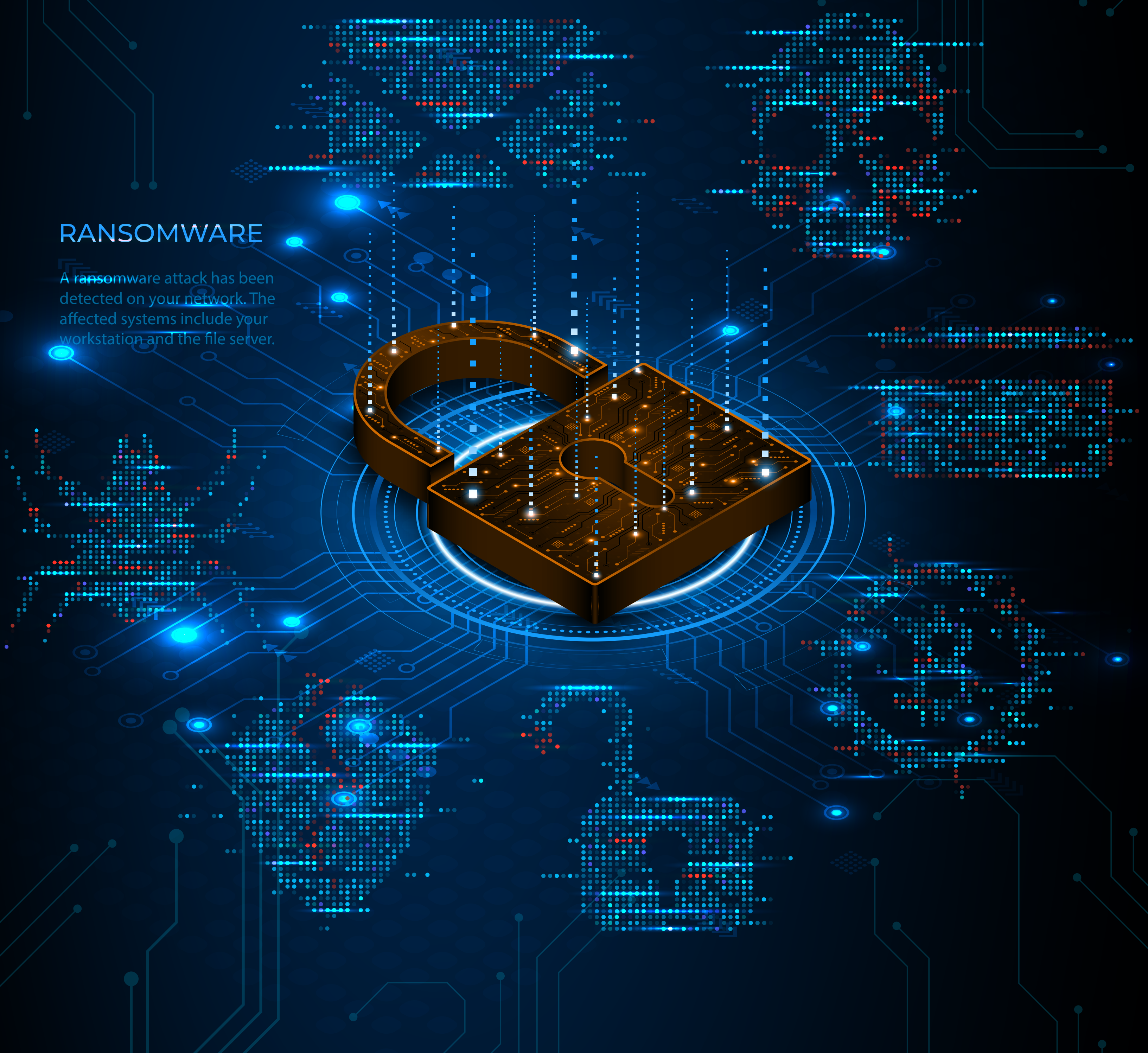
NetDiligence®

CYBER CLAIMS STUDY

2025 REPORT


RANSOMWARE
A ransomware attack has been detected on your network. The affected systems include your workstation and the file server.

CONSTANGY Brooks Smith & Prophete

experian

RSM

SUREFIRE CYBER

Contents

Introduction

Welcome to the fifteenth annual NetDiligence® Cyber Claims Study. This report is based on the summary statistical analysis of over 10,000 cyber claims for incidents that occurred during the five-year period 2020–2024. By comparison, the first Cyber Claims Study, published in 2010, analyzed fewer than 100 cyber insurance claims.

By the Numbers

- 10,402 claims analyzed, arising from incidents occurring 2020–2024
- 4,108 new and updated claims collected in 2025, from incidents occurring 2022–2024
- 1,691 claims analyzed arising from incidents occurring in 2024
- 98% of claims ($2.4B in total) from small to medium enterprises (SMEs) with less than $2 billion in annual revenue
- 2% of claims ($2.4B in total) from large companies with more than $2 billion in annual revenue
- 2,675 claims due to ransomware, 41% of which occurred between 2022 and 2024
- 1,864 claims due to business email compromise, 58% of which occurred between 2022 and 2024

With Appreciation

We want to sincerely thank the cyber insurers listed on page 50 for their support of this report and their dedication to industry education. Many of them have contributed to this research every year for the past 15 years. Without their support, this educational report would not be possible.

Suggestions

If you have ideas or requests for next year's study, please let us know. Send us your thoughts at cyberclaims@netdiligence.com.

Key Findings

- We see enormous variances in the magnitude of loss data. The smallest claims were less than $1,000; the largest were over $500M. The numbers of records exposed ranged from 1 to over 140M.
- There were dramatic differences between the numbers for SMEs and for large companies—multiples of 10x, 1000x, or more. The biggest large company in the dataset (over $290B in annual revenue) was approximately 29 million times larger than the smallest organization (less than $10K in annual revenue). The average large company ($12.5B in annual revenue) was more than 116 times larger than the average SME ($108M).
- Even though large companies represented only 2% of claims (N=239), these claims accounted for 51% of the total incident cost analyzed in the report ($2.4B/$4.8B).
- The dataset contains 8 claims >$100M, 55 claims $10M–$99M, and 432 claims $1M–$10M. Of the 8 claims >$100M, two occurred at organizations with <$700M in annual revenue.
- In SMEs, there were 395 claims ≥$1M (4%). In large companies, there were 100 claims ≥$1M (43%)
- Ransomware and business email compromise were the two leading causes of loss. At SMEs, they accounted for 50% of claims ≥$1K in the five-year period 2020–2024, and nearly 55% in 2024.
- Ransoms rose to new and unprecedented levels, with initial demands as high as $150M and ransoms paid as high as $75M. There were 50 ransoms paid ≥$10M.

In short, incidents were more costly than ever.

Company Size

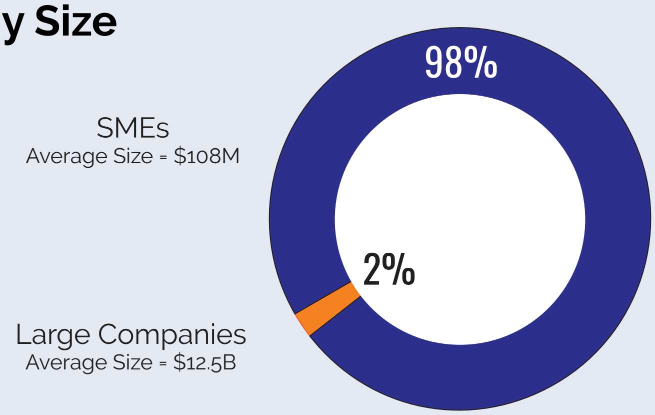


Figure 1

Average Costs for All Claims

SMEs

Large Companies

Crisis Services (N=115)
3.0M

Incident (N=235)
10.3M

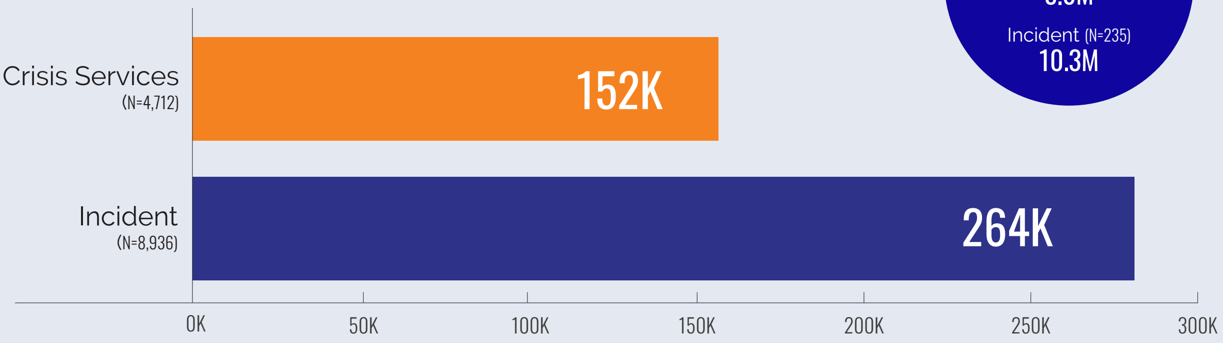


Figure 2

TERMS

Breach Coach

A qualified data security and privacy attorney who provides legal guidance for cyber incident response.

Incident Cost

Because the proportion of "recordless" events is so large, we replaced the term "breach" with "incident." The term *incident cost* in this report means the aggregate total of all types of costs/expenses associated with the incident.

Crisis Services Costs

Costs associated with responding to the breach event. These costs include, but are not limited to, breach coach counsel, forensics, notification, credit/ID monitoring, and public relations.

Legal Costs

Legal and regulatory expenses incurred due to the event. These costs include, but are not limited to, lawsuit defense, lawsuit settlement, regulatory action defense, and regulatory fines.

Self-Insured Retention (SIR)

The dollar amount that the insured organization had to pay before the insurer paid anything on the claim. In this study, the SIR is included in incident cost.

Small to Medium Enterprise (SME)

Categorized in this study as organizations with less than $2 billion in annual revenue.

Large Company

Categorized in this study as organizations with $2 billion or more in annual revenue.

All findings are for the five-year period 2020–2024 unless otherwise noted.
NetDiligence is a registered trademark of Network Standard Corporation, dba NetDiligence.

Average Costs for Business Interruption

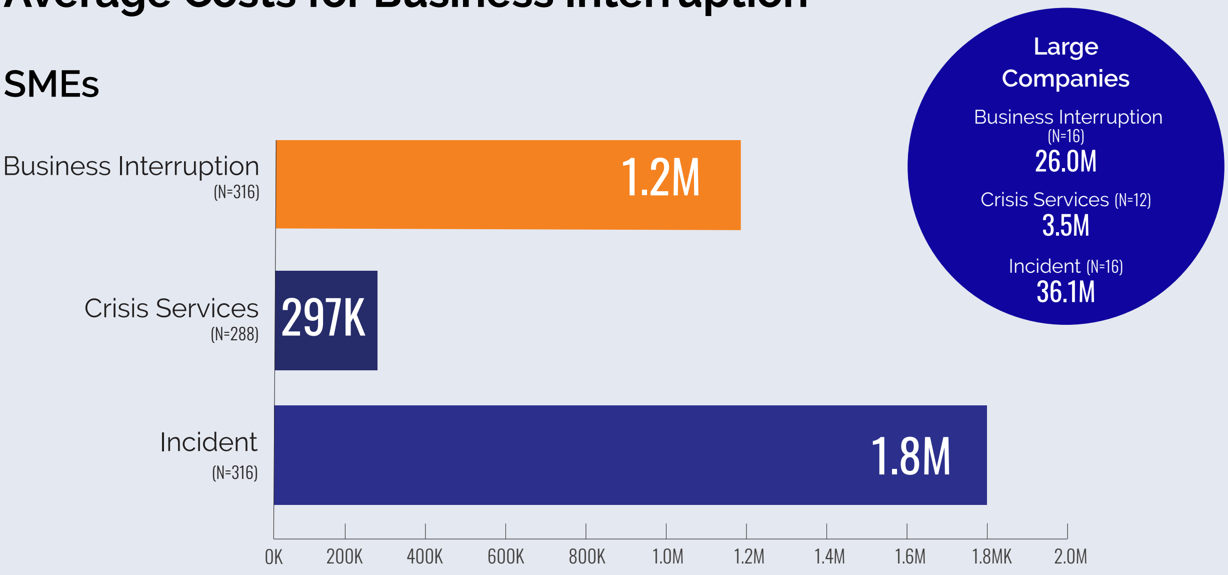


Figure 3

This year's data paints a complex picture of the evolving cyber threat landscape. Ransomware and BEC remain the top drivers of loss, with ransomware seeing significant increases in both threat actor monetary demands and (to a slightly lesser extent) in the actual payment amount.

We continue to see increases in business interruption and recovery costs—particularly among SMEs.

On the positive side, incident costs in healthcare appear to have stabilized, and manufacturing losses have remained at five-year lows. Anecdotally, we also learn from our Ransomware Advisory Board members that policyholders continue the trend of not wanting to pay the threat actor, with an estimate of only 15-20% opting to pay the extortion demand.

These findings reinforce the need for organizations of all sizes to not only invest in cyber defenses but also to maintain a clear, actionable response plan they can rely on when incidents occur.

Mark Greisiger, President & CEO, NetDiligence

Business Sector

Top 5 by Number of Claims—SMEs

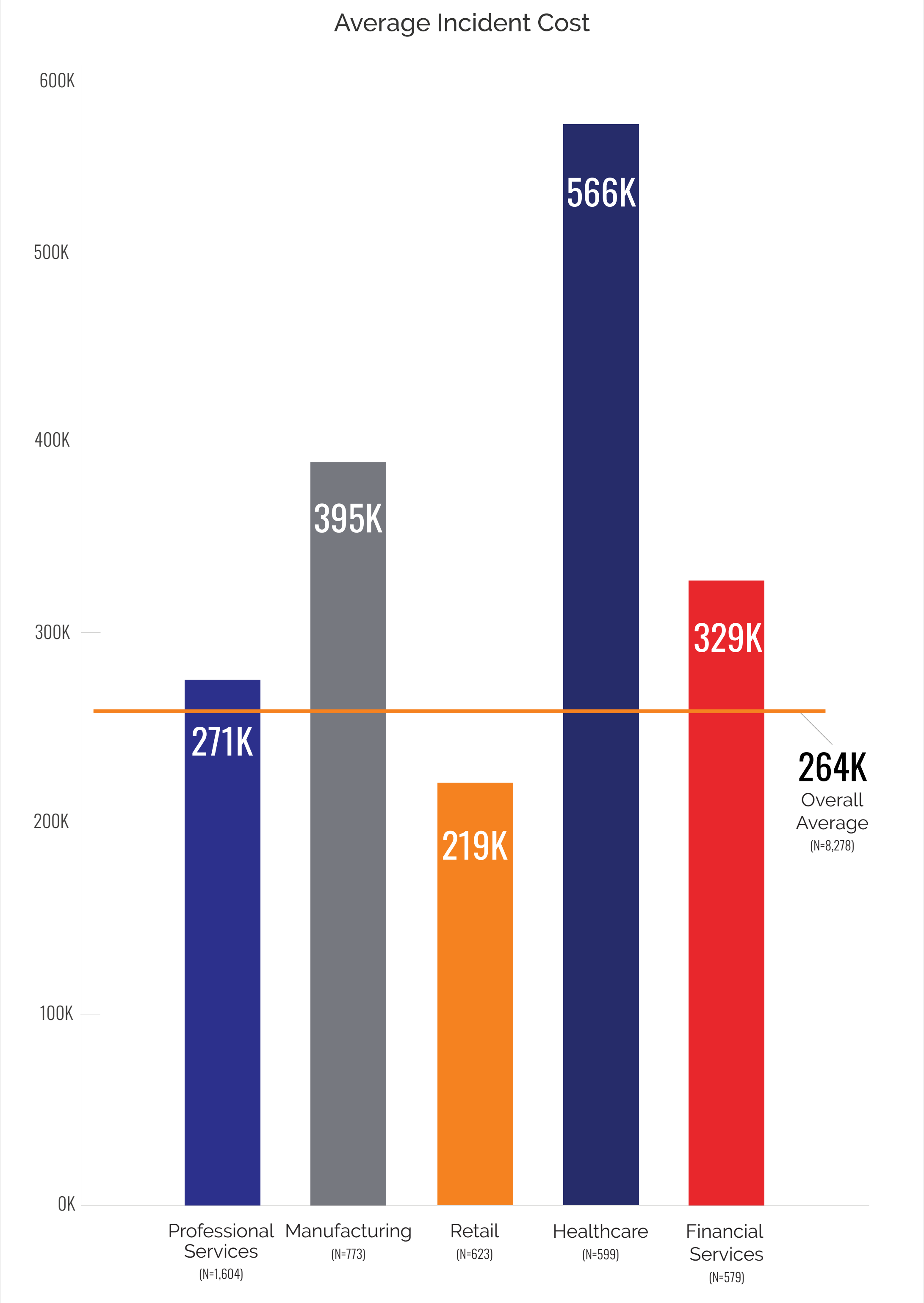


Figure 4

Cause of Loss

Top 5 by Number of Claims—SMEs

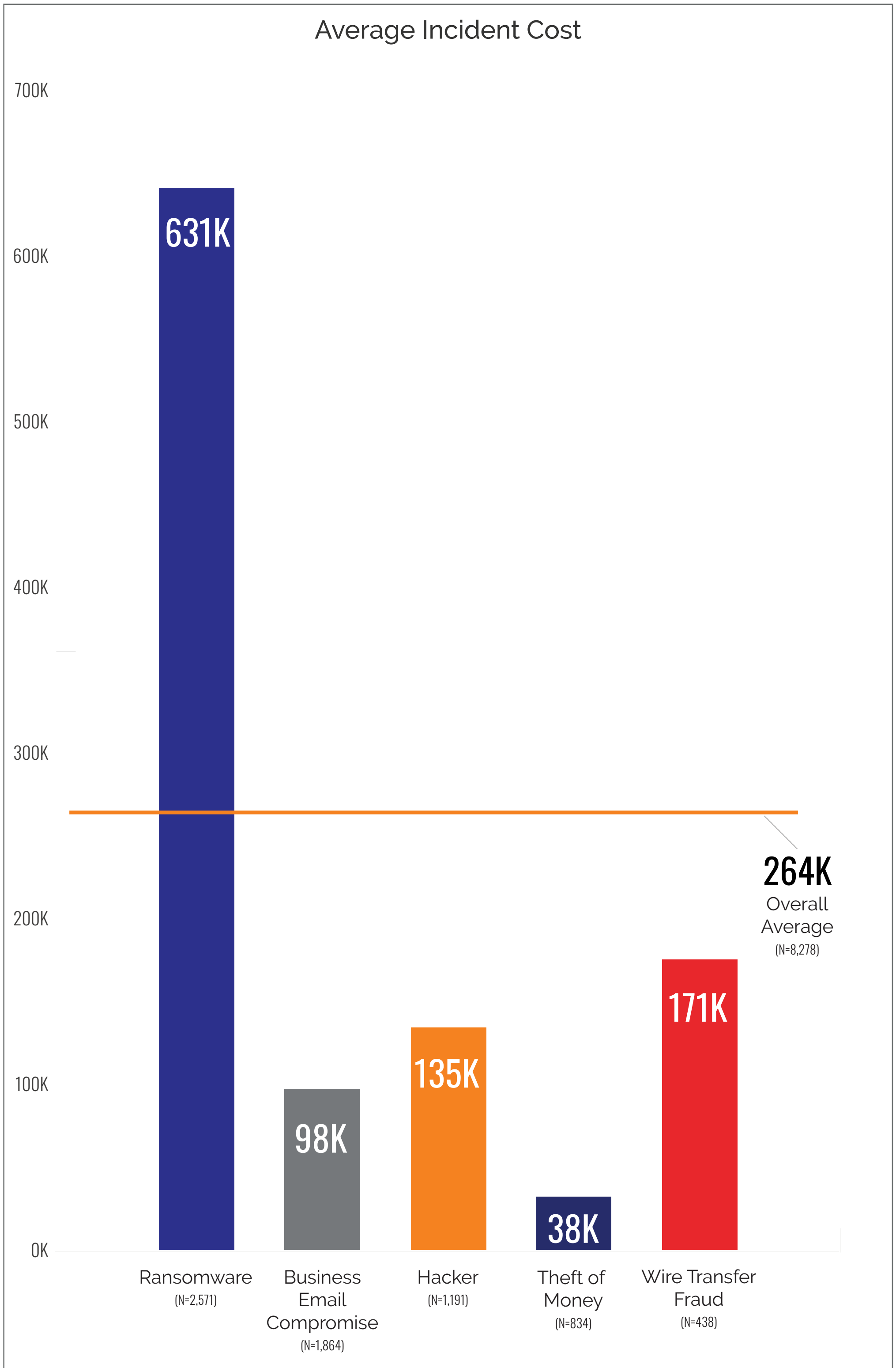


Figure 5

An Overview of the Data

The claims analyzed in this study come from organizations of all sizes, the smallest with less than $10K in annual revenue and the largest with over $290B. As the dataset is overwhelmingly weighted with claims from smaller companies, this may dilute the findings for large companies. Likewise, large companies can function as outliers, skewing the findings for small organizations. Therefore, the dataset has been divided into two categories based on the size of the insured entity. Organizations with less than $2B in annual revenue are defined as small to medium enterprises (SMEs), while those with $2B or greater in annual revenue are defined as large companies.

66% of study participants provided estimates of the annual revenue of the insured entities. Analysis of this data provides the following company demographics:

- SMEs: annual revenue ranged from less than $10K to $1.9B. The average was $108M. SMEs accounted for 98% of claims but only 49% of total incident cost.
- Large companies: annual revenue ranged from $2B to more than $290B. The average was $12.5B. Large companies accounted for only 2% of claims but 51% of total incident cost.

Proportion of Claims by Company Size
2020-2024
(N=10,402)

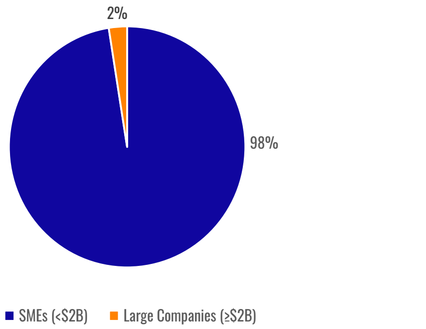


Figure 6

Proportion of Cost by Company Size
2020-2024
(Total Cost=$4.8B)

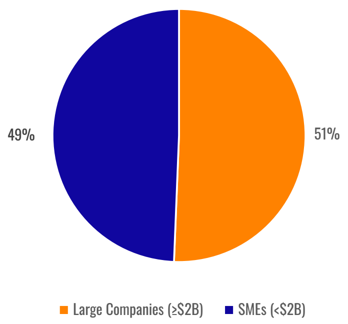


Figure 7

As artificial intelligence (AI) revolutionizes the ways in which we work and communicate, its integration into business operations has created new risks that are reshaping the cyber insurance landscape. Coupled with the persistent threat of third-party vulnerabilities, cyber insurers are facing unprecedented challenges in accurately assessing emerging risks. These challenges place cyber insurers in a unique position to effect critical change within information security frameworks by requiring more from insureds. By embracing a more agile approach to underwriting and requiring more programmatic "skin in the game" from insureds, cyber insurers can preserve or increase market share, protect or reduce loss ratios, and contribute to a more secure digital environment.

Sean B. Hoar, Partner & Chair, Constangy Cyber Team

Claims by Year of Event

The study includes 10,402 incidents occurring 2020-2024. The incident distribution by year is depicted in Figure 8.

Demographic analyses are based on all 10,402 claims while cost analyses are based upon the 9,171 claims that reported incident cost ≥$1,000.

The claims analyzed in this report come from incidents at organizations in 7 revenue groupings and 18 business sectors, across 25 causes of loss and 13 types of data.

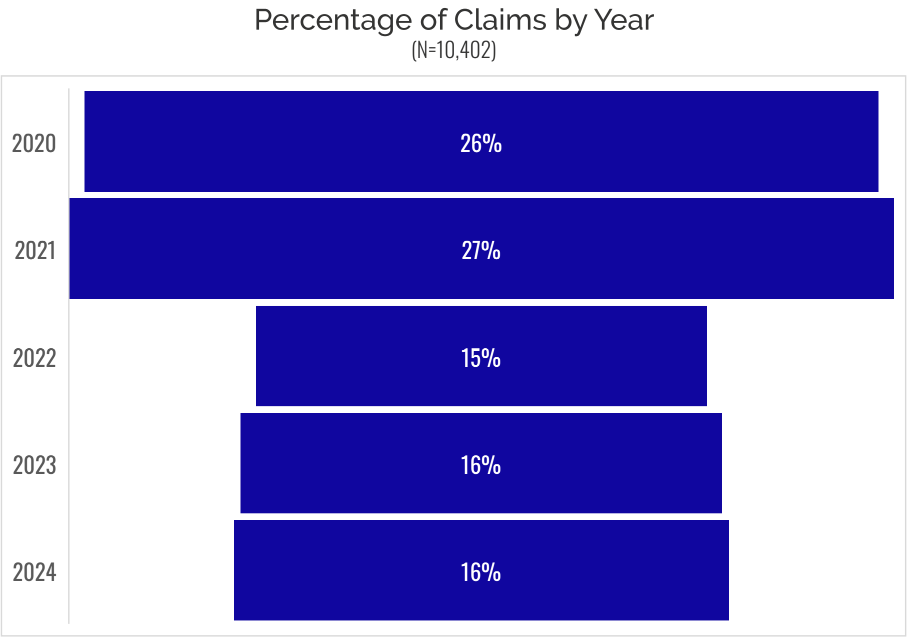


Figure 8

Incident Cost and Payout

Study participants were asked to provide information about the amount of money paid on a claim and to give an estimate of the total cost of the incident, including self-insured retention (SIR) and other costs that may have been excluded due to the terms of the policy.

There were 395 SME claims over $1M, and another 341 claims $500K–$1M. The largest SME claims occurred in 2022 (>$100M). These incidents happened in the manufacturing and healthcare sectors. Both involved ransomware with very large ransoms and extremely large business interruption losses (>$90M). Neither company was extremely large—annual revenue for each was <$700M.

The largest incident at a large company occurred in 2021 (>$500M). Between 2020 and 2024, there were 11 claims at large companies with over $50M in total incident cost, and another 29 claims with $10M-$50M in total incident cost.

Payouts for all organization sizes covered 32% of the total incident cost. For SMEs, the five-year payout was 69% of the total incident cost. At large companies, this number was 27%.

For SMEs, these proportions have dropped from last year's report (69% vs 81%). For large companies, they remain steady (27% vs 24%).

Figures 9 and 10 provide year-by-year averages of payout versus total cost, plus the five-year averages of payout amount and total incident cost for both SMEs and large companies.

The five-year numbers for SMEs are significantly higher than reported last year. Average total incident cost rose from $205 to $264K while average payouts increased from $167 to $183K.

At large companies, the changes were less dramatic. Average total incident cost and payouts for 2020-2024 were $10.3M and $2.7M, compared to $12.7M and $3.1M for the period 2019-2023.

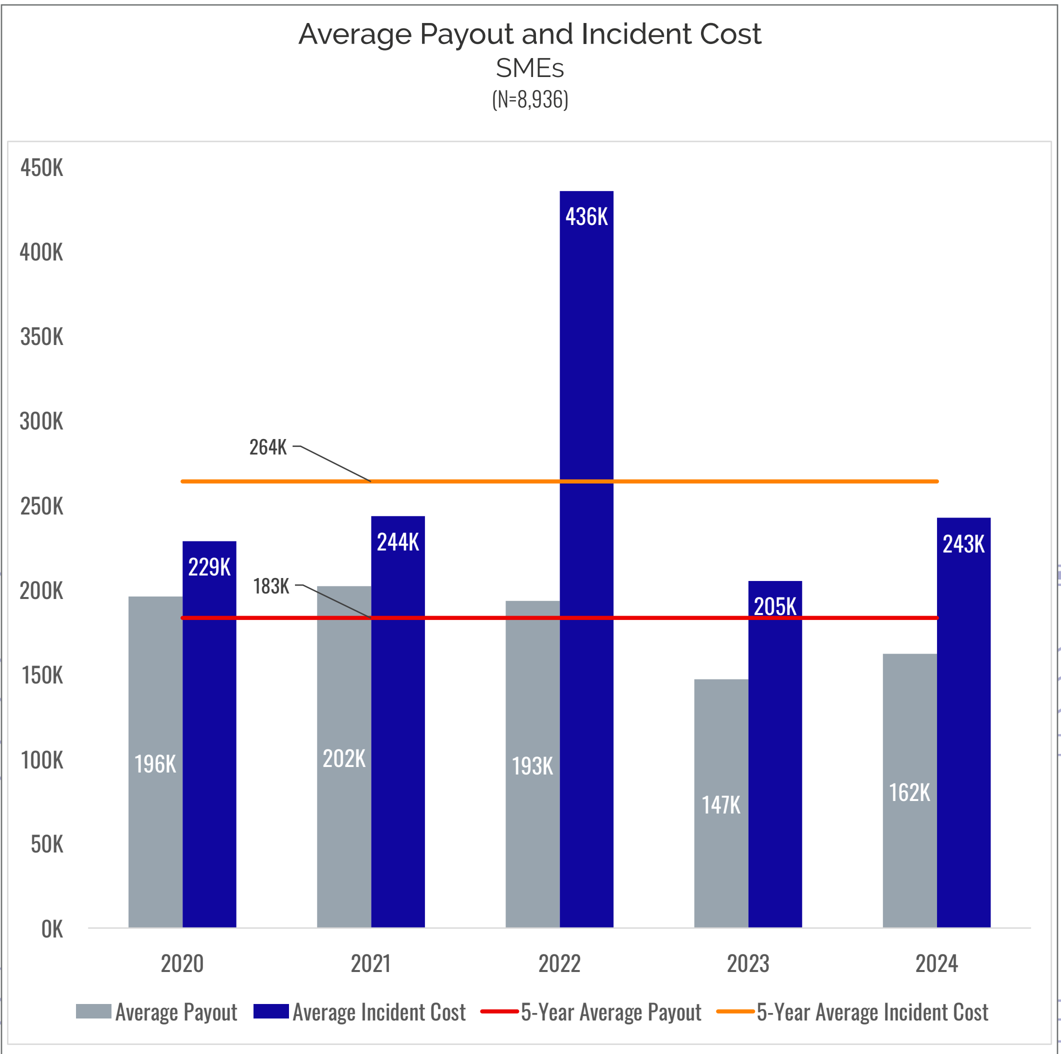


Figure 9

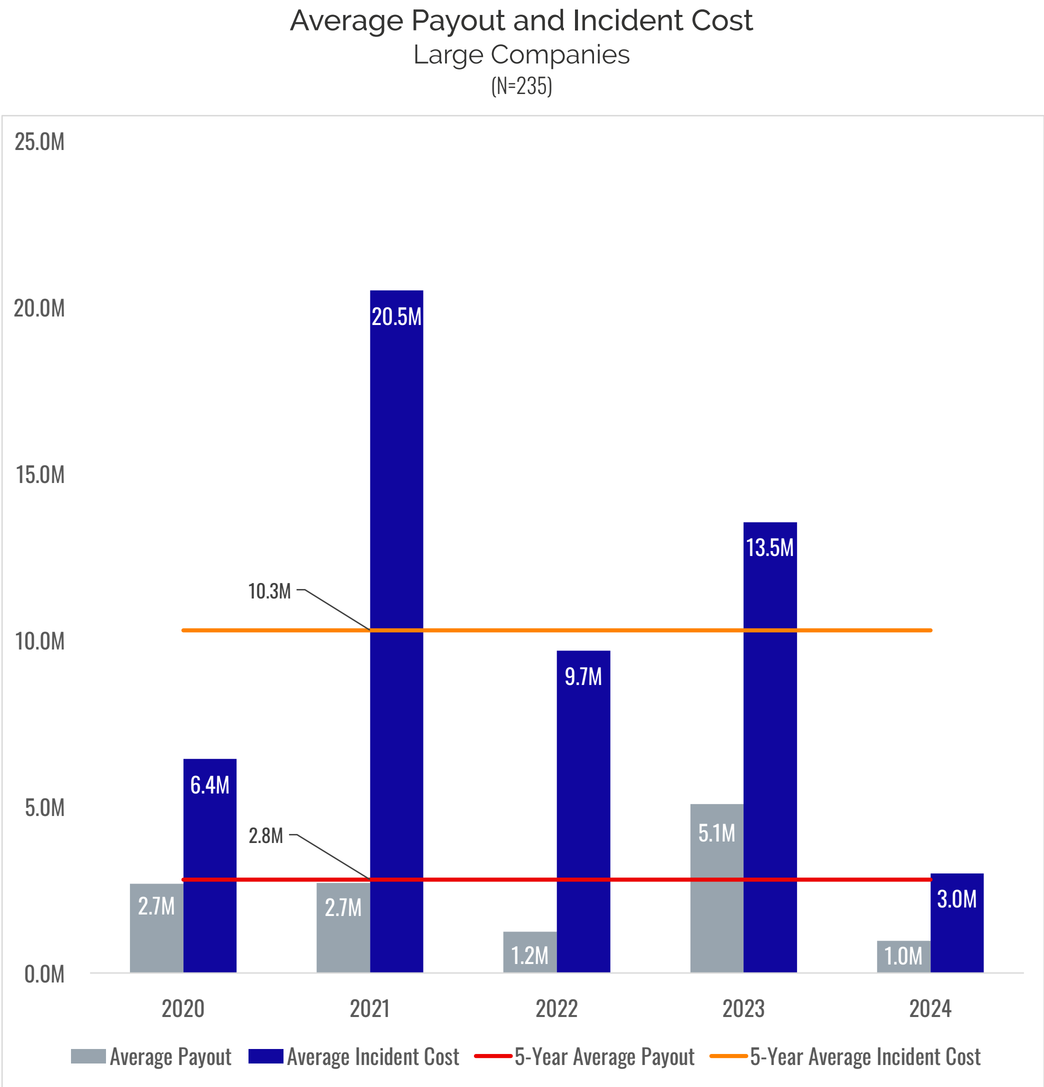


Figure 10

You're never going to keep threat actors out forever. It's about limiting your exposure. When they get in, if they can only impact a single user's PC, a single server or a single application, it's a lot easier and cheaper to recover than it is to recover all PCs, all servers, and all applications.

George Kohlhofer, Principal,
Cybersecurity and Privacy Risk, RSM US LLP

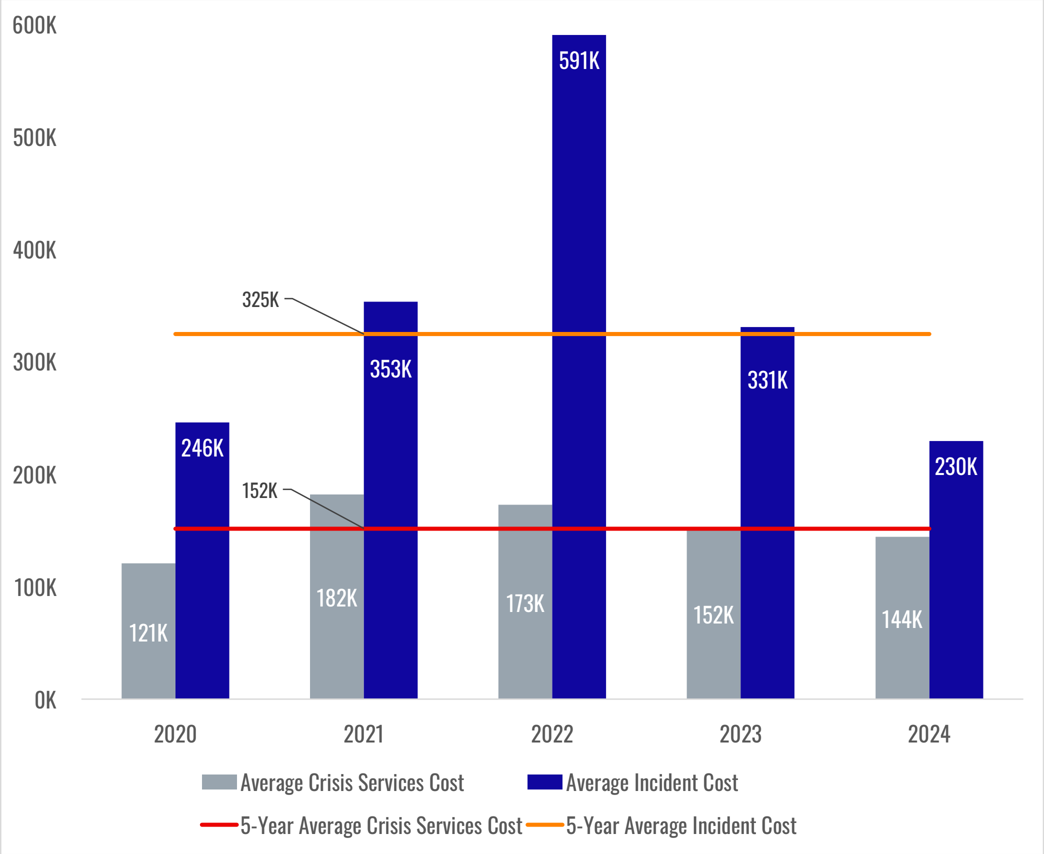
Incident and Crisis Services Costs

For all organizations, crisis services costs ranged from less than $100 to almost $26M. Incident costs for these claims, inclusive of SIR, ranged from less than $1,000 to over $160M. The averages were influenced by some very expensive claims. Not every claim involves a crisis services element, causing the number of claims or the "N" values on the graphs to vary.

SMEs

At SMEs, average crisis services costs ranged from $121K in 2020 to $144K in 2024, as shown in Figure 11.

Figure 12 depicts the percent of total cost expended on crisis services—47% for the five-year interval 2020–2024. Notably, this represents a dramatic increase since our last report, 40% higher than the 2019-2023 average.



Average Crisis Services and Incident Costs
Where Crisis Services Costs >0
SMEs
(N=4,712)

Figure 11

Crisis Services as a Percentage of Incident Cost
Where Crisis Services Costs >0
SMEs
(N=4,712)

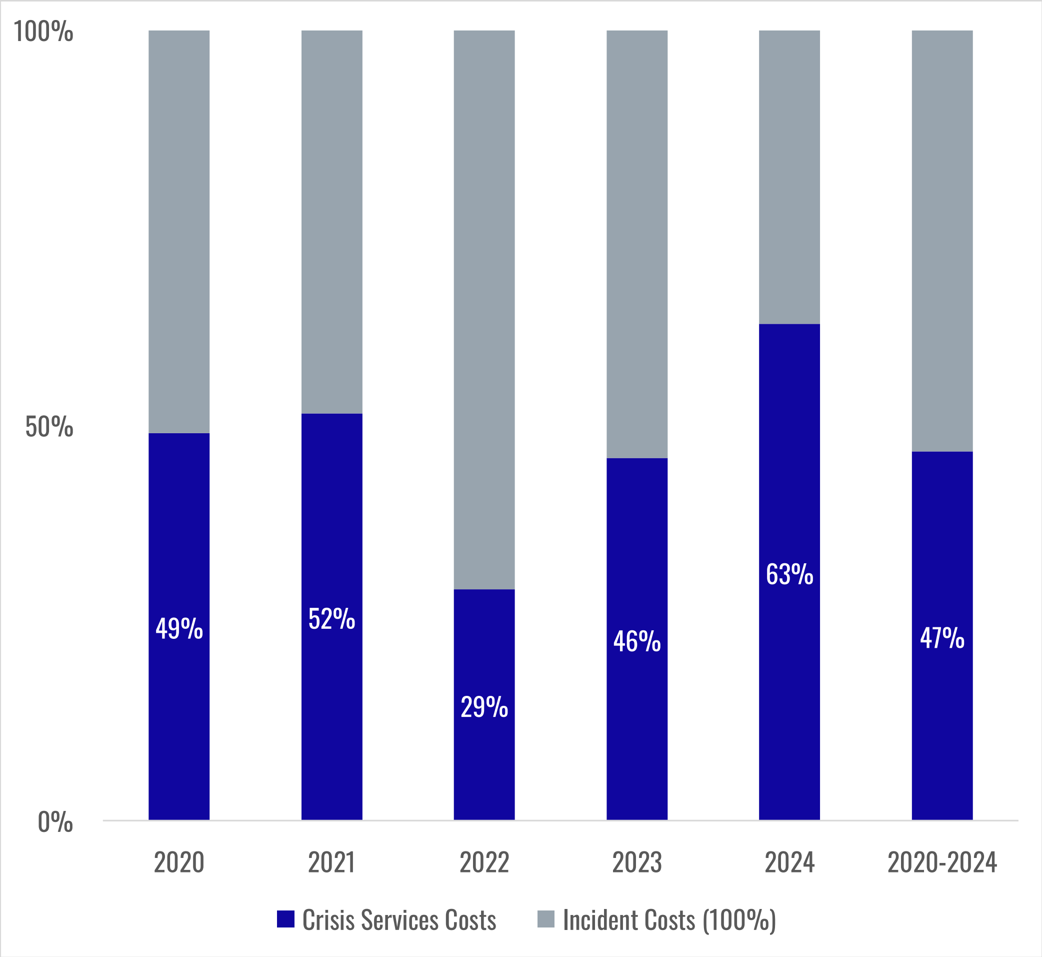


Figure 12

Figures 13 and 14 depict average crisis services costs by individual component, as well as the percentage of total crisis services cost that each component represents. During the five-year period, forensics accounted for 21% of the total, and legal guidance accounted for another 9% of the total. These proportions are similar to those reported last year.

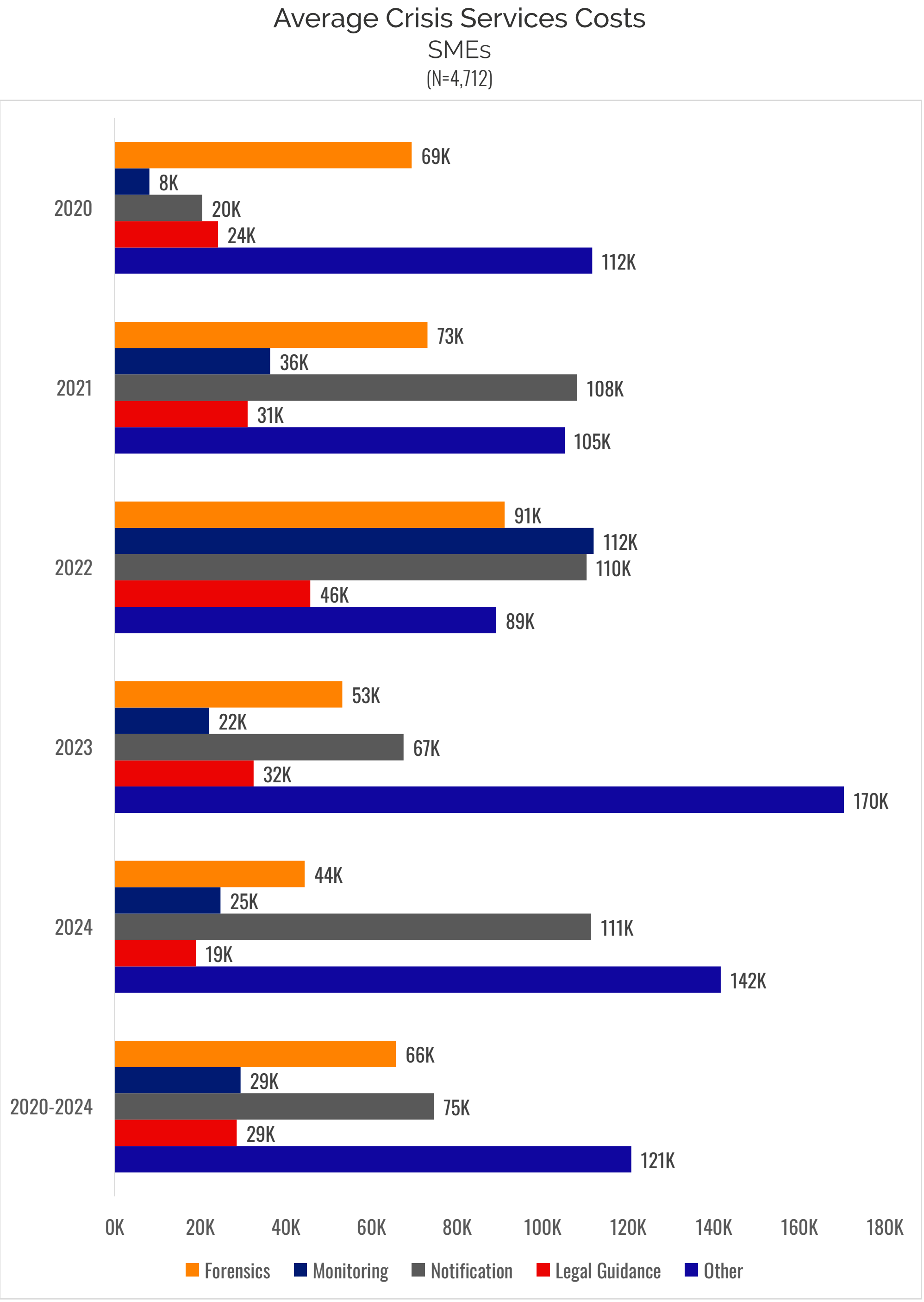


Figure 13

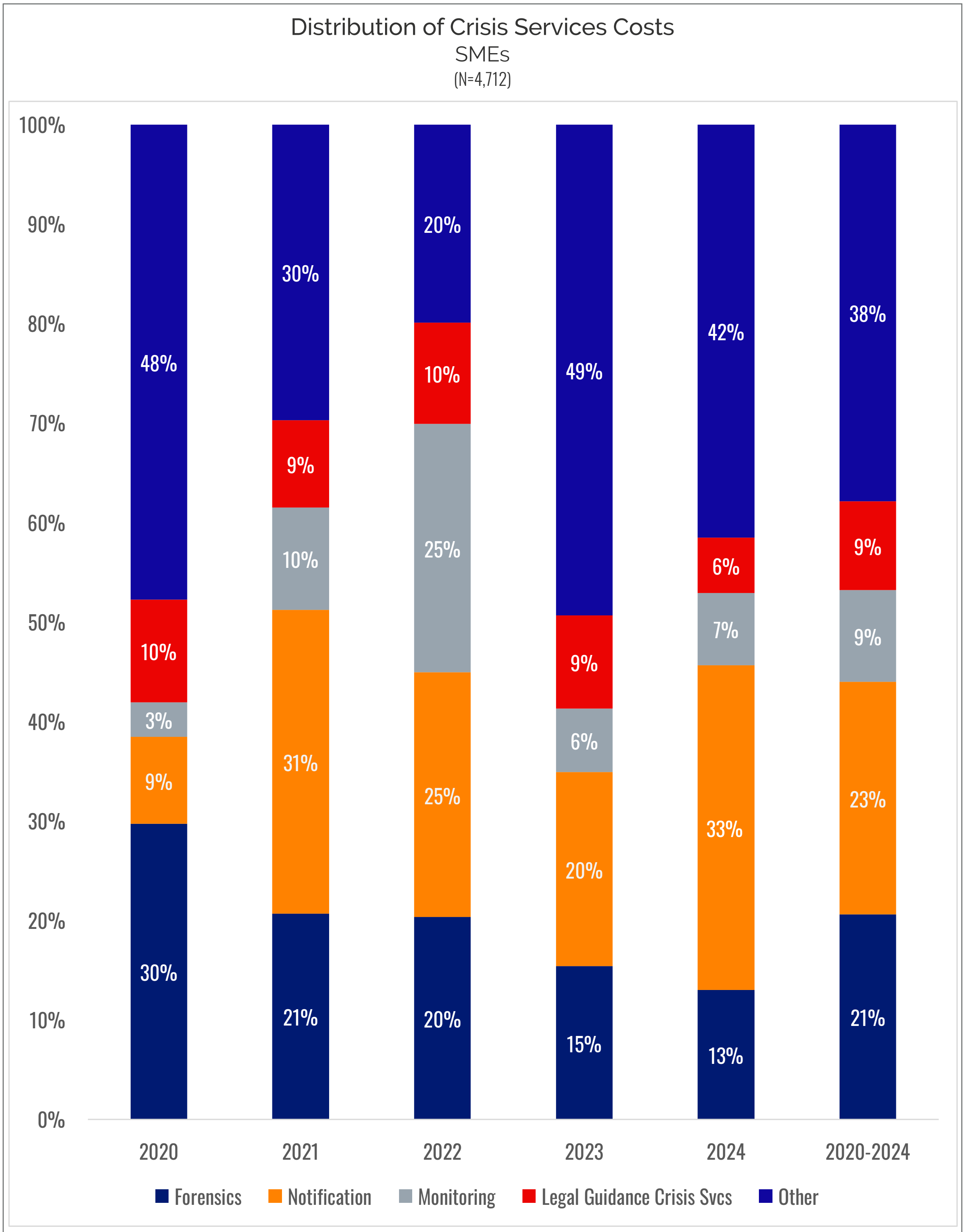

Distribution of Crisis Services Costs
SMEs
(N=4,712)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2020
2021
2022
2023
2024
2020-2024
48%
10%
3%
9%
30%
30%
9%
10%
31%
21%
20%
10%
25%
25%
20%
49%
9%
6%
20%
15%
42%
6%
7%
33%
13%
38%
9%
9%
23%
21%
Forensics
Notification
Monitoring
Legal Guidance Crisis Svcs
Other

Figure 14

Large Companies:

Figure 15 illustrates considerable variability in both the average crisis services cost and the incident cost at large companies. Here, average incident cost ranged from $4.7M to $22.5M. Outlier events in 2021 and 2023 contributed to spikes in averages for those years.

Figure 16 shows crisis service cost as a percent of total cost. Over the five-year period, this percentage ranged from 20% to 75%, with an average of 25%. The previous five-year period showed a similar average (28% from 2019-2023).

Figure 17 breaks down crisis services costs into a variety of service components and shows much variability.

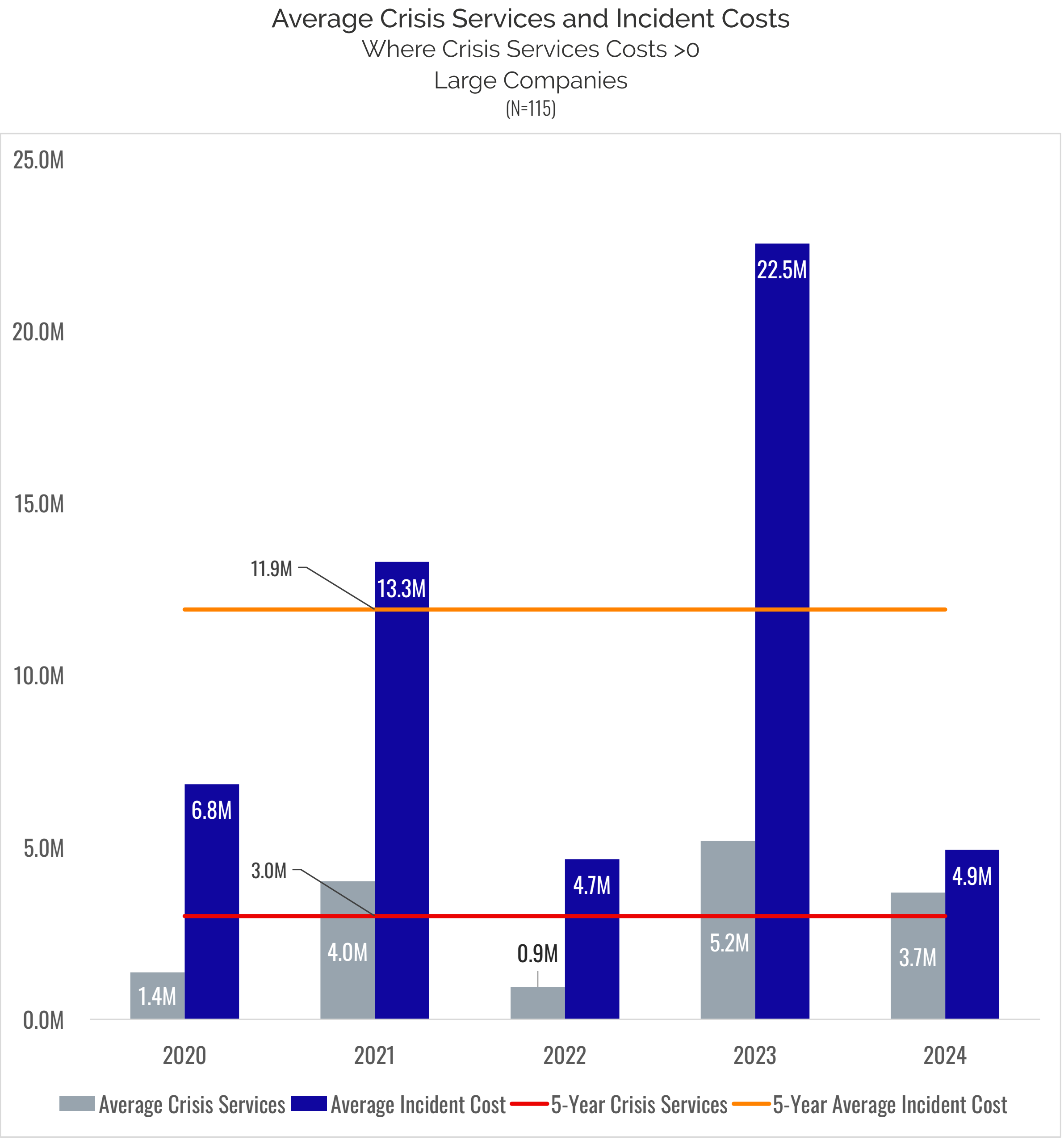


Figure 15

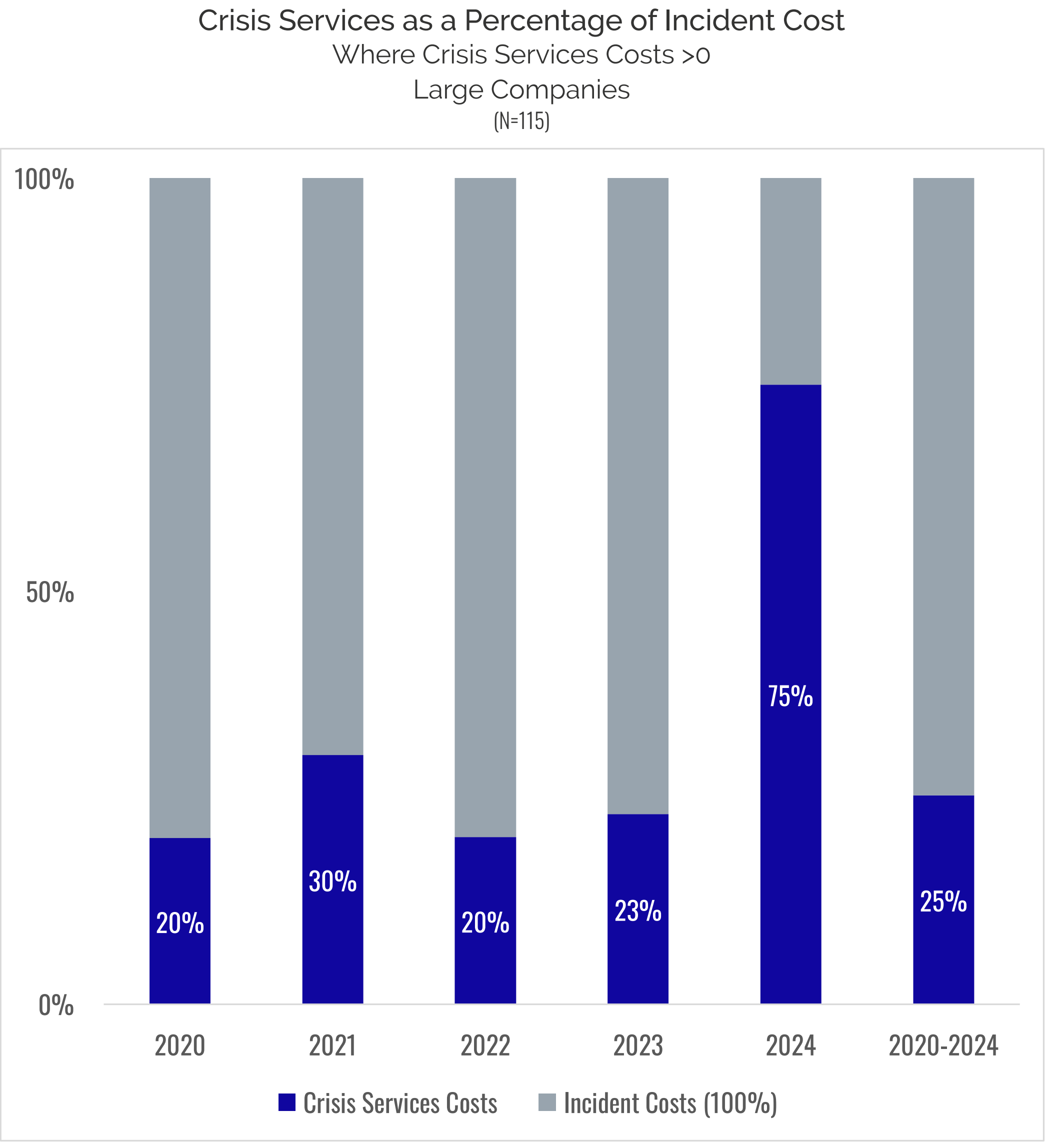


Figure 16

Experian saw a shift in breach dynamics last year: fewer events overall, but enterprise organization breaches were 22% larger and impacted more individuals. This contributed to higher overall crisis services costs, as organizations needed to notify more individuals and scale response efforts accordingly. Services like notifications, call center support, and identity protection continue to represent a significant portion of total incident costs and play a key role in managing stakeholder expectations.

Michael Bruemmer, Head of Global Data Breach Resolution & VP of Consumer Protection, Experian

Distribution of Crisis Services Costs
Where Crisis Services Costs >0
Large Companies
(N=115)

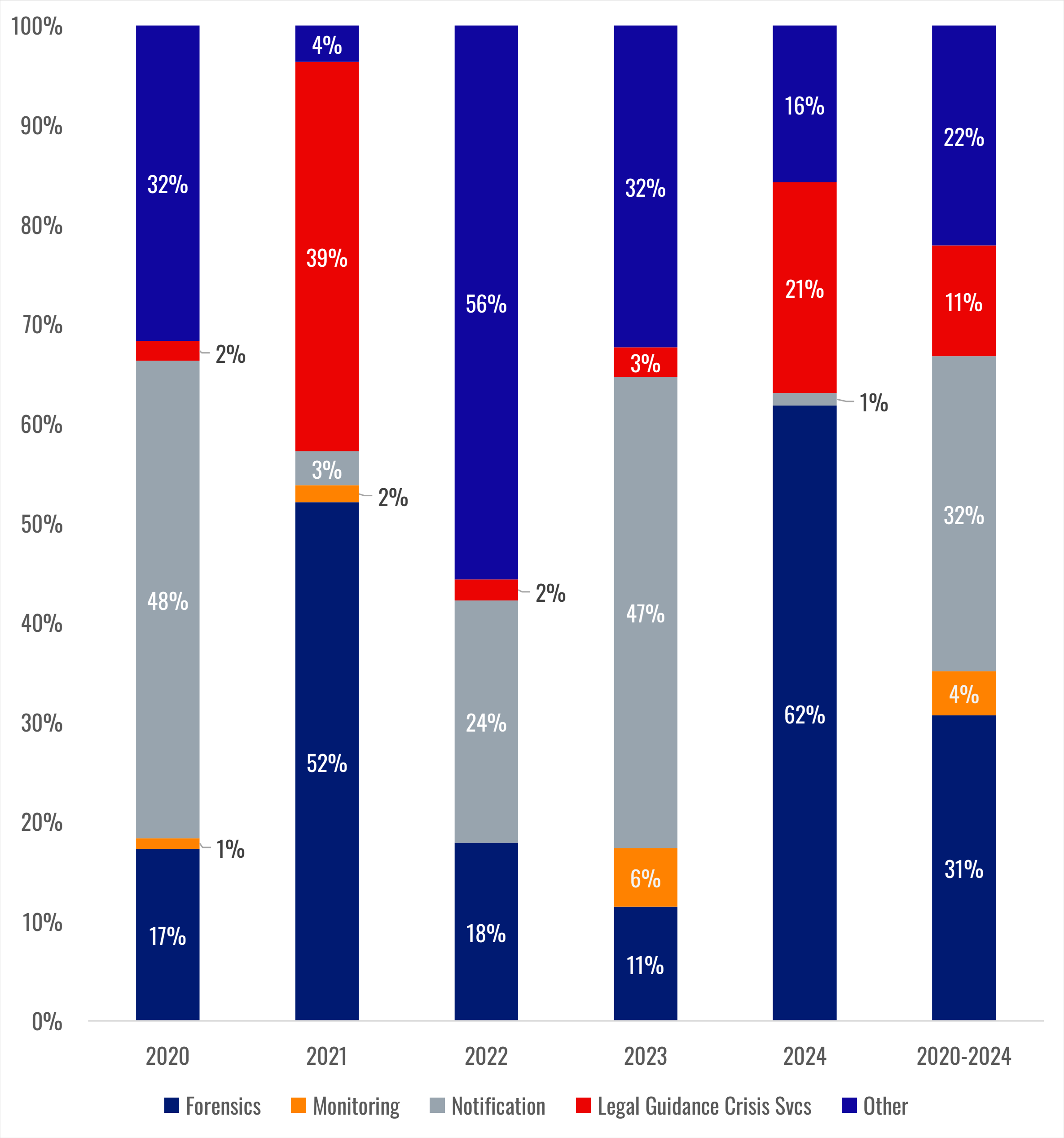


Figure 17

Business Interruption (BI)

SMEs

BI costs were reported for 316 incidents. Since 2020, the average BI cost and corresponding average incident cost have remained high. The increase in 2022 was caused by two very large outlier incidents, each in excess of $100M.

Additional analysis shows that the five-year average incident cost of a claim with BI was over 650% greater than a claim without BI. In 2024, the average claim involving BI was 250% greater than one that did not.

Further, ransomware incidents at SMEs accounted for 81% of claims with a BI component. The five-year average BI cost for ransomware incidents was $1.4M with a total incident cost of $2.1M. In 2024, these numbers were $751K and $1.1M, respectively.

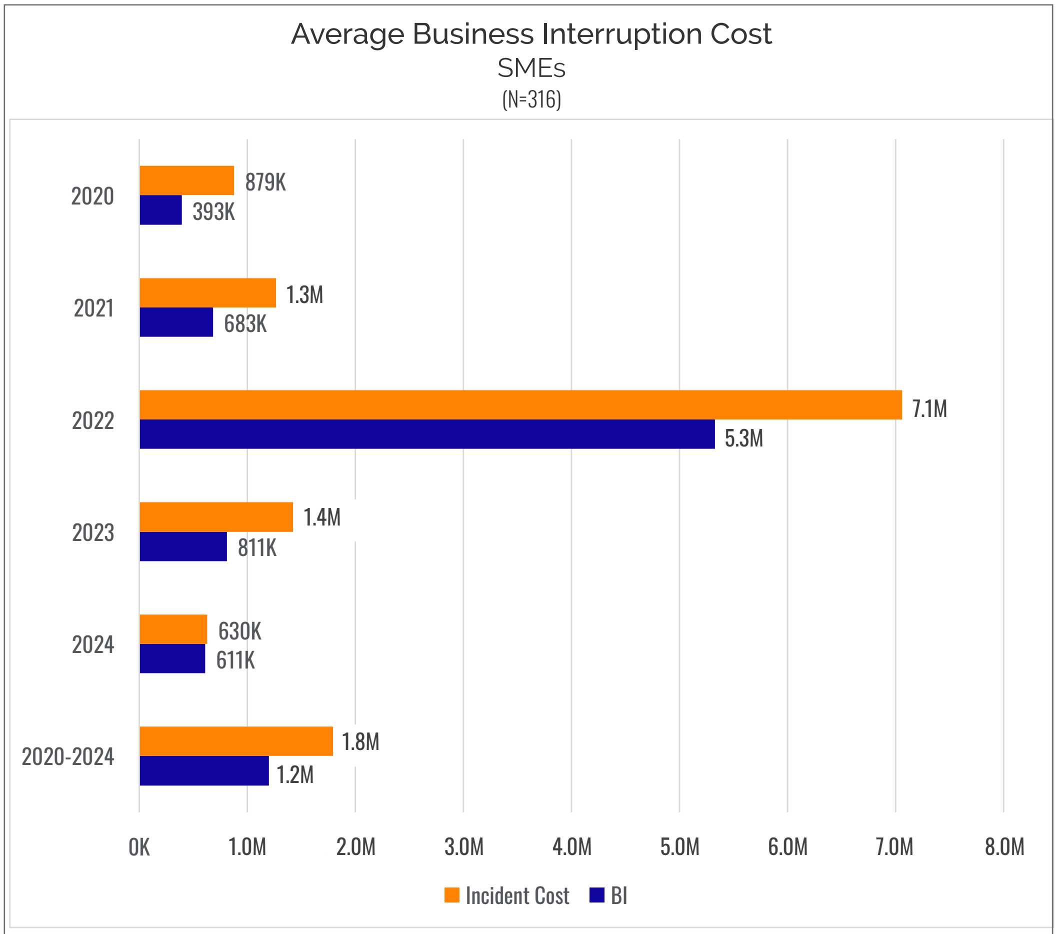


Figure 18

Large Companies

Figure 19 depicts average BI and total incident cost at large companies. Though the number of claims is small and there is much variability, the numbers are substantial. No BI claims at large companies were collected for 2024.

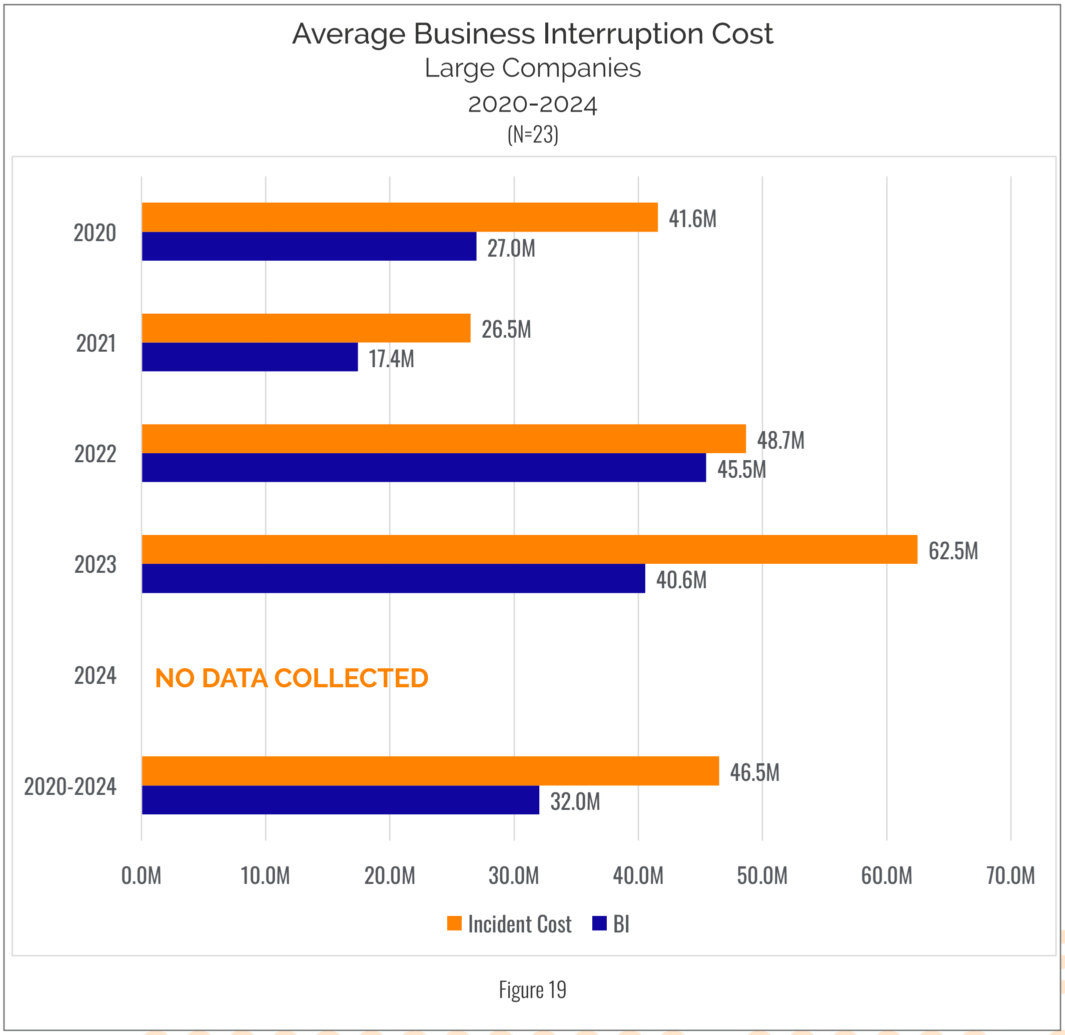


Figure 19

Companies need security hygiene and good control of their identities, multifactor authentication, and reduction of privileged identities. Those things alone will help shrink the attack surface. But there's always a chance they're going to get in. So now, what's your resiliency plan? Do you have one? Have you tested it? Do you have the vendors in place to help you recover?

Alden Hutchison, Principal
Cybersecurity and Privacy Risk, RSM US LLP

Recovery Expense

SMEs

274 claims reported recovery expense. As Figure 20 shows, both recovery expense and total incident cost have been steadily increasing since 2020. The average five-year incident cost of these claims is over 300% higher than incidents without recovery expense.

Ransomware incidents accounted for 78% of the claims with reported recovery expense. The five-year average incident cost of these events was $961K, 400% higher than incidents without recovery expense. In 2024, these incidents cost almost 130% more.

Large Companies

Eleven large company claims reported recovery expense spanning 2020-2024. Recovery expense for these incidents ranged from $20K to $4.5M (average=$822K). The corresponding incident cost ranged from $25K to $28.0M (average $10.2M). Nine of these claims were due to ransomware, with ransoms averaging $7.2M paid in six incidences. The corresponding average incident cost for these six claims was $11.7M.

So far, we have collected no claims with recovery expense in 2024. That may change next year as we collect additional data for 2024.

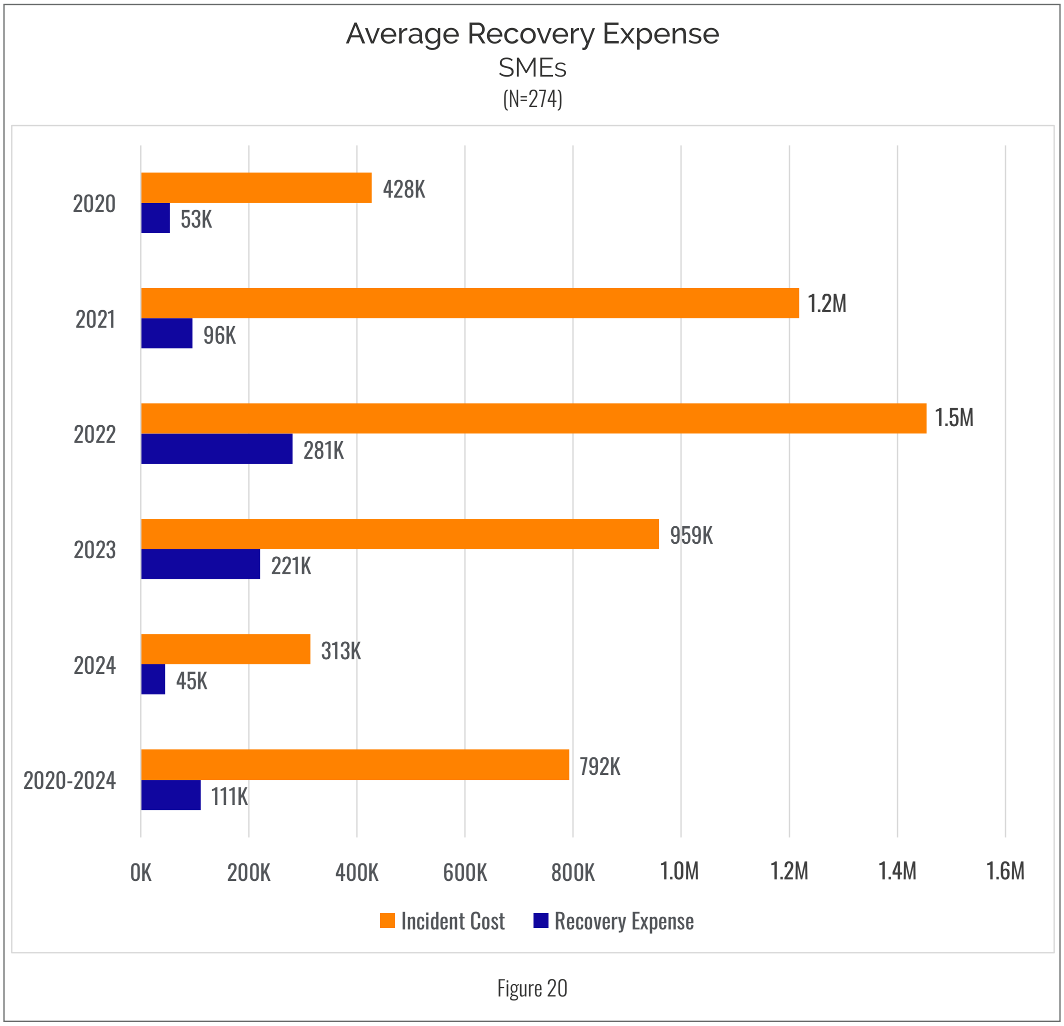


Figure 20

Legal Costs

SMEs

There were 203 claims in the dataset that reported legal or litigation expense from one or more of these categories: legal settlement, legal defense, regulatory fines, and regulatory action. Figure 21 depicts the year-by averages for these four categories as well as their five-year averages. There was much year-by-year variability in these costs.

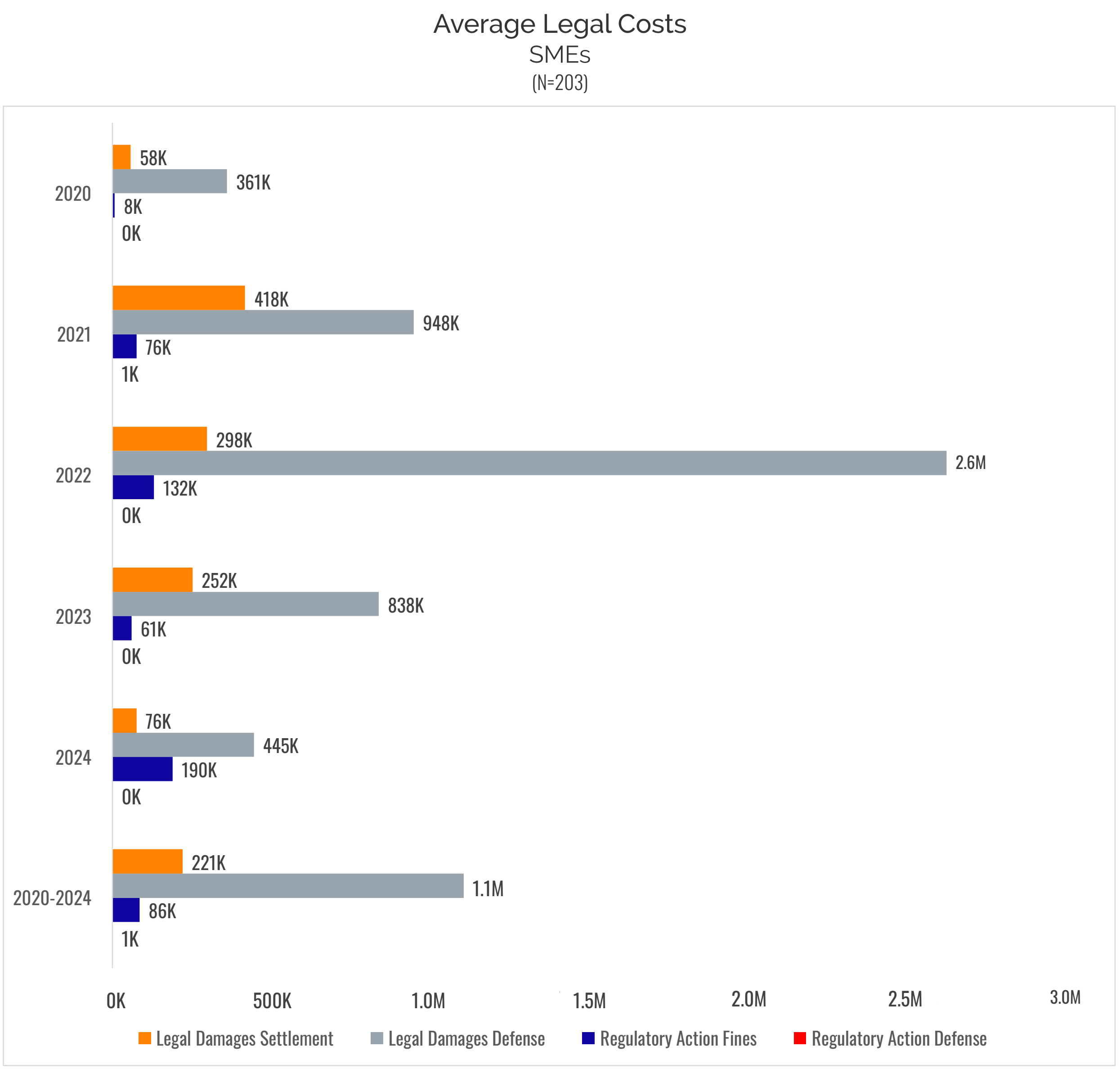


Figure 21

Large Companies

The dataset contained only 15 claims reporting at least one type of legal or litigation expense. For the five-year period, the overall average was $20.1M, with a maximum of over $500M (settlement). This large settlement drives up the overall averages. Average settlement defense cost was $155K. There were no regulatory fines in the five-year data.

This study appears to indicate that the increasing number of lawsuits arising from data privacy/security events have driven down the average cost. As the leader of our firm's cybersecurity litigation practice—currently defending over 150 data privacy/security-related class actions—I know that smaller populations notified of data breaches are triggering more class actions, especially in the healthcare and financial services industries.

Allen E. Sattler, Partner & Vice-Chair
Constangy Cyber Team

Records Exposed

When looking at the five-year window, we see both the number of claims reporting records exposed and the overall number of records continuing to decrease. The 2020–2024 range contains 396 claims that reported more than one[1] record exposed, whereas the 2019–2023 range contained 436 of these claims. These incidents exposed over 715M records—260M at SMEs and 455M at large companies—down 20% from last year's report.

We cannot pinpoint why the number of claims with exposed records is decreasing, nor can we say whether this represents a change in exposure or a change in reporting. However, we can speculate:

- The large proportion of ransomware and BEC claims since 2020 do not involve exposed records.
- Perhaps (as we have speculated in the past) the lack of utility of per record metrics is causing insurers to be less concerned with the number of records than they once were.

Figures 22 and 23 illustrate the number of exposed records year-by-year and with a five-year average. There is no clear pattern. As found in previous NetDiligence Cyber Claims reports, the number of records exposed does not correlate well with either the size of an organization or the total incident cost.

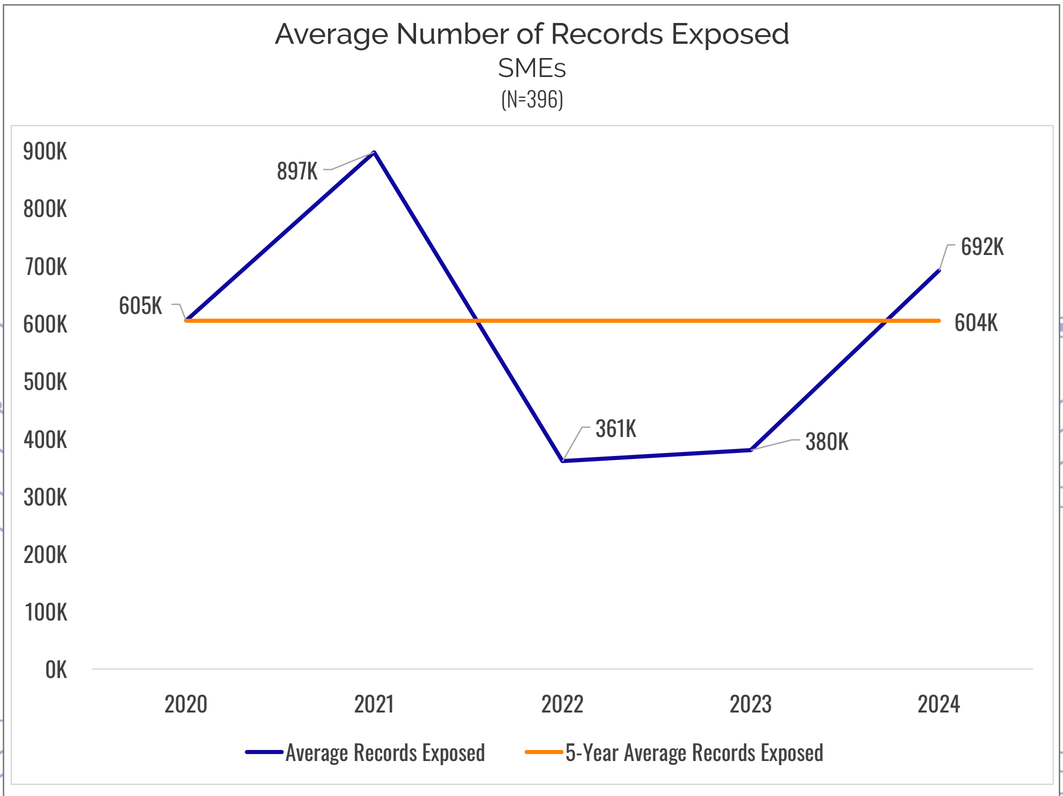


Figure 22

[1] Claims with blank, 0, or 1 records exposed were excluded from this sub-analysis.

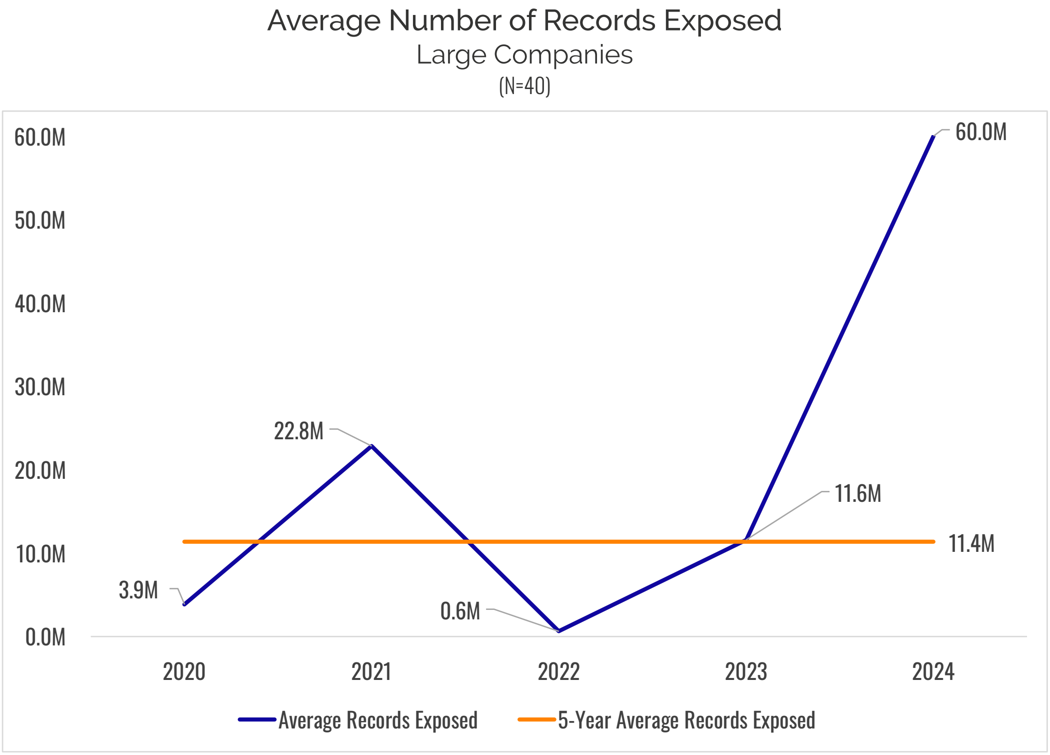

Average Number of Records Exposed
Large Companies
(N=40)
60.0M
50.0M
40.0M
30.0M
20.0M
10.0M
0.0M
3.9M
22.8M
0.6M
11.6M
60.0M
11.4M
2020
2021
2022
2023
2024
Average Records Exposed
5-Year Average Records Exposed

Figure 23

Recordless Claims and Claims with Exposed Records

“Recordless” claims are incidents that do not expose records. Ransomware, business email compromise (BEC), wire transfer fraud, DDoS (Distributed Denial of Service), and theft of money accounted for most of these incidents.

As Figure 24 shows, the average incident cost for each category is about the same over five years.

Please note that in a certain number of incidents, study participants indicated that records were exposed but did not provide a number. We included these incidents in the records exposed analysis here but excluded them from the number of records analysis above.

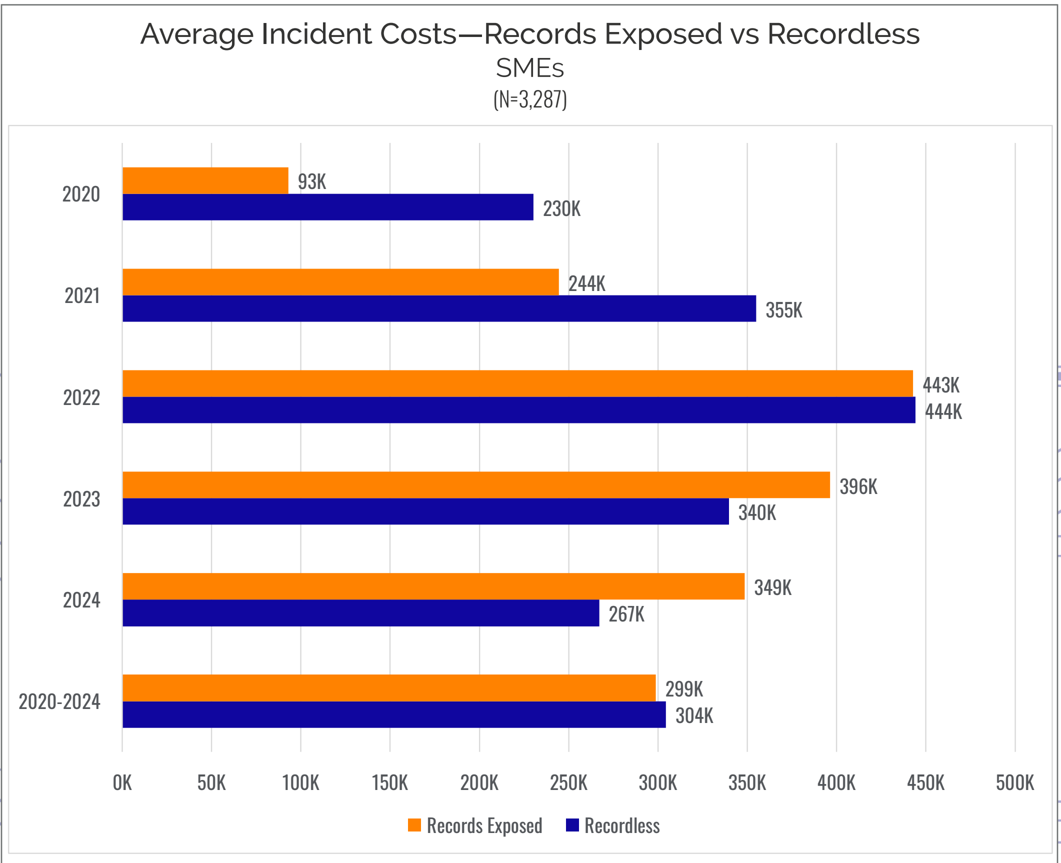


Figure 24

Criminal and Non-Criminal Activities

Criminal activities include:

- Hacking
- Ransomware
- Social Engineering
- Business Email Compromise (BEC)
- Phishing
- Distributed Denial of Service (DDoS) Attacks
- Stolen Devices
- Theft of Money
- Banking/ACH Fraud

Non-criminal events include:

- Staff Mistakes
- Mishandling of Paper Records
- Improper Disclosure
- Lost Laptops
- Programming Errors
- System Glitches
- Legal Actions

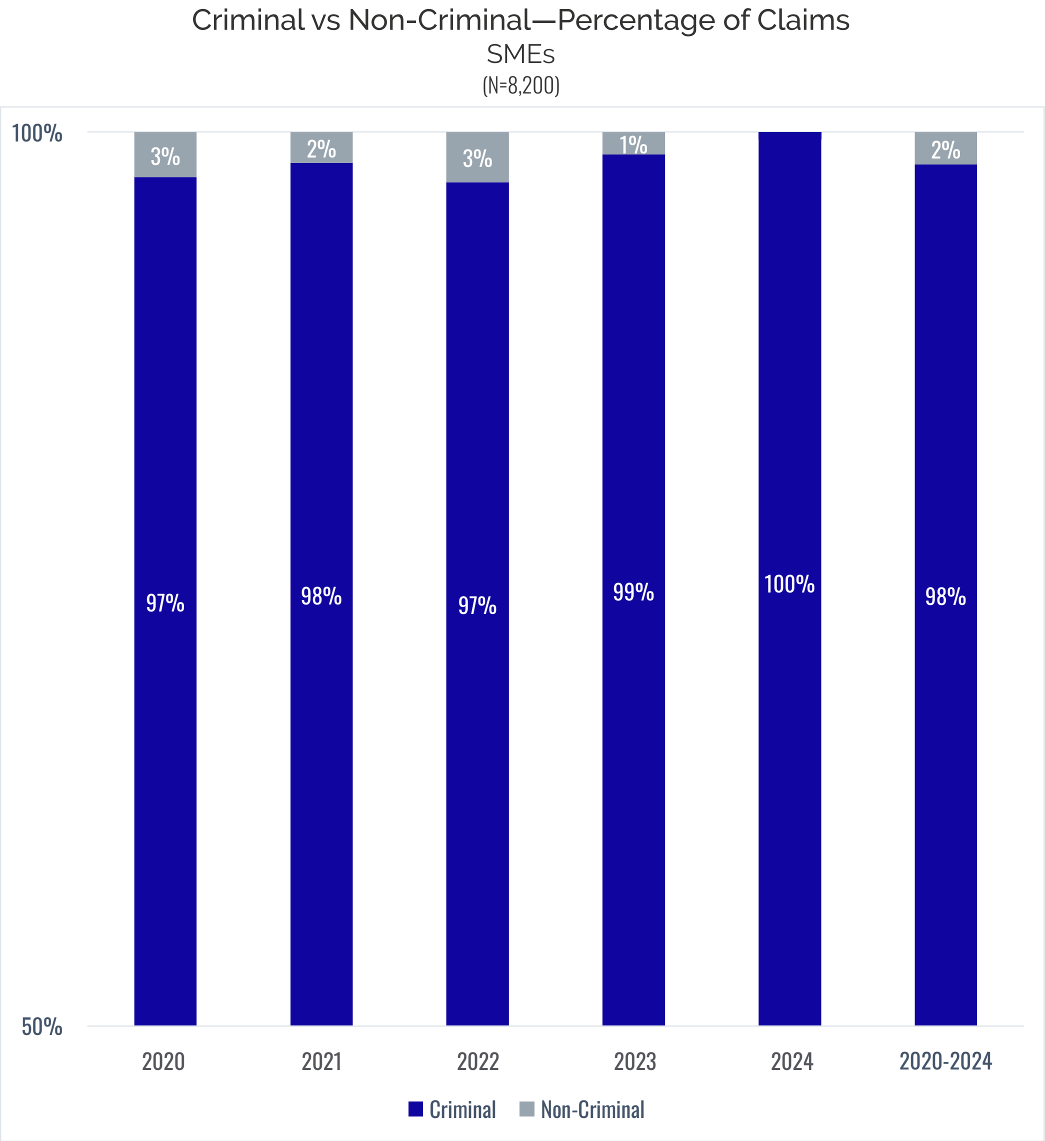


Figure 25

There are fewer and fewer non-criminal incidents, which may be attributed to better employee training and more sophisticated controls. At SMEs, the proportion of claims caused by criminal activities ranged from a low of 97% in 2020 to a high of 100% in 2023. This proportion has been over 97% since 2020.

Over five years, criminal incidents at SMEs were, on average, much more costly than non-criminal incidents. Several large events in 2022 involving wrongful data collection, trademark infringement, and privacy breaches (incident cost between $1M and $5M) caused the non-criminal average cost in that year to exceed the criminal average cost by a large margin. (Figure 26, below)

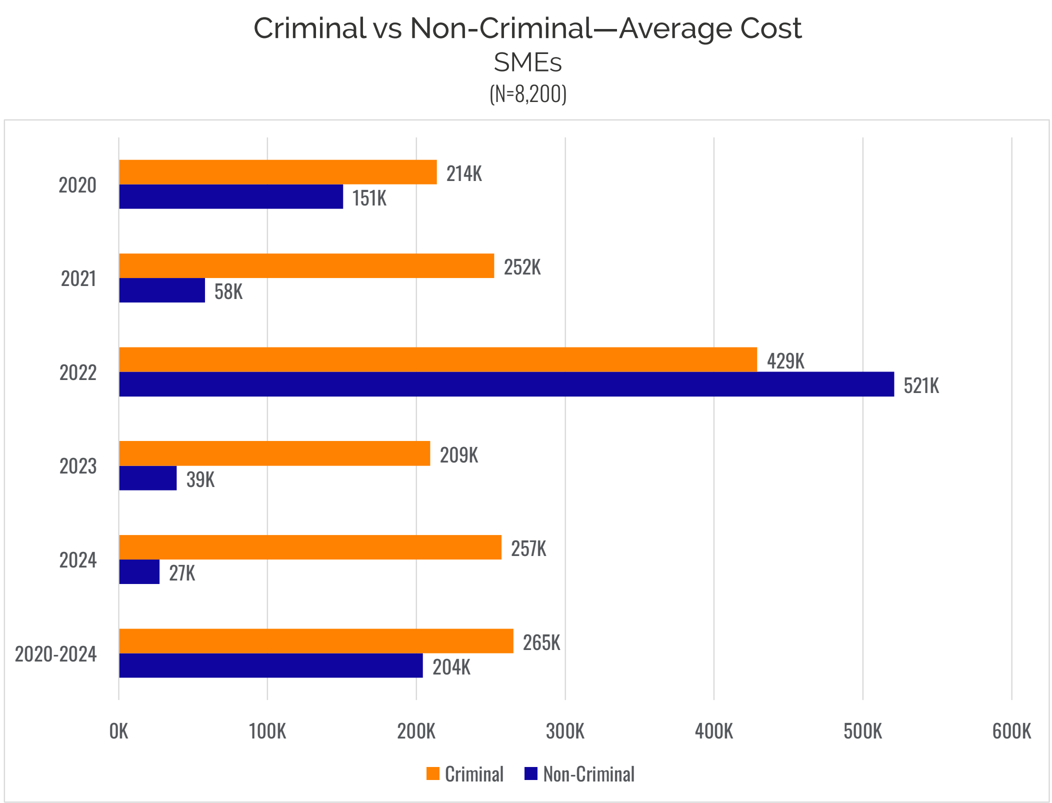


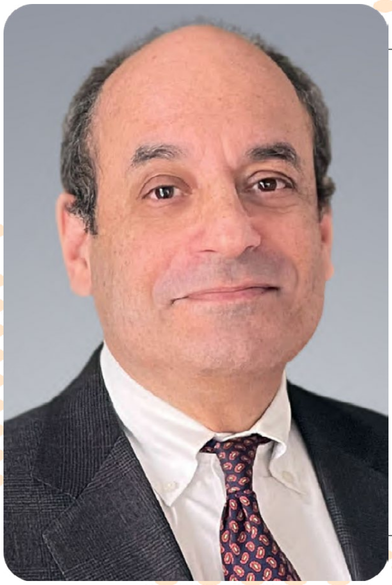
Figure 26

> *The sophistication of hacking groups varies, so ransom demands don't always match a company's revenue. Instead, attackers often consider a combination of factors: the company's revenue, access to sensitive data that could be further exploited, and the urgency to restore critical services. This combination creates a strong incentive for attackers to strike.*
>
> Billy Gouveia, CEO, Surefire Cyber

Criminal vs Non-Criminal—SMEs
2020-2024

Time Period	Impact	Type of Activity	Average	Maximum	Total
2024	Records Exposed	Criminal	826K	16.0M	38.0M
		Non-Criminal	0K	0K	0K
	Crisis Services	Criminal	159K	5.0M	122.2M
		Non-Criminal	0K	0K	0K
	Incident Cost	Criminal	257K	26.0M	322.8M
		Non-Criminal	27K	67K	137K
2020-2024	Records Exposed	Criminal	628K	30.0M	225.4M
		Non-Criminal	190K	3K	3.4M
	Crisis Services	Criminal	158K	25.9M	689.1M
		Non-Criminal	20K	0.1M	1.1M
	Incident Cost	Criminal	265K	108.0M	2.1B
		Non-Criminal	204K	5.1M	30.5M

Table 1



Malicious actors target funds transfers as a relatively easy means of stealing substantial sums of money. They compromise an email account of someone who likely has authority to authorize ACH payments or wire transfers. There is a myth that unless you respond immediately, fraudulently transferred funds are unrecoverable. Our team has recovered millions of dollars in funds weeks and months after the fact.

Richard W. Goldberg, Partner & Vice Chair
Constangy Cyber Team

Comparisons of criminal to non-criminal incidents at large companies are outlined in Figures 27 and 28 below. Here we see that 90% of incidents reported at large companies involved criminal activity. The cost of criminal incidents was dramatically higher than the cost of non-criminal ones.

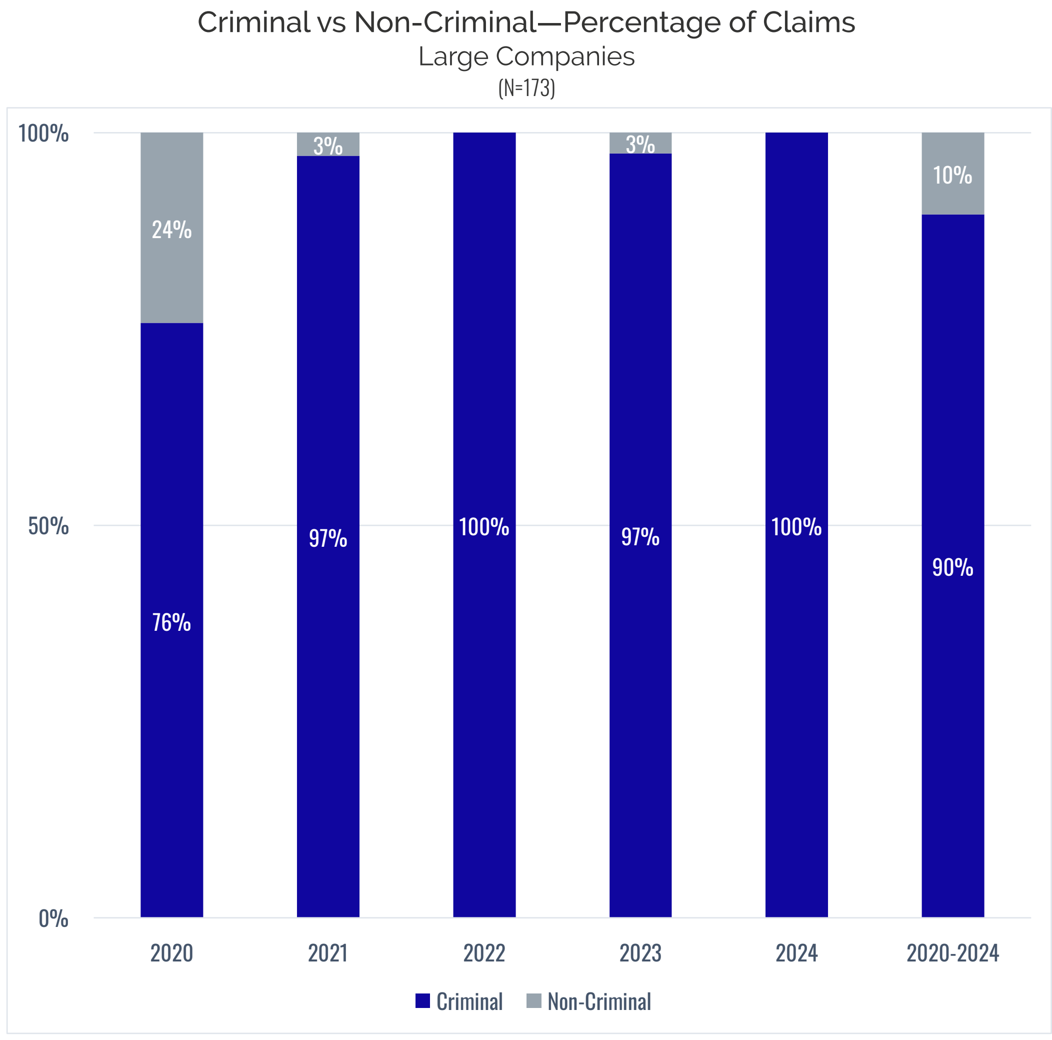


Figure 27

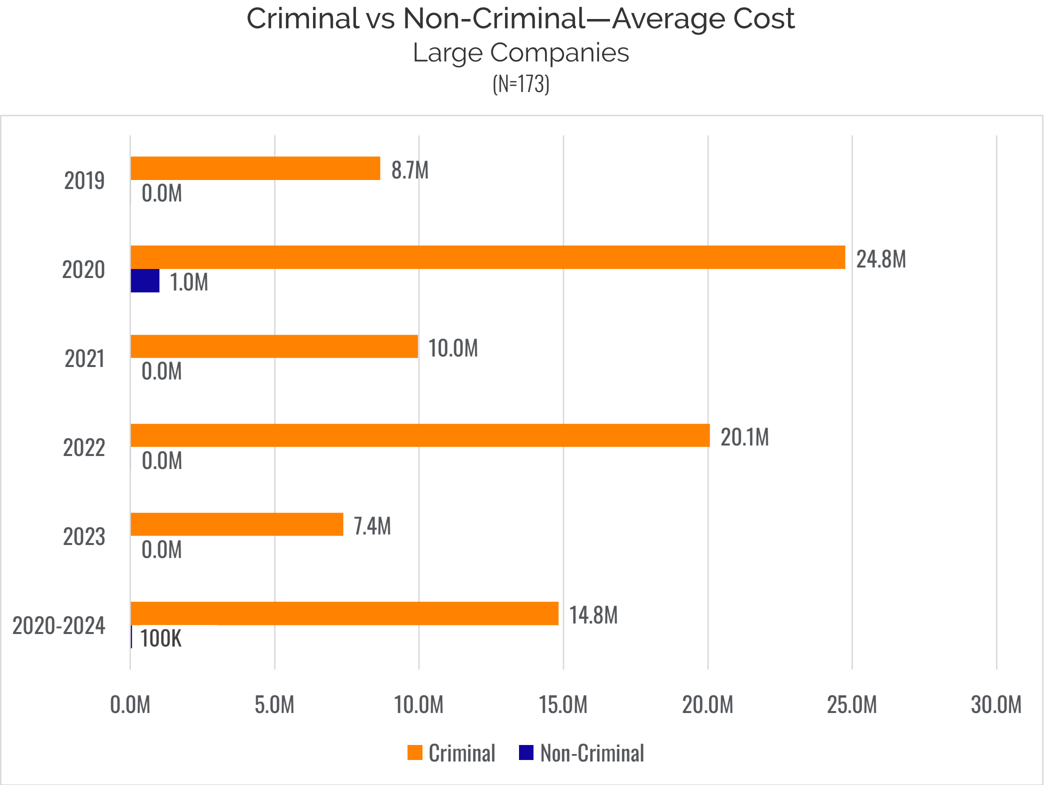

Criminal vs Non-Criminal—Average Cost
Large Companies
(N=173)
2019
8.7M
0.0M
2020
24.8M
1.0M
2021
10.0M
0.0M
2022
20.1M
0.0M
2023
7.4M
0.0M
2020-2024
14.8M
100K
0.0M
5.0M
10.0M
15.0M
20.0M
25.0M
30.0M
Criminal
Non-Criminal

Figure 28

Self-Insured Retentions (SIR)

The dataset contained 5,576 claims for SMEs that provided an amount for SIR . These amounts ranged $0–$10M. Year-by-year averages are shown below.

The dataset contained 139 claims for large companies that reported an amount for SIR. These amounts ranged $0–$10M. The year-by-year averages are shown below. Since 2020, the average SIR has been rising steadily for large companies—the average SIR in 2024 was over three times the amount in 2020.

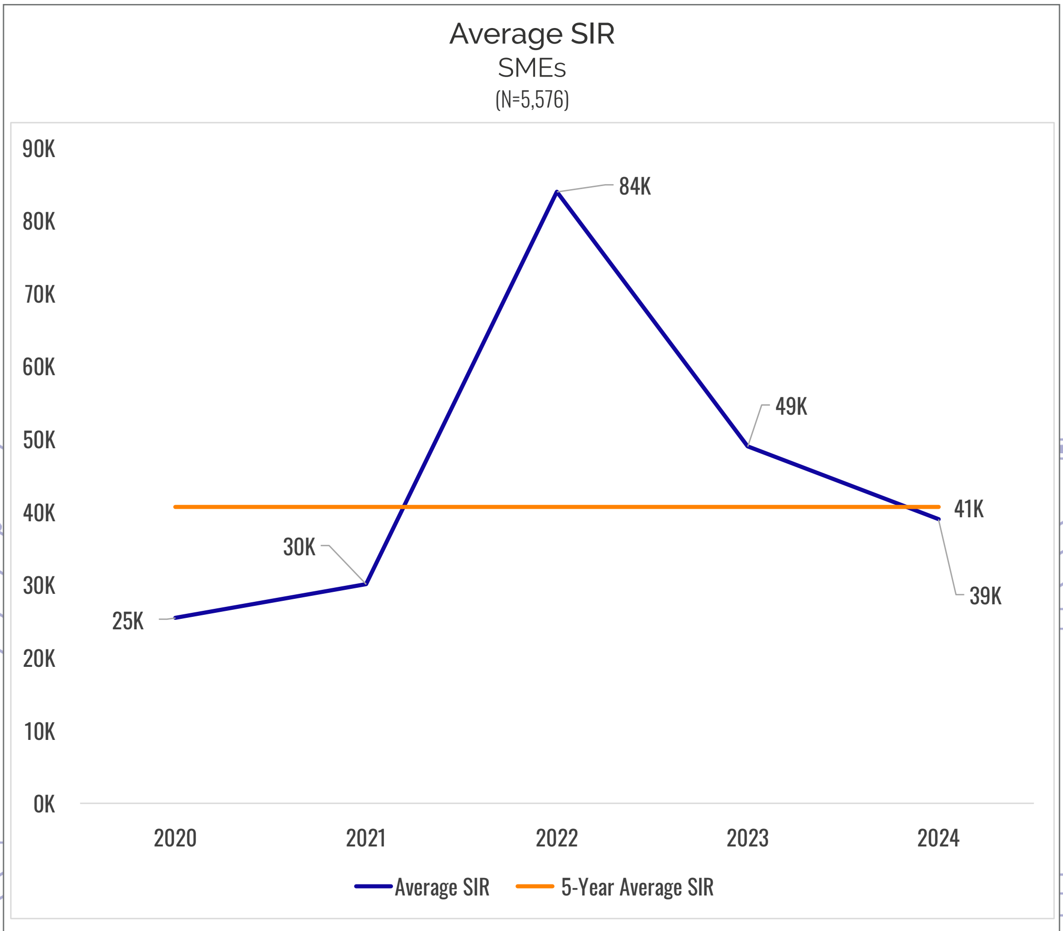


Figure 29

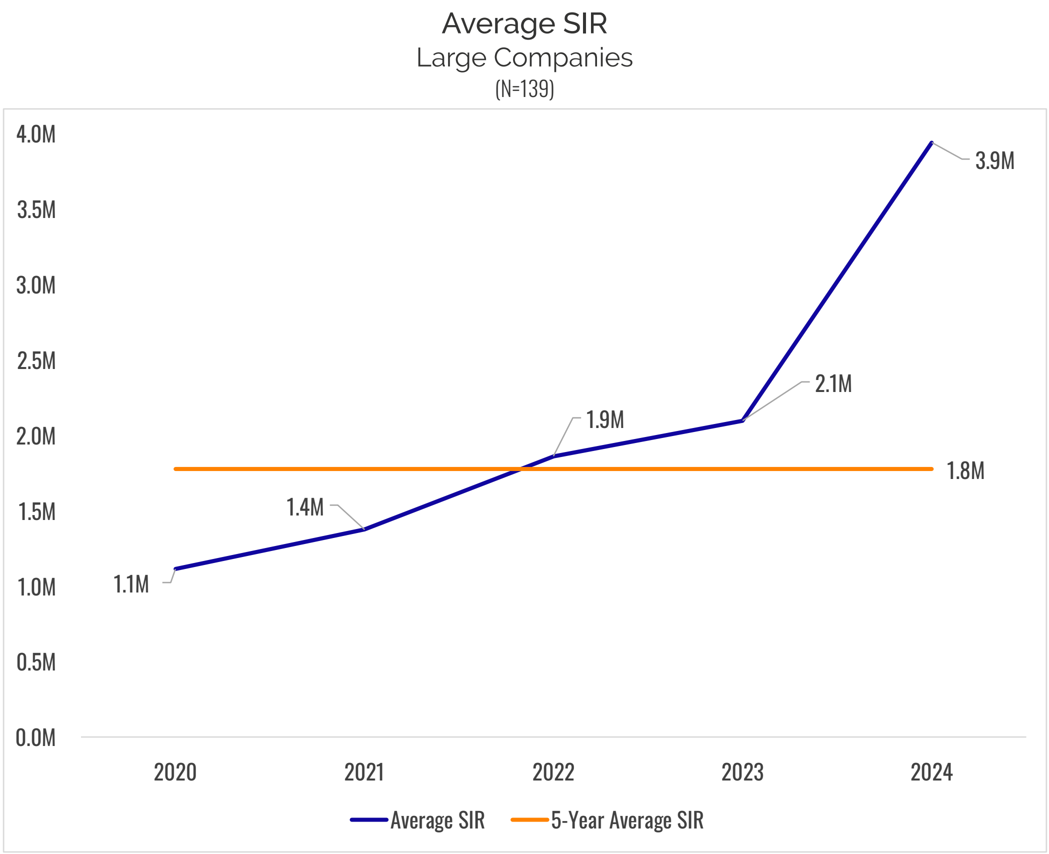

Average SIR
Large Companies
(N=139)
4.0M
3.5M
3.0M
2.5M
2.0M
1.5M
1.0M
0.5M
0.0M
2020
2021
2022
2023
2024
1.1M
1.4M
1.9M
2.1M
3.9M
1.8M
Average SIR
5-Year Average SIR

Figure 30

Causes of Loss

The top four causes of loss at SMEs were

- Ransomware
- Business Email Compromise (BEC)
- Hackers
- Wire Transfer Fraud

Losses in these four categories accounted for 72% of claims and 85% of total incident cost ($2.0B). For metrics on all sectors, please see the graphs and tables in the appendices.

Top Causes of Loss—SMEs

Number of Claims, Aggregate Incident Cost, Percent of Total Incident Cost

Top 5 Responsible for 72% of Claims, 85% of All Losses

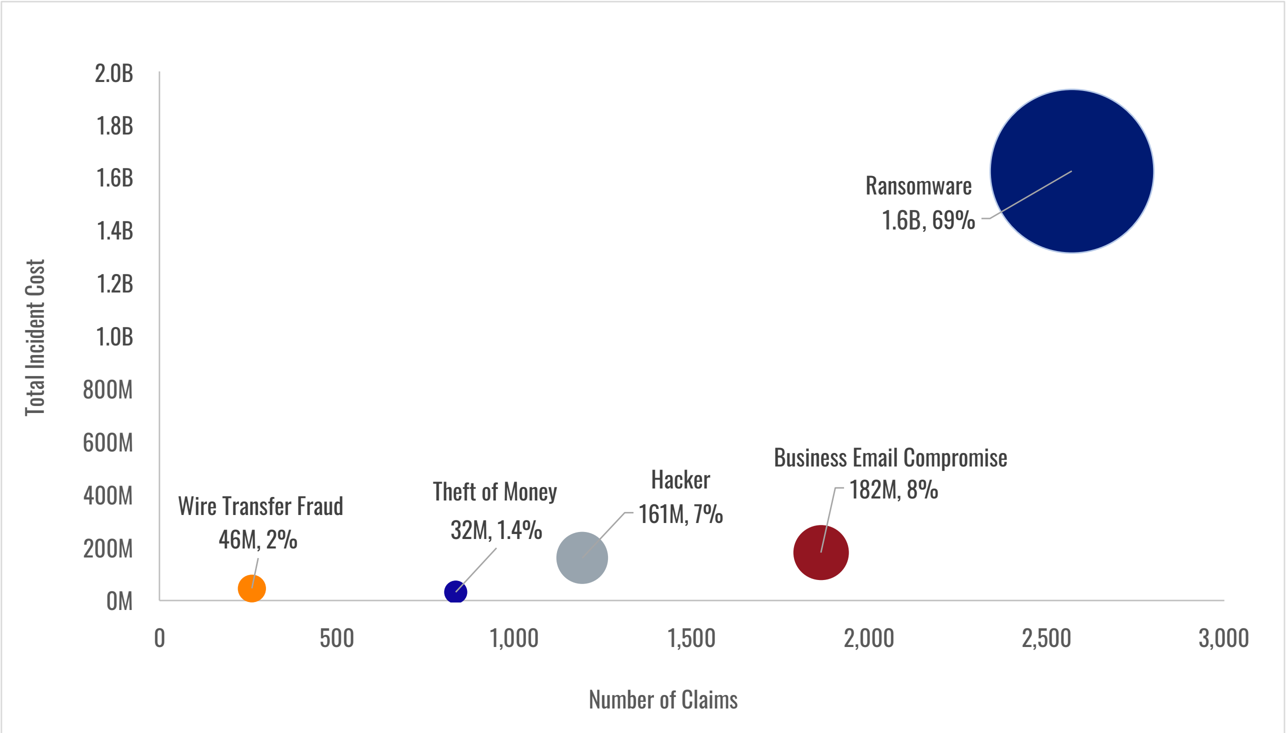


Figure 31

Ransomware

The number of ransomware incidents reported to NetDiligence decreased from 757 in 2020 to 397 in 2024. Since anecdotal evidence does not support the narrative of decline in ransomware, we posit that apparent decreases may be due to delays in reporting. Each Cyber Claims Study collects data for three previous years. As more data for 2023 and 2024 is added to the composite picture, totals will likely climb.[2]

Ransom amounts and total incident cost have increased dramatically over the past five years.

At SMEs, outlier events drove up the average incident cost in 2022. At large companies, outlier events heavily impacted the averages in 2021 and 2023.

Average Incident Cost—All Ransomware Claims
SMEs
(N=2,571)

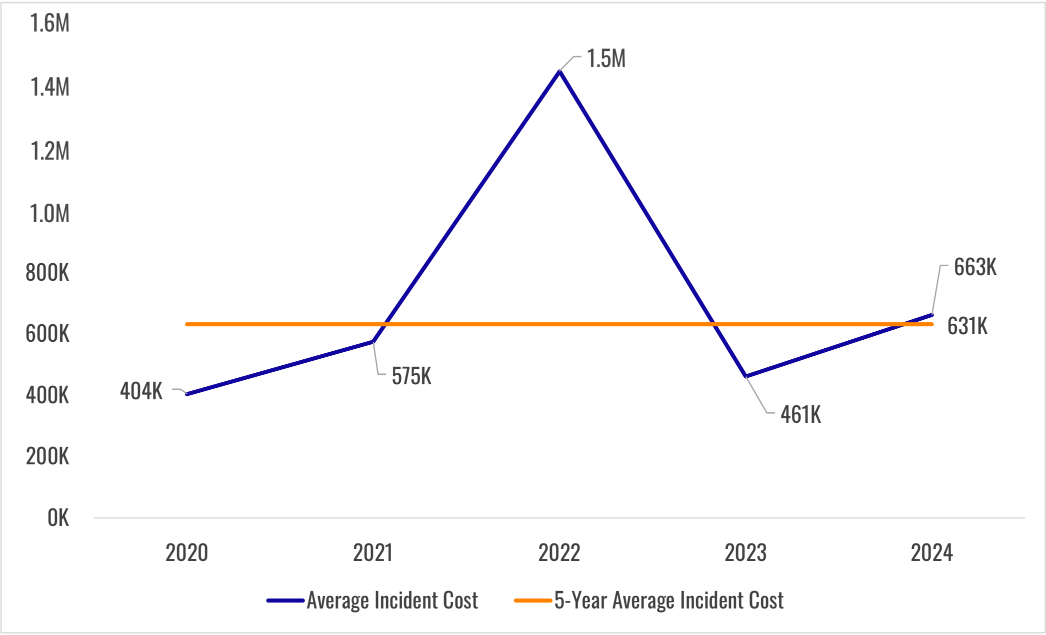
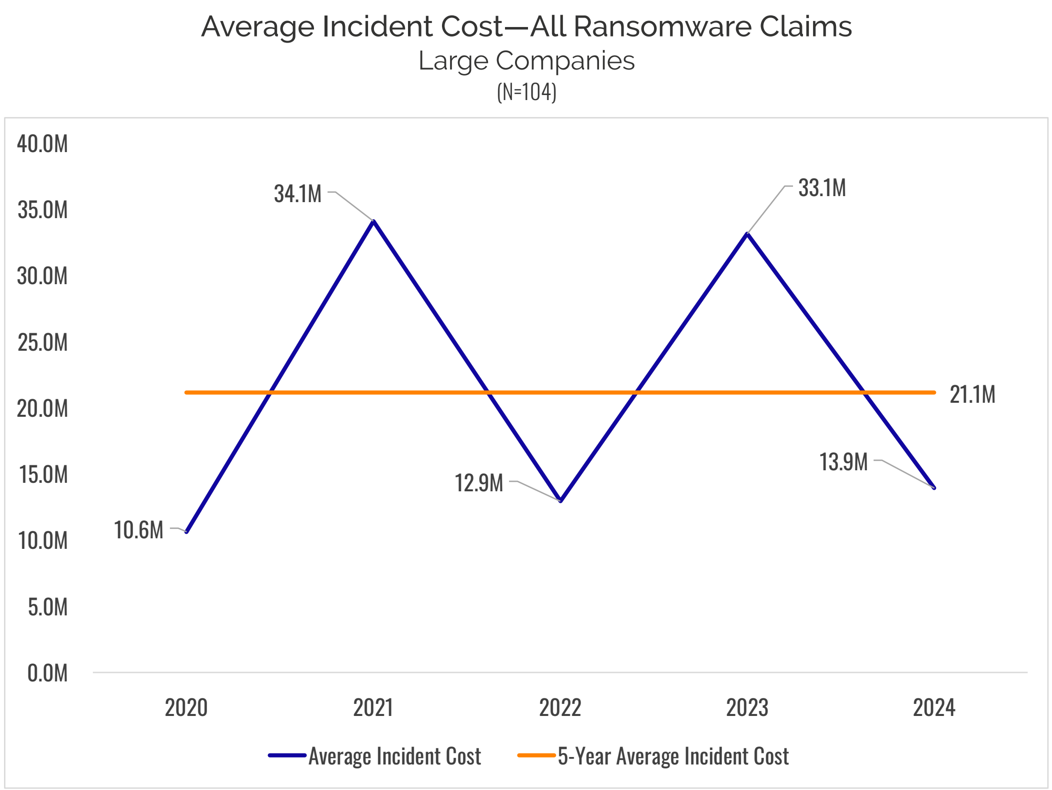


Figure 32

Once again, ransomware is the primary driver of losses in this year's report—it's the most impactful type of attack, potentially creating significant financial, operational and reputational harm. Recently, we've seen multiple third-party and supply chain breaches across industries. As demonstrated in the survey, these breaches have enabled threat actors to be able to ratchet up ransom demands and, in some cases, secure payments. This is because the service provider needs to restore lots of clients, since the attack doesn't just affect them as a company. With businesses deeply integrated with third parties, software providers and SaaS platforms, recovery can take weeks, causing considerable business and productivity losses. These challenges emphasize the importance of implementing effective controls and recovery strategies.

Alden Hutchison, RSM US LLP

[2] Each year, we collect data from the three previous years. For this report (2025) we collected claims for 2022-2024. We will continue to collect claims for incidents in 2024 for two more years.



Average Incident Cost—All Ransomware Claims
Large Companies
(N=104)

Figure 33

Business Email Compromise (BEC)

BEC was the second leading cause of loss at SMEs. The number of BEC claims per year had been consistent from 2020-2023, ranging from 300 to 400 per year. We have seen a notable increase in the number of BEC claims in 2024 (N=468), although the average incident cost is low ($75K).

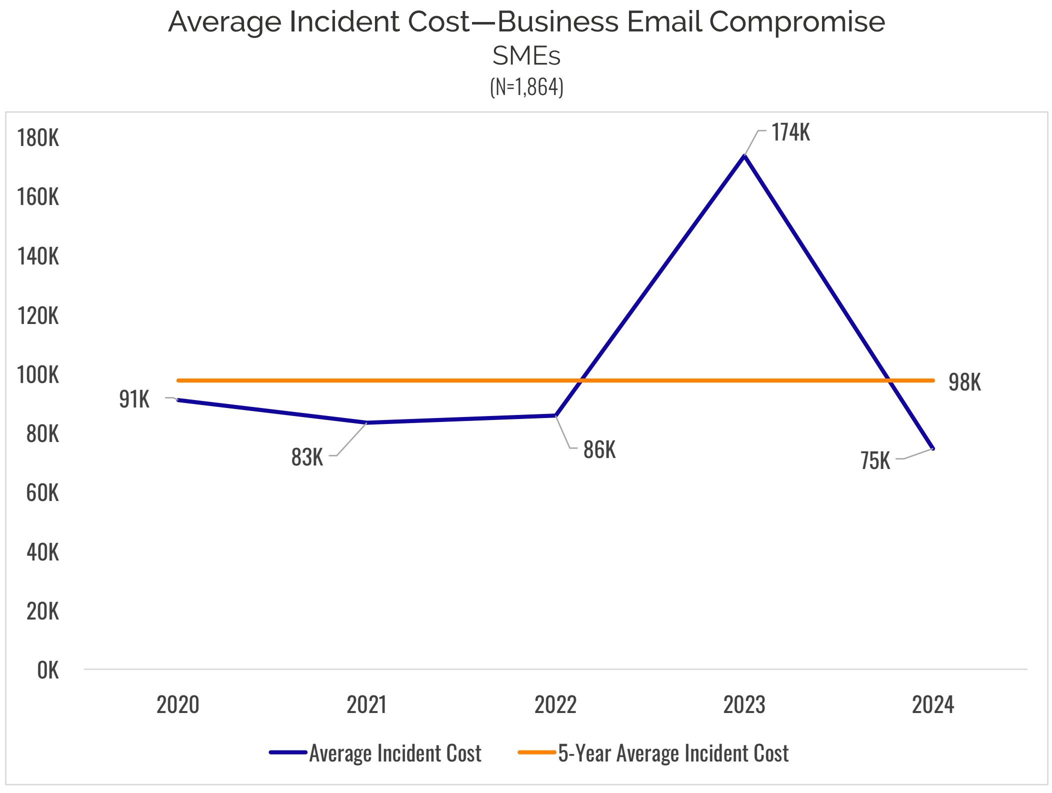


Figure 34

> *We saw a notable increase of BEC cases in 2024. Despite worries of sophisticated compromises, 84% of those cases involved someone clicking an email link. Email security that prevents accidental clicking on a malicious attachment from turning into a compromised network is more critical than ever, and strong payment controls to validate transaction identities can prevent fraudulent funds transfers altogether.*
>
> Billy Gouveia, Surefire Cyber

Hackers

Hackers were the third leading cause of loss at SMEs. Figure 35 below tells the good news: after large increases in 2022 and 2023, the average cost of a hacking incident has dropped in 2024.

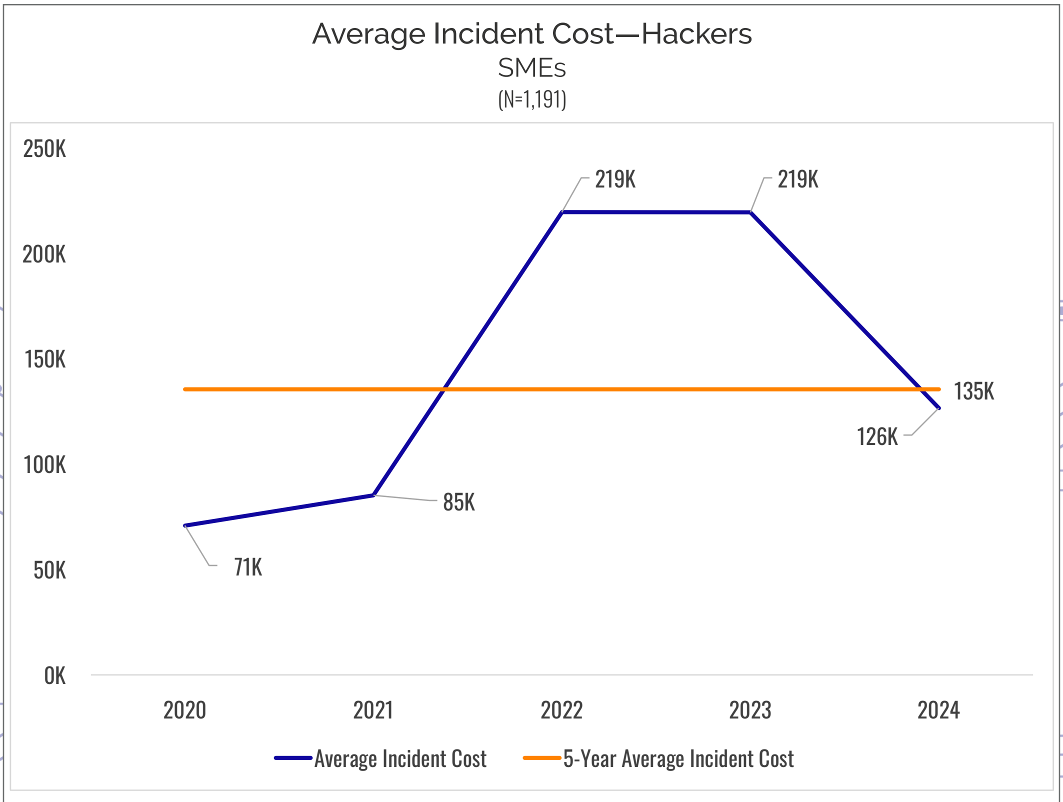


Figure 35

Wire Transfer Fraud

Wire transfer fraud was the fourth leading cause of loss at SMEs. Organizations of all sizes were victims (annual revenue $40K–$1.2B; average=$75M). After four years of steady declines, the average incident cost from wire transfer fraud began to rise in 2024.

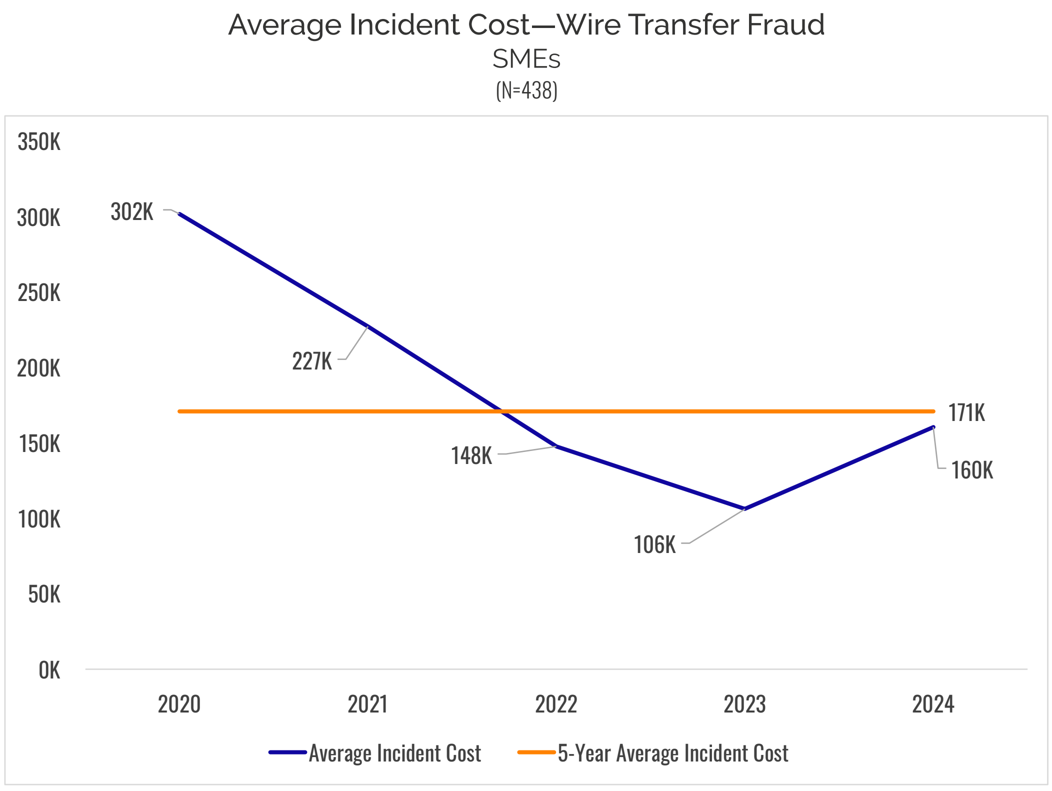


Figure 36

The Cyber Claims Study showed an increase in wire transfer fraud losses in 2024. This finding mirrored what Surefire Cyber experienced firsthand. Not only did the average dollar amounts rise, but we also responded to a case where $15 million was stolen. Threat actors continue to target organizations of all sizes, exploiting urgency and trust. We urge clients to develop clear protocols for verifying financial transactions and changes to account information. They should remain alert to last-minute changes to email account addresses and require a second verification method and dual approval before altering employee payment details. These layered defenses help stop fraud before the funds leave the account. By implementing these safeguards into daily operations, organizations can significantly reduce their risk of falling victim to these attacks.

Billy Gouveia, Surefire Cyber

Staff Mistakes

Over the period 2020-2024, the number of incidents involving staff mistakes and programming errors has remained low. The number of claims during the current five-year period (2020–2024) has decreased to 88 from 235 reported last year.

While none of these events has proven too costly, there is no clear pattern to be discerned.

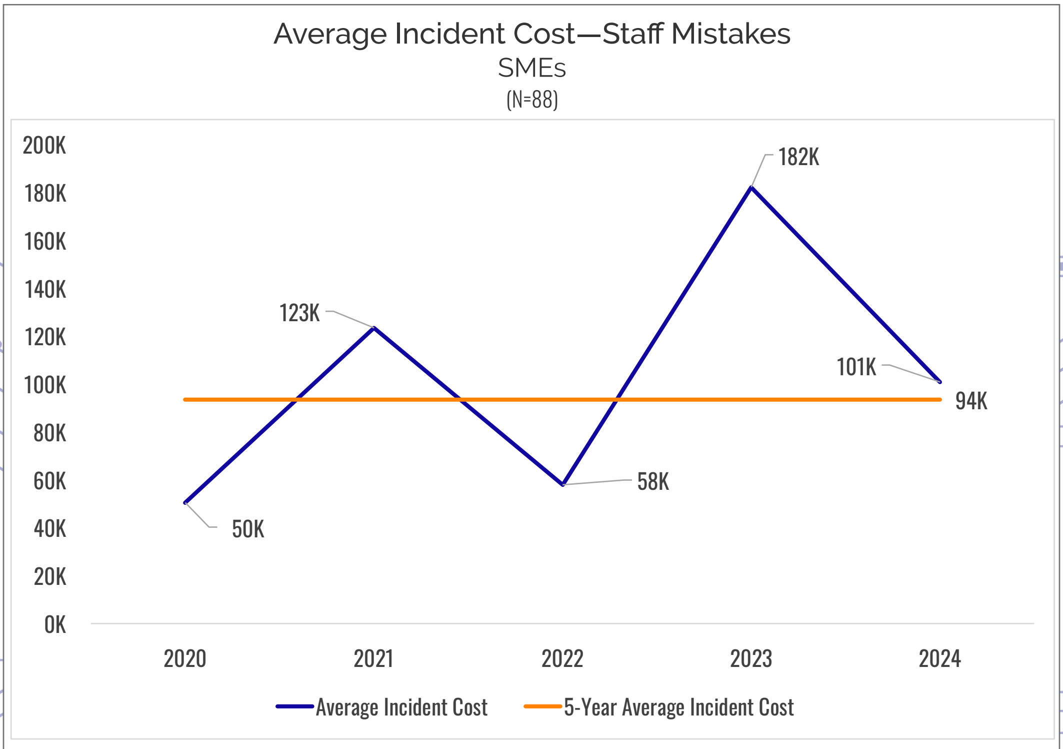


Figure 37

Rogue Employees

Over the past five years, the number and magnitude of incidents caused by malicious employees and ex-employees have been declining. The number of incidents decreased from 65 in 2020 to 11 in 2024. The average incident cost decreased from $116K in 2020 to $25K in 2023. Excepting an extreme outlier event in 2022, average incident cost has been low.

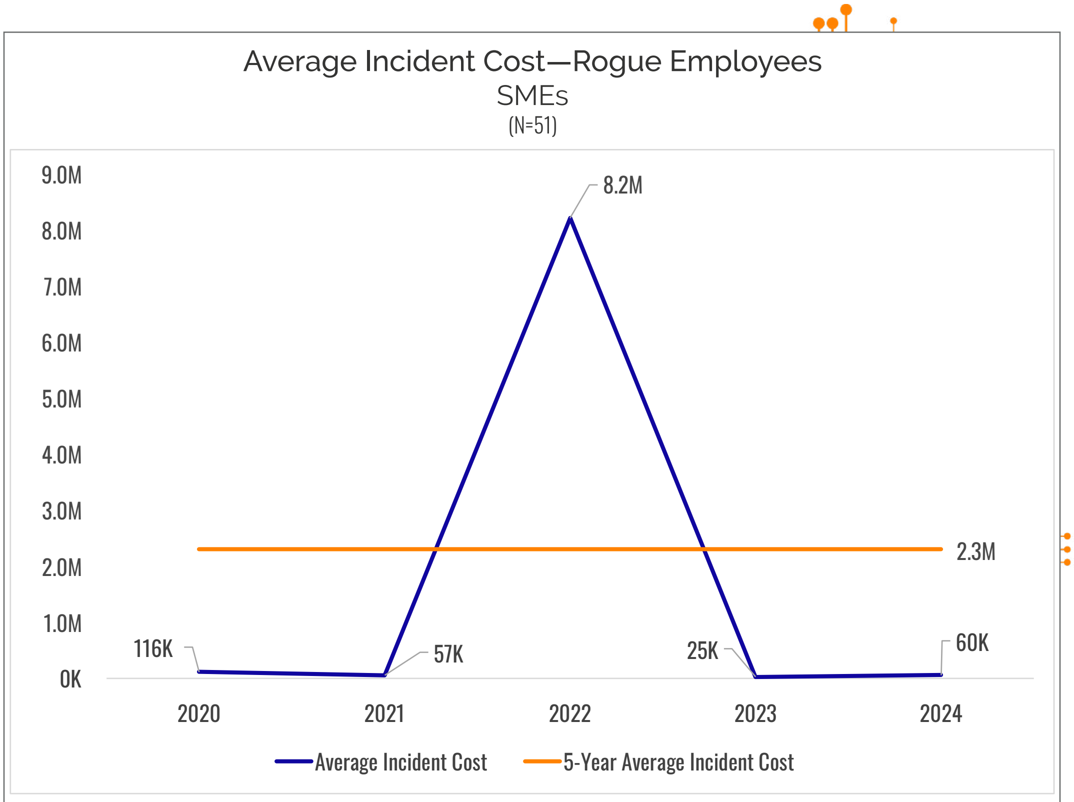


Figure 38

Third-Party Incidents

Third-party incidents can be caused by both malicious and non-malicious actors, and they remain a notable cause of loss.[3] Since 2020, the cost of third-party events caused by malicious actors has been much greater than events stemming from non-malicious accidents or mistakes. The cost of these incidents has been increasing steadily since 2020, and dramatically so in 2024.

There were 33 incidents classified as "supply chain related". Fourteen of these were criminal events, mainly ransomware (N=7). The ransoms paid ranged from $2M to $25M. Total incident costs ranged from $355K to $25M.

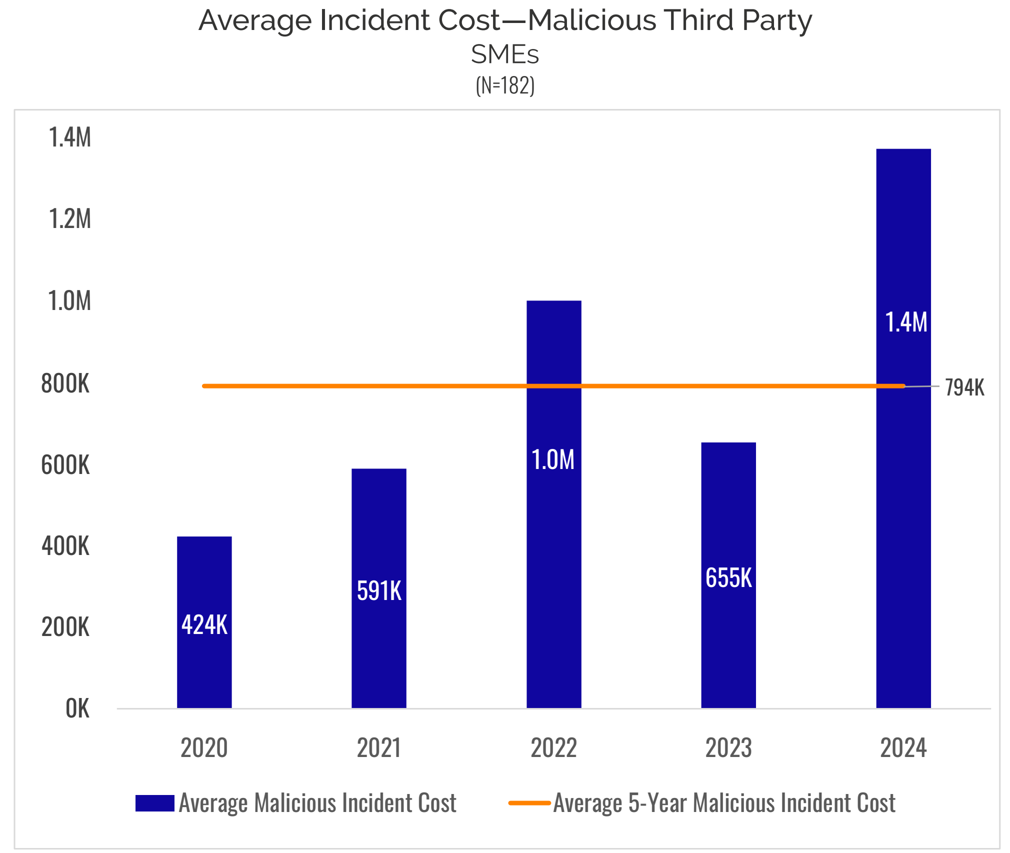


Figure 39

> *Supply chain breaches made up 32% of the incidents Experian responded to globally last year. These aren't isolated events; they're system-wide shocks that affect entire networks. A single vendor's vulnerability can lead to cascading losses across industries. It's not just about assessing your own posture anymore. It's about demanding visibility, accountability, and breach readiness from every partner you do business with.*
>
> Michael Bruemmer, Experian

[3] We are focusing on those third-party incidents that are clearly criminal in nature (N=182). There are only 8 third-party incidents in the dataset that can be clearly classified as non-malicious. A large number of third-party incidents were provided as "Other" cause of loss. Since they could not be classified, they were not included.

Sectors

As measured by the number of claims over five years, the top five affected business sectors at SMEs are the same as in last year's report:

- Professional Services
- Manufacturing
- Healthcare
- Retail
- Financial Services

These five sectors accounted for 47% of all claims and 60% of all total incident cost at SMEs.

Although the rank order changes from year to year, most of these sectors have been at the top of the list for many years. The graph below provides insight into the frequency and magnitude of claims, as well as the percentage of the aggregate SME incident cost. For metrics on all sectors, please see the appendices.

Top Sectors—SMEs

Number of Claims, Aggregate Incident Cost, Percent of Total Incident Cost

Top 5 Account for 47% of Claims, 60% of All Losses

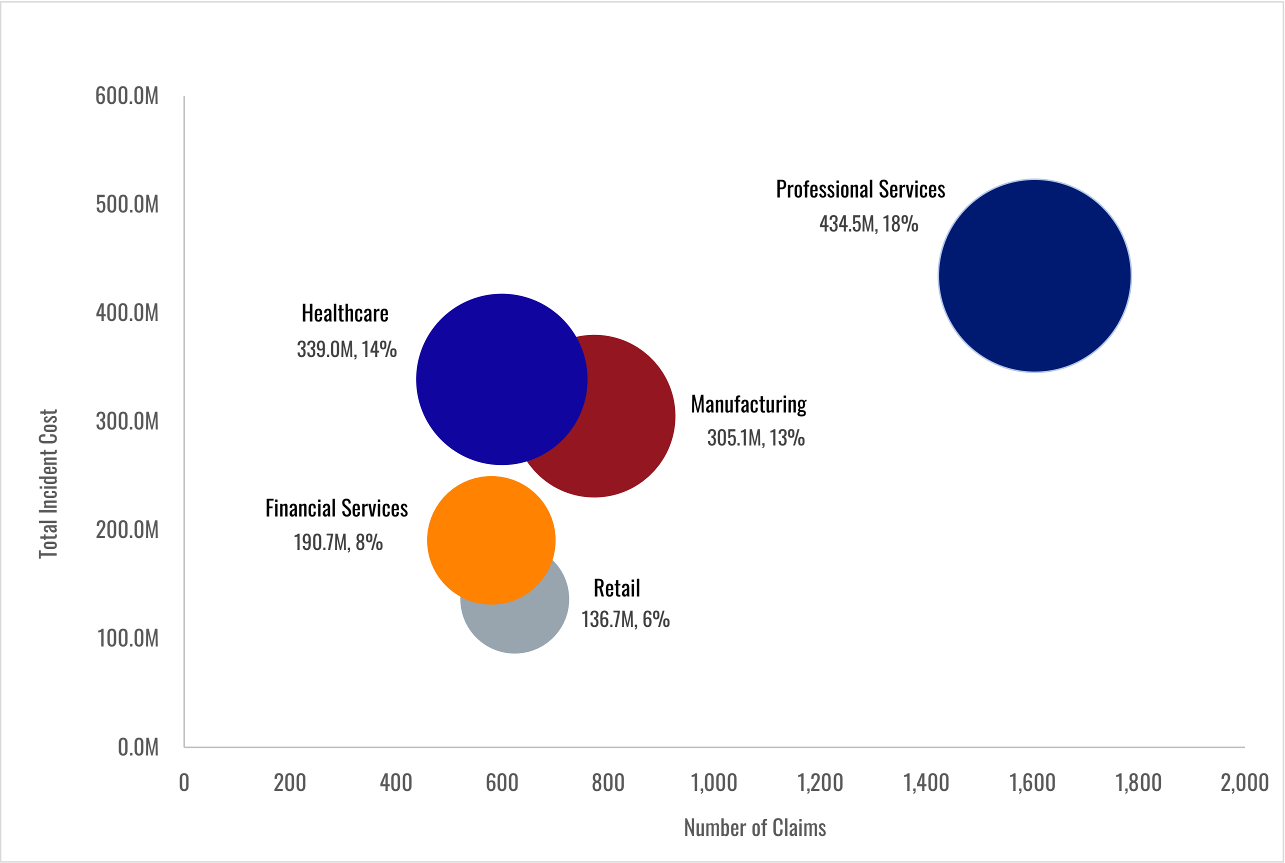


Figure 40

Professional Services

The professional services sector encompasses a broad array of organizations including law firms, accounting and tax firms, consulting firms, and real estate firms. The average and maximum annual revenue of these firms was similar to those in last year's report: $59M and $1.6B.

At SMEs, professional services claims accounted for 18% of all claims and 18% of total incident cost greater than $1K. Total incident cost ranged from $1K to $30M. The top causes of loss were the same as in the 2024 Claims Study: ransomware, BEC, and hackers.

Figure 41 shows the year-by-year and five-year average incident cost for this sector.

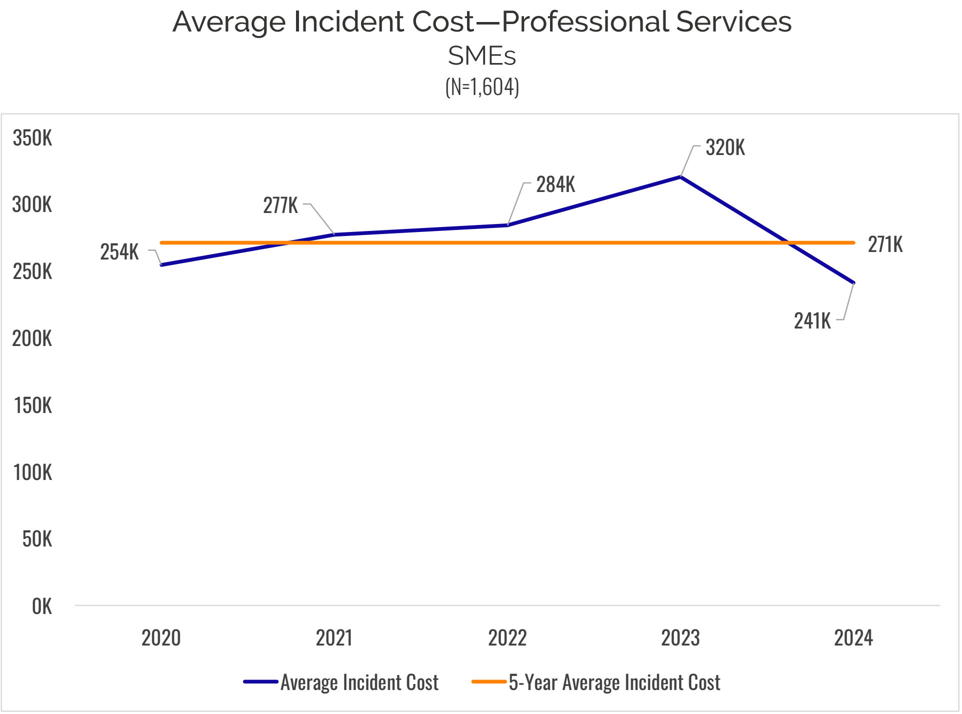


Figure 41

> *This study is consistent with our experience in handling approximately 3,000 incidents this past year, especially as it relates to the primary affected business sectors. Malicious actors are often opportunistic criminals, but they tend to go where the reward is worth the risk. Extortionate attacks on heavily regulated professional services firms, health care providers, and financial services firms often produce results for malicious actors.*
>
> Lindsay B. Nickle, Partner & Vice-Chair, Constangy Cyber Team

Manufacturing

The average annual revenue of organizations in the manufacturing sector was $123M (maximum=$1.9B).

Manufacturing claims accounted for 9% of all claims and 13% of total incident cost at SMEs. Total incident cost ranged from $1K to $108M. The top causes of loss were ransomware, BEC, and wire transfer fraud.

Figure 42 below shows the year-by-year and five-year average incident cost for this sector. The spike in average incident cost 2022 resulted from a very large outlier event.

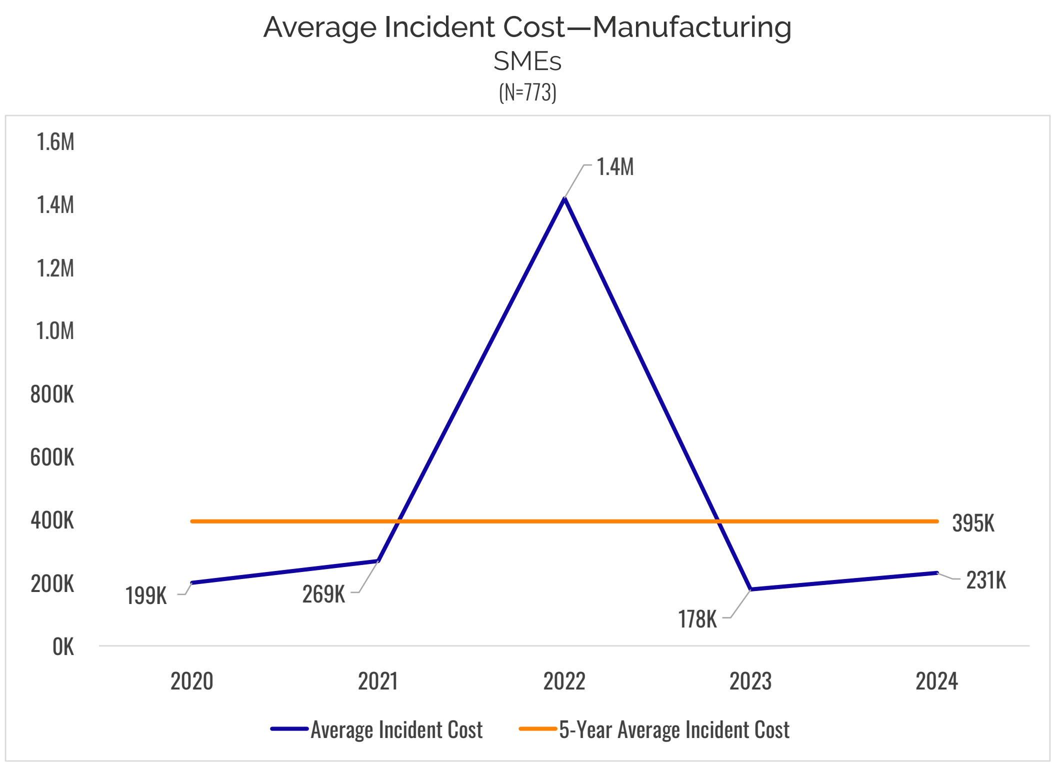


Figure 42

> *Many manufacturing companies have antiquated systems and those are harder and more specialized to restore. When you're doing recovery work, everybody knows how to restore a Windows server, but if you're talking about a very specific application running a manufacturing line or a piece of equipment, securely restoring those can drive the costs up.*
>
> George Kohlhofer, RSM US LLP

Retail

The average annual revenue of organizations in the retail sector was $139M (maximum=$1.9B). Retail claims accounted for 7% of all claims and 6% of total incident cost at SMEs. Total incident cost ranged from $1K to $7.5M. The three top causes of loss were ransomware, BEC, and theft of money.

Figure 43 below shows the year-by-year and five-year average incident cost for this sector.

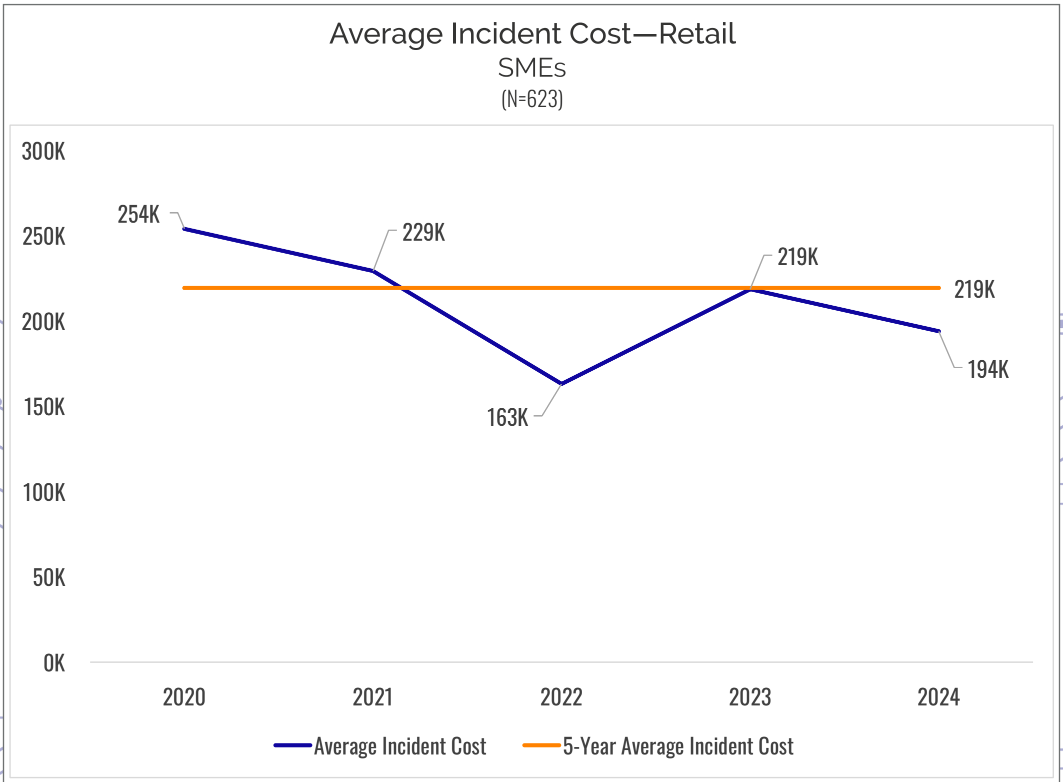


Figure 43

Healthcare

The average annual revenue of organizations in the healthcare sector was $116M (maximum=$1.95B). Healthcare claims accounted for 7% of all claims and 14% of total incident cost at SMEs.

Figure 44 below shows the year-by-year and five-year average incident cost for this sector.

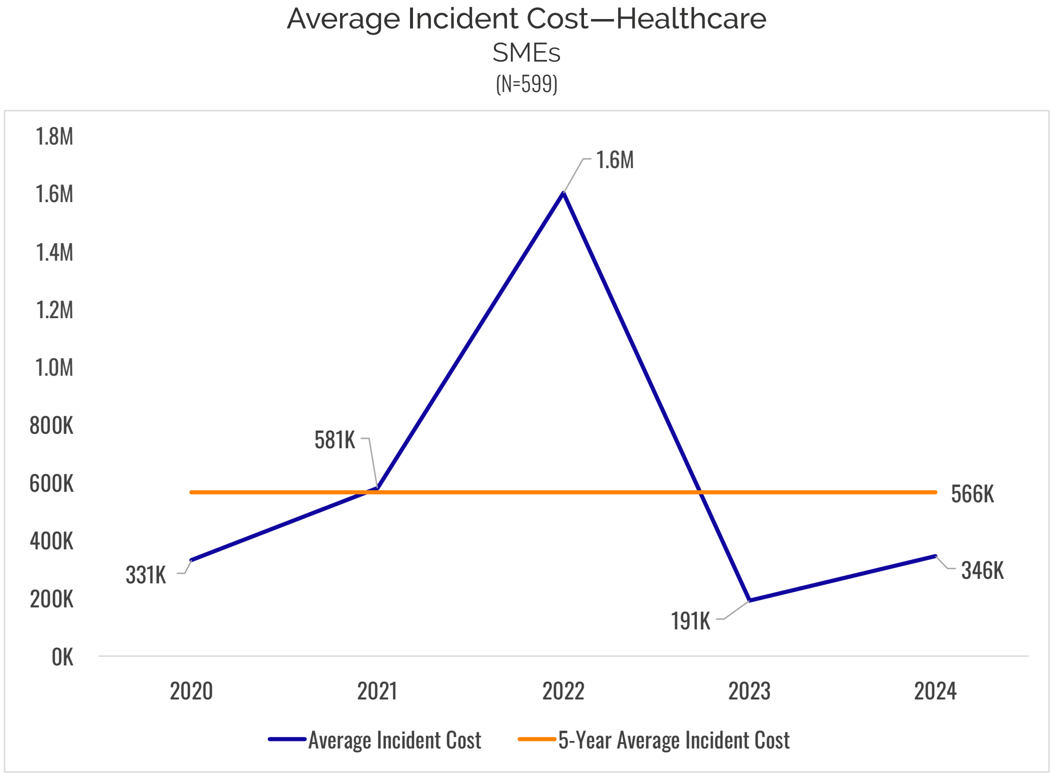


Figure 44

> *Healthcare made up over one-third of data breach events Experian supported globally in 2024. The combination of high-value data, operational urgency, and outdated systems continues to make the sector a consistent target. As ransomware groups focus on industries with low tolerance for downtime, organizations must prioritize preparedness through tested response plans, layered defenses, and regular third-party reviews.*
>
> Michael Bruemmer, Experian

Financial Services

The average annual revenue of organizations in the financial services sector was $113M (maximum=$1.9B). Financial services claims accounted for 6% of all claims and 8% of total incident cost at SMEs. Total incident cost ranged from $1K to $11.5M. The top causes of loss were unchanged from last year: BEC, ransomware, and hackers.

Figure 45 below shows the year-by-year and five-year average incident cost for this sector.

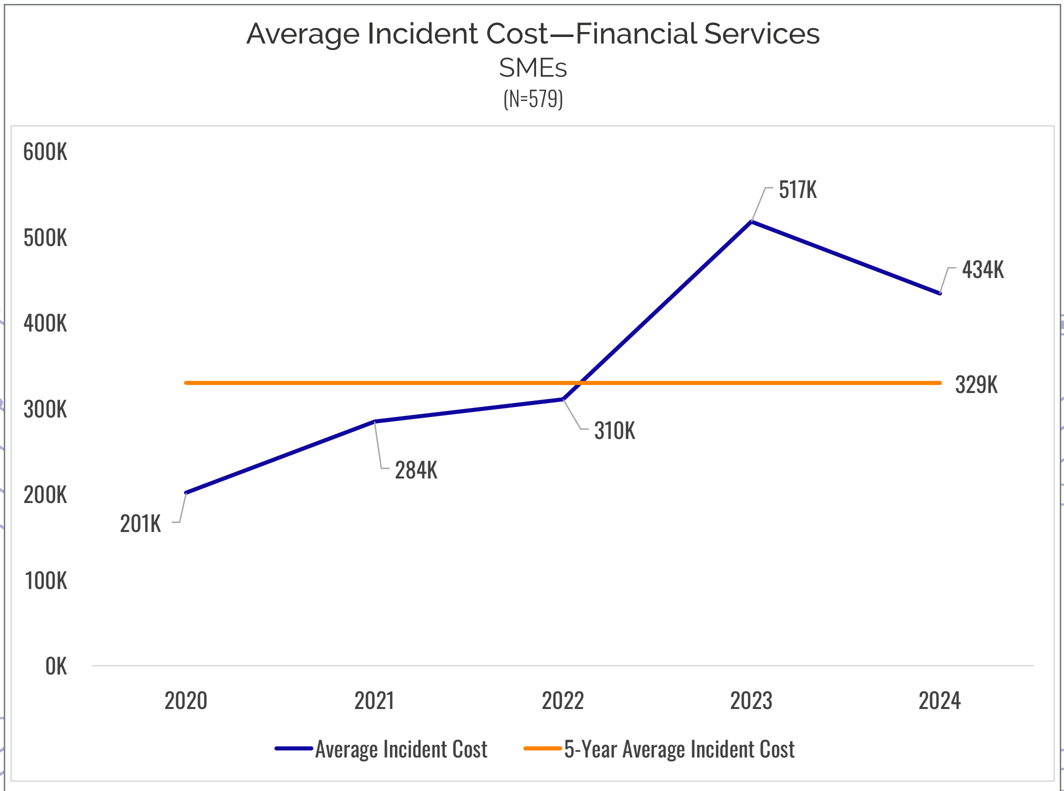


Figure 45

Public Entities

The average annual revenue for public entities was $126M (maximum=$1.7B). Claims from public entities represent around 2% of all claims and 3% of total incident cost. Total incident cost ranged from $1.5K to $4.0M. The average incident cost has increased substantially since 2022. Top causes of loss were ransomware, BEC, and wire transfer fraud.

Average Incident Cost—Public Entity
SMEs
(N=300)

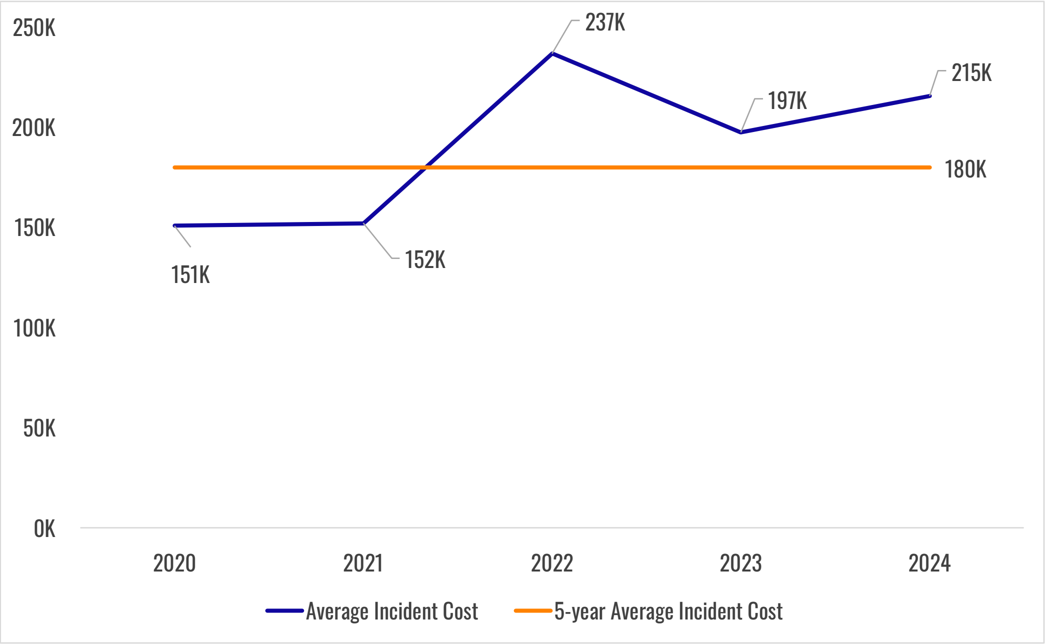


Figure 46

Construction

The average annual revenue for the construction industry was $94M (maximum=$1.8B). Total incident cost ranged from $3.4K to $1.7M. The average incident cost has been low and flat since 2020. Top causes of loss were ransomware (N=246) and BEC (N=176). The average ransom payment was $254K.

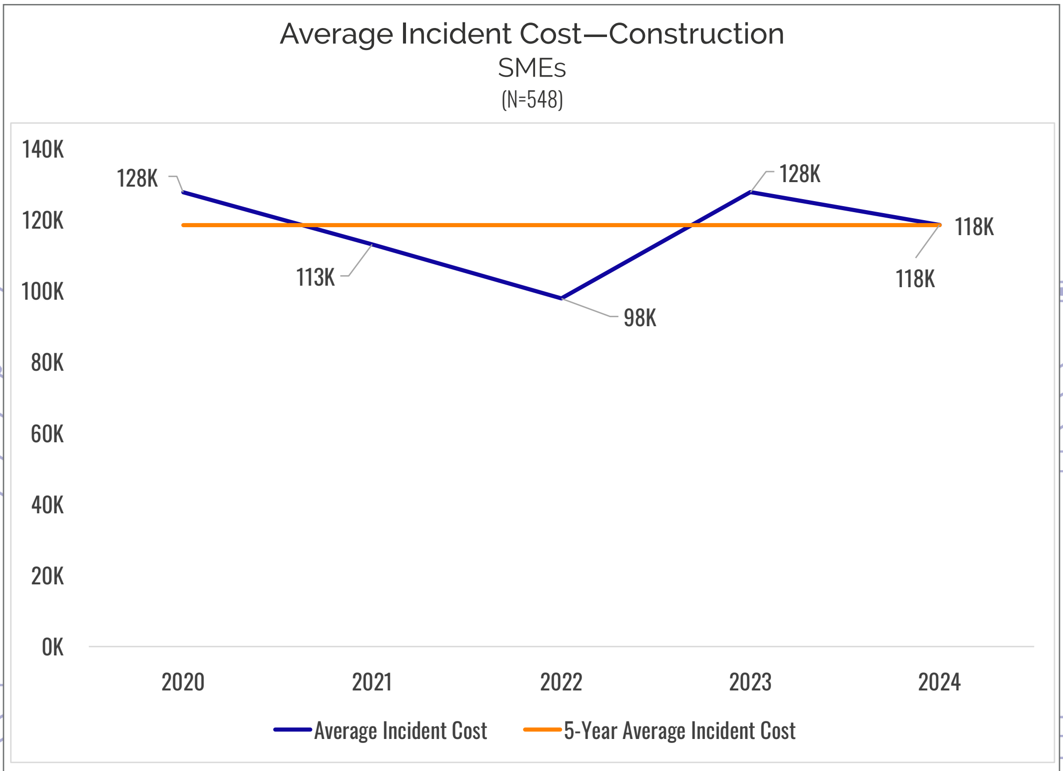


Figure 47

Claims from Canada

Claims from Canada are limited (<1.0%). However, these incidents represent an important subset of the dataset. The average annual revenue of a Canadian organization in this study was 654M USD (maximum=17B USD). The average five-year total incident cost was 874K USD (maximum=15M USD).

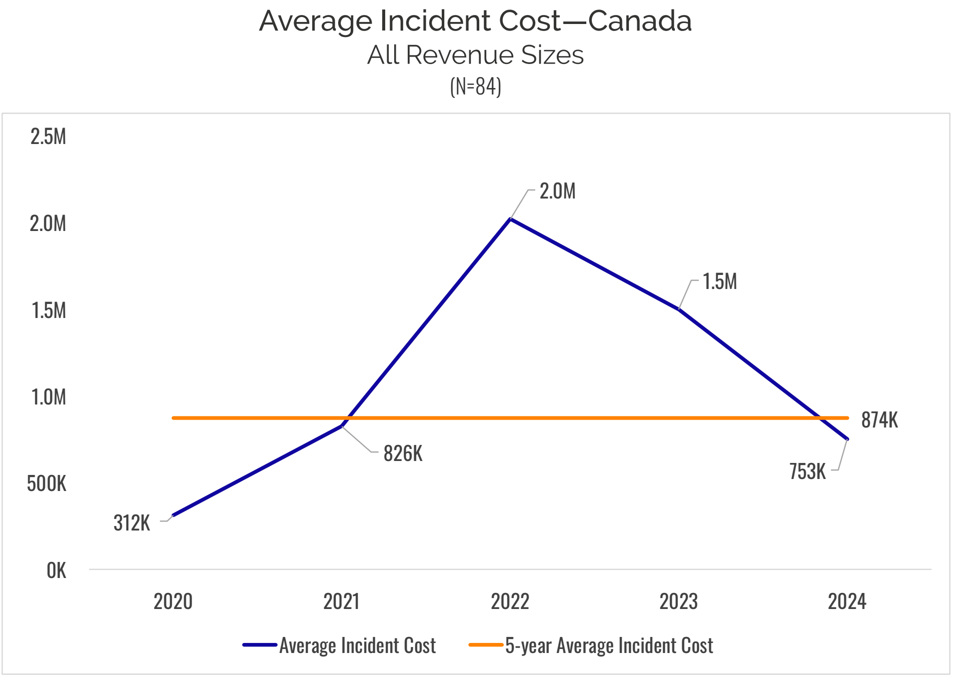

Average Incident Cost—Canada
All Revenue Sizes
(N=84)

Figure 48

Canada
Top Causes of Loss
2020-2024

Cause of Loss	Claims	Average Incident Cost
Ransomware	44	1.3M
Business Email Compromise	13	234K
Hacker	8	66K
Wire Transfer Fraud	6	558K
Staff Mistake	3	39K
Malware/Virus	3	39K
Wrongful Data Collection	1	333K
Rogue Employee	1	8.1M
Lost/Stolen Laptop/Device	1	2K
Other	4	586K

Table 2

In Canada, ransomware remains the leading driver of cyber insurance claims, fueled by criminal groups deploying ever more aggressive extortion tactics. At the same time, wire fraud continues to be a damaging threat, with average incident costs rivaling ransomware due to unrecoverable financial losses. This trend highlights that Canadian organizations face a dual challenge: protecting critical systems from crippling ransomware events while also safeguarding financial operations against social engineering and payment fraud schemes.

Patrick Bourk
Strategic Consultant, NetDiligence

Conclusion

For fifteen years, NetDiligence has raised the bar for presenting and understanding cyber insurance loss for both cyber insurers and other key stakeholders.

This year, over 4,000 new claims were submitted. These were added to an existing dataset of over 6,000 claims. The result has been a comprehensive dataset of cyber claims incidents, including their causes and monetary impacts.

The single, unavoidable takeaway from this study: total incident costs at SMEs are up in almost every category. In last year's study, the five-year average incident cost was $205K. In this year's study, the five-year average was $264K—an increase of almost 30%.

Conversely, at large companies, overall average incident costs have dropped: $10.3M vs. $12.7M for the five-year window, a decrease of 19%.

For the benefit of the industry overall, all underwriters are encouraged to participate in next year's NetDiligence study. All participating insurers are encouraged to share a larger percentage of their cyber claims, especially those for companies with more than $2B in annual revenue. As participation in the study expands in these two ways, its findings will be richer and more representative of changing market conditions.

Insurance Industry Participants

Over the years, many insurance companies have contributed claims data for this study. We thank them all, as without their participation this study would not be possible. Special thanks go to the following companies for contributing a significant number of new claims for the 2025 study.

Allied World

Association of Washington Cities Risk Management Services Agency (AWC RMSA)

At-Bay

Beazley

Berkley Cyber Risk Solutions

CFC

Cowbell

Crum & Forster

Great American Insurance Company

Markel

Sompo

Tokio Marine HCC

Travelers–US

Travelers–Canada

An Invitation to Insurers

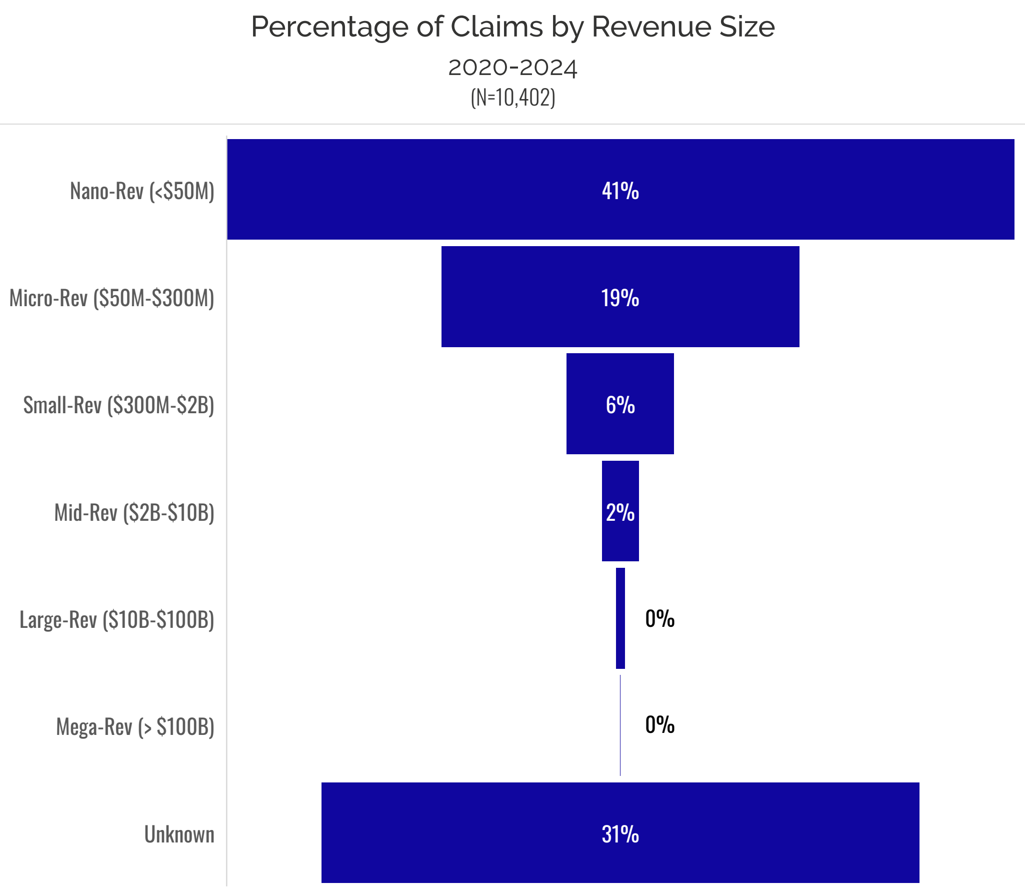
We hope you will consider joining this elite group of participating companies. We'll be starting next year's study in January. Email cyberclaims@netdiligence.com to learn more about participating.

Appendices

Revenue Size

Analysis of claims by annual revenue size of the claimant has been an important part of every NetDiligence study. The graphics and tables below provide insight into the proportion of claims in the dataset for each company size grouping and the costs of crisis services and incidents.

To review: SMEs (companies with annual revenue less than $2B) account for 98% of the claims analyzed and 49% of total incident cost. Large companies (companies with annual revenue greater than $2B) account for only 2% of the claims analyzed but 51% of total incident cost.



Percentage of Claims by Revenue Size
2020-2024
(N=10,402)

Figure 49

Incident Cost by Revenue Size

Claims ≥ $1K

2020-2024

Revenue Size	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Nano-Rev (<$50M)	4,009	1K	142K	10.4M	570.1M	12%	1	6
Micro-Rev ($50M–$300M)	1,775	1K	374K	25.0M	663.1M	14%	3	5
Small-Rev ($300M–$2B)	508	1K	2.0M	108.0M	1.0B	21%	4	4
Mid-Rev ($2B–$10B)	187	1K	5.1M	268.0M	954.3M	20%	5	3
Large-Rev ($10B–$100B)	43	4K	30.5M	503.5M	1.3B	27%	6	2
Mega-Rev (>$100B)	4	10.6M	38.3M	75.0M	153.2M	3%	7	1
Unknown	2,645	1K	47K	2.7M	123.4M	3%	2	7

Table 3

Average Crisis Services Costs by Revenue Size

Claims ≥ $1K

2020-2024

Revenue Size	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Nano-Rev (<$50M)	41K	49K	6K	19K	78K	88K	6
Micro-Rev ($50M–$300M)	83K	69K	37K	30K	150K	186K	5
Small-Rev ($300M–$2B)	240K	279K	130K	125K	308K	610K	4
Mid-Rev ($2B–$10B)	364K	1.1M	161K	72K	833K	2.0M	3
Large-Rev ($10B–$100B)	3.9M	1.2M	0K	3.3M	708K	6.8M	1
Mega-Rev (>$100B)	0K	0K	0K	0K	0K	4.9M	2
Unknown	51K	10K	9K	21K	57K	70K	7

Table 4

Business Sector

Claims are categorized in one of the following nineteen business sectors:

- Agriculture
- Education
- Energy
- Entertainment
- Financial Services
- Gaming & Casino
- Healthcare
- Hospitality
- Manufacturing
- Media
- Nonprofit
- Professional Services
- Public Entity
- Restaurant
- Retail
- Technology
- Telecommunications
- Transportation
- Other

The graphic and tables below provide a detailed look at various metrics by business sector.

Percentage of Claims by Sector
All Revenue Sizes
2020-2024
(N=10,402)

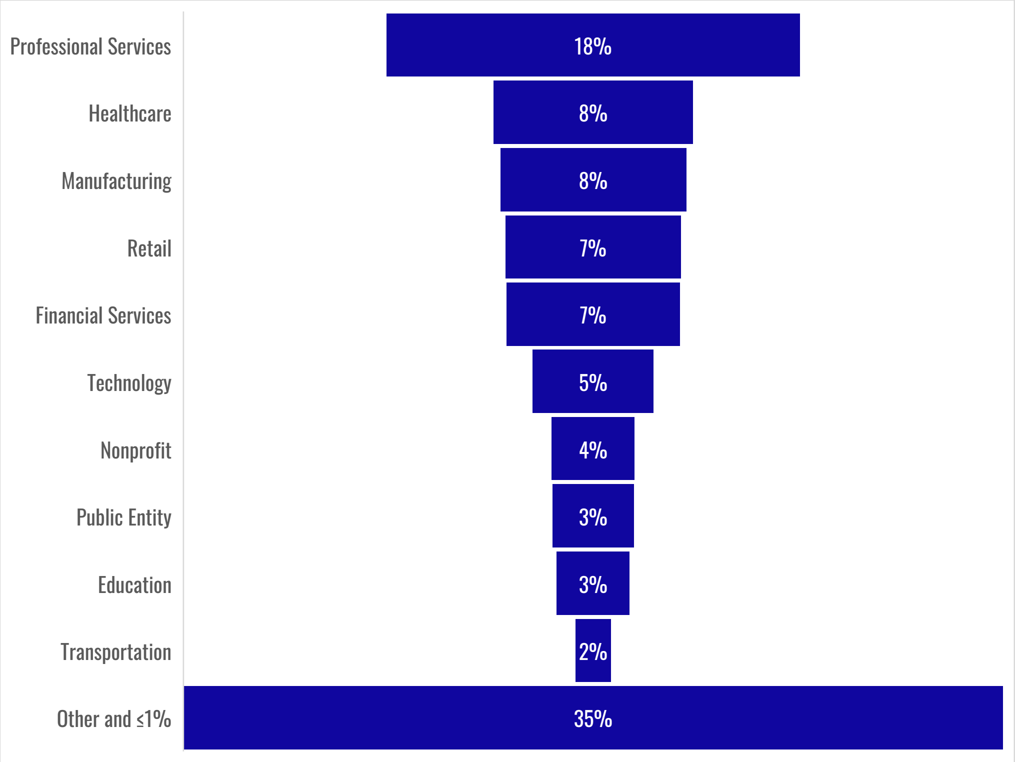


Figure 50

Incident Cost by Sector—SMEs

2020-2024

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Agriculture	55	2K	112K	490K	6.1M	0.3%	15	18
Education	277	2K	172K	12.0M	47.5M	2.0%	10	17
Energy	62	2K	431K	15.0M	26.7M	1.1%	13	9
Entertainment	52	4K	318K	2.6M	16.5M	0.7%	16	12
Financial Services	579	1K	329K	11.5M	190.7M	8.1%	6	11
Gaming & Casino	5	20K	1.6M	4.3M	8.2M	0.3%	19	1
Healthcare	599	1K	566K	105.0M	339.0M	14.4%	5	7
Hospitality	119	2K	182K	3.2M	21.7M	0.9%	12	15
Manufacturing	773	1K	395K	108.0M	305.1M	12.9%	3	10
Media	57	2K	722K	11.0M	41.2M	1.7%	14	4
Nonprofit	370	1K	108K	2.9M	40.1M	1.7%	8	19
Professional Services	1,604	1K	271K	30.0M	434.5M	18.4%	2	13
Public Entity	300	2K	180K	4.0M	53.9M	2.3%	9	16
Restaurant	18	2K	646K	5.2M	11.6M	0.5%	18	5
Retail	623	1K	219K	7.5M	136.7M	5.8%	4	14
Technology	450	1K	876K	26.0M	394.3M	16.7%	7	3
Telecommunications	21	18K	1.6M	8.7M	32.7M	1.4%	17	2
Transportation	142	1K	531K	15.0M	75.4M	3.2%	11	8
Other	2,828	1K	62K	5.2M	176.1M	7.5%	1	20
Unknown	2	174K	566K	1.0M	1.1M	0.0%	20	6

Table 5

Average Crisis Services Costs by Sector—SMEs

2020-2024

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Agriculture	33K	6K	6K	16K	93K	84K	18
Education	62K	13K	10K	19K	103K	101K	15
Energy	143K	3K	1K	42K	118K	188K	7
Entertainment	42K	54K	4K	26K	152K	119K	13
Financial Services	70K	145K	74K	26K	118K	168K	9
Gaming & Casino	83K	7K	0K	36K	39K	629K	2
Healthcare	134K	195K	34K	45K	113K	290K	3
Hospitality	47K	12K	3K	14K	78K	86K	17
Manufacturing	71K	7K	2K	22K	98K	138K	11
Media	53K	10K	1K	18K	139K	143K	10
Nonprofit	57K	22K	5K	19K	71K	81K	19
Professional Services	57K	79K	17K	34K	187K	171K	8
Public Entity	65K	54K	27K	33K	131K	123K	12
Restaurant	105K	138K	18K	27K	84K	225K	5
Retail	52K	34K	6K	23K	104K	112K	14
Technology	83K	109K	54K	48K	102K	211K	6
Telecommunications	234K	1.1M	806K	75K	100K	837K	1
Transportation	60K	7K	4K	42K	164K	241K	4
Other	43K	7K	5K	16K	106K	97K	16
Unknown	0K	44K	0K	30K	0K	74K	20

Table 6

Incident Cost by Sector—Large Companies

2020-2024

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Agriculture	1	5.0M	5.0M	5.0M	5.0M	0.2%	14	9
Education	5	226K	1.1M	2.4M	5.5M	0.2%	8	14
Energy	4	187K	1.9M	5.0M	7.5M	0.3%	10	12
Financial Services	91	2K	1.7M	50.0M	156.4M	6.5%	1	13
Gaming & Casino	2	26.7M	63.3M	100.0M	126.7M	5.2%	11	3
Healthcare	37	3K	17.9M	165.0M	662.6M	27.4%	2	4
Hospitality	1	268.0M	268.0M	268.0M	268.0M	11.1%	14	2
Manufacturing	23	29K	8.5M	55.0M	195.3M	8.1%	3	6
Nonprofit	1	4K	4K	4K	4K	0.0%	14	17
Professional Services	13	72K	3.3M	13.2M	42.3M	1.8%	6	10
Public Entity	2	40K	2.8M	5.5M	5.5M	0.2%	11	11
Restaurant	2	10K	603K	1.2M	1.2M	0.0%	11	15
Retail	16	1K	12.1M	111.0M	193.1M	8.0%	5	5
Technology	21	46K	8.2M	60.0M	171.4M	7.1%	4	7
Telecommunications	1	503.5M	503.5M	503.5M	503.5M	20.8%	14	1
Transportation	5	200K	351K	598K	1.8M	0.1%	8	16
Other	10	25K	7.4M	65.8M	74.0M	3.1%	7	8

Table 7

Average Crisis Services Costs by Sector—Large Companies

2020-2024

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Education	203K	351K	31K	77K	123K	526K	12
Energy	449K	0K	210K	79K	50K	683K	11
Financial Services	4.5M	4.5M	0K	58K	69K	1.6M	8
Gaming & Casino	0K	0K	0K	0K	0K	14.8M	2
Healthcare	181K	2.0M	302K	59K	582K	4.1M	4
Hospitality	0K	0K	0K	0K	0K	24.0M	1
Manufacturing	535K	78K	18K	622K	860K	2.2M	6
Nonprofit	0K	0K	0K	0K	4K	4K	15
Professional Services	284K	1.6M	200K	119K	93K	2.1M	7
Public Entity	0K	0K	0K	0K	0K	520K	13
Restaurant	162K	415K	0K	0K	159K	736K	10
Retail	1.1M	118K	0K	3.0M	1.0M	2.8M	5
Technology	2.2M	0K	0K	500K	3.3M	7.5M	3
Transportation	0K	0K	0K	0K	100K	100K	14
Other	246K	0K	68K	32K	0K	1.5M	9

Table 8

Cause of Loss

Claims are assigned to one of the following twenty-five causes of loss:

- Business Email Compromise
- Cyber Event—Unspecified
- Hacker
- Intellectual Property
- Legal Action
- Lost/Stolen Laptop/Device
- Malware/Virus
- Negligence
- Paper Records
- Phishing
- Privacy Breach
- Programming Error
- Ransomware
- Rogue Employee
- Social Engineering
- Staff Mistake
- System Glitch
- Theft of Money
- Third Party
- Trademark/Copyright Infringement
- Unauthorized Access
- Wire Transfer Fraud
- Wrongful Data Collection
- Other
- Unknown

The graphic and tables below provide a detailed look at various metrics by cause of loss.

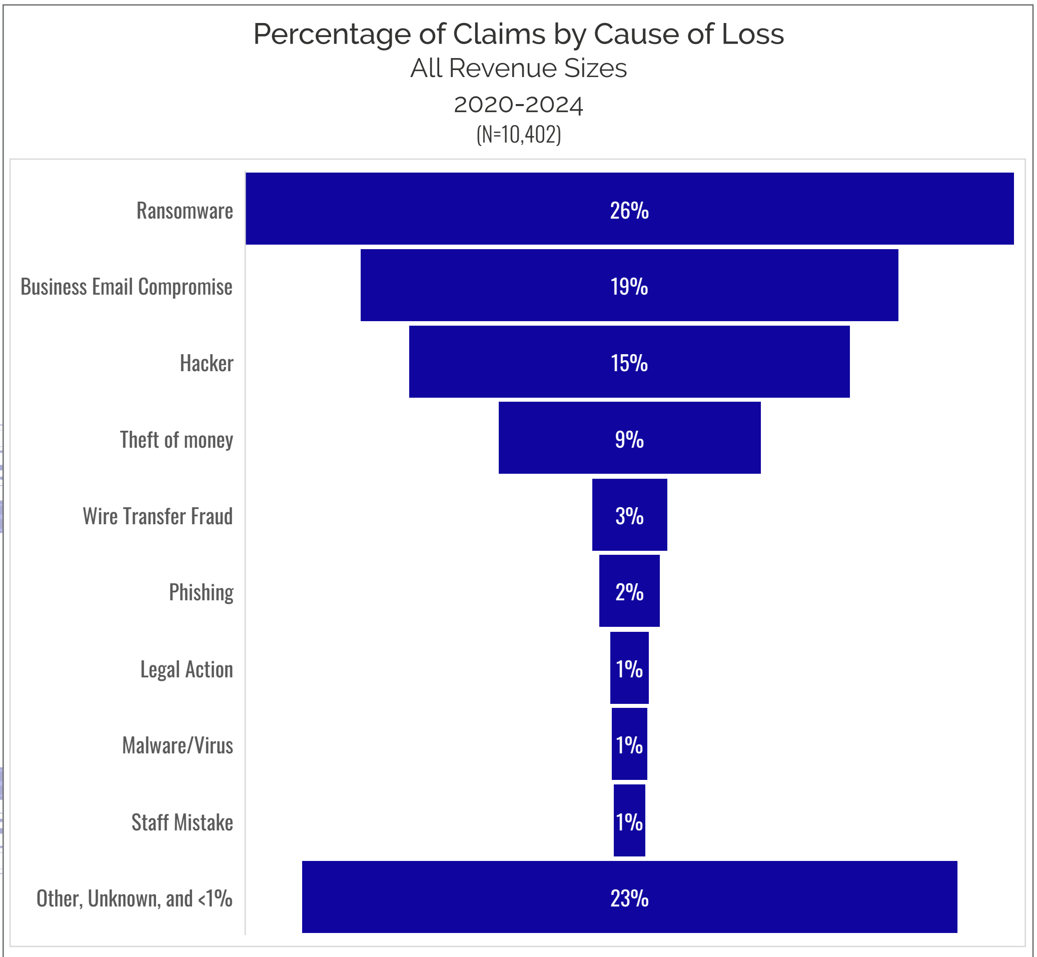


Figure 51

Incident Cost by Cause of Loss—SMEs

2020-2024

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	1,864	1K	98K	30.0M	182.1M	7.7%	2	14
Cyber Event—Unspecified	810	1K	68K	5.0M	55.3M	2.3%	6	18
Hacker	1,191	1K	135K	22.0M	161.4M	6.8%	3	12
Legal Action	51	1K	124K	4.2M	6.3M	0.3%	11	13
Lost/Stolen Laptop/Device	25	1K	44K	341K	1.1M	0.0%	13	20
Malware/Virus	118	4K	77K	1.0M	9.1M	0.4%	9	16
Negligence	1	450K	450K	450K	450K	0.0%	23	5
Paper Records	4	13K	35K	100K	141K	0.0%	19	22
Phishing	159	1K	56K	489K	8.9M	0.4%	8	19
Privacy Breach	2	1.1M	1.5M	1.9M	3.0M	0.1%	21	2
Programming Error	7	12K	149K	515K	1.0M	0.0%	17	11
Ransomware	2,571	1K	631K	108.0M	1.6B	68.8%	1	4
Rogue Employee	38	1K	71K	403K	2.7M	0.1%	12	17
Social Engineering	2	11K	197K	383K	393K	0.0%	21	8
Staff Mistake	74	1K	84K	1.1M	6.2M	0.3%	10	15
System Glitch	18	6K	182K	1.0M	3.3M	0.1%	14	9
Theft of Hardware	13	5K	22K	57K	291K	0.0%	15	23
Theft of Money	834	1K	38K	500K	32.1M	1.4%	5	21
Trademark/Copyright Infringement	3	111K	1.5M	4.1M	4.6M	0.2%	20	1
Wire Transfer Fraud	260	2K	178K	3.8M	46.3M	2.0%	7	10
Wrongful Data Collection	13	15K	826K	5.1M	10.7M	0.5%	15	3
Other	873	1K	229K	11.0M	199.8M	8.5%	4	7
Unknown	5	2K	256K	1.2M	1.3M	0.1%	18	6

Table 9

Average Crisis Services Costs by Cause of Loss—SMEs
2020-2024

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	25K	27K	7K	18K	79K	71K	6
Cyber Event—Unspecified	51K	10K	1K	11K	0K	59K	7
Hacker	52K	86K	20K	25K	21K	84K	3
Legal Action	14K	7K	9K	33K	0K	58K	8
Lost/Stolen Laptop/Device	23K	2K	2K	22K	164K	41K	13
Malware/Virus	20K	116K	2K	8K	105K	47K	11
Paper Records	0K	0K	0K	10K	0K	10K	19
Phishing	21K	3K	1K	14K	0K	31K	16
Programming Error	29K	0K	0K	5K	3K	29K	17
Ransomware	101K	98K	52K	41K	174K	293K	1
Rogue Employee	64K	10K	1K	12K	7K	48K	10
Social Engineering	6K	0K	0K	0K	156K	81K	4
Staff Mistake	16K	19K	5K	18K	41K	33K	15
System Glitch	25K	20K	14K	12K	16K	35K	14
Theft of Hardware	6K	1K	0K	5K	0K	8K	20
Theft of Money	48K	9K	2K	11K	47K	46K	12
Wire Transfer Fraud	15K	0K	0K	14K	140K	52K	9
Wrongful Data Collection	15K	0K	0K	12K	9K	21K	18
Other	26K	134K	19K	21K	83K	72K	5
Unknown	0K	0K	0K	11K	0K	87K	2

Table 10

Incident Cost by Cause of Loss—Large Companies

2020-2024

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	9	21K	334K	1.2M	3.0M	0.1%	6	12
Cyber Event—Unspecified	2	226K	653K	1.1M	1.3M	0.1%	12	8
Hacker	12	13K	3.0M	14.5M	35.7M	1.5%	5	5
Lost/Stolen Laptop/Device	1	32K	32K	32K	0.0M	0.0%	14	14
Malware/Virus	6	13K	1.1M	5.7M	6.8M	0.3%	7	6
Privacy Breach	1	8K	8K	8K	8K	0.0%	14	16
Ransomware	104	1K	21.1M	503.5M	2.2B	90.8%	1	1
Rogue Employee	3	55K	7.1M	13.2M	21.3M	0.9%	9	3
Social Engineering	3	17K	27K	39K	82K	0.0%	9	15
Staff Mistake	18	2K	284K	5.0M	5.1M	0.2%	4	13
Theft of Money	3	187K	553K	1.2M	1.7M	0.1%	9	10
Third-Party Incident	1	7.5M	7.5M	7.5M	7.5M	0.3%	14	2
Unauthorized Access	33	2K	3.1M	101.0M	102.0M	4.2%	2	4
Wire Transfer Fraud	4	125K	644K	1.6M	2.6M	0.1%	8	9
Wrongful Data Collection	2	10K	505K	1.0M	1.0M	0.0%	12	11
Other	33	3K	1.1M	12.6M	34.8M	1.4%	2	7

Table 11

Average Crisis Services Costs by Cause of Loss—Large Companies

2020-2024

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	11K	15K	0K	28K	366K	247K	9
Hacker	181K	2.6M	0K	130K	313K	1.1M	5
Lost/Stolen Laptop/Device	19K	0K	0K	13K	0K	32K	11
Malware/Virus	448K	4.5M	0K	288K	83K	3.0M	4
Ransomware	1.5M	711K	116K	788K	1.1M	4.8M	3
Rogue Employee	9K	13K	0K	33K	0K	5.0M	1
Staff Mistake	0K	0K	0K	5K	0K	284K	8
Theft of Money	162K	415K	0K	0K	159K	736K	7
Third-Party Incident	0K	0K	0K	0K	0K	5.0M	2
Wire Transfer Fraud	0K	0K	0K	0K	75K	75K	10
Other	273K	2.4M	521K	110K	73K	844K	6

Table 12

Type of Data

All claims are assigned to one of the following types of data:

- Email—Unspecified
- Files—Critical
- Intellectual Property
- Non-Card Financial
- Other Non-Public Data
- PCI
- PHI
- PII
- Trade Secrets
- User Credentials (Login & Passwords)
- User Online Tracking
- Other
- N/A
- Unknown

Because a large percentage of incidents (ransomware, DDoS, and wire transfer fraud) do not expose records at all, a new category was created in 2018 to capture these incidents. This category is "Files—Critical". An example of an incident with "Files—Critical" data would be a ransomware event that locked a database, system, or network deemed essential.

The graphic and tables below provide a detailed look at various metrics by type of data.

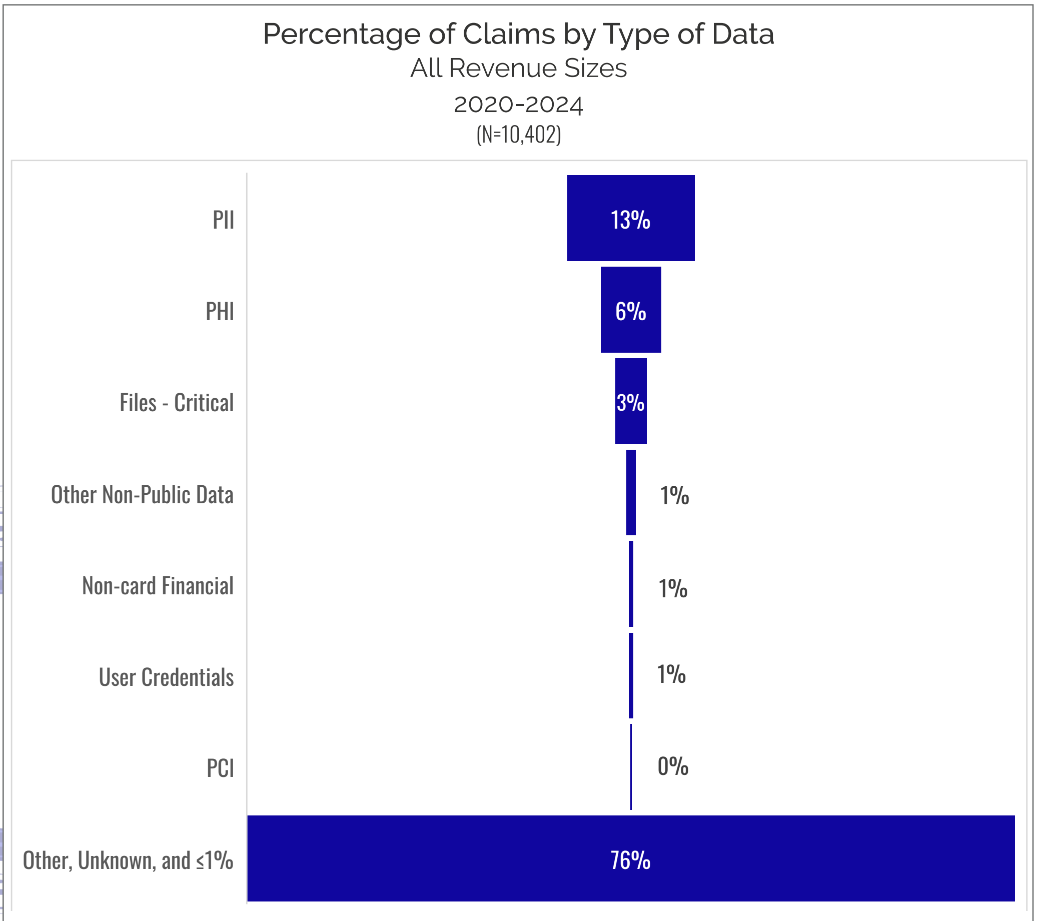


Figure 52

Incident Cost by Type of Data—SMEs

2020-2024

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Email—Unspecified	14	3K	52K	200K	724K	0.0%	11	17
Files—Critical	290	2K	276K	4.7M	80.1M	5.5%	5	13
Intellectual Property	6	26K	4.5M	13.6M	27.1M	1.9%	14	2
Non-Card Financial	49	2K	700K	7.0M	34.3M	2.4%	8	10
Other Non-Public Data	87	1K	1.1M	15.0M	92.7M	6.4%	6	6
PCI	15	1K	339K	2.3M	5.1M	0.3%	10	12
PHI	370	1K	794K	105.0M	294.0M	20.2%	4	8
PII	1,132	1K	631K	108.0M	714.6M	49.2%	2	11
PII & PHI	7	49K	3.9M	20.0M	27.5M	1.9%	12	3
PII, Non-Card Financial	1	761K	761K	761K	761K	0.1%	16	9
Trade Secrets	7	250K	931K	2.1M	6.5M	0.4%	12	7
User Credentials	39	1K	196K	1.3M	7.6M	0.5%	9	14
Video viewing data	2	4.2M	4.6M	5.1M	9.3M	0.6%	15	1
None	1	2.6M	2.6M	2.6M	2.6M	0.2%	16	4
N/A	498	1K	165K	5.2M	82.0M	5.6%	3	15
Other	66	7K	1.3M	30.0M	85.4M	5.9%	7	5
Unknown	6,352	1K	140K	26.0M	888.9M	61.2%	1	16

Table 13

Average Crisis Services Costs by Type of Data—SMEs
2020-2024

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Email—Unspecified	14K	4K	0K	9K	157K	42K	16
Files—Critical	65K	57K	1K	22K	57K	107K	13
Intellectual Property	167K	0K	0K	15K	521K	2.0M	2
Non-Card Financial	178K	95K	783K	82K	92K	300K	6
Other Non-Public Data	166K	20K	3K	53K	61K	349K	5
PCI	171K	40K	20K	136K	34K	235K	8
PHI	168K	297K	143K	82K	92K	522K	4
PII	135K	140K	25K	46K	84K	269K	7
PII & PHI	102K	51K	0K	58K	42K	191K	10
PII, Non-Card Financial	0K	0K	0K	17K	0K	111K	12
Trade Secrets	77K	6K	1K	93K	50K	224K	9
User Credentials	68K	28K	0K	21K	20K	77K	14
None	0K	0K	0K	0K	0K	2.5M	1
N/A	22K	11K	0K	9K	52K	46K	15
Other	114K	1.2M	369K	261K	835K	848K	3
Unknown	49K	29K	5K	19K	121K	113K	11

Table 14

Incident Cost by Type of Data—Large Companies

2020-2024

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Files—Critical	5	3.3M	19.3M	55.0M	96.6M	4.2%	6	3
Intellectual Property	3	24K	455K	1.3M	1.4M	0.1%	8	12
N/A	11	25K	1.1M	5.0M	12.0M	0.5%	4	11
Non-Card Financial	1	1.3M	1.3M	1.3M	1.3M	0.1%	9	10
Other Non-Public Data	7	1K	2.6M	13.2M	18.2M	0.8%	5	8
PHI	25	22K	18.7M	101.0M	467.1M	20.5%	3	4
PHI, PII, SSN, DL	1	12.0M	12.0M	12.0M	12.0M	0.5%	9	5
PII	76	2K	20.0M	503.5M	1.5B	66.7%	2	2
User Credentials	5	13K	27.3M	111.0M	136.3M	6.0%	6	1
None	1	7.5M	7.5M	7.5M	7.5M	0.3%	9	7
Other	1	8.1M	8.1M	8.1M	8.1M	0.4%	9	6
Unknown or N/A	99	2K	1.4M	33.5M	137.9M	6.0%	1	9

Table 15

Average Crisis Services Costs by Cause of Loss—Large Companies

2020-2024

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Files—Critical	338K	0K	0K	45K	13K	2.0M	4
Intellectual Property	568K	0K	14K	69K	0K	644K	7
Other Non-Public Data	304K	0K	0K	29K	40K	1.9M	6
PHI	133K	2.1M	94K	79K	753K	2.0M	5
PHI, PII, SSN, DL	0K	0K	0K	0K	0K	10.0M	1
PII	1.3M	901K	204K	543K	897K	4.1M	2
User Credentials	108K	0K	0K	11K	0K	83K	9
N/A	119K	415K	0K	4K	117K	203K	8
Unknown or N/A	2.7M	55K	161K	739K	1.0M	2.0M	3

Table 16

AI and Third-Party Incidents:

Reshaping the Cyber Insurance Landscape

Sean B. Hoar, Partner & Chair, Constangy Cyber Team

As artificial intelligence (AI) revolutionizes the ways in which we work and communicate, its integration into business operations creates new risks that are reshaping the cyber insurance landscape. Coupled with the persistent threat of third-party vulnerabilities, cyber insurers are facing unprecedented challenges in accurately assessing emerging risks. By embracing a more agile approach to underwriting and requiring more programmatic "skin in the game" from insureds, cyber insurers can preserve or increase market share, protect or reduce loss ratios, and contribute to a more secure digital environment.

AI-Driven Risks

AI technologies, particularly generative models and autonomous systems, are becoming integral to modern business. Their complexity and unpredictability, however, create novel liability risks. AI systems have produced false, biased, and infringing outputs, leading to potential liability for professional malpractice, data privacy violations, defamation, misinformation and intellectual property infringement. The malicious use of AI has resulted in the explosive growth of criminal attacks on corporate networks. Credential phishing attacks increased over 700% in the latter half of 2024 with over 80% of phishing email messages using AI technology, and phishing campaigns being deployed 40% faster using generative AI. Ransomware attacks have increased over 125% this year and a percentage of them involved the malicious use of AI. AI-driven deepfakes are being used to bypass facial recognition and other verification systems, and AI-powered voice cloning tools are being successfully used in social engineering attacks.

Malicious attacks involving AI have serious consequences. Over the past three years, significant incidents involving AI affected the financial, technology and healthcare sectors. Some examples:

- Several major financial institutions experienced AI-powered phishing attacks that compromised a substantial amount of customer data,
- A cloud service provider's AI as a service (AIaaS) platform was exploited to conduct surreptitious user surveillance,
- A social media platform was involved in a misinformation campaign using deepfake videos and bots,
- An e-commerce company experienced data poisoning in which false data was injected into consumer facing systems,
- A healthcare provider's AI system was compromised, resulting in incorrect diagnoses and treatment plans.

Third-Party Incidents

While AI is an emerging and yet unpredictable risk, third-party vulnerabilities have repeatedly shown their devastating impact across business sectors. Studies found that third-party incidents in 2024 resulted in almost one-third of cyber insurance claims, and almost two-thirds of the incidents in the insurance sector. The reality is that certain business sectors rely upon only a few common third-party providers for core applications and systems. If any one of those providers experiences an incident, it could adversely impact a substantial portion of the business sector. As an example, a third-party incident in the healthcare sector did just that in 2024—affecting thousands of providers and millions of consumers. A survey of nearly 1,000 hospitals about the incident found that 74% incurred a direct impact on patient care, 94% reported a financial impact with 33% reporting over half their revenue was disrupted, and 60% reported requiring between two weeks and three months to resume normal operations. Other major incidents in 2024 affected thousands of businesses in the automobile industry and millions of students and educators in the education sector.

The Regulatory Environment

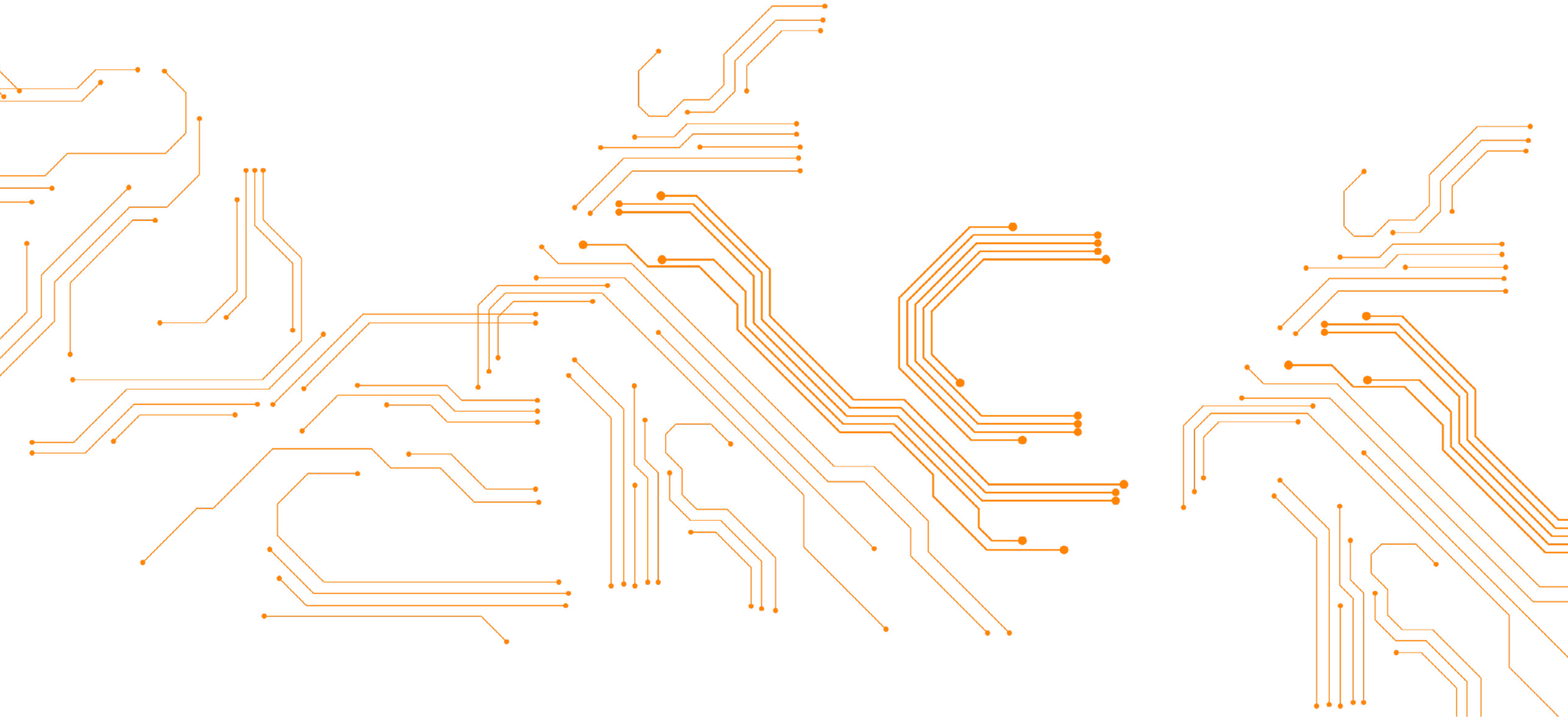
The developing regulatory environment regarding AI involves numerous states and federal agencies. Over 20 states have introduced AI-related legislation and federal agencies have initiated AI-related enforcement actions. The legislation and enforcement actions have focused on consumer protections when AI is used for profiling, automated decisions, employment decisions, and when it results in disinformation or "deepfakes" affecting people and activities. Similar to information security mandates, some AI legislation requires governance programs to implement protections. As an example, the Colorado AI Act requires AI developers and deployers to implement AI governance programs. Furthermore, it requires AI developers to identify and apprise deployers of known or foreseeable risks within their AI system and report to the Colorado attorney general and known deployers within 90 days of learning about the occurrence of algorithmic discrimination. Although there is potential liability for lack of compliance, the immediate costs will likely be from increased infrastructure and operational expenses for governance systems.

Reshaping the Cyber Insurance Landscape

Cyber insurers should take a cue from regulators and require AI developers and deployers to maintain AI governance systems. Legitimate systems must have administrative and information security programs to mitigate risk, and requiring such programs is only responsible. This may help manage risk, limit claims, and contribute to a more secure digital environment. Regardless of how cyber insurers respond to the convergence of AI-driven risks and third-party incidents, however, these forces are reshaping the cyber insurance landscape.

About Constangy, Brooks, Smith & Prophete LLP

The Constangy Cyber Team is composed of over 85 members, including nearly 60 attorneys, offering a full suite of cybersecurity and data privacy services. These include compliance advisory (proactive services), incident response (over 3,000 incidents annually), and litigation (defending class actions in over 30 states). In 2025, the team was recognized by *Intelligent Insurer* as "Law Firm of the Year."



When Ripples Become Waves:

Why Third-Party Breaches and AI Threats Demand a New Response Strategy

Michael Bruemmer, Head of Global Data Breach and Vice President of Consumer Protection, Experian

Toss a stone into still water and the ripples spread far beyond the initial splash. The same is true in today's cyber landscape. A single point of compromise, whether it's a vulnerability in a partner's software, a misconfigured cloud setting, or an AI-powered bot attack, can set off cascading effects well beyond the original breach.

Increasingly, we're seeing these ripples evolve into waves. At Experian®, we're on the frontlines of breach response, and we've seen a rise in supply chain breaches impacting not just one organization, but multiple, through shared digital ecosystems. Third-party attacks, supply chain failures, and AI-fueled exploits are no longer emerging threats; they're defining characteristics of the modern breach.

Third-party breaches are growing

We've seen it time and time again in our breach response work: Third-party and supply chain breaches are no longer isolated events; they ripple across entire networks. In 2024, 32% of the breaches Experian supported were tied to third- or fourth-party exposures.

These breaches can start with something small: an unmonitored credential, a delayed patch, or a misconfigured cloud setting. But when attackers move laterally through trusted integrations, they gain access to far more systems and data. The impact is growing. According to IBM's 2025 Cost of a Data Breach Report, U.S. data breaches now cost an average of $10.22 million, and third-party vulnerabilities continue to be among the most expensive to remediate.

Organizations are increasingly being held accountable for breaches in environments they don't directly manage. Breach readiness must expand beyond your internal network to every vendor, contractor, and platform in your digital supply chain.

AI is accelerating both sides of the threat equation

We're in an AI arms race. Cybercriminals are using generative tools to launch scalable, hyper-personalized attacks faster than ever, automating phishing, credential stuffing, and deepfake social engineering. But on the defense side, adoption isn't keeping pace. According to Experian's 2025 U.S. Identity & Fraud Report, only 37% of companies are currently using AI, including generative AI, to fight fraud. And the pressure is building. In fact, 72% of business leaders expect AI-generated fraud and deepfakes to rank among their top operational challenges by 2026, further widening the gap between threat acceleration and organizational readiness.

And the stakes are rising. According to the same Experian report, the FTC reported a record $12.5 billion in consumer losses to fraud—a 25% increase over the previous year. The FBI echoed this trend, citing a 60% spike in fraud losses to businesses.

At Experian, our frontline experience in breach response has shaped a readiness approach that emphasizes speed, clarity, and control—critical elements in an age where AI accelerates both attacks and responses. As attackers leverage AI to move faster, breach response must evolve to match that pace. Our data breach response services help organizations prepare for and manage high-stakes incidents with agility, minimizing operational and reputational fallout.

It's also about trust. More than 80% of consumers expect companies to act when they raise security or privacy concerns, underscoring the stakes of inaction. Closing the gap between awareness and readiness demands more than tools: it requires education, governance, and a coordinated strategy that puts people and speed at the center of AI-era defense.

The human factor still matters

The 2025 *NetDiligence Cyber Claims Study* lists ransomware, BEC, and hacking as the top causes of loss. "Staff mistakes," by comparison, accounted for only 88 claims in 2020-2024—a steep drop from 150 reported in 2019-2023 and 235 in 2018-2022.

But in breach response, we often see a more layered story. Many top-coded incidents begin with a misstep: a phishing email clicked, a password reused, an MFA prompt ignored. These may not appear in the final claim, but they often serve as the breach's ignition point.

Root cause and coded cause don't always align. Most claims reflect how a breach was detected, not what enabled it. That disconnect can obscure the role of human behavior.

Addressing this gap requires more than controls. It takes ongoing education, simulation, and a culture where accountability and preparedness are shared across every layer of the organization.

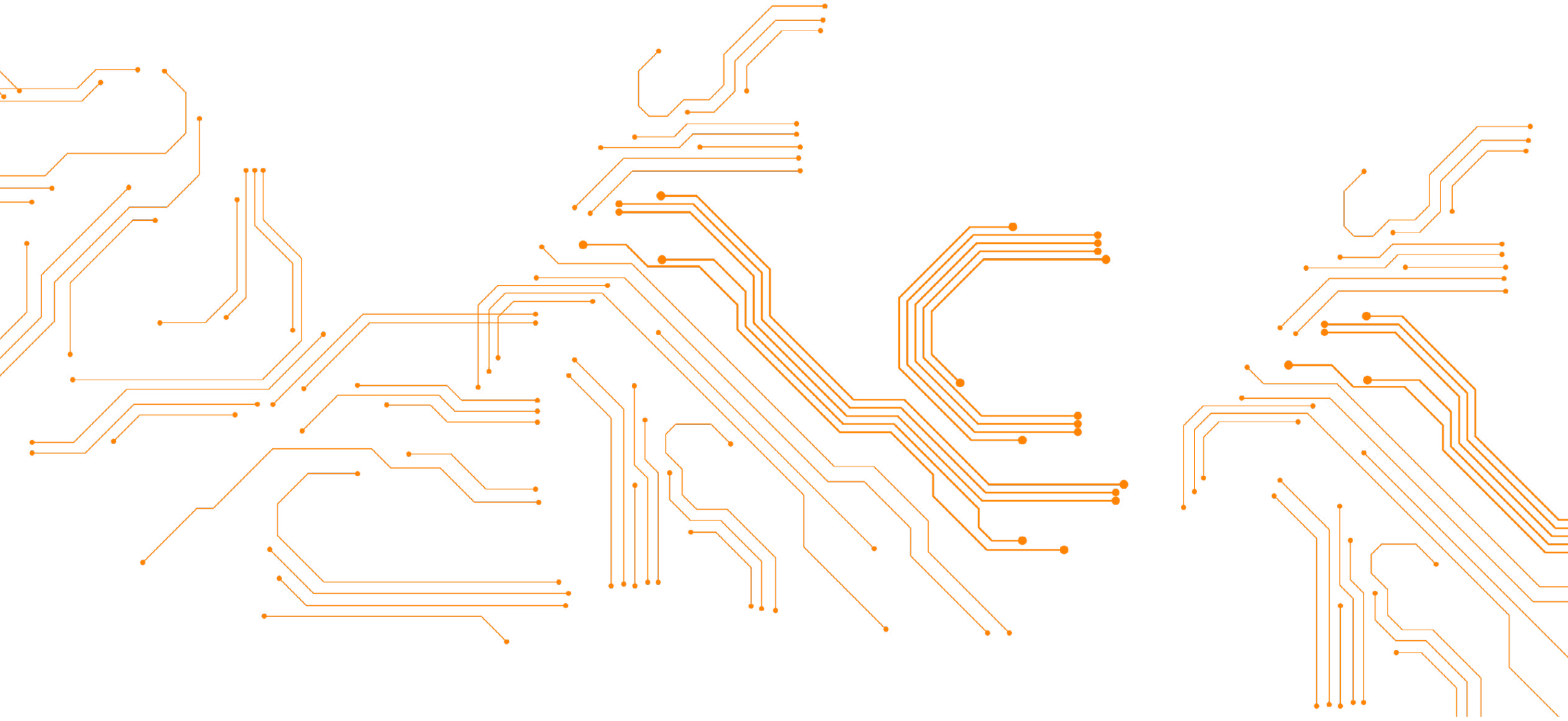
Looking forward

The threat landscape in 2025 is marked by speed, scale, and shared exposure. From AI-powered attacks to supply chain compromises, the risk environment is growing more complex and more connected by the day. But so are the opportunities to respond better. Organizations that embrace ecosystem-wide readiness, operationalize AI responsibly, and elevate human-layer defenses will be the ones most prepared to weather what's next.

At Experian, we've seen that cyber resilience isn't defined by whether a breach occurs, but by how effectively and quickly you respond. The ripple effects may be inevitable. But with the right strategy, tools, and partners, they don't have to become waves.

About Experian

When every minute counts, count on Experian Data Breach Resolution for the partnership, solutions, and performance to create the best possible outcome. With 20+ years' experience, we've managed some of the largest and highest-profile breaches in history. Our turnkey offerings include Experian Reserved Response™, data breach response, crisis response management, and identity protection. Discover more at http://www.experian.com/databreach or email databreachinfo@experian.com



Creating a Blueprint for Cybersecurity Resilience

Measures to reduce the likelihood of attacks and limit their impact

George Kohlhofer, Principal, Cybersecurity and Privacy Risk, RSM US LLP

The current cybersecurity threat environment is an ongoing critical challenge for companies in all industries. Threat actors are leveraging emerging innovations such as artificial intelligence to launch sophisticated attacks, and an increasing reliance on vendors and third parties can create additional vulnerabilities without effective protective measures in place. With recovery costs never higher and reputational risks and regulatory requirements on the rise, companies need to take a proactive approach to protecting their sensitive data and intellectual property.

Nearly one in five companies (18%) reported experiencing a data breach in the last year in the RSM US Middle Market Business Index Special Report: Cybersecurity 2025. With the frequency and evolving nature of cybersecurity attacks, the likelihood that a company will face a breach attempt is high. Therefore, companies need to implement a double-faceted strategy to counter potential risks—taking actions to limit the company's attack surface and establishing an effective resiliency plan for when an attack occurs.

The following five steps can help companies focus on these two main goals and establish an effective foundation to strengthen ongoing cybersecurity efforts.

Double down on fundamental protections

Companies need to invest in strong identity management (multi-factor authentication, access governance and user training) as a first line of defense. Data shows that these controls can reduce internal mistakes and blunt many attacks before they can cause harm.

Manage vendors and third parties

Cybersecurity should be treated as a team sport across the supply chain. Companies should perform comprehensive due diligence on vendor and partner security practices and demand improvements where weaknesses are found. Sharing threat information and requiring incident notification from vendors can buy time to respond. It's important to remember that an attack on any one of a company's providers or vendors can create significant ramifications for their business, as seen in recent supply chain ransomware events that have affected thousands of organizations.

Embrace the cloud securely

The cloud can offer enterprise-grade security capabilities, but only if configured and used correctly. Companies should leverage cloud providers' security tools—from encryption to continuous monitoring—and consider trusted advisors or managed services providers to fill any gaps in cloud security know-how. Companies can't assume cloud data is safe simply by default; it should always be verified. Regular audits for misconfigurations should take place as well as periodic practice to recover from cloud backups in case a ransomware strike occurs.

Stay ahead of emerging threats

Organizations must stay informed about how new technologies like AI can introduce novel threats. For example, protocols should be in place to verify unusual requests (especially those made over phone or email) through secondary channels to counter evolving deepfake scams. What might have seemed like an outlier attack technique just a year ago can quickly become commonplace and extremely harmful. Incorporating threat intelligence into organizational security strategies can help companies anticipate shifts (for instance, the recent surge in business email compromise tactics).

Incident response and resilience

Finally, companies need to accept that no defense is 100% secure and increase focus on resilience. An incident response plan should be developed, implemented, and regularly updated to reflect the current threat environment. This plan should include specific playbooks for major attack types highlighted in the NetDiligence and RSM US reports—ransomware lockdowns, business email compromises and third-party breaches. In addition, companies should conduct regular tabletop exercises with their cybersecurity team to ensure everyone understands how threats can manifest themselves and what their role is when a crisis hits. Also, cyber insurance should be a key consideration of a thorough risk mitigation strategy, although insurance should be viewed as a safety net, not a substitute for good security practices.

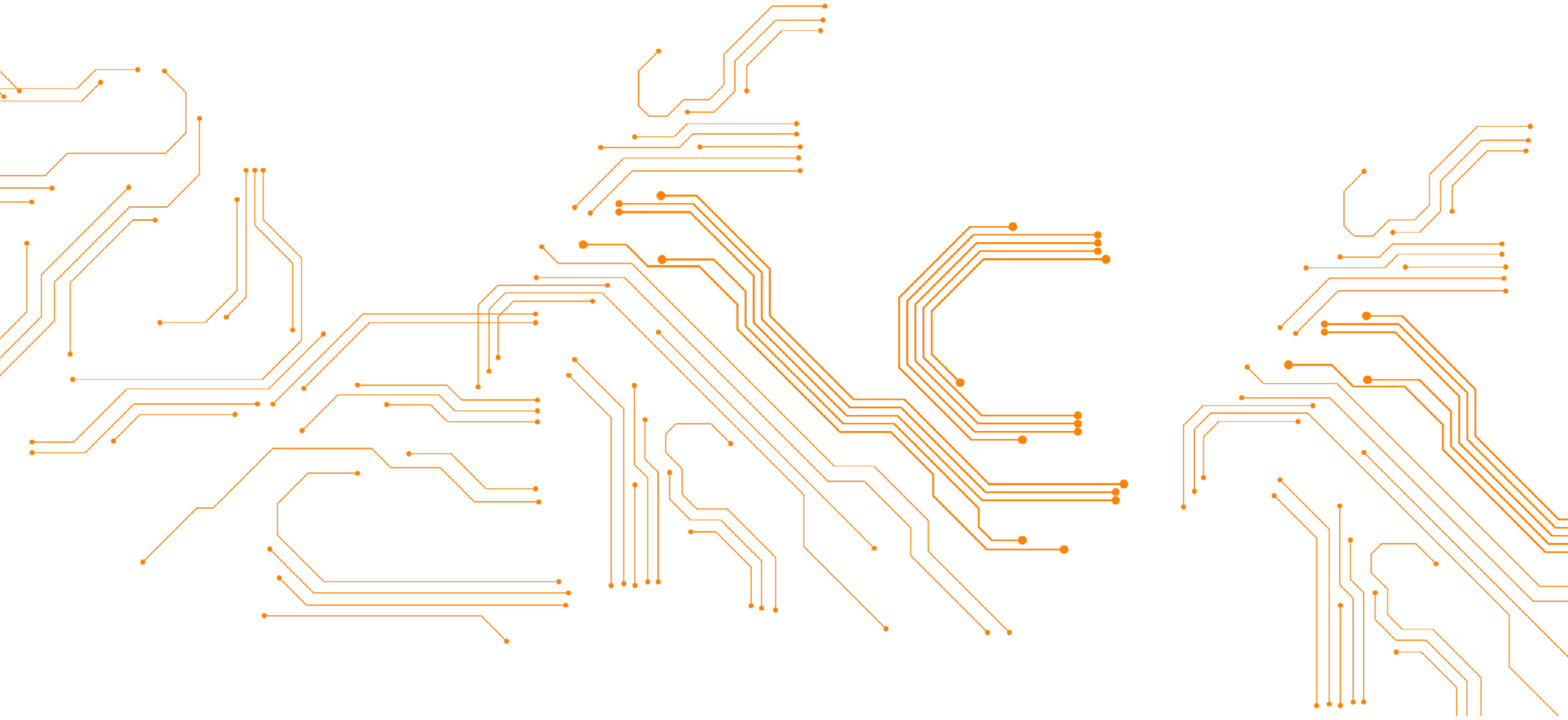
Conclusion

No matter how effective and mature a company's control environment and cybersecurity defenses are, nobody is completely immune to a data breach. Threat actors also have an extensive number of advanced tools at their disposal and are quick to act on any gaps or vulnerabilities, whether an opening comes from unpatched servers, compromised security credentials, or insufficient security at a vendor or supplier.

Protecting data and safeguarding sensitive information presents an increasing challenge, but with the level of risks and costs involved, companies must be agile and proactive to stay ahead of those that seek to do harm. By shrinking the overall attack surface and establishing a more resilient environment, companies can mitigate current and future risks and limit damage if and when an attack occurs.

About RSM US LLP

RSM is the leading provider of professional services to the middle market. The clients we serve are the engine of global commerce and economic growth, and we are focused on developing leading professionals and services to meet their evolving needs in today's ever-changing business landscape. For more information, visit rsmus.com, like us on Facebook, follow us on X and/or connect with us on LinkedIn.



Changing Ransomware Outcomes for Small Businesses

Billy Gouveia, CEO, Surefire Cyber

Small businesses carry a disproportionate share of the ransomware burden. When attacks hit, they suffer the most—not only in direct financial losses, but also operational disruption.

Compounding the issue, small businesses are the least likely to have access to timely and meaningful intelligence that could help them protect themselves. It's not simply about buying a tool or subscribing to a feed. Small businesses often lack the time, resources, and expertise to keep up with the constant shifts in ransomware.

This is where the insurance ecosystem can make a tangible difference—by helping them cut through the noise and focus on high-impact insights that genuinely improve their security posture.

The Unpredictability of Ransomware Groups

If 2024 proved anything, it's that ransomware is anything but predictable. The disappearance of LockBit and BlackCat created a vacuum quickly filled by a rotating cast of threat actors, each with different tactics, levels of sophistication, and success rates.

For claims teams, this volatility made it impossible to treat all incidents the same. Some groups were more likely to publish stolen data, others pushed aggressive ransom demands, offered steep discounts, or settled quickly. Their tactics, professionalism, and behaviors vary widely, and knowing exactly who you're facing is central to managing negotiations and claims effectively.

Early 2025 has shown a continuation of this behavior, though perhaps slightly more controlled. We've seen groups taken over in hostile "mergers" of criminal enterprises. Others disappeared entirely, only to resurface months later under the same or new branding.

Yet amid the chaos, there's been a slight stabilizing trend. Groups like Akira and Qilin have sustained a steady presence, showing consistency in operations and tactics. This consistency presents both opportunity and risk: patterns can be studied and anticipated, but these groups also have the chance to refine their methods, making them harder to counter over time.

Relevancy to Negotiation and Claims

Not all threat actors are created equal. They differ in fundamental ways:

- ***Ransom demands:*** Some start high and negotiate aggressively; others set a price and won't budge.
- ***Data leak threats:*** For some, a promise to publish stolen data is bluff; for others, it's part of their playbook.
- ***Operational impact:*** Certain groups cause longer downtime and broader disruption, leading to higher indirect costs.

These differences directly influence negotiation strategies, claims assessments, and recovery timelines. Without timely and accurate intelligence on a group's behavior, insurers risk overpaying, delaying resolution, or misjudging the true scope of damage.

Data as the Driver of Adaptability

Effective negotiation starts with credible and current data. Determining whether a ransom is reasonable means knowing a group's history of demands, past behavior, and whether their threats carry weight.

The same applies to understanding how the incident occurred—phishing, credential theft, or brute-force attack—since root cause analysis directly impacts claims handling and informs underwriting.

For example, 2024 saw a sharp rise in brute-force activity fueled by automation tools in the hands of cyber criminals. This shift fundamentally changed the speed and scale of certain attacks, and only those closely monitoring the data saw it in real time.

From Raw Data to Actionable Intelligence

The insurance ecosystem has access to a vast amount of threat intel from digital forensics and incident response firms and intelligence providers. While the industry is gathering more than ever, data on its own doesn't drive better outcomes.

Challenges remain in classifying incidents consistently, ensuring data is comparable across cases, and capturing it quickly enough to stay relevant. Just as important is translating that data into clear, actionable intelligence.

That's the differentiator. A spreadsheet of statistics won't help negotiations, but intelligence framed in the context of current threat activity can shape underwriting decisions, steer negotiation strategy, and accelerate recovery. For carriers, that translates into faster resolution and reduced claims costs.

The ransomware landscape is volatile, and it isn't slowing down. For the insurance ecosystem, the ability to adapt quickly—guided by targeted, real-time intelligence—is no longer a nice-to-have. It's the foundation of effective claims handling, underwriting, and client service.

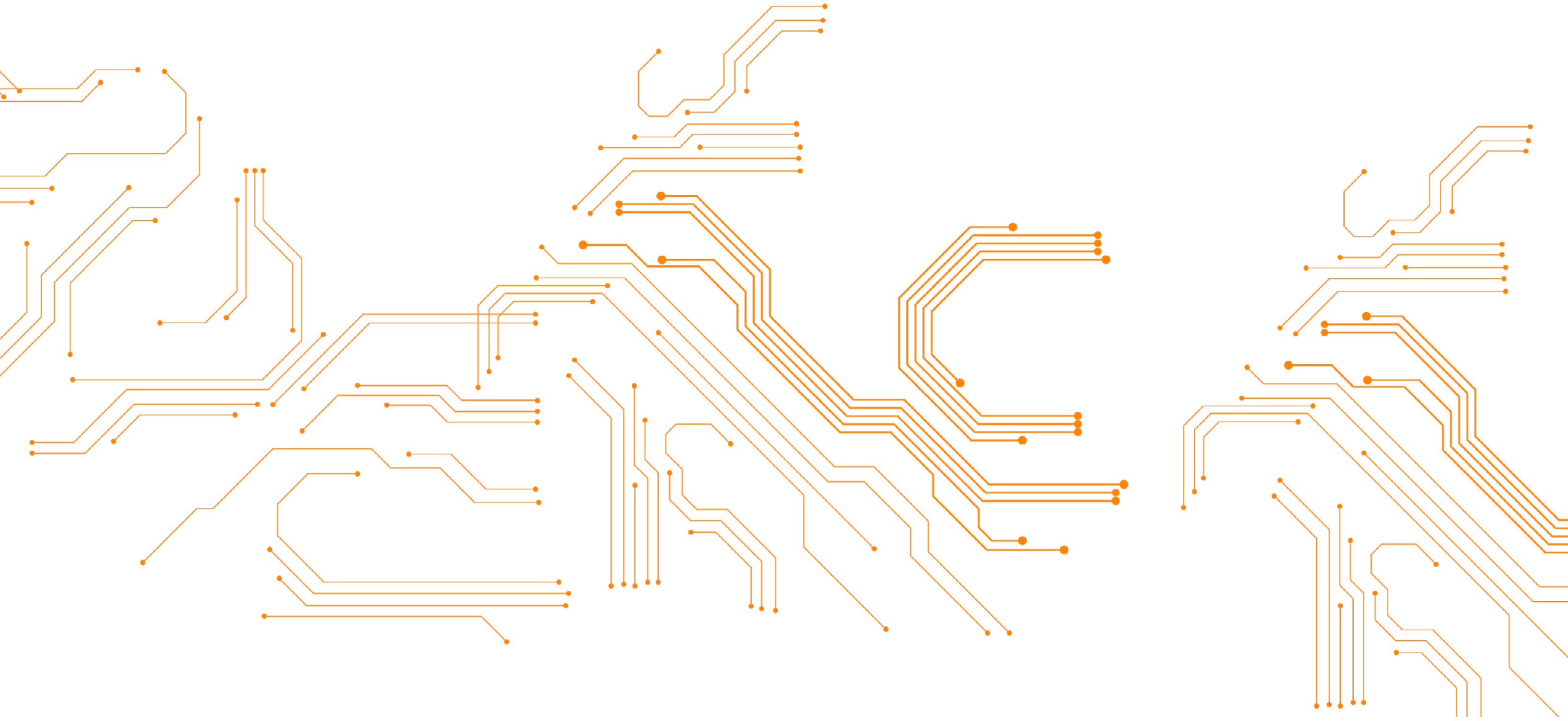
For small businesses, this approach can be transformative. Distilled, relevant insights from their insurer allows them to make informed decisions. For insurers, it's an opportunity to protect clients and improve outcomes in an increasingly high-stakes cyber environment.

The bottom line: data is only as valuable as the decisions it enables. In ransomware response, the difference between a chaotic, costly incident and a measured, cost-effective resolution comes down to how quickly—and how well—intelligence is put into play.

About Surefire Cyber

Surefire Cyber is redefining the incident response model by delivering a swifter, stronger response to cyber incidents such as ransomware, email compromise, malware, data theft, and other threats. Our client-centric approach reduces stress and provides clients the confidence needed to prepare, respond, and recover from cyber incidents—and fortify their cyber resilience after an event.

SUREFIRE CYBER



About NetDiligence®

NetDiligence® is a trusted leader in Cyber Risk Readiness & Response—serving the cyber insurance ecosystem for over two decades. Since 2001, we've helped insurers, brokers, and policyholders reduce the impact of cyber incidents with proven tools, services, and education rooted in real-world claims data.

Our mission is twofold: **proactively support cyber resilience** and **empower swift, effective response** when incidents occur. From benchmark research and interactive tools to policyholder portals and mobile apps, our solutions help make cyber risk more manageable—and insurable.

Breach Response, Ready When You Need It

Breach Plan Connect® is a dynamic, cloud-hosted incident response solution designed to keep organizations operational in the face of a cyber crisis. Pre-loaded with expert-vetted best practices and fully customizable, it helps teams respond decisively to ransomware, BEC, and more.

Key features include guided plan-building, integrated breach response playbooks, and a **mobile app** for anytime-anywhere access—even when systems are compromised. It's trusted by insurers, IT leaders, and legal teams to turn chaos into clarity during critical moments.

A Smarter Portal for Cyber Policyholders

The eRiskHub® is more than just a policyholder resource—it's an interactive cyber risk management platform that insurers use to **educate, empower, and differentiate** their cyber product. Fully white-labeled and customizable, it delivers threat intelligence, risk tools, breach response vendors, and much more.

With over 70,000 users globally, eRiskHub helps insureds build readiness—and insurers control loss ratios.

Cyber Risk Assessments Beyond the Checklist

Our QuietAudit® suite of assessments helps organizations truly understand their cyber risk exposure—not just check a compliance box. We combine deep-dive consultant-led reviews with automated self-assessments, offering actionable insights for organizations of all sizes and industries.

Assessments are tailored to support underwriting, vendor due diligence, and litigation defense, and include add-on options like network vulnerability scans and tabletop exercises.

Where the Industry Connects

Our Cyber Risk Summits are the cyber insurance industry's premier networking events—bringing together underwriters, claims professionals, breach response experts, and risk managers from around the world.

Programs are expertly curated to address both emerging threats and practical challenges faced by cyber insurers and their clients. In 2026, join us in Miami Beach, Toronto, San Diego, and Philadelphia for next-level insights and connections that move the industry forward.

Contact Us

For more information, visit us at netdiligence.com or reach us directly at management@netdiligence.com.

NetDiligence®

About the Study

Contributors

Risk Centric Security, LLC.

A special thank you goes to Heather Goodnight-Hoffmann and Patrick Florer of Risk Centric Security, LLC, who provided material support to the data collection, data analysis, and writing and editing of the report. Risk Centric Security offers research, analysis, and reporting services, as well as state-of-the-art quantitative risk analysis and training for risk and decision analysis. For more information, visit www.riskcentricsecurity.com.

The NetDiligence Team

We would also like to acknowledge the following individuals for their contributions to this annual study:

- Mark Greisiger, President
- Heather Osborne, Director of Global Events & Programming
- Steve Kopanski, Director of Marketing
- Cait Osborne, Digital Media & Communications

For more information, visit us at netdiligence.com, or email us at management@netdiligence.com.

Methodology

For this study, we invited the major underwriters and carriers of cyber liability insurance to submit claims information based on the following criteria:

- The incident occurred in 2022, 2023, or 2024.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to over 104 individuals at 67 organizations in the United States, Canada, and the United Kingdom. From this group, 16 individuals representing 16 organizations provided 4,108 analyzable new and updated claims.

The 2025 report also includes data from NetDiligence studies published in 2020-2024, representing 6,294 incidents that occurred in 2020, 2021, 2022, and 2023 making a total of 10,402 claims that could be analyzed. All of these were included in the demographic analyses. 9,171 claims with a total incident cost ≥$1,000 were included in the financial analyses. There were eight claims in excess of $100M. Whereas in previous years we have excluded these claims, with comments in the main body of the report, this year we have included them in the analysis.

There are 10,150 claims in the dataset from American organizations, 127 claims from Canadian organizations, and 14 claims from organizations in the United Kingdom. There are also a small number of claims from organizations in Australia, EU Countries, South Africa, South America, and organizations with a global footprint. The country was not specified in 56 claims.

When factoring in SIRs, we were able to calculate total incident cost to date for all 9,171 (100%) of the claims with total incident cost >$1,000. 4,827 claims (46%) included an accounting of crisis services costs. 406 claims (4%) specified a number of records exposed ≥2. The number of claims reporting the number of records exposed decreased again since last year due to the large number of claims for incidents that do not expose records (ransomware, social engineering, BEC, etc.).

8,964 (89%) claims in the dataset were flagged as closed and 1,427 (11%) as open. The claim status was unknown for 11 claims. 6,073 (58%) claims were for primary coverage, 140 (1.3%) for excess coverage, and 4,189 (40%) had an unknown, but most likely primary, coverage level.

There were 3,275 claims in the dataset for which the revenue size of the organization was unknown. After comparing the distribution of their incident costs to those of SMEs and large companies, the decision was made to include these claims, with a few exceptions, in the SME group.

Readers should keep in mind the following:

- Our sampling, although large, is a subset of all incidents. Some of the data points are lower than other studies because we focus on claims payouts and total cost for specific incident-related expenses and do not factor in other financial impact, including in-house investigation and administrative expenses, customer defections, opportunity loss, etc.
- There is no attempt here to consider whether claims associated with the same incident appear more than once in the data set. Given the fact that claims are anonymized when they are sent to us, there is no possible way for us to know this. We believe that the number of duplicated claims, though not zero, is very small.

- We are not privy to the terms of the cyber insurance policies governing the claims provided to us. Apart from SIR, we have no insight into specific exclusions, limits, or sub-limits that might be involved. For this reason, the reader is advised to consider the costs reported in this report as lower bounds—i.e., we know that a given incident had a cost of at least $X but cannot say how much more than this amount.

- Having said that, beginning in 2017, we began asking respondents to provide us with an estimate of the total cost of the incident, including amounts that were excluded due to policy provisions. While a few participants in 2017 provided these estimates, a greater number of participants have done so since then, thereby increasing our ability to understand the true cost of an incident.

- Most claims submitted were for total insured losses and so included self-insured retentions (SIRs), which ranged from $0 to $30 million.

- In statistical terms, our sample is a “convenience” sample, which means that we have taken the data we have been given and have described it. We cannot make any statements about “significance” or “non-significance.”

It is important to note that 11% of the claims submitted for this study remain “open.” Therefore, aggregate costs as presented in this study include “payouts to-date” and “incident cost to-date.” It is virtually certain that additional payouts will be made on some of the claims in the dataset, and therefore the costs in this study are almost certainly understated.