RIPPLES ACROSS THE RISK SURFACE

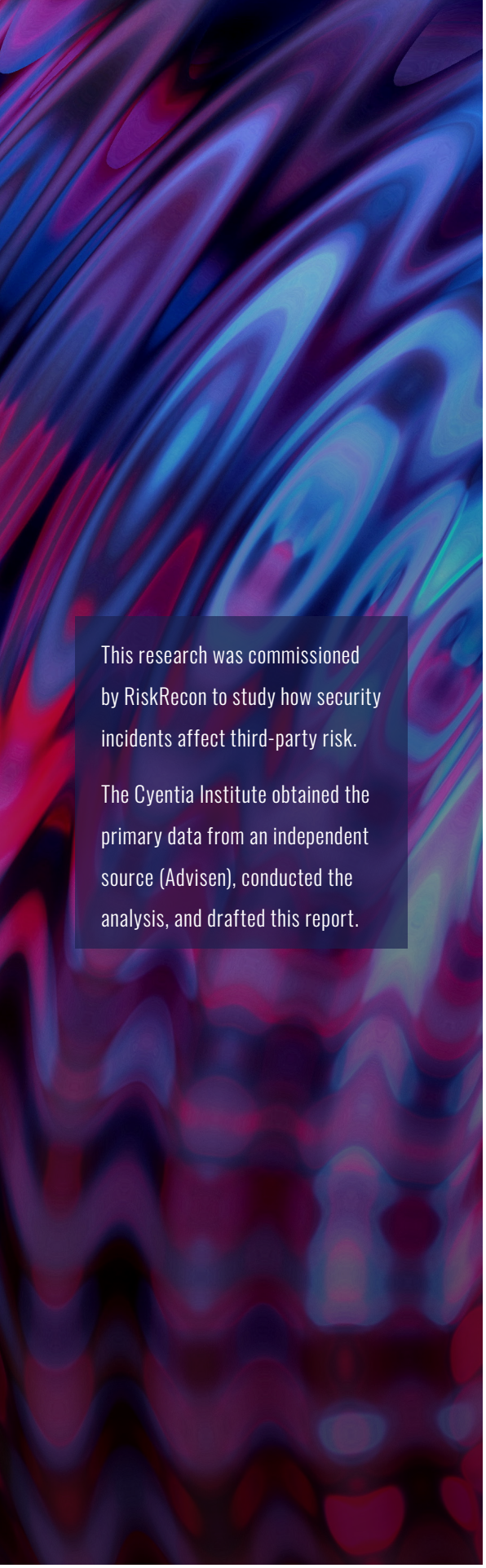
A STUDY OF THE CONTINUING IMPACT OF INCIDENTS AFFECTING MULTIPLE PARTIES

A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon

mastercard

119 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

INTRODUCTION & KEY FINDINGS

Data breaches and security exposures are bad enough when they impact one or two businesses at a time. But in today's interconnected digital world, we're seeing an increasing number of security exposures that create a ripple effect across numerous organizations. The growing body of observational data across more than a decade of publicly reported breaches points to how widely the waves of impact from a security incident at a single organization can spread across industries and other individual organizations.

One breach at a technology service provider, for example, could expose the records of hundreds of their business customers if the system is central to the services they provide. Additionally, the security weaknesses of so-called Nth parties—4th party, 5th party and so on across the business value stream—can and do affect organizations that do not necessarily do business with them directly.

These multi-party security breaches form the basis of this recurring RiskRecon Ripples Across the Risk Surface report, which analyzes all the dimensions of breaches involving three or more interrelated companies. Since our 2019 report on the security ripple effect, the technological world has been shocked by several dramatic examples of the damage a single incident can do, wreaking havoc on many downstream organizations.

The SolarWinds incident stands foremost among them, providing the strongest anecdotal evidence and warning of how a damaging ripple event can unfold. Our argument here is that SolarWinds was not an anomaly or a singular event, and we've got the data and stories to prove it.

In this second edition of the Ripples report, we bolster the evidence gathered in our first analysis of not only the risks associated with third-party direct vendors and partners but also the dangers posed by the rest of the supply chain.

Key Findings

- 897 multi-party breach incidents, also referred to as ripple events, have been observed since 2008.
- 147 newly uncovered ripples were observed across the entire data set, with 108 occurring in the last three years.
- A median ripple breach event causes 10x the financial damage of a traditional single-party breach.
- The worst of the multi-party breach events causes 26x the financial damage of the worst single-party breach.
- It takes 379 days for a typical ripple event to impact 75% of its downstream victims.
- The median number of organizations impacted by ripple events across the data set was 4.

DEFINING RIPPLE EVENTS

In today's technology-led business climate, organizations don't just share information rampantly across company lines—they also share platforms and technology ecosystems. Due to this, multiple organizations end up boating in the same proverbial pond. And when an attacker compromises one organization within an ecosystem, it's like a boulder hitting that pond's surface. The effects from that initial impact cause an outward ripple that threatens to swamp everyone's vessels—or at least get all the passengers wet.

As in the 2019 report, we refer to these ripple events interchangeably as multi-party incidents. For the sake of enumeration and statistical analysis, we define these multi-party incidents as:

> Breaches where there are effects upon three or more firms (the initial victim and at least two others) and where there exists some kind of business-to-business (B2B) relationship between the firms involved.

The mentioned B2B relationship is not necessarily between the initial victim and those caught up in a ripple's downstream loss events. However, the relationships that exist between various upstream and downstream organizations of multi-party incidents distinguish these ripple events from sweeping cybercriminal campaigns that may successfully hit numerous victims who have no other connection between them.

Multi-party impacts can be multifaceted, but there are two primary ways they push ripples across industries and organizations:

WIDESPREAD THIRD-PARTY BREACH: This is a breach impacting multiple downstream organizations that have a direct third-party relationship to the victim organization that generated the ripple event.

SUPPLY CHAIN BREACH: This refers to a breach exhibiting cascading impacts on the generator organization's customers, such that the exposure at one or more third parties also exposes systems or data owned by Nth-party organizations with no direct relationship to the initial victim.

These two categories are not mutually exclusive, and what often happens with larger ripple events is that a breach first impacts the flow to multiple organizations with third-party relationships to the generator and then push downstream to affect many of those organizations' customers and their customers' customers. Thus, many ripple events start as a widespread third-party breach that kicks off multiple supply chain breaches all at once.

This is the kind of scenario we witnessed most recently with the 2021 Kaseya ransomware event, wherein an attacker leveraged management software commonly used by managed service providers to simultaneously attack the client base of multiple companies at once.

THE RIPPLE DATA SET

For the second time in a row, we used Advisen's Cyber Loss Database to uncover the scope of multi-party incidents since 2008. Containing over 103,000 cyber events collected from publicly verifiable sources, the database is widely used for long-term analyses of breaches over the last decade and beyond. Two features that make it particularly apropos for this ripple research is that it associates organizations involved in or impacted by a common incident, and it tracks losses disclosed publicly in the wake of those events.

Since 2008, more than 2,726 incidents in the Advisen database involve more than one organization. However, only a subset of those are true ripple events involving some form of B2B relationships between multiple parties. Using that as a filter, our incident base totaled 897 incidents.

Our goal for the latest analysis of this base was not only to understand how things changed with new ripple events in the last year but also gain deeper insights into the entire data set. We not only performed a different analysis this year to bolster last year's look into over a decade of ripple events but also revisited our previous data observations to account for changes to the data set that might naturally occur over time due to the nature of how ripple events unfold.

Clearly, the relationships between various 3rd, 4th, and Nth parties involved in ripple events can be complex and difficult to track. At times, an organization may be a customer of the generator as well as of other third parties caught in the downstream impact of the ripple. However, a comprehensive mapping of all the connections between firms is not available, preventing us from completely untangling the relationships and providing a crystal-clear analysis of how many ripple events are widespread third-party breaches and how many are also supply chain events.

Nevertheless, the data we do have is sound, and it provides a good sense of how common ripple events are today, the scope of their impact, and the costs of these multi-party incidents on a downstream ecosystem.

IMPORTANT TERMINOLOGY FOR THIS REPORT

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

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

Downstream Loss Event: This refers to direct or indirect losses incurred by parties beyond the central victim organization in a cyber incident; the 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.

Ripple Generator: This term refers to the initial victim of a ripple event.

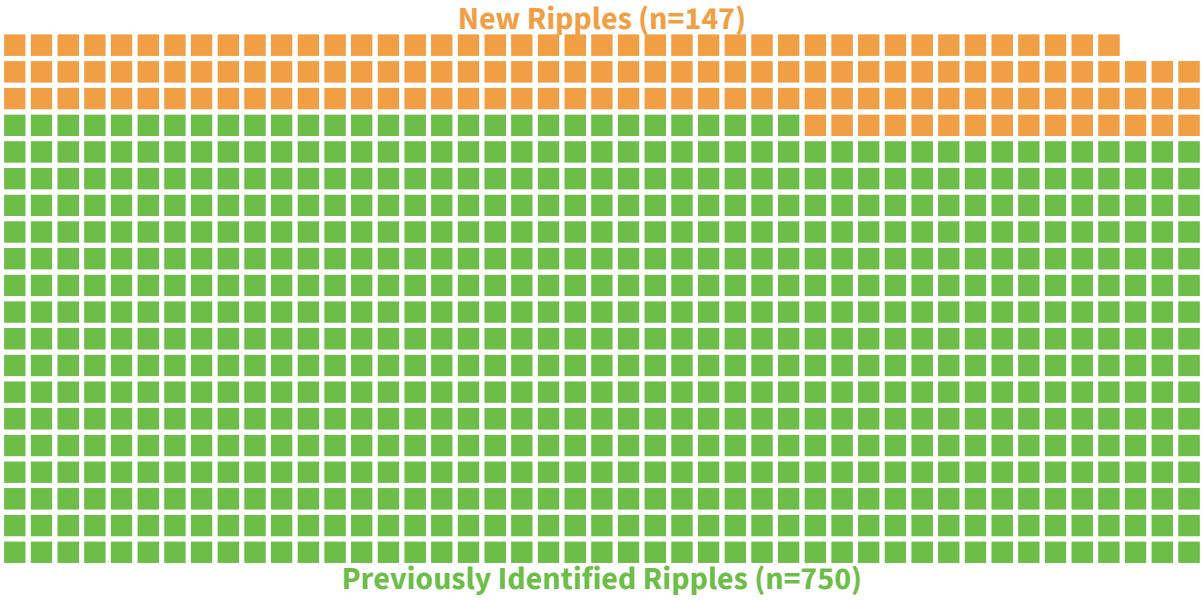
Ripple Receiver: The organizations that are connected to the initial victim and experience a downstream loss event are the ripple receivers.

WHAT'S NEW: RE-ANALYZING RIPPLE INCIDENTS OVER TIME

One of the most difficult elements of analyzing the numbers around ripple events is determining how long it takes for the secondary and tertiary effects of a generating event to progress across multiple organizations, let alone the time it takes to investigate and observe them. For this reason, the observable ripples experienced from 2008 onward comprise a living data set. In this second edition of our analysis, the new data about old incidents that cropped up made it clear that some were not ripple events, making them fall off the list, and other multi-party incidents that happened years ago were added to the tally as new evidence was observed and reported in our source database.

As you can see in Figure 1, based on our analysis in April 2021, 897 multi-party incidents were experienced from 2008 to 2020. Most of those were previously identified ripples.

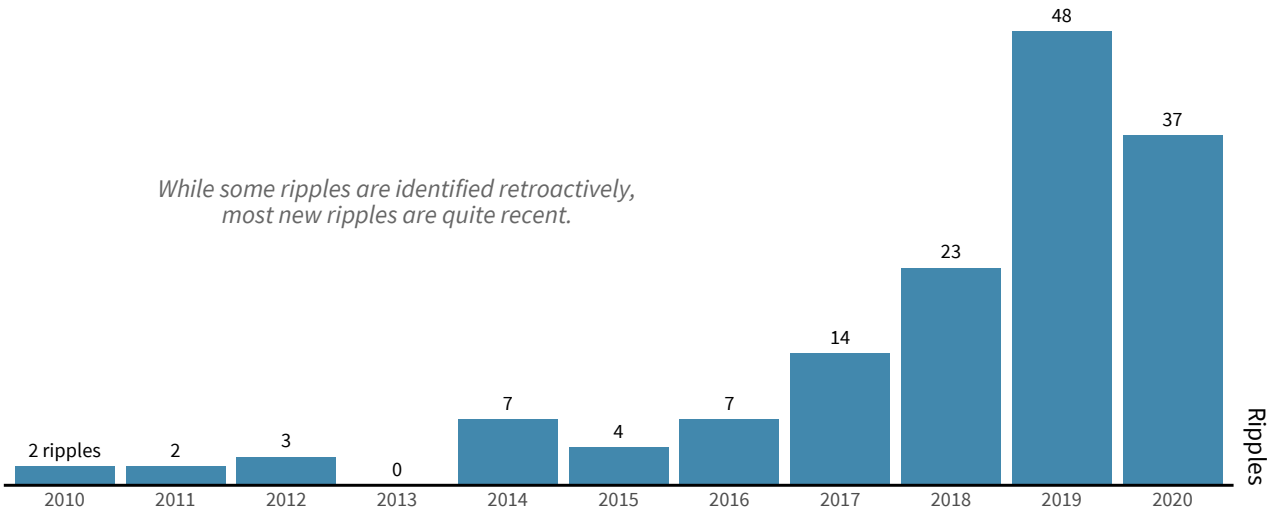
Figure 1: 897 Ripples, New and Pre-existing



Going further back in time for our latest analysis, we observed 147 newly identified ripples across our entire measurement period. Again, this is expected as more and better information about past events becomes available. Unsurprisingly, the biggest increases can be found in recent years, with a good number of events detected in the mid-2010s as well.

One of the most difficult elements of analyzing the numbers around ripple events is determining how long it takes for the secondary and tertiary effects of a generating event to progress across multiple organizations, let alone the time it takes to investigate and observe them.

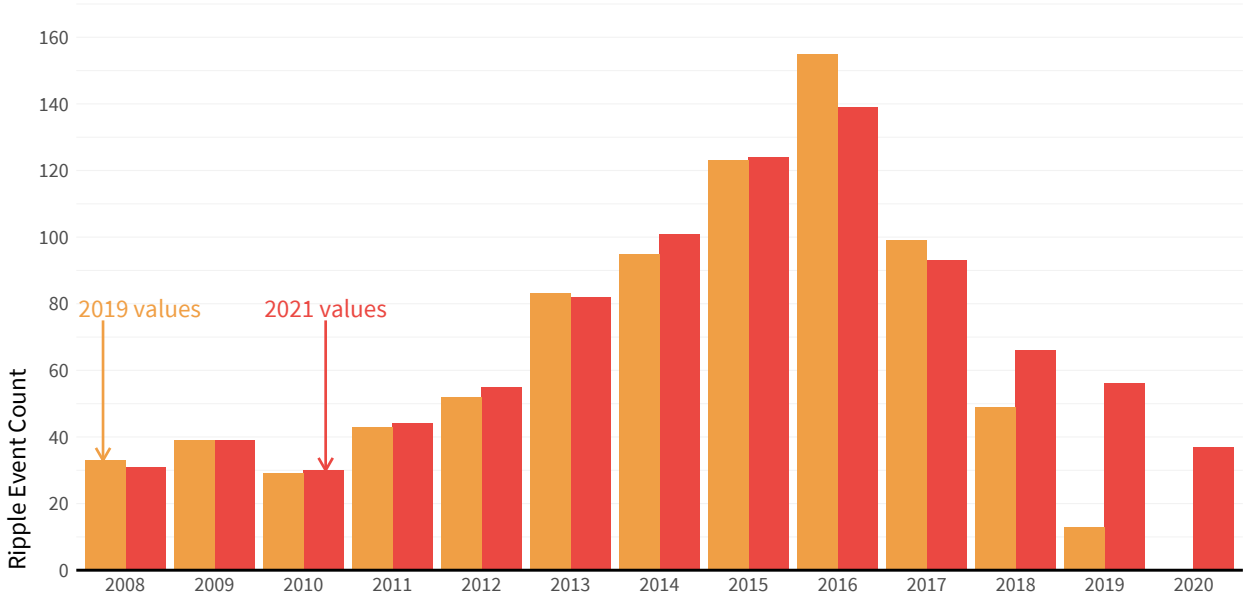
Figure 2: New Ripples Detected Since Last Report



As we can see above, over half of the newly identified ripples were in 2019 and 2020. Our postulation from the last iteration of this report rings true here as we noted then that there's at least a two-year delay for many ripple effects to fully unfold—and, as this chart indicates, it may even take five years or more for them to become apparent. That's likely why we see new events from 2019 outpace those for 2020.

We warned in our first report that this lag in observable ripple effects would make it difficult to accurately forecast multi-party incidents. We dived in nevertheless and took our previous projections to task, as depicted in the chart below.

Figure 3: Revisiting Projected Ripples



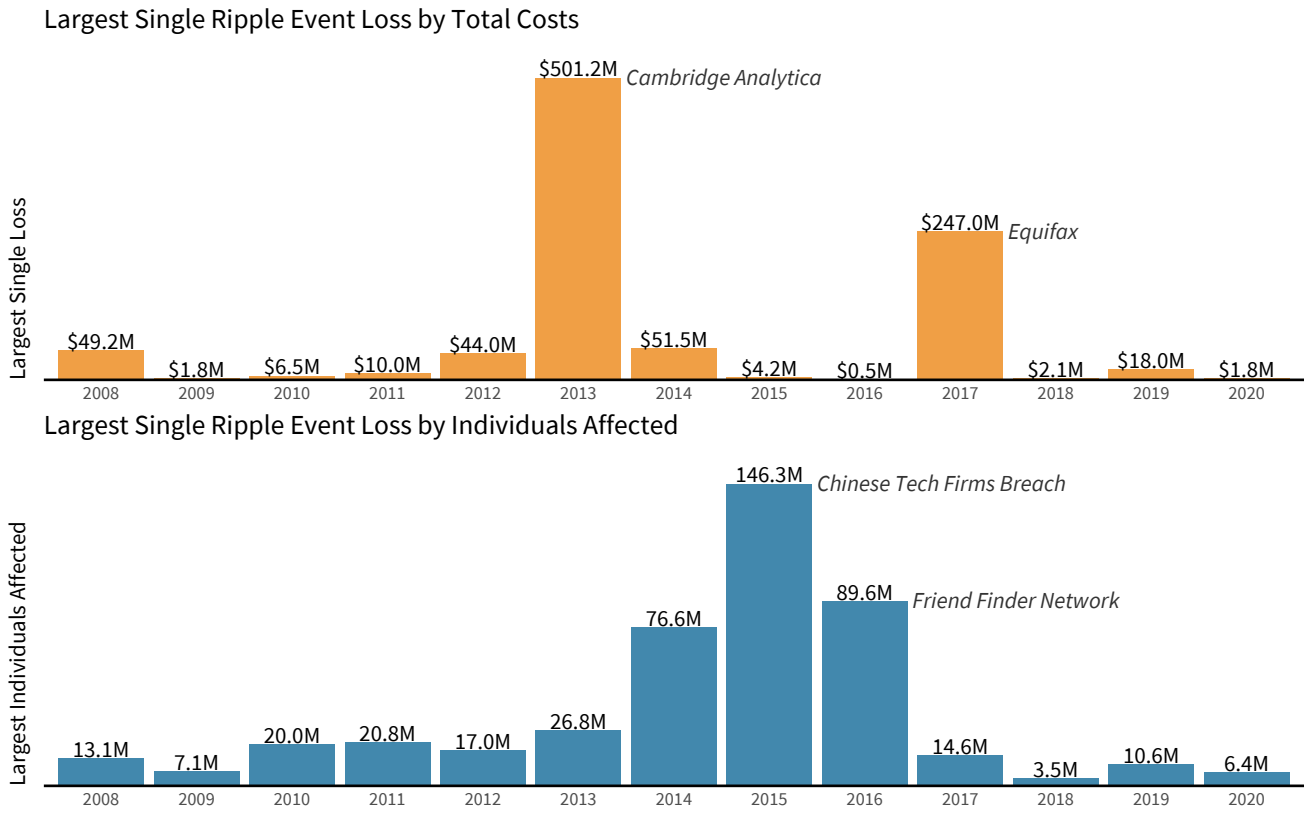
In orange are the ripples recorded in our 2019 report, and in red are the yearly totals of ripples identified as of now. While the number of ripples didn't explode as we had suspected back in 2019, the yearly number of ripples is relatively stable in recent years (remember that there is typically a lag for events in the past 12–18 months to be identified as true ripples).

There could be a number of different dynamics in play here. It's conceivable that the number of ripple events really did peak a bit in 2016 and that we will no longer see the perpetual incremental gains up that curve as in years past. However, we do urge caution in concluding that ripple numbers have plummeted or will fall further in 2021, as we believe there are other variables to consider. The observation lag that we've noted is an approximation of the public disclosure processes. It is possible that increases in reported ripple events from 2018 through 2020 won't really stabilize until 2022 or 2023. Once all the long-term observations shake out, we may find that there was a slight peak in 2016 and that the numbers plateaued for the last three years.

However, one thing we definitely don't expect is for ripple events to decrease significantly over the next few years. The extreme efficacy and very public success of the SolarWinds attack in late 2020, closely followed by the Kaseya attack in July 2021, has provided the bad guys with a proven playbook for supply chain and digital ecosystem attacks that will likely fuel ripple activity in 2021 and beyond.

Finally, even though the total number of ripples has fallen year-over-year, the impact of the largest ripples remains huge. As we can see below, the largest ripples by total costs and total number of individuals affected can vary significantly by year, as outlier events rarely sit on a nice curve.

Figure 4: Largest Ripple Events per Year by Costs and Individuals Affected



NEW 2020 RIPPLE EVENT EXAMPLES IN ACTION

Before we broadly discuss who is getting caught in ripple events, how much ripples are costing organizations, how long they take to unfold, and what's potentially causing them, it's important to zoom in on a few individual examples first.

While a stable number for multi-party breaches in 2020 is not likely, our analysis has already dug up 37 ripple events that swept up victims across a range of industries and scenarios last year. We've encapsulated an assortment of these latest breaches to provide a feel for how varied ripple events can really be.

The triggering events are often different, the business relationships vary, the scope of impact can vary wildly, and the depth of downstream reach is changeable. The one unifying factor is the technical integration or data sharing—direct and indirect--that spiderwebs across the generating organization and the recipients of downstream loss events.

ACCELLION USA LLC

The mass exploitation of vulnerabilities in the company's file transfer appliance has allowed criminal gangs to target the sensitive information of thousands of Accellion clients—and subsequently the victims' customers and clients—including the personally identifiable information (PII) handled by the Washington State Auditor's Office, New Zealand's central bank, and the high-profile law firm Jones Day.[1]

ADVANCED COMPUTER SOFTWARE

This software developer for the legal industry exposed data held by more than 190 law firms when a cloud-based database for legal forms was left publicly accessible on the Internet. The open database in Advanced's Laserform platform left more than 10,000 legal documents exposed online, including "extensive details of transactions, payment terms, and client agreements," according to security researchers.[2]

BLACKBAUD

A cloud computing provider for non-profit organizations, foundations, education firms, and healthcare entities, Blackbaud experienced a double extortion ransomware attack that not only encrypted the systems running its client's environments but also exfiltrated millions of sensitive records held by 550 different organizations. Rough estimates show that some 10 million individuals had their PII exposed by this ripple event. The downstream organization impacted the most was Inova Health Systems, which had 1 million of its patients exposed. Due to the number of organizations affected and records involved, this ripple event is the biggest healthcare breach on record for 2020.[3]

CLOUD CLUSTERS

This US-based hosting provider left a database containing monitoring and system logs open to the Internet with no password protection. This lapse exposed the credentials of numerous organizations' Magneto eCommerce and WordPress accounts, along with the PII from 63.7 million records of shoppers and other individuals. [4]

[1] https://www.wired.com/story/accellion-breach-victims-extortion/
[2] https://community.turgensec.com/190-law-firms-data-breach-disclosure/
[3] https://healthitsecurity.com/news/blackbaud-confirms-hackers-stole-some-ssns-as-lawsuits-increase
[4] https://securethoughts.com/hosting-provider-exposed-63-million-customer-records/

GODADDY

One of the most prolific hosting providers on the web, GoDaddy was first informed of its 2020 ripple event via an email from the State of California Department of Justice, which stated that someone had gained unauthorized access to the login information for SSH accounts. An investigation into the matter showed that the attackers had access to the firm's hosting environment for six months—the kind of access that could have been used to launch a range of chained attacks—compromising the hosting accounts of 28,000 different GoDaddy customers in the process.[5]

MJ BRUNNER

This marketing company developed and supports the investment dashboard and online enrollment portal for SEI Investments Co., which provides platforms and services to dozens of wealth management funds. When Brunner was hit by a Maze ransomware attack that it refused to pay extortion money for, the attackers publicly posted the data they'd exfiltrated during the attack. This exposed SEI and, in turn, the clients of 100 different financial funds doing business with SEI, including PIMCO.[6]

NETGAIN

This cloud hosting provider specializes in providing services to healthcare companies. When it was struck by a ransomware attack, the impacts rippled across numerous third-party relationships. The impacts were felt by many smaller health providers and service companies. A notable example was Crystal Practice Management, a software company that provides solutions to optometrists and vision therapy pros. Its clients were unable to access patient data or the software required to serve their patients for days as a result of the attack.[7]

SOLARWINDS

The crop of 2020 ripples was punctuated by the big exclamation point that was the SolarWinds breach. A major provider of IT management tools, SolarWinds was compromised via a vulnerability in its Orion suite of tools, which are used by thousands of organizations to manage their IT networks. This flaw allowed the attackers to insert a backdoor in the tool that could then be leveraged to compromise the SolarWinds customer environments. Some 18,000 organizations were potentially exposed to the backdoor, with confirmed compromises including the U.S. Department of Homeland Security, Microsoft, and FireEye. The latter two compromises kicked off further Nth party attacks, and many in the security industry say that it will take years to understand the widespread ripples that this single incident will broadcast across the globe.[8]

WAYDEV

This platform provider for Git analytics had a database breach in which the hackers stole GitHub and GitLab Oauth tokens and used these to compromise the company's customers and customer's customers. Associated ripple impacts included a breach of the fintech firm Dave, which compromised 7.5 million banking users, and a breach of the software testing firm Flood.iO, which eventually exposed the hosted cloud credentials of its entire customer base.[9]

[5] https://www.cpomagazine.com/cyber-security/godaddy-web-hosting-accounts-data-breach-underscores-need-for-stronger-authentication/
[6] https://www.wsj.com/articles/fund-administrator-for-fortress-pimco-and-others-suffers-data-breach-through-vendor-11595857765
[7] https://siliconangle.com/2020/12/09/cloud-hosting-provider-netgain-struck-ransomware-attack/
[8] https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
[9] https://www.zdnet.com/article/hackers-stole-github-and-gitlab-oauth-tokens-from-git-analytics-firm-waydev/#:~:text=Waydev%2C%20an%20analytics%20platform%20used,tokens%20from%20its%20internal%20database

WHO IS INVOLVED?

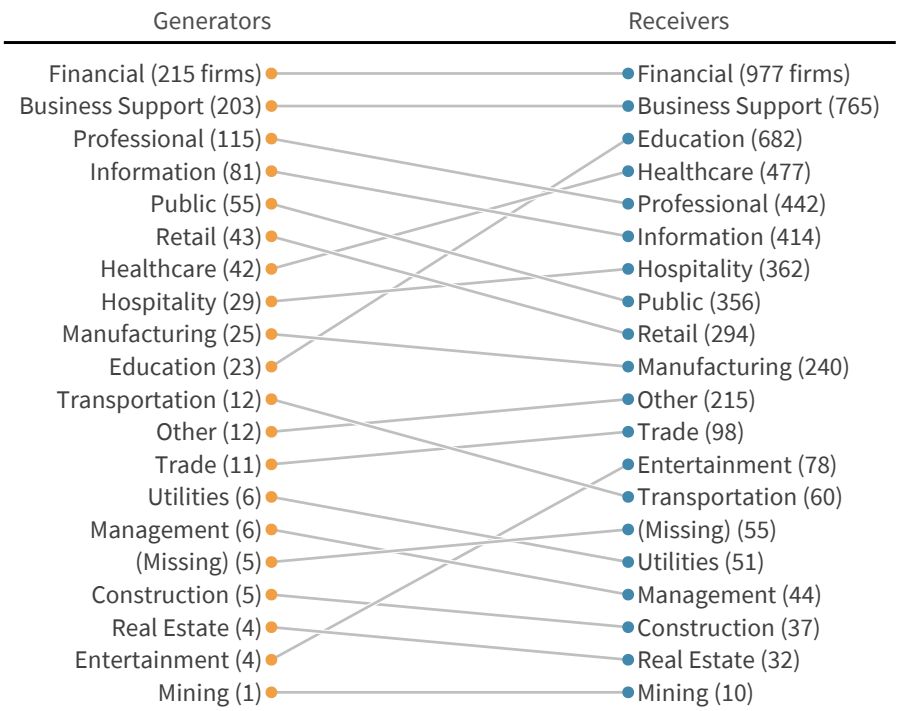
Drawing our lens back again to our revised data set from 2008 onwards, let's take a look at the kinds of organizations most likely to be involved in a ripple event, including the generating organizations, recipients of downstream loss events, and threat actors.

THE VICTIMS

As with last year's report, we leaned on the North American Industry Classification System (NAICS) for this analysis. NAICS is widely used, well-documented, and conveniently integrated into Advisen's cyber loss database. This year, we started with the work performed by our partners at Advisen in identifying the generating sources of ripples and completed additional research on a large portion of the ripple events.

In doing so, we were able to more precisely identify the source of ripple events than in the last edition of this report. While we're confident in our determinations, putting the numbers from each report side by side does lead to an apples-and-oranges comparison. Instead, we focus on the picture of where things stand in the overall dataset, keeping in mind that this covers a 10-year period.

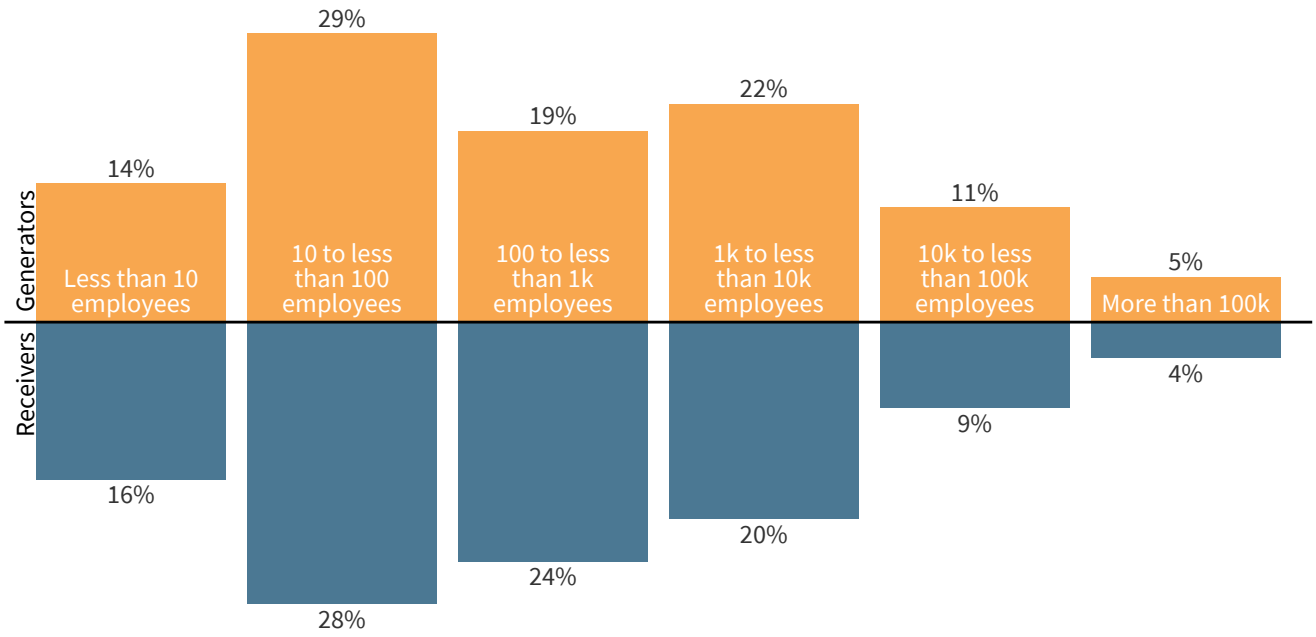
Figure 5: Most Common Industries as Generators and Receivers



As you can see in Figure 5, comparing ripple-generating victims against recipients of downstream loss events, financial and business support organizations dominate the top two slots in both categories. One of the lessons we want to convey with this comparison chart is that there are a lot of crossovers between the generators and receivers. Many companies are, at some point, both the generator of one ripple event and the downstream recipient of others generated by different organizations. This is a testament to the tight technical ties that bind suppliers, customers, and partners in today's digitally dominated business environment.

By comparing generators (orange) and receivers (blue), we also examined our ripple victims by company size. The data below is made up of a subset of companies for which we had employee data available, which accounts for about 89% of all companies involved.

Figure 6: Employee Data for Companies Involved



One thing of note here is that the generators (orange) are much more oriented toward smaller firms than the balance we saw in 2019. In contrast, a fairly constant balance remained between the larger and smaller receiving firms. Similar to our breakdown by industry, the ratios by the number of employees between the two groups seem nearly symmetrical, indicating that the company size doesn't make firms any more or less likely to be a ripple generator or receiver.

MORE INFORMATION ON NAICS CLASSIFICATION CODES

North American Industry Classification System (NAICS) codes are six digit identifiers that roll up into top-level (two-digit) sectors and (three-digit) subsectors. So, when we use the label "Finance (52)" in Figure 6 below, we're referring to the Finance and Insurance sector that has the top-level NAICS code of 52. The NAICS site contains descriptions and examples of all sectors, subsectors, 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 fall into the same subsector, Business Support Services (5614), we opted to label it "Business Support" to be more specific.

Among the newly observed ripples, generating organizations saw a surge among the professional industry in particular, even if the overall data set showed financials led the way. Meanwhile, downstream organizations in the newly observed ripples more closely matched the existing ratios, with financial services firms and professional organizations coming in first and second, respectively.

Figure 7: Generating Sectors with New Ripples

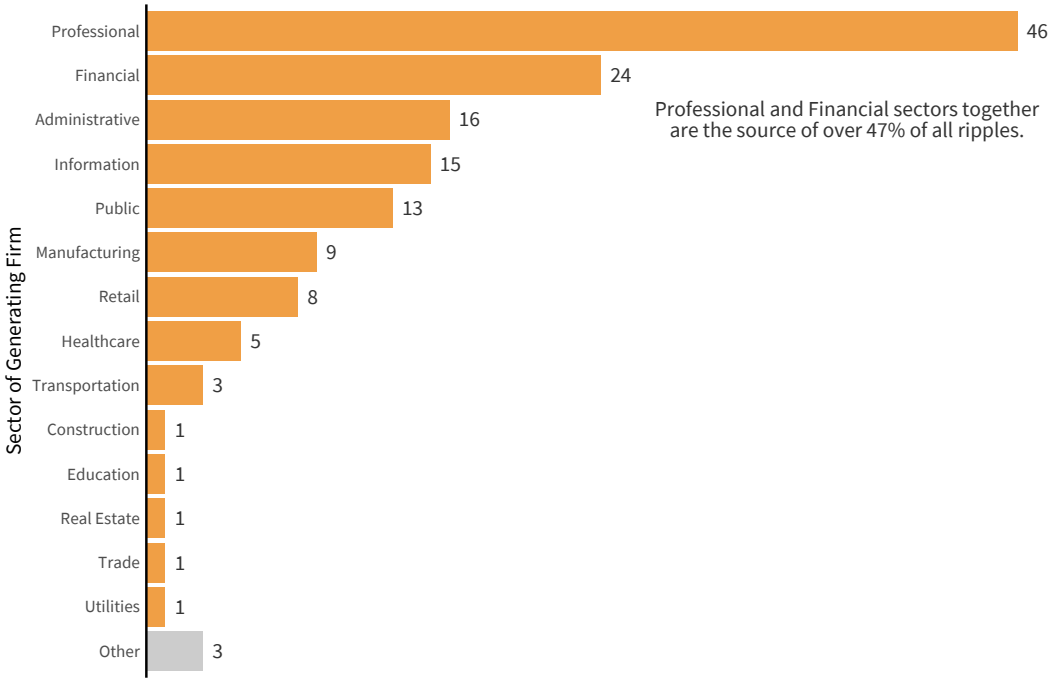
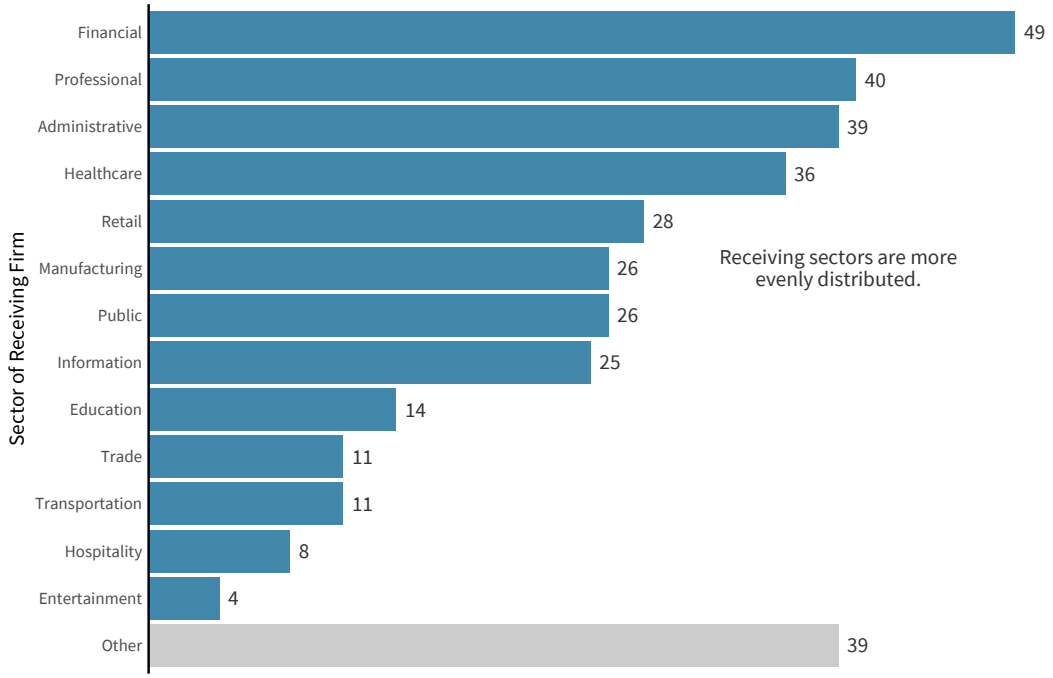


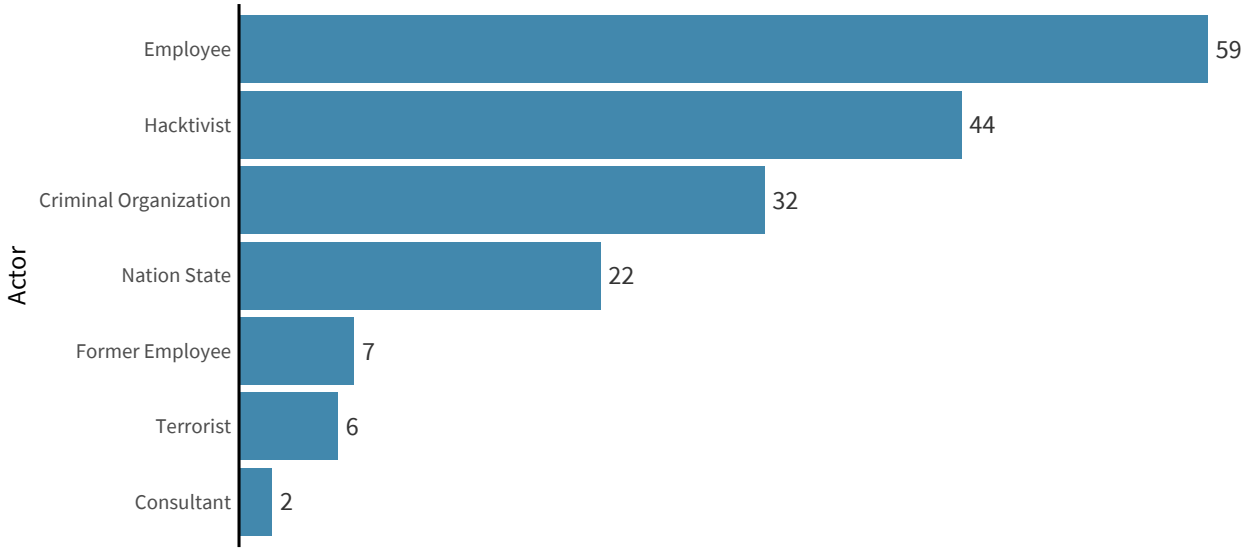
Figure 8: Downstream Sectors with New Ripples



THE THREAT ACTORS

The threat actors who trigger ripple breach events can be difficult to trace. Here, we present the data from events for which we have information about the primary actors involved. Ripples can have multiple "primary" parties, so a single ripple may appear in several of the following bars.

Figure 9: Threat Actors Involved with Ripples



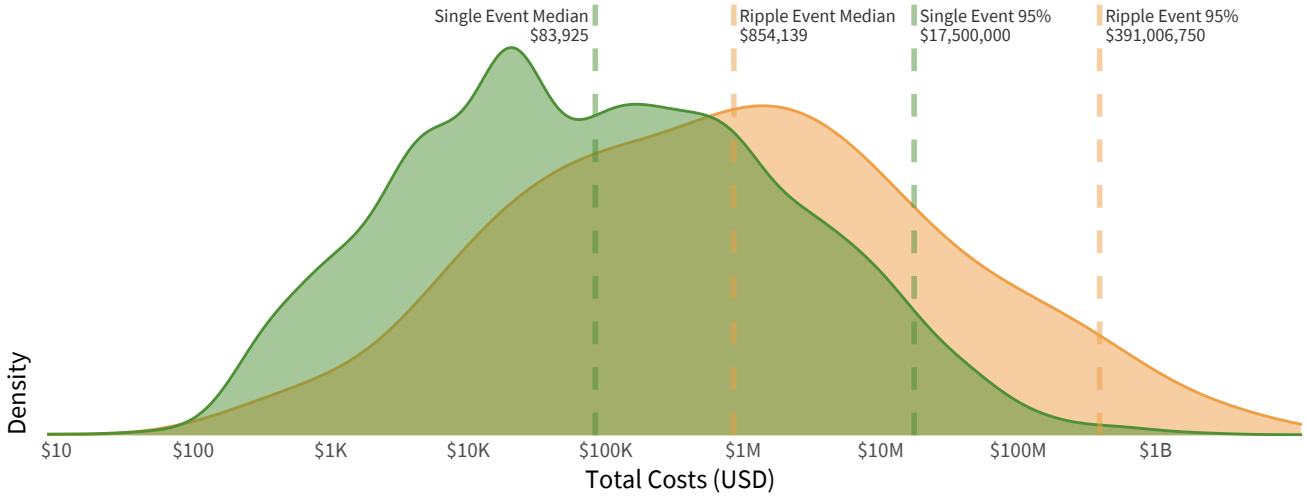
We've removed the ripple events wherein the actor is a trusted third-party vendor. All of these ripples are third-party types by nature, as we're looking to understand the events associated with the ultimate genesis of a ripple. We have also removed the "Organization" actor type; this often represents one firm suing another (or regulatory action), and we're looking for the ultimate source of ripples.

WHAT'S THE DAMAGE?

Most of the ripples we analyzed involved only four firms, but the financial impacts of all of these multi-party incidents far outweighed their traditional single-party breach event counterparts. In the below chart, we display the distribution of event density by financial costs, with ripple events in orange and single-party events in green. The placement of each curve clearly shows that ripple events have costs that far exceed single-party events.

This chart looks very similar to the 2019 one. As new information comes to light, the median cost of single events is slightly higher than in 2019 while the median costs for ripple events is slightly lower, yet the cost of these ripple events is still nearly 10x the median cost of single party events. More troubling, when looking at the worst of these events (those single or ripple events in the 95th or greater percentile), the spread has grown larger, with ripple events now over 26x more financially damaging than the worst single-party breach events.

Figure 10: Cost Distributions of Ripples vs. Single Events



Digging into the kinds of losses incurred by multi-party incidents, depicted in Table 1 below, we can observe that direct damages and response costs still dominate.

Table 1: Presence and Magnitude of Different Loss Components

Form of Loss	Percent of Ripples with this Form	Percent of Costs	Typical Amount	Extreme Value (95th Percentile)
Financial Damages Amount	80.7%	52.4%	$432,049	$163,307,500
Other Fines Penalties	20.5%	60.7%	$1,735,852	$307,126,658
Response Total Cost	15.1%	24.8%	$8,322,254	$341,940,000
Plaintiff Legal Fees Expenses	13.3%	2.3%	$496,875	$26,668,898
Loss of Business Income Amount	3.6%	78.1%	$36,433,944	$1,328,177,500
Loss of Assets Amount	0.6%	0.0%	$5,000	$5,000
Other Expenses	0.6%	26.3%	$600,000	$600,000

Among those ripple events for which we have cost information, 80% involve some sort of direct financial damage. One out of five of the ripples involved ends up incurring fines and penalties, and one in 10 of them incurs response costs.

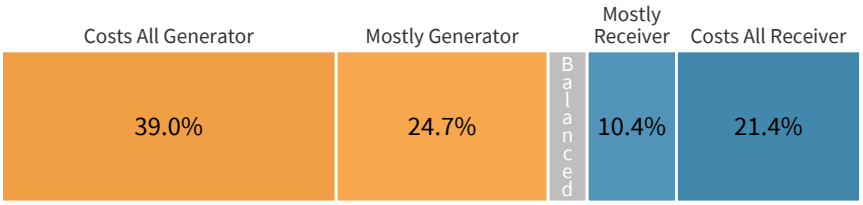
While only a small fraction of ripples cause a loss of business income, such losses are particularly devastating. In those cases, the loss of income makes up 78% of costs. When a ripple event triggers a loss of income, it typically equals a staggering $36M per event.

The detailed cost data available in the Advisen database only covered a fraction of our entire data set. However, there were still enough ripple events to provide statistically relevant analysis of how the costs are split between the generator and downstream victims. By parsing this subset of 154 ripples, we found that the most costs are, by far, borne by the initial victims of a multi-party breach.

This offers a strong lesson for suppliers with many customers within their data sharing or technology ecosystem. With ripple events typically costing 10x more due to the downstream impacts, organizations must keep in mind the risk they expose to their customers and partners should they trigger a multi-party incident, especially because there is a high chance they'll be footing a much higher bill once all of the impacts shake out.

On the flip side, organizations responsible for managing the third-party risk of their vendors should keep in mind that they are never going to be immune to the financial impact of ripples. The data shows that more than one in four downstream victims end up paying most or all of the costs of a ripple incident.

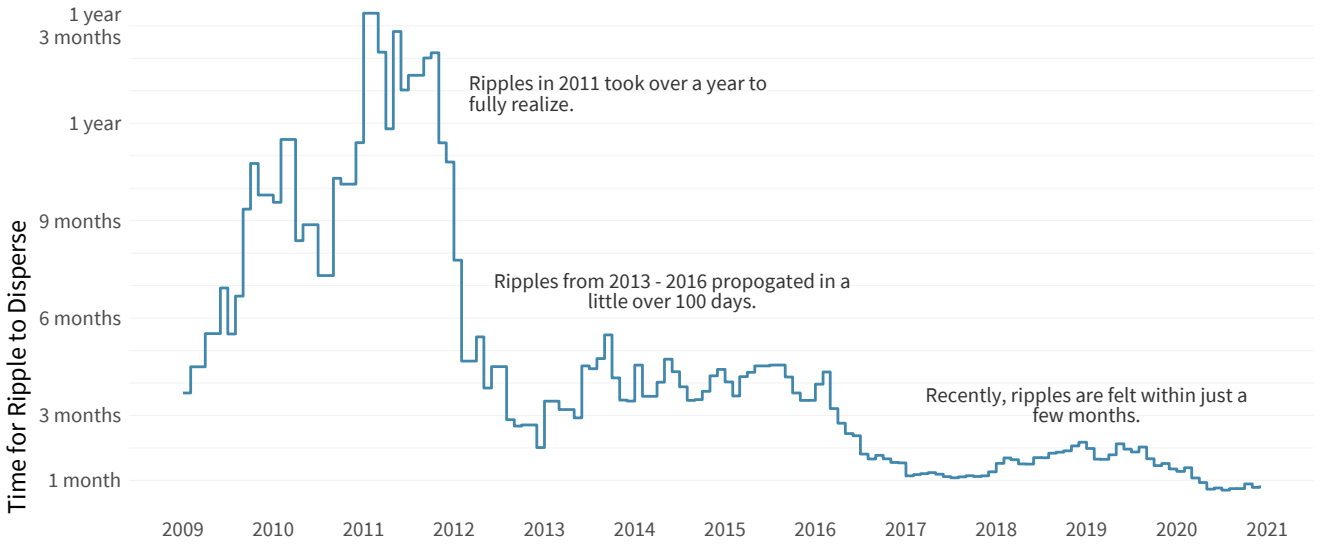
Figure 11: Distribution of Costs Between Generator and Downstream Organizations



DURATION OF RIPPLES

If we take a look back at the yearly rolling average from the time of the triggering incident to that of the last observed activity in a ripple, we can get an idea of the duration of the impact of ripple events. Obviously, this is an imperfect measure as it is based on observed impacts rather than on how long an attacker leverages the access or data they gathered from that initial breach. Nevertheless, Figure 12 provides valuable information about how these events tend to play out from a timeline perspective.

Figure 12: Time for Ripples to Propagate vs. the Initial Event

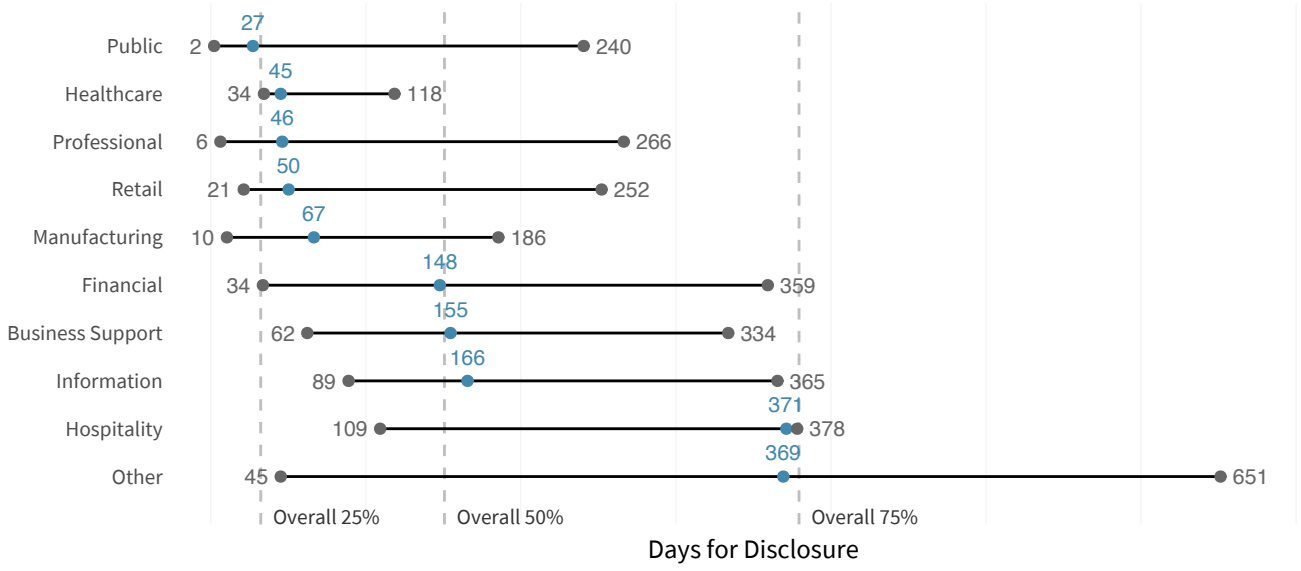


Our observation here is that the impacts are starting to be felt more quickly as time goes on—some of this is likely a result of attackers learning how to leverage the interconnection between organizations to steal more data profitably across corporate boundaries.

The time for ripples to disperse through third-party networks and beyond dropped significantly between 2012 and 2013 to less than 200 days. We saw another significant drop again in 2018 to around 50 days. There was a smaller dip in 2020, but readers shouldn't place too much importance on that until we have a year or so to account for the lag and learn about the effects of these incidents.

Thinking about the duration of ripples differently, we sliced the data to examine the intervals of time it took for some, half, and most of the downstream recipients to feel the impact of a multi-party incident. This gives us a different view of the timelines and provides a way to find out how long it takes for firms to experience the effects of the ripples, based on the industry of the generating organization. Overall, 25% of firms are involved within 32 days after the initial event, 50% by 151 days, and 75% by just over a year at 379 days.

Figure 13: Disclosure Time for Generator Industry (25, 50, 75 pct)



This shows that the fastest impacts rippled out from incidents within healthcare, likely due to the strong reporting requirements in that space. Meantime, the hospitality and information industries take approximately a year before most downstream victims fully feel a ripple.

WHAT'S MAKING WAVES: CATEGORIZING RIPPLE EVENTS

In our inaugural edition of this ripples analysis, we didn't dig nearly enough into the data on what exactly has been causing these ripples. Distinguishing a root cause from all of the other activities in a ripple is a challenge, but we thought we'd at least try to examine high-level event categories this year and enumerate the types of ripples occurring across the entire data set.

Table 2: Common Types of Ripples

Cause	Pre-Existing	New Ripples
Data Breach Incident	366	104
Denial/Disruption of Service	85	13
Privacy Violation	358	24
Other	4	6

The table above breaks up ripple incidents into three main categories: traditional data breaches, denial of service or disruption of service events (DoS), and privacy violations. The latter tends to comprise the exposures of cloud data stores and cloud misconfiguration that have been especially coming into light over the last four or five years.

The data shows that data breaches remain the dominant generating event for ripples, with privacy violations coming in a close second. DoS events are far less common than ripple events, although that doesn't necessarily mean they aren't a source of concern. As we mentioned earlier, loss of revenue can be extremely significant in multi-party incidents, and this can be a common side effect of the high-level DoS category.

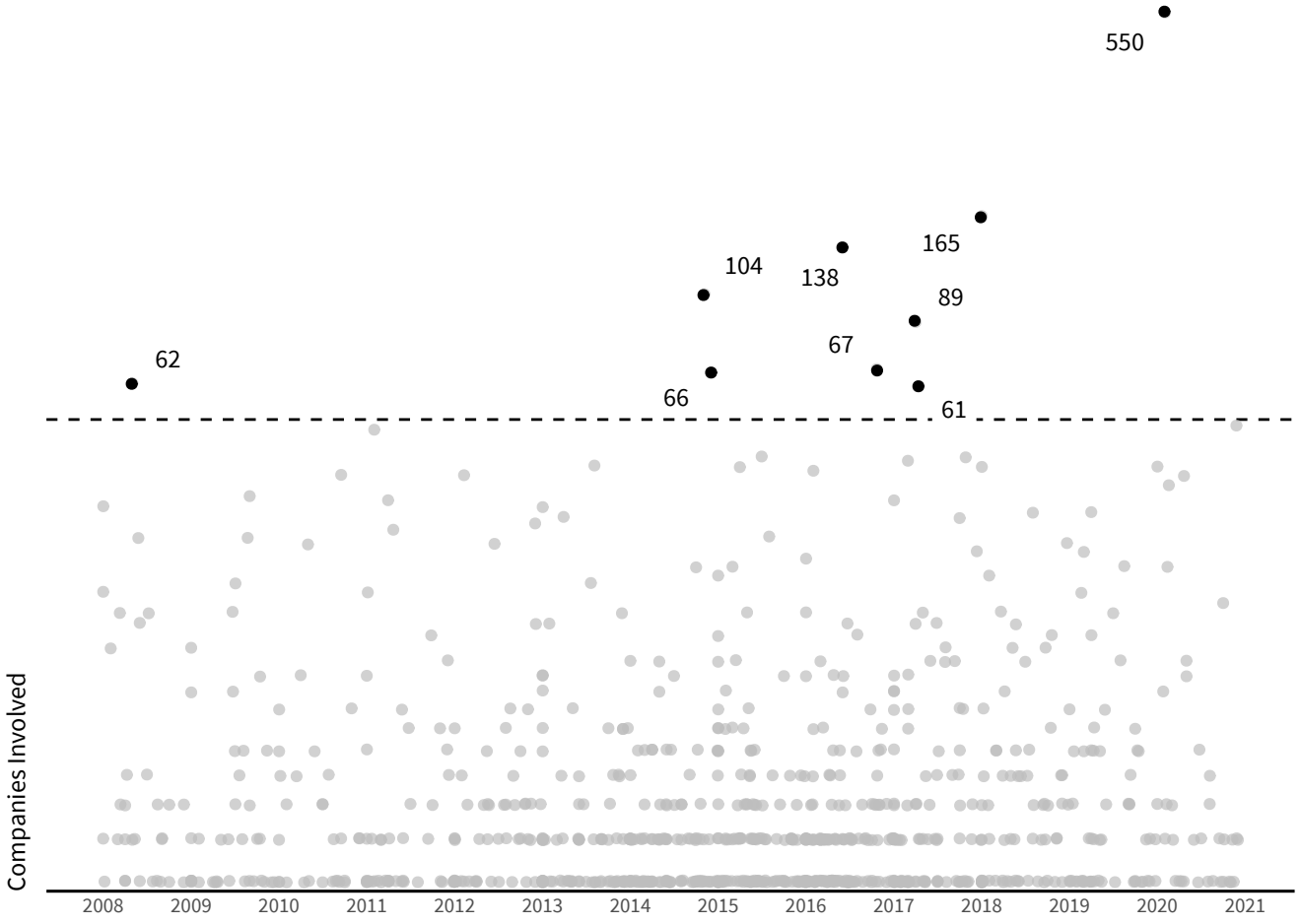
WHAT ABOUT RANSOMWARE RIPPLES?

One specific category you won't see in the chart here is ransomware. This is the byproduct of the struggle we're currently facing in the data in distinguishing a "root" cause from all the other actions in a ripple. Our manual analysis found that 34 ripple events in our data set had some kind of ransomware style action somewhere in the chain, but they weren't identified primarily as ransomware in nature. Some of these events fell in the data breach category and others in DoS. This data point shows that ransomware attacks do happen and not infrequently. A fair amount of ransomware attacks that hit multiple connected companies, but statistically, at this point, it's less common for losses to spread between firms. Nevertheless, that risk still lurks. The Kaseya incident this year highlights how devastating ransomware can be in a supply chain-style attack.

THE RISE OF THE RISK TSUNAMI

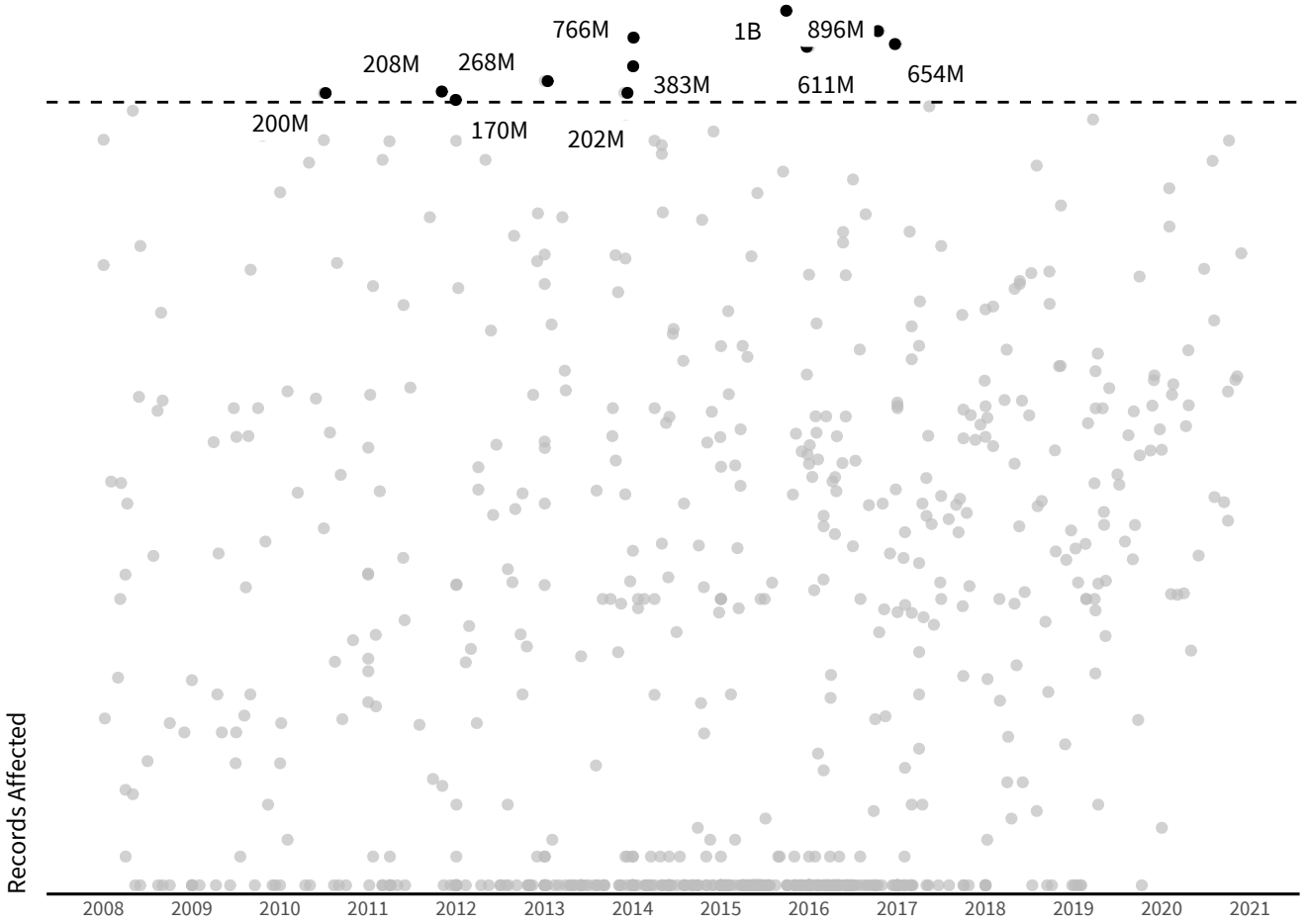
One thing we've drawn greater clarity on in the past year is the rising number of outlier ripple events that are causing a much greater surge in downstream loss events than the typical ripple. These events impact so many third- and N-th party relationships that they are more like tsunami events than mere ripples. They impact 50 or more companies from a single triggering incident, and one of them uncovered in this year's research—the Blackbaud incident referenced in our examples—actually impacted 11x more organizations than that, 550 to be precise.

Figure 14: Rise of Tsunami Events by Companies Involved



It's only logical to see that the number of records exposed or breached from these tsunami events is also many times more than the typical ripple event. The smallest tsunami event in our data set impacted 200M records, and the largest topped out at 1B records exposed.

Figure 15: Rise of Tsunami Events by Records Affected



Due to the outsized impacts of tsunami events, we plan on examining these with further scrutiny in a future report later this year. Expect more data and analysis on this soon.

One thing we've drawn greater clarity on in the past year is the rising number of outlier ripple events that are causing a much greater surge in downstream loss events than the typical ripple. These events impact so many third- and N-th party relationships that they are more like tsunami events than mere ripples.

KEEPING THE RIPPLES AT BAY

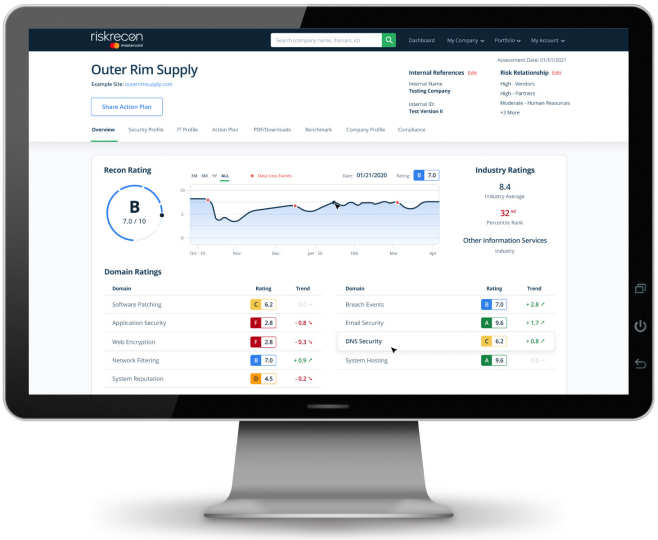
From the data presented in this report, one thing should be crystal clear - no organization is safe from a multi-party ripple event. As firms of all shapes and sizes continue to allow companies to access their data, client information, employee details, etc., they also open up more paths for security incidents that can harm their business. The reality is while you can't protect yourself from every third-party threat, you can take control over the risks that will impact your business the most.

The interconnectivity of different third- and fourth-party relationships is often hard to visualize and address. However, using RiskRecon cybersecurity insights and ratings allows users to gain a streamlined understanding of their organization's supply chain environment including, fourth-party software dimensions, hosting providers, and other relationships, enabling you to address critical issues faster.

FREE OFFER: KNOW YOUR 3PTY SECURITY RISKS

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.

riskrecon

mastercard

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

A collaborative research project between RiskRecon and the Cyentia Institute