Cyentia INSTITUTE

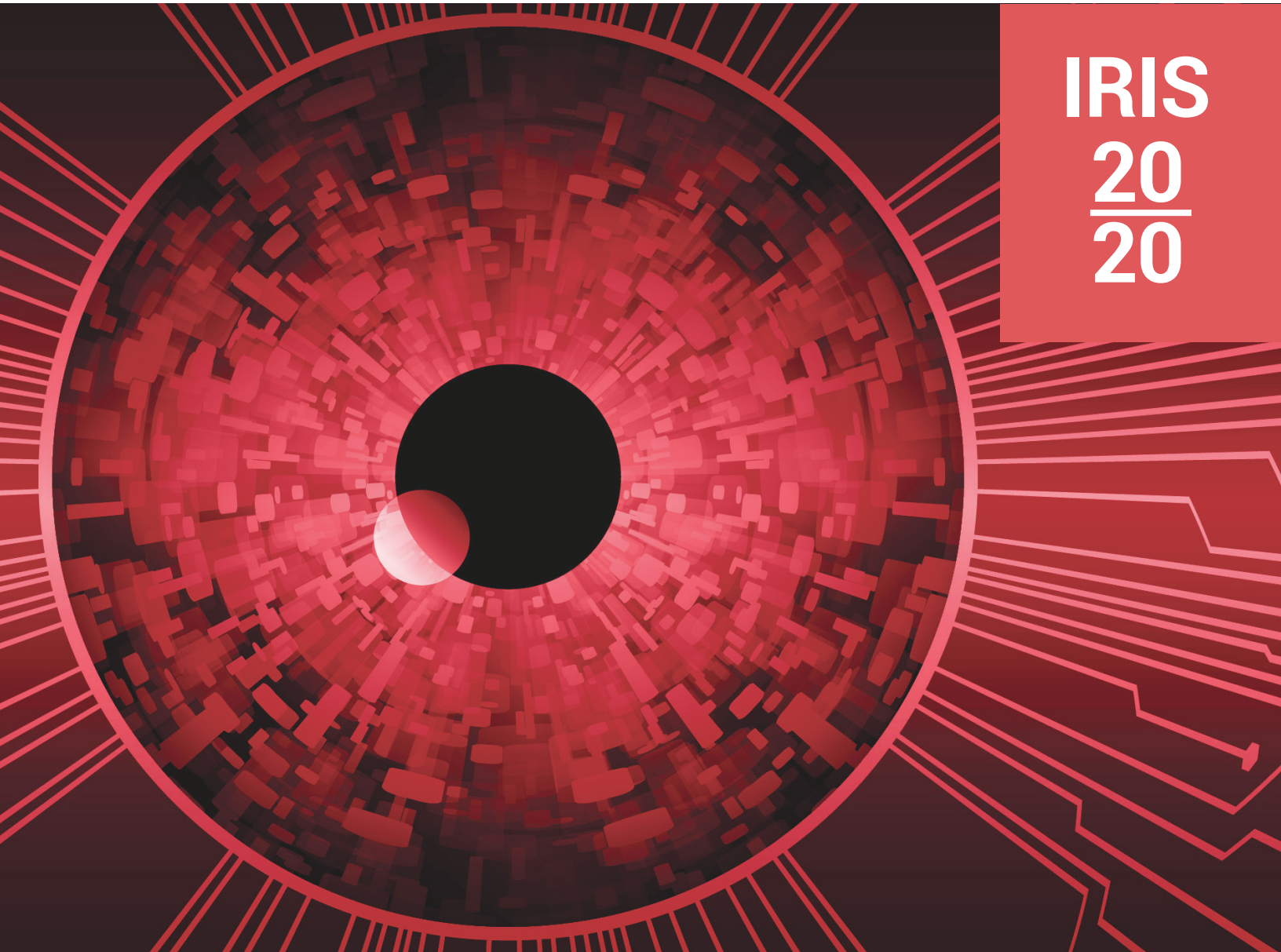
Sponsored by:

VISIBLERISK

IRIS 20/20 XTREME

Information Risk Insights Study

Analyzing the 100 largest cyber loss events of the last five years



Light Through the IRIS

Early in 2020, the Cyentia Institute published the Information Risk Insights Study (IRIS 20/20). This first-of-its-kind study leveraged a vast dataset from Advisen, spanning tens of thousands of cybersecurity incidents over the last decade. Our extensive analysis of that dataset yielded valuable insights about the frequency and financial impact of cyber incidents to organizations of all types and sizes.

The IRIS 20/20 Xtreme is a follow-up to that research, focusing on the 100 largest cyber incidents of the last five years, totaling $18 billion in reported losses and 10 billion compromised records. We once again started with Advisen's Cyber Loss Data and then collected hundreds of additional data points on each of these extreme cyber loss events. Our goal was to breakdown the costs, categorize incident types, identify the actors behind these events and the actions they employed, and better understand how these events impacted the organizations involved. Our primary goal remains the same as the IRIS 20/20—to clear the fog of fear, uncertainty and doubt (FUD) surrounding cyber risk and help managers see their way to better data-driven decisions.

Share your thoughts: #iris2020

Table of Contents

Like what you see? *Join the vision!*

We will continue the IRIS research series in the future to discover even more insights for managing information risk. If you'd like to join in that effort by contributing relevant data or sponsoring a study, please reach out to us at research@cyentia.com.

Key Findings

$47M The median loss for incidents meeting our qualifications for "extreme" is $47M, with just over one-in-four exceeding $100M; five events racked up $1B or more in losses.

Relative to annual corporate revenues, losses from these events range from less than 0.1% to nearly 100 times the affected firm's revenue!

Response costs, lost productivity, and fines and judgements are the most common forms of loss in extreme events.

Firms that bungle the incident response process show costs that are nearly 2.8 times larger than those without signs of poor response.

Apart from hard costs, 27 events were reported in U.S. Securities and Exchange Commission (SEC) filings, 25 triggered executive changes, and 23 prompted government inquiry.

The financial and information sectors, with their large holdings of funds and data, have experienced the largest number of extreme loss events (22 and 18, respectively).

Data breaches, ransomware, fraud, and cryptocurrency theft are by far the most common and costliest types of extreme cyber events.

One in five of the largest losses over the last five years are attributed to state-affiliated actors. All told, they're responsible for 43% of all monetary losses in this study!

A single campaign, NotPetya, was responsible for nearly 20% of all financial losses across these 103 extreme events.

$10B Stolen passwords and other credential-related attacks led to more incidents (46) and more total losses ($10B) than any other threat action.

Remote access malware planted by actors contributed to the second-highest totals for event frequency (31) and losses ($9.2B).

Web application attacks placed third in frequency (25 events; $2B), but exploitation of known and patchable vulnerabilities ranked third in cost (22 events; $8B).

Looking for Xtreme Data?

The Cyentia Institute and Advisen have partnered to make this rich dataset of extreme cyber loss events available as a subscription. In addition to the 103 incidents analyzed in this study, Cyentia will continue collecting data on new extreme events that occur in the future. If interested in learning more, reach out to extremeevents@advisen.com.

119 Cy cyentia

Some Opening Thoughts

The number of high-profile cyber attacks during the last decade have caused businesses—along with their directors and executives—to finally acknowledge that these attacks have the potential to create serious consequences for employees, investors and customers.

Now that we can all agree these are important, how should business leaders calibrate their expectations for mitigating the risks associated with these events?

On one end of the spectrum are high frequency, but relatively low impact, events. These day-to-day issues are the remit of information security practitioners who must maintain a rising defensive baseline in order to rapidly identify and contain threats that jeopardize their business, and their employees' and customers' security and safety. More importantly, these teams must constantly evaluate these smaller events to make sure they do not persist and metastasize into something more significant.

But what does "significant" mean? It depends on your business—its size, its sector, the way in which it delivers value to customers. A significant cyber event often results in damage to a company's reputation, increases its oversight by regulators, and can even impact the careers of the executives involved. In a traditional context, risk experts often classify these events as "maximum loss" at two standard deviations, or roughly the 95% on a loss chart.

When I first met with Wade Baker to discuss IRIS Xtreme, what resonated with me was the idea that there were some very business-relevant events existing in the gray area between commonplace events and the worst kinds of cyber breaches that live at the very edge of the curve.

These extreme events, which sit somewhere slightly left of that maximum loss, are interesting for a very specific reason -- they are happening with surprising regularity. This paper seeks to further explore these events. I believe this will be an important starting point for the next chapter in how we communicate about these cyber events and protect our organizations.

- Derek Vadala, CEO at VisibleRisk

VISIBLERISK

VisibleRisk is a joint venture between Moody's Corporation, a global leader in risk assessment, and Team8, a cybersecurity-focused company creation platform, that is focused on creating a standard benchmark for communicating cyber risk to Boards of Directors and senior business executives in order to improve the global dialog about this important issue. Learn more at www.visiblerisk.com

119 Cyentia INSTITUTE

The Cyentia Institute is a research and data science firm working to advance cybersecurity knowledge and practice. We do this by partnering with vendors and other organizations to publish a range of high-quality, data-driven content like this study. Learn more at www.cyentia.com

Join the IRIS 20/20 Xtreme discussion on Twitter: #iris2020

What is an "Extreme" Cyber Event?

This section kicks things off by establishing what we mean by an "extreme" loss, and how we identified the events for inclusion in this study. Let's begin by revisiting a key chart from the IRIS 20/20[1], based on Advisen's Cyber Loss data. Readers may recall that the typical loss across 10 years of publicly discoverable incidents was about $200K. The distribution around that typical loss formed a long tail to the right, which is why we made a point of using a log scale for the chart. Losses from cyber incidents neatly fit a lognormal distribution.

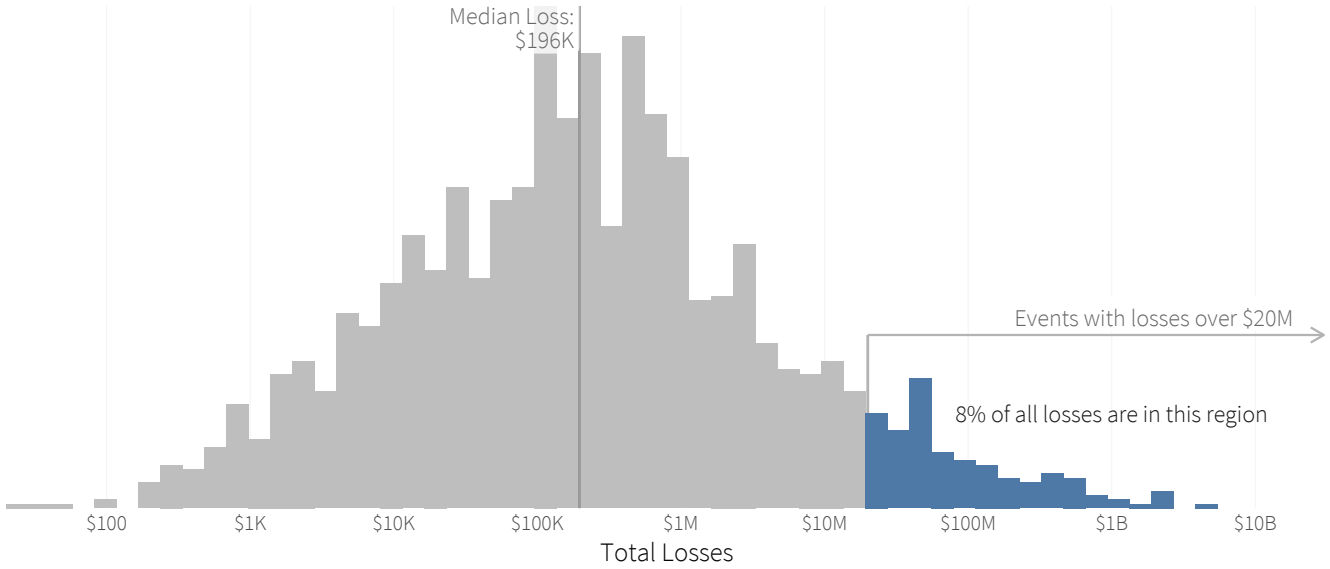


Figure 1: Distribution of cyber event losses on a log scale

According to Figure 1, roughly 10% of all the IRIS 20/20 loss events exceed $20M. For the more stat-philic readers, a $20M loss represents the 92nd percentile or 1.5 standard deviations from the mean (in log space). That $20M mark created a convenient threshold for our study of extreme events.

We set out with the goal of including 100 events in this study but were surprised to find that we weren't able to hit that target based on a $20M threshold. Only 56 security incidents over the last five years have publicly discoverable losses of or above $20M. That little data point by itself serves up some food for thought, but we're on a mission, so let's move on.

To bridge the gap to reach our goal of 100 events, we added data breaches that exposed at least 20M records. Across all breaches in our dataset, only about 0.5% exceeded that number. We're talking about the razor's edge here, folks (of the distribution—not the AC/DC album)! After removing events that didn't qualify or have sufficient information, this added 47 incidents to our Xtreme dataset for a total of 103. Goal met, huzzah!

[1] https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf

The SEC **provides guidance** on what constitutes the "materiality" of cyber events, but it doesn't provide any quantifiable criteria. The gist is that companies should weigh the nature and extent of damages, importance of compromised information, operational impacts, and risk of litigation or regulatory actions. Our approach of identifying the largest financial and/or data loss events seems to be in line with that guidance.

Of the 103 events in this study, we found a reasonable estimate of loss for 74. However, our confidence in the totality and accuracy of those values varied substantially. For some events, we had very detailed information provided by the victim organization in their official financial reports. Those numbers were scrutinized by regulators and investors and ostensibly represented reality to the best of the firm's knowledge. For others, we found only part of the overall loss (i.e., fines or response costs). We also saw a lot of "could be as much as $X" type estimates and did our best to track down more precise numbers, not accepting vague hand-waving estimates. The main point to keep in mind is that the losses we analyze in this study represent conservative estimates from public sources.

Extreme: More than Words

A wise group of musicians once said that "more than words is all we have to do to make it real."[2] So in that spirit, this section offers some examples and statistics to help you get familiar with these extreme events. We start off with plotting losses for each incident in our sample in Figure 2.

We need to be careful with summary statistics on these extreme losses because they represent just the tail end of the broader distribution. That said, they're a handy reference. The median loss *for incidents meeting our qualifications for "extreme"* is $47M, with just over one-in-four exceeding $100M. Only five events racked up $1B or more in losses, and those are labeled in Figure 2. If $1B is the threshold for tech unicorns, perhaps we need a Dark Unicorn theme for these largest of the large losses?

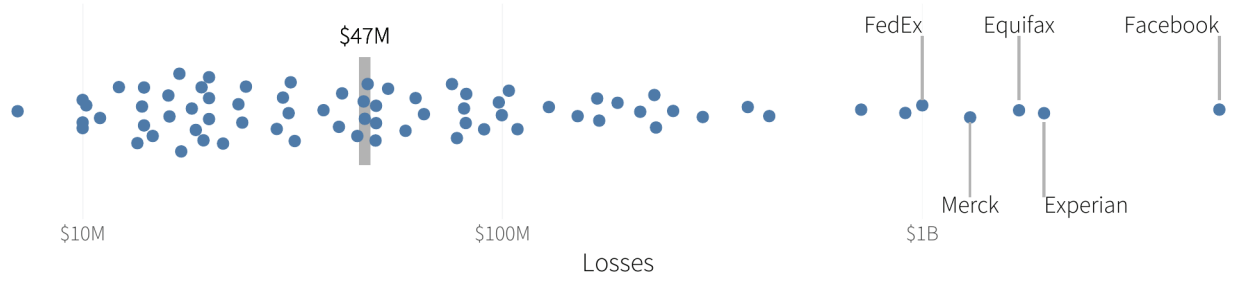


Figure 2: Distribution of extreme cyber event losses by overall magnitude

Table 1 lists those Dark Unicorns and the next five largest loss events to round out the top 10. Absolute losses—especially when they're as large as these—demand attention, but what constitutes "extreme" is an admittedly relativistic concept. And that's why we've included a column presenting these incident costs as a percentage of annual revenue. From that perspective, it's clear that relative losses range from less than 1% of revenue to over 130% for these 10 largest events. But you ain't seen nothing yet.

[3] *Enjoy the memories: https://www.youtube.com/watch?v=UrIiLvg58SY*

Top 10 Losses by Total Loss

Company	Percent of Revenue	Loss
Facebook	7.2%	$5.1B
Experian Plc	41.8%	$2.0B
Equifax Inc.	48.2%	$1.7B
Merck & Co Inc.	2.8%	$1.3B
FedEx Corp.	1.4%	$1.0B
Monex Group, Inc.	134.1%	$911.0M
British Airways Plc	4.2%	$715.1M
Marriott International Inc	2.1%	$432.0M
Saint-Gobain	0.8%	$384.0M
Maersk	0.8%	$300.0M

Table 1: Largest cyber loss events by absolute value

Typical Extreme Loss

$47M

OVER $100M

28%

OVER $1B

5%

As we demonstrated in the IRIS 20/20, the size of the organization (as measured by annual revenues) is a very useful discriminator when analyzing the impact of incidents. We pick up this torch again to review the extremity of losses as a percentage of revenue in Figure 3 and Table 2.

Figure 3 reveals a clean 70/30 split between events costing below/above 10% of the affected firm's annual revenue. However, the losses run the gamut from less than 0.1% of revenues to nearly 100 times revenue! We find it interesting that even this extreme tail of losses has a tail (and a tale) of its own.

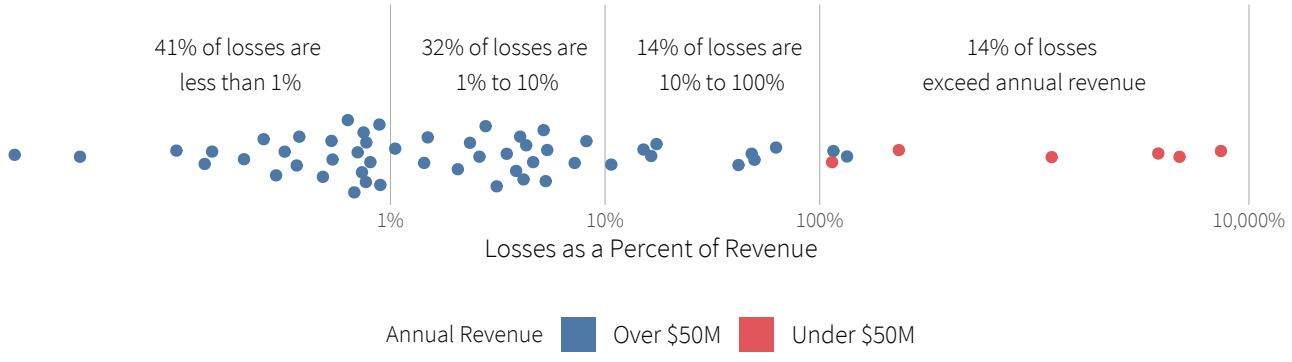


Figure 3: Distribution of extreme event losses as a percentage of annual revenue

Now, we're ready to bring the company size distinction from Figure 3 into focus. It's immediately apparent that blues (the larger organizations) cluster toward the lower end of the scale, while the reds (the smaller firms) are in the upper tail. This reinforces findings from the IRIS 20/20 that major cyber loss events cause far greater relative harm to small and medium-sized businesses (SMBs) than larger enterprises.

Top 10 Losses as a Multiple of Revenue

Company	Loss	Revenue Multiple
Remixpoint Inc	$32M	74.1x
Tether	$31M	47.5x
Ruby Corp.	$213M	37.8x
Tech Bureau, Corp.	$62M	12.1x
Pathe	$22M	2.3x
Monex Group, Inc.	$911M	1.3x
Crelanco	$76M	1.2x
AMCA	$10M	1.1x
Mondelez International Amea Pte. Ltd.	$188M	0.6x
Leanus	$50M	0.5x

Table 2: Largest cyber loss events as a multiple of revenue

Table 2 adds some context to the rightmost dots in Figure 3. It's worth noting that the majority of companies are classified as SMBs, further emphasizing the point made above about greater potential relative harm for smaller companies. Another thing we quickly noticed is that several of these most extreme relative losses are cryptocurrency exchanges or play in that space. The loss-to-revenue ratios venture well into funny money style figures—ironic, no?

Though not the largest relative loss, one event worth highlighting is the infamous Ashley Madison (Ruby Corp) breach,[3] where the losses reflected a cancelled IPO estimated at a value of $200M (many times their annual revenue). This also serves as a good example of the many gray areas in conducting research on the impact of cyber events. Ashley Madison didn't actually lose that money out of pocket, but it's a reminder of softer opportunity costs that also need to be considered. Beyond this example, we employed a hard-nosed approach of requiring evidence of actual loss.

> "This reinforces findings from the IRIS 20/20 that major cyber loss events cause far greater relative harm to small and medium-sized businesses (SMBs) than larger enterprises.

[3] *Infamous for largely picking up a pool of people looking to commit affairs on their spouses: https://en.wikipedia.org/wiki/Ashley_Madison_data_breach*

Who's Getting Caught-up in the Tail?

Going beyond the specific companies listed in Tables 1 and 2, there's a more general question we hear a lot from risk managers—"are organizations, like mine, especially susceptible to these extreme losses?" We'll now shed some light on that with a brief review of the regions and industries represented in the rightmost tail of cyber events.

From a regional perspective, these incidents span organizations headquartered across the globe. The majority of firms hailed from North America (46%), Europe (24%), and Asia (21%), with the heaviest single-country concentration in the United States. Of potential interest here is that the proportion of extreme events involving non-U.S. companies is noticeably higher than for all incidents in the IRIS 20/20 dataset. Presumably, this stems from stronger disclosure laws in the U.S. that creates a larger denominator of non-extreme events.

We've already discussed how organization size factors into loss dynamics, so we won't dig into that again here. Suffice it to say that the majority of these extreme events involved larger enterprises, but small and midsize firms suffered more losses relative to revenues.

The industries with the highest prevalence of extreme events shown in Figure 4 will be of no surprise to many. To paraphrase a famous quote from bank robber William Sutton, extreme events occur where the money (or the data) are found. The Finance and Information sectors each have an abundance of these elements. However, it's still nice to replace supposition with real information.

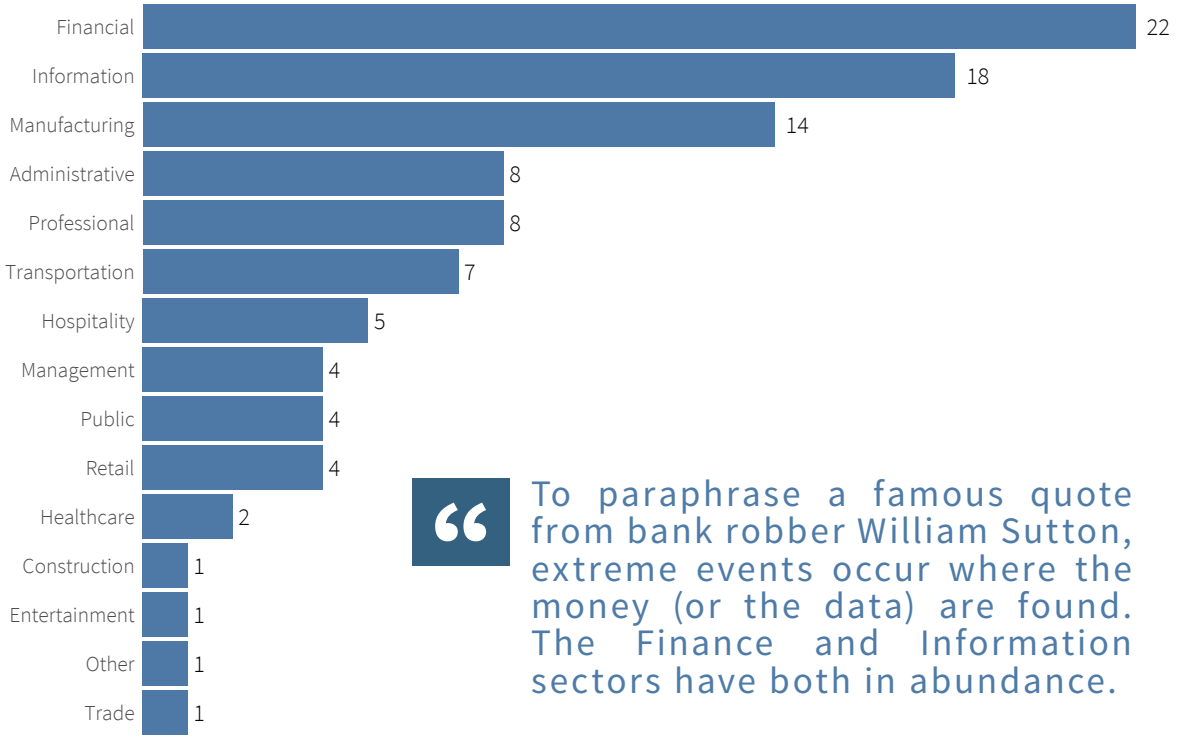


Figure 4: Industries represented among firms impacted by extreme cyber loss events.

It's important to keep in mind that this set of extreme events represents a small subset of all the incidents we covered in the IRIS 20/20. Because of that, some may wonder how the sector breakdown among major loss events compares to that of the overall population of publicly known incidents. To a limited extent, you can eyeball the differences between Figure 4 here to Figure 6 in the IRIS 20/20. But do be careful about jumping to conclusions. We can tell you that based on statistical testing, there is a difference in the mix of industries in the two groups (overall vs. extreme), but the number of events we have to work with is too small to make any definite claims for specific industries.

Things shift around a bit when looking at the total losses labeled for each industry in Figure 4. The Information sector moves up a notch to seize the crown for highest total losses, trouncing the runner up (Administrative) by a 60% margin. Interestingly, as far as total losses are concerned, the Finance sector falls all the way down to fifth place. Perhaps their long history of risk management helps in mitigating the impact, despite frequent incidents.

Are Extreme Events Growing More Common?

Aside from the losses sustained, the question of how often extreme events occur is one that we're sure leaps to many readers' minds. Establishing the date of incidents is not a trivial process, but we've done our best to nail down the key dates of when each event occurred. Figure 5 presents the number of extreme events that occurred in each quarter, over the entire sample period.

> That spike in mid-2017 is largely from a single destructive malware campaign known as NotPetya, which we'll speak more about later.

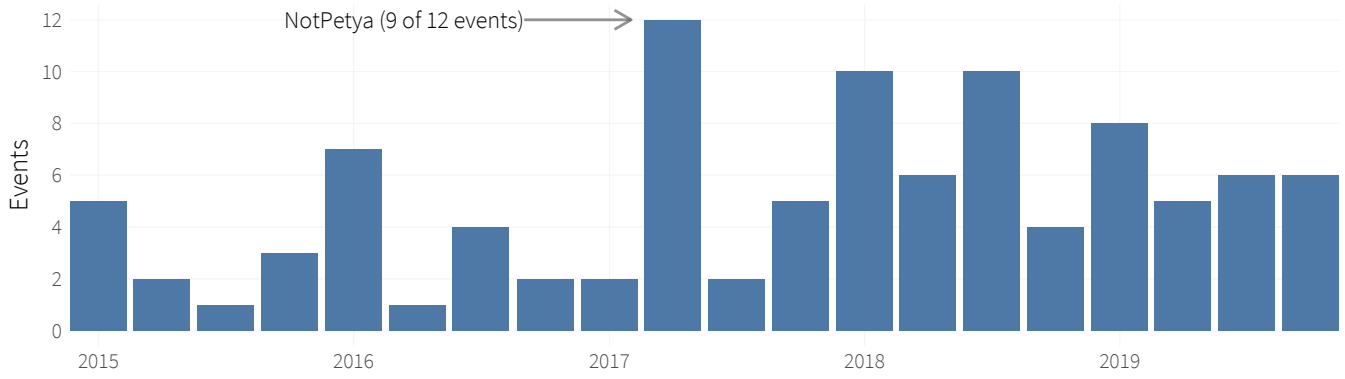


Figure 5: Number of extreme cyber loss events per quarter from 2015 through 2019

The number of extreme events each quarter, in Figure 5, follows an erratic pattern, with perhaps a slight uptick at the end. That spike in mid-2017 is noteworthy, as 75% of the events in that quarter were all from a single destructive malware campaign known as NotPetya, which we'll speak more about later. Overall, Figure 5 suggests (but doesn't offer definitive proof) that extreme events grew more common between 2015 and 2020.

> Overall, Figure 5 suggests (but doesn't offer definitive proof) that extreme events grew more common between 2015 and 2020.

Campaigns and Losses

Major Campaigns

Campaign	Percent of Losses	Total Loss
NotPetya	19.5%	$3.5B
Magecart	4.0%	$715.1M
WannaCry	1.4%	$255.0M
SWIFT Hacks	1.0%	$186.0M

Because of that spike in Figure 5 related to NotPetya, we wanted to understand the contribution of major campaigns to our population of extreme events. In Table 3 below we show all campaigns that contributed to more than 1% of the total losses across our events. NotPetya, with its well-publicized impact to numerous organizations in 2017, dominates this short list. About 20% of all losses included in this study come from this one massive campaign. Other campaigns, while noteworthy, pale in comparison.

Keep in mind that Table 3 doesn't tally ALL losses for these campaigns. This shows the total for the 103 extreme loss events analyzed in this study.

Table 3: Losses associated with major campaigns

But are Xtreme events also becoming more costly over time? Performing a quarterly roll up of losses in Figure 6 reveals that they're holding surprisingly steady. We suspected there might be climbing costs due to, for instance, larger fines imposed by The General Data Protection Regulation (GDPR), but those effects aren't yet apparent in the data we have here. We think this is an important question deserving further study as more data becomes available.

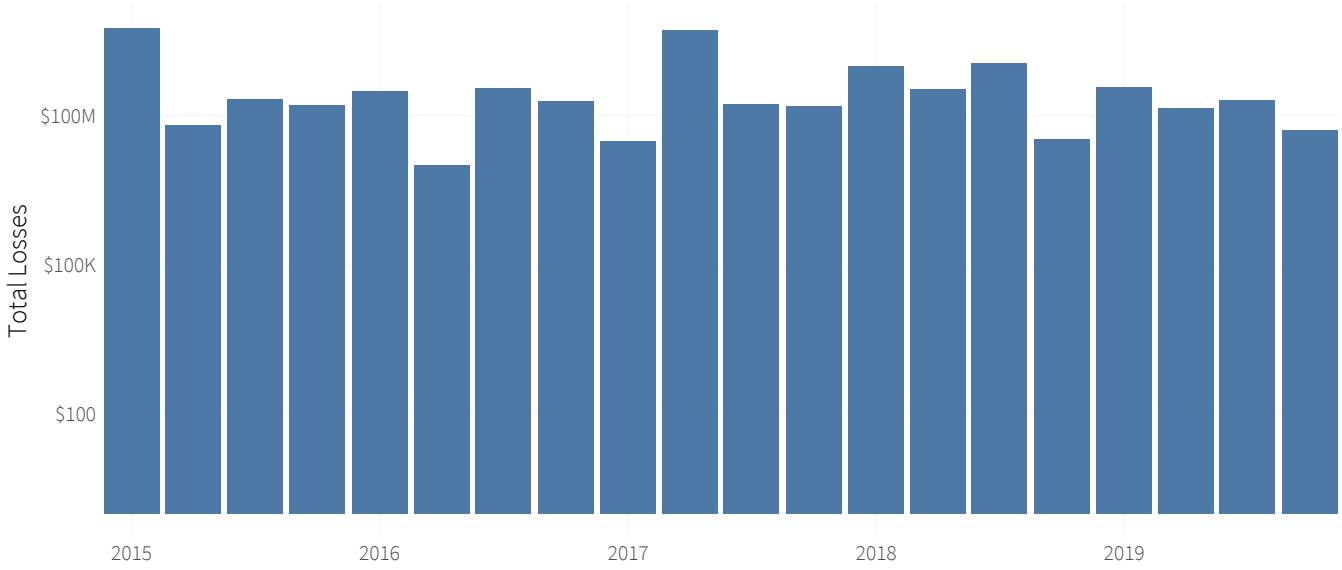


Figure 6: Total losses from extreme cyber events per quarter from 2015 through 2019

How Much is an Extreme Loss?

Comparing one extreme event to another has some of the same limitations as comparing natural disasters—while some share similar characteristics (e.g., wind or water), the type of damage caused by them differs considerably. It's the same with cyber loss events; we need to dig deeper into the forms of loss experiences to better understand how those events impact organizations.

We'll offer up this caveat, up front, that solid information on the breakdown of losses is difficult to obtain. It's not as though incidents come with an itemized invoice of all costs incurred. While statements of total costs are common, getting to the different components of the costs is very difficult with public information. Even so, we endeavored to piece together that hypothetical invoice of misery from financial reports, public records, and other available sources. We were able to obtain at least some data on the specific types of costs, for a little under half of all the incidents in our sample (49 events). For organizing this information, we adopted the forms of loss detailed in the Open FAIR™ methodology summarized below.

Competitive Advantage: Recorded costs from lost business due to an event.
Fines and Judgements: Regulatory fines and judgements against a firm.
Productivity or Revenue Loss: Measured losses in employee productivity and deals lost.
Response Costs: Expenses related to directly responding to a cyber event.
Replacement Loss: Costs involved with replacing damaged or lost assets.
Reputation Damage: Expenses related to damage to a firm's reputation.

With these variations on loss defined, we can now look at the frequency of occurrence of these forms of loss, across events, in our Xtreme dataset. Figure 7 presents the number of events we were able to identify as having individual loss components in each category.

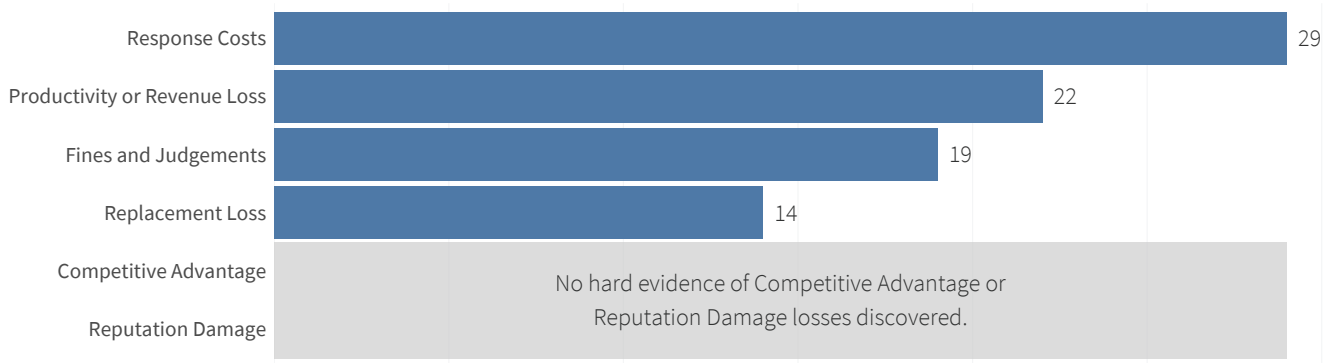


Figure 7: Forms of loss attributed to extreme cyber events

Unsurprisingly, for events where losses can be at least partially itemized, it's the response costs that we find most often. It also makes sense that productivity and/or revenue losses are next on the list because both the first two categories result directly from the incident itself. Fines and judgments, representing the perennial boardroom bogeyman of regulatory compliance, lands in third place. Replacement costs fall at the bottom of Figure 7 and are most commonly associated with making victims of cryptocurrency thefts whole.

> "Our overall takeaway is that losses caused directly from the event itself are more common—or at least more discoverable—than those incurred by the reaction of outside parties.

Comparing the bulleted loss categories and Figure 7 exposes two glaring omissions. We found zero attributable losses in either the reputational damage or competitive advantage categories. That's not to say we're certain none of the organizations in this study experienced these forms of indirect impact, but rather that they were never cited[4] or observable in any quantifiable[5] way in these well-publicized events. It is possible that some reputation damages are reflected in softer elements of organizational impact, which we'll get to in a moment.

Our overall takeaway is that losses caused directly from the event itself are more common—or at least more discoverable—than those incurred by the reaction of outside parties. Based on that, it would seem having insurance contracts in place and incident response staff or service retainers lined up, look to be well justified investments.

But what about stock price?

The effects breaches have upon stock price is an evergreen topic. Exploring this question properly would take a dedicated paper and, in fact, there are several existing academic reviews[6] of just this problem. Rather than retread well-covered ground, we'll summarize that the effects between breach announcements and stock prices are tenuous at best.

Commonality is one thing, but which forms of impact tend to be relatively larger or smaller? Figure 8 presents what we observed about the magnitude of loss per event for each category. There we see that productivity losses show the largest typical (median) value, while fines and judgements post the largest max value.

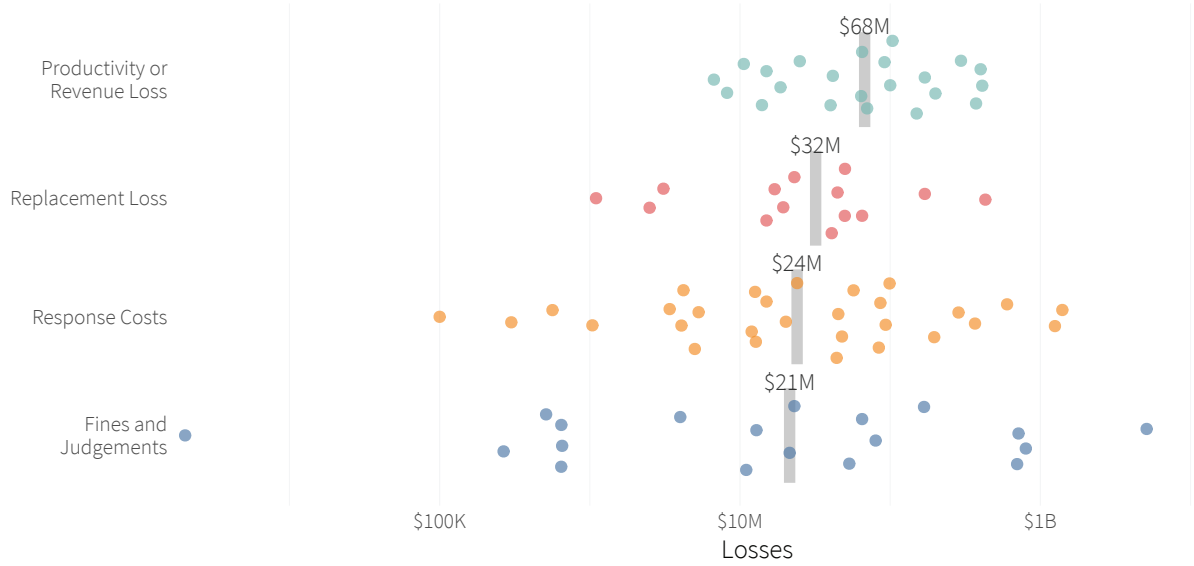


Figure 8: Costs attributed to each form of loss from extreme cyber events

While on the topic of fines and judgements, we were curious to see if the potential for substantial fines levied under the GDPR[7] could result in a discernible shift for recent events—we saw no such evidence. A chart totaling fines and judgements per quarter is boringly steady over time. So much so, in fact, that we decided not to show it. But this is definitely something to monitor in the coming years.

---

[4]Strictly speaking, there was one case where competitive advantage was mentioned. In that case (Taiwan Semi), the firm explicitly said there were no recorded competitive advantage costs.
[5]Several breaches of cryptocurrency exchanges mentioned a possible loss of market share, but we found little to no information on how temporary or permanent that was.
[6]As an example, reference Sebastien Gay, Strategic news bundling and privacy breach disclosures, Journal of Cybersecurity, Volume 3, Issue 2, June 2017, Pages 91–108, https://doi.org/10.1093/cybsec/tyx009
[7]Your authors have painful memories of some risk assessments that focused on the 4% of global revenue maximum of GDPR fines with laser precision.

Does Poor Response Raise Costs?

A close look at response costs in Figure 8 reveals that this is the only loss form that spans all orders of magnitude, from $100K to $1B+. We couldn't help but wonder whether that variation might have something to do with how the response processes are handled. So, we kept an eye out for signs that the organization responded poorly, such as being slow to respond, bungling the investigation, covering up information, repeatedly changing their story, etc. We determined that to be the case for 26 incidents, of which we have 21 events with good loss data.

Figure 9 compares losses for events, where we observed that the firm in question responded poorly vs. those where we did not detect such signs. The median total incident costs for those events with clear issues in response is over two and a half times that of incidents where there was no sign of a poor response. We confirmed that these two groups are statistically different from each other. The takeaway? If you are unfortunate enough to experience one of these extreme events, making obvious errors in your response process is an "own goal."

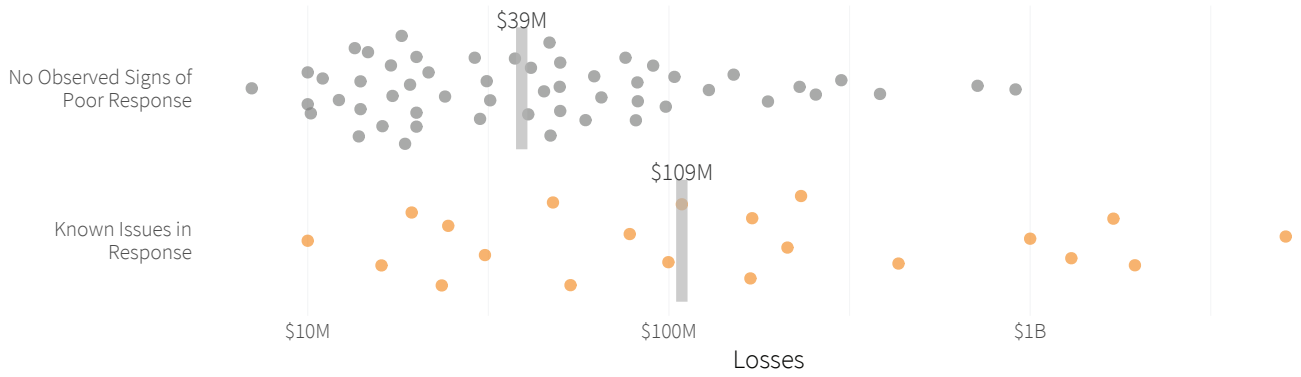


Figure 9: Comparison of total losses for events involving a poor response

Can cyber events impact a company's credit rating?

Yes, in fact, it's already happened. Equifax has the dubious distinction of being the first company in history to have it's outlook downgraded by Moody's due to a cyber event. **Moody's lowered Equifax's rating from 'stable' to 'negative' in 2019**, stating that the massive 2017 breach of consumer data will have a lasting effect on the company's financial stability due to response costs, class action lawsuits, potential regulatory fines, increased security investments, etc. In April, **Equifax was further downgraded** due to weak cash flows related to elevated information technology spending and economic headwinds, much of which stemmed from its well-covered cyber data breach.

Up to the present year, there have been several credit rating actions directly tied to a cyber event. For example, DTI, a global provider of legal solution services, was **downgraded by Moody's** for similar reasons, where a cyber event weakened liquidity reserves, damaged reputations, and ultimately stressed revenues.

While Equifax might have been the first to receive such a downgrade, it won't be the last. In order for cyber events to impact credit, the event needs to result in some form of material weakness to a company's business or financial profile. A single event can have swift and severe long-term impacts on a company. While these impacts can affect **supply chains**, logistics, and production capacity, the vast majority of cyber events can be absorbed by companies, with only short duration implications, and no lasting effects on credit. Moody's views on extreme cyber events as important indicators of issuers' financial outlook, including information about how it directly incorporates cyber risk into its credit analysis, **can be found here**.

What About Costs Beyond Dollars?

Anyone who's experienced or studied cyber events knows that there are impacts beyond the quantifiable values of dollars and record counts. While hard to measure, consequences like executive churn, organizational bankruptcy, and SEC scrutiny can make board members sit up and pay attention more than any single dollar value can. An in-depth analysis of such costs goes beyond the scope of this study, but we can't ignore them altogether either. As a middle ground, we selected several "indicators of impact" that were reasonably discernable from public sources.[8] These are presented along with their frequency of occurrence, in Figure 10.

Mentions of cyber events in an organization's SEC 10-Q or 10-K reports were the most common impacts we observed. We have a sub-section expounding on what we found in these reports, so we'll leave it at that for now.

We saw evidence of executive churn following 25 events. In some cases, it was explicitly stated that this related to the incident. In others, a causal link wasn't certain; we simply observed executive changeover within a timeframe corresponding to the incident in question.

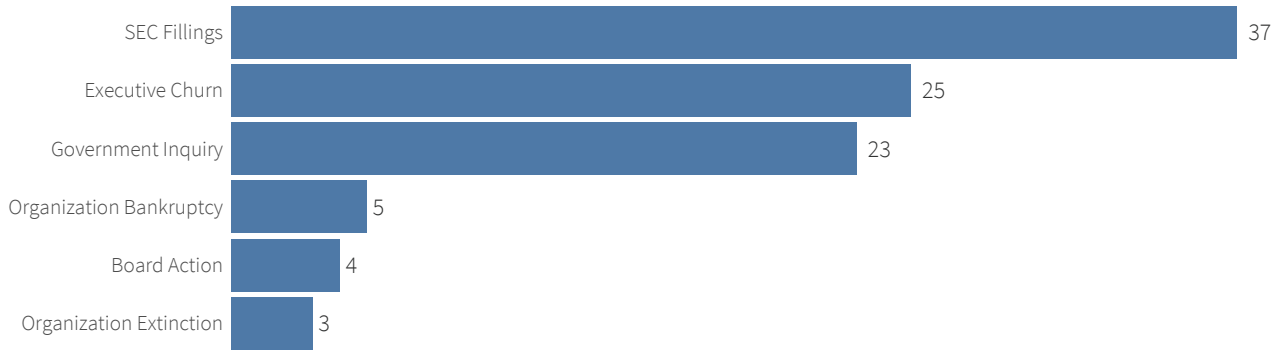


Figure 10: Non-financial impacts attributed to extreme cyber events

Government inquiries, hearings, and investigations were launched in response to 21 events. These undoubtedly led to expenditures of time and resources, but that's almost certainly not the costliest aspect of falling under the government spotlight. Far more dreaded is the negative PR and reputational harm from infamous post-breach hearings that we've all been privy to.

> "Consequences like those in Figure 10 can make board members sit up and pay attention more than any single dollar value can.

The last three on the list all fall under 5% of incidents, but they're also the worst of the bunch. The risk of going out of business often serves as the ultimate "what if?" trump card for security investments, and from that perspective, it's perhaps surprising that so few of the largest cyber loss events resulted in that end. That said, this proves it's a real concern.

The board action impact comes to bear when we found evidence of board-level management taking direct action in response to an event. These actions range from establishing standing board risk committees, to the addition of personnel focused on cyber risk, or even the departure of directors. While we expect any event significant enough to show up in this dataset to be covered at the board level of our victim organizations, these special actions reveal an extra level of pain at the top of the firm's governance structures.

[8] *We based these on a paper presented at the Workshop on the Economics of Information Security (WEIS) titled How Bad Is It? – A Branching Activity Model to Estimate the Impact of Information Security Breaches.*

Extreme Events as Seen Through SEC Reports

You may recall that the SEC requires public companies to report material cyber events in their financial filings, to provide investors with a clear view of the impact of these events on the organization. Just under half of all firms in our data set are U.S. publicly traded firms, giving us a terrific opportunity to view extreme cyber events through the lens of SEC filings.

All except four of the companies included coverage of the cyber event in their financial reports filed with the SEC. However, we weren't able to find verifiable financial losses for those four exceptions; so it's reasonable to conclude the impact wasn't material enough to trigger mandatory reporting.

Figure 11: Amount of coverage given to cyber loss events in SEC filings

For those companies that mentioned the cyber event in their 10-Q or 10-K reports, there's quite a diversity in the amount of coverage of the related losses. We kept things simple by recording whether the event received a few cursory sentences, a dedicated section, or extensive coverage in multiple sections of the report. According to the tally in Figure 11, allotting a dedicated section to discuss the cyber event was the most common approach. Aside from covering the basic financial numbers, much of that space was devoted to assuring investors that the event was being handled and the company would be all right.

While reviewing SEC filings, we were inspired by some independent research[9] on the coverage of breaches in the quarterly earnings transcripts. These analyses established a record of 13 consecutive quarters shared by both the TJ Maxx and Heartland Payment Systems breaches. Our research makes it a three-way tie by adding Ubiquiti Networks' 2015 BEC incident to that list. Though, technically, coverage of Experian's breach in four annual reports from 2016 through 2019 may take the crown for overall length of time.

We anticipated that financial reports would often make mention of other events or losses that dwarf the cyber incidents in question, but we did not find many instances of that occurring. One of those was a contamination issue in semiconductor wafers, and another was bracing investors for emerging losses associated with the COVID-19 pandemic. Does that mean cyber losses are usually more impactful than other types of loss events? Is the threshold for reporting lower? Something else? Share your thoughts on Twitter (@cyentiainst) or LinkedIn.

Reports of our debt may be greatly exaggerated

During our scouring of SEC filings, we observed significant differences between what public sources (largely media) reported as losses and what the organization filed in their 10-Q or 10-K. We were able to find estimates for total losses from both SEC filings and public sources for 20 incidents. **In 13 of those, the SEC-reported losses were smaller, except in two cases.** We also noted that some very large losses were not mentioned in SEC reports.

[9] *Hat tip to Ryan McGeehan, who shared some historical findings on breach mentions in SEC filings via Twitter on 5/15/2020. Link: https://twitter.com/magoo/status/1261406326275452931?s=21*

I'll Take 'Words for Cyber Events' for $400, Alex

If you've ever wondered how companies refer to cybersecurity incidents in their public financial reports, Figure 12 should satisfy that curiosity. Word clouds are the dataviz equivalent of playing Stairway to Heaven in a guitar store, but we're going to do it anyway. It appears that forms of "cyber attack," "incident," and "breach" are currently in vogue. But our favorite is the deliciously dodgy "developer that shared data with third parties." Can you guess who was trying to save Face with that one?

Figure 12: Terms used to refer to cyber events in SEC filings

> "Do cyber events that warrant inclusion in financial reports have higher losses than those not reported? Figure 13 makes that comparison.

All this talk of cyber events in SEC filings begs the question of whether any of it matters. Do cyber events that warrant inclusion in financial reports have higher losses than those not reported? Figure 13 makes that comparison, and analysis confirms that the differences in medians depicted there are statistically significant. Not only are they meaningfully different, but the median losses for firms that choose (or are compelled) to mention the events in their SEC filings are three times of that of other public firms with extreme events. That shouldn't be taken to mean reporting incidents increases losses, but rather confirmation that losses triggering the materiality clause tend to be larger than those that don't.

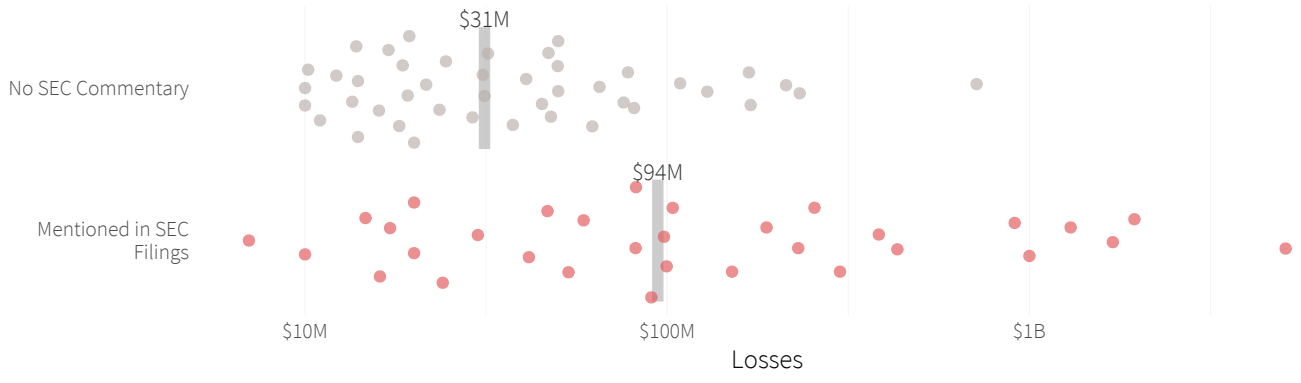


Figure 13: Comparison of losses for cyber events reported in SEC filings vs. not reported

Which Events are the Most Extreme Risk?

When discussing major cyber loss events, questions invariably arise, such as the one posed in the title of this section. What exactly are these incidents? Who's behind them? How do they occur? And perhaps most importantly, what can we learn to help avoid similar events in the future?

To answer such questions, we need to ratchet our analysis down to a tad more tactical level. Since we're still dependent on public data, we cannot get into the nitty-gritty details of forensic evidence. But we can help shed some light on common cyber event types and patterns, so we're better informed to avoid similar events impacting our own organizations.

> It's common at the executive and board levels to slot cyber events in high-level categories that look something like those in Table 4.

It's common at the executive and board levels to slot cyber events in high-level categories that look something like those in Table 4. These categories focus more on how the organization is affected than the incident occurred. Business interruptions are the most numerous and have fairly high median losses. Over half of all total losses are attributable to this category.

Event Top Level Category

	Events	Median Loss	Total Loss
Business Interruption	43	$82.0M	$9.6B
Data Disclosure	30	$90.7M	$1.0B
Fraud	30	$34.7M	$7.0B

Table 4: Count and losses associated with top-level cyber event categories

Data disclosure has the highest median losses, but the lowest total loss. The latter is a function of many data breaches not publicly reporting loss amounts. Several of these events involved substantial numbers of records exposed but not necessarily compromised and no (known) financial impacts.

Fraud events have the lowest median loss. The second place, in terms of total losses, is the result of our old friend, the Cambridge Analytica event.

> Business interruptions are the most numerous and over half of all total losses are attributable to this category.

Beyond these top categories, many corporate risk registers we've seen over the years present a tad more specific set of cyber incidents. These tend to group common actors, actions, technical impacts, etc., into broad incident patterns or scenarios. We've adopted a similar approach for grouping incidents in our Xtreme dataset based on the information collected about them. These incident patterns are described below and analysis of the associated frequency and losses follow straight after.

Cryptocurrency theft: Includes all attacks on cryptocurrency exchanges or the underlying cryptocurrency systems themselves.

Exposed data store: Data stores that are inadvertently left accessible to unauthorized parties, typically through misconfigurations on the part of the data custodian.

Fraud or scam: Incidents that primarily involve deception and other social engineering tactics. Business email compromise (BEC) was the most common form in this dataset.

Hack or intrusion: All attempts to compromise applications and systems 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.

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 service outages resulting from failed systems and programs. Distributed denial of service (DDoS) attacks as externally sourced, are not included in this category.

Physical theft: Stealing or tampering with physical assets, including laptops, storage media, documents, etc.

Which Incident Patterns are Most Common?

Among all cyber loss events in our Xtreme dataset, various forms of hacking and network intrusions were by far the most common. They represented 37% of the 103 incidents we examined and double of the next most-frequent category, ransomware. According to the description above, that pattern includes both extortion-based ransomware and destructive malware like NotPetya; the split between those forms was even.

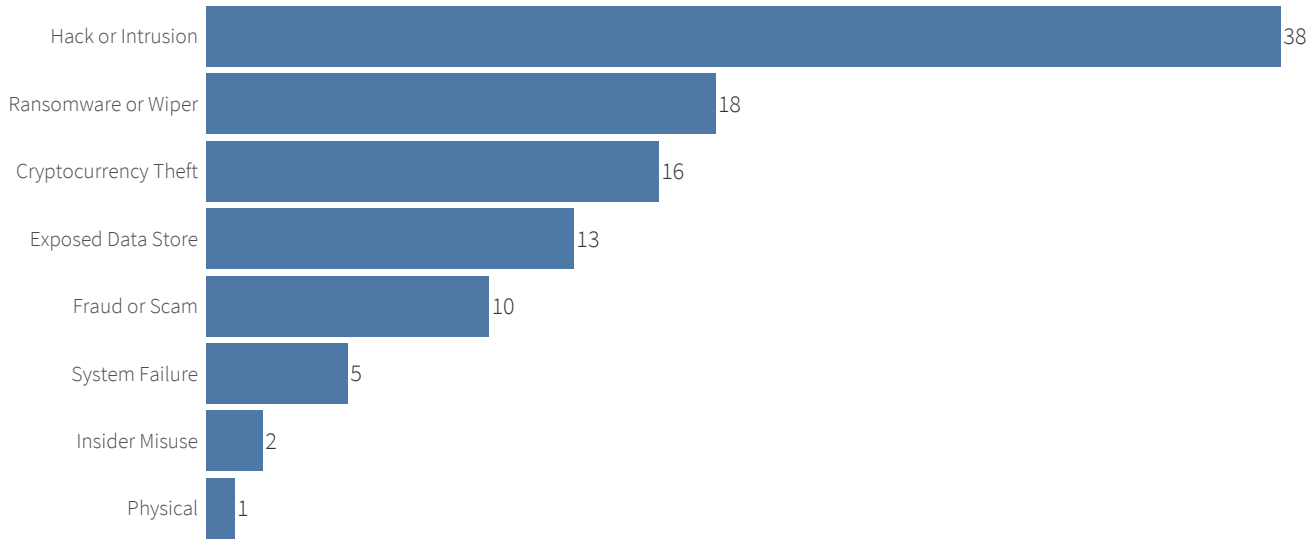


Figure 14: Count of incident patterns associated with extreme cyber events

Cryptocurrency theft is a niche threat that likely isn't on the cyber risk register of many readers. But their presence among these major loss events was too large to ignore. The next one on the list, exposed data store, is far more applicable to most organizations. The fact that it ranks #4 among the most common types of costliest incidents provides a strong reason to find and lock down datasets in cloud environments and other external-facing systems.

We won't spend much time on the bottom half of the list, but the stats are there for those interested. However, we do feel compelled to highlight the fact that insider misuse falls dead last on the list of incidents patterns resulting in major losses. Some of us behind this study have been looking for evidence to back the "insiders are the greatest threat" mantra for 15 years now. We're still looking.

Which Incident Patterns are the Costliest?

Let's now move from the commonality to the costliness of these event types. We can measure that in two ways—event based or en masse. We hate to pick favorites, so Table 5 shows both the total and typical (median) losses for each incident type.[10]

Key Loss Measures by Type of Event

	Events	Median	Total Loss
Cryptocurrency Theft	16	$36M	$2B
Fraud or Scam	10	$46M	$5B
Hack or Intrusion	38	$31M	$6B
Insider Misuse	2	$82M	$82M
Physical	1	$17M	$17M
Ransomware or Wiper	18	$101M	$4B
System Failure	5	$117M	$485M

Table 5: Count and Losses for incident patterns associated with extreme cyber events

We'll start with total losses, which, to be honest, isn't really a fair comparison. Events that occur more frequently stand a better chance of racking up higher losses, and that's more or less what we see happening in Table 5. Hacks account for one-third of the total losses represented by this study and adding in ransomware moves that share to over half. Heck, we're feeling generous, so let's go ahead and toss in fraud and scams to bump us over the 80% threshold. With so many cyber threats out there to worry about, it's part alarming and part refreshing that we can account for 80% of the most extreme losses with just three event types.

If Table 5 works for you, feel free to stick with it for the per-event view of loss magnitude. But we invite those who would like a little lagniappe to turn their attention to Figure 15. Like other charts of this format, dots represent individual loss events and we've segmented those by incident type. The vertical bars mark the median loss value for each category from Table 5.

This view offers several advantages, one of which is a reminder that some of these incident types include a very small number of events. Consider that before quoting, "ya know, every insider breach costs $82M" at the next cyber risk team meeting. Another major perk of viewing individual loss events in Figure 15 is that it gives a sense of range and outliers. Hacks are all over the place, whereas—barring one major outlier[11] —fraud losses exhibit a fairly tight range. Physical failures stay relatively low, but system failures and ransomware deserve due care.

> "Hacks account for one-third of the total losses represented by this study and adding in ransomware moves that share to over half.

[10] *The category of exposed data store is not listed because no events had confirmed loss information.*
[11] *We know you're wondering, so the outlier is the 2018 Facebook/Cambridge Analytica scandal.*

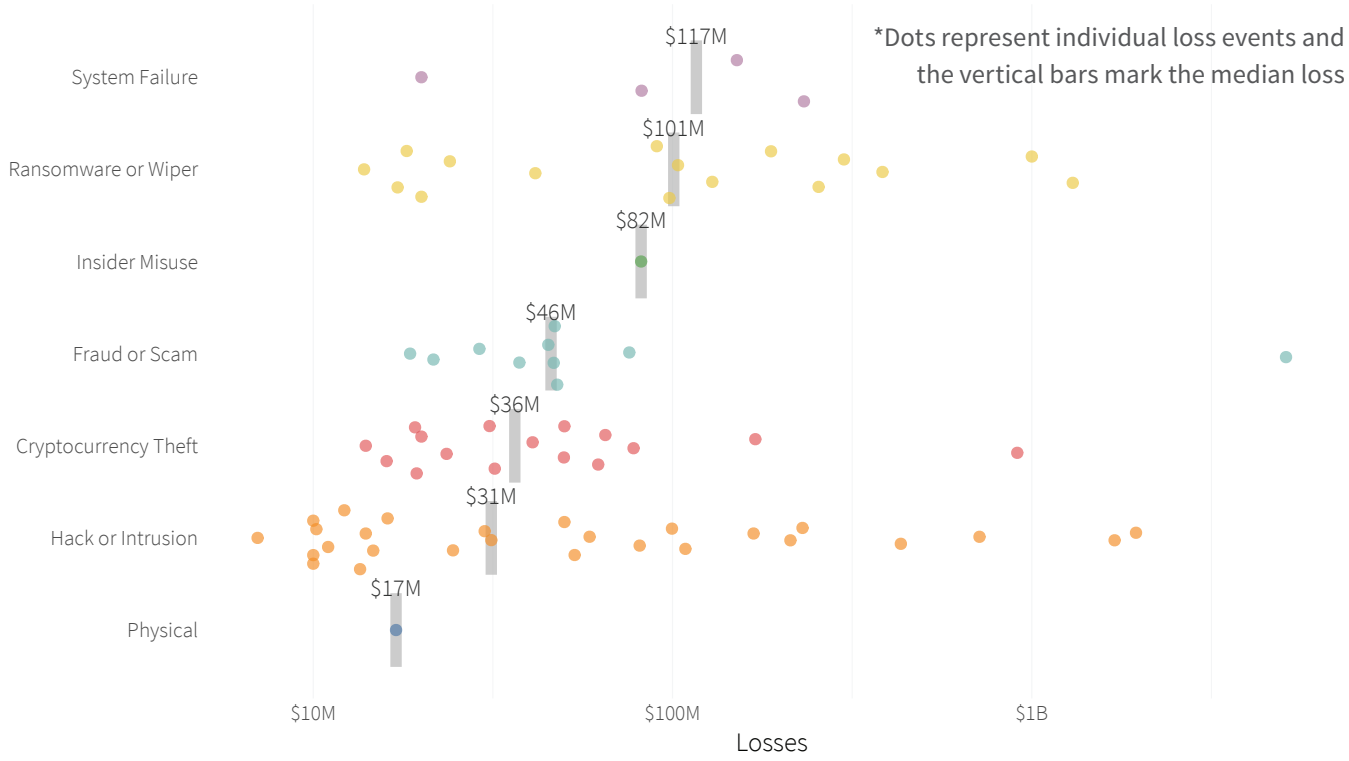


Figure 15: Loss distribution for incident patterns associated with extreme cyber events

A little more on how we collected this data

As described earlier in this study, we set a threshold of $20M in losses or 20 million data records affected to identify loss events in the Advisen dataset for inclusion in this study. That was based on the (admittedly fuzzy) guidance from the SEC around the materiality of events, but it also conveniently fit the IRIS 20/20 branding of this report. We also reviewed public listings of incidents outside Advisen's cyber loss data to ensure there were no significant gaps in our extreme event candidates.

In addition to the list of events, we created an expanded set of target data points to collect on each event. These data points pertained to the threat actors involved, primary actions and vectors utilized, assets and data impacted, key dates in the incident response timeline, a more detailed breakdown of costs associated with the event, etc. We based many of these data points on the Vocabulary for Event Recording and Incident Sharing (VERIS) and Factor Analysis of Information Risk (FAIR) frameworks. We also selected several 'Indicators of Impact'[12] to supplement our loss data.

To collect the data values, we reviewed multiple public sources on every event to obtain the most reliable information, cross-referencing across sources as much as possible for validation. Where sources contradicted (particularly common with cost estimates), we either went with the most recent information and/or the most credible source. Sometimes that was a judgement call. Every event was analyzed and validated separately by at least two Cyentia Institute team members to maximize the completeness and accuracy of the Xtreme dataset.

The Cyentia Institute and Advisen have partnered to make this rich dataset of extreme cyber loss events available as a subscription. If interested in learning more, reach out to extremeevents@advisen.com.

[12]*Thomas, R., et al. (2013). How Bad Is It? – A Branching Activity Model to Estimate the Impact of Information Security Breaches. Presented at the 12th Workshop on the Economics of Information Security. Link: https://www.econinfosec.org/archive/weis2013/papers/ThomasWEIS2013.pdf*

Which Incident Patterns are the Riskiest?

Let's bring it all together now to answer the burning question—which of these incident patterns represent the greatest relative risk? Since event frequency and loss magnitude are the primary components of assessing risk, you could probably infer this on your own from the previous figures, but we don't want to make you work that hard. Figure 16 holds the answer you seek.

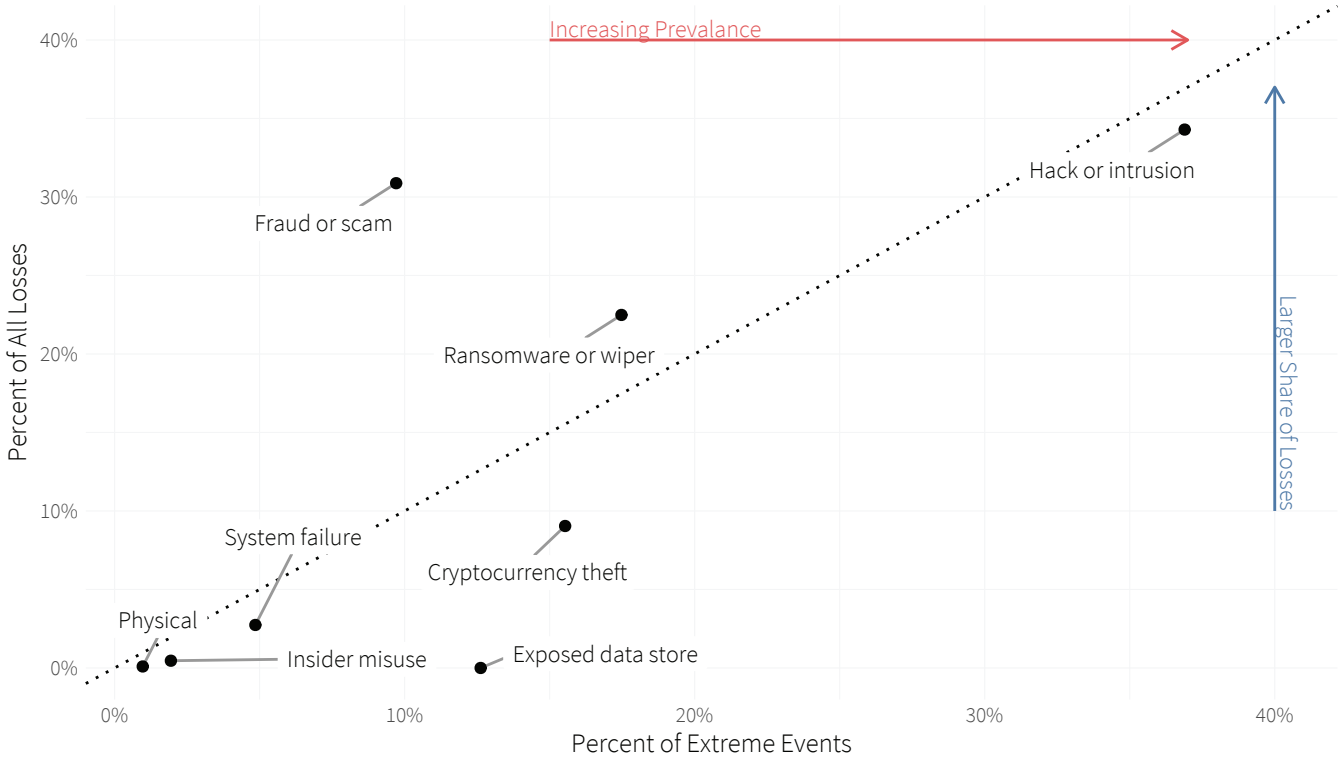


Figure 16: Percentage of extreme cyber events and losses by incident pattern

Figure 16 is pretty much your standard issue risk matrix, with the percentage of events represented along the horizontal axis and proportion of total losses for each event type on the vertical axis. We're going to stop short of attempting to quantify, categorize, or color risk levels and simply assess the positioning of these incident patterns. Figure 17 offers a similar view of frequency but tallies total losses rather than median for each pattern.

Based on this depiction, hack or intrusion takes the crown for the riskiest extreme cyber loss event type. They're by far the most frequent, and while on the lower end of the spectrum for median loss (see Figure 15), about a third of all losses can be attributed to this one pattern.

Ransomware or wiper is another big-ticket item in Figure 16, and that's probably not unexpected. They've caused a lot of pain and sleepless nights over the last several years. The last pattern we'll call out individually is fraud or scam—it's below 10% of all events but over 30% of all losses. The thing to remember here is that nearly all of those losses are associated with one event (the Facebook-Cambridge Analytica scandal). Don't let the fact that we're not devoting more airtime to the others cause you to ignore them. After all, they made the cut to be included in this report, regardless of where they land in Figure 16.

> Based on this depiction, hack or intrusion takes the crown for the riskiest extreme event type. They're by far the most frequent and about a third of all losses can be attributed to this one pattern.

Who's Behind these Events?

Based on the incident patterns from the previous section, you can probably surmise that a large majority of these events originate from sources outside the victim organization. For those who like specific numbers, 82% of extreme events and two-thirds of losses involved external threat actors.

Due to this predominance of external actors, we wanted to further distinguish the perpetrators behind these events. The most common by far are organized criminal (52 events) and state-affiliated (20) groups. Most of those remaining were attributed to force majeure (4) and activist groups (2). Figure 17 compares the magnitude of loss events between these key actors groups.

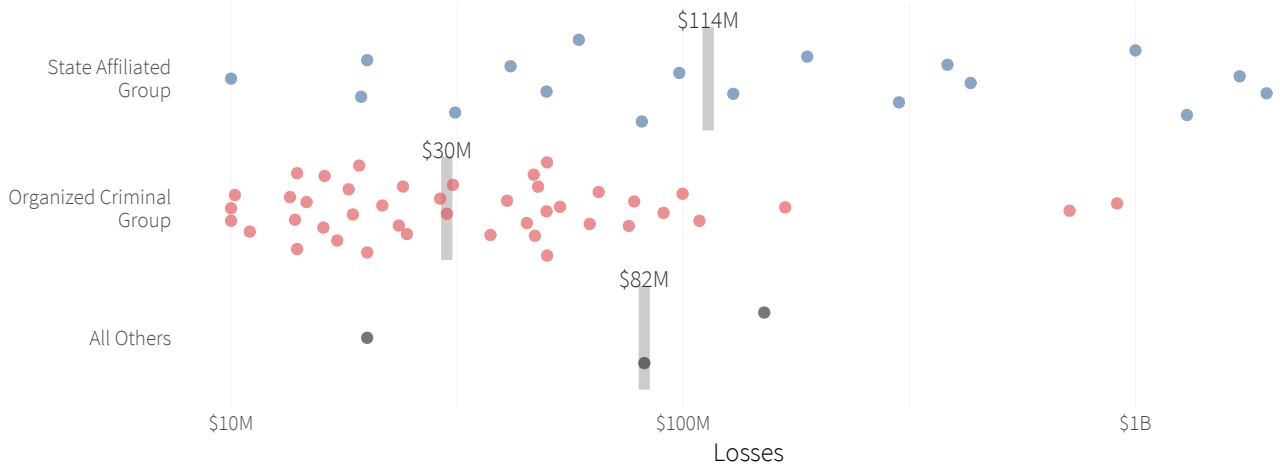


Figure 17: Total losses for extreme cyber events attributed to state-affiliated and organized criminal groups

We've come to expect cybercriminal gangs to drive a large proportion of incidents, so it's not surprising to see them active among these extreme events as well. The real story here is that one in five of the largest losses, over the last five years, can be attributed to state-affiliated actors. What's more, these state actors have caused $7.8B in damages—43% of all known losses in this study!

When your humble authors first saw these numbers, we were a little taken aback. In our experience, nation-state attacks or advanced persistent threats (APTs) are often seen as "Acts of God" that most enterprises are not equipped to defend against. That so many of these extreme events are attributed to APTs forces us to recognize that as a dangerous cop out. They might not be common in the grand scheme of cybersecurity incidents, but nation-state actors account for a large portion of tail risk. Resilient enterprises must plan for and defend against this reality.

> "The real story here is that one in five of the largest losses, over the last five years, can be attributed to state-affiliated actors. What's more, these state actors have caused $7.8B in damages—43% of all known losses in this study!

A Quick Take on Regional Actors

In Figure 18 we explore where these actors are geographically located. Some of our events have actors in multiple geographic regions, so there is some duplication in the total amounts. We can still use this to determine the hotspots of extreme actor activity. By total loss volume alone, Europe (both East and West) and East Asia dominate the landscape. If the inclusion of West Europe surprises you, keep in mind that 98% of that $5.2B in losses is attributed to a single event, the Cambridge Analytica incident.

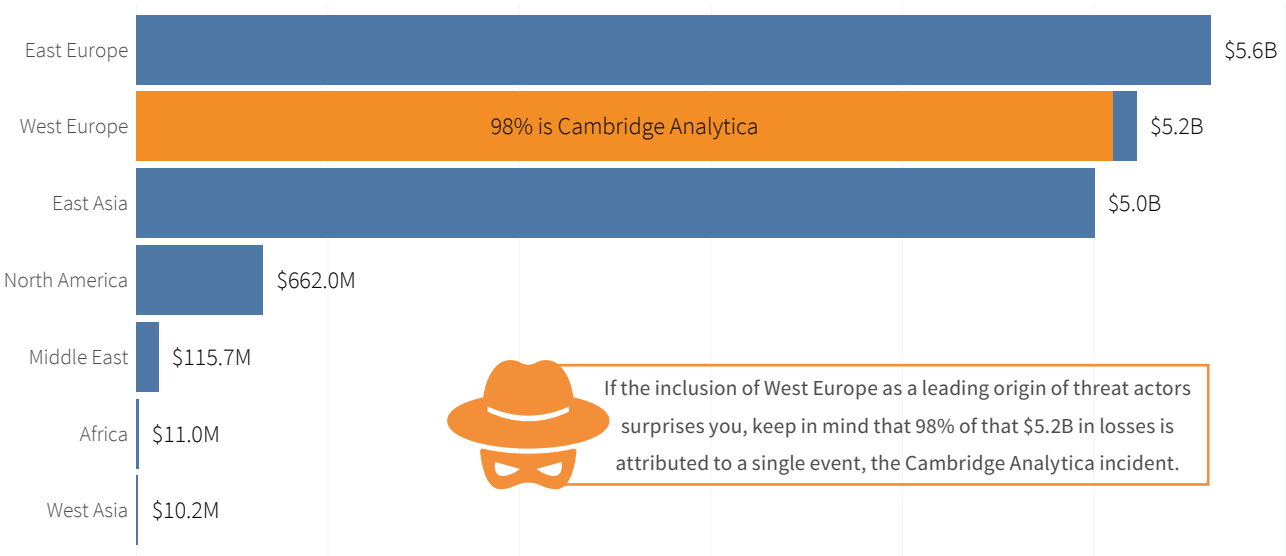


Figure 18: Losses attributed to regional threat actors

What Actions Lead to these Events?

Having lined up the suspects indicted for extreme loss events, we'll now investigate the tactics employed to pull off these crimes. "Investigate" might be a little misleading, because we don't have any forensic evidence to sift through for clues; but, we did scour public sources to piece together as much as possible and were generally able to confirm a few specific VERIS-based threat actions per incident. We could wax for weeks about the results of those efforts captured in Figure 19 and Table 6, but don't worry—we'll stick to the high points, so you can get back to preventing incidents like these.

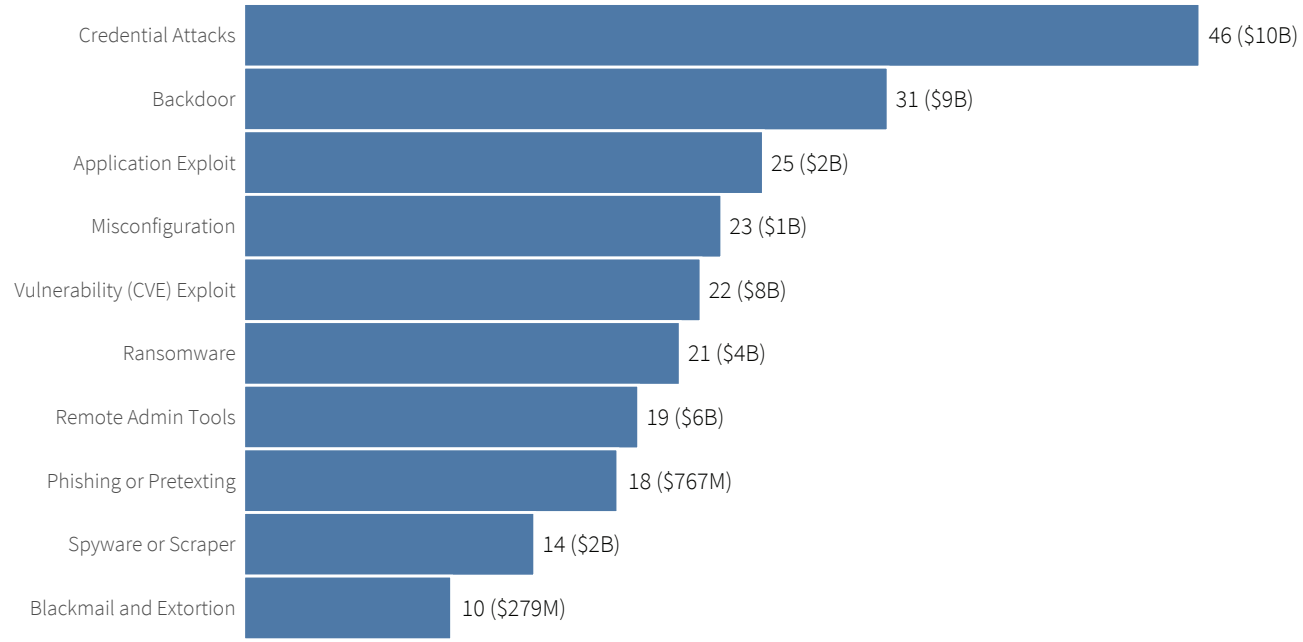


Figure 19: Count and total losses for top 10 threat actions identified in extreme cyber events

Threat Actions Identified

Category	Variety	Events	Total Loss
Error	Device Malfunction	4	$253M
Error	Misconfiguration	23	$1B
Error	Publishing Error	1	$0
Hack	Application Exploit	25	$2B
Hack	Credential Attacks	46	$10B
Hack	DDOS	2	$140M
Hack	Remote Admin Tools	19	$6B
Hack	Vulnerability (CVE) Exploit	22	$8B
Malware	Backdoor	31	$9B
Malware	Cryptominer	2	$295M
Malware	Ransomware	21	$4B
Malware	Spyware or Scraper	14	$2B
Misuse	Knowledge Abuse	3	$356M
Misuse	Policy Violation	6	$5B
Misuse	Privilege Abuse	5	$5B
Physical	Equipment Tampering	1	$14M
Physical	Theft	1	$17M
Social	Blackmail and Extortion	10	$279M
Social	Phishing or Pretexting	18	$767M

The highest of these high points is undoubtedly credentials. Cracked or stolen passwords and other credential-related attacks led to more incidents (46) and total losses ($10B) than any other threat action. If you work for an organization that's not yet using multi-factor authentication, please share this chart with your colleagues and bosses. You can blame it on us.

If criminals can't get in through the front door by stealing your password, chances are they'll sneak in (or return) via a backdoor. Remote access malware planted by actors contributed to the second-highest totals for events frequency (31) and losses ($9.2B).

Our third and final high point from Table 6 is vulnerabilities. About a quarter of incidents (25) involved web application attacks, such as SQL injection or cross-site scripting, making that the third most common type of action. Exploits against known vulnerabilities (CVEs) in (mostly common) software round out the top three for total losses at $8.5B. It sounds like hyperbole to claim that prompter patching might have avoided half of all costs across all events in this study, but facts are facts.

If you thought these extreme cyber events would require some cutting-edge cyber solution nobody's ever heard of, we're sorry to disappoint. Even the big ones still point back to the basics, but, like G.I. Joe taught us, knowing is half the battle. Now get out there and win the other half!

> Credential attacks led to more incidents (46) and more losses ($10B) than any other threat action!

Table 6: Count and total losses for all threat actions identified in extreme cyber events

Discussing Extreme Events With the Board of Directors

This report makes clear what we all suspected to be true: extreme cyber events are real and can have severe impacts on organizations. Considering this, Board-level conversations about extreme cyber events are required to make Directors aware of them. But how? For starters, these discussions should include general reporting on security processes and controls used to manage run-of-the-mill cyber events so that directors can appreciate what their security team is facing every day. That said, it is important not to conflate daily security event management with extreme cyber events. Directors need to understand the potential impact of, and mitigation strategies for, extreme cyber events.

Boards need to know exactly what was reported here in the IRIS Xtreme report. They need to know what a significant, adverse cyber event would look like for their organization. Only then can they truly understand what is required to protect their organization in a holistic way.

The potential impact of these events should be a part of any Board level discussion about cyber risk. The data presented in this report is an important tool that risk and security professionals can use to engage their management and Board in improved dialogue. At VisibleRisk, we believe that combining this type of research with case studies and tabletop exercises strengthens a Board's ability to understand and evaluate these risks and their potential impact.

So how can you leverage what's in this report to improve your Board's understanding of extreme events?

Help the Board understand if their cyber insurance is adequate. Directors are interested in whether there is adequate insurance coverage for an extreme cyber event. Presenting information from this report about extreme losses and comparing them to levels of protection in relevant insurance policies will help Directors make better decisions about the adequacy of such protections and what else can be done to further insulate the balance sheet.

Evaluate whether a "rainy day fund" is sufficient (or needs established). Whether it's called capital reserve, capital allocation, or capital surplus, a "rainy day fund" is effectively an organization's earmarked savings account to cover adverse events. Financial services organizations are required to compute and set aside these funds, but it's good management for all organizations to consider putting money aside to cover unanticipated, major losses. That said, allocating too much money to such an account can be as harmful as allocating too little. Cash in reserve generates no return for the business. The findings of this report can help organizations optimize their capital allocations to account for extreme events without overcommitting potential investment capital.

Justify and expand security spending. Many CISOs take their concerns to the Board in the hopes of securing additional budget for technology, staff, and consulting services. Significant diligence is required to link these investments to the relevant risks. The results of this report can be used for scenario planning purposes, to connect the circumstances of these extreme losses to relevant scenarios affecting your organization. In turn this allows evaluation of the changes in frequency and value of extreme losses before and after proposed cybersecurity investments. This also helps Board members better understand whether a particular investment would actually mitigate these extreme impacts, either by making them less likely or by reducing the losses to a more reasonable value.

Independent research such as IRIS Xtreme is incredibly valuable for the information security industry as it seeks to demystify extreme cyber events. Running financial analyses that consider the extreme losses articulated herein lets Boards better understand the potential outcome of such an event.

Many organizations are concerned about the theoretical impacts of extreme cyber events. Although this concern is warranted, access to data about such extreme events is invaluable in terms of managing these conversations and refocusing efforts around improving security and resilience.

- Jack Freund, PhD, Head of Methodology at VisibleRisk