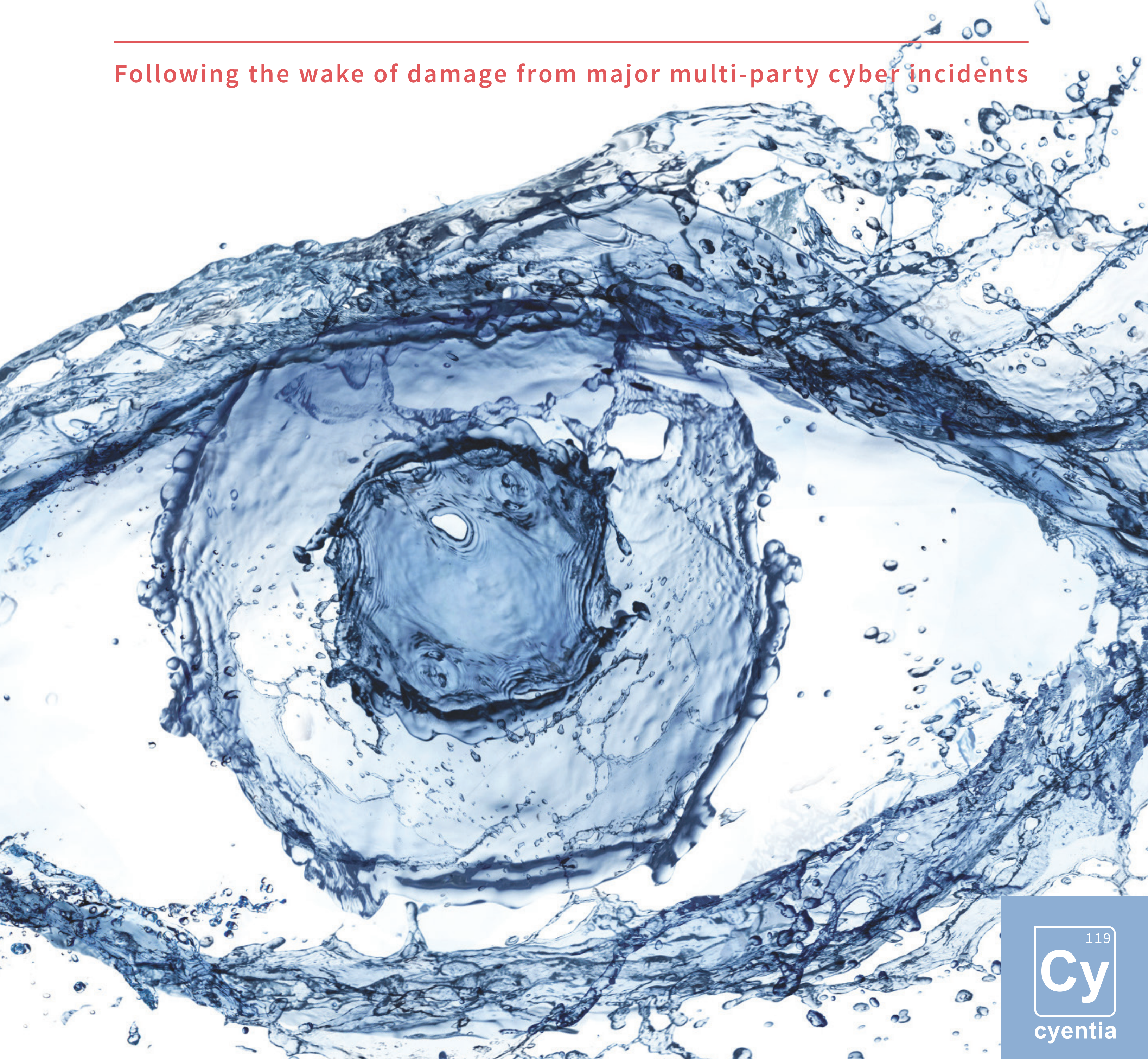
riskrecon mastercard

interos

CyberGRX

Information Risk Insights Study IRIS TSUNAMI

Following the wake of damage from major multi-party cyber incidents



cyentia

Light Through the IRIS

In almost every way imaginable, we live in a hyperconnected world. This connectivity has brought many benefits to modern business models, but it has also introduced myriad challenges and risks. If you take the time to decompose even the simplest of business transactions, you'll find in the mix a surprising number of parties from technical components supporting the transaction to the completed delivery of products to the customer. But what happens to all these parties when something goes wrong?

That is ultimately the question that this study seeks to explore. We identified 50 of the largest multi-party cyber incidents over the past several years in an effort to understand their causes and consequences from beginning to end. If you are familiar with our other research in the Information Risk Insights Study (IRIS) series, Tsunami draws from the same rigorous methodology. We started with a huge dataset of cyber loss events, identified those that involved multiple organizations, and then researched each event to understand who was behind it, what happened, how the after effects propagated through the supply chain, and the financial losses for all parties involved.

Thank you for joining us once again as we focus the IRIS to enlighten another important area of cyber risk management.

Share your thoughts: **#CyentiaIRIS**

Table of Contents

Key Findings

$90M The median cost of these 50 extreme multi-party events stands at a whopping $90M. To put that in perspective, the typical incident runs a comparably measly $200K.

The median number of organizations impacted in these cyber tsunami events is 31, but we recorded swells enveloping as many as 800 secondary victim firms.

System intrusions were by far the most common type of incident, and they also impacted the largest number (57%) of downstream organizations.

Ransomware lags as a distant second in terms of frequency but ran up 44% of the recorded financial losses across the 50 tsunami events in this study.

Cracked and stolen credentials were the most common (50% of incidents) and costly (68% of losses) initial access technique.

Exploitation of public-facing applications led to more collateral victim organizations (63%) compared to any other initial access vector.

Aggregated data and shared systems were the most common ways in which cyber loss events propagated from primary to secondary victim organizations.

Supply chain compromises led to the biggest share of recorded financial losses ($7.4 billion) and the largest number of secondary victim firms.

Organized cybercriminal groups were ultimately responsible for 80% of all collateral damage to downstream firms.

$10B State-affiliated actors were behind one out of five incidents and caused the majority of financial losses, with over $10 billion recorded on their tab!

Insiders and third parties contributed to 34 of the 50 extreme events we analyzed in this study. Those 34 events carry a combined price tag of $17.3 billion—99% of all recorded losses!

Facing a drought in cyber risk data?

If so, we might be able to help open the floodgates. Our brand new IRIS Risk Retina service puts Cyentia's analytical prowess to work for you by quantifying cyber risk along multiple dimensions of your choosing, thereby enabling more informed risk decisions. To learn more, visit https://www.cyentia.com/retina.

Methodology

How was the data collected?

Like its predecessors in the IRIS series, this study leverages Advisen's Cyber Loss Data, containing nearly 100,000 cyber events collected from publicly verifiable sources. Three features make this dataset uniquely suitable for this research: 1) it has comprehensive coverage across a wide variety of incidents, 2) it links organizations that are involved in or impacted by a common incident, and 2) it tracks losses that were publicly disclosed in the wake of those events.

From Advisen's Cyber Loss Data, we identified the 50 largest multi-party cyber incidents (see criteria in next section) and sought to collect hundreds of additional data points on those events. We followed the same data collection procedures used for the IRIS Xtreme, scouring public information sources to categorize incident types, identify the actors behind these events, record the techniques they employed, etc. Additionally, we gave special attention to discover the methods by which these incidents (or their effects) propagated from initial to secondary victim firms.

What's a multi-party cyber incident?

Many cybersecurity incidents involve not only involve the primary organization, but also generate secondary loss events that impact various other 3rd/4th/Nth parties. We refer to these multi-party incidents as "ripple events," reflecting how their after effects swell outward from the central victim to envelop others in their wake. Extending that metaphor, we've designated ripple events that propagate the furthest or cause the most damage as tsunamis. You'll find a broad analysis of 900 multi-party cyber loss events in our joint report with RiskRecon titled Ripples Across the Risk Surface.

> **"We refer to these as "ripple events," reflecting how their after effects swell outward to multiple parties. Extending that metaphor, we've designated ripple events that cause the most damage as "tsunamis."**

What constitutes a "tsunami" event?

We used several criteria to identify a subset of the largest ripple events (aka "tsunamis"):

- The largest 30 multi-party events as measured by total reported financial losses.
- The largest 30 multi-party events as measured by the number of data records affected.
- The largest 30 multi-party events as measured by the number of firms involved.

Any multi-party cyber incident meeting any of these criteria was a candidate for inclusion, and we then selected the top 50 based on the combined totals as well as information availability. These 50 digital tsunamis form the corpus of the analysis that follows in this study.

Are ripple events different from supply chain attacks?

Yes. All supply chain attacks are ripple events, but not all ripple events are supply chain attacks. It is not necessary to compromise hardware or software components to generate downstream loss events. For example, if a data aggregator is breached, the owners/providers of that data may suffer losses even though their systems remain uncompromised.

How big are the waves?

This question is likely top of mind for many readers of this report. After all, “Tsunami” connotes waves that swell up, travel far, and leave a trail of damage in their wake. Hydrologists have several methods of measuring real-world tsunamis, and we’ll look at a few different ways of sizing up the cyber tsunamis in this study (albeit with far less precision).

Number of impacted organizations

Let’s begin with the number of secondary firms impacted by these mega multi-party cyber incidents. We took a conservative approach to enumerating, relying either on specific entities identified in Advisen’s dataset or on a number reported publicly by the central organization itself.[1] Also keep in mind that this isn’t the only criterion by which an event might be considered a tsunami (which is why a quarter of these incidents encompass just three to four firms).

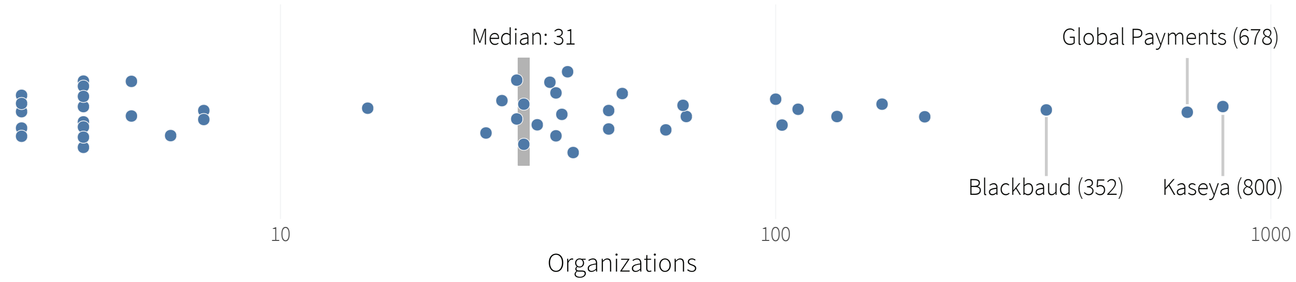


FIGURE 1: NUMBER OF SECONDARY FIRMS IMPACTED BY EXTREME MULTI-PARTY CYBER INCIDENTS

The median number of secondary organizations swept up in the wake of one of these digital tsunamis is 31. One in four of these incidents impacted 55 firms or more, and the largest among them encompassed no less than 800 organizations! These numbers serve as a reminder of the highly interdependent nature of modern business where one firm’s breach can have spillover effects across many, many more.

How long does it take ripples to propagate to all parties?

To shed light on this question, we queried 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 provides a way to find out how long it takes for firms to experience the effects of the ripples. 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.

You might be thinking that delay would be a challenge to research like this, and you’d be correct. For instance, after we completed analysis for this study and moved into the layout phase, an update to the dataset bumped the number of organizations impacted by the Blackbaud breach to over 800. That’s frustrating for efforts like this, but it’s also encouraging that we can begin to measure and anticipate ripple effects from the data.

[1] If the reported number of secondary firms was a range, we recorded the lower bound of that range.

Amount of data compromised

We've **gone on record** saying that the number of records compromised is not a good predictor of the financial losses associated with a breach. So don't worry—we're not going to attempt that here. Taken alone, it simply serves as another way of sizing up these events.

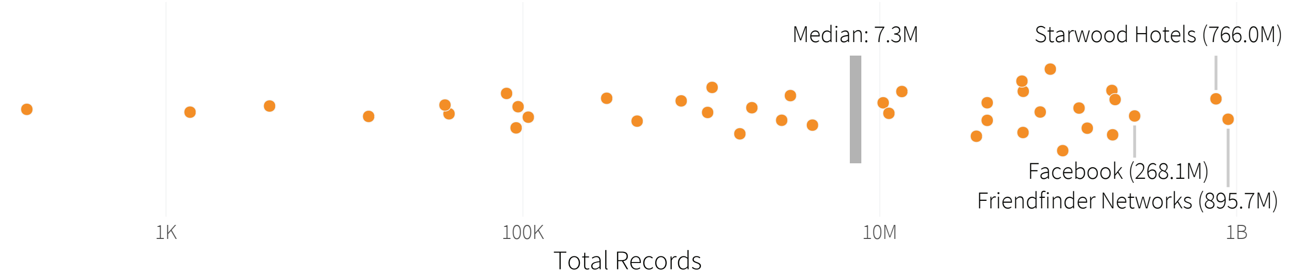


FIGURE 2: NUMBER OF DATA RECORDS COMPROMISED FOR EXTREME MULTI-PARTY CYBER INCIDENTS

As measured by the median, the typical tsunami swallows up over seven million data records across all organizations affected. The 75th percentile swells to over ten times that number, reaching beyond 82 million records. Nearly one in five of these events exceeded the vaunted 100 million mark! We won't go into detail on the types of data compromised, except that personal information (37 events) and payment account data (26 events) led the pack.

Total financial losses

We feel obliged to offer a couple of caveats before sharing statistics on the financial impact of tsunami events. First, these figures represent publicly-reported quantifiable losses that are tied to these incidents. They do not include many of the soft or indirect costs experienced by the victim organizations that go unreported in public documents such as Securities and Exchange Commission (SEC) filings. Second, note that we were only able to find verifiable data on losses for 30 of the 50 incidents. And lastly, remember that we're focusing on a small set of the largest multi-party cyber loss events, so what you see here doesn't in any way represent the broader distribution of all security incidents.[2]

With that out of the way, let's inspect the price tag on these mega multi-party incidents. The median loss magnitude stands at a whopping $90 million. To put that in perspective, our analysis of all loss events in the **IRIS 20/20** pegged the median at a "paltry" $200,000. It even doubles the median loss of $47 million set by the **IRIS Xtreme** for the 100 largest security incidents over the past five years.

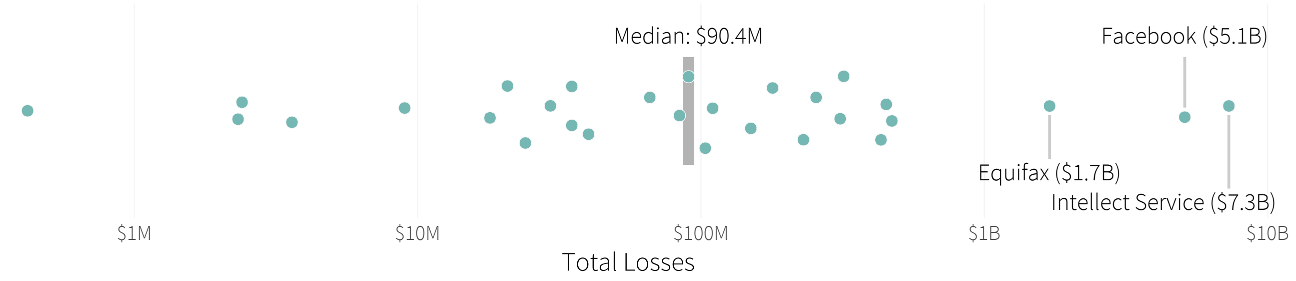


FIGURE 3: TOTAL RECORDED FINANCIAL LOSSES FOR EXTREME MULTI-PARTY CYBER INCIDENTS

[2] But you can view the broader loss distribution in the IRIS 20/20 (https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf)

More parties, more pennies

Figure 4 comes straight outta the latest version of our joint report with RiskRecon, Ripples Across the Risk Surface. It compares the loss magnitude for single (green) vs. multi-party (orange) incidents. Notice how the distribution for multi-party events shifts substantially to the right. The median loss for multi-party incidents is over 10x that of their single-party cousins. Also notice that the tail is much thicker, indicating higher propensity for major loss events. Extreme losses (95th percentile) for ripple events near $400 million but fall well below $20 million for traditional incidents.

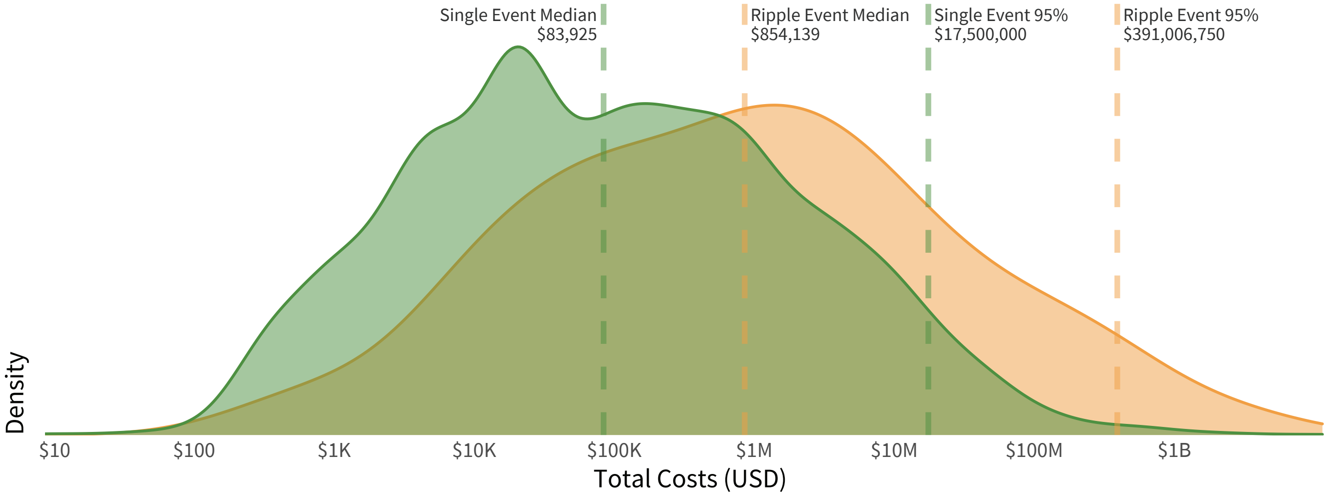


FIGURE 4: TOTAL RECORDED FINANCIAL LOSSES FOR SINGLE-PARTY VS. MULTI-PARTY SECURITY INCIDENTS

The fact that multiple parties contribute to multiplying costs is far from shocking. But it still serves as a reminder of risk accumulation. We tend to focus on assessing "our" (own) risk and don't always consider "our" (collective) risk. Are you ready if all those downstream losses wash back over your organization?

> “ **The median loss for multi-party incidents is over ten times that of their single-party cousins. Also notice that the tail is much thicker, indicating a higher propensity for major losses among ripple events.**

What caused the surge?

Having taken a few different readings about the size and scope of these digital tsunamis, our next question is what causes them. And just like in the previous section, there are several ways we can examine that. We'll start by dividing up events into high-level categories, then grouping them according to common incident patterns, and end with listing the most prevalent contributing threat actions.

Loss event category

It is common at the executive and board levels to slot cyber events in high-level categories that resemble those in Figure 5. These categories focus more on how the organization is affected rather than how the incident occurred. Some events exhibited both disruption and disclosure aspects, but we chose the category that best describes the primary nature of the incident.

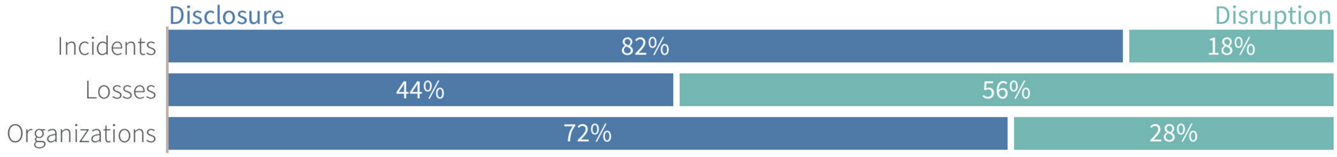


FIGURE 5: DISCLOSURES VS. DISRUPTIONS AMONG EXTREME MULTI-PARTY CYBER INCIDENTS

It is clear that most massive multi-party cyber incidents (41/50) fall in the data disclosure bucket. Also, it is apparent that these disclosure events are responsible for the majority of all downstream victim organizations (72%) identified in this study. Most secondary impacts were to either owners of the data compromised at a central victim organization or those experiencing losses from related fraudulent activity.

But those facts should, by no means, cause you to dismiss disruptive events. They racked up more total losses (almost $10 billion!), larger per-event costs, and a higher median number of affected parties. Thus, one could argue that, when they do occur, business disruptions tend to cause bigger ripples across business relationships than data disclosures.

Incident patterns

Beyond the broad categories of disclosures and disruptions, we'll now group incidents according to basic patterns that we've seen used in cyber risk management programs. These patterns are based on common actors, actions, technical impacts, etc. that collectively describe a general scenario. These incident patterns are described below, and an analysis of their frequency and impact follows suit.

- **DDoS attack**: Any attack intended to render online systems, applications, or networks unavailable, typically by consuming processing or bandwidth resources.
- **Exposed data**: Data stores that are inadvertently left accessible to unauthorized parties, typically through misconfigurations on the part of the data custodian.
- **Scam or fraud**: Incidents that primarily employ various forms of deception to defraud the victim of money, property, identity, information, etc.
- **System intrusion**: All attempts to compromise systems, applications, or networks by subverting logical access controls, elevating privileges, deploying malware, etc.

- **Insider misuse**: Inappropriate use of privileged access, either by an organization's own employees and contractors, or a trusted third party.
- **Physical threat**: Threats that occur via a physical vector, such as device tampering, snooping, theft, loss, sabotage, assault.
- **Ransomware or wiper**: The broad family of malware which seeks to encrypt data with the promise to unlock upon payment or seeks to completely eradicate data/systems without the pretense of collecting payment.
- **System failure**: All unintentional service disruptions resulting from system, application, or network malfunctions or environmental hazards.

Similar to when we studied **extreme cyber events**, system intrusions were by far the most common pattern (31/50 events). These incidents also impacted the largest number (57%) of downstream organizations and accounted for nearly a quarter of all financial losses. Again, we view this as a reflection of highly integrated B2B relationships.

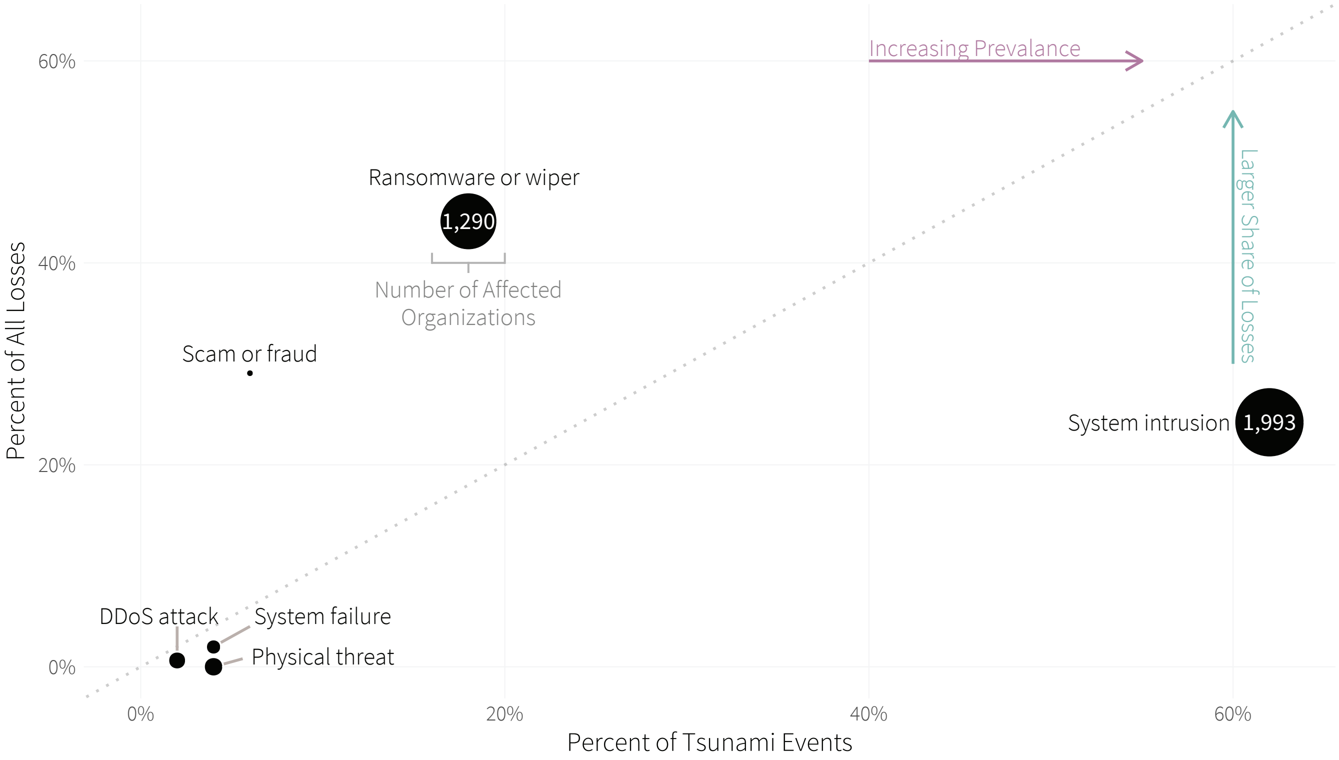


FIGURE 6: BASIC INCIDENT PATTERNS AMONG EXTREME MULTI-PARTY CYBER INCIDENTS

Ransomware lags as a distant second in terms of frequency but sprints to the top of the charts for total losses. It is responsible for an impressive 44% of recorded losses across all incidents. Add the 37% of secondary victims to that rap sheet, and it is apparent that ransomware is a heavyweight among major multi-party cyber loss events.

With one exception, the other patterns in Figure 6 come in ones and twos, not causing huge direct or collateral damage. The exception, of course, is fraud or scams with a big price tag of over $5 billion. But nearly that entire amount comes from an unusually hefty fine associated with just one incident—the **Facebook / Cambridge Analytica scandal**.

Initial Access Techniques

Now, we're shifting from the question of "what?" (categories and patterns) to a question of arguably more practical importance: "how?" We'll begin by reviewing the techniques for gaining **initial access** to target environments as defined in MITRE's **ATT&CK framework**.[3] Keep in mind that we're only looking at the initial vector into the first (central) victim organization here, which is why **supply chain compromise** is zeroed out. But don't despair—a more complete listing of all observed threat actions and the methods of propagation to downstream parties is coming right up.

It seems that abuse of **valid accounts** tops every single incident dataset that we examine, and this one is no exception. Guessed, cracked, stolen, or otherwise compromised (note **phishing** at number 5), credentials offer adversaries not only an entry vector, but elevated privileges and a cloak of legitimacy to boot. It is really no surprise that this technique was more common and more costly than any other means of initiating a successful attack.

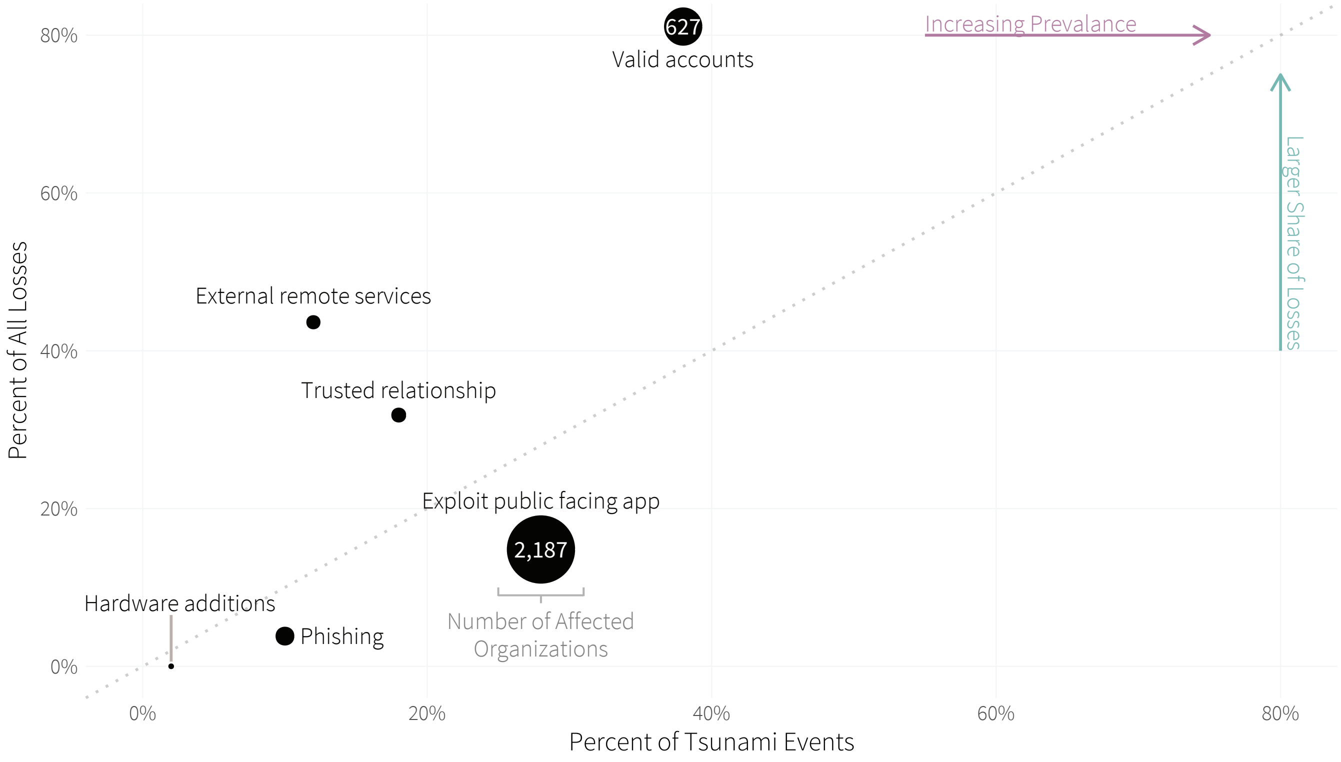


FIGURE 7: ATT&CK INITIAL ACCESS TECHNIQUES IN EXTREME MULTI-PARTY CYBER INCIDENTS

> **It seems that abuse of valid accounts tops every single incident dataset that we examine, and this one is no exception.**

[3] We attempted to identify one initial access technique for each incident, but the sequence of events was difficult to discern for a handful of events. We recorded both techniques in such instances, which is why incidents sum up to more than 50 and percentages exceed 100% in Figure 7.

While on the topic of subverting valid accounts, let's briefly touch on exploitation of trusted relationships. Similar to the abuse of valid accounts, the notion of trust is central to this technique. Why bother stealing credentials if you already have access? And for many organizations these days, the list of third parties capable of misusing that access is loooooong.

Circling back to the second-most frequent technique, we're reminded once again of how much threat actors love exploiting public-facing applications. This technique also led to more collateral victim organizations (63%) than any other. In the words of whoever's talking to Becky in *Baby Got Back*, they're "just so big" and "like out there." And all too many of them are riddled with unpatched vulnerabilities that make them the proverbial low-hanging fruit.

We'll end with a couple comments on external remote services because though not extremely prevalent, this technique led to surprisingly high financial losses. Again, we can't help but see the trust theme here because such services are deployed to support legitimate access. Figure 7 attests to what can happen when those services fall into the wrong hands.

> **"We're reminded once again of how much threat actors love exploiting public-facing applications. This technique led to more collateral victim organizations (63%) than any other.**

All observed threat actions

This section offers a broader view of every identifiable threat action[4] that is taken by actors across all phases of all incidents. The word *identifiable* is a key caveat here because this, as with everything else in this report, is based on what we could ascertain from publicly available information. An incident response team combing through the forensic evidence would undoubtedly be able to record it in more detail. That said, there are solid takeaways from Table 1, and we'll highlight just a few.

In case you're wondering, yes, credential attacks in Table 1 are pretty much synonymous with valid accounts from Figure 7. And call it what you will, compromising legit credentials once again reigns supreme as the leading contributor to both frequency and losses among this cohort of large multi-party incidents. The numbers don't line up because Table 1 includes events where credential attacks were used after initial access (e.g., for lateral movement). But seriously, don't fixate on those pedantries; just focus on rolling out multi-factor authentication across your enterprise and third-party accounts.

If criminals can't get in through the front door by stealing credentials, Table 1 suggests that they'll probably attempt to gain entry via a backdoor. Remote access malware contributed to the second-highest totals for event frequency (20) and losses ($11.6 billion). And it looks like there's a good chance they'll toss in malware that captures data (spyware, scrapers) while they're at it.

Since application exploits and abuse of legit admin tools (external remote services in ATT&CK lingo) have already been discussed, we'll skip over those. But the high costs associated with vulnerability exploits deserve a special mention…even though the importance of patching is cybersecurity 101. We know that it's impossible to patch all the things, but **our research** has proven that it is possible to patch the things most likely to lead to incidents such as those in this report.

There's a lot of additional commentary we could add from Table 1, but this report is long enough as is. Plus, you're a professional who's fully capable of picking out what's most useful for your unique needs and interests. We'll leave you to it—good luck!

[4] The threat actions in Figure 15 are based on VERIS, which has long been used in Verizon's vaunted Data Breach Investigations Report (DBIR).

Threat Actions

Category	Variety	Incidents	Total Losses	% of Losses	% of Orgs
Hack	Credential attacks	25	$11.9B	67.7%	55.2%
Malware	Backdoor	20	$11.6B	66.1%	43.9%
Malware	Spyware or scraper	17	$1.8B	10.4%	37.6%
Hack	Application exploit	12	$2.6B	14.7%	59.6%
Hack	Abuse legit admin tool	10	$10.2B	58.2%	31.4%
Hack	Vulnerability (CVE) exploit	10	$9.2B	52.6%	28.4%
Malware	Ransomware	10	$7.8B	44.3%	37.0%
Social	Phishing or pretexting	8	$1.0B	5.9%	4.8%
Misuse	Privilege abuse	4	$5.1B	29.1%	0.5%
Error	Misconfiguration	4	$540.0M	3.1%	7.0%
Physical	Theft	2	$150.0M	0.9%	1.2%
Social	Blackmail and extortion	2	$90.4M	0.5%	1.4%
Misuse	Policy violation	1	$5.1B	29.0%	0.1%
Malware	Cryptominer	1	$230.0M	1.3%	0.1%
Misuse	Knowledge abuse	1	$230.0M	1.3%	0.1%
Hack	DDoS	1	$110.0M	0.6%	1.9%
Error	Device malfunction	1	$35.0M	0.2%	0.1%
Physical	Physical destruction	1	$420.0K	-	1.3%
Physical	Equipment tampering	1	$420.0K	-	1.3%

TABLE 1: ALL THREAT ACTIONS OBSERVED AMONG EXTREME MULTI-PARTY CYBER INCIDENTS

How do ripples propagate?

This question may well be top of mind moreso than any other for a study on this topic. That is why we made it a point to learn as much as we could about how these incidents, or their impacts, spread from the initial victim organization to downstream parties.

While reviewing the findings in this section, it is important to remember that the nature of what we call "ripples" varies substantially among incidents. For some events, ripples may come in the form of threat actors that move from the systems of one organization into those of another. For others, ripple effects may take the form of operational or financial impacts to partners and customers. This concept of ripples is probably best exemplified by the categories we derived from studying these cyber tsunami events, so let's jump right into Figure 8.

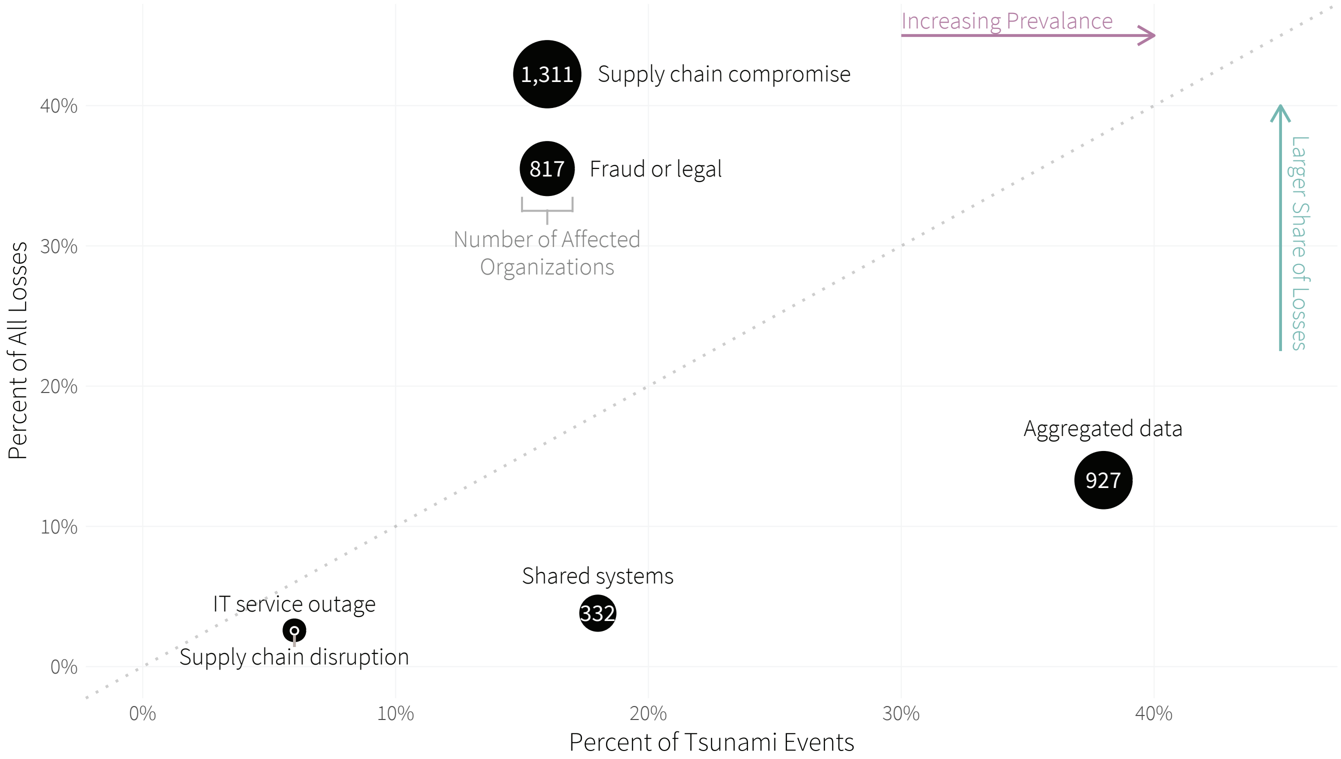


FIGURE 8: DOWNSTREAM PROPAGATION METHODS IN EXTREME MULTI-PARTY CYBER INCIDENTS

The most common form of ripple propagation that we observed is the compromise of multi-party data aggregated by the initial victim organization. The systems of downstream parties are not breached in this scenario, but those organizations nevertheless suffer various consequences as owners of the disclosed data. This is doubly unfortunate for the original data owners because they have little ability to protect the data once it has been shared. The best protection is to choose data custodians wisely and check regularly to ensure that they uphold their end of the bargain.

> **For some events, ripples may come in the form of threat actors that move from the systems of one organization into another. For others, ripples may cause operational or financial impacts to partners and customers.**

The ripple vector of shared systems comes next on the list in terms of frequency. This scenario *does* involve the compromise of systems owned or used by downstream parties. In some cases, all organizations share centralized applications such that a breach of one escalates to become a breach of many. But in others, interconnectivity and trusted access enable propagation to additional systems and organizations. If you are curious about how actors accomplish this feat, refer back to the threat actions listed in Table 1. The lesson here is that trusted systems easily become busted systems without proper 3rd party access controls.

Ripples taking the form of supply chain compromises led to the biggest share of recorded financial losses ($7.4 billion) and the largest number of secondary victim firms. This seemed rather important, so we leveraged **sub-techniques** defined by ATT&CK to dig deeper into this ripple propagation vector. This breakdown can be found in Table 2.

ATT&CK Supply Chain Sub-techniques

	Incidents	Total Losses	% of Losses	% of Orgs
Compromise software supply chain	5	$7.4B	42.1%	27.8%
Compromise software dependencies & development tools	3	$29.4M	0.2%	9.8%

TABLE 2: SUPPLY CHAIN COMPROMISE TECHNIQUES USED IN EXTREME MULTI-PARTY CYBER INCIDENTS

We came across no examples involving compromised **hardware components** moving through the supply chain prior to receipt by the end customer. Of the eight supply chain attacks we identified, five targeted **software distribution** mechanisms and three exploited third-party or open source **software dependencies**. Nearly all losses were associated with the former, and it was this sub-technique that was leveraged in the recent high-profile breaches of SolarWinds and Kaseya. The need to distribute and update code as well as leverage the benefits of third-party dependencies is fundamental to modern software development practices. Cyber adversaries, of course, are well aware of this, meaning this trend is likely to get worse before it gets better.

While on the topic of supply chains, we'll go ahead and mention ripples that take the form of disruptions flowing downstream from the central firm. The key difference here is that no hardware or software distribution channels were compromised. Instead, think of scenarios where an incident hampers a firm's ability to deliver goods and services to their partners and customers. Those organizations will experience impacts and losses because of delays or disruptions.

The other big-ticket item among ripple vectors is fraudulent activity or legal action. All of these stem from large data breach events in which impacted parties sought compensation for damages incurred. As Figure 8 makes plain, these damages can be quite hefty. Ripples of this kind can propagate more slowly, sometimes taking years to fully manifest.

Last, but not least, IT service outages made our set of ripple vectors. Of them all, this is the quickest and most direct method of propagation. As soon as the central organization (typically a hosting or SaaS provider) experienced the outage, so too did all parties relying on those services.

> **“ The most common form of ripple propagation we observed is the compromise of multi-party data aggregated by the initial victim organization. But ripples taking the form of supply chain compromises led to the biggest share of recorded financial losses ($7.4 billion) and the largest number of secondary victim firms**

Who's making waves?

With "*what?*" and "*how?*" in the bag, this last section is dedicated to "*who?*" You could argue that we should have started here since every one of these incidents began with someone who precipitated everything we've discussed so far. But that's exactly why we saved this for last; the prior context should help us better understand the threat actors behind extreme multi-party cyber events. As a heads up, they might be who you'd expect.

Threat actors

Similar to most other incident data sets that we've seen, this one featuring large ripple events points to external threat actors as the most common perpetrator. As per Figure 9, they were also behind more total financial losses (69%) and nearly all secondary organizations (97%) that were impacted by these incidents. Since outsiders encompass a large and diverse collection of potential ne'er-do-wells, we attempted to distinguish the type of external threat actor in Figure 10.

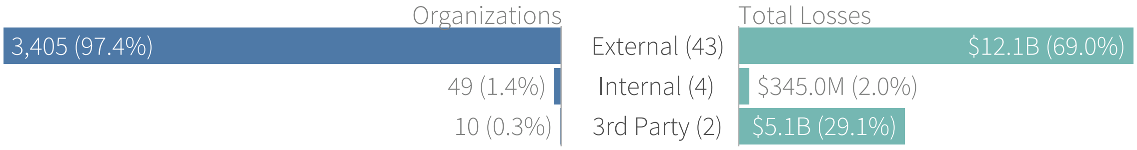


FIGURE 9: THREAT ACTOR CATEGORIES IN EXTREME MULTI-PARTY CYBER INCIDENTS

It probably won't come as a surprise to anyone to learn that the majority of external actors behind these events represent various professional cybercriminal organizations. We can also point to them as being responsible for 80% of all collateral damage caused to downstream firms. They're constantly adding to the hot mess that the modern Internet has become. May they one day eat the "fruits" of their labor.

What might come as a shock from Figure 10 is how prevalent and pernicious state-affiliated groups are among these incidents. We attribute one in five of the largest multi-party loss events in recent history to state-affiliated actors. Furthermore, those actors caused the majority of financial losses, with over $10 billion recorded on their tab! Who says government can't be effective?

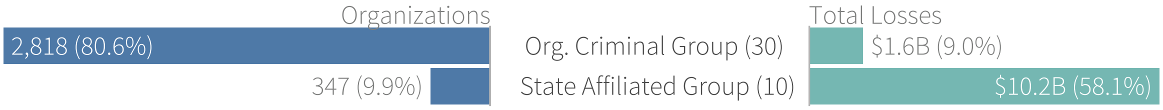


FIGURE 10: ORGANIZED CRIMINAL VS. STATE-AFFILIATED ACTORS IN EXTREME MULTI-PARTY CYBER INCIDENTS

It's an old mantra in InfoSec that insiders are responsible for 80% of risk, and our research bears that out. But not in the way you think. Insiders are *villains* far less often than they're *vectors*. Figure 9 focuses on the former, which is why the numbers seem less than impressive to insider risk proponents. But a quick glance back at Table 1 will reveal numerous threat actions that rely on insiders as a vector—including the top dog of them all, credential attacks.

As trusted entities, the same "*vector more than villain*" principle applies to third parties. They didn't intentionally or maliciously take part in many of these events, but credentials, remote services, etc. provided to them certainly made a big contribution behind the scenes. Also, don't forget that Figure 9 is concerned strictly with who was behind the initial incident. Every single one of the thousands of secondary loss events that resulted from those initial incidents can be attributed to third parties.

We could leave it there, but we have a thing against making claims without backing them up with data. So we're going to quickly do that. If you take the incidents from Figure 9 along with threat actions from Table 1 that involve or target trusted parties, some pretty big numbers pop out of the calculator. All told, insiders and third parties caused or indirectly contributed to 34 of the 50 extreme events we analyzed for this study. Those 34 events carry a combined price tag of $17.3 billion—99% of all recorded losses!

Bottom line - don't assume your employees and third parties are out to do you harm. That won't create a healthy or secure business relationship. But you also shouldn't assume that all will be well if everyone just joins hands and sings *Kumbaya*.

Initial victims / Ripple generators

We'll touch on one final aspect of the "who" behind these mega multi-party loss events—the central victim firm. More specifically, which types of organizations most often generate tsunami events? Figure 11 lists the generating sectors as well as the ripple propagation methods observed among them. We caution against drawing too much from these 50 incidents, but there are a few interesting observations we feel safe in making.

	Information	Profession.	Financial	Administra.	Hospitality	Manufactur.	Retail	Public
Aggregated data	4	7	5	2				1
Shared systems	3			2	4			
Supply chain compromise	4	3		1				
Fraud or legal	2	1	1		1		3	
Supply chain disruption						3		
It service outage	1	1	1					

FIGURE 11: SECTORS OF CENTRAL VICTIM ORGANIZATIONS AND VECTORS OF SECONDARY IMPACTS

First, the Information and Professional sectors were most often at the center of cyber tsunamis in this study. This makes even more sense when we understand that these typically map to software development and IT service providers, respectively. Similarly, most victims in the Administrative sector (fourth in the pack by total tsunamis) can be viewed as ancillary services to the Financial sector (third by total tsunamis)–think credit bureaus, consumer credit ratings, collection agencies, etc.

The prevalence of fraud or legal ripples among the Hospitality and Retail sectors checks out given their contact with cardholder information, although Hospitality (read: mostly chain restaurants) serves up the largest number of secondary impacts via Shared systems. As a sector, it has all the ingredients of a prime target for criminals: small margins to dedicate to overmuch security, an emphasis on speed, and tasty data.

Lastly, Manufacturing, the sole representative of the Supply chain disruption type: as much as security professionals may talk about availability impacts on a company's bottom line, these tsunamis are in a class of their own where delays can result in train cars backing up literally.

Sponsor Insights

interos

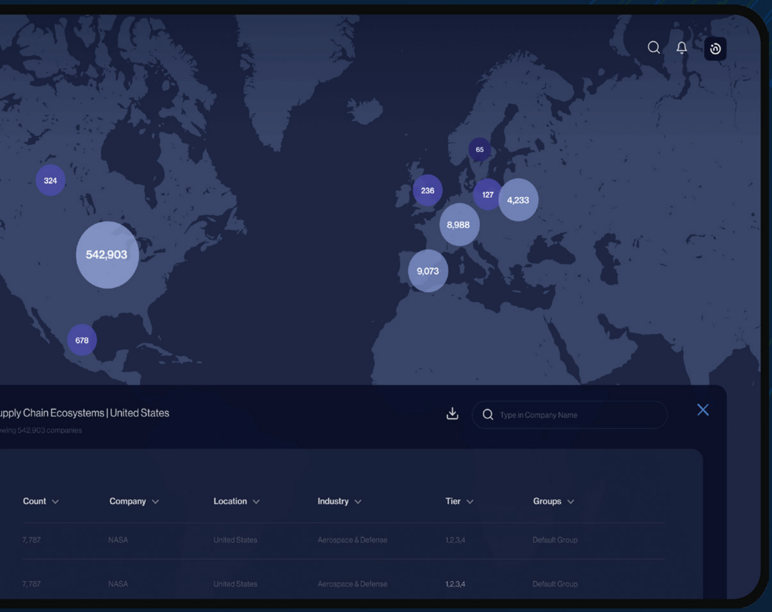
Organizations cannot afford to ignore the staggering cost of supply chain driven cyberattacks compared to single party incidents. But how can you prevent a single event from turning into a tsunami that ripples throughout your supply chain? As our analysis demonstrated, ripple events don't occur just through compromises of all partner organizations. They can also occur through shared systems, multiple parties with access to data, as well as compromised software. To build resilience against these ripple events, let's return to our emphasis on focusing on the "vector more than the villain."

Third parties aren't inherently malicious, they don't intentionally compromise their partners, but they do introduce significant risks to your data and your business. By thinking beyond perimeter defenses and reframing third parties as extended insiders, organizations can become more resilient against the vast range of ways ripples propagate. So how should organizations get started?

First, companies need to begin tackling the fundamental flaw that leaves almost every business vulnerable: limited insight into their extended supply chain. They may know their initial suppliers well but lack visibility into their extended supply chain beyond the first tier. This visibility is essential to foster collective security across your supply chain network and can help promote vital information sharing and collaboration to raise the security posture of everyone in the network.

Second, businesses need to look for ways to break the annual cycle of supply chain monitoring. These relationships require continuous monitoring and assessment as both the threat landscape and business relationships can evolve and change quickly. Staying on top of these changes is essential to stopping these ripple events and can inform a range of data strategies such as access controls, minimization, and storage.

Finally, the average global brand has tens – if not hundreds – of thousands of suppliers. It is almost impossible (and extremely inefficient) to manually monitor and investigate all of them. Fortunately, technology and big data can help! Look for automated solutions that allow you to easily surface and navigate your extended supply chain.



upply Chain Ecosystems | United States

wing 542,903 companies

Count	Company	Location	Industry	Tier	Groups
7,787	NASA	United States	Aerospace & Defense	1,2,3,4	Default Group
7,787	NASA	United States	Aerospace & Defense	1,2,3,4	Default Group

Resilient companies should look to make use of every bit of threat information they can, beyond the standard sources of information. Tools using advanced analytics or machine learning coupled with traditional threat intelligence, logs, and other information gathered from structured and unstructured data can expose relationships you may not have been aware of, while also revealing unknown risks and alerting you to potential threats in near-real time. Which suppliers have a history of compromised data? Or conversely, which ones are proving more resilient?

The scale of losses from tsunamis shouldn't be minimized, but companies should be encouraged by the similarities among these and more run-of-the-mill incidents. An otherwise sound data protection strategy combined with a plan to uncover your company's extended supply chain could be all it takes to keep from being swept away.

Sponsor Insights

Ready to take the insights from this report and manage your third-party cyber risk surface? Here are some pointers to get you started:

» Don't rely on only one risk management method to get the job done. When it comes to third-party cyber risk management, companies need a methodology that blends an array of safeguards, including threat intelligence and comprehensive data analytic capabilities.

» Utilize an extensive tool like the CyberGRX platform that incorporates threat intelligence for visibility. Complete visibility into the security posture of one's vendor ecosystem is key to combating the ripple effects of a tsunami.

» When doing business with third parties, only share data that's absolutely necessary given the nature of the relationship with the other organization.

» Work with a vendor that helps you identify trends and create benchmarks by leveraging structured data and actionable intelligence.

Build a cyber-centric risk management program to help you make fast, informed decisions to support business needs while protecting from cyber threats, both emerging and existing. You can learn more about one such emerging cyber threat ("extortionware") on page 5 of our ebook https://content.cybergrx.com/ransomware-v2/Ransomware-third-parties-ebook.

Exclusive Study: *Why Your Third Parties Aren't Prioritizing Cyber Risk*

Executed by Forrester Consulting, the research uncovered that 67% of organizations surveyed experienced a third-party risk incident in the last year.

Did you know that even though organizations recognize third-party threats expose them to great risk, many fail to take adequate measures to mitigate it?

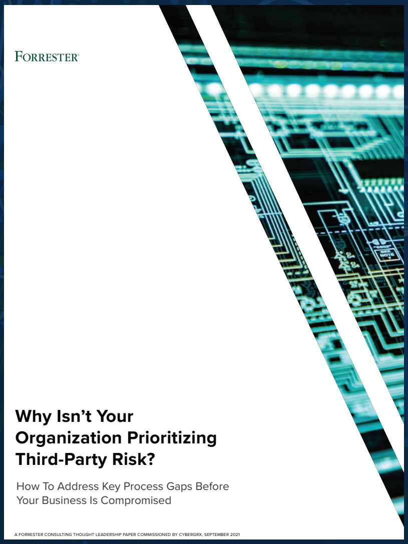
The report identifies four major themes:

» How today's organizations constantly exchange confidential information with third parties and why this exposes both sides to significant cyber risk

» Why current third-party risk prevention strategies leave organizations vulnerable

» Who tends to ignore safe risk management practices the most

» What a third-party risk strategy must contain in order to be successful


FORRESTER

Why Isn't Your Organization Prioritizing Third-Party Risk?

How To Address Key Process Gaps Before Your Business Is Compromised

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY CYBERGRX, SEPTEMBER 2021

Download your complimentary copy today! https://info.cybergrx.com/download-forrester-report

Sponsor Insights

The waves created from multi-party cybersecurity incidents can range from tiny to epic, as noted in this report. The goal of this study was not to scare people, it was created to raise further awareness about the wide-reaching scale of cyber threats posed by third parties, fourth parties, and Nth parties. Threats might not affect you directly, but the main takeaway from this report should be that you do not want to be a part of any wave, tsunami, or otherwise. Every organization needs to have complete visibility into these risks and has to be able to move quickly, acting on threats that could cause serious harm to their business.

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 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)

Outer Rim Supply

Example Site: outerrimsupply.com

Internal References Edit
Internal Name
Testing Company
Internal ID:
Test Version II

Risk Relationship Edit
High - Vendors
High - Partners
Moderate - Human Resources
+3 More

Software Patching — Base Weight: 30%

Security Criteria	Rating	Issues
Application Server Patching	F 2.8	100
Open SSL Patching	A 9.6	0
CMS Patching	B 7.0	5
Web Server Patching	C 6.2	10

Application Security — Base Weight: 12.5%

Security Criteria	Rating	Issues
CMS Authentication	F 2.8	890
HTTP Security Headers	A 9.6	0
External Threat Intelligence Alerts	Info	1
High Value System Encryption	Info	2
Malicious Code	Info	5

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

Appendix A: Detailed Data Tables

Top Level Incident Categories

	Incidents	Total Losses	Median Losses	Total Orgs	Median Orgs
Disclosure	41	$7.7B	$40.1M	2,522	30
Disruption	9	$9.9B	$182.5M	973	49

TABLE A1: DISCLOSURES VS. DISRUPTIONS AMONG EXTREME MULTI-PARTY CYBER INCIDENTS

Incident Patterns

	Incidents	Total Losses	% of Losses	% of Orgs	Median Orgs
System intrusion	31	$4.3B	24.2%	57.0%	30
Ransomware or wiper	9	$7.8B	44.1%	36.9%	49.5
Scam or fraud	3	$5.1B	29.1%	0.4%	-
System failure	2	$345.0M	2.0%	1.2%	-
Physical threat	2	$420.0K	-	2.4%	-
DDoS attack	1	$110.0M	0.6%	1.9%	-
Exposed data	1	-	-	0.1%	-
Insider misuse	1	-	-	0.1%	-

TABLE A2: BASIC INCIDENT PATTERNS AMONG EXTREME MULTI-PARTY CYBER INCIDENTS

ATT&CK Initial Access Techniques

	Incidents	Total Losses	% of Losses	% of Orgs
Valid accounts	19	$14.3B	81.1%	17.9%
Exploit public facing app	14	$2.6B	14.8%	62.6%
Trusted relationship	9	$5.6B	31.8%	2.6%
External remote services	6	$7.7B	43.6%	2.4%
Phishing	5	$672.4M	3.8%	4.0%
Hardware additions	1	$420.0K	-	1.3%

TABLE A3: ATT&CK INITIAL ACCESS TECHNIQUES IN EXTREME MULTI-PARTY CYBER INCIDENTS

Ripple Propagation

	Incidents	Total Losses	% of Losses	% of Orgs
Aggregated data	19	$2.3B	13.3%	26.5%
Shared systems	9	$669.3M	3.8%	9.5%
Supply chain compromise	8	$7.4B	42.2%	37.5%
Fraud or legal	8	$6.2B	35.5%	23.4%
IT service outage	3	$455.0M	2.6%	3.1%
Supply chain disruption	3	$449.0M	2.6%	-

TABLE A4: DOWNSTREAM PROPAGATION METHODS IN EXTREME MULTI-PARTY CYBER INCIDENTS

Generating Industries

	Incidents	Total Losses	% of Losses	% of Orgs
Information	14	$5.5B	31.2%	30.9%
Professional	12	$7.6B	43.3%	33.9%
Financial	7	$2.8B	16.0%	21.9%
Hospitality	5	$497.6M	2.8%	9.1%
Administrative	5	$66.0M	0.4%	1.2%
Retail	3	$651.4M	3.7%	1.9%
Manufacturing	3	$449.0M	2.6%	0.0%
Public	1	-	-	1.1%

TABLE A5: SECTORS OF CENTRAL VICTIM ORGANIZATIONS AND VECTORS OF SECONDARY IMPACTS

Cyber GRX

CyberGRX brings a revolutionary approach to Third-Party Cyber Risk Management. Using sophisticated data analytics, real-world attack scenarios, and real-time threat intelligence, we provide a complete portfolio analysis of a company's third-party ecosystem, helping the world's leading businesses prioritize their risks and make smart decisions.

interos

Interos is the operational resilience company — reinventing how companies manage their supply chains and business relationships — through our breakthrough SaaS platform that uses artificial intelligence to model and transform the ecosystems of complex businesses into a living global map, down to any single supplier, anywhere. For more information, visit www.interos.ai.

riskrecon
mastercard

RiskRecon is the only continuous vendor monitoring solution that delivers risk-prioritized action plans custom-tuned to match your risk priorities, providing the world's easiest path to understanding and acting on third-party cyber risk. Learn more about RiskRecon and request a demo at www.riskrecon.com.

119 Cyentia INSTITUTE

The Cyentia Institute is a widely-respected research and data science firm working to advance cybersecurity knowledge and practice. We accomplish that goal by collaborating with security companies to publish data-driven reports on a range of topics and through analytic services that help our enterprise customers manage cyber risk.