but two features make it uniquely suitable to this research: 1) It associates organizations involved in or impacted by a common incident, and 2) it tracks losses disclosed publicly in the wake of those events. Since 2008, more than 2,300 incidents in the Advisen database involve more than one organization. In the spirit of studying true "multi-party" cyber loss events, we focus on 813 incidents that impacted at least three organizations. Read on to discover what we learned from studying these ripple events.

IMPORTANT TERMINOLOGY FOR THIS REPORT

Cyber Incident: Event that compromises the confidentiality, integrity, or availability of an information asset.

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

Downstream Loss Event: Direct or indirect losses incurred by parties beyond the central victim organization in a cyber incident. These impacted parties generally share a business relationship with the primary victim.

Third Party: We adopt the colloquial usage of this term to refer to any 3rd/4th/Nth party relationships.

[1] According to Advisen's categorization, 45% of those events are data breaches, 44% are various privacy violations and disclosures, 10% are service disruptions, with the remaining <1% a smattering of other causes. We make no attempt to redefine those categories or do additional root cause analysis on these incidents. We leave that for future research.

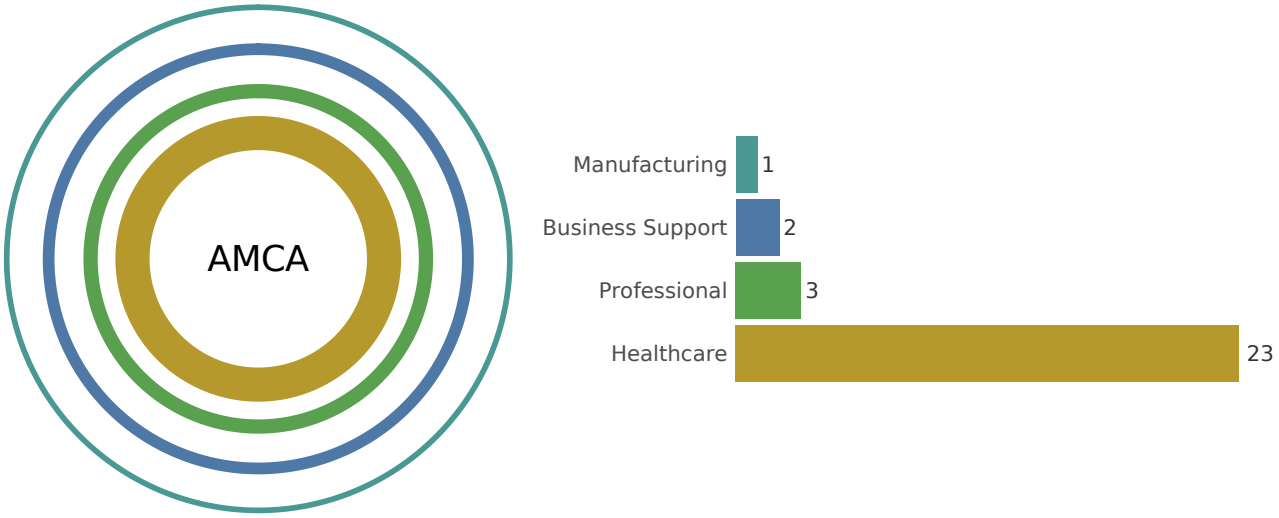
PART 2

Multi-Party Incidents in the Headlines

Before diving into the broad statistics and trends, a close examination of real-world incidents that triggered impacts across multiple other parties will add useful context to our investigation. We'll focus on a recent breach that's still rippling outward, and then briefly look at one where the effects have, for the moment, run their course. We don't intend to blame and shame here, so please read this section without those connotations.

In May of 2019, the American Medical Collection Agency (AMCA) disclosed a breach of its systems that compromised the personal information of over 24 million individuals. Most of the individuals affected had no direct relationship with AMCA; they provided their data to various other entities and those entities sent the data to AMCA for debt collection. Even though only AMCA's systems were compromised, those other organizations were caught up in the fallout from the breach.

FIGURE 1: RIPPLE EFFECTS PROPAGATING ACROSS INDUSTRIES FROM THE AMCA BREACH



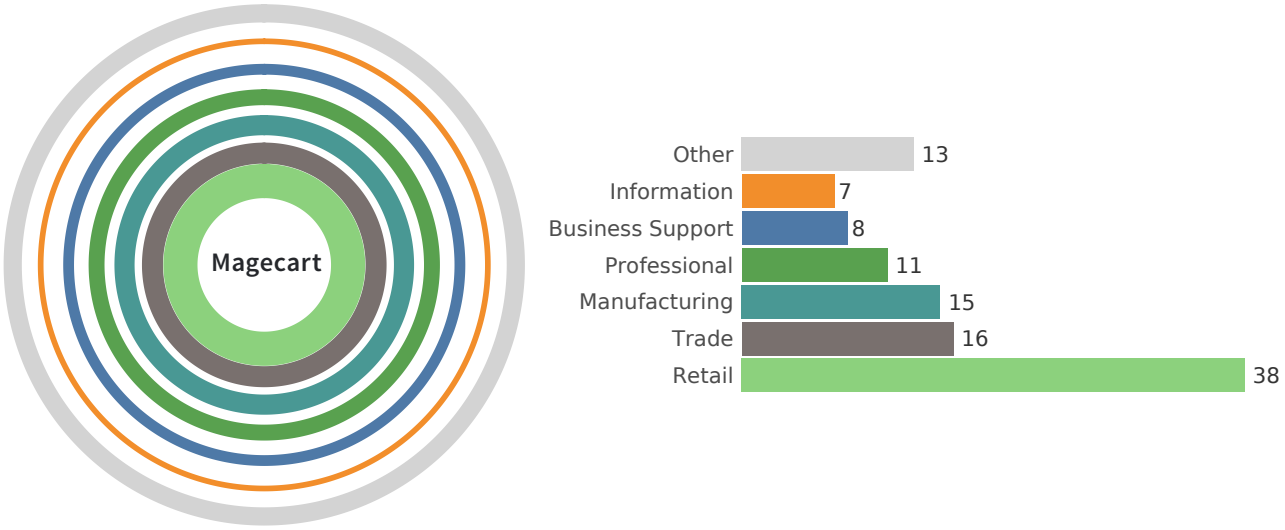
Events like this happen all too often and there's nothing particularly remarkable about the breach itself. It's the ripples propagating outward from AMCA to other firms (and that also crashed back on AMCA) that make it worthy of an example. The dataset records 29 organizations[2] that have suffered known loss events in the wake of the AMCA breach. We don't want to take the ripple metaphor too far, but it is a nice way to conceptualize and visualize these events. Figure 1 shows the central victim in the center of the incident with the ripple effects spreading outward across other sectors. The bars on the right give a count of organizations affected by those ripples within each sector.

[2] It should be noted that the Advisen dataset is not an exhaustive record of every organization involved in the incidents we study, but it is representative of loss events that become public knowledge. As such, counts and losses should be viewed as minimum estimates based on "known knowns."

Letters were sent by several senators to AMCA and multiple companies impacted by the breach, stating concerns about their supply chain management and third-party monitoring processes[3]. As further evidence of downstream liability, several of these entities face costly lawsuits and investigations. These cascading events caused AMCA's parent company to file for bankruptcy, stating "enormous expenses that were beyond the ability of the debtor to bear[4]."From this example, we see that multi-party loss events affect not only the central victim firm, but surrounding third parties as well (not to mention the millions of individuals affected).

Not all multi-party incidents have a clear single central organization, however. One of the larger examples in our dataset (in terms of affected parties) centered around the cybercriminal collective known as Magecart that infamously hacked Ticketmaster in 2018. Although the breach is often attributed to Ticketmaster, the merchant was not compromised directly. Two third-party suppliers of plugins integrated into Ticketmaster's website for payment processing were the source of the breach. Code hosted by those suppliers, Inbenta and SocialPlus, was swapped with malicious scripts that skimmed credit cards processed by Ticketmaster and its affiliates during the period.

FIGURE 2: RIPPLE EFFECTS PROPAGATING ACROSS INDUSTRIES FROM THE MAGECART CAMPAIGN



But the Magecart campaign didn't stop there. By exploiting code hosted by Inbenta and SocialPlus, the actors backdoored their way into numerous online retailers as well. Figure 2 shows industries experiencing the ripple effects of the Magecart campaign, with retailers and wholesalers closest to the epicenter. Those breaches continued to reverberate through supply chains to affect a wide variety of organizations shown in the figure. This demonstrates the diverse and sprawling nature of third-party relationships and why multi-party incidents like the ones we analyze in this paper are critical to understand.

[3] Source HealthIT article: https://healthitsecurity.com/news/sens.-demand-amca-quest-labcorp-explain-failure-to-detect-breach
[4] Source HealthIT article: https://healthitsecurity.com/news/amca-files-chapter-11-after-data-breach-impacting-quest-labcorp

PART 3

Analyzing Multi-Party Cyber Incidents

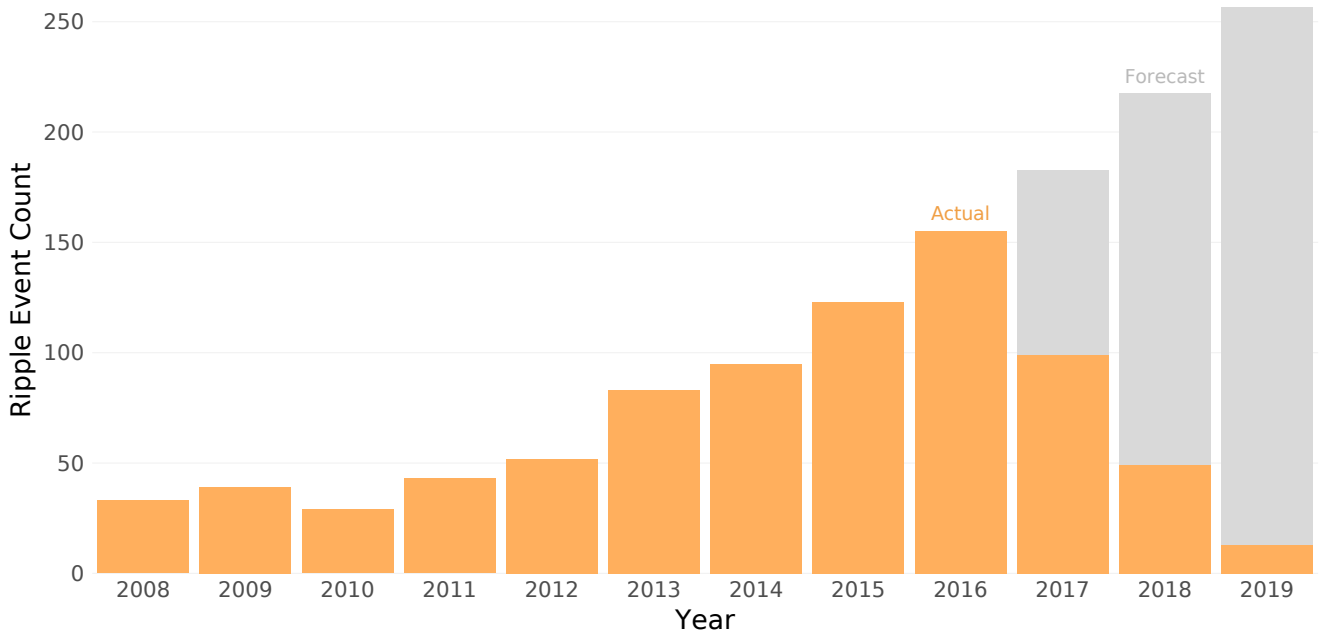
We've reviewed two examples of multi-party incidents, but what about the other 811 in our dataset? This section provides an analysis of the frequency, scope, industries, and impact of these ripple events. Our analysis will provide ample evidence to make solid recommendations about how organizations can better prepare for multi-party incidents.

How common are multi-party incidents?

We suspect that many—perhaps even most—cyber incidents impact organizations beyond the central victim to some degree. But those distal impacts often do not become public knowledge and are therefore never linked to the primary incident. Advisen attempts to associate such incidents and related loss events across all known parties and, as previously mentioned, their cyber loss dataset contains 813 incidents affecting three or more organizations since 2008. We believe this number falls well short of the actual frequency of multi-party incidents, but that does not mean we can't draw any conclusions about the frequency of multi-party incidents from the data at hand.

Figure 3 depicts the number of recorded multi-party incidents each year with orange bars. Don't let the apparent decline after 2016 fool you; it's an artifact of the discovery process rather than an actual trend. While approximately 75% of all incidents enter into the Advisen data feed within a year of occurrence, establishing the relationships among them takes longer. Only about 25% of ripple events are recorded within a year of occurrence, while another quarter enter the dataset within four years, and a good number of incidents that happened a decade ago have only recently come to light.

FIGURE 3: NUMBER OF ACTUAL MULTI-PARTY INCIDENTS (ORANGE) WITH FORECASTS ACCOUNTING FOR RECORDING DELAYS (GRAY)



To account for this delay (and to help prevent misinterpretation), we forecast the number of multi-party incidents expected for 2017 through 2019 based upon historical discovery, disclosure, and data lag. The gray bars reflect those forecasts, showing that far from slowing down, the number of ripple events is only increasing.

The main takeaway here is that multi-party incidents appear more commonplace over time. They've increased at an average rate of 20% per year based on the known data at hand. We may not know the upper limit of how many multi-party incidents are occurring, but the trend is clear in Figure 3. We can't help but see in those rising numbers the influence of the incredible amount of interdependencies that exist among organizations in the modern era.

How large are multi-party incidents?

Given our topic of study, it's appropriate to ask exactly how many parties these multi-party cyber incidents typically involve. "Typically" turns out to be a tad challenging here because the number of ripples per event is heavily skewed. But let's get some overall numbers first.

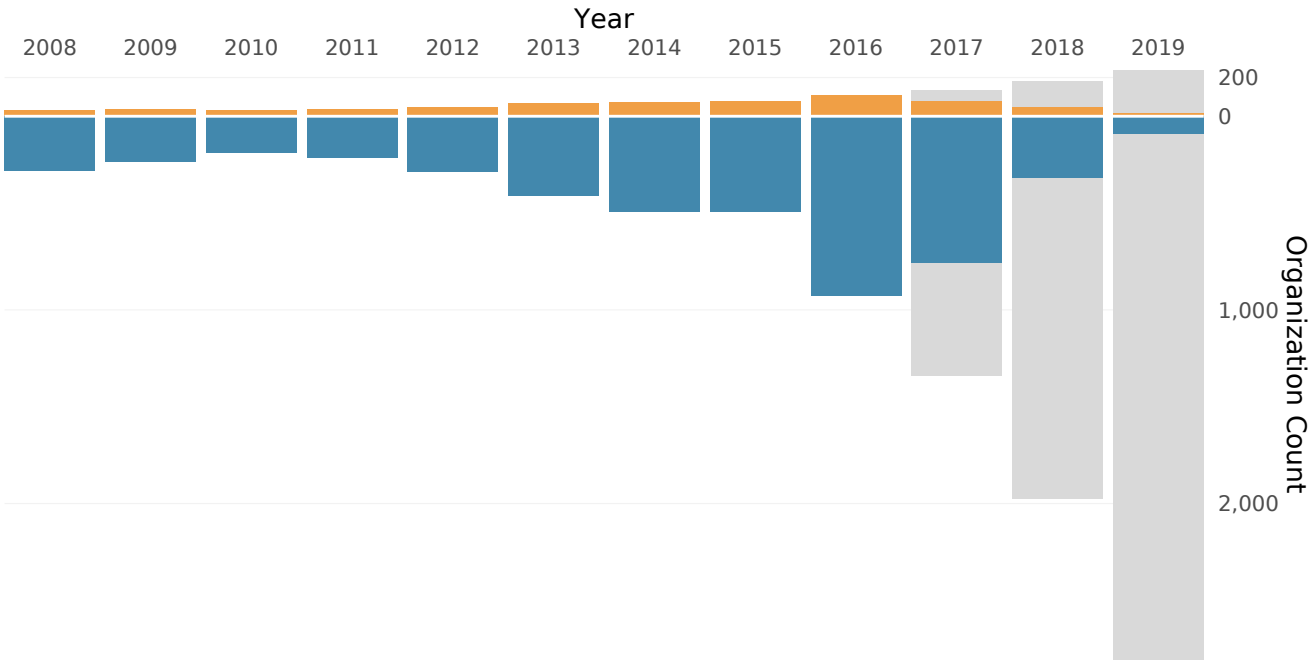
The 813 multi-party incidents identified in the dataset generated a total of 5,437 downstream loss events. Quite a few of these involved repeat victims on both the source and receiving ends of the ripples. Adjusting for that, we identified 512 unique firms central to the incident and another 4,180 unique organizations that experienced losses because of those incidents. That makes for a rather startling comparison—downstream entities affected by multi-party incidents outnumber primary victims by over 800%! We've known for a long time that cybersecurity management was plagued by externalities, but these findings cast a whole new light on that challenge.

FIGURE 4: NUMBER OF CENTRAL VS. DOWNSTREAM ORGANIZATIONS AFFECTED IN MULTI-PARTY INCIDENTS

The imbalance between central and downstream victim organizations in ripple events brings a realization that the annual frequencies from Figure 3 on the previous page paint only part of the picture. Figure 5 extends our forecasting from the base number of multi-party incidents to the total number of firms reporting loss events in their wake.

This perspective better captures how things look from further down the supply chain. The top portion carries over from Figure 3, depicting the number of central victims of multi-party incidents each year. It's barely visible at this scale because the bottom portion tallies the much-larger number of downstream organizations reporting loss events tied to those incidents. From this, it's readily apparent that the ripples from these events spread much wider than where the initial impact breaks the surface.

FIGURE 5: NUMBER OF ACTUAL AND FORECASTED GENERATORS OF RIPPLE EVENTS (TOP) VS. FIRMS IMPACTED DOWNSTREAM (BOTTOM)



Now that we have a good sense of why these events are important for organizations trying to manage their risk posture, let's return to measuring the size of particular ripple events. On average, each of the multi-party incidents we examined affected seven organizations. The largest event in the dataset impacted 131 firms, indicating a very long-tailed distribution. Those statistics vary somewhat among industries, but they share the same general pattern: ripple events typically impact a handful of firms but can swell to envelop scores of third parties.

Which sectors are involved in ripple events?

If the last section left you wondering what types of organizations are typically involved in multi-party loss events, you're in luck! That's exactly where we're headed now, starting with the sectors that generate the most ripple events.

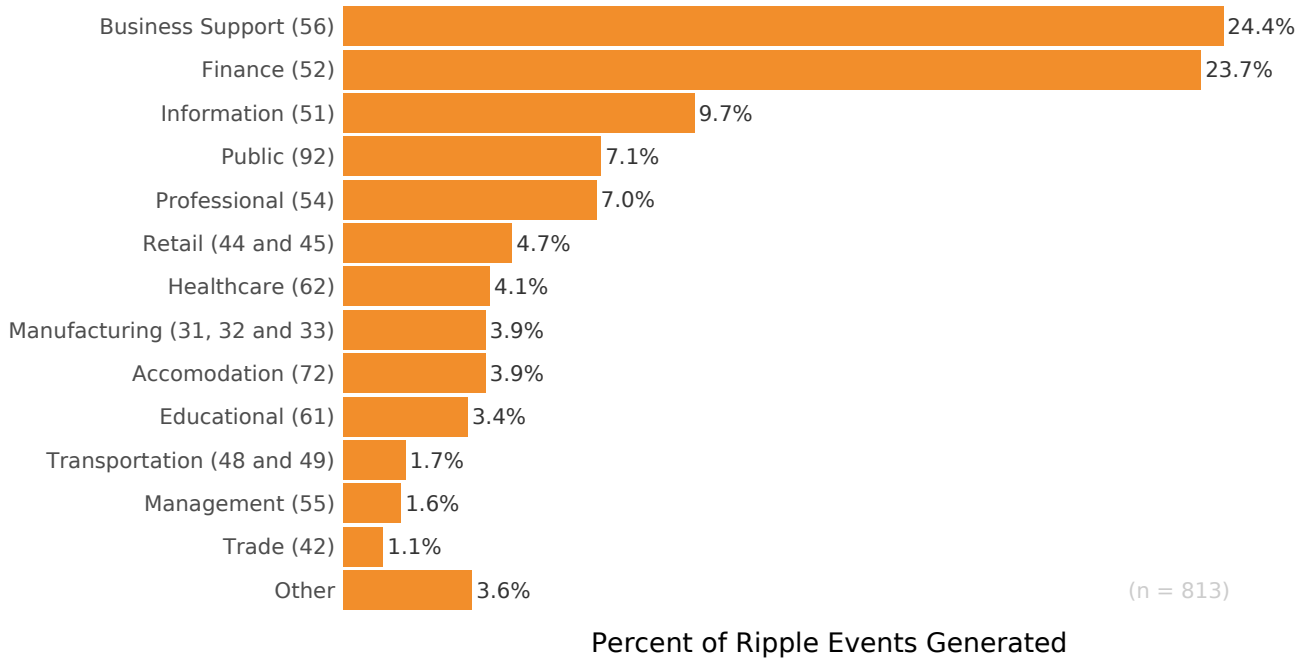
INDUSTRY CLASSIFICATIONS USED IN THIS REPORT

We adopt the North American Industry Classification System (NAICS) for this analysis. We do this because it is widely used, well documented, and conveniently integrated into Advisen's cyber loss data. NAICS codes are comprised of six digits that roll up into top-level (two-digit) sectors and (three-digit) subsectors. So, when we use the label "Finance (52)" in Figure 6 on the following page, we're referring the Finance and Insurance sector that has the top-level NAICS code of 52. The NAICS site contains descriptions and examples of all sectors, sub-sectors, and industries for those wanting more information on what we present here.

With the exception of Administrative Services (56), we use the top-level sector in the NAICS hierarchy. Because all organizations in that sector fell into the same subsector, Business Support Services (5614), we opted to label it "Business Support" to be more specific.

In Figure 6, we categorize organizations central to the 813 multi-party incidents into high-level NAICS sectors. It's immediately apparent that the Business Support and Finance sectors dominate all others. We understand these sector titles aren't very descriptive, but we'll break them down further in a moment. For now, let's simply recognize that nearly half of all ripple events are generated by just two sectors. The Information and Public sectors comprise the next tier and further establish a pattern of information aggregators at the center of multi-party incidents.

FIGURE 6: SECTORS COMMONLY AT THE CENTER OF MULTI-PARTY INCIDENTS



We dive all the way down to the most granular level of the NAICS hierarchy in Figure 7 to identify specific industries that commonly spawn ripple events. Here we can see that collection agencies, commercial banks, and credit bureaus sit firmly on top. Scanning down the list reveals quite a few others from the Finance (52) and Business Support (56) sectors, further strengthening our earlier observation that such firms control gobs of our personal information. Comforting, isn't it?

"THE SECTORS SHOWN IN FIGURE 6 DON'T MATCH MY INTUITION..."

Aside from confusing NAICS labels, the ordering of Figure 6 may strike some as odd. Remember that we're not just looking at data breaches here—over 40% of the incidents involve privacy-related loss events. Filtering out all events pertaining to the Fair Credit Reporting Act (FCRA), for instance, causes the Business Support sector to drop way down the list. We could focus solely on breaches, but we feel the wider scope is more in keeping with our definition of "risk surface" as anywhere an organization's ability to operate, reputation, assets, legal obligations, or regulatory compliance are at risk.

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 Information (51) sector is well represented in Table 1, with industries that house many of the internet, media, hosting, and software giants that run our online personas and activities. Seeing a trend yet?

As for the types of organizations that tend to run our offline lives, we note examples from the Public (92) and Healthcare (62) sectors. Executive offices (federal, state, and local) and various government support comprise the bulk of multi-party incidents originating from the Public sector. Hospitals are the lone representative from Healthcare that make the cutoff in Table 1. Review the rest as you like, and keep the NAICS site handy for those less-than-intuitive industry designators.

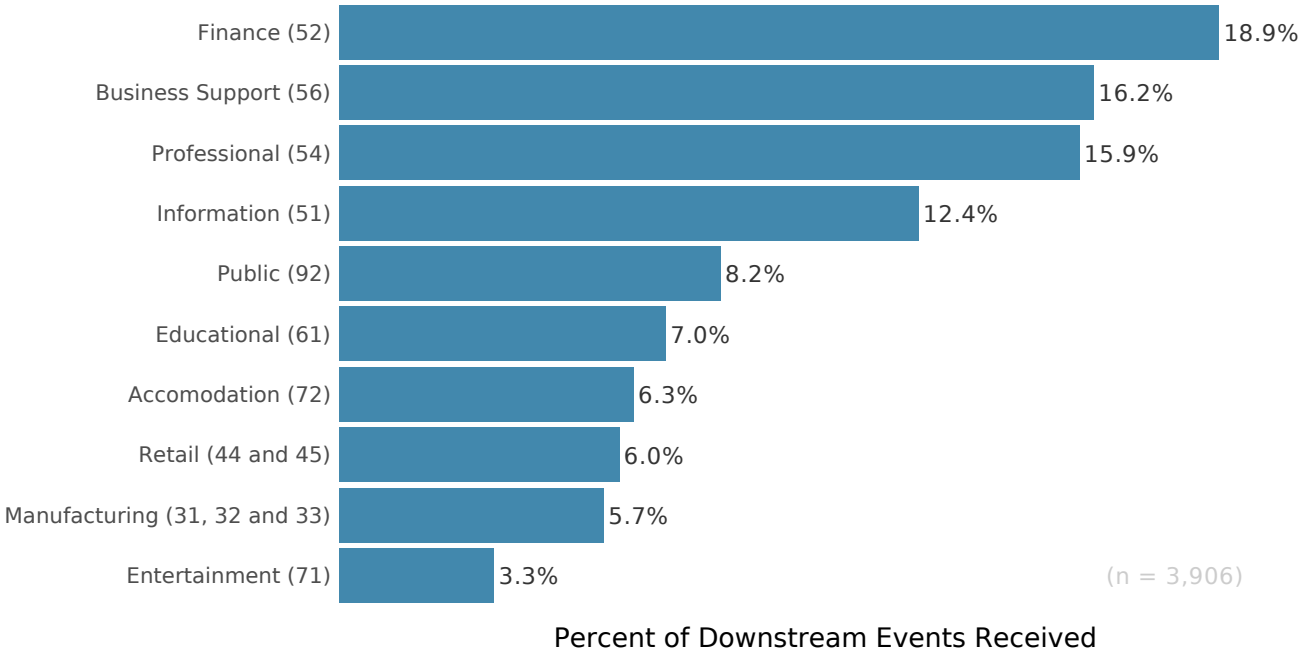
TABLE 1: SPECIFIC INDUSTRIES COMMONLY AT THE CENTER OF MULTI-PARTY INCIDENTS

Industry (NAICS sector code)	Ripple Events	Percent of All Ripple Events
Collection Agencies (56)	109	13.4%
Commercial Banking (52)	81	10.0%
Credit Bureaus (56)	64	7.9%
Executive Offices (92)	30	3.7%
Computer Systems Design and Related Services (54)	26	3.2%
Internet Publishing and Broadcasting and Web Search Portals (51)	23	2.8%
Other Nondepository Credit Intermediation (52)	22	2.7%
Other General Government Support (92)	20	2.5%
Credit Card Issuing (52)	19	2.3%
Hotels (except Casino Hotels) and Motels (72)	17	2.1%
Colleges, Universities, and Professional Schools (61)	15	1.8%
General Medical and Surgical Hospitals (62)	15	1.8%
Wired and Wireless Telecommunications Carriers (eff from 6/15/2002) (51)	14	1.7%
Management of Companies and Enterprises (55)	13	1.6%
Restaurants and Other Eating Places (72)	13	1.6%
Software Publishers (51)	13	1.6%
Credit Unions (52)	10	1.2%
Direct Life, Health, and Medical Insurance Carriers (52)	10	1.2%
Management Consulting Services (54)	9	1.1%
Other Activities Related to Credit Intermediation (52)	9	1.1%
Automobile and Light Duty Motor Vehicle Manufacturing (33)	8	1.0%
Office Administrative Services (56)	8	1.0%

While it's easy (perhaps too easy) to focus on where ripple events originate, it's likely more relevant for risk managers to consider who gets caught up in their wake. Figure 7 starts our exploration of this world, depicting the sectors most commonly impacted by multi-party incidents.

The top three carryover from the list of frequent generators, which isn't too surprising when you think about it. These organizations collect a huge amount of valuable information, typically have large digital footprints, and maintain extensive third-party relationships. A breach of one often reverberates to the others.

FIGURE 7: SECTORS COMMONLY IMPACTED DOWNSTREAM IN MULTI-PARTY INCIDENTS



We suspect most readers of this report will want to know if their organization is likely to be on the receiving end of ripple events. Because of this, Table 2 gives a long listing of industries prone to downstream losses from multi-party incidents. Rather than offering commentary on each industry, we'll just make a general observation that we again see the reflection of third-party and supply chain dependencies throughout these results. We apologize if your industry or one like it isn't listed—but that's actually a good thing. That absence doesn't mean your organization will never be impacted by the security failures of others, but it does suggest history is your side.

TABLE 2: SPECIFIC INDUSTRIES COMMONLY IMPACTED DOWNSTREAM IN MULTI-PARTY INCIDENTS

Industry (NAICS sector code)	Downstream Loss Events from a Ripple	Percent of All Ripple Events
Credit Bureaus (56)	411	9.3%
Commercial Banking (52)	339	7.7%
Hotels (except Casino Hotels) and Motels (72)	176	4.0%
Computer Systems Design and Related Services (54)	124	2.8%
Collection Agencies (56)	109	2.5%
General Medical and Surgical Hospitals (62)	103	2.3%
All Other Support Services (56)	101	2.3%
Colleges, Universities, and Professional Schools (61)	99	2.2%
Restaurants and Other Eating Places (72)	92	2.1%
Elementary and Secondary Schools (61)	83	1.9%
Offices of Physicians (62)	80	1.8%
Software Publishers (51)	71	1.6%
Wired and Wireless Telecommunications Carriers (eff from 6/15/2002) (51)	68	1.5%
Other General Government Support (92)	67	1.5%
Other Nondepository Credit Intermediation (52)	67	1.5%
Internet Publishing and Broadcasting and Web Search Portals (51)	66	1.5%
Credit Unions (52)	63	1.4%
Executive Offices (92)	61	1.4%
Management Consulting Services (54)	54	1.2%
Financial Transactions Processing, Reserve, and Clearinghouse Activities (52)	50	1.1%
Offices of Lawyers (54)	50	1.1%

While reviewing findings in this section, you may have noticed several industries listed as both generators and receivers of ripple events. In the words of Alan Jackson, we can't help but wonder "who's cheatin' who, who's being true, and who don't even care anymore?" Figure 8 helps untangle that web of relationships at the heart of the interconnected nature of modern business. It displays the top twenty (as measured by the number of occurrences) pairings among subsectors for multi-party incidents. On the left, we have the central subsector of the ripple event and those impacted by it are on the right. The thickness of connecting ribbons corresponds with the volume of loss events flowing between subsectors.

FIGURE 8: TOP PAIRINGS AMONG CENTRAL AND DOWNSTREAM SUBSECTORS IN MULTI-PARTY INCIDENTS[5]

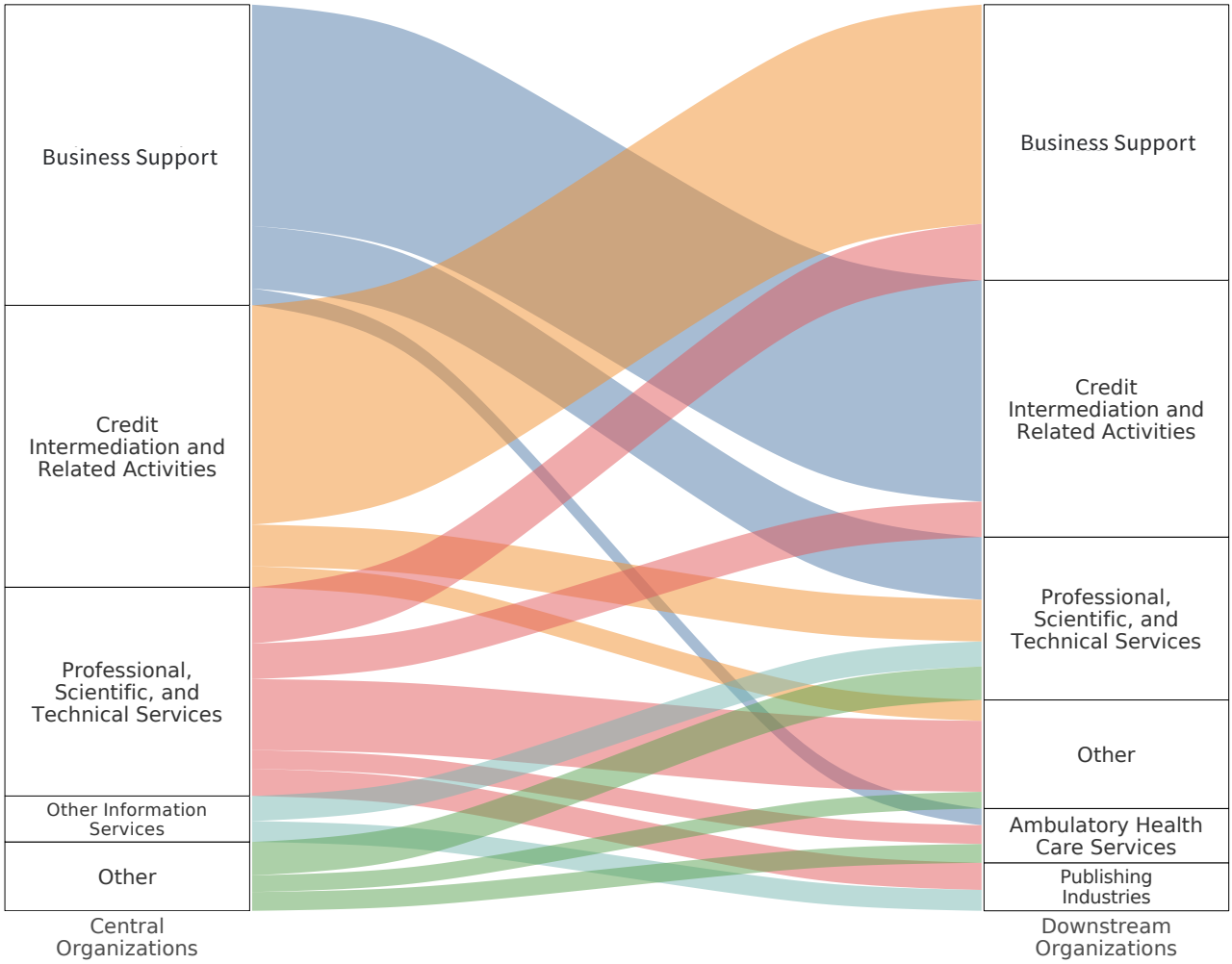


Figure 8 displays the top twenty pairings among subsectors for multi-party incidents. On the left, we have the central subsector of the ripple event and those impacted by it are on the right. The thickness of connecting ribbons corresponds with the volume of loss events flowing between subsectors.

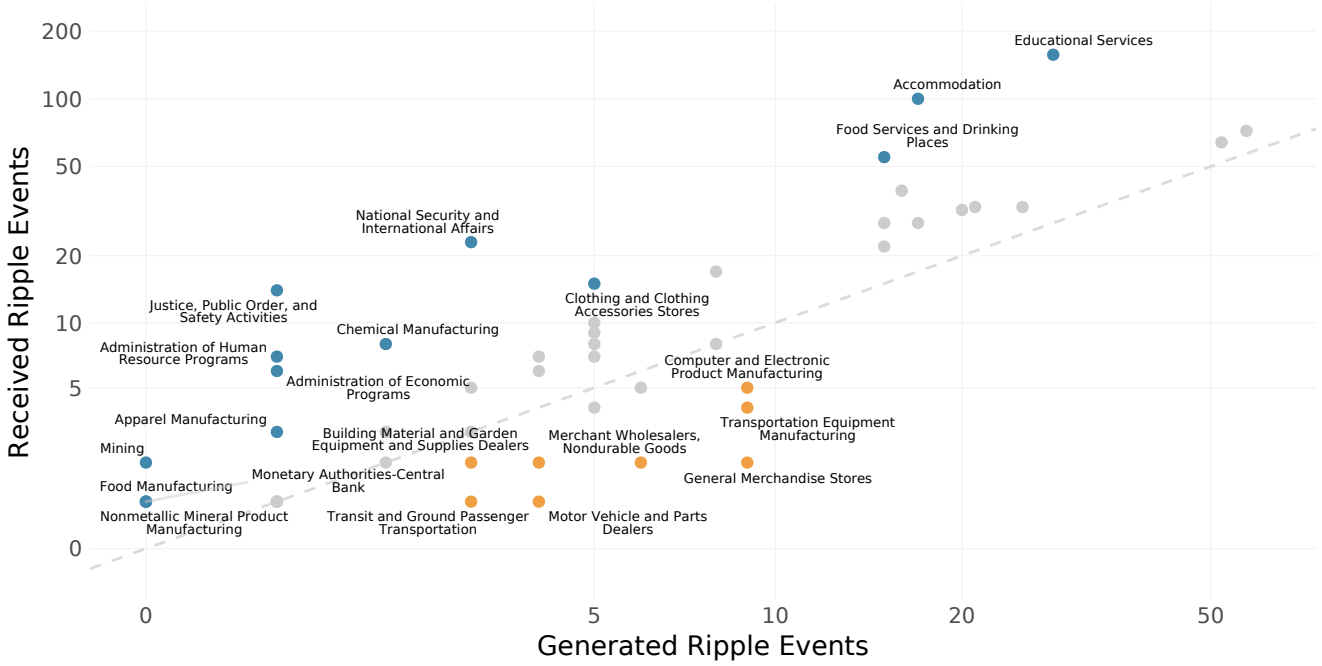
There are several takeaways from this chart for those able to parse the NAICS designations. First, the Business Support Services (5614) subsector has deep connections to the Credit Intermediation and Related Activities (522) subsector. That basically says incidents among credit bureaus and collection agencies (521) frequently propagate to banks and credit card issuers (522) and vice versa. Those interactions make sense when viewed as an ecosystem.

It's interesting to see the many ripples flowing into Professional, Scientific, and Technical Services (541). By nature of providing services to organizations of all types, losses affecting that subsector come from all different directions. That's an important angle to consider if your organization maintains a diverse array of customer and third-party relationships.

[5] Figure 8 focuses on multi-party events where the central and at least one of the downstream organizations lie in different subsectors. That excludes roughly 20% of the connections between the central organization and the downstream firms. Another way of expressing this would be that 4 out of 5 firms impacted in a ripple event are from subsectors outside of that of the central organization.

This line of analysis caused us to wonder about the balance between upstream and downstream involvement in multi-party incidents. Figure 9 plots subsectors according to the number of ripple events they generate vs. the number they receive. It's apparent that few tend appear to appear exclusively on one or the other side of that line. Subsectors along the dotted line (gray) balance giving and receiving. Those well above the line (blue) often get the wrong end of the stick, while those falling below the line (orange) routinely jab others with it (though usually by accident).

FIGURE 9: RATIO OF CENTRAL VS. DOWNSTREAM RIPPLE EVENTS BY SUBSECTOR



Do ripple events affect large or small firms?

You probably already guessed the answer to this one; it's both. Despite the title, it isn't so much a question of "or" but rather "more or less." Organizations of all sizes have at least some history of involvement in multi-party cyber incidents. Figure 10 makes a distinction between central and downstream organizations in ripple events based on the number of employees. It carries several important messages.

We'll start above the horizontal line in Figure 10 with a size breakdown of firms that spawn cyber incidents affecting third parties. The steady rise in events generated as organizations grow from SMBs to large enterprises is one of the starkest indicators of ever-increasing complexity of third party networks. As organizations grow and their supply chains become more complex, the difficulties of managing these vital relationships grow at a pace that often doesn't match the security and risk management capabilities at these organizations. Colloquially, we see that security practices lag the maturation of other core business practices.

FIGURE 10: NUMBER OF CENTRAL VS. DOWNSTREAM RIPPLE EVENTS BY ORGANIZATION SIZE (EMPLOYEE COUNT)

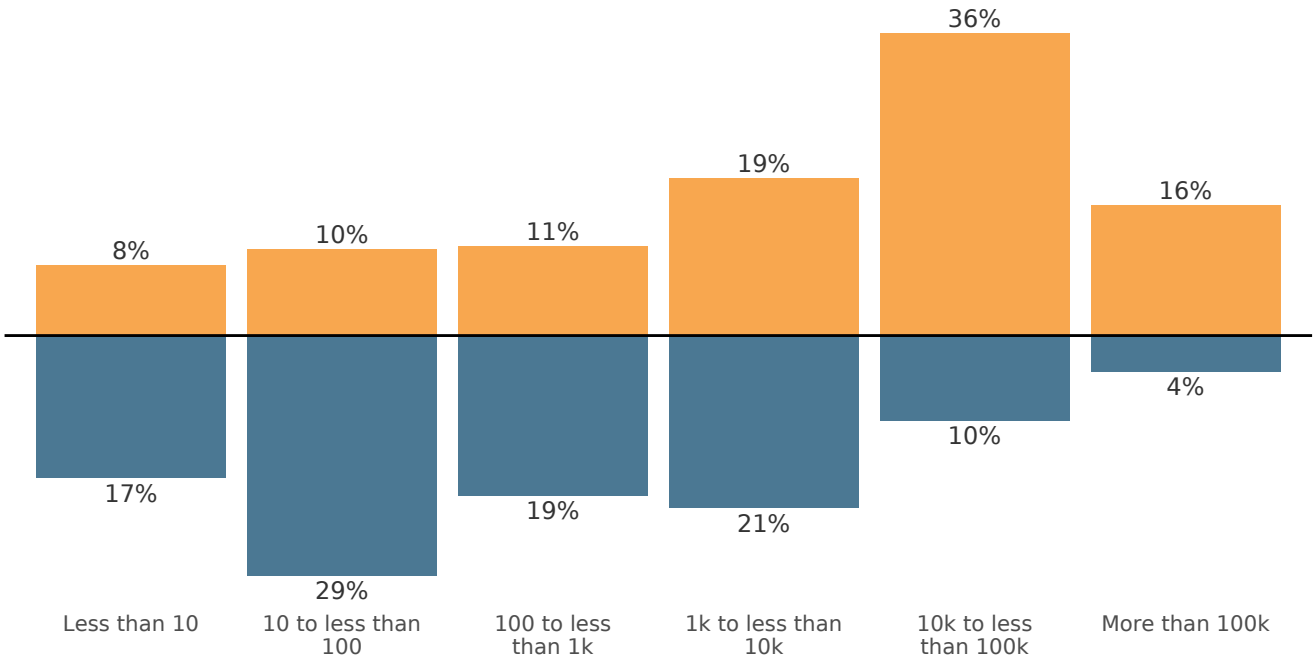


Figure 10 makes a distinction between central and downstream organizations in ripple events based on the number of employees. The top half gives a size breakdown of organizations that spawn cyber incidents affecting third parties (i.e., 8% of central firms in ripple events have less than 10 employees). The bottom half tallies organizations impacted by those ripples (i.e., 17% of downstream firms have less than 10 employees). The top (orange) and bottom (blue) segments horizontally sum to 100%.

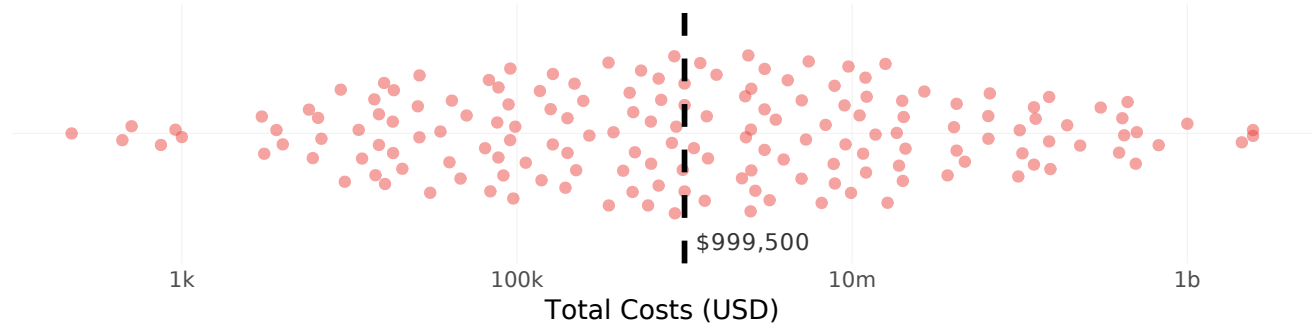
Let's now look below the line, where the story turns full circle. Here we see counts of organizations in each size grouping impacted by multi-party incidents and it's clear that SMBs bear the brunt. This high prevalence of downstream loss events reflects that smaller firms are both more reliant upon larger third-party entities and generally less equipped to handle complex security challenges that go along with those relationships. While large organizations often seek to manage risk by pushing stringent security measures on smaller suppliers, SMBs must realize that they themselves are also at risk from the blowback of incidents affecting their larger customers.

What is the impact of multi-party incidents?

We've covered a lot about ripple events thus far, but we have not yet addressed what is perhaps the biggest factor in assessing their risk—the magnitude of associated losses. It's obvious that multi-party incidents occur with some frequency and we now know more about who's involved in them, but without understanding the costs incurred it's hard to put them in proper context with a plethora of other security concerns. We seek to give that all-important context in this final section before moving on to some recommendations.

Figure 11 presents a distribution of recorded losses for ripple events. Each dot represents the central incident and all related downstream loss events for each impacted party (the initial splash and all ripples). The distribution appears very normal at first glance, but note that the axis is shown in log scale. That indicates losses from these incidents conform to a lognormal distribution, which should help those trying to model risk.

FIGURE 11: DISTRIBUTION OF TOTAL LOSSES RECORDED FOR MULTI-PARTY INCIDENTS

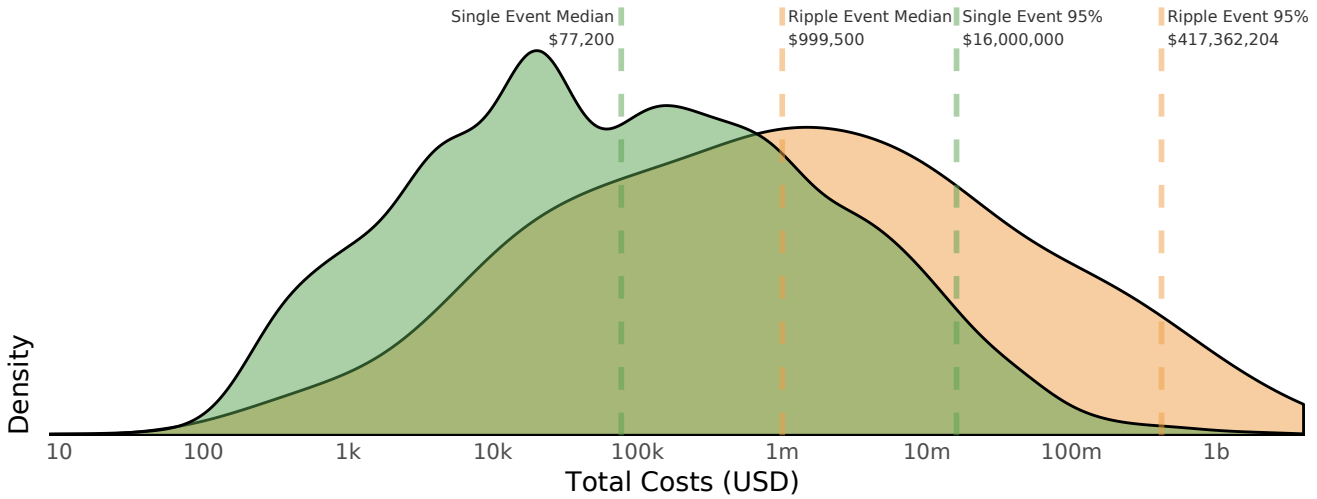


The long-tailed distribution (on a linear scale) also means that taking the average loss isn't going to effectively represent what's typical. The median is a much more appropriate measure of typical costs, and that rings up at about $1 million per incident. Of course, the median just marks the midpoint and it's clear that losses range from sub-$1,000 to over $1 billion. We should also note that many loss events did not specify a value, so these should be viewed as conservative estimates based solely on known/recorded costs.

Armed with a better sense of expected losses from ripple events, two additional questions come to mind. The first relates to how they compare against traditional single-party incidents and the second concerns the relative impact to downstream victims versus those compromised directly.

Figure 12 compares the loss magnitude for single (green) vs. multi-party (orange) incidents. Notice how the distribution for ripple events shifts substantially to the right. The median loss for multi-party incidents is nearly 13x that of single-party incidents. Also notice that the tail is much thicker, indicating higher propensity for major loss events for multi-party incidents. Extreme losses (95th percentile) for ripple events exceed $400 million but fall to a comparably scant $16 million for traditional incidents.

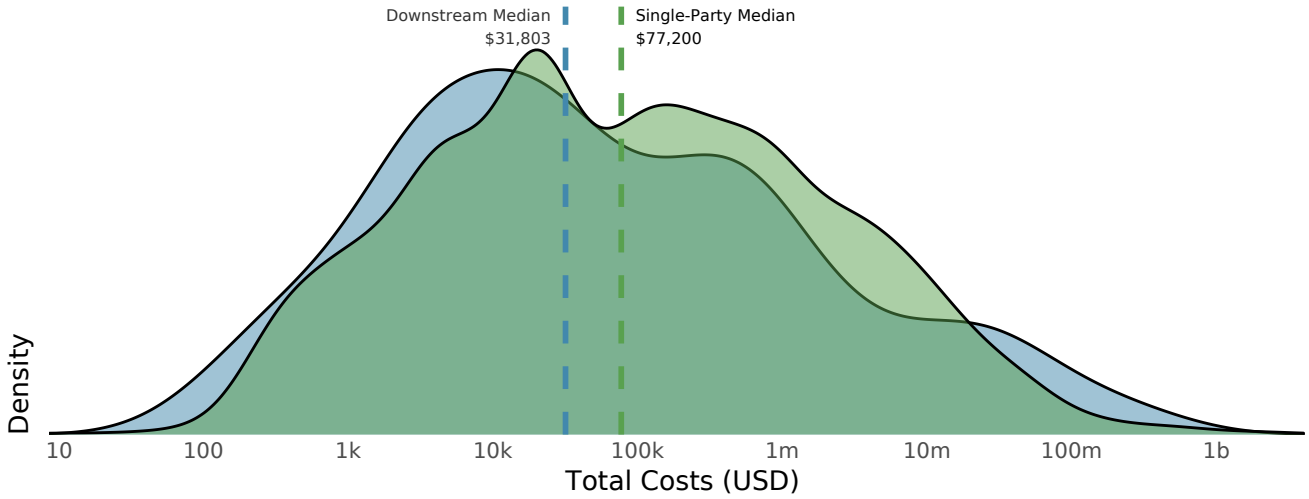
FIGURE 12: DISTRIBUTION OF TOTAL LOSSES FOR SINGLE-PARTY INCIDENTS VS. MULTI-PARTY INCIDENTS



We should recognize that Figure 12 isn't exactly comparing apples to apples. Since we're comparing losses for single vs. multi-party loss events, it's not entirely surprising that the former exceeds the latter. However, the extent of that difference is key. Since downstream victims outnumber central organizations by a factor of 8-to-1 in ripple events, we might expect downstream losses to exceed single party losses by a similar margin. In that light, the fact that downstream losses dwarf upstream losses by 13x seems particularly noteworthy.

Figure 13 addresses our second question, comparing costs to firms compromised directly by single-party incidents (green) vs. those on the receiving end of ripple events (blue). Median losses for direct victims are more than double for downstream victims, but tail risk appears somewhat higher for the latter.

FIGURE 13: DISTRIBUTION OF TOTAL LOSSES FOR SINGLE-PARTY INCIDENTS VS. DOWNSTREAM LOSSES IN MULTI-PARTY INCIDENTS



Despite these minor differences, the big takeaway here is that the loss profiles aren't dramatically different. That means your organization could be impacted equally or worse by another firm's breach as from one that compromises your own systems. This provides good incentive for firms of all types and sizes to be aware of risks associated with multi-party incidents and how to manage them. On that note, let's get to some recommendations for doing just that.

LOOKING FOR A LITTLE SOMETHING EXTRA?

If you'd like more insight into industries that may generate ripple events impacting your organization, we've created an interactive vizualization that allows you to explore common generator-receiver pairings among sectors. Visit www.riskrecon.com/ripples-across-the-risk-surface to highlight your sector in the circular "chord plot" to identify where incidents historically originate.

PART 4

Recap & Recommendations

Having read this report, it should be clear that multi-party cyber incidents aren't something that we, as a digitally-transforming society, can ignore. Does third-party risk deserve a top spot on your organization's risk register? If your crown jewels are resident in the systems of third-parties, perhaps it does. After all, while you can outsource your systems and services, you can't outsource your risk. To that end, we've pulled together some recommendations based on what we learned in this analysis.

1. All risk management, whether internal or third party, starts with asset awareness. Know your third-party providers and partners and the nature of your risk relationship with each. Without knowing who has your data or systems, an incident of passing interest in the morning RSS feed could be the one that just exposed your crown jewels.

2. Manage the risk of your outsourcing relationships and related data with the same rigor as your internal assets. In ripple events, downstream firms are impacted just as if their own systems were compromised. They must file the loss events with regulators, communicate the incident to impacted persons, provide loss compensation, and so forth. In the case of the AMCA breach, AMCA customers came under the scrutiny of Senators for poor third-party risk management.

3. Hold your third parties accountable to a higher standard of performance. Ripple events are growing at a rate of 20% per year. Better third-party accountability can help reverse that trend, but the benefits are directly proportional to the level of visibility you have into their security posture and performance.

4. It is a tall order to ensure that your vendors are actually meeting your cybersecurity requirements. Leverage cybersecurity ratings providers to monitor and assess your third-party relationships. They provide highly curated opensource intelligence that can help inform you of their overall performance and alert you when things go sideways.

5. Modern enterprises are highly interconnected. Financial and Business Support sectors, more than any others, have intricate digital supply chains and information flows. If you are in a sector with a high degree of connections, extra spend on identifying and managing your portfolio of third-party relationships is a good investment.

6. Companies who process data on behalf of other companies likely require more cyber insurance than they currently carry. Multi-party incident losses are typically 13 times larger than single-party incidents.

7. SMBs, which may already be heavily incentivized to accept contracts from larger business, should consider the data and responsibility they take on from their larger enterprise customers and implement wide-ranging measures (assessments, security controls, insurance, contract terms, etc.) to limit their exposure.

8. Third-party relationships are not bad! Oursourcing and productive partnerships can bring new capabilities, improve time-to-market, increase agility, decrease cost, and sharpen organizational focus on core value-adding activities. Third-party risk is unavoidable; those who manage it within tolernances enable business rather than stifle it.

riskrecon™

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 objective, data-driven research that improves cybersecurity knowledge and practice.

www.cyentia.com

A collaborative research project between RiskRecon and the Cyentia Institute

RIPPLES ACROSS THE RISK SURFACE

A study of security incidents impacting multiple parties