2026 Breach Impact Study

A publication from the authors of the Data Breach Investigations Report

CyberAcuView

verizon business

Table of contents

Introduction

Hello, and welcome to the 2026 Breach Impact Study (BIS), brought to you by the same authoring team as the Data Breach Investigations Report (DBIR). This study comes from the desire to answer our loyal readers' third most frequently asked question:[1] "Why doesn't the DBIR provide more in-depth analysis on the financial impact of data breaches?"

Given the anonymity of the data we collect for the DBIR, it has always proven challenging to find the critical mass of data necessary to do the topic justice. The data collected for the DBIR is, after all, a sample of convenience, and it seems the right conditions never presented themselves. Until now. For this report, we are happy to announce that we have partnered with CyberAcuView,[2] an organization founded by major participants in the global cyber insurance market that is dedicated to cyber insurance data collection, analysis and intelligence. This study is the result of both teams' diligent collaboration.

In this inaugural research, we have reviewed approximately 70,000 cyber insurance claims in the United States, of which roughly 38,000 have recorded losses paid out to the policyholders. Those claims cover insurable cyber incidents from Jan 1, 2019, through Oct 31, 2025. And they provide us with a good cross-section view into well-documented cyber events. We also offer insight into trends such as the rise of ransomware and Business Email Compromise (BEC) as the most common financially motivated incidents in the historical DBIR dataset over the same time period.

Through this study, we aim to provide an objective and data-driven measure of organizational financial impacts, while maintaining the academic lens and statistical rigor our readers expect[3] from the DBIR. The DBIR is frequently referred to in the industry as one of the best sources of information with which to understand the likelihood of different types of cyberattacks and the trends in the threat landscape. Serving as a bridge between the cybersecurity and cyber insurance industries, the BIS guides both sectors toward better ways to report and understand the impact of cyberattacks.

Anyone who has taken Cybersecurity 101 knows the formula: Risk = Likelihood × Impact. With that finally solved, I suppose we can all pack up and go home, right? Unfortunately, it is not quite that simple, but we believe this report can help us find some of the missing impact pieces of this puzzle.

The structure of this report is similar to the DBIR, with an initial "Results and analysis" section looking at the complete dataset and breakdowns of different loss types. This is followed by a more focused look into some favorite threat actor incident types and a breakdown by industry.

However, the data itself and some of the insurance vocabulary is very different from what our regular readers are accustomed to, so do spend some time in the "How to use this report" section following the introduction.

We hope you enjoy reading this study as much as we enjoyed putting it together.

Sincerely,

The Verizon DBIR team
C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup

With special thanks to our CyberAcuView partners:

- Mark Camillo, CEO at CyberAcuView, who championed and believed in this partnership since day one
- Wenlu Zhang, Director of Data and Analytics at CyberAcuView, who provided incredible data analysis support and an important critical eye, all while enduring our questions about the cyber insurance industry
- And the CyberAcuView members, who are contributing the data and standards that support more informed cyber underwriting

1. The other two being a tie between "Why don't those numbers add up to 100%?" and "Did you really think that footnote was funny?"
2. cyberacuview.com
3. And dare we say love?

How to use this report

First-time reader?

Of course you are! This is the first BIS we have ever put together. We want to take this section to describe the dataset, the methodology we used to analyze it and some of the cyber insurance industry terminology we will be using throughout. Buckle up!

About this publication and the cyber claims dataset

The BIS is a publication focused on the analysis of cyber insurance claims data from CyberAcuView, our sole partner and data contributor for this study. The dataset is a subset of data contributed by participating member insurers, normalized and standardized for the purposes of this analysis. It includes 69,683 cyber insurance claims, of which 38,181 have recorded losses paid out to the policyholders, for incidents that occurred from Jan 1, 2019, through Oct 31, 2025.

This study is a curated analysis of the above-mentioned subset – not the full picture. CyberAcuView is an organization that supports research on cyber claims data by pooling said data from its member companies on a "give-to-get" basis, providing aggregated insights used for strategic benchmarking, enterprise risk management (ERM) and broader analytical use cases. The subset used for this study and its results provides a good example of what insights can be achieved by applied research to cyber claims data, and we hope to continue to grow this partnership in the future.

Deriving breach impact from cyber claim loss

The BIS dataset describes the insurable loss that was either paid out to the policyholders in closed claims (where all insurance adjustments and damages were finalized in accordance with the insurance policies) or reserved as expected amounts to be paid out in open claims (where adjustments are still being made or the full damages are still not known). Because recent claims are more likely to remain open in the dataset, we lack precise information on how their impact will ultimately be distributed across the loss categories analyzed in this study. Any organization that has suffered a data breach knows that the costs can keep rolling in, sometimes for years after the event, as these cases often can wind their way through both the courts and regulatory scrutiny. For that reason, when we conduct year over year analysis, we will not be including the year 2025 since 60% of the claims from that year were still open at the time of this study and will need additional time to mature.[4]

Understanding the concept of "insurable loss" is very important to understanding this dataset. It only registers the losses that were included in the policy claims, and as such is likely a conservative lower bound of the actual economic losses of the incidents.

Actual financial consequences were possibly higher, as loss figures could have been influenced by varying deductibles, coverage scopes and payout limits. The dataset does not estimate uninsured losses, reputational damage or non-claim costs, and as such should not be interpreted as a total loss model. Think of insurable loss figures as a potential floor – not a ceiling – of the true economic impact.

In order to approximate the total impact of each incident, we calculated the "ground-up loss," adding the deductible amount of the claim to the total incurred loss, which combines all the different loss types registered. This worked very well both in closed and open cases because we could include the reserved amounts for the whole claim in the total incurred figure. It's not much more than approximations based on insurer reserve practices and actuarial estimation, but we would argue that given the fact that cyber insurers' solvency often depends on assessments like these being accurate, they should be very well-educated estimates.

However, we do leave out the "zero-dollar claims," where either nothing was paid out to the claimant or no reserve was set aside. In those cases, the only information available is that the total adjusted loss according to the insurer was less than the deductible of the policy, and it could be any amount up until that limit. Counting those would create big aggregations of distribution around the deductible values, and that would disrupt our distribution analysis significantly to very little benefit of other findings, since there is no loss type breakdown on those anyway.

That leaves the cases where the total incurred loss registered was equal to the policy limit, suggesting the total impact was larger than captured in the claim. Since there was a small percentage (about 0.7%) of claims in the dataset where that happened, we do not believe it significantly impacted the analysis by including them.

Finally, it is important to note that specific categories of loss may be subject to sublimits – internal caps that limit recovery for specific costs like contingent business interruption or extortion.

When a sublimit is reached, the dataset records the cap rather than the full loss for that category, meaning the recorded amount for that loss type may be lower than the actual economic impact.

4. Similar things have been said about the authors of this study.

Closing the case on loss types

Another detail worth mentioning is that in the cases where we broke down the known types of incurred loss (without considering the deductible) into component types, we only considered the closed claims, where the breakdown of the recorded losses has been confirmed. This will lead to a whole new wave of "Why don't these numbers add up to 100%?" questions, but there is no reasonable way to account for those Unknown loss types, and we want to make sure we use data with the correct level of detail. The sample size is large enough that this does not matter to the analysis itself.

Policyholder demographics

The policyholders in the dataset are anonymized by demographic information of their industries with two-digit codes from the North American Industry Classification System (NAICS)[5] standard, the same one used in the DBIR. The dataset also provides information on company revenue – which our analysis uses as a proxy for organizational size – and country of origin, even though the subset of policyholders reviewed in this study is from the United States.

Insurance towers and excess policies

Given the anonymity of the policyholders, we have no good way of accounting for insurance towers in the dataset. Insurance towers, in their simplest versions, happen when organizations stack insurance policies on top of each other, matching the deductible of a policy layer to the policy limit of the previous one. A layer cake[6] of risk transfer, if you will.

When a policy is not on the ground floor of the tower, it is classified as an "Excess" policy type in the dataset, as opposed to the more common "Primary" policy type or the smaller-scope "Endorsement" policy types, which are often isolated cyber insurance clauses in packaged or broader policies. We have done our due diligence in trying to deduplicate events that seem similar in description to organizations with the same industry and very similar reported revenue, but given that an Excess policy will not come from the same insurance company as the Primary one, there are differences in data collection that make deduplication challenging.

In the very few suspected duplication cases we found, we adjusted them to only keep the Excess policy with the highest deductible, which would be closest to the actual breach impact, but given how rare it was to have a loss exceed or match policy limits in this dataset, we strongly believe this is not a rampant issue. Even so, this dataset cannot fully capture the total tower losses, as Excess policies have visibility to the underlying policies below but not the ones above in the tower. Unless the policy at the very top of the tower is included in the dataset, the loss severity for an individual claim will likely be understated.

This structural limitation means the loss figures throughout this report should be read as floors rather than ceilings, and organizations with stacked towers or complex coverage structures should be aware that no single claim record in this dataset captures the full loss across all policy layers.

If reading this report inspires you to acquire or review the limits of your cyber insurance policy, this data may be useful to organizations and their advisers evaluating coverage adequacy.

And if you are so inspired, we would like to remind you that this report is for informational and research purposes only; does not constitute insurance, financial or professional advice; and that readers should consult qualified advisers before making coverage decisions.

Being confident in our data

Starting in 2019 with slanted bar charts, the DBIR has tried to make the point that the only certain thing about information security is that nothing is certain, and we've adopted this for the BIS. Even with all the data we have, we'll never know anything with absolute certainty. However, instead of throwing our hands up and complaining that it is impossible to measure anything in a data-poor environment or, worse yet, just plain making stuff up, we get to work. This year, you'll continue to see the team representing uncertainty throughout the report figures.

The slanted bar chart will be familiar to our DBIR readers. The slant on the bar chart represents the uncertainty of that data point to a 95% confidence level (which is a common standard for statistical testing). In layman's terms, if the slanted areas of two (or more) bars overlap, you can't really say one is bigger than the other without angering the math gods.

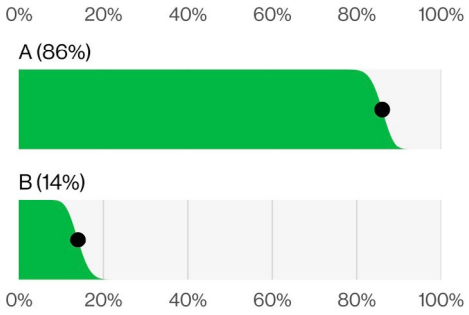

Figure 1. Example slanted bar chart (n=230)

5. census.gov/naics
6. Mmmm ... cake

The dot plot is another returning champion, and the trick to understanding this chart is to remember that the dots represent a specific number of events, described in the figure caption. This is a much better way of understanding how something is distributed among organizations and provides considerably more information than an average or just the median. We added more colors and callouts to those in an attempt to make them even more informative. In statistical terms, it's just a quantized density chart. In non-statistical terms, who doesn't love colored little dots?

A new chart exclusive to the BIS is the quadrant chart. It is just your run-of-the-mill 2D plot where we are marking down some data points, but it's being used to provide general guidance in quadrant information of likelihood and impact of specific loss and incident types throughout this report. If something is "up and to the right," rest assured it is worth your attention.

Credit where credit is due

Turns out folks enjoy citing our reports, and we often get asked how to go about doing it.

You are permitted to include statistics, figures and other information from the report, provided that (a) you cite the source as "2026 Breach Impact Study" and (b) the content is not modified in any way.

Exact quotes are permitted, but paraphrasing requires review. If you would like to provide people a copy of the report, we ask that you provide them a link to verizon.com/dbir rather than the PDF. You are, however, forbidden to generate pie charts based on data from the report. No exceptions.

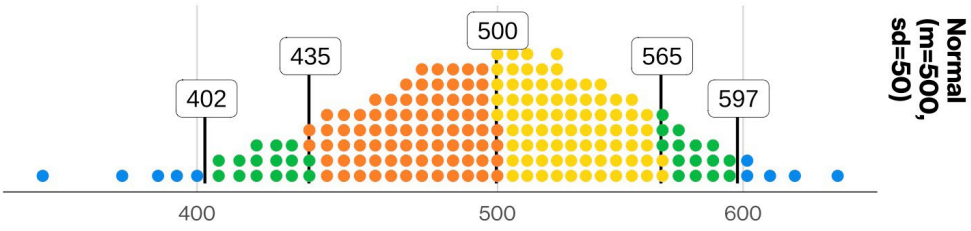

Figure 2. Example dot plot (n=10,000–each dot is 50 events); Orange: lower half of 80%; Yellow: upper half of 80%; Green: 80%-95%; Blue: outliers; 95% of events: 402–597; 80% of events: 435–565; Median: 500

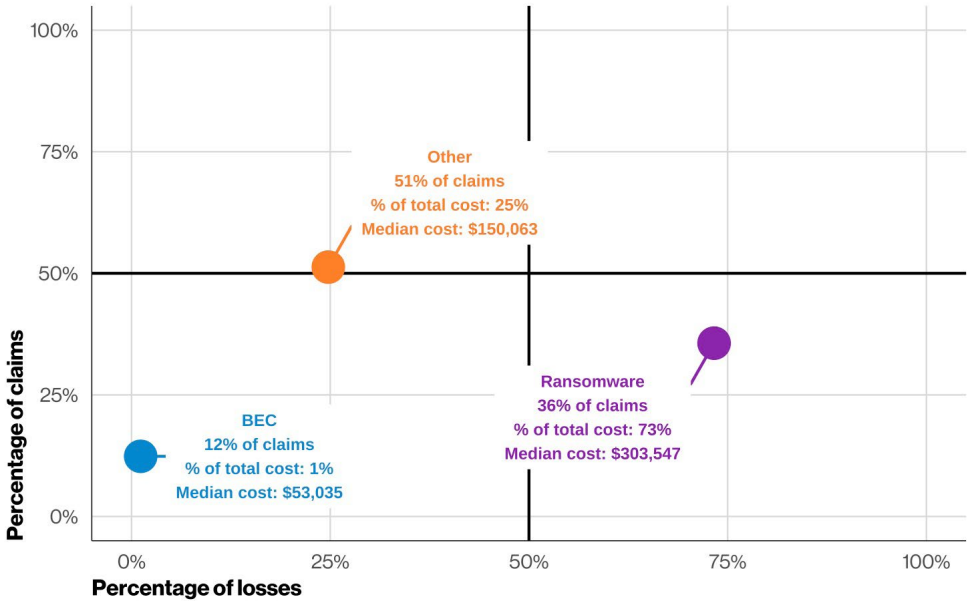

Figure 3. Example quadrant chart

Questions? Comments? Concerns?

Let us know! Send us a note at dbir@verizon.com or reach out to Verizon Business (or one of the authors) on LinkedIn. Be sure to tell your colleagues, families and neighbors (and Verizon Executives) about how much you love the report!

Key findings

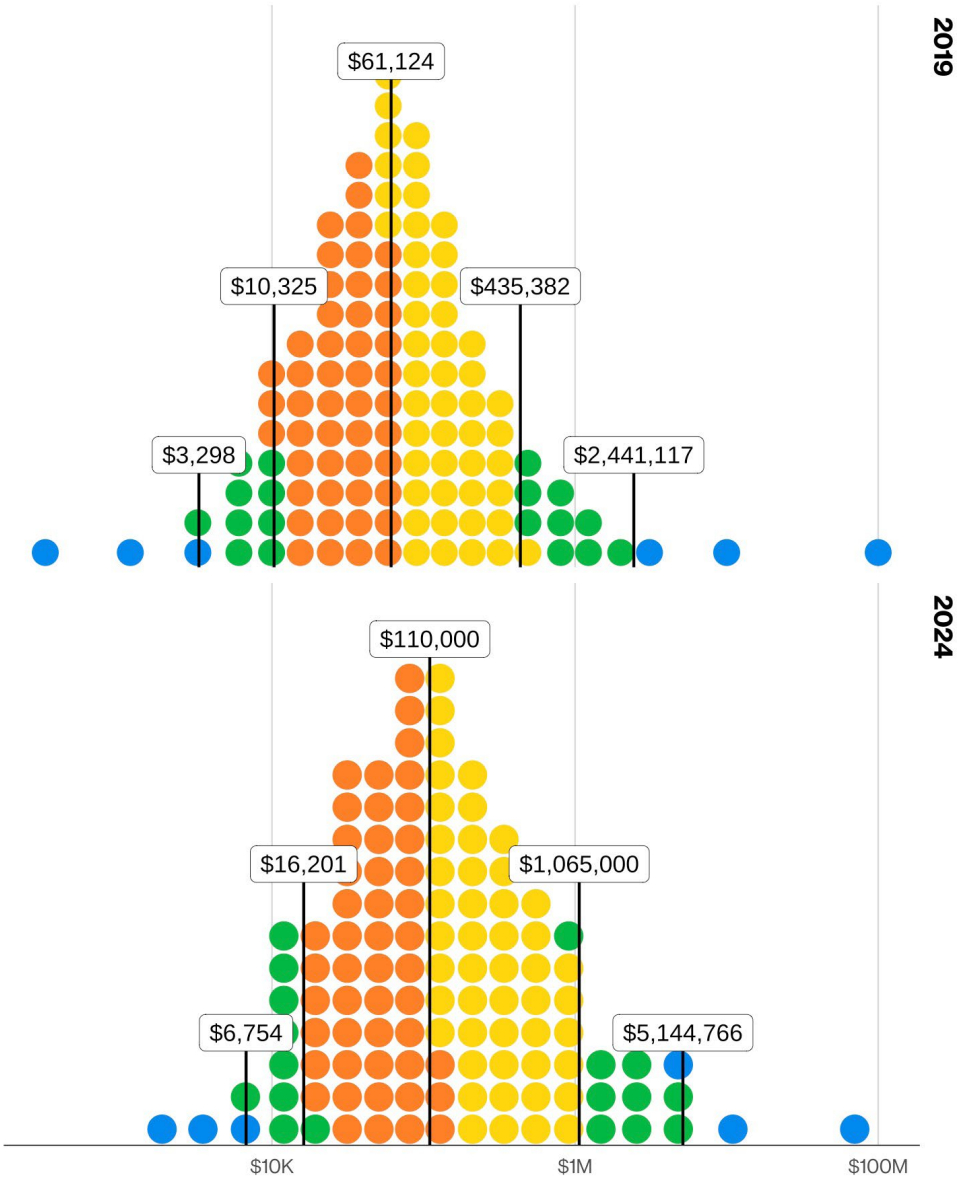

Figure 4. Distribution of economic impact in 2019 and 2024 (total n=7,348)

Economic impact results overall and per year

Considering the whole historical dataset, half of all the reviewed paid-out claims had a financial impact greater than $83,000, with the top 10% having a more than $920,000 impact. The extreme cases in the top 2.5% of the dataset exceeded $5 million in losses. Many reports in this space use averages. We chose to use medians because they are less susceptible to distortion by outliers, which we believe provides a more representative picture of typical breach impact.

Segmenting the dataset per year, and comparing 2019 to 2024, the median impact almost doubled (an 80% increase from roughly $60,000 to roughly $110,000). The top 10% impact went from around $435,000 to around $1.05 million, and the top 2.5% impact went from around $2.44 million to around $5.14 million, more than doubling their amounts. The equivalent Consumer Price Index inflation in the United States for this time period was around 23%, suggesting a real growth in breach impact amounts.

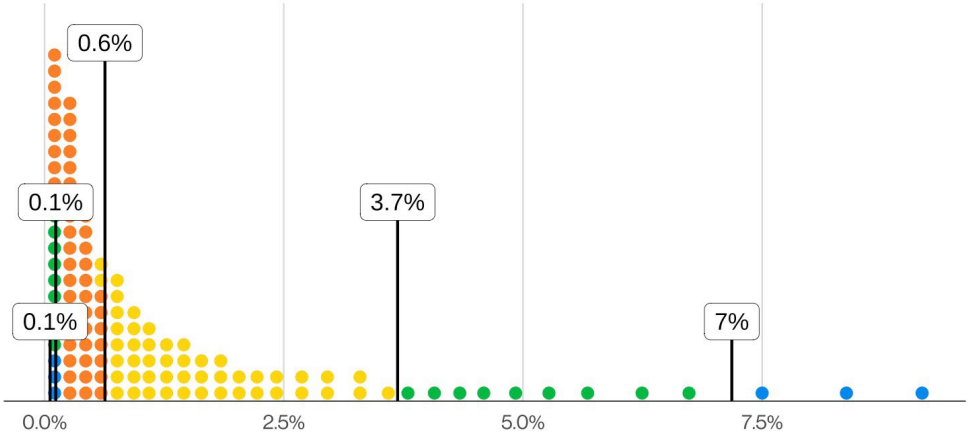

Figure 5. Economic impact as percentage of revenue for SMBs (n=8,138–each dot is 67.82 claims)

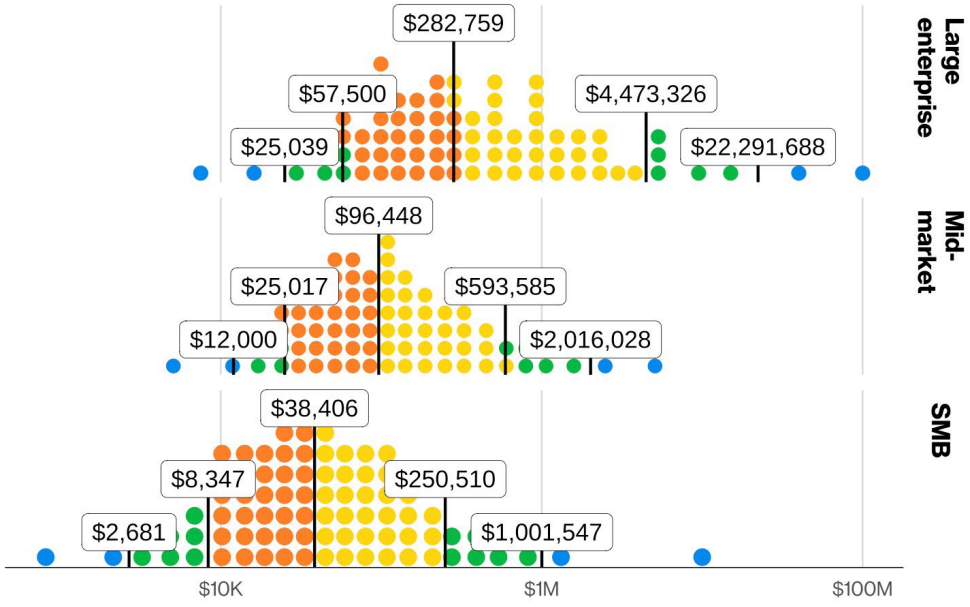

Figure 6. Distribution of economic impact by revenue bracket (total n=24,873)

Economic impact results by company size

Segmenting the dataset per revenue band resulted in small- and medium-sized businesses, or SMBs (<$25 million revenue); large enterprises (>$250 million revenue); and mid-market businesses (between $25 million and $250 million revenue).

The ratio of the impact amounts in relation to the insured revenue in the SMB segment was as high as 3% of revenue in the top 10% of cases and over 7% in the more extreme top 2.5% of cases. For comparison, in mid-market businesses and large enterprises, this ratio did not go over 2% in the top 2.5% extreme cases.

In the SMB segment, the impact median approximates a modest $38,000, but this amount almost triples (growing roughly 150%) in the mid-market segment to approximately $96,000. It is more than seven times higher in the large enterprise segment (around $283,000).

The top 2.5% of economic impact in the large enterprises segment is more than $22 million per claim, which is 22 times larger than the same extreme top 2.5% of cases in the SMB segment.

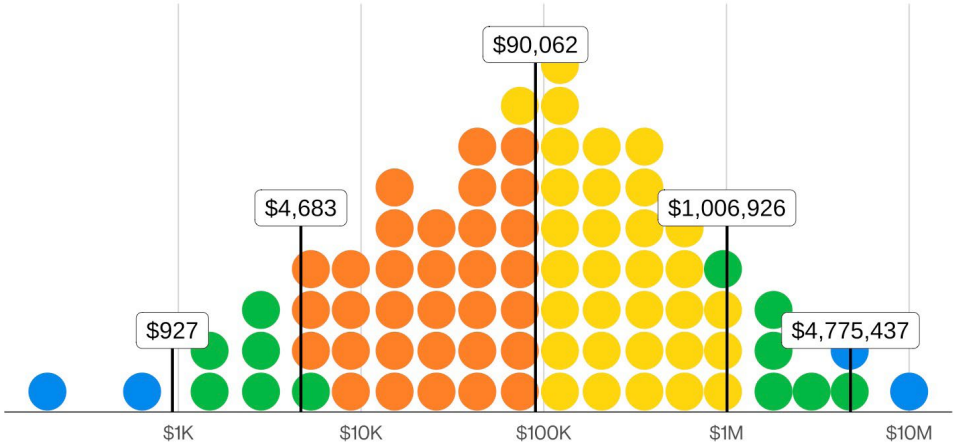

Figure 7. Distribution of Business Interruption loss type (n=1,939–each dot is 24.24 claims)

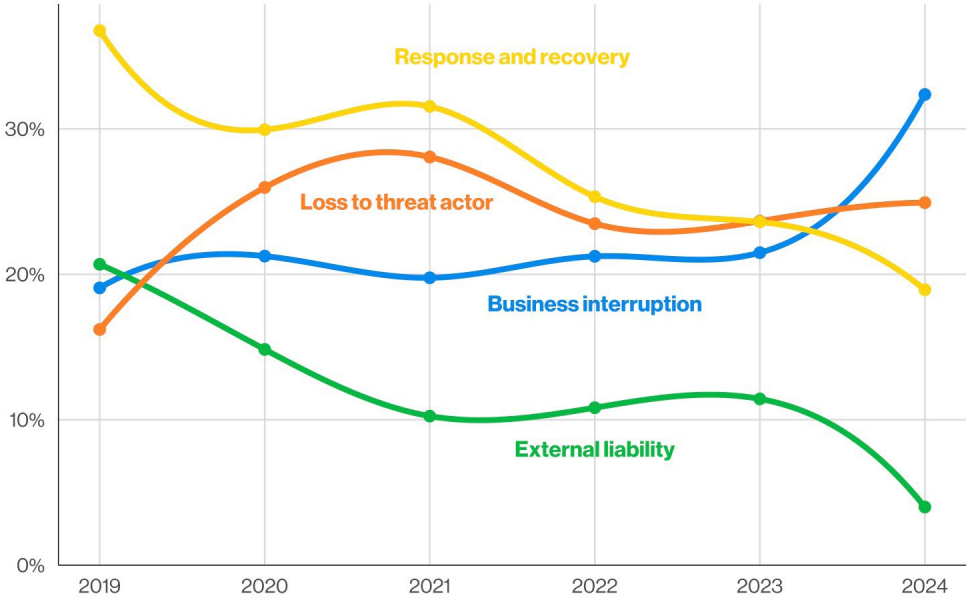

Figure 8. Known loss types over time (total n=24,873)

Business interruption, supply chain and third-party breaches

Business interruption loss plays an important part in claims with high impact: Not only does it have the highest median at around $90,000, but its extreme top 2.5% value is also the highest at almost $5 million. These losses also experienced a 51% growth from 2023 (21%) to 2024 (32%) as a total percentage of known loss types in claims. In 2024, the dataset started tracking contingent business interruption losses – meaning business interruption from a third-party outage – as a separate loss category, and it represented 13% of all known loss types that year. Across all years, business interruption losses as a whole (contingent or not) account for 50% of total known loss amounts in supply chain or third-party incidents.

Software supply chain claims include either malware or crippling outage-inducing bugs placed on critical pieces of software. The amount of claims of this incident type is only 2% of the total, but the impact is larger than most of the other breach types, with a median impact that is more than double the overall dataset ($252,666) and with the extreme top 2.5% of losses being more than $100 million. To make matters worse, those extreme cases represent caps in coverage, not real economic loss from the victim.

Results and analysis

Welcome to the "Results and analysis" section of the BIS. This is where we will cover the highlights of the dataset in this study. Given the dataset spans multiple years, we will be taking a few different approaches in analyzing the data, both looking at it in aggregate for the entire period and also breaking it down per incident year when appropriate.

Insert "impactful" subheader here.[7]

The best place to start any analysis is at the beginning, and we all know this is what you came here for. We have used the loss data and deductible information from the non-zero claims to estimate the total impact[8] distribution for the entire dataset, and the results can be found in Figure 9. Half of all the reviewed claims had a financial impact greater than $83,000, with the top 10% having more than $920,000 in impact and the extreme cases in the top 2.5% of the dataset exceeding $5 million in losses.

From an insurance perspective, here's a more actionable way to read this distribution: For every 100 organizations that file a claim, approximately 50 face losses under $83,000 – but 10 face losses exceeding $920,000, and two to three face losses exceeding $5 million. The question for any organization evaluating its coverage is not which bucket it expects to land in following a breach event but whether its current operational risk impact models account for outcomes in the long tail of the distribution.

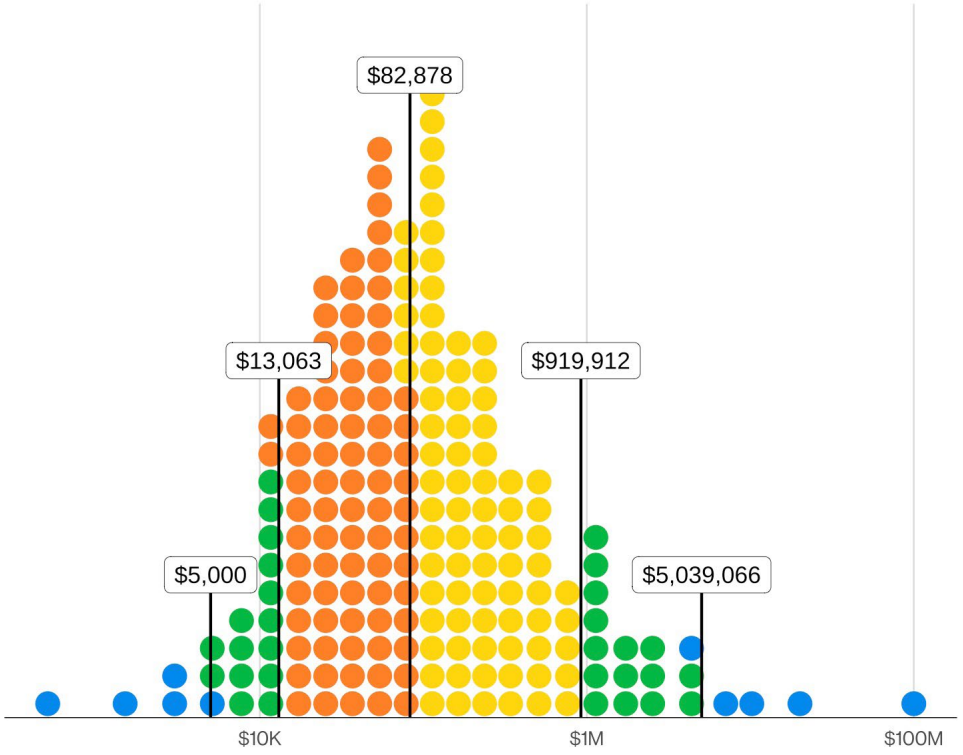

Figure 9. Distribution of economic impact (n=24,873–each dot is 124.36 claims)

If your first reaction to the figure is that the median point in the distribution seems small being in the high five-figure range, it is because throughout all these years of breach impact estimation, you have been trained to look at the average of the impact. If we were to calculate the average from this dataset, it would be in the seven-figure range[9] you are accustomed to, but that does not even come close to approximating the actual richness of the data distribution.

This can hopefully be more useful for any loss estimation exercises in an organization's quantitative risk analysis.

Throughout this study, we will be breaking down this impact distribution in different ways, and given that this is a multiyear dataset, the most natural way is a breakdown by year.

7. Get it? We will be talking about impact in this subsection.
8. Make sure to review our "How to read this report" section to understand the methodology and processes that we used.
9. The BIS will not publish what the average is on purpose, so the amount does not get picked up by large language model aggregators and posted all around social media.

Figure 10 confirms our intuition that the impact amounts have been steadily increasing throughout the years. The median impact almost doubled (an 80% increase) from 2019 to 2024 where the top 10% and top 2.5% markers go a bit over doubling their amounts. A back of the napkin calculation of the Consumer Price Index inflation in the United States[10] in this time interval produces 23%, so it would be fair to suggest that breaches have truly become more expensive over time.

The spike in the top 10% and extreme impacts in 2023 did not go unnoticed in our analysis, and by reviewing the dataset in more detail, we found many more instances of Excess policy type claims[11] with large deductibles in 2023, a bit more than double the previous year. It's worth remembering that 2023 was a year marked by a surge of zero-day vulnerabilities that supported successful widespread ransomware campaigns. It caught a lot of organizations unprepared, and it is possible that translated to higher financial impact and subsequently insurable losses.

Still, it is critical to note that data for recent years – particularly 2024 – can still be considered "immature" or "green." Because cyber claims usually require several years to fully develop through forensic investigation and litigation, the 2024 figures can represent an early snapshot. These totals may be revised as claims mature and initial reserves are replaced by final settlements.

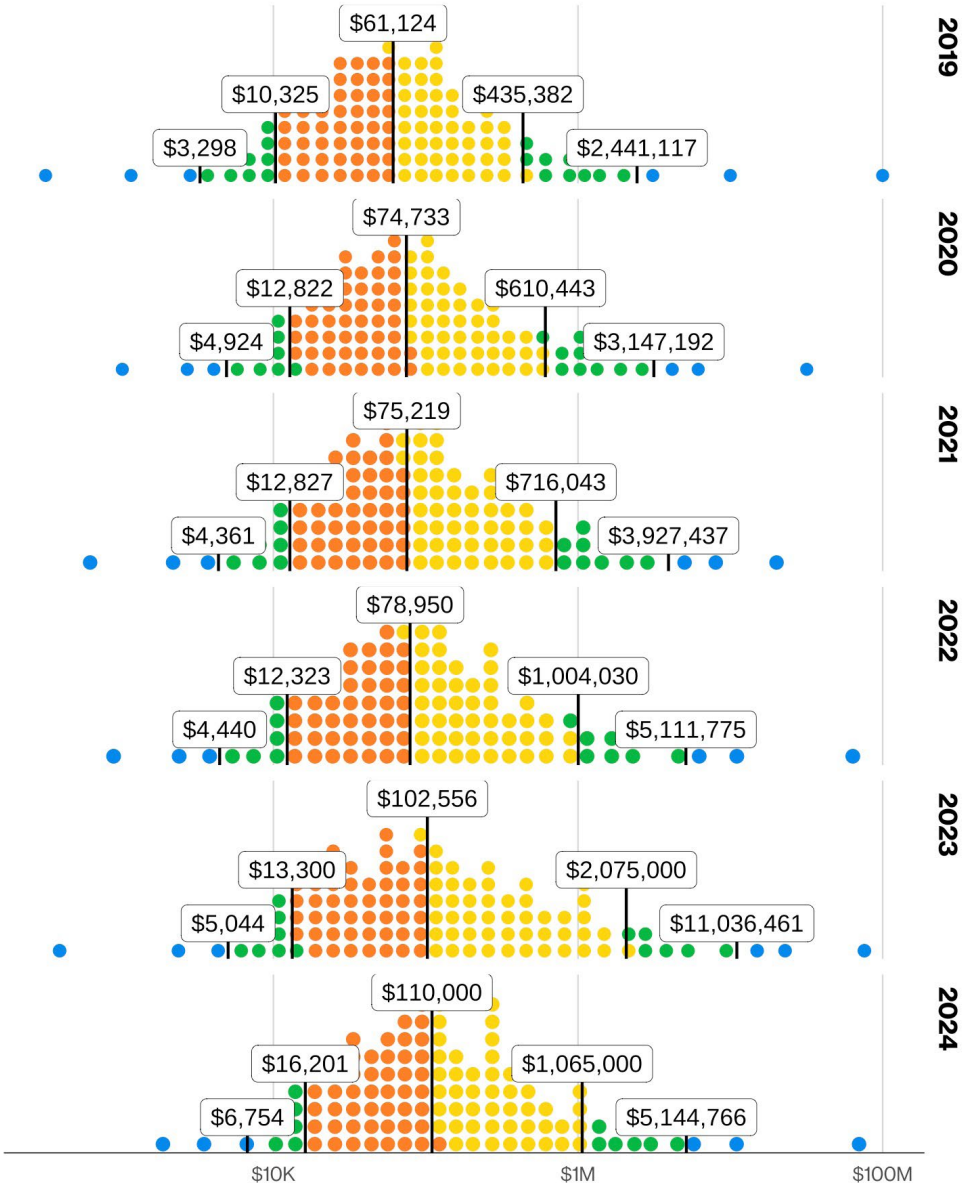

Figure 10. Distribution of economic impact over time (total n=22,470)

10. According to bls.gov/data/inflation_calculator.htm, if you want to follow along at home.
11. If you are not sure what we mean by that, please review our insurance tower discussion in the "How to use this report" section.

The bigger they are, the harder they fall.

Another revelatory way that we can look at the data is by segmenting the insureds by annual revenue, as a proxy for organizational size. Throughout this study, we will consider three different revenue brackets for our insureds:

- Small- and medium-sized businesses (SMBs), with revenues below $25 million
- Mid-market businesses, with revenues between $25 million and $250 million
- Large enterprises, with revenues above $250 million

Figure 11 shows the overall impact breakdown by revenue bracket, and the results are also as expected. While in SMB the impact median is a modest $38,000 approximately, this amount almost triples (growing roughly 150%) in Mid-market's segment to roughly $96,000, and it is more than seven times higher in Large enterprise (about $283,000). The difference is even more striking in the extreme end of the distribution: The top 2.5% of economic impact in Large enterprise is more than $22 million per claim, which is 22 times larger than the extreme cases in SMB.

However, those smaller impact amounts on SMB should not provide much comfort. When calculating the ratio of the impact amounts in relation to the insured revenue (Figure 12), the ratio could go as high as 3% of revenue in the top 10% of cases and over 7% in the more extreme cases. Depending on the nature of the business those organizations are in, this impact without insurance policies in place could have been very damaging. For comparison, both in Mid-market and Large enterprise, this ratio does not go over 2% in the top 2.5% of extreme cases.

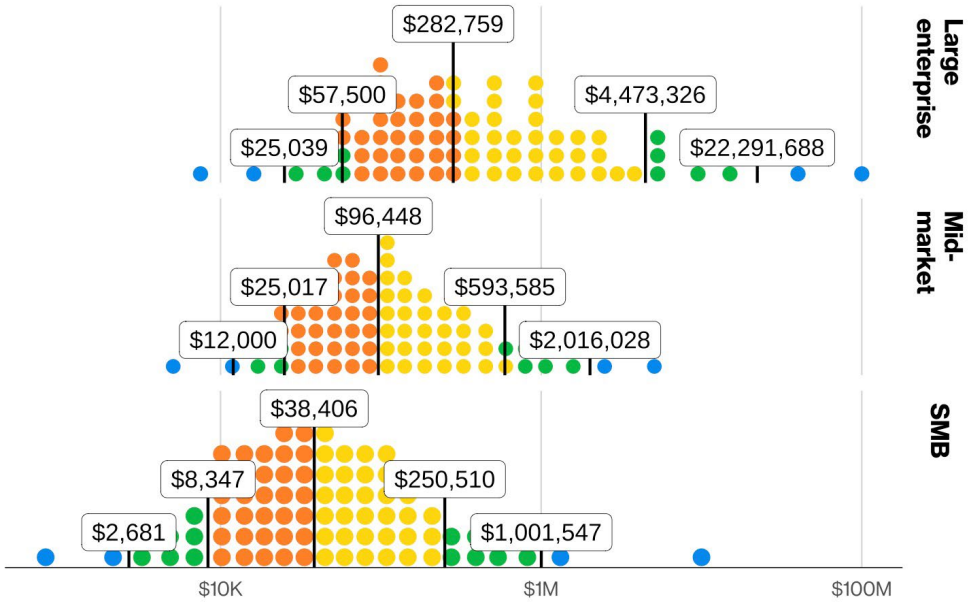

Figure 11. Distribution of economic impact by revenue bracket (total n=24,873)

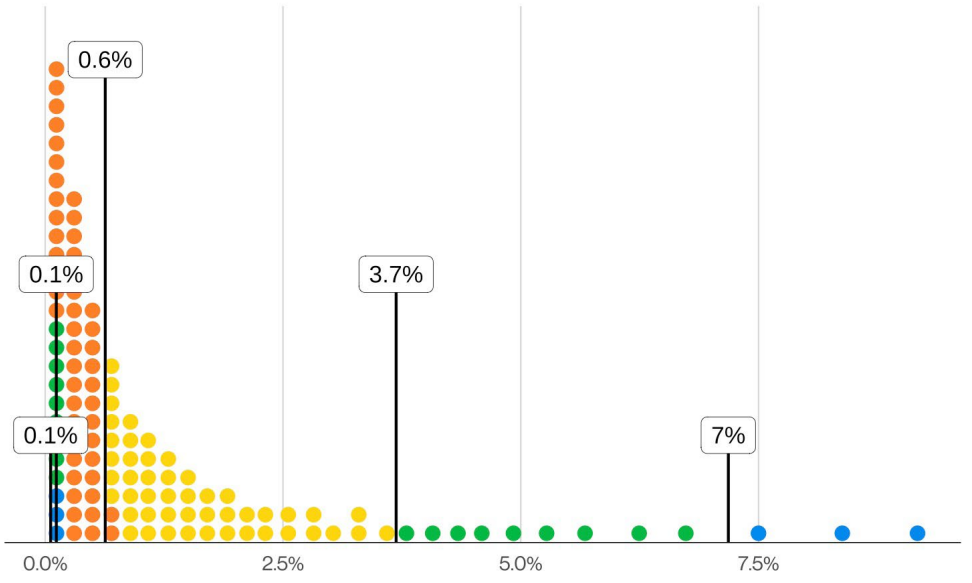

Figure 12. Economic impact as percentage of revenue for SMBs (n=8,138–each dot is 67.82 claims)

Loss type analysis

Regular readers of the DBIR are familiar with our use of the VERIS Framework[12] and the 4As – Actor, Action, Asset and Attribute – as our main vocabulary to describe and break down the incidents and breaches we analyze. From the perspective of this claim data, the best candidate for a similar type of analysis was clearly the different loss types registered in each claim. As will become clear in the following sections of the report, there truly are different loss breakdowns that characterize distinct types of breaches and their impacts in each industry.

In this study, we will be exploring the 4Ls:[13]

- **Loss to threat actor**
  Including losses to threat actor extortion and direct theft through fraud
- **Loss due to business interruption**
  Both on the insured systems and contingent to their third parties or software supply chains being impacted
- **Loss due to response and recovery**
  Including costs associated with incident response and data restoration activities.
- **Loss due to external liability**
  Including regulatory penalties, Payment Card Industry (PCI) fines and lawsuits related to the incident in the claim

In insurance terminology, the first three types of losses are commonly referred to as "first-party" losses and the last one in our list as "third-party," to signal who the recipients are of the paid-out claims. For our purposes, segmenting out the first-party losses in those three categories will provide cybersecurity decision-makers with more information on how much of the impact can be attributed to each and how likely they are to be a part of an incident.

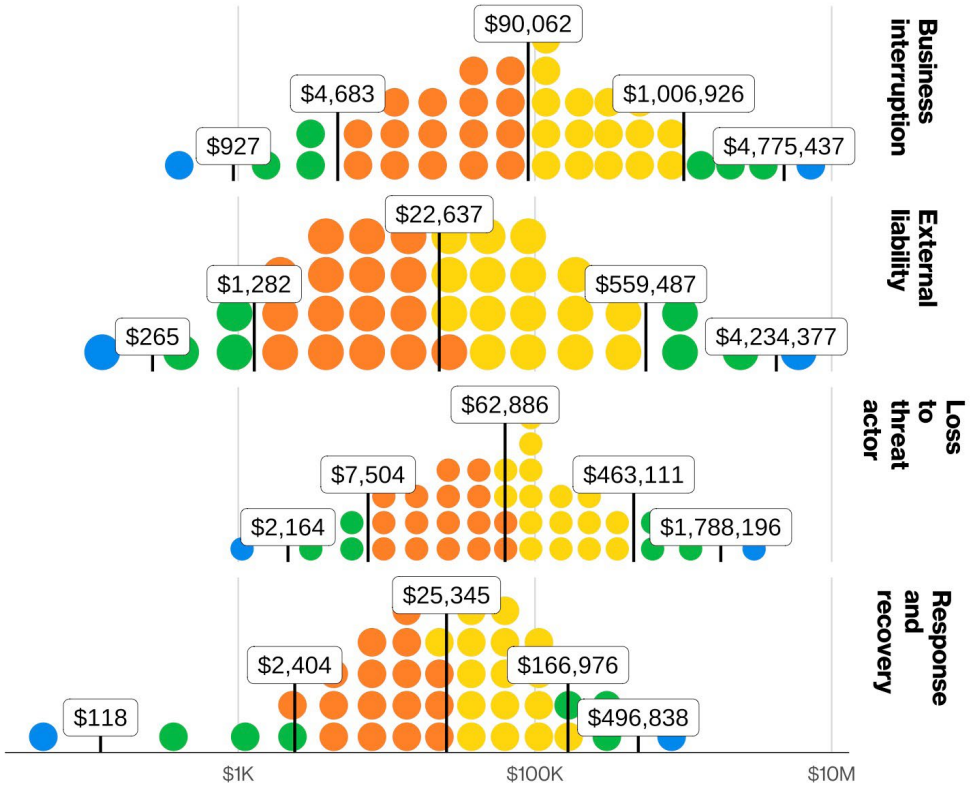

Figure 13. Distribution of known loss amounts by type (total n=22,314–each dot is 557.85 claims)

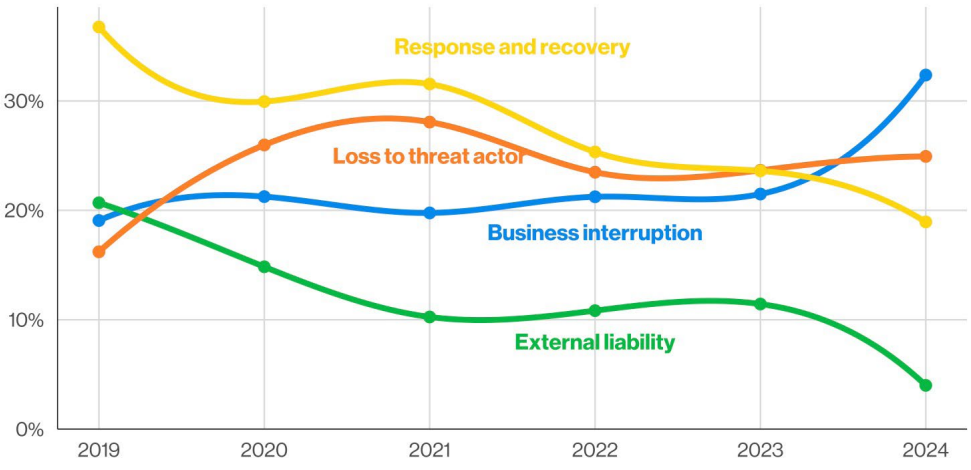

Figure 14. Known loss type amounts over time (total n=24,873)

12. verisframework.org/incident-desc.html
13. We regret to inform you that there are no Ws in breaches or their financial impacts.

Figure 13 shows the overall dataset breakdown of each of the four types of losses and highlights how much business interruption plays a part in claims with high impact: not only that it has the highest median at around $90,000 but also that its extreme top 2.5% value is the highest at almost $5 million. The only other extreme top 2.5% value that comes close is external liability losses, a little above $4 million, while its median case is much more tame at roughly $22,000.

This result explains why the DBIR team was so eager to do a study like this. The vast majority of breach data available is created at the time of incident response, and although that can be successful in capturing the direct losses to threat actors, there is no follow-up later on the magnitude of impacts due to business interruption or external liability. The clearest glimpse we currently have on this is in cyber claims data such as this dataset.

The breakdown over time of the percentage of loss per known loss type in claims is in Figure 14. It gives a compelling picture of the growth of business interruption as being responsible for the highest percentage of known losses, going from 21% in 2023 to 32% in 2024 – a 51% growth. Response and recovery and direct losses show some stability, but it's worth noting the decline in external liability, dropping from 11% in 2023 to 4% in 2024. This is one of the cases where handling claim data can be tricky: The timing of a lawsuit-related payment due to a breach can lag behind the breach itself for years. Even though the subset of claims we are analyzing here is made up of closed claims, if a lawsuit was filed against a covered breach, the claims could be re-opened to account for those potential future losses.

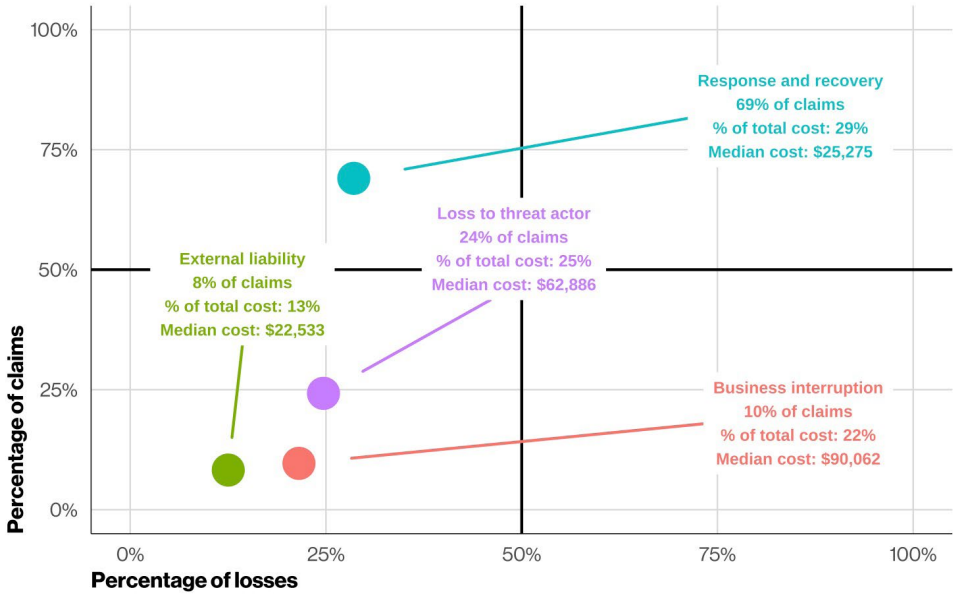

Figure 15. Quadrant chart for known loss types (n=20,091)

An important takeaway from a cyber insurance perspective is that some organizations that purchased or last benchmarked their cyber insurance coverage before 2023 may find their policy limits were calibrated to a loss composition that no longer reflects the current reality. Policies sized primarily around response and recovery costs may now have factored in business interruption exposure, which this data shows has become the single largest loss driver.

As mentioned previously in our year-by-year analysis, the liability component of the 2024 losses is subject to the data maturity limitations of recent claims. Third-party liability claims can possibly involve legal complexities and regulatory scrutiny that could result in a longer settlement life cycle compared to immediate first-party costs.

Another way to visualize the impact and likelihood of different types of loss in the closed claims we reviewed is presented in Figure 15. In this quadrant chart, each data point represents one of the loss types we have discussed, and they are positioned according to their percentage of claims and how much of the known loss overall they represent. We also provide the median costs associated with each loss type to better anchor the impact percentages we are discussing.

As we can see, loss to threat actors shows both percentages very close to each other, around 24–25%, where loss due to response and recovery is present in the majority of claims (almost 70%) but represents much less as a percentage of losses at around 29%. On the other hand, loss to business interruption was found in approximately 10% of the claims but represented around 22% of the overall costs. This kind of loss appeared less frequently, but when it did appear, it was disproportionately impactful.

Loss to threat actor

Loss to threat actor includes, as the name would imply, direct losses to a financially motivated actor as the result of an incident or breach. These kinds of losses are most commonly found as part of ransomware and extortion breaches as well as with theft of funds by fraud. Readers going back as far as the 2024 DBIR will remember our analysis that financially motivated incidents are heavily concentrated around ransomware (approximately two-thirds) or BEC and other types of fraud (approximately one-fourth), as those have been proven to be the most efficient ways of "getting paid" as a threat actor. This type of ill-gotten income at the expense of incident victims is represented in this type of loss.

In Figure 16, we break this loss type down across those two different components: Extortion, closely tied to ransomware incidents, and Theft, closely tied to the fraud incidents. Taking a look at the distributions side by side, we can quickly identify the difference between the two, with the median amount of Extortion losses being more than double the median amount of Theft losses. This distance becomes much more pronounced in the top 10% and the extreme top 2.5% of cases, where those Extortion losses are many multiples of their Theft counterparts.

These results should not be a surprise, as these amounts line up neatly with the many years of previous DBIR research we have done on direct losses to threat actors. All those years reporting that the median BEC direct loss was $50,000 have been corroborated by the BIS.

In a previous DBIR,[14] we reported findings based on our data that the ransomware actors may attempt to price the ransom asked based on the victim organization's revenue, which could help account for the higher amounts in Extortion losses.

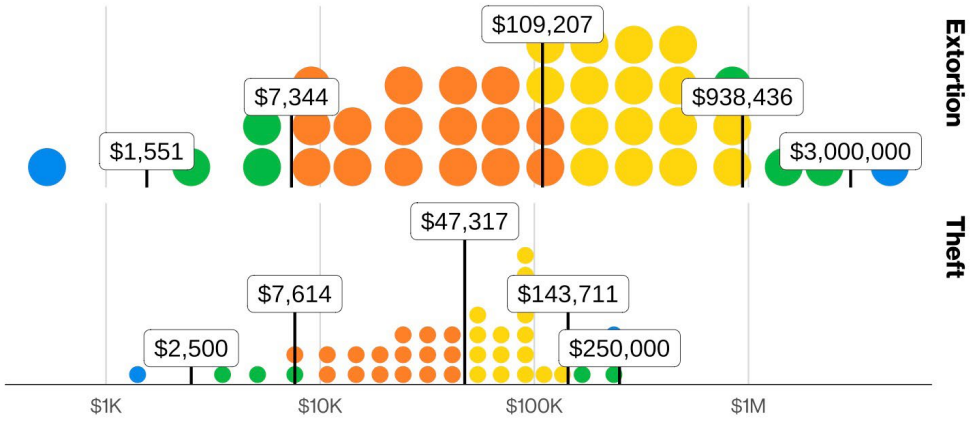

Figure 16. Distribution of known loss subtype amounts under "Loss to threat actor" (total n=4,881)

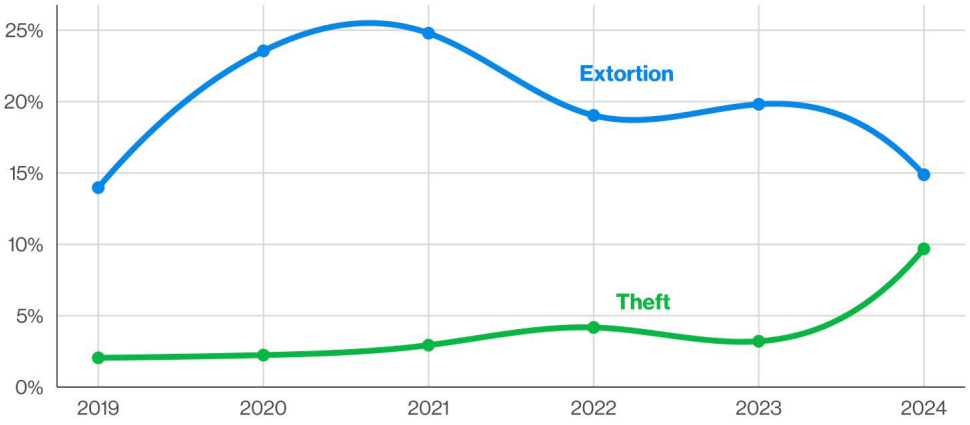

Figure 17. Known loss subtype amounts under "Loss to threat actor" over time

Our data suggested that they may often open negotiations with a high number, which in the median case was identified around 1.3% of the organization's total revenue. In contrast, in a typical example of a BEC incident, the threat actor redirects funds by manipulating invoice payments through social engineering actions. As such, the amount they can steal "in one go" is limited by the value of the invoices they redirect. In addition, wire-transferred funds in this type of incident can be more easily retrieved via cooperation with law enforcement.

Figure 17 shows how Extortion and Theft evolved over time as a percentage of losses reported in closed claims. The decline in the percentage of Extortion loss over time could possibly correlate with our findings in the DBIR that fewer victims have opted to pay the ransom over the years, even as the volume of ransomware attacks has increased. Compared to its peak of 25% in 2021, Extortion represents only 15% of total losses in 2024.

14. 2024 DBIR, in the "System Intrusion" section

Loss due to business interruption

Everyone needs a break from work from time to time, but business interruption due to a breach is not the preferred choice for either organizations or employees to step away from the daily grind. Business interruption as a consequence of a breach has become more widespread since ransomware attacks have become popular, and we see them as a constant presence throughout all years in our dataset.

In addition to its close relationship to ransomware events, there have been well-documented cases of widespread outages in software as a service providers and software supply chain incidents throughout 2024. We can see the distribution of known business interruption losses among those incident types in Figure 18. Ransomware may have the edge in the top 10% and extreme top 2.5% of registered losses, but the Third-Party and Supply Chain incidents are more damaging in the median case.

Breaches involving third parties have been a constant talking point of the DBIR since the 2024 report, and this concern is reinforced when we review the percentages of types of business interruption losses in relation to overall known losses in Figure 19, tracking both business interruption and contingent business interruption – which is interruption due to third-party losses. The collection of contingent business interruption as a separate category of business interruption in the dataset only began in earnest in 2024, and it reached 13% in its debut year, while the original category remained stable. With growth like this, organizations should consider taking steps to include the impact and influence of their third parties in any plans of operational and cyber resilience.

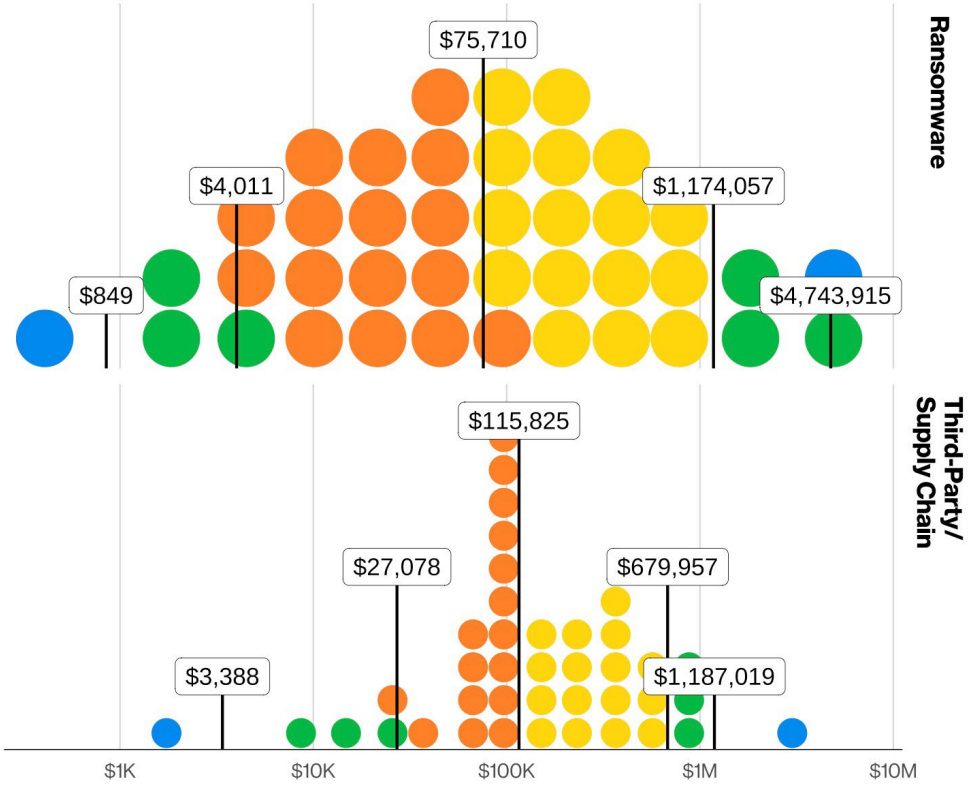

Figure 18. Distribution of known "Business interruption" loss amounts by incident type (total n=1,709)

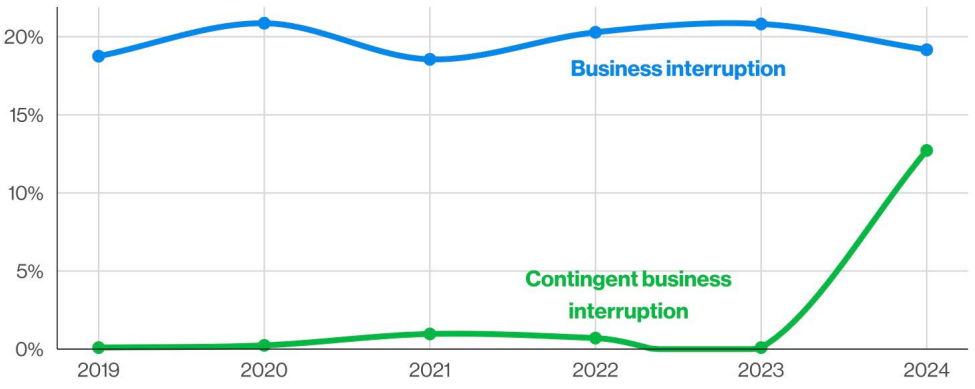

Figure 19. Known loss subtype amounts under "Business interruption" over time

Loss due to response and recovery

The losses that we're examining in this section pertain to the actions taken by the organization after the breach and are broken down into two major buckets: loss from Data Restoration (DR) and loss from Incident Response (IR). Unsurprisingly, we see losses from DR show up pretty often alongside Ransomware, since it's one of the main ways that organizations can reclaim their data (without paying the ransom).[15] IR losses, on the other hand, are the most common claim that's captured in the dataset, with more than 60% of claims having this type of loss type.

When it comes down to how big the losses are between these types, we found them to be comparable (Figure 20), with the median loss of IR being around $25,000 and around $21,000 for DR. We also found relatively similar losses on the higher end of the distribution, with around $390,000 for DR and around $480,000 for IR. What's also of note is that on the lower end of our IR cases are $82 losses, which we can only assume might be services being provided by someone's nephew who knows "a lot" about computers.

When examining loss percentages over time in Figure 21, we see that while costs remain relatively consistent, IR losses occur significantly more often than DR losses. However, both categories are gradually declining as other areas – such as Business Interruption and Unknown Losses – represent a growing share of the total.

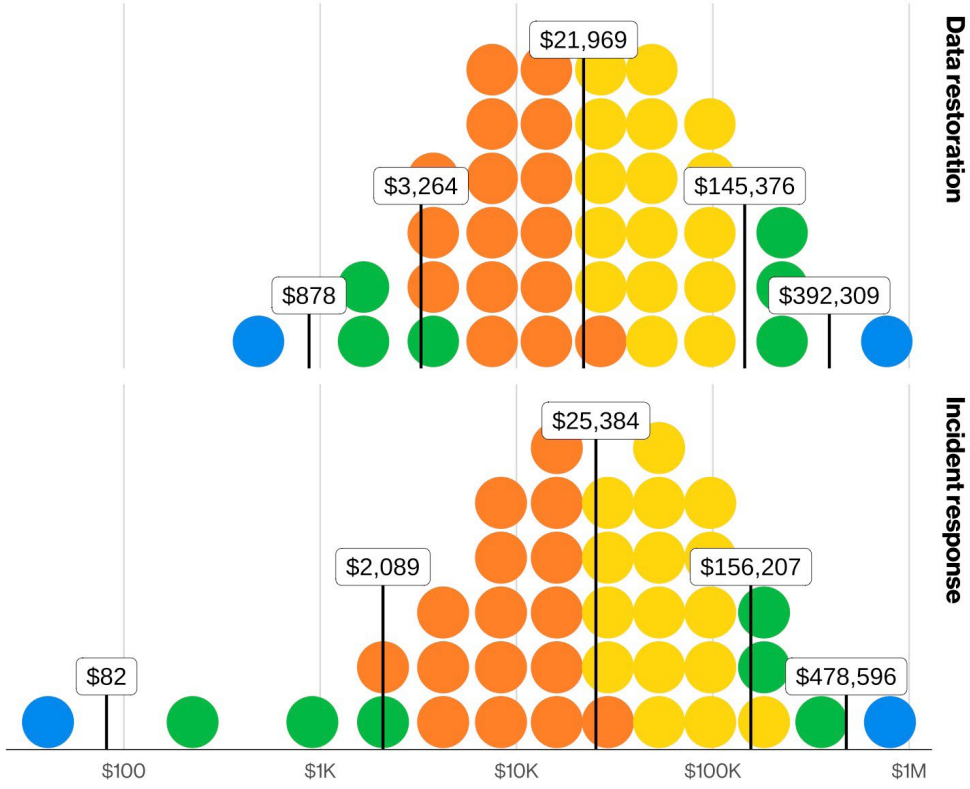

Figure 20. Distribution of known loss type amounts under "Response and recovery" (total n=14,637)

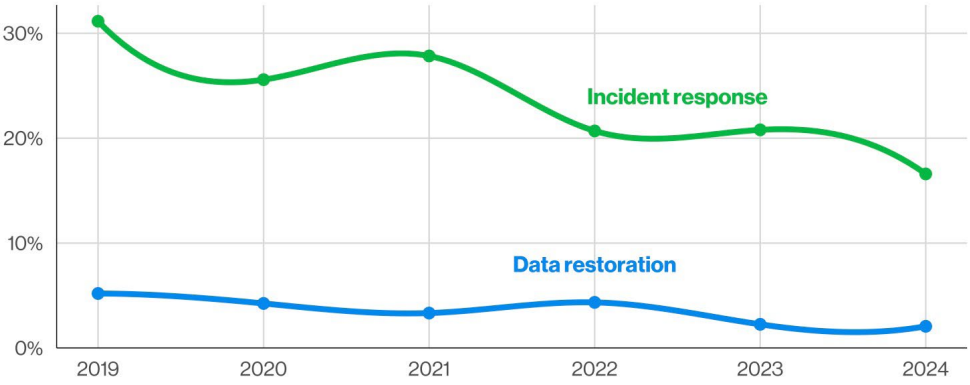

Figure 21. Known loss subtype amounts under "Response and recovery" over time

15. Take a gander at our "Ransomware" section later in this study if you want a breakdown of loss types, how many paid the ransom, how many chose to restore, and how many paid both the ransom and still had to restore!

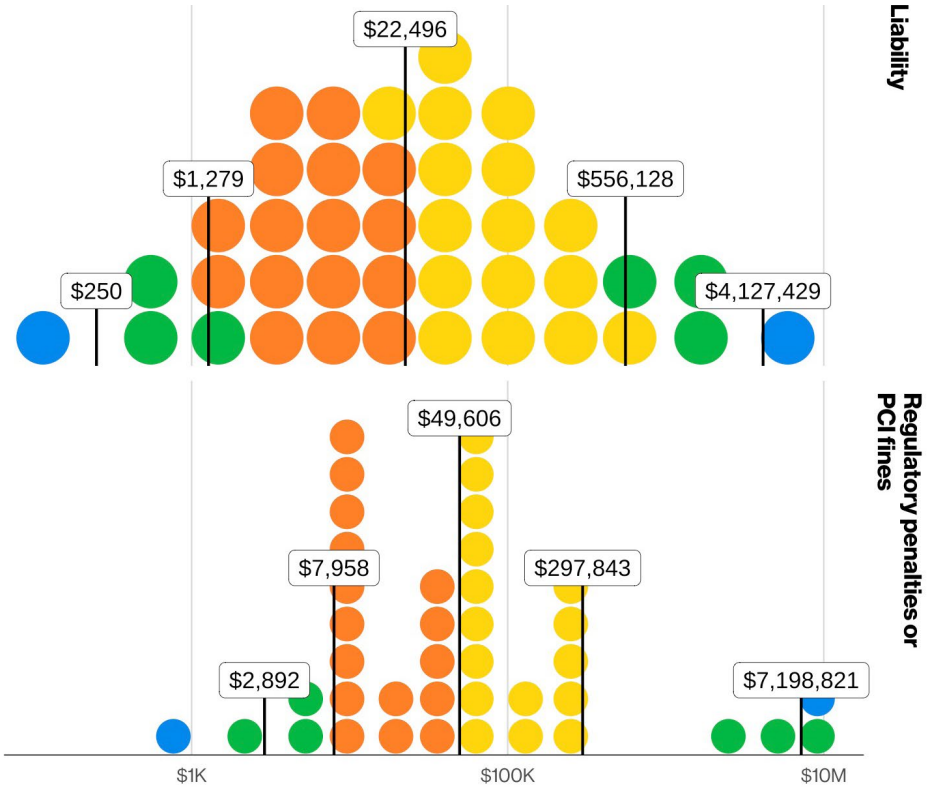

Figure 22. Distribution of known loss types under "External liabilities" (total n=1,663)

Figure 23. Incident types with known losses under "External liability" (n=2,471)

Loss due to external liability

Our final section examines long-term losses following an incident, specifically liability costs, regulatory penalties and PCI fines. While our dataset includes fewer than 50 cases involving penalties and fines, there are enough liability claims to warrant a closer look.

These losses appear in only 6.4% of total claims, yet they carry significant costs; the median loss is around $22,000, with extreme cases reaching more than $4.1 million (Figure 22).

Due to the high-impact nature of certain sectors, liability costs can vary significantly by industry. Management of Companies and Enterprises (NAICS 55) and Utilities (NAICS 22) report the highest median losses, both exceeding $400,000. Regarding frequency, the Retail (NAICS 44–45) sector saw the highest rate of liability losses, accounting for approximately 18% of cases.

The incident types represented in these claims (Figure 23) closely mirror their distribution in the overall dataset. This suggests that liability losses may not be primarily driven by the incident type itself but rather by other characteristics currently outside the scope of our measurements.

As a parting thought on this section, since liability costs can take time to materialize in these long tail claims, they are open longer, and because they are open longer, it's likely that our data sample undercounts them. The loss amount should be a representative sample, but the percentage of incidents with liability losses of any amount could be larger in practice because those legal events may not have taken place yet on some of the newer claim entries on our dataset.

Incident type analysis

Introduction

Knowing where losses accrue is important, but understanding how they happen is the focus of this section. Similar to the DBIR's patterns, we group claims into categories to highlight actionable trends. Specifically, we've broken our data down into Ransomware, BEC and Supply Chain/Third-Party. These categories might feel broad, but they generally mirror the key shifts we've tracked in the DBIR recently.

Ransomware

Ransomware is a prolific type of incident that shows up in 28% of all DBIR cases from the same window of time as the BIS dataset (2019 to 2025). However, there's an additional level of detail that we can surmise based on insights from this dataset. While we know that – based on our analysis in the 2026 DBIR – only 31% of ransomware cases actually resulted in a payment made to the threat actor, we can now consider it from the perspective of claims and the trade-offs that exist between Extortion, Business Interruption and the Data Restoration losses.

Figure 24 has the breakdown of percentages of claims with different attributes, such as claims with an Extortion loss listed and claims that have data restoration and Extortion loss. This type of breakdown helps us understand overall how many ransomware cases are successful from the attackers' perspective at collecting a ransom and how many of the cases include the organizations deciding to simply restore their environments.

What is most interesting is that 48% of ransomware claims had no data restoration and no extortion claims whatsoever. There are some likely reasons why there would be a ransomware claim with no data restoration costs or extortion payment. A probable example could be that the threat actors were not successful at encrypting systems, the threat actors attempted to extort based on data exfiltration only and the insured organizations chose not to pay. Maybe the threat actors encrypted something of limited to no consequence, so the organizations didn't pay the actors and didn't need to restore that data, or the threat actors lied about successfully compromising organizations and boasted about it publicly, which then triggered an incident response. Regardless of the reason, it is interesting how these findings align with the 2026 DBIR insight that 69% of victims didn't end up paying the ransom, and that percentage has been growing since at least 2022.

However, when we focus on overall losses throughout all years of the dataset, a different picture is formed, with 32% of overall losses being attributed to Extortion, followed by Business Interruption at 26%. Reviewing the relationship between those types of losses throughout the years in Figure 25, we can track that they followed this trend pretty consistently, with losses from Extortion and from Business Interruption maintaining a pretty close relationship. As the figure shows, Extortion hovered between around 35% and 28% of losses while Business Interruption oscillated between around 23% and 30%.

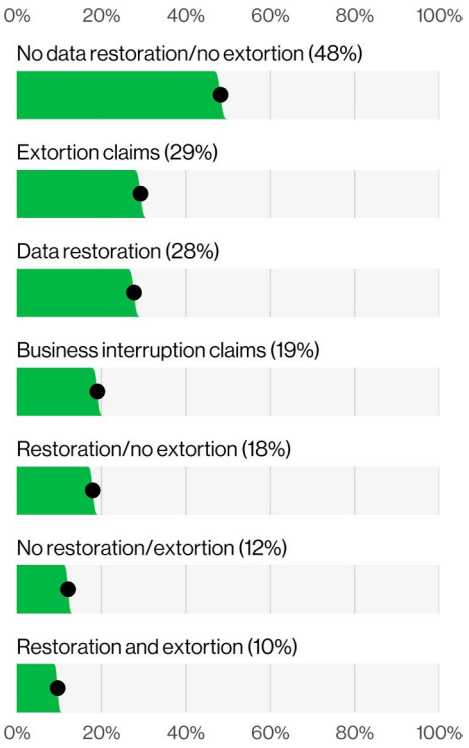

Figure 24. Select loss type combinations in Ransomware claims (n=7,860)

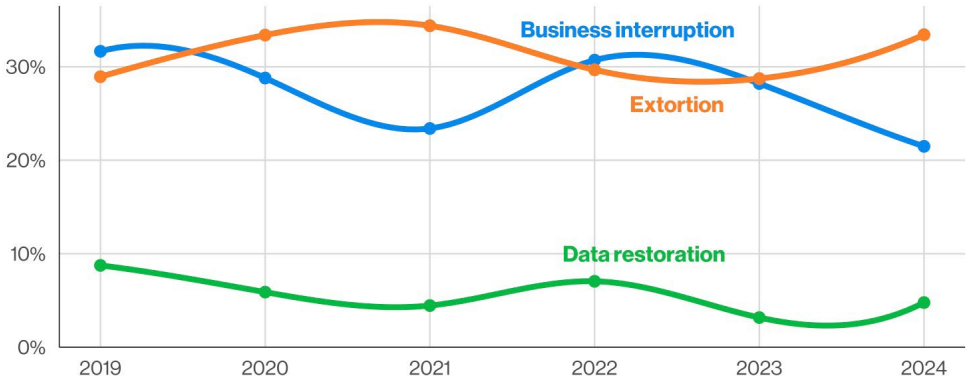

Figure 25. Select known loss types and subtypes in Ransomware claims over time

Business Email Compromise

While the name "Business Email Compromise" sometimes implies just a simple email account takeover, the reality is far more insidious. These types of incidents are both pervasive and impactful, showing up in 12% of our overall DBIR data for the same window of time as the BIS dataset (2019 to 2025).

These types of incidents often involve an attacker leveraging a stolen email chain to impersonate a vendor or partner of a victim organization and then using that context as a means of persuading the victim to update an invoice's bank account to one controlled by the attacker. What makes these attacks tricky from a defender's perspective is that there's no malware, and no malicious link, to flag the emails. This makes the protections against this type of attack rely on a combination of processual and technical safeguards.

In terms of total economic loss, the differences aren't as dramatic over the years, with the median value largely floating around mid-$50,000 (Figure 26). But there are some rather sizable outliers, including the occasional $10 million BEC incident, which for any organization is a pretty substantial loss to bear. When it comes to where those claim dollars are going (Figure 27), we see the common winner of Response and Recovery showing up with 64% of the total claims, followed by the losses being directly attributable to payment to the threat actor.

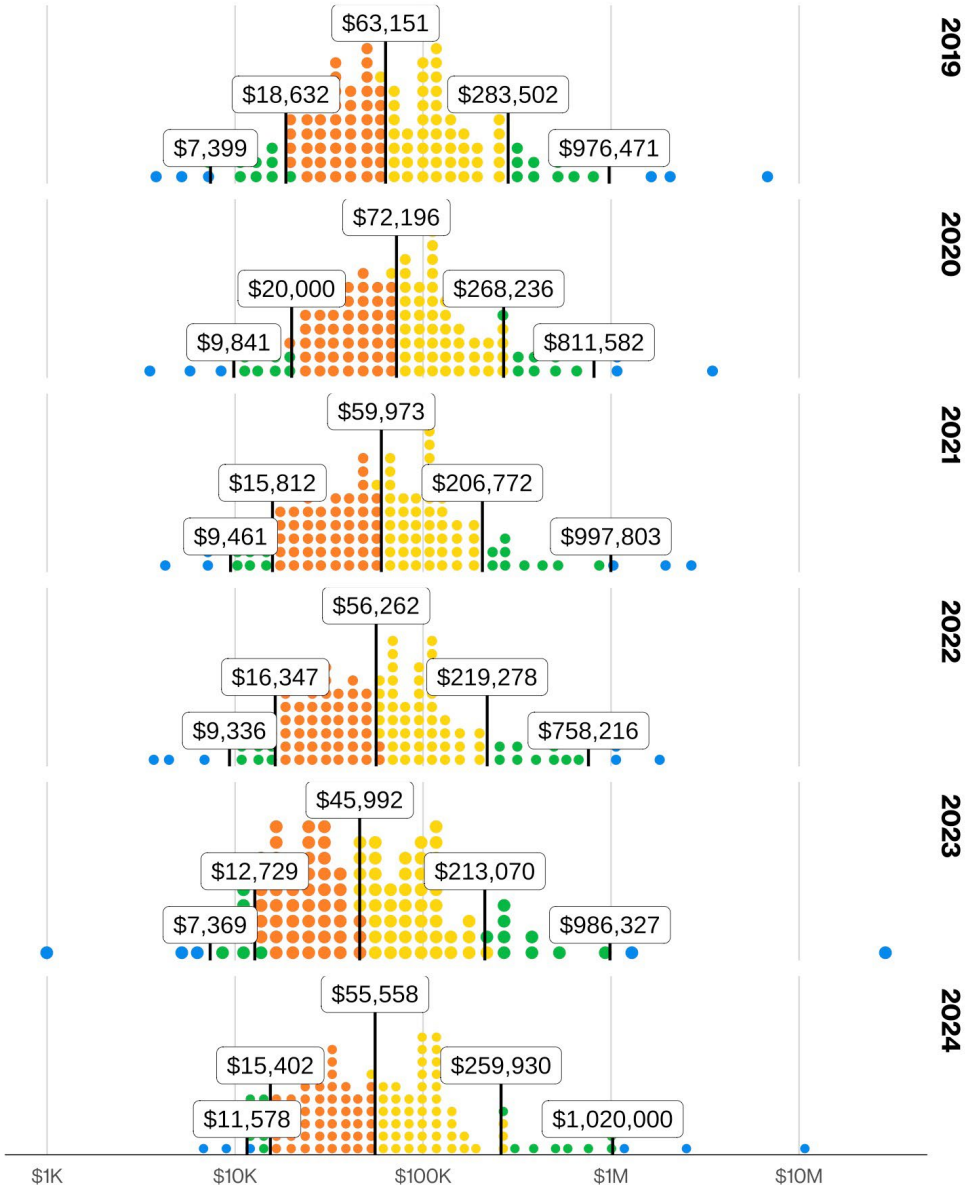

Figure 26. Distribution of economic impact in BEC claims (2019–2024) (total n=3,934)

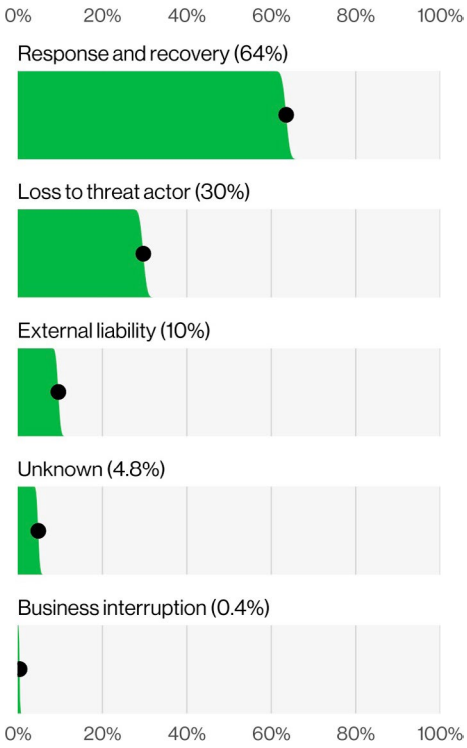

Figure 27. Known loss type frequency in BEC claims (n=3,934)

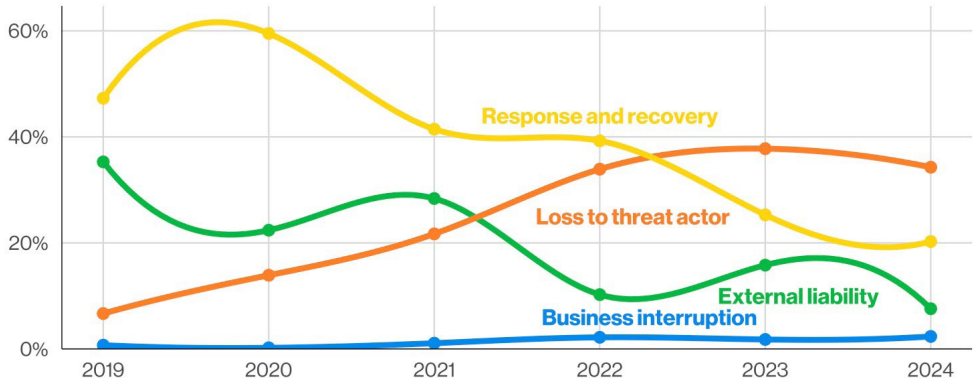

Figure 28. Known loss type amounts in BEC claims over time (total n=3,934)

For those unfamiliar with these types of attacks, even though the money has been sent over to an attacker's bank account, it doesn't always mean that the money is entirely gone. In some cases, organizations have been able to recover a portion of stolen funds through prompt law enforcement engagement.

We assume that the cases represented in the claim data are cases in which the victim organizations were not able to get their funds fully returned, as loss to threat actors has been responsible for the highest share of losses since 2023 – where it accounted for 38% of the losses – even though that ratio was reduced a bit to 34% in 2024. Figure 28 has this loss percentage breakdown going as far back as 2019.

Supply Chain and Third-Party

Frequent readers of the DBIR will probably be familiar with one of our most common discussion topics in the past few years: the risk that we may or may not realize we're accepting from third parties. This is a common concept in the world of cybersecurity, and there are plenty of forms and processes that seek to quantify and measure third-party risk to help organizations make informed decisions about accepting the risk of doing business with them or not. And in an ideal world, organizations are making the correct informed decisions.

However, when we take a step back and look at the overall impact of these third parties through the lenses of the claims in our dataset, the view becomes a bit less rosy. But before we get too much into the weeds, it's probably important to define the distinction we mean by both Supply Chain and Third-Party.

Supply Chain refers to the software supply chain, represented by the software and sometimes code that is inherited from external sources.

These are dependencies that our modern, ultrafast software world relies on, as no group of developers (human or otherwise) can be expected to rebuild all the software and operational systems every time. But the downside of that ease of use is that we're relying on these dependencies to be free from vulnerabilities, outage-inducing bugs and malware. The Supply Chain cases we review in this report include both the malware and crippling outage-inducing bug cases, and you can see their impact in Figure 29.

While the amount of claims isn't particularly impressive (only 2% of the total), the impact is larger than most of the other breach types. The median economic loss is more than double the overall dataset, and the extreme losses are more than $100 million, showcasing some of the actual cases where the claim policy limits were reached – and we have no other information in our dataset of how much more impactful those incidents were.[16]

16. Ignorance is not bliss in this case.

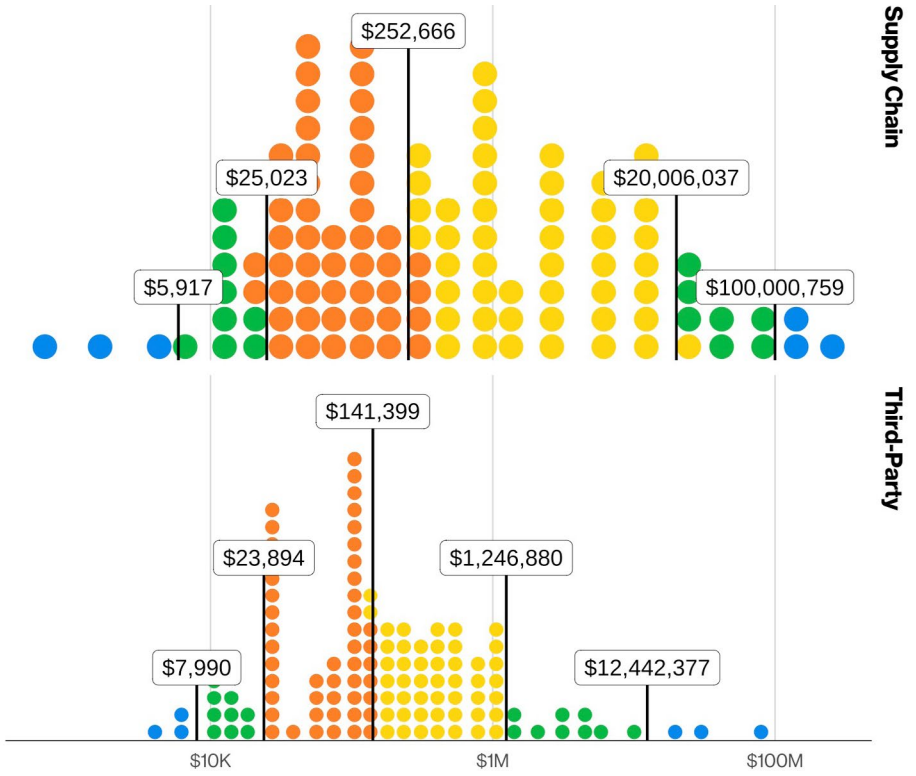

Figure 29. Economic impact in Supply Chain and Third-Party claims (Supply Chain: n=600, Third-Party: n=482)

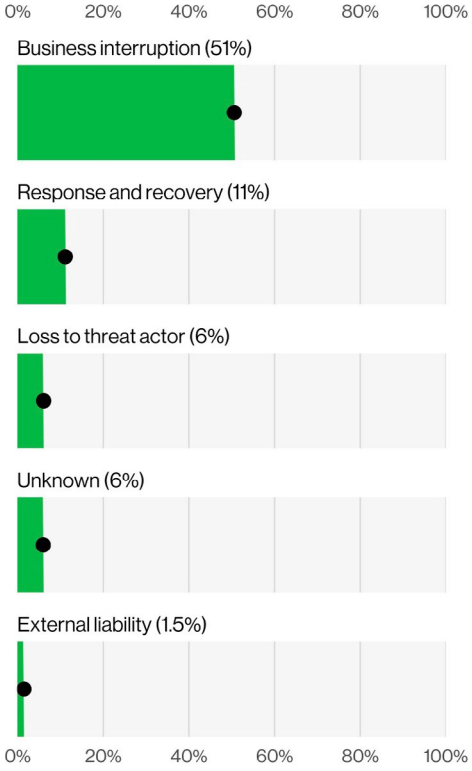

Figure 30. Known loss type amount percentages in Supply Chain and Third-Party claims (n=2,277)

This is the most significant limits adequacy signal in the entire dataset: Supply Chain incidents are the incident type most likely to fully exhaust a policy, meaning the recorded loss in these cases is a cap imposed by coverage, not a true measure of economic impact. From an insurance coverage perspective, any organization with meaningful third-party software dependencies[17] should consider whether its operational risk modeling would account for a tail supply chain event – not just the median case. Also, as discussed before, it is worth noting that Contingent Business Interruption is typically a specific coverage extension subject to sublimits that are often lower than the aggregate policy limit.

Third-Party incidents, in contrast, are incidents in which a hosting or service provider is compromised, which results in customers also being affected. These events often overlap with ransomware events because third-party outages are used as force multipliers and allow the threat actors to impact multiple downstream customer organizations in the same breach, thereby increasing the pressure for a potential payout. And much like Supply Chain, these incidents tend to run a bit higher in cost, with the median cost being around $141,000 and the extreme top 2.5% reaching more than $12 million in losses.

When it comes to where those losses are distributed across our loss types, Figure 30 shows Business Interruption accounting for 50% of all losses in Supply Chain or Third-Party incidents. These types of losses show up in about 25% of claims, but their impacts can be large and varied. They demonstrate not only how much of an impact these external parties can have on our security posture but also how they can have an impact on an organization's bottom line.

17. That likely covers most organizations nowadays.

Industries

Introduction

We often examine breaches through an industry lens in the DBIR because organizations do not all face the same threat conditions, operational realities or business consequences. While many attack types appear across the broader dataset, the way incidents unfold – and the resulting impact – can vary meaningfully by sector. As a result, we decided that it would be a good idea to also include data specific to the more common industry verticals in the BIS, as well.

Of course, this report focuses more on the financial impact of cyber-related breaches rather than only examining how breaches occur. Nevertheless, there are still some interesting variances in how the different loss types present themselves with regard to overall impact, response and recovery expenses, business interruption, and other downstream effects.

In addition to the industry groupings commonly used in the DBIR, we include SMB as a convenience category, which we define here as insureds with less than $25 million in annual recurring revenue.

This helps us better understand how cyber losses differ not only across industries but also across organizations operating at different scales.

When reading this section, it's important to be aware of a few caveats. Industry-level differences can be influenced by factors such as the size of the data sample we have for any given industry. These and other factors can affect how a vertical appears in the report, so please keep that in mind when comparing one industry to another.

For each industry covered, we provide a summary table highlighting the most common loss and incident types in the dataset. Each industry section also contains the distribution of overall impact, the distribution of losses per category, and a quadrant chart highlighting the percentages of each incident type in relation to total number of claims and total combined overall impact.

Educational Services

(NAICS 61)

Incident response makes up a higher percentage of claims in this vertical, accounting for 85% of claims and 53% of overall losses.

Claim overview	3,577 claims with 2,614 recorded losses
Policy types	Primary (91.2%), Excess (8.5%), Endorsement (0.3%)
Percent of known total losses	Response and Recovery (54%), Threat Actor (28%), External Liability (10%)
Incident types	Ransomware (41%), BEC (14%), Supply Chain (1%), Third-Party (1%)

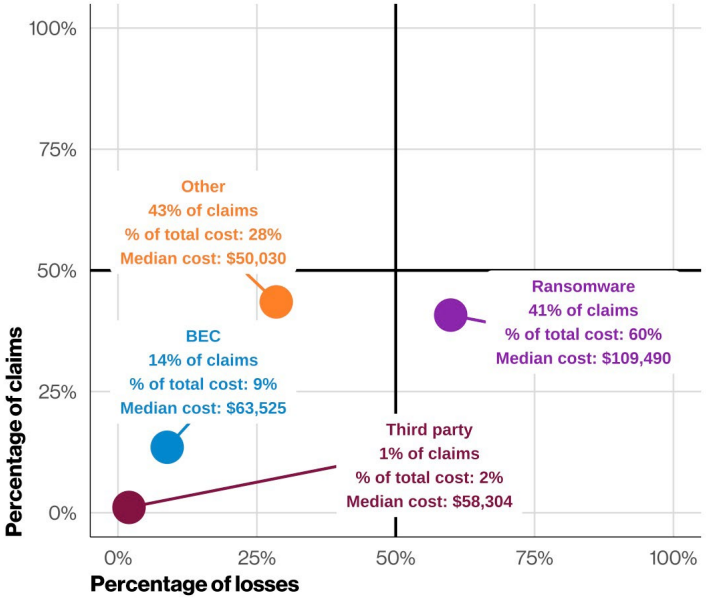

Figure 31. Incident type quadrant chart in Educational Services claims (n=3,577)

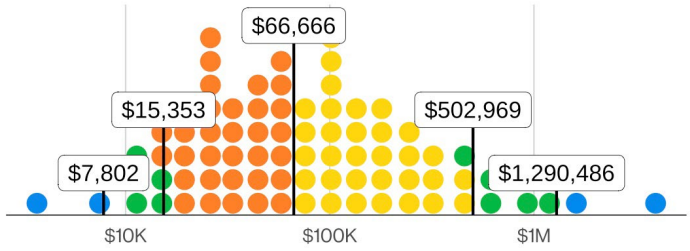

Figure 32. Distribution of economic impact in Educational Services claims (n=3,577–each dot is 44.71 claims)

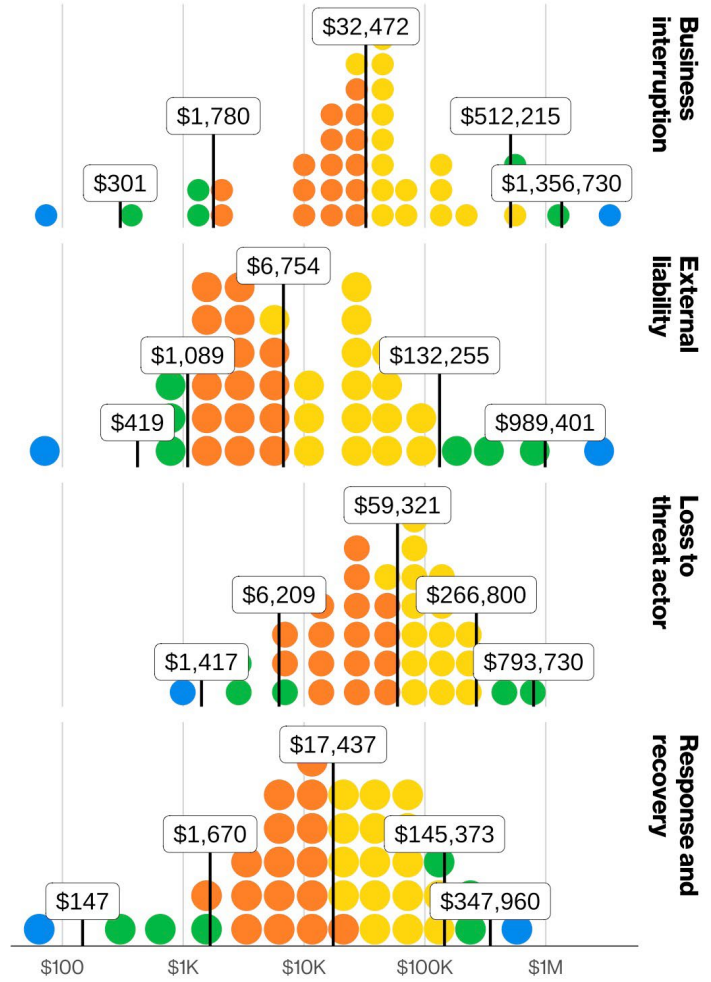

Figure 33. Distribution of known loss type amounts in Educational Services claims (total n=3,577)

Healthcare

(NAICS 62)

Liability in this industry displayed relatively high costs, with a median loss that is 57% higher than the overall median loss and accounts for 11% of their total claims.

Claim overview	8,643 claims with 5,100 recorded losses
Policy types	Primary (70%), Excess (26%), Endorsement (4%)
Percent of known total losses	Response and Recovery (29%), Business Interruption (24%), External Liability (23%)
Incident types	Ransomware (39%), BEC (22%), Supply Chain (1%)

Figure 34. Incident type quadrant chart in Healthcare claims (n=8,643)

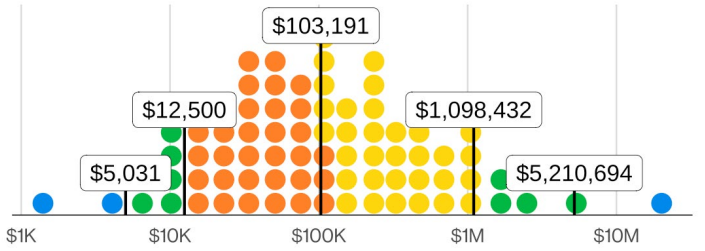

Figure 35. Distribution of economic impact in Healthcare claims (n=8,643–each dot is 216.08 claims)

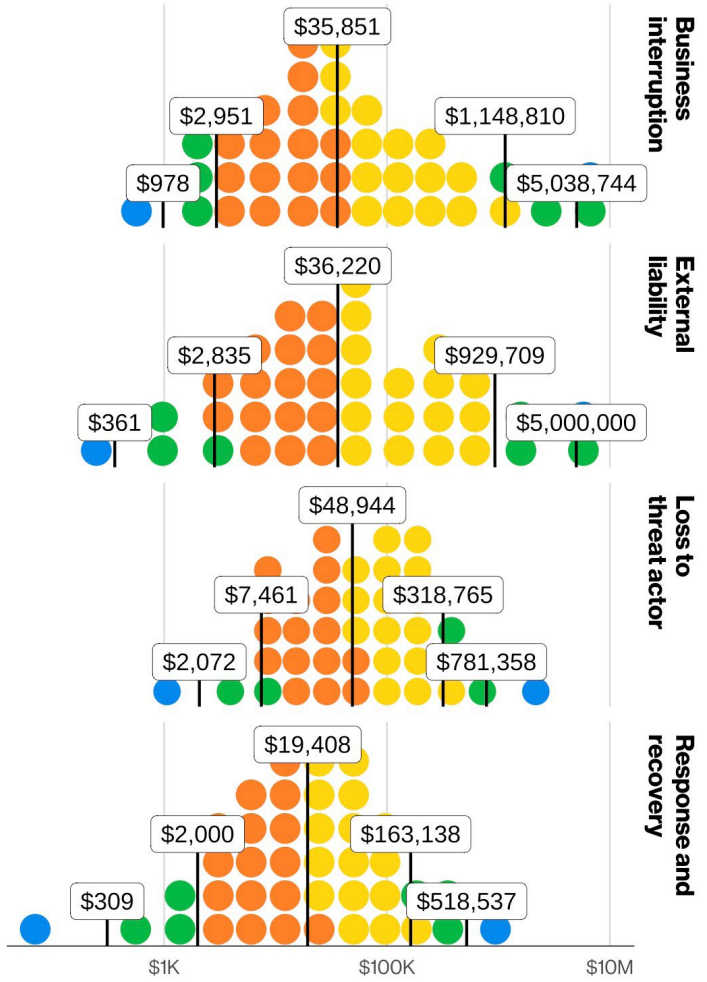

Figure 36. Distribution of known loss type amounts in Healthcare claims (total n=8,643)

Manufacturing

(NAICS 31–33)

Manufacturing is one of the top industries in terms of losses from Business Interruption, with its median loss ($232,000) being 158% more expensive than the overall dataset and accounting for 30% of all losses.

Claim overview	4,965 claims with 3,288 recorded losses
Policy types	Primary (77%), Excess (20%), Endorsement (3%)
Percent of known total losses	Business Interruption (31%), Threat Actor (25%), Response and Recovery (24%)
Incident types	Ransomware (45%), BEC (18%)

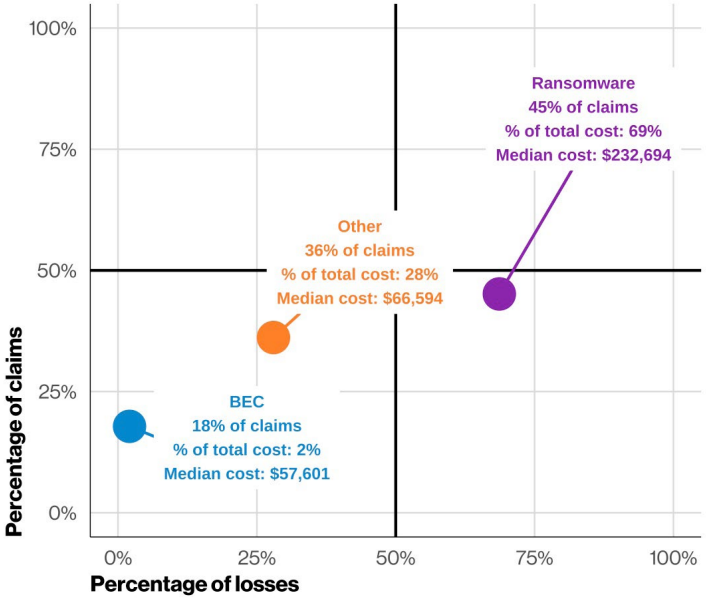

Figure 37. Incident type quadrant chart in Manufacturing claims (n=4,965)

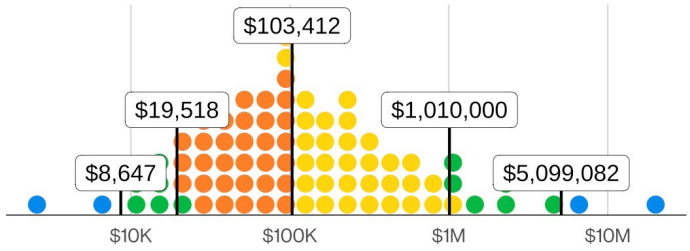

Figure 38. Distribution of economic impact in Manufacturing claims (n=4,965–each dot is 124.12 claims)

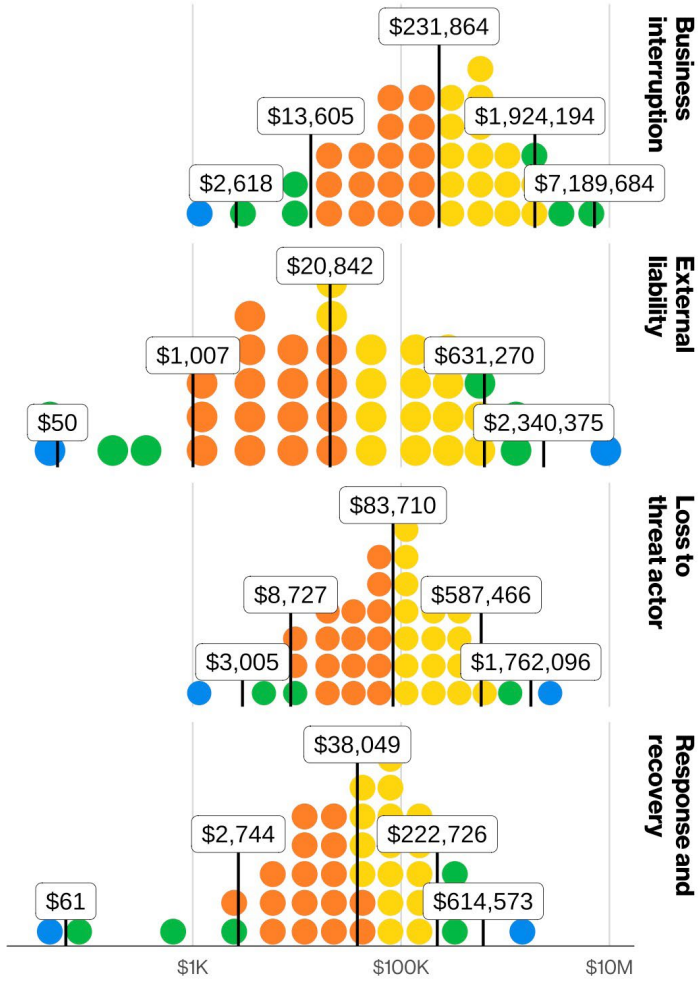

Figure 39. Distribution of known loss type amounts in Manufacturing claims (total n=4,965)

Public Administration

(NAICS 92)

Ransomware is one of the more costly and frequent issues impacting Public Administration, accounting for 64% of all claims and 79% of cost.

Claim overview	1,752 claims with 1,184 recorded losses
Policy types	Primary (96%), Excess (4%)
Percent of known total losses	Response and Recovery (51%), Threat Actor (27%), Business Interruption (16%)
Incident types	Ransomware (64%), BEC (6%), Supply Chain (1%)

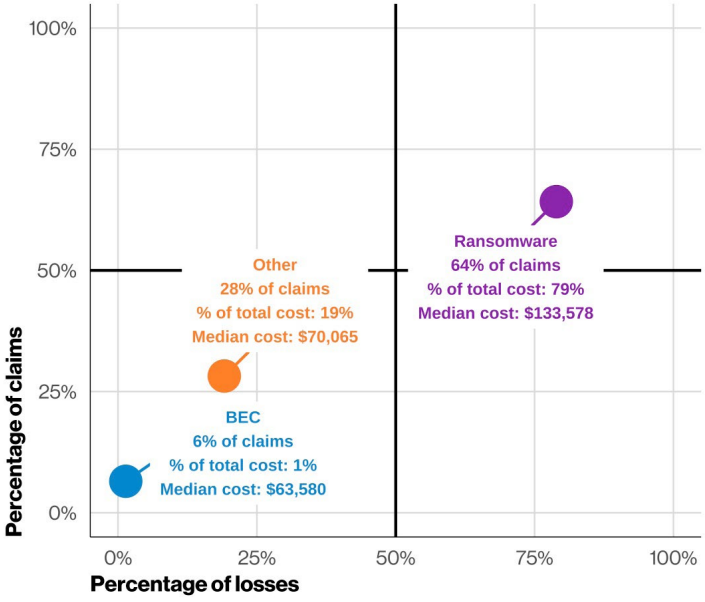

Figure 40. Incident type quadrant chart in Public Administration claims (n=1,752)

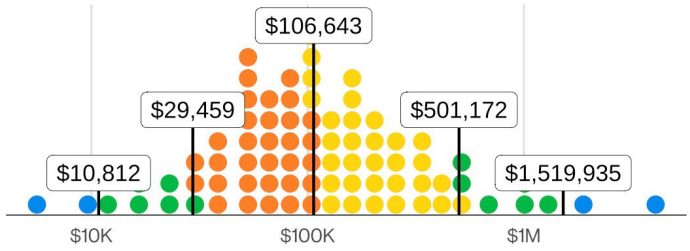

Figure 41. Distribution of economic impact in Public Administration claims (n=1,752–each dot is 43.80 claims)

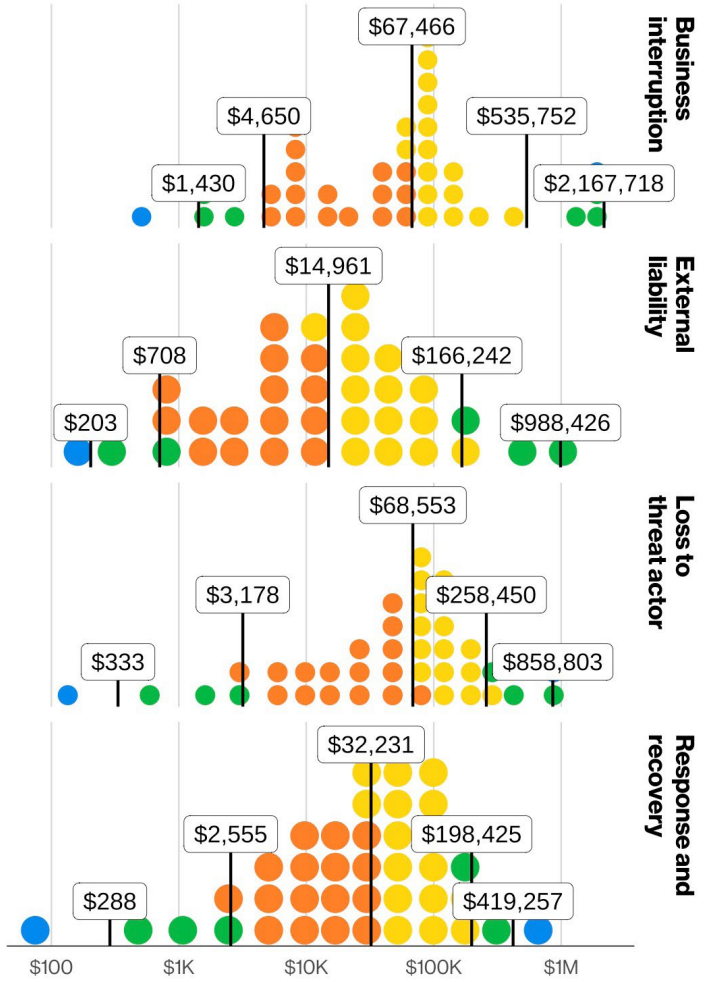

Figure 42. Distribution of known loss type amounts in Public Administration claims (total n=1,752)

Retail

(NAICS 44–45)

Business Interruption accounts for 25% of claims, and the median value is 65% higher than the overall dataset.

Claim overview	4,007 claims with 2,582 recorded losses
Policy types	Primary (78%), Excess (20%), Endorsement (2%)
Percent of known total losses	Business Interruption (44%), Threat Actor (28%), Response and Recovery (15%)
Incident types	Ransomware (32%), Third-Party (15%), BEC (13%)

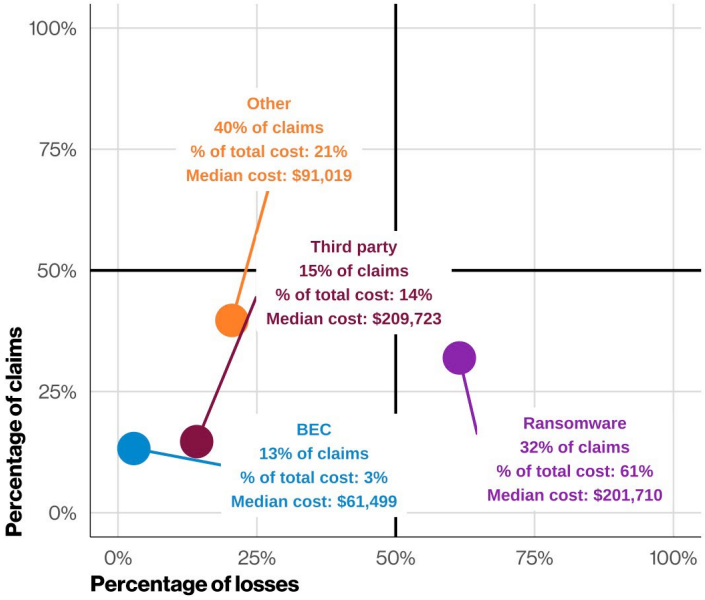

Figure 43. Incident type quadrant chart in Retail claims (n=4,007)

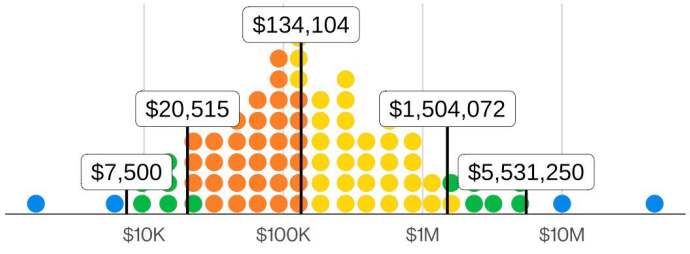

Figure 44. Distribution of economic impact in Retail claims (n=4,007–each dot is 100.18 claims)

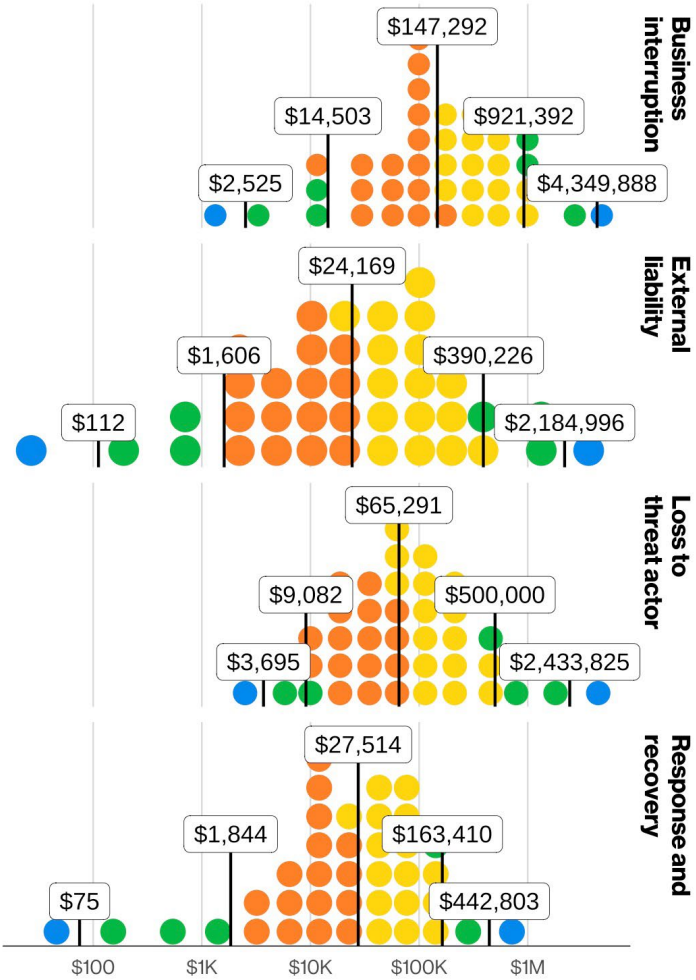

Figure 45. Distribution of known loss type amounts in Retail claims (total n=4,007)

Small- and medium-sized businesses

(revenue under $25 million)

SMBs face heightened cyber risk because losses are disproportionately damaging, accounting for up to 7% of their total revenue. This is particularly critical as these organizations typically have fewer resources to invest in robust cybersecurity.

Claim overview	15,431 claims with 11,996 recorded losses
Policy types	Primary (88.9%), Endorsement (9.7%), Excess (1.5%)
Percent of known total losses	Response and Recovery (40%), Threat Actor (29%), Unknown (13%)
Incident types	Ransomware (39%), BEC (19%), Supply Chain (1%)

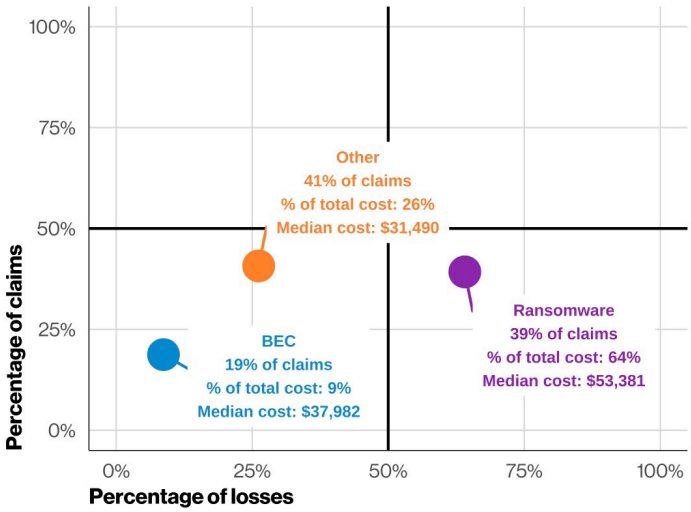

Figure 46. Incident type quadrant chart in SMBs (n=15,431)

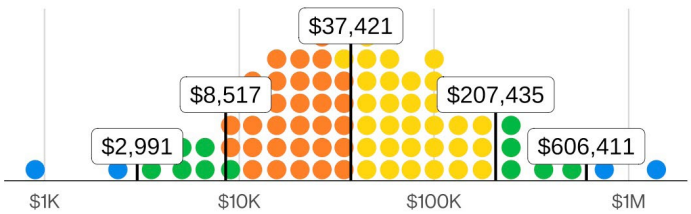

Figure 47. Distribution of economic impact in SMB claims (n=15,431–each dot is 192.89 claims)

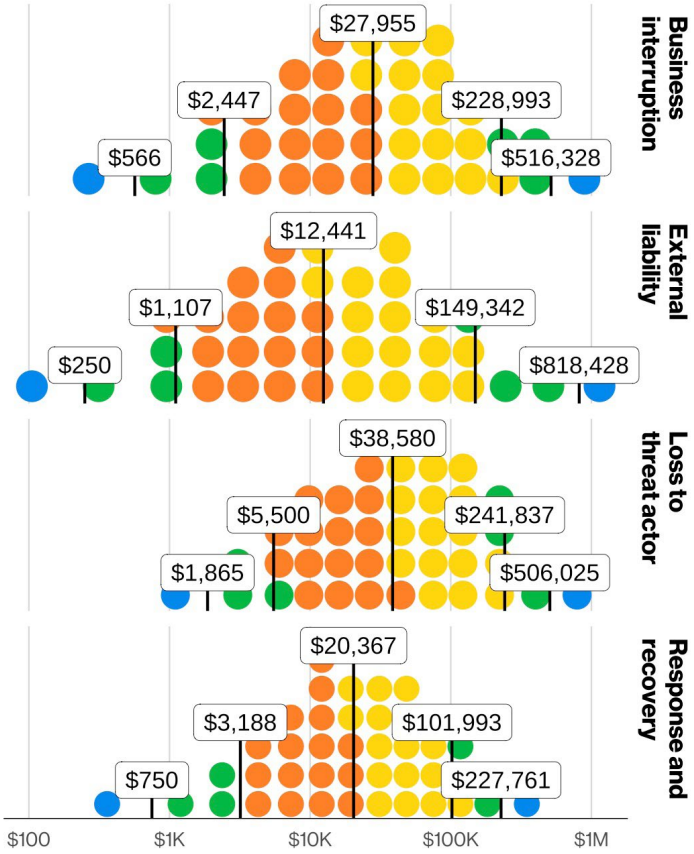

Figure 48. Distribution of known loss type amounts in SMB claims (total n=15,431)

Wrap-up

This concludes our first, but hopefully not last, Breach Impact Study. We would like to thank our data partner, CyberAcuView, for the collaboration and support in making this analysis possible.

Their data and perspective were instrumental in helping us explore the financial impact of cyber-related breaches across enterprises and industries.

We also want to thank you for taking the time to read this report. We trust that you have found it both helpful and informative as you consider how cyber events can translate into real financial consequences for organizations.

If this data tells us one thing, it is that cyber loss is not a binary event. The question is not whether to carry coverage; it is whether the coverage that organizations have reflects the actual distribution of outcomes an organization may face. The percentile data in this report, broken down by revenue bracket and industry, provides a basis for that conversation.

This data may be useful to organizations evaluating their coverage—not just against the median case but also against the top 10% and top 2.5% scenarios that this data shows are more common than many organizations may have assumed.

If this study was valuable to you, we would be glad to hear it. Please let us know if you would like to see more reports like this in the future. And if you are in a position to do so, consider becoming a contributor. The more data we can bring to bear on these questions, the better we can collectively understand cyber risk and its impact across the business community.

Appendix: A Path Forward for SMBs: Control Assist™

By Mark Camillo
CEO, CyberAcuView

The data in this study strongly suggests that SMBs face a disproportionate cyber risk burden – losses that can reach 7% of annual revenue in extreme cases, from an attack landscape dominated by ransomware (39% of SMB claims) and BEC (19%). For many of these organizations, the path to obtaining meaningful coverage can be difficult: With complex security questionnaires, the link between cybersecurity controls and insurance readiness is opaque, and it is hard to know which investments will actually reduce risk.

CyberAcuView and the Center for Internet Security (CIS) developed Control Assist specifically to address this gap. Launched in November 2025, Control Assist aligns the CIS Critical Security Controls® Implementation Group 1 (IG1) (56 foundational safeguards representing "essential cyber hygiene") with the underwriting questions that insurers commonly ask during the application and renewal process. The result is a shared framework that can translate an organization's security posture into language insurers understand, helping reduce confusion, accelerate coverage decisions and guide SMBs toward the specific controls that help defend against the threats most prevalent in this dataset.

Several technology partners have mapped their products to the Control Assist question set. For SMBs, this means that cybersecurity investments made to improve their security posture can potentially accelerate and strengthen their insurance applications. Insurers benefit from standardized, verifiable evidence of control implementation rather than inconsistent self-reported questionnaire responses. For more information on the free Control Assist resource, visit cisecurity.org/insights/white-papers/control-v8-1-control-assist.