NetDiligence®

CYBER CLAIMS STUDY

2024 REPORT

CONSTANGY BROOKS, SMITH & PROPHETE LLP

experian.

RSM

KYND

Contents

Introduction

Welcome to the fourteenth 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 2019–2023. By comparison, the first Cyber Claims Study, published in 2010, analyzed fewer than 100 cyber insurance claims.

By the Numbers

- 10,464 claims analyzed, arising from incidents occurring 2019–2023
- 4,991 new and updated claims collected in 2023, from incidents occurring 2021–2023
- 1,301 claims analyzed arising from incidents occurring in 2023
- 98% of claims ($1.9B in total) from small to medium enterprises (SMEs) with less than $2 billion in annual revenue
- 2% of claims ($2.0B in total) from large companies with more than $2 billion in annual revenue
- 2,754 claims due to ransomware, 54% of which occurred between 2021 and 2023
- 1,714 claims due to business email compromise, 56% of which occurred between 2021 and 2023

With Appreciation

We want to sincerely thank the cyber insurers listed on page 49 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 14 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 $230B in annual revenue) was approximately 23 million times larger than the smallest organization (less than $12K in annual revenue). The average large company ($13.3B in annual revenue) was more than 140 times larger than the average SME ($93M).
- Even though large companies represented only 2% of claims (N=222), these claims accounted for 51% of the total incident cost analyzed in the report ($2.0B/$3.9B).
- The dataset contains 5 claims >$100M, 40 claims $10M–$99M, and 361 claims $1M–$10M. Of the 5 claims >$100M, two occurred at organizations with <$700M in annual revenue.
- In SMEs, there were 327 claims ≥$1M. In large companies, there were 79 claims ≥$1M
- Ransomware and business email compromise were the two leading causes of loss. They accounted for 53% of claims ≥$1K in the five-year period 2019–2023, and nearly 39% to date in 2023.
- Ransoms continue to be off the charts, with initial demands as high as $80M and ransoms paid as high as $50M. There were 15 ransoms paid ≥$10M.
- Industry concern about third-party events is on the rise. We plan to collect additional data in future studies so that we may provide more specific information about cause of loss in these cases.

Company Size

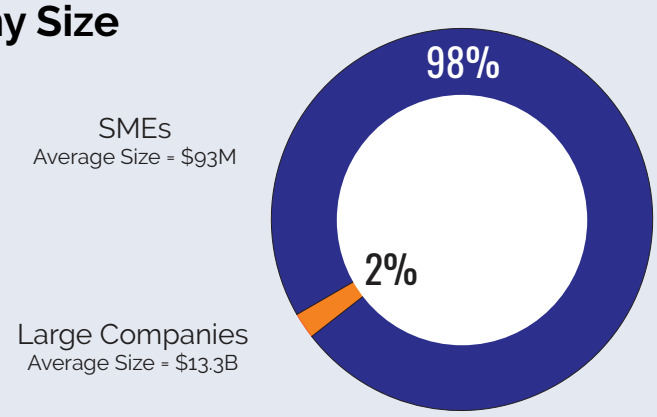


Figure 1

Average Costs for All Claims

SMEs

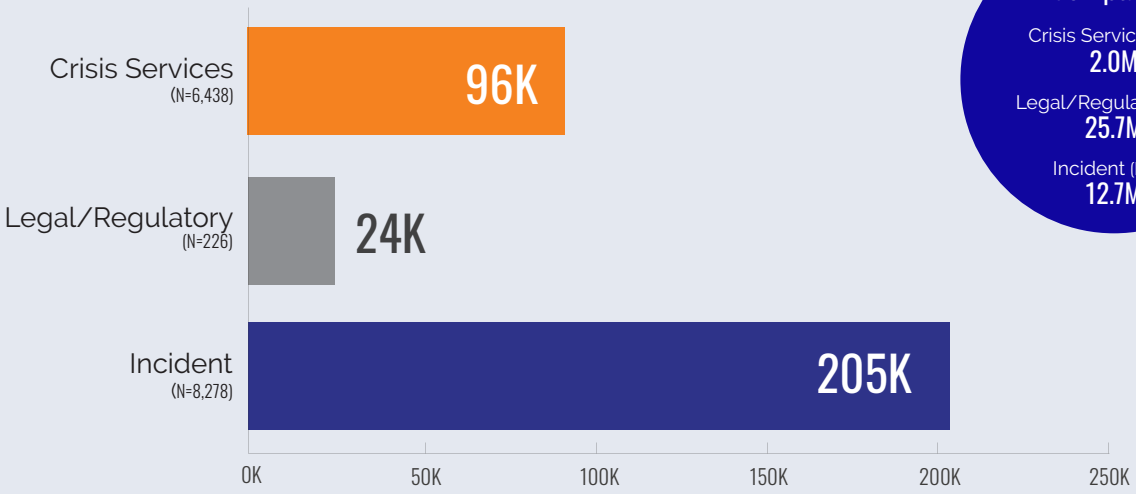


Figure 2

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 2019–2023 unless otherwise noted.
NetDiligence is a registered trademark of Network Standard Corporation, dba NetDiligence.

Ransoms Demanded vs Ransoms Paid

SMEs

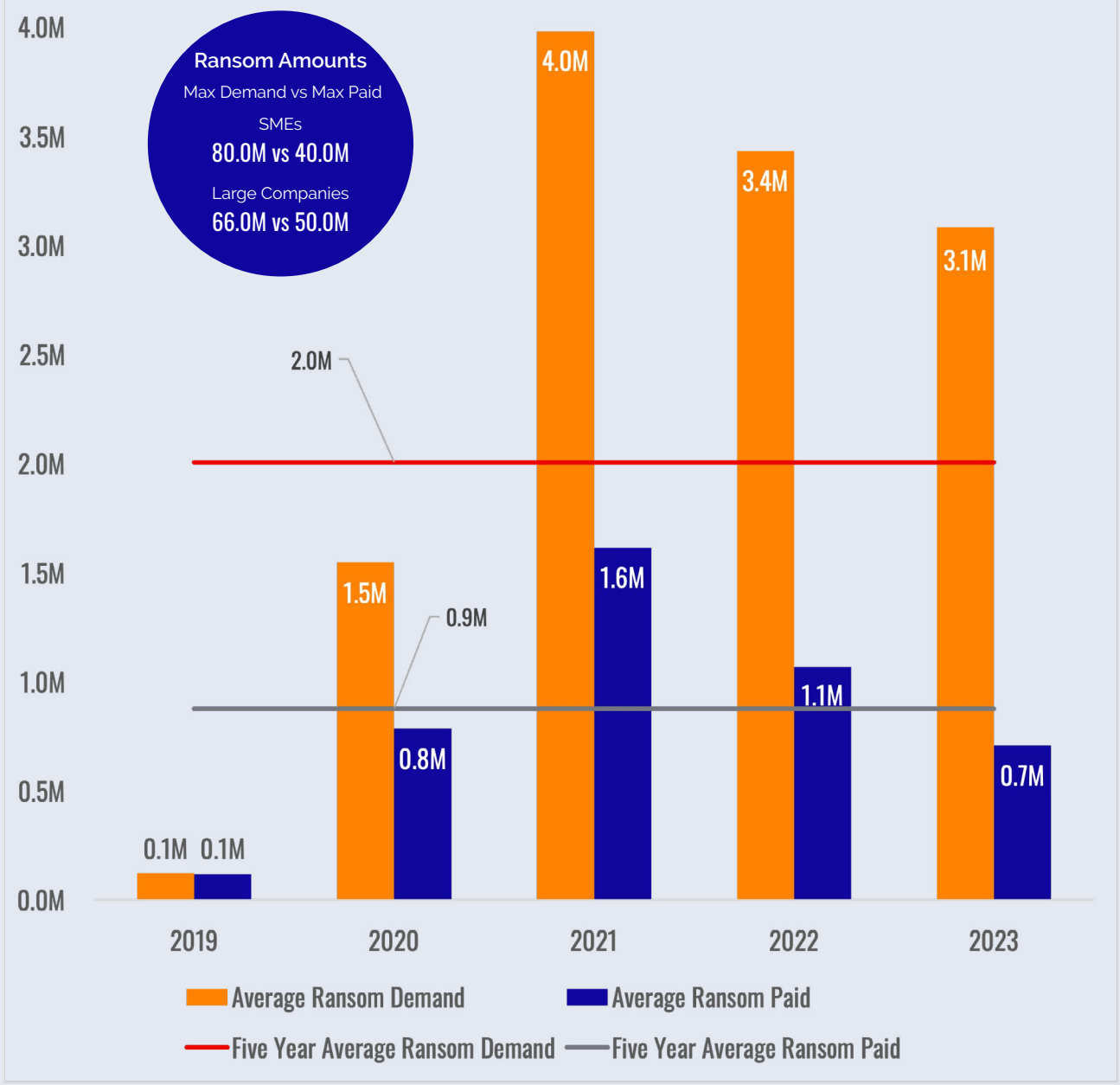


Figure 3

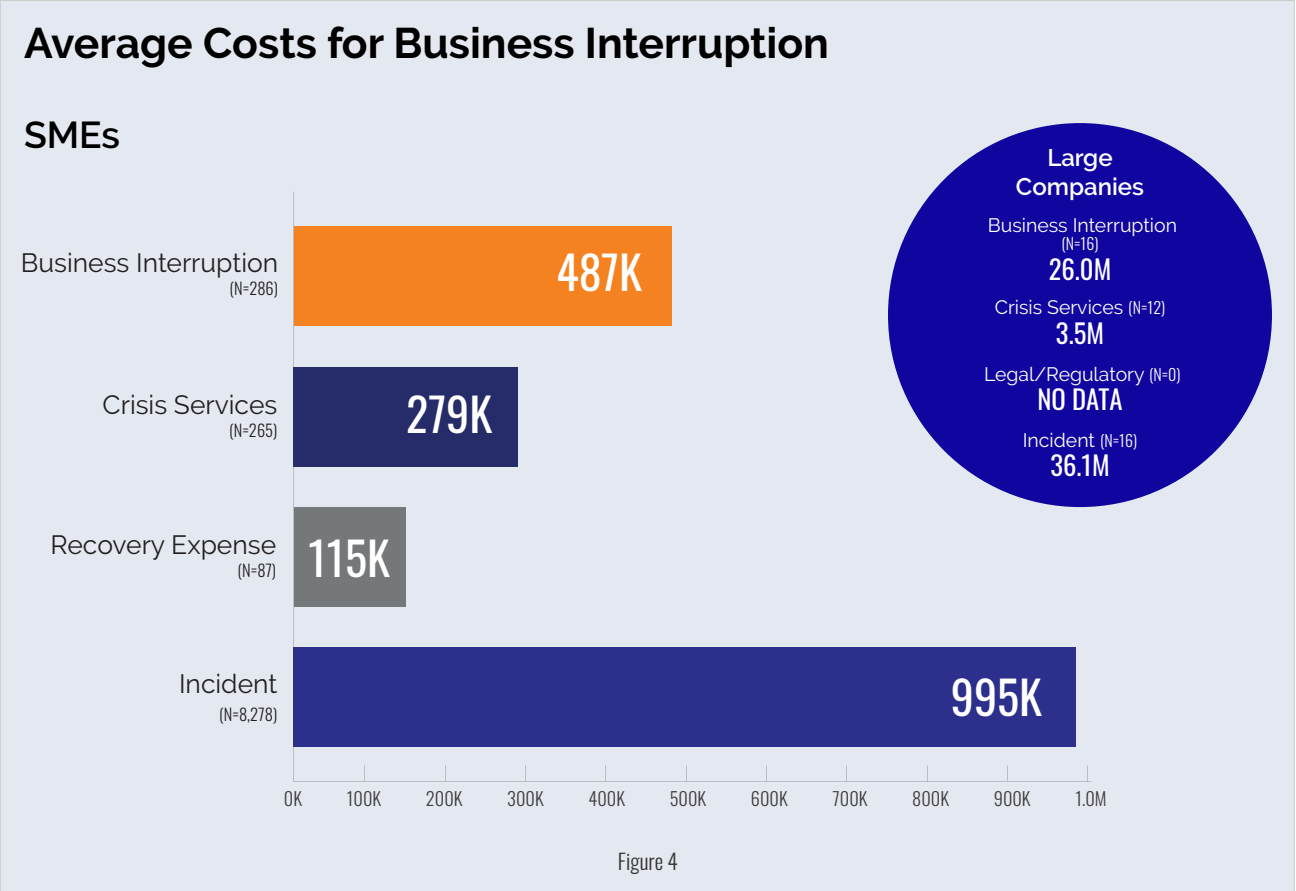


Figure 4

In 2023, our data reveals some interesting contrasts—both positives and negatives—in the cyber claims landscape, especially for SMEs across various industries. While we've seen a significant increase in incident costs for business email compromise claims, there's also been a reduction in losses related to general "hacker" incidents. Some additional positive trends noted include: wire fraud costs have steadily declined since 2020; healthcare SMEs appear to have continued to benefit from decreasing average incident costs; and manufacturing SMEs saw their costs drop to a five-year low. Conversely, the financial services sector appears to have experienced a sharp increase in incident costs, which continues to underscore the fact that cyber risk can—and usually does—evolve in different ways for different sectors.

Mark Greisiger, President & CEO, NetDiligence

Business Sector

Top 5 by Number of Claims – SMEs

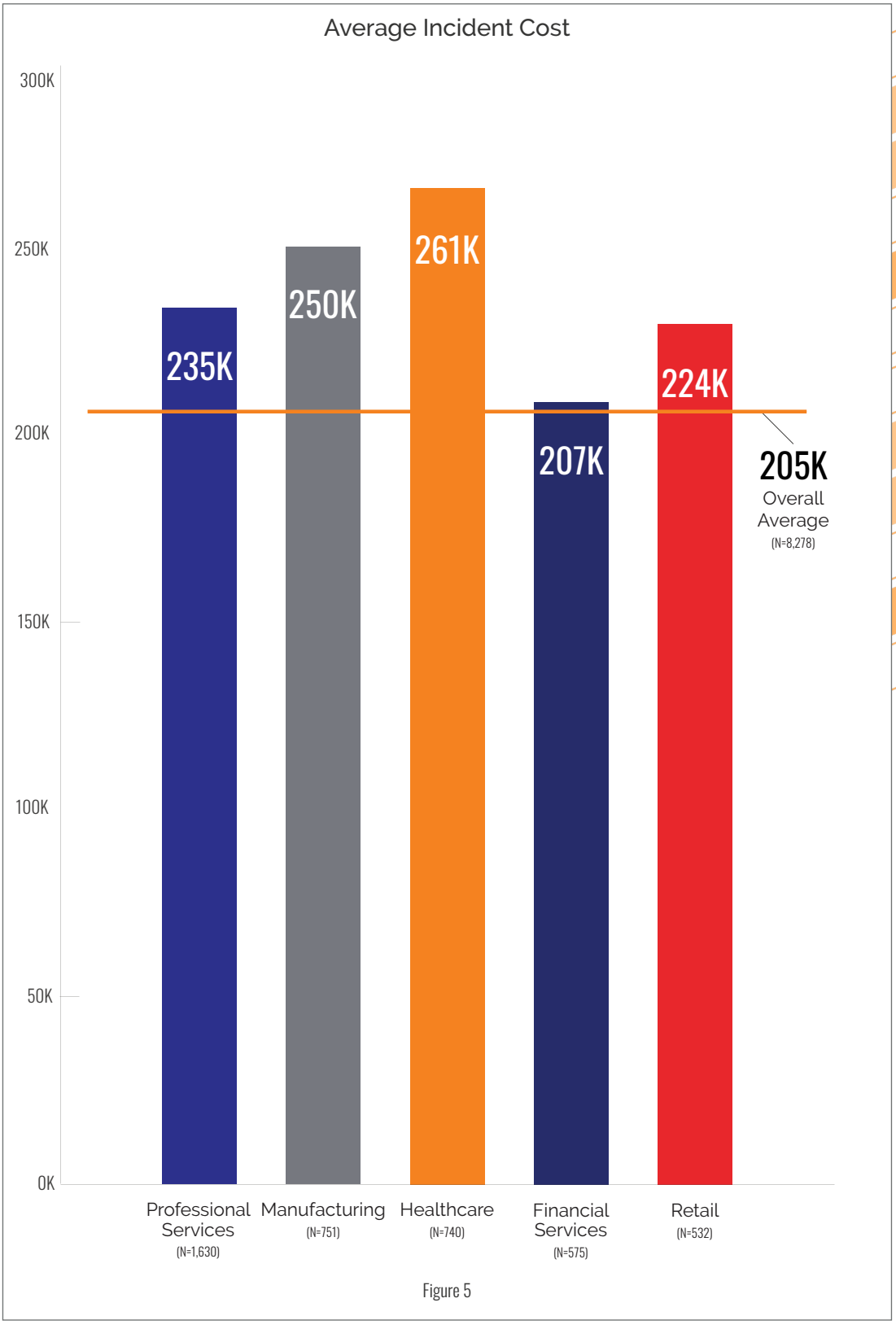


Figure 5

Cause of Loss

Top 5 by Number of Claims – SMEs

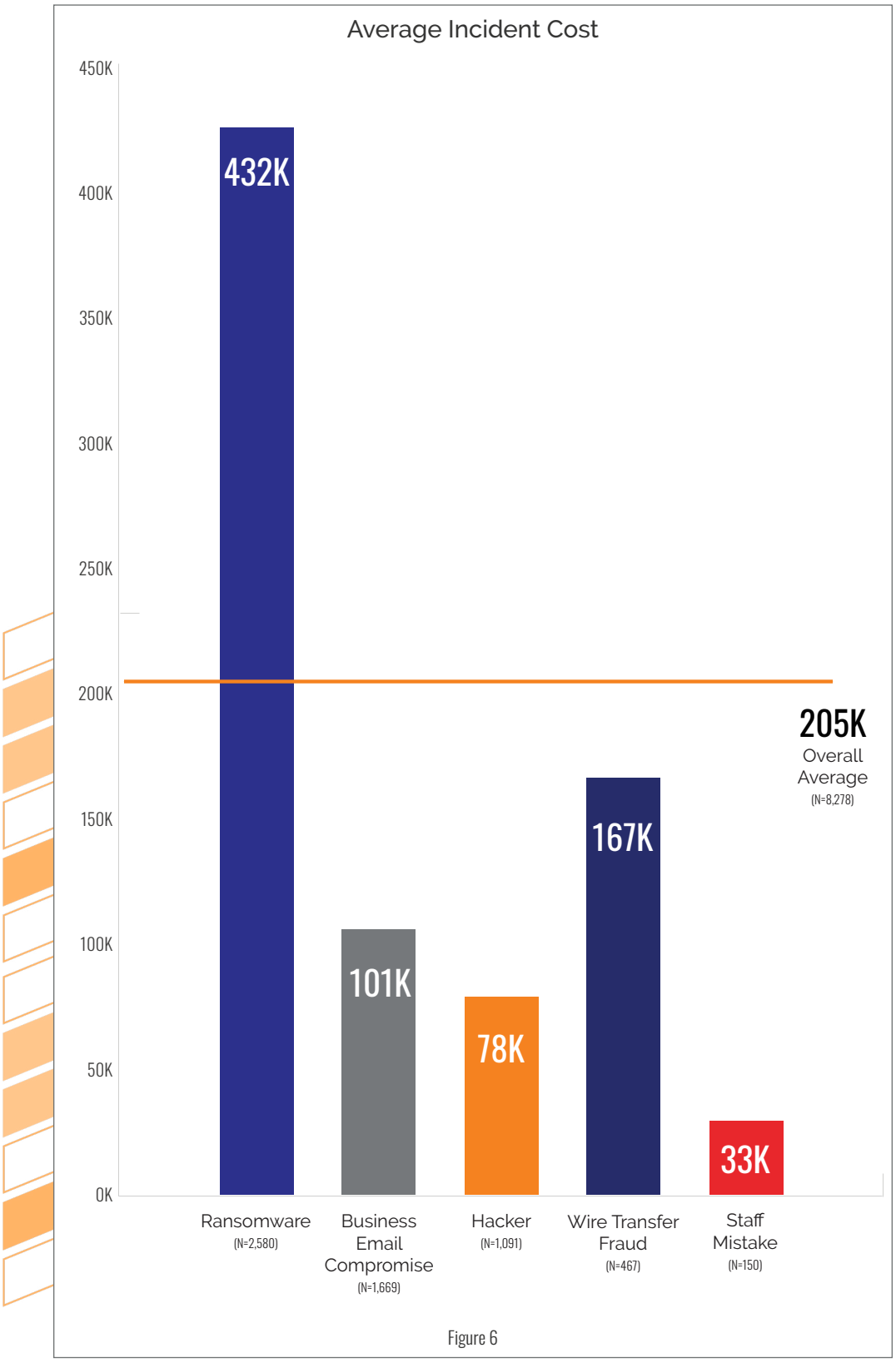


Figure 6

An Overview of the Data

The claims analyzed in this study come from organizations of all sizes, the smallest with less than $12K in annual revenue and the largest with over $230B. 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.

55% 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 $12K to $1.9B. The average was $93M. SMEs accounted for 98% of claims but only 49% of total incident cost.
- Large companies: annual revenue ranged from $2B to more than $230B. The average was $13.3B. Large companies accounted for only 2% of claims but 51% of total incident cost.

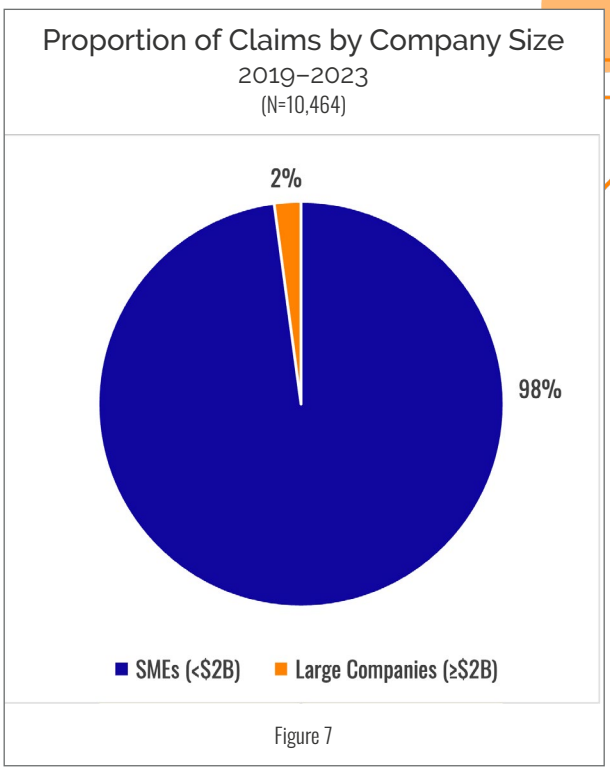


Figure 7

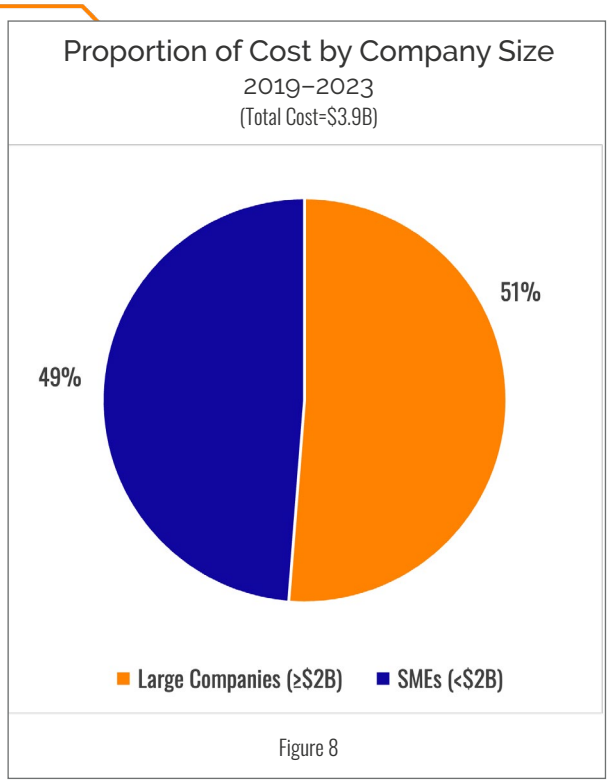


Figure 8

Claims by Year of Event

The study includes 10,464 incidents occurring 2019-2023. The incident distribution by year is depicted in Figure 9.

Demographic analyses are based on all 10,464 claims while cost analyses are based upon the 8,414 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.

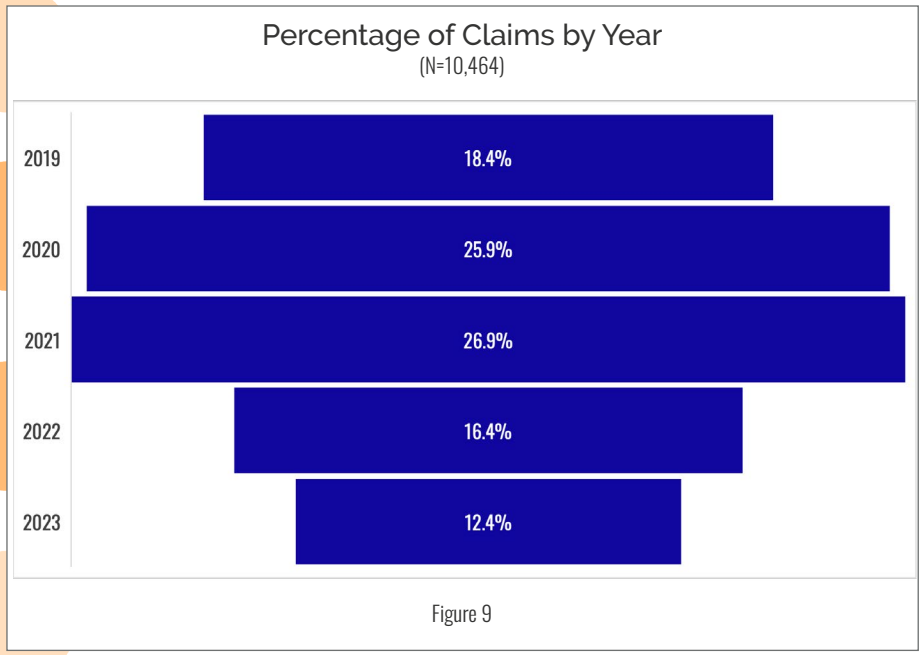


Figure 9

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 327 SME claims over $1M, and another 307 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.

Please note: *because each of these claims was an extreme outlier, both have been excluded from the analysis of all SME claims.*

The largest incident at a large company occurred in 2021 (>$500M). Between 2019 and 2022, there were 9 claims at large companies with over $50M in total incident cost, and another 11 claims with $10M-$50M in total incident cost.

Payouts for all organization sizes covered 47% of the total incident cost. For SMEs, the five-year payout was 81% of the total incident cost. At large companies, this number was 24%.

Figures 10 and 11 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.

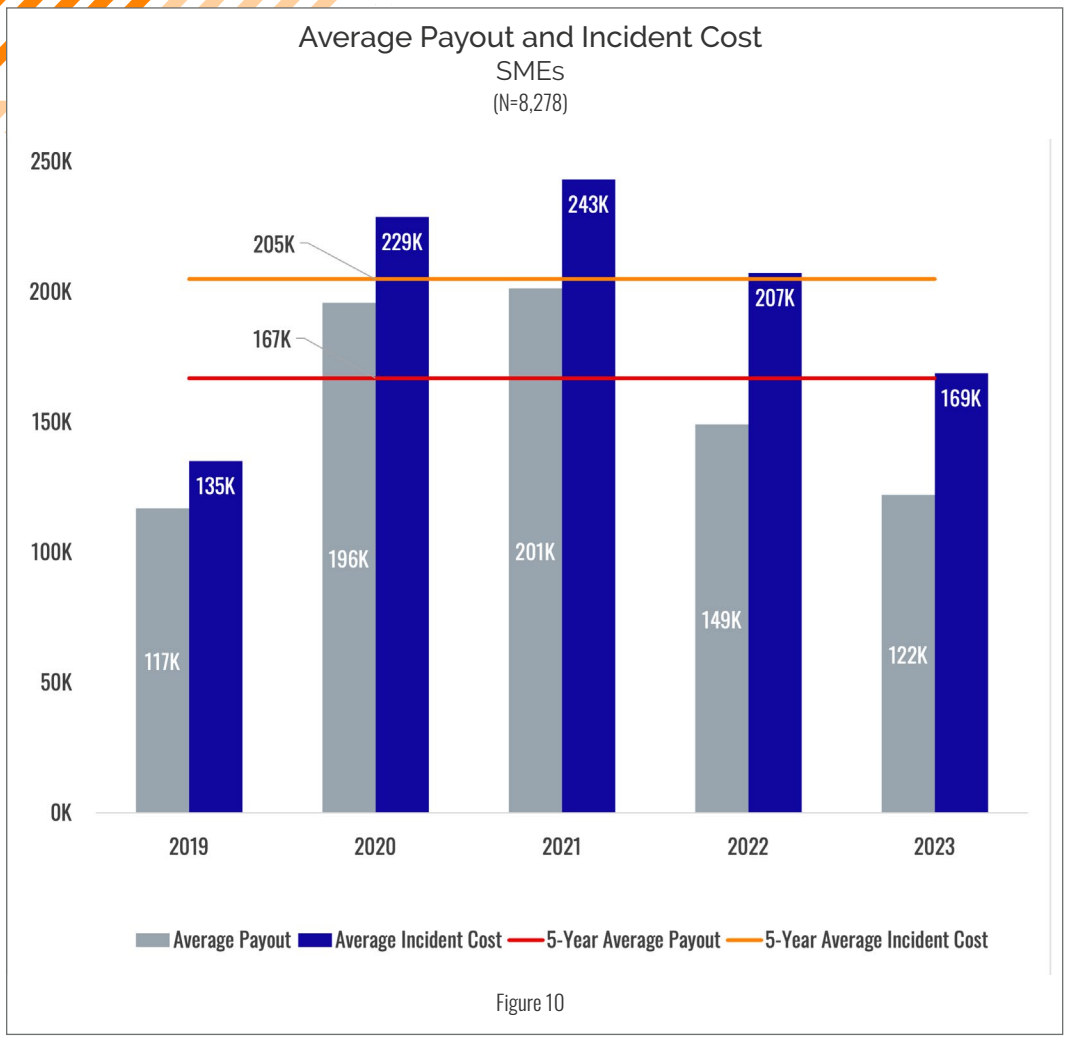


Figure 10

The cost of cyber insurance claims remains significant, making addressing the issues leading to high payouts crucial. The ~$40k gap and significant correlation between incident costs and payouts underscores the particular value of cyber insurance in mitigating issues, helping insureds avoid uncovered costs. Organizations must continue to move beyond a reactive stance and adopt a proactive, holistic approach to cyber risk.

Ben Duffy, Head of North America, KYND

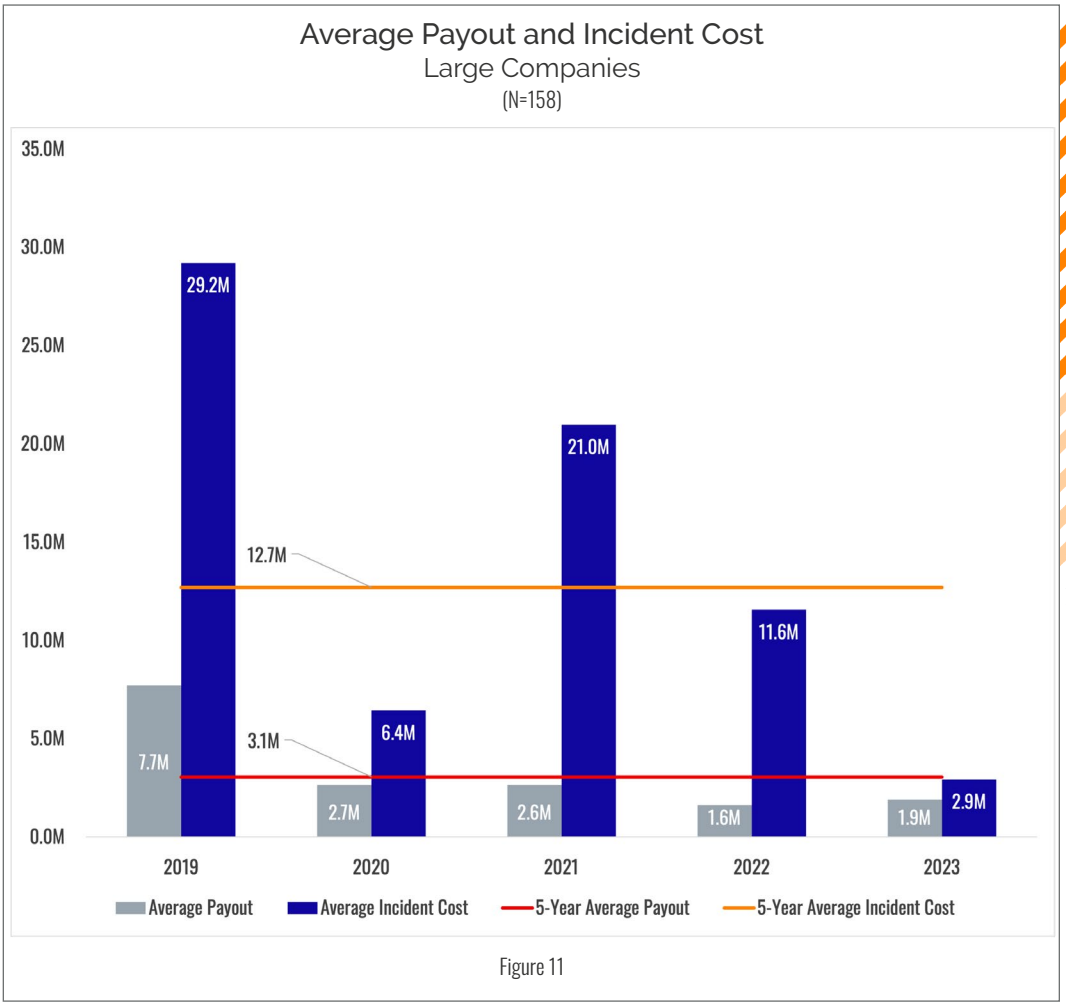


Figure 11

The cyber insurance industry continues to be in a unique position to affect critical change within the information security industry. The number and type of claims emanating from third party incidents, such as claims from thousands of businesses affected by "industry" incidents like the MOVEit Transfer, Change Healthcare and CDK Global events, will be substantial—with significant economic impact to carriers. This impact clearly justifies additional inquiry into third party risk during the underwriting process. It highlights the need to require prospective insureds to have vendor management programs and to provide proof of these programs during the underwriting process. Doing so will not only facilitate more secure networks but will also produce much better underwriting risks.

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

Incident and Crisis Services Costs

For all organizations, crisis services costs ranged from less than $100 to almost $26M. Incident cost for these claims, inclusive of SIR, ranged from less than $1,000 to almost $110M. 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 $69K in 2019 to $146K in 2023, as shown in Figure 12. Over five years, crisis services costs for SMEs averaged about 51% of total cost, as shown in Figure 13.

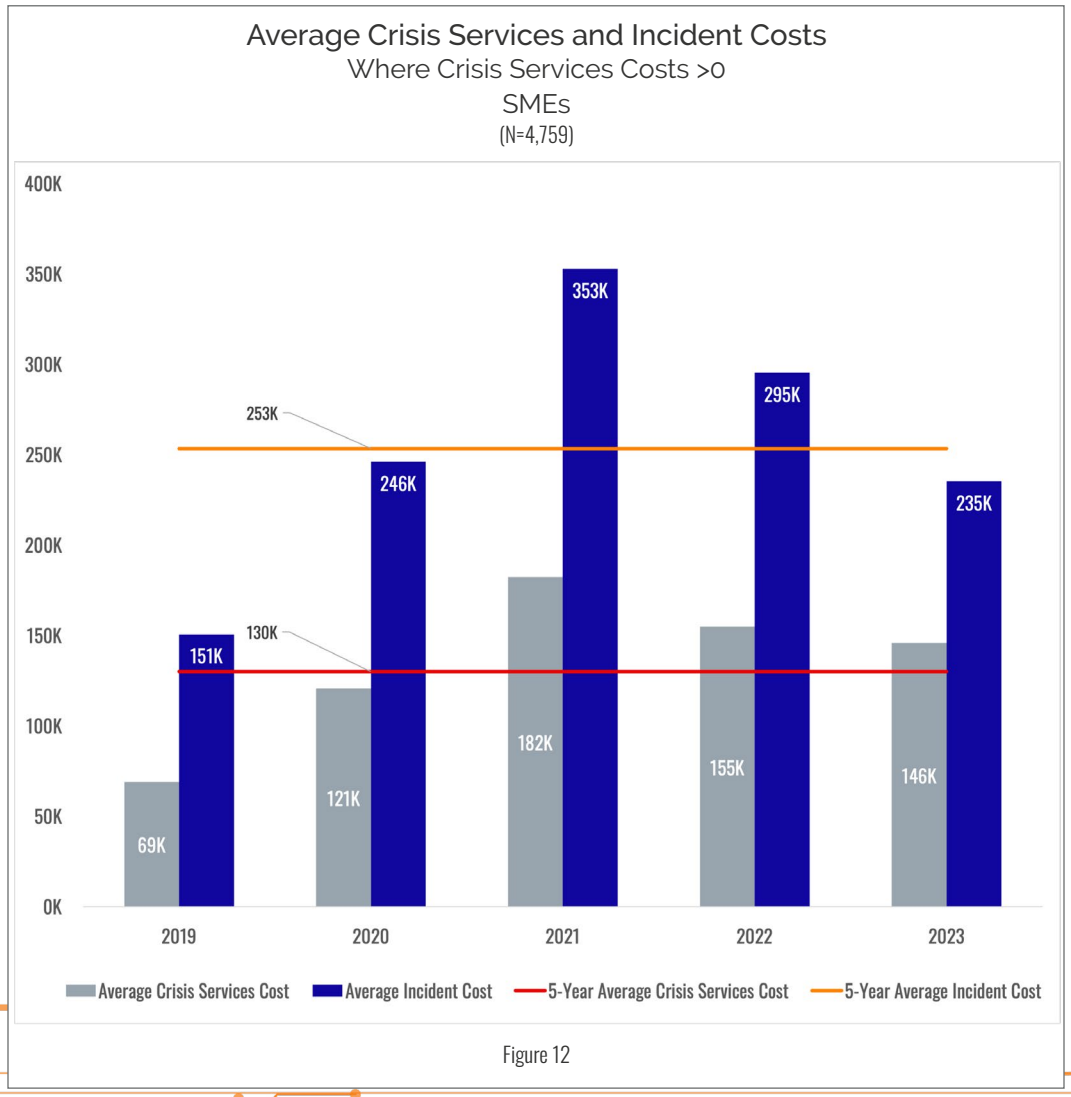


Figure 12

Rapid response, combined with the most comprehensive and accurate information, is crucial in mitigating cybersecurity issues as they arise. Continuous portfolio monitoring helps insurers identify affected organizations before notifications arrive, providing incident responders with the data they need to act quickly. Swift and effective action enables insurers to reduce both professional service costs and business interruption impacts.

Ben Duffy, KYND

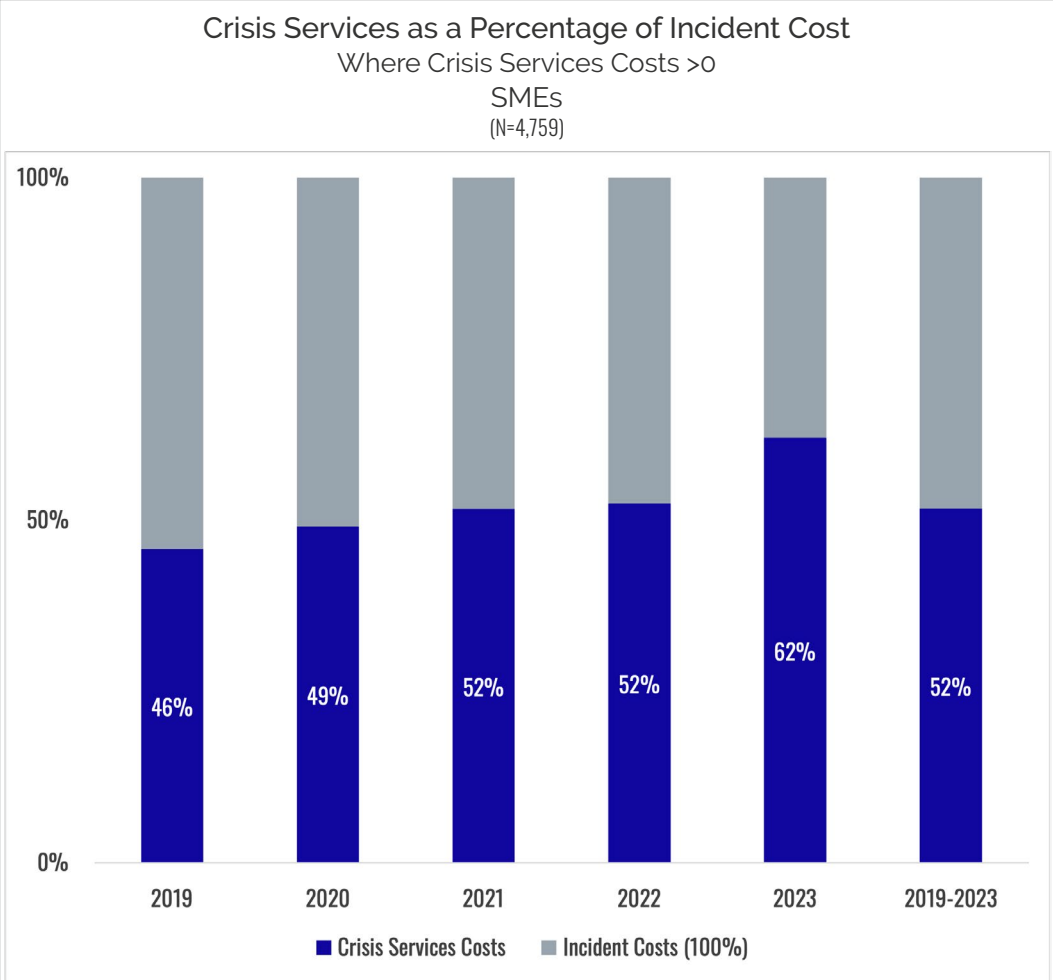


Figure 13

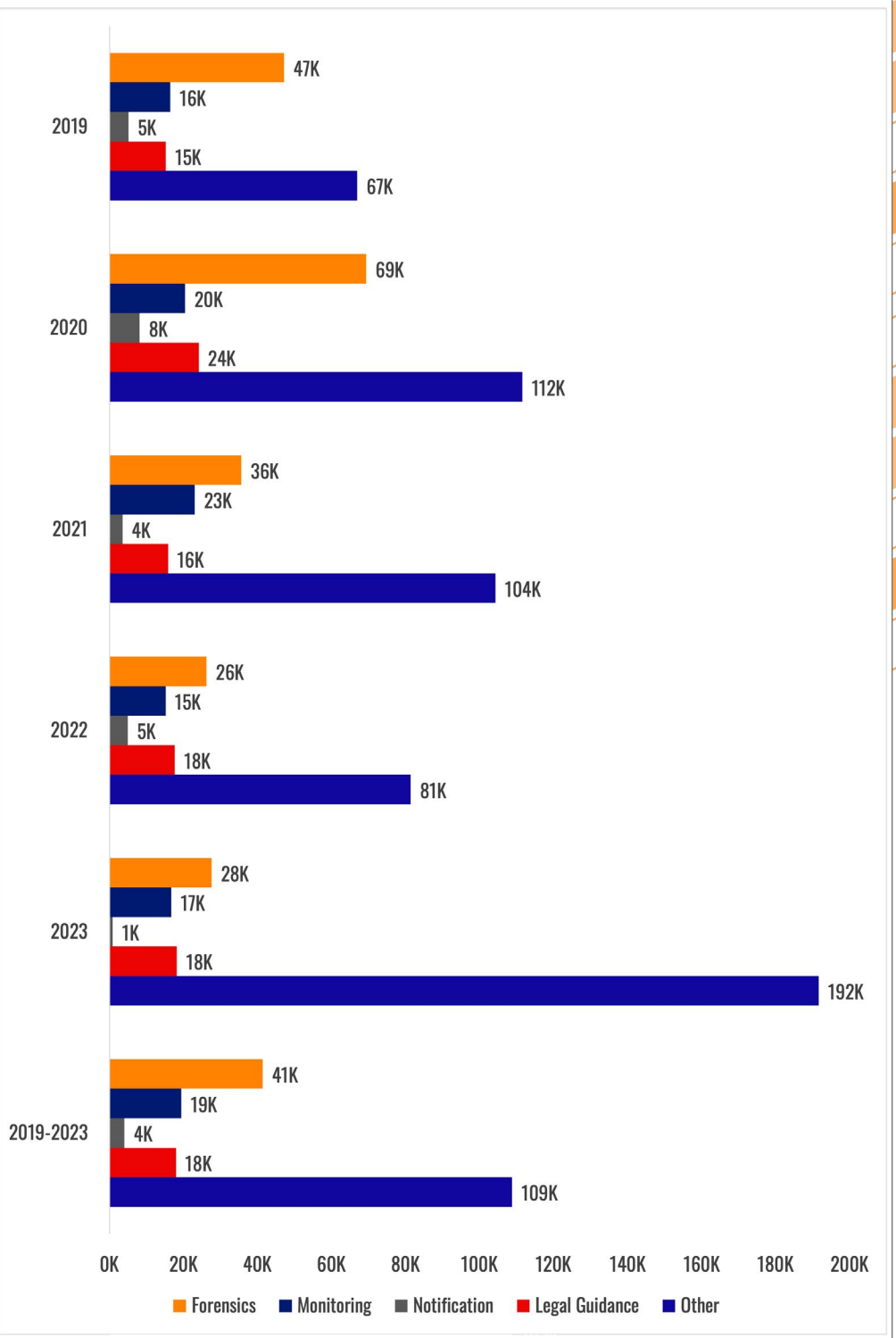

Average Crisis Services Costs
SMEs
(N=4,759)
2019
47K
16K
5K
15K
67K
2020
69K
20K
8K
24K
112K
2021
36K
23K
4K
16K
104K
2022
26K
15K
5K
18K
81K
2023
28K
17K
1K
18K
192K
2019-2023
41K
19K
4K
18K
109K
0K
20K
40K
60K
80K
100K
120K
140K
160K
180K
200K
Forensics
Monitoring
Notification
Legal Guidance
Other

Figure 14

Figures 14 (above) and 15 (below) 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 22% of the total, and legal guidance accounted for another 10% of the total. "Other" crisis services include the costs of PR, data restoration, and sometimes the cost of ransom.

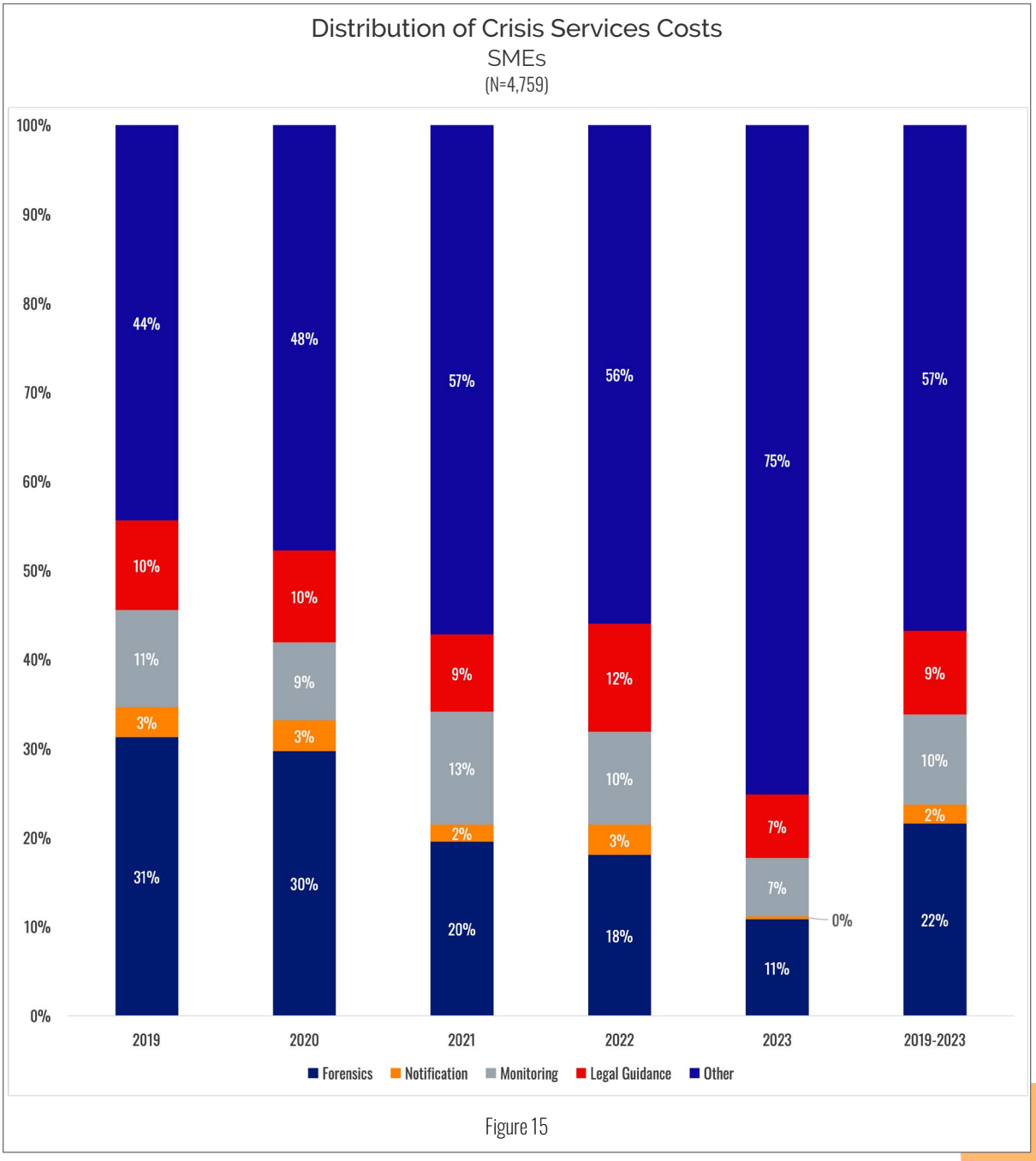


Figure 15

Large Companies:

Figure 16 illustrates considerable variability in both the average crisis services cost and the incident cost at large companies. Here, average incident cost ranged from $3.1M to $14M. Additionally, an outlier event in 2021 caused a spike in the average crisis services and incident costs.

Figure 17 shows crisis service cost as a percent of total cost. Over the five-year period, this percentage ranged from 20% to 60%, with an average of 28%. The previous five-year period showed a similar average (26% from 2018-2022).

Figure 18 breaks down crisis services costs into a variety of service components.

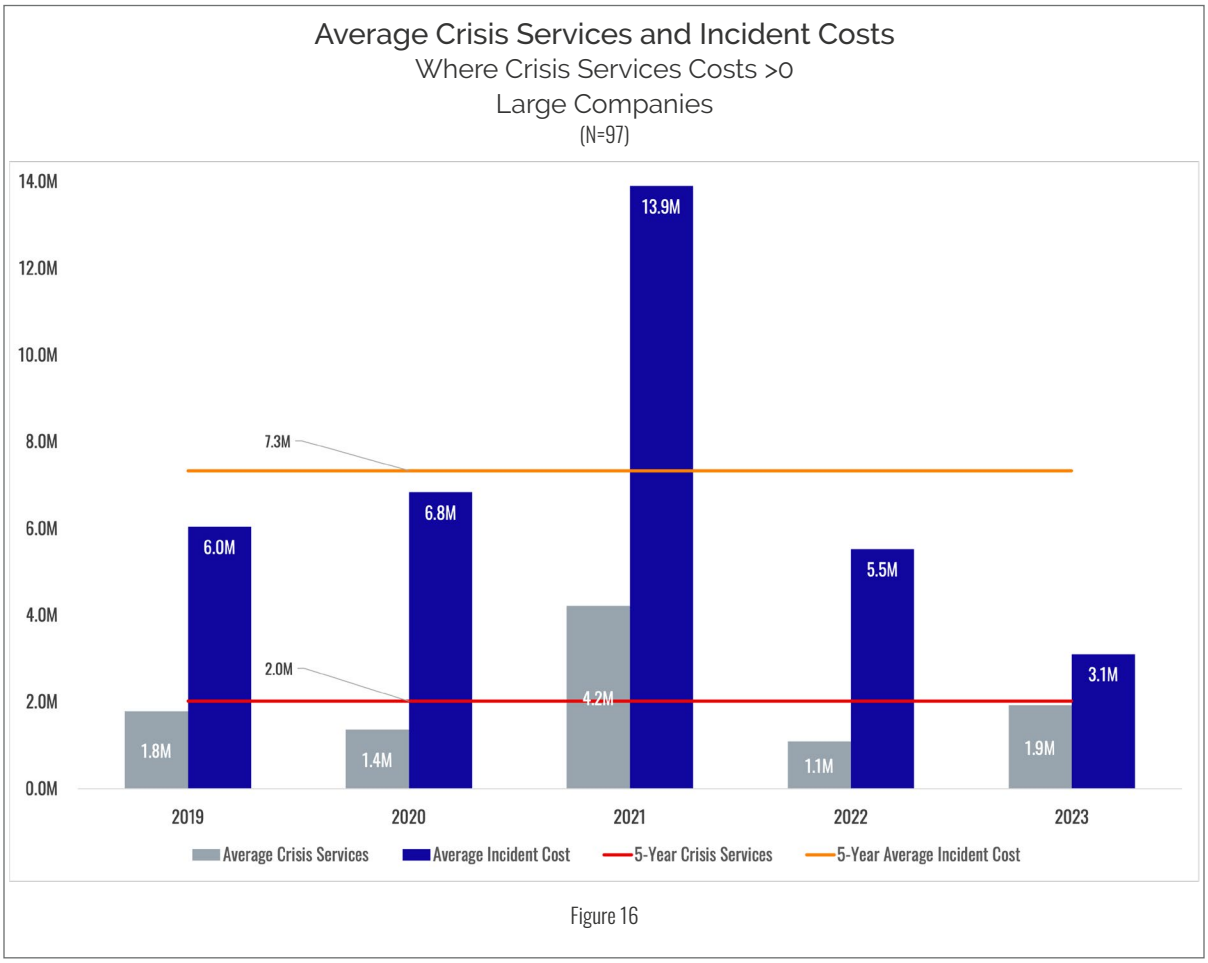


Figure 16

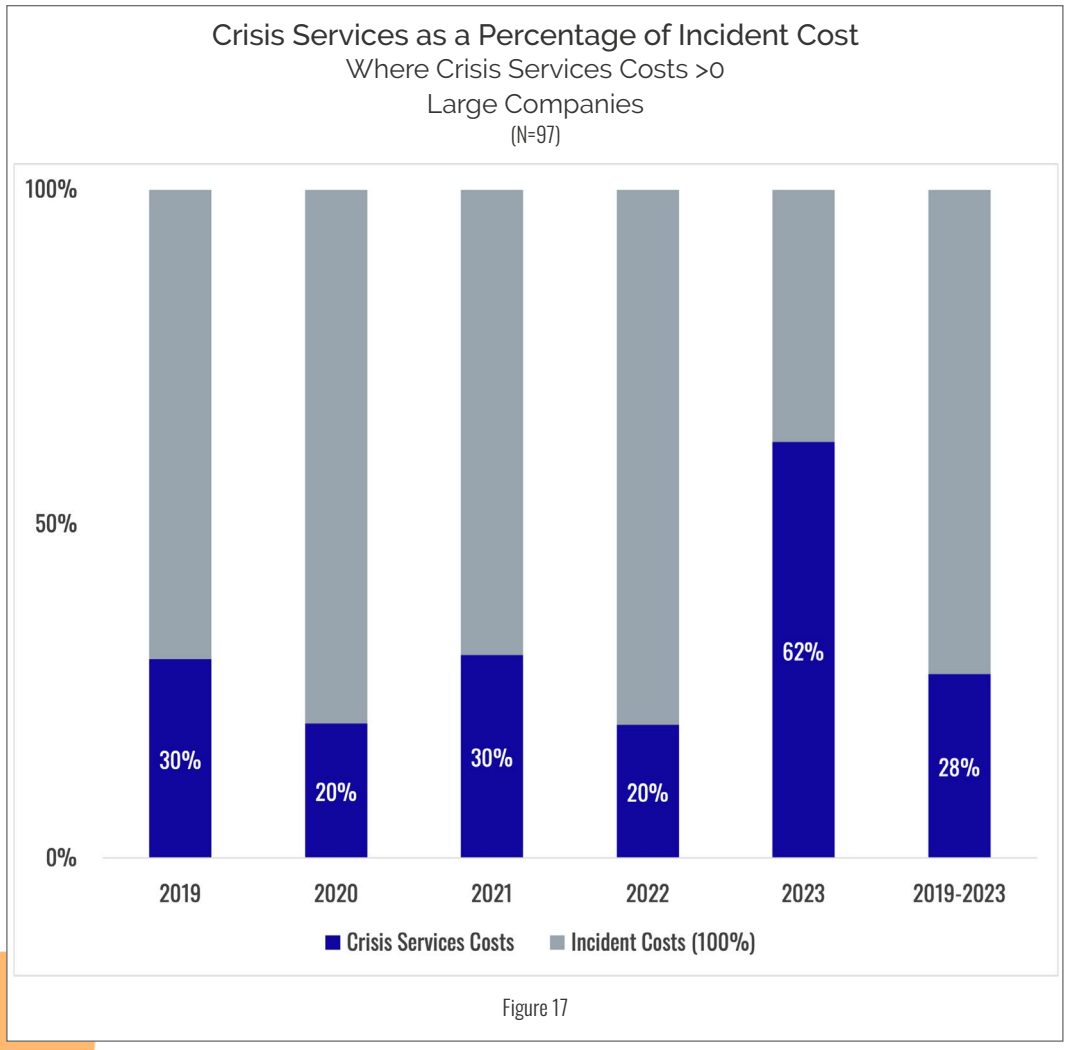

Crisis Services as a Percentage of Incident Cost
Where Crisis Services Costs >0
Large Companies
(N=97)
100%
50%
0%
30%
20%
30%
20%
62%
28%
2019
2020
2021
2022
2023
2019-2023
Crisis Services Costs
Incident Costs (100%)

Figure 17

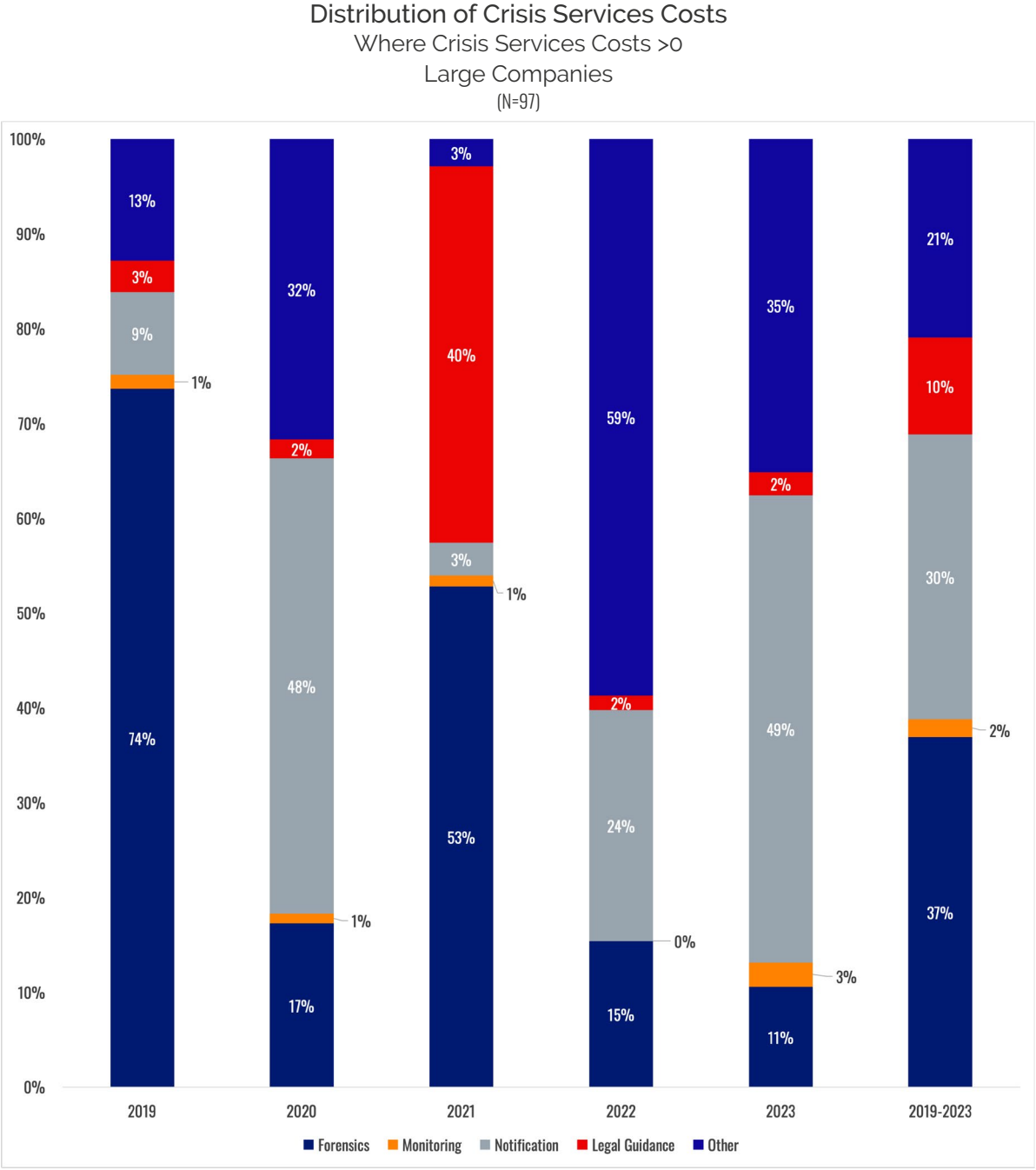

Distribution of Crisis Services Costs
Where Crisis Services Costs >0
Large Companies
(N=97)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
13%
3%
9%
1%
74%
32%
2%
48%
1%
17%
3%
40%
3%
1%
53%
59%
2%
24%
0%
15%
35%
2%
49%
3%
11%
21%
10%
30%
2%
37%
2019
2020
2021
2022
2023
2019-2023
Forensics
Monitoring
Notification
Legal Guidance
Other

Figure 18

Business Interruption (BI)

SMEs

BI costs were reported for 315[1] incidents. Since 2019, the average BI cost and corresponding average incident cost have remained high. The decrease in 2023 shown in the graph below is most likely a result of a smaller set of claims collected so far for 2023.

Additional analysis shows that the five-year average incident cost of a claim with BI was over 450% greater than a claim without BI. In 2023, the average claim involving BI was 270% greater than one that did not.

Further, ransomware incidents at SMEs accounted for 91% of claims with a BI component. The five-year average BI cost for ransomware incidents was $487K with a total incident cost of $995K. In 2023, these numbers were $593K and $1.3M, respectively.

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, especially in 2022.

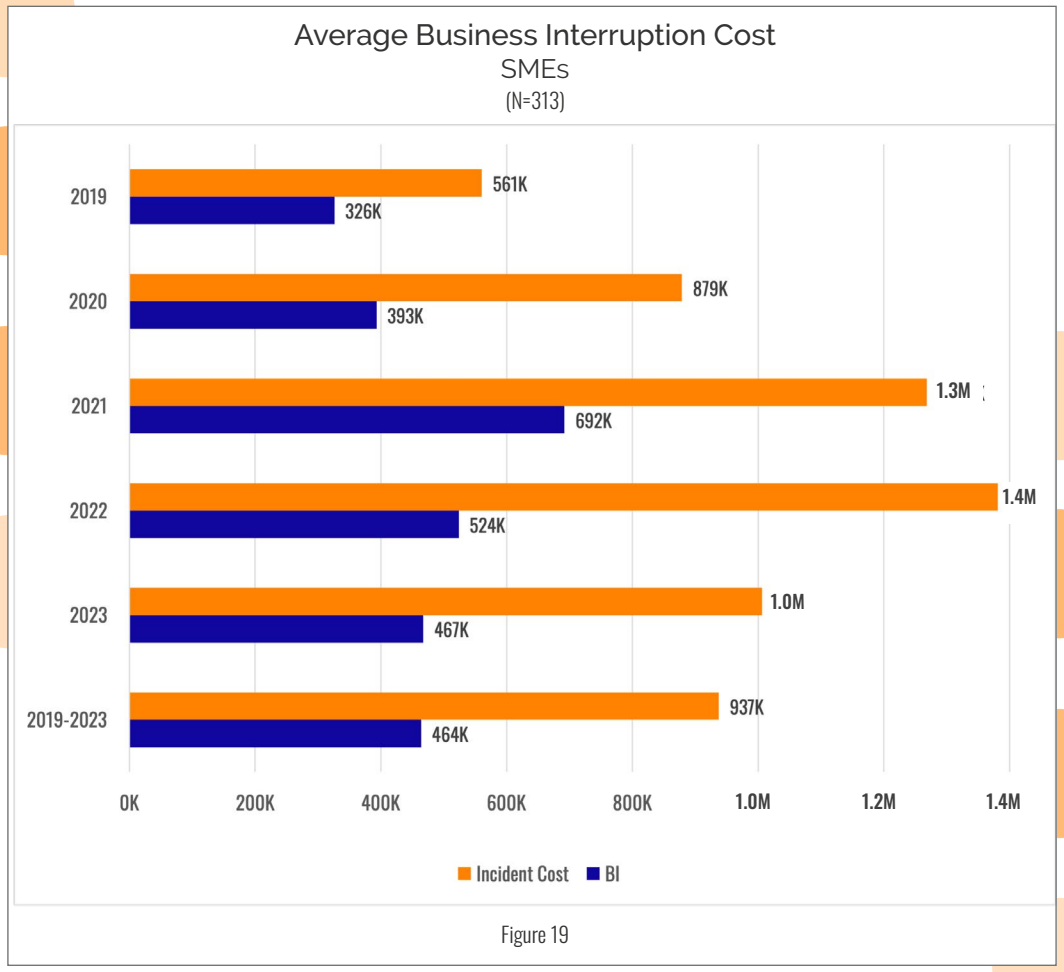


Figure 19

[1]Although 315 claims reported BI losses, very large incidents at 2 organizations have been excluded from this analysis, resulting in 313 incidents analyzed.

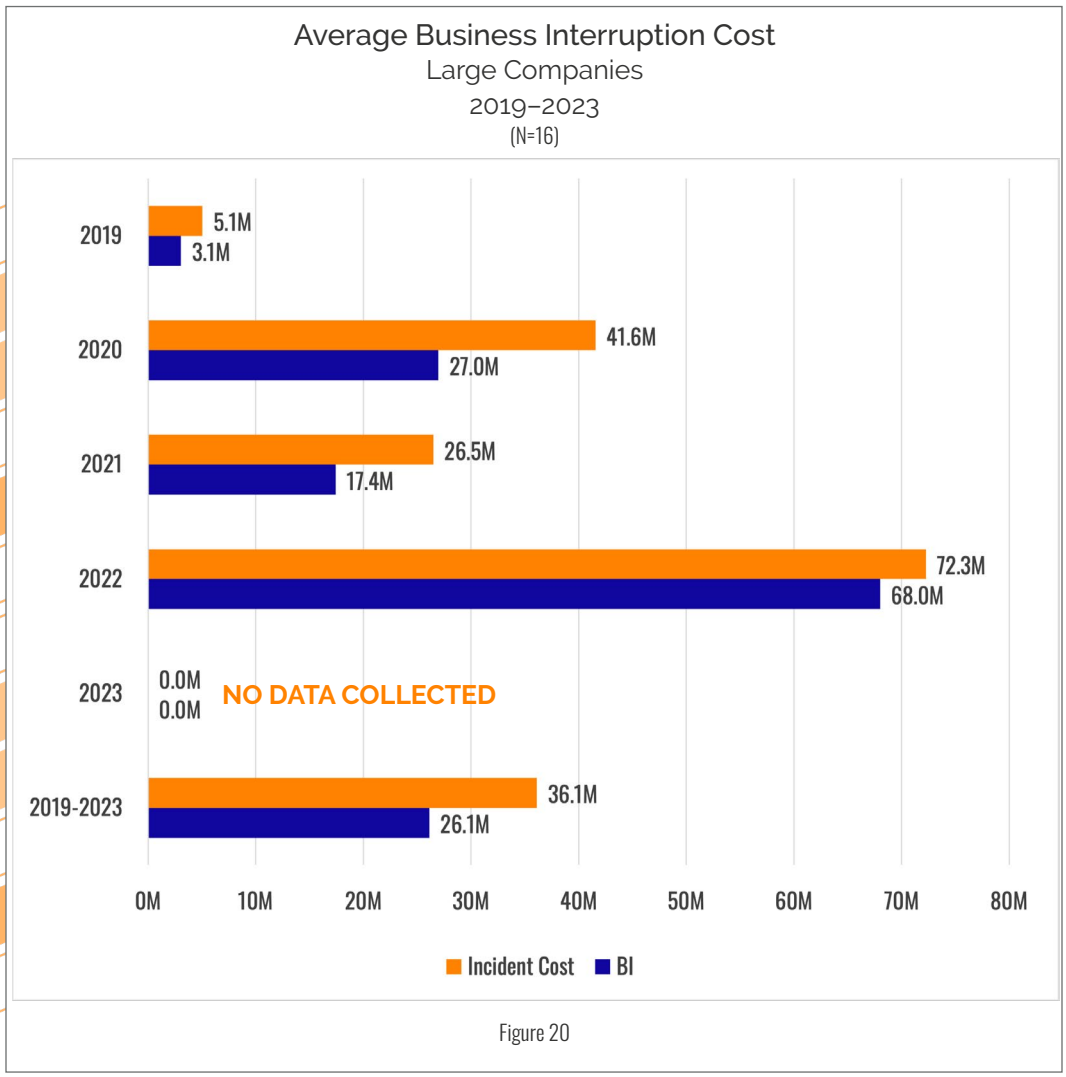


Figure 20

We continue to see SME clients transform their businesses to be more reliant on digital systems while failing to understand the inherent risks that come from complex digital ecosystems. This becomes very evident during the recovery process for a client where it's clear they haven't planned for resilience in their digital platform nor practiced operating their business processes during a crisis scenario. Helping educate companies on their digital systemic risks and build a proper resiliency plan for the business is vital.

Alden Hutchison, Principal, RSM US LLP

Recovery Expense

SMEs

252 claims reported recovery expense. As Figure 21 shows, both recovery expense and total incident cost has been steadily increasing since 2019. The average five-year incident cost of these claims is about 350% higher than incidents without recovery expense. In 2022, the incident cost was over 400% greater when recovery expense was incurred.

Ransomware incidents accounted for 85% of the claims with reported recovery expense. The five-year average incident cost of these events was 350% higher than incidents without recovery expense. In 2023, these incidents cost almost 400% more.

Large Companies

Seven large company claims reported recovery expense. Recovery expense for these incidents ranged from <$20K to $4.5M (average=$953K). The corresponding incident cost ranged from <$25K to $28M (average $11.3M). Five of these were due to ransomware and one was due to malware.

So far, we have collected no claims with recovery expense in 2023. That may change next year as we collect additional data for 2023.

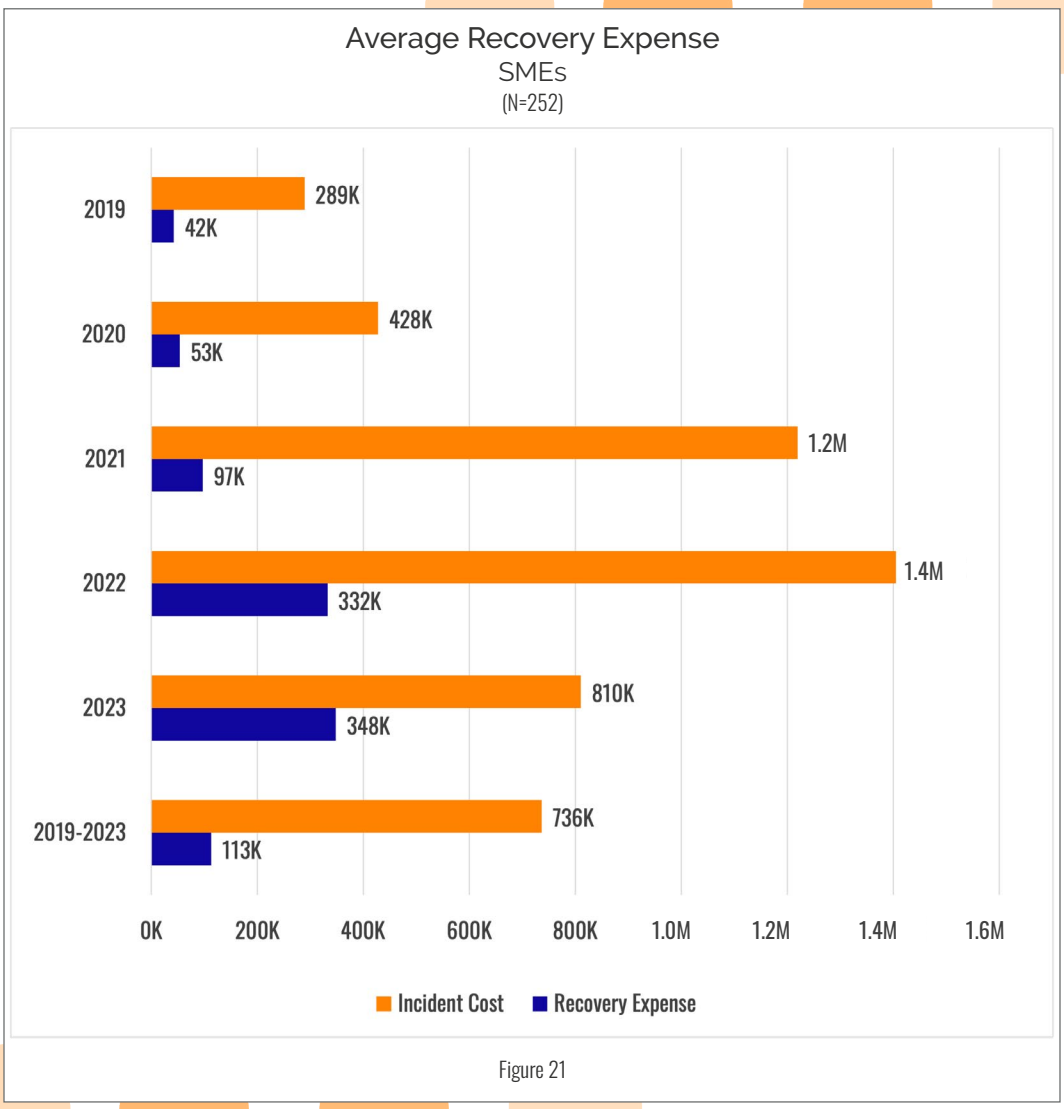


Figure 21

Legal Costs

SMEs

There were 226 claims in the dataset that reported legal or litigation expense from one or more category: legal settlement, legal defense, regulatory fines, and regulatory action. Figure 22 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.

Large Companies

The dataset contained only 12 claims reporting at least one type of legal or litigation expense. For the five-year period, the overall average was $25.7M, with a maximum of over $500M (settlement). This large settlement drives up the overall averages. Average settlement defense cost was $747K. There was only one regulatory fine in the five-year data ($21M).

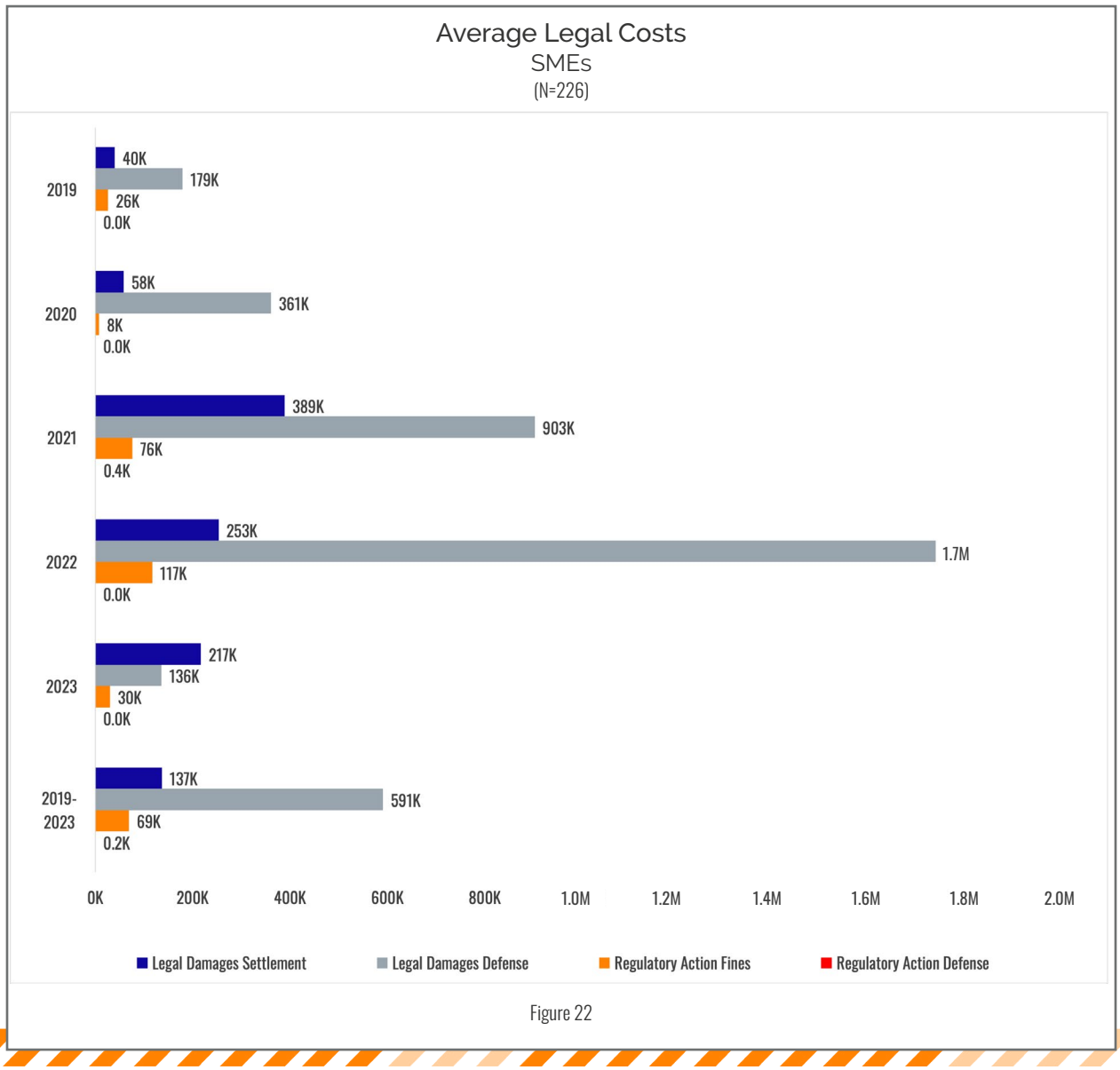


Figure 22

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 going down. The 2019–2023 range contains 436 claims that reported more than one[2] record exposed, whereas the 2018–2022 range contained 611 of these claims. Similarly, the total reported number of records exposed dropped 20% since 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 23 and 24 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.

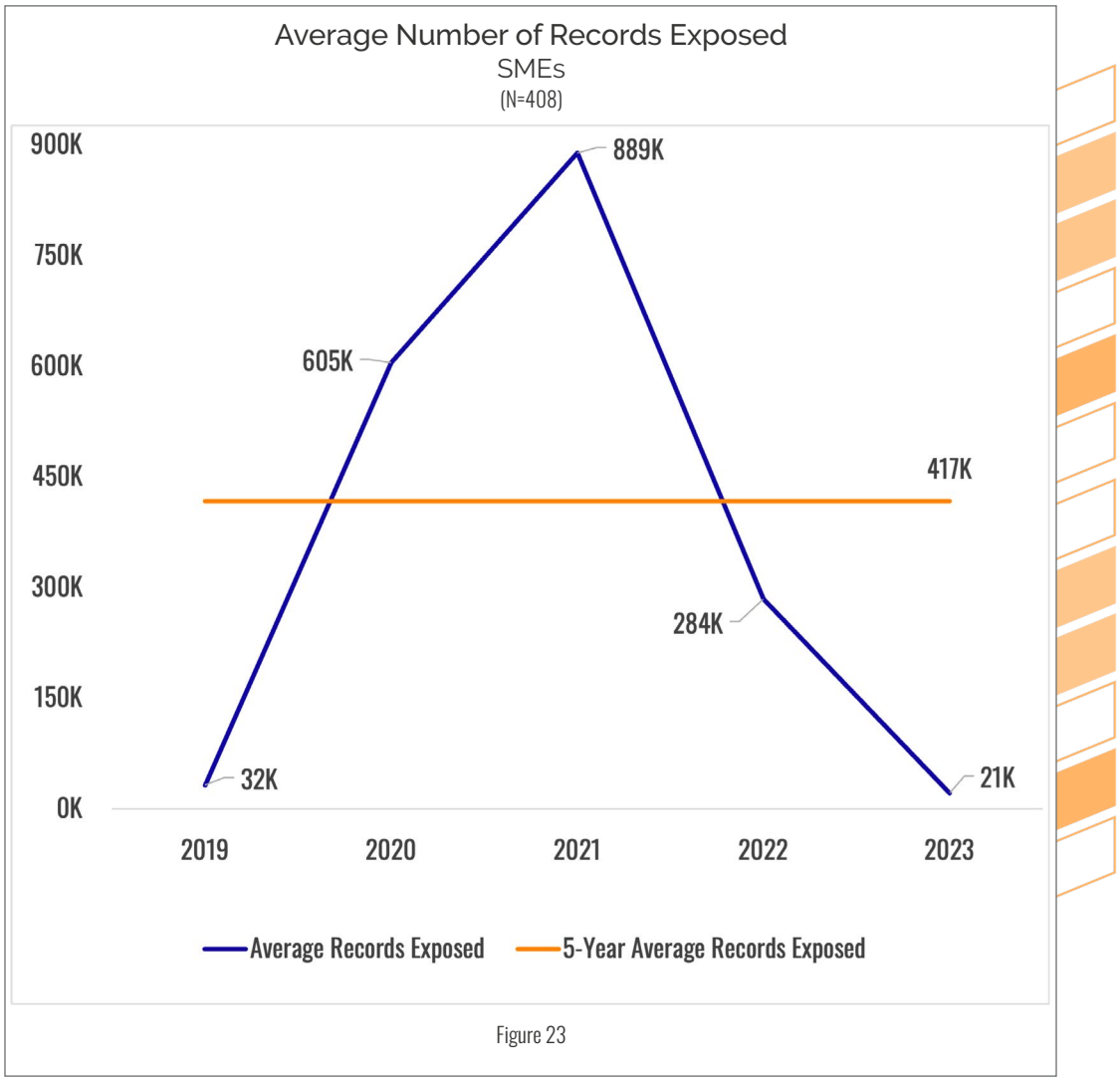


Figure 23

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

Experiencing a data breach can understandably be alarming, but it's essential for consumers not to feel discouraged. Today, there are a wealth of identity protection and fraud resolution resources available to assist those affected. These tools are designed to help consumers navigate the aftermath of a data breach, offering comprehensive support to prevent identity theft and fraud.

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

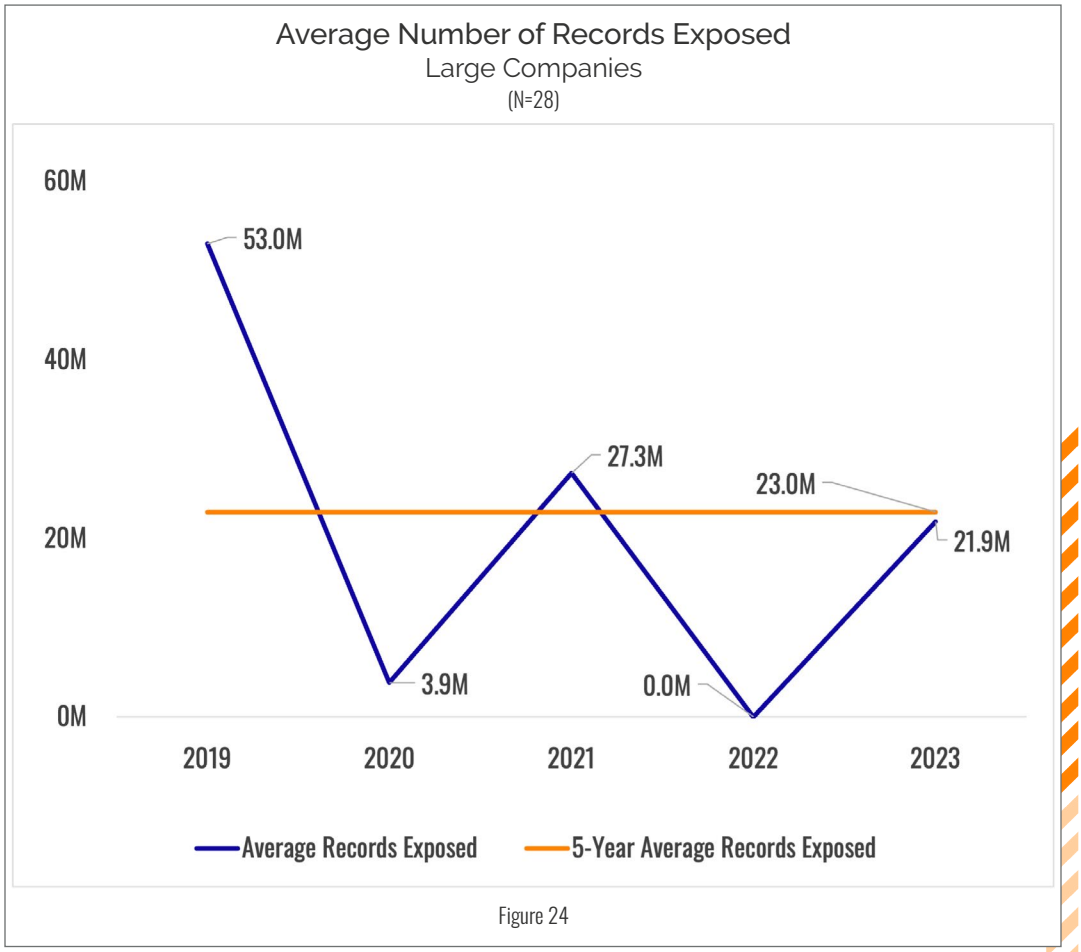


Figure 24

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—91% over five years.

As Figure 25 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.

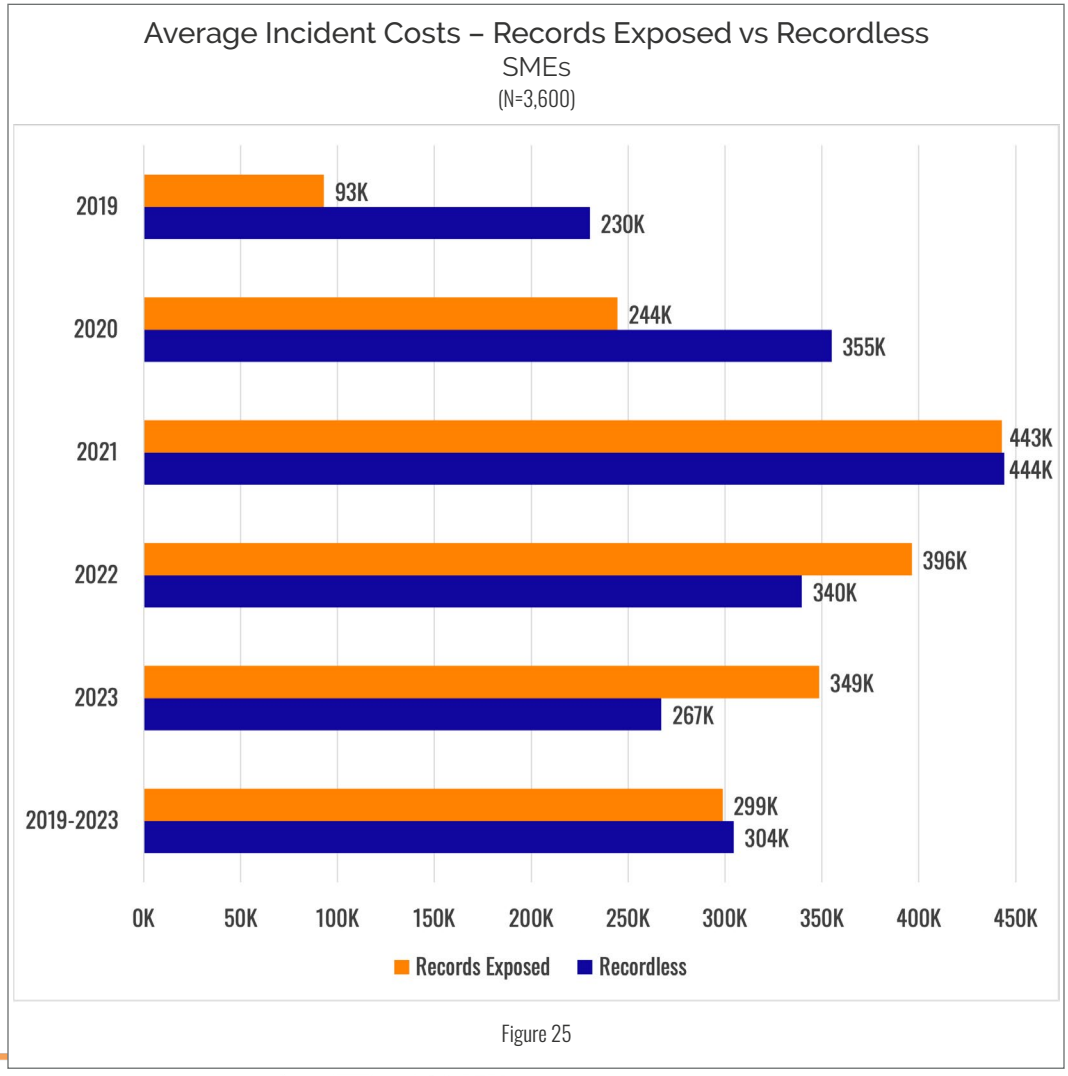


Figure 25

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

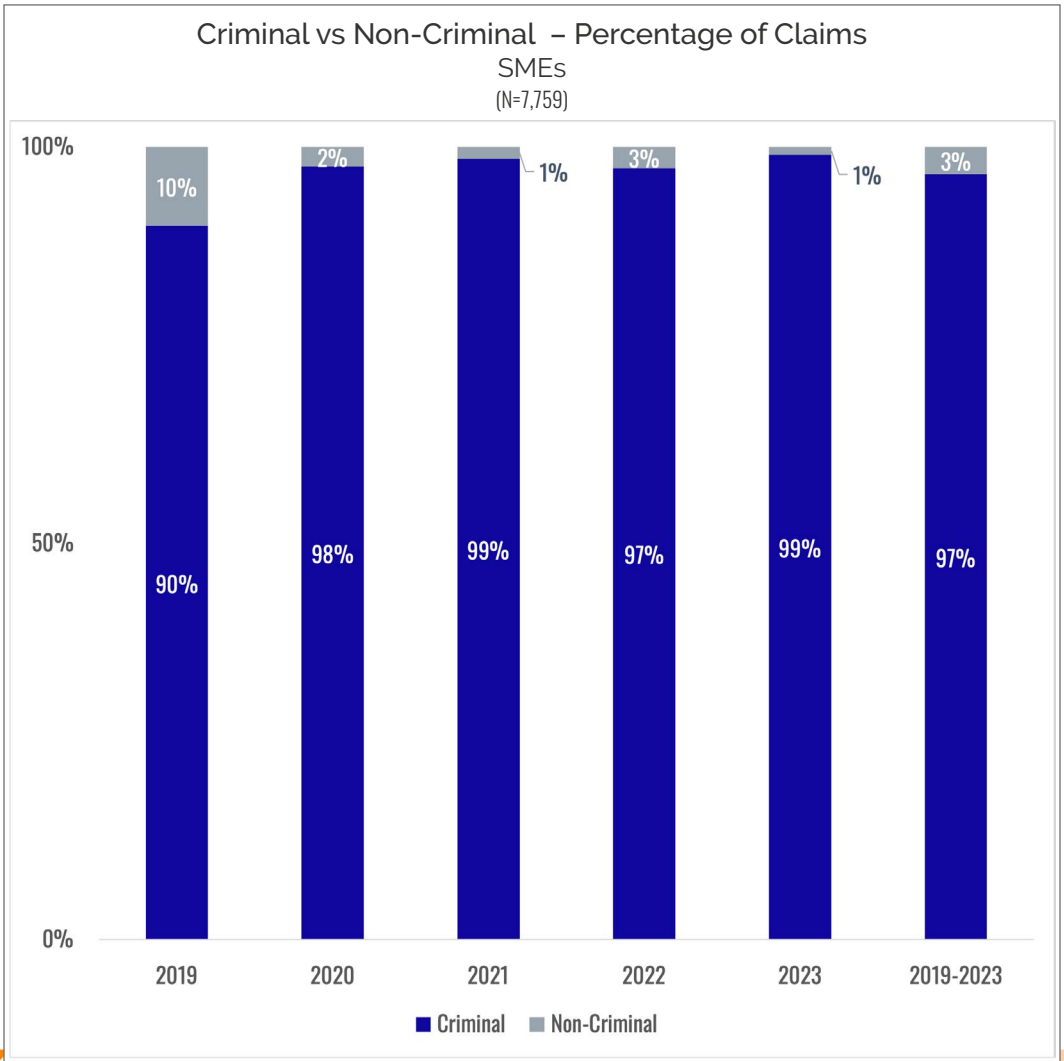


Figure 26

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 was 90% in 2019, Since then, the proportion has been ≥97%. (Figure 26, above)

Over five years, criminal incidents at SMEs were, on average, much more costly than non-criminal incidents. Four large events in 2022 involving wrongful data collection and trademark infringement (incident cost between $3M and $5M) caused the non-criminal average cost in that year to exceed the criminal average cost by a large margin. (Figure 27, below)

Comparisons of criminal to non-criminal incidents at large companies are outlined in Figures 28 and 29 below. Here, we see that 86% of incidents reported at large companies involved criminal activity. The cost of criminal incidents was dramatically higher than the cost of non-criminal ones.

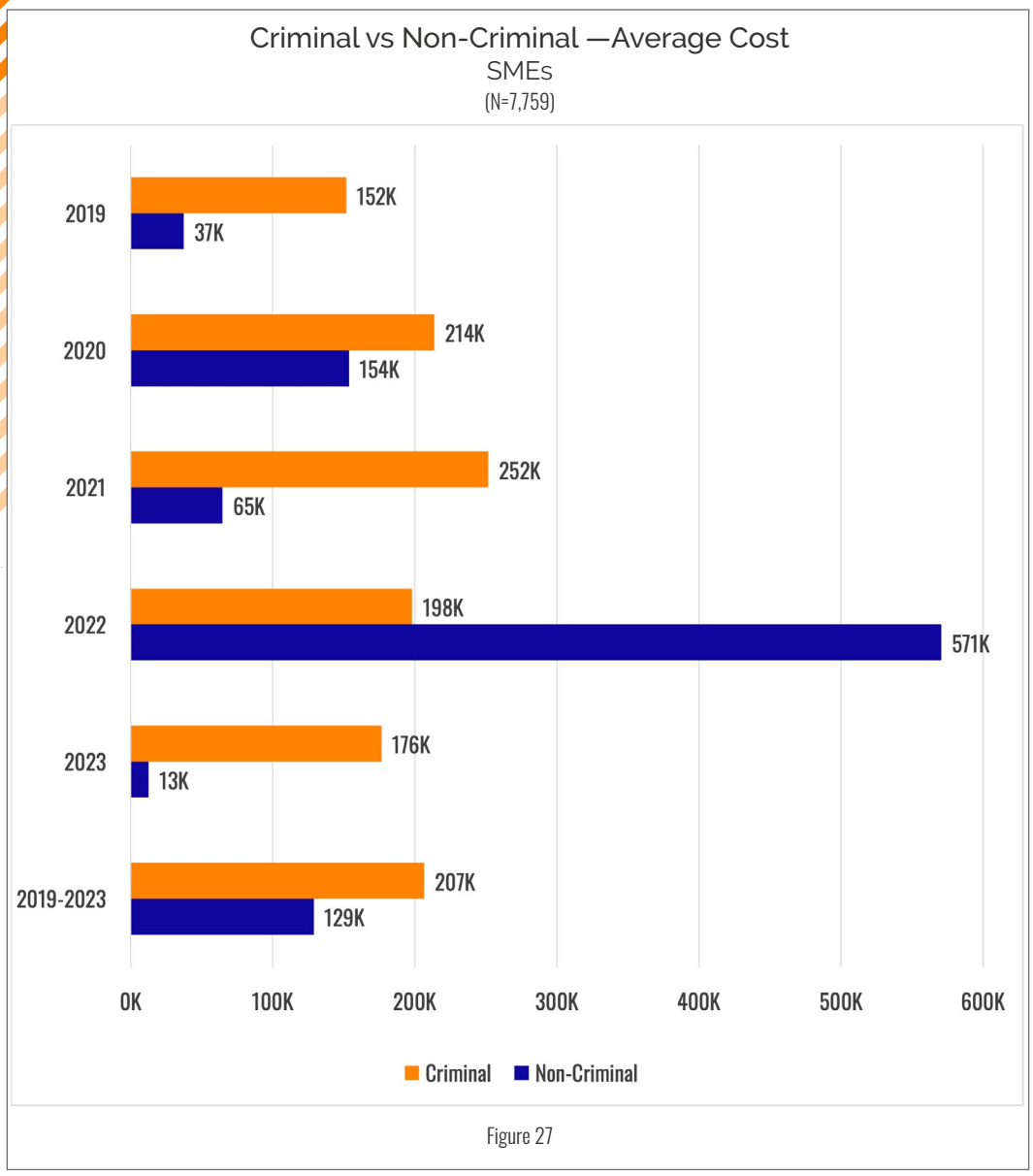


Figure 27

AI is supercharging cyberattacks, making them more sophisticated and rapid than ever before. As hackers leverage AI to enhance their capabilities, it's imperative for organizations to elevate their defenses. Regularly testing and updating your cybersecurity measures is no longer optional—it's essential. The stakes are higher, and staying ahead requires a proactive and rigorous approach to security, ensuring that your defenses are both robust and resilient against evolving threats.

Michael Bruemmer, Experian

Criminal vs Non-Criminal—SMEs
2019–2023

Time Period	Impact	Type of Activity	Average	Maximum	Total
2023	Records Exposed	Criminal	22K	487K	886K
		Non-Criminal	0K	0.1K	0.1K
	Crisis Services	Criminal	155K	25.9M	77.8M
		Non-Criminal	10K	30K	68K
	Incident Cost	Criminal	176K	30.0M	156.1M
		Non-Criminal	13K	30K	113K
2019-2023	Records Exposed	Criminal	463K	30.0M	162.9M
		Non-Criminal	72K	3K	3.5M
	Crisis Services	Criminal	100K	25.9M	610.1M
		Non-Criminal	18K	1.0M	3.1M
	Incident Cost	Criminal	207K	30.0M	1.6B
		Non-Criminal	129K	5.1M	34.7M

Table 1

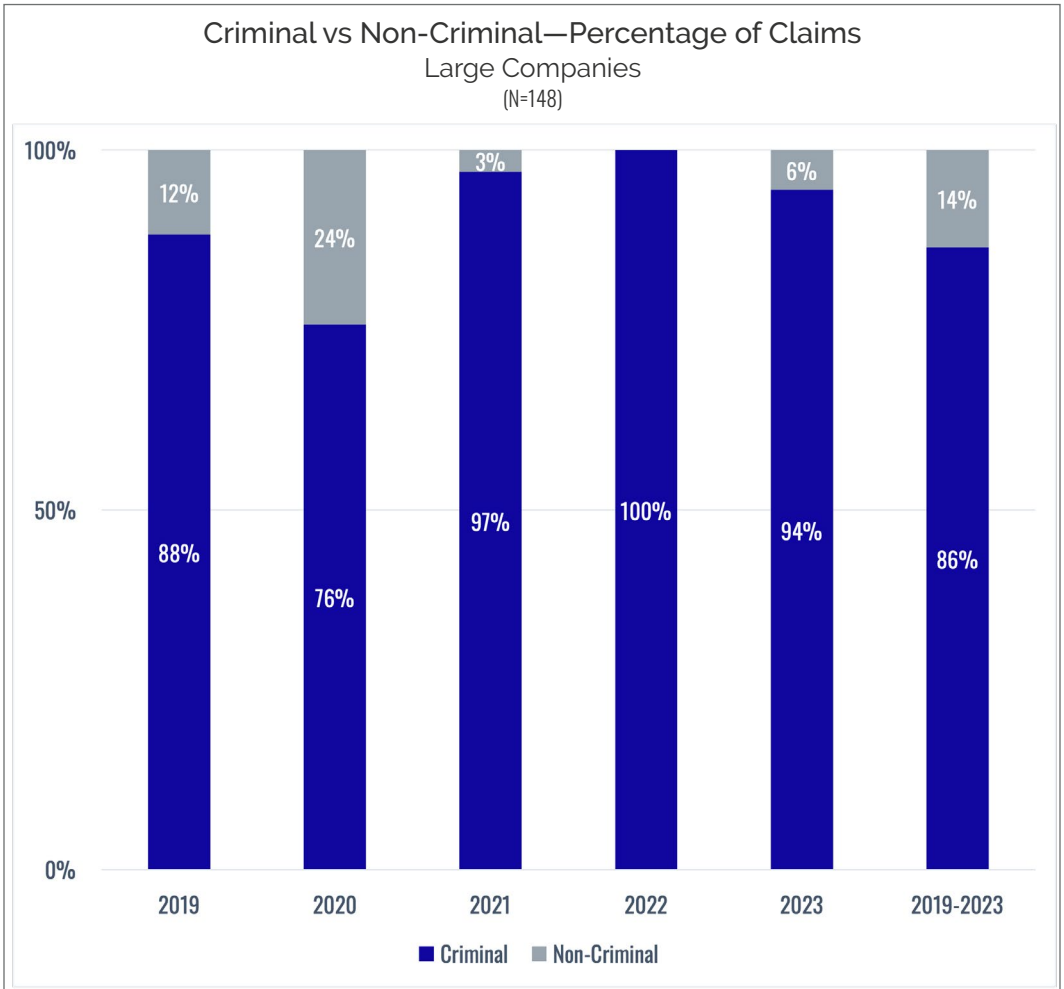

Criminal vs Non-Criminal—Percentage of Claims
Large Companies
(N=148)
100%
50%
0%
12%
88%
24%
76%
3%
97%
100%
6%
94%
14%
86%
2019
2020
2021
2022
2023
2019-2023
Criminal
Non-Criminal

Figure 28

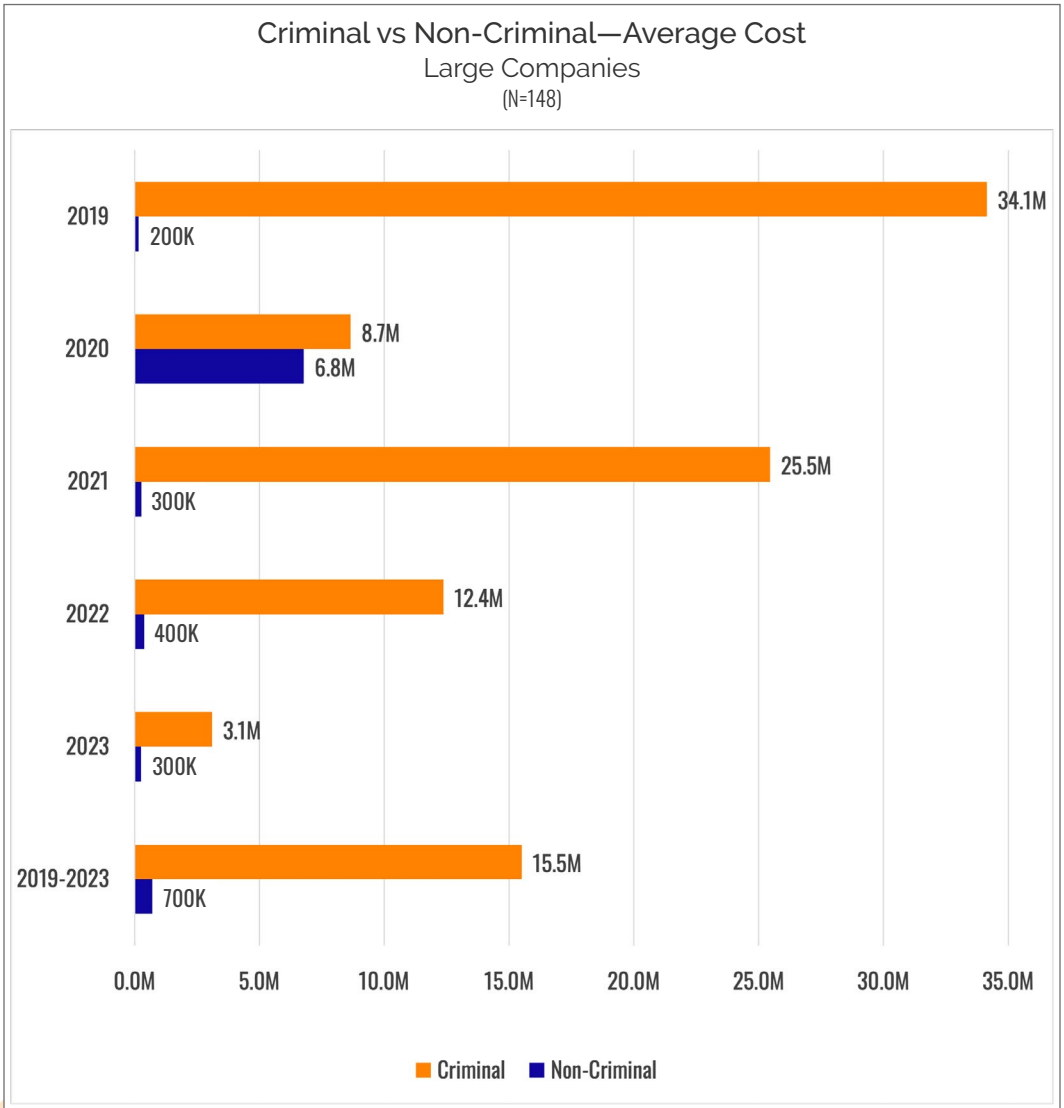

Criminal vs Non-Criminal—Average Cost
Large Companies
(N=148)
2019
34.1M
200K
2020
8.7M
6.8M
2021
25.5M
300K
2022
12.4M
400K
2023
3.1M
300K
2019-2023
15.5M
700K
0.0M
5.0M
10.0M
15.0M
20.0M
25.0M
30.0M
35.0M
Criminal
Non-Criminal

Figure 29

Self-Insured Retentions (SIR)

The dataset contained 5,233 claims for SMEs that provided an amount for SIR . These amounts ranged $0–$10M. Year-by-year averages are shown below.

The dataset contained 121 claims for large companies that reported an amount for SIR. These amounts ranged $0–$10M. The year-by-year averages are shown below. The average SIR in 2023 was almost double the SIR amount in 2020.

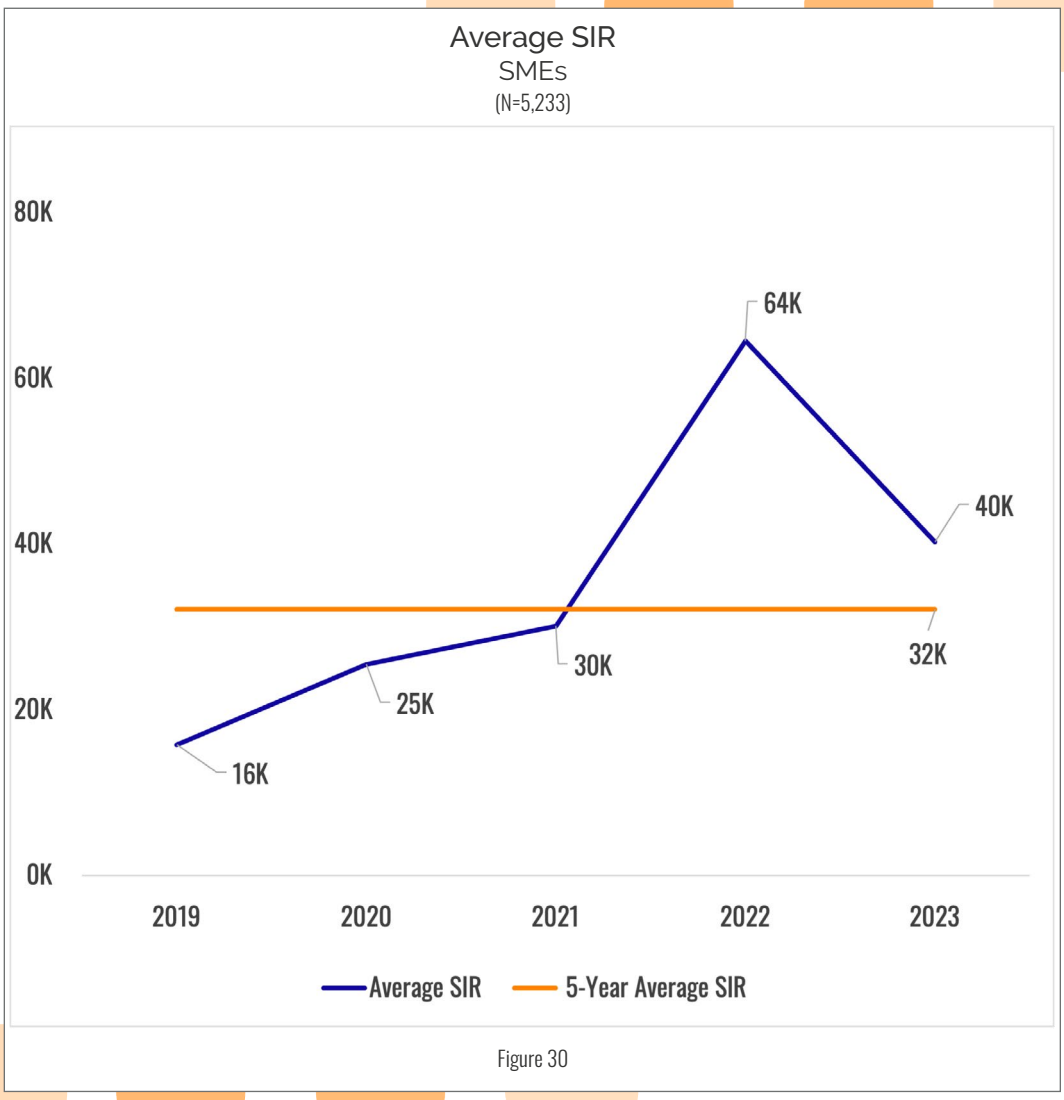


Figure 30

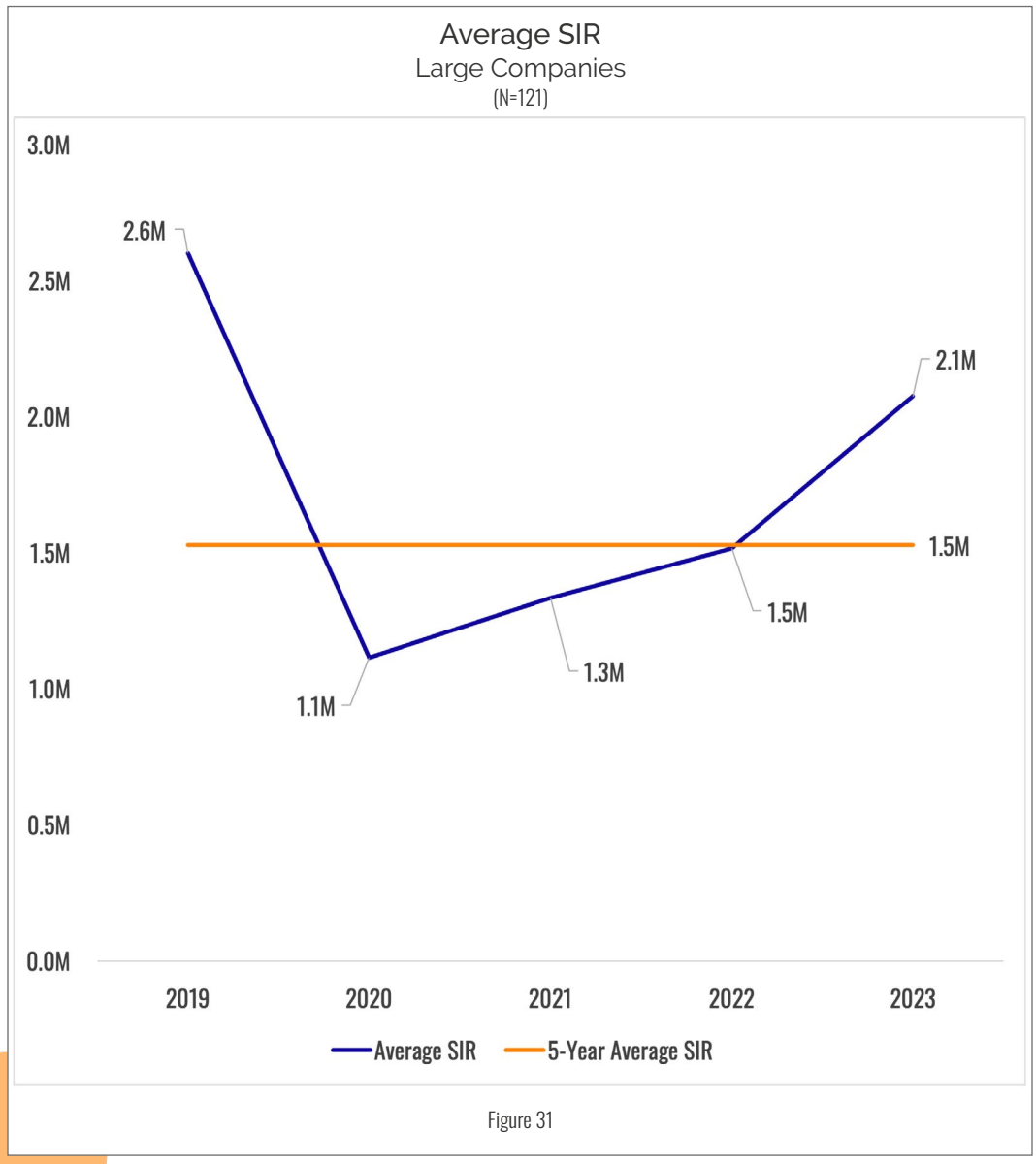

Average SIR
Large Companies
(N=121)
3.0M
2.5M
2.0M
1.5M
1.0M
0.5M
0.0M
2.6M
1.1M
1.3M
1.5M
2.1M
1.5M
2019
2020
2021
2022
2023
Average SIR
5-Year Average SIR

Figure 31

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 68% of claims and 84% of total incident cost ($1.5B). 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 4 Responsible for 68% of Claims, 84% of All Losses

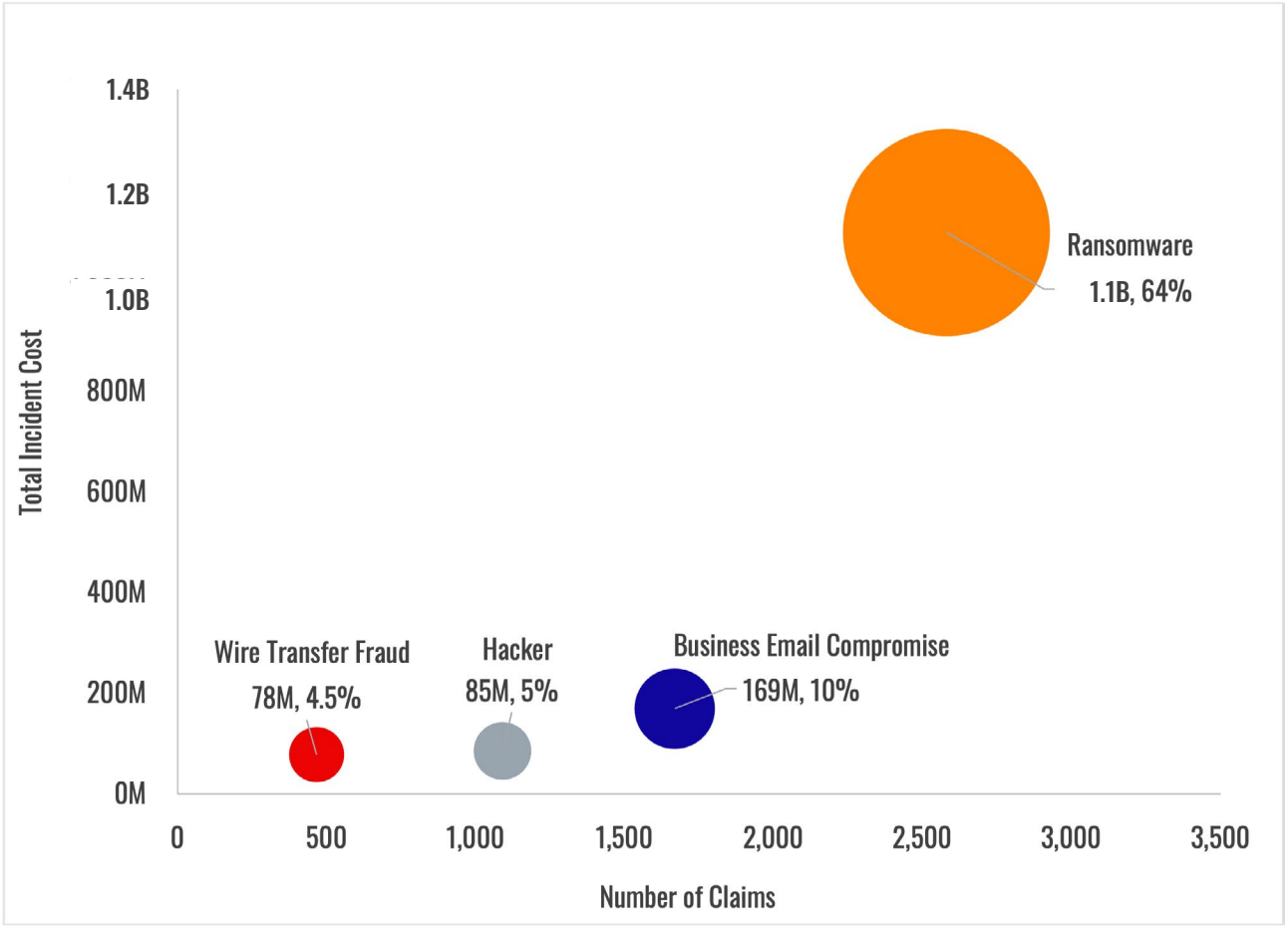


Figure 32

Ransomware remains a dominant and costly cyber threat for companies, but efforts to target this will have outsize effects on claims. Effective risk selection avoiding the most significant ransomware risk vectors, combined with vigilant monitoring for these controls, and proactive alerting are crucial strategies in preventing these attacks, thereby avoiding the substantial claims and financial losses they can incur.

Ben Duffy, KYND

Ransomware

The number of ransomware incidents increased from 553 in 2019 to 749 in 2021. For 2022 and 2023, the incident counts stand at 277 and 244 so far, with additional incidents to be added to the total in the 2025 and 2026 Cyber Claims Reports.[3] Ransom amounts and total incident cost have increased dramatically over the past five years.

The average cost of a ransomware incident decreased slightly in 2023 when compared to costs in 2020, 2021, and 2022. This is almost certainly due to the small number of ransomware claims collected for 2023 so far.

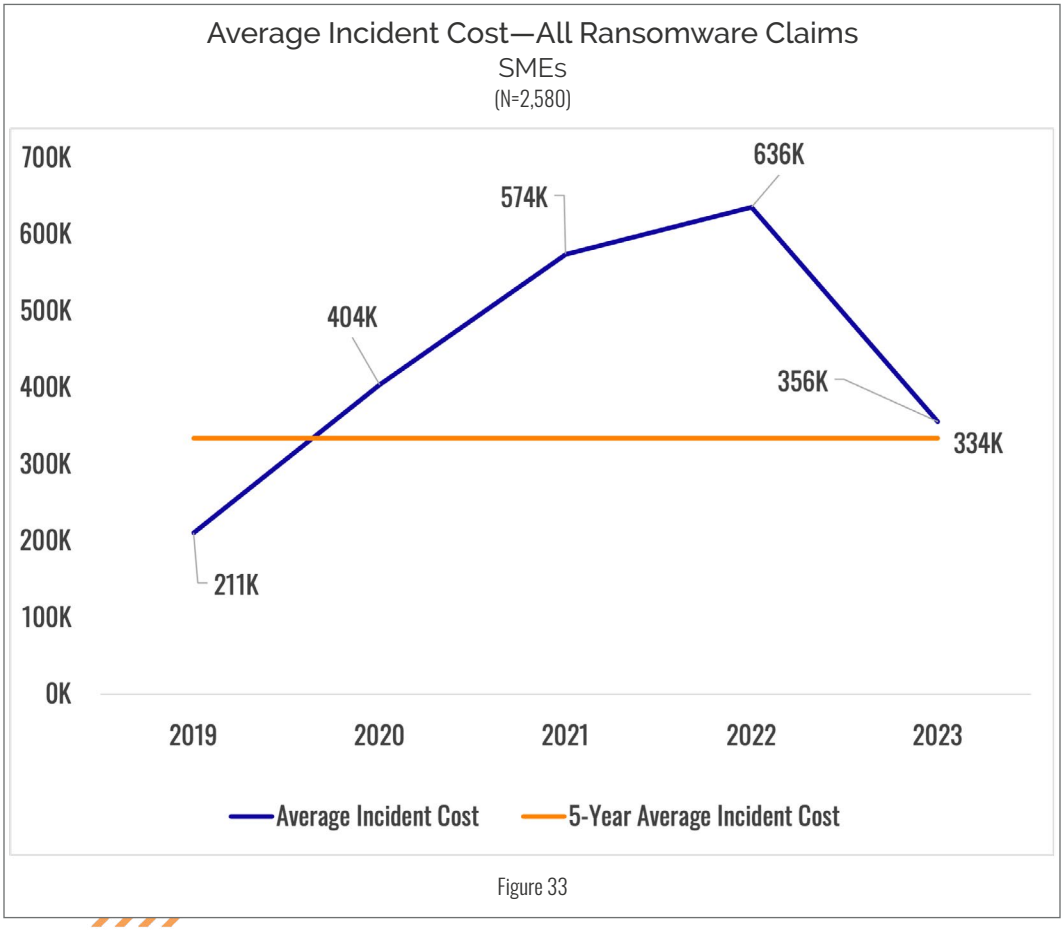


Figure 33

[3]Each year, we collect data from the three previous years. For this report (2024) we collected claims for 2021-2023. We will continue to collect claims for incidents in 2023 for two more years.

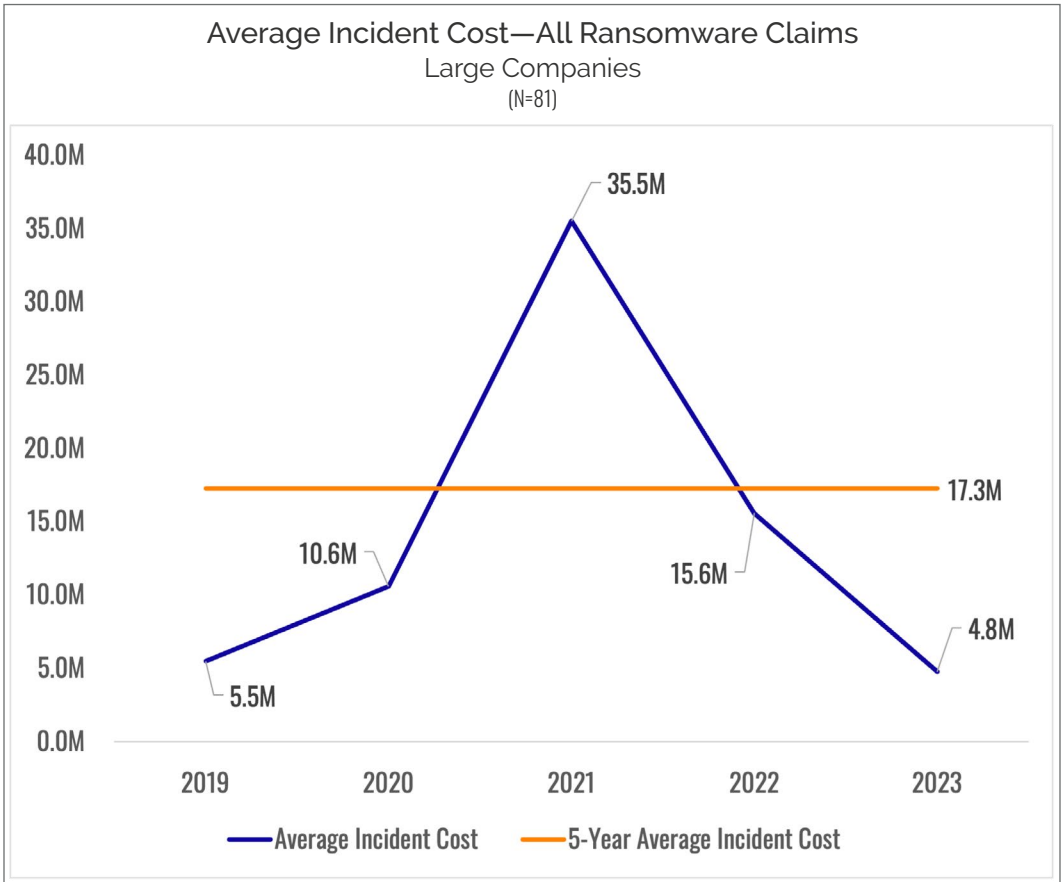

Average Incident Cost—All Ransomware Claims
Large Companies
(N=81)
40.0M
35.0M
30.0M
25.0M
20.0M
15.0M
10.0M
5.0M
0.0M
35.5M
17.3M
10.6M
15.6M
4.8M
5.5M
2019
2020
2021
2022
2023
Average Incident Cost
5-Year Average Incident Cost

Figure 34

Business Email Compromise (BEC)

BEC was the second leading cause of loss at SMEs. The number of BEC claims per year has been consistent over the past five years, ranging from 305 in 2022 to 393 in 2020. The 242 claims in 2023 are a result of limited data collection in 2024—this number will surely increase in next year's report.

The cost of BEC incidents had been dropping until 2023, from a low of $91/92K in 2019-2020 to a high of $193K in 2023.

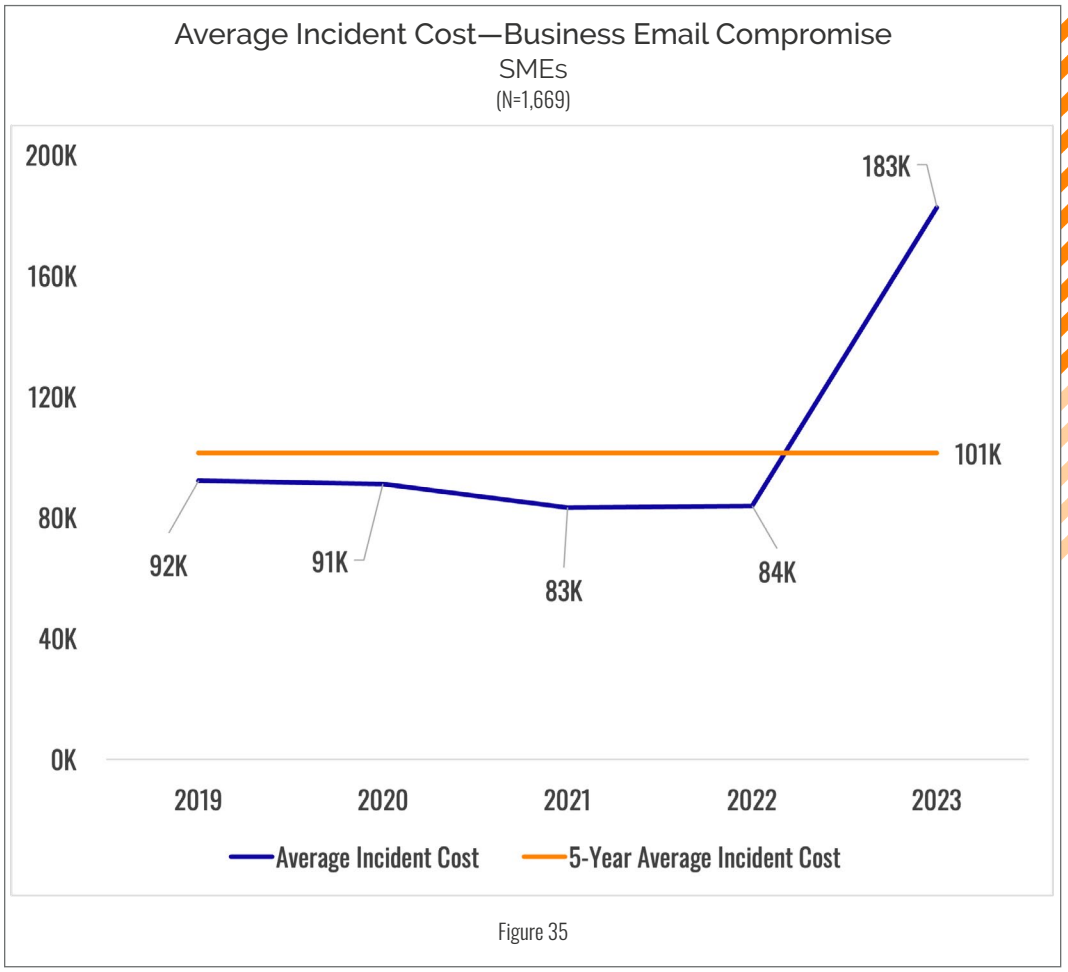


Figure 35

The consistency of the number of BEC claims impacting SMEs highlights the effectiveness of social engineering and the ongoing need for effective training and preventative measures. MFA cannot be viewed as a silver bullet. The implementation of preventative protocols and tools is a must.

Lindsay B. Nickle, Partner & Vice-Chair, Constangy Cyber Team

Hackers

Hackers were the third leading cause of loss at SMEs. Figure 36 below tells the good news: based on the five-year data, the average cost of a hacking incident has dropped since 2019 and has remained low since then.

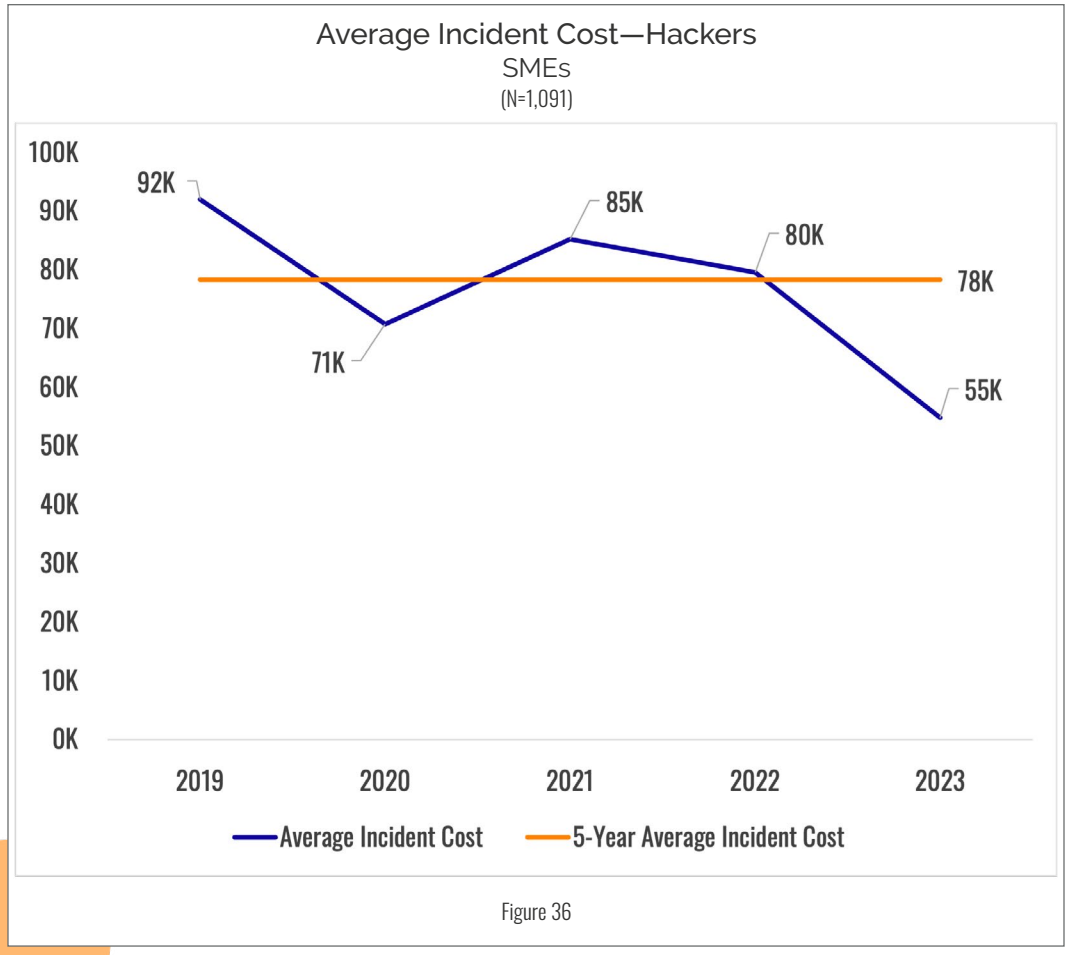


Figure 36

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=$70M). Based upon the five-year data, the average cost of a wire transfer fraud incident has dropped steadily since 2019.

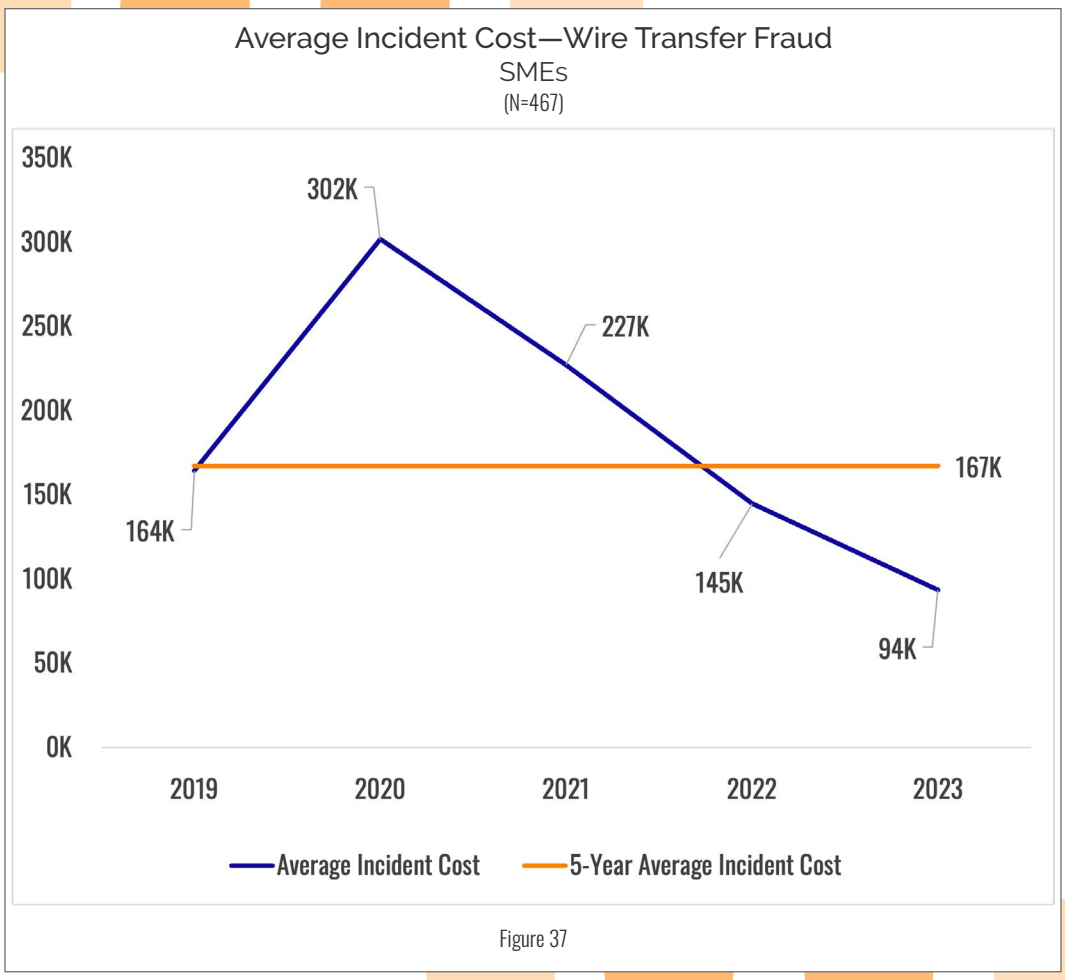


Figure 37

Staff Mistakes

Over the period 2019-2023, the number of incidents involving staff mistakes and programming errors has been steadily declining. The number of claims during the current five-year period (2019–2023) has decreased to 150 from 235 reported last year.

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

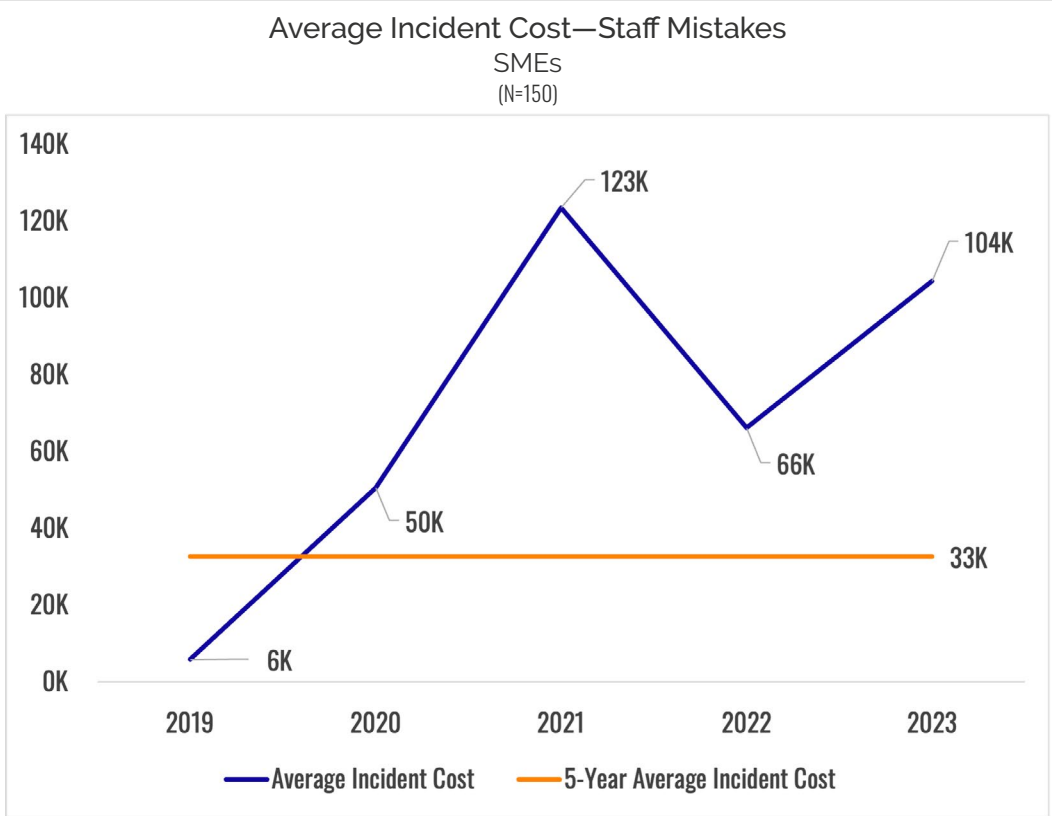


Figure 38

Rogue Employees

Over the past five years, the number and magnitude of incidents caused by malicious employees and ex-employees have also been declining. The number of incidents decreased from 65 in 2019 to 7 in 2023. The average incident cost decreased from $116K in 2020 to $25K in 2023.

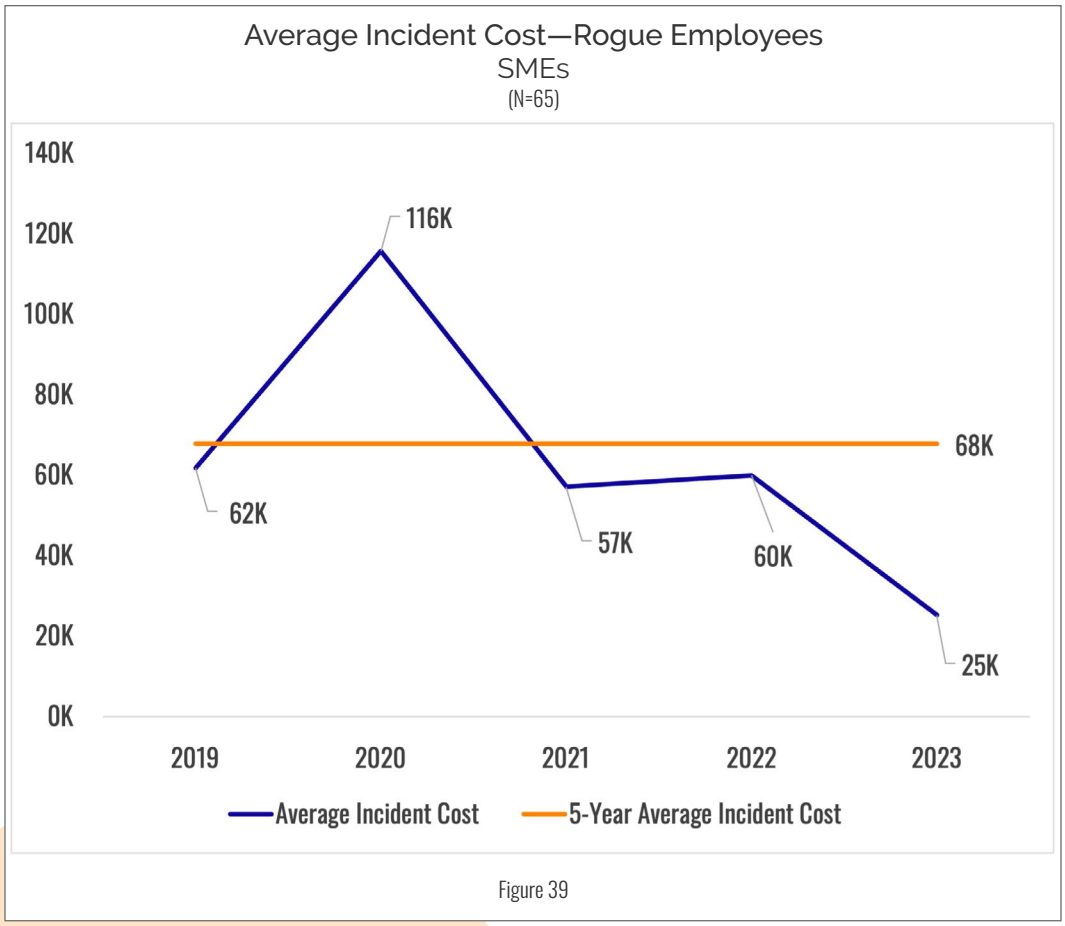


Figure 39

Third-party Incidents

Third-party incidents can be caused by both malicious and non-malicious actors, and they remain a notable cause of loss. Since 2019, the cost of third-party events caused by malicious actors has been much greater than events stemming from non-malicious accidents or mistakes.

Unfortunately, the cost of a third-party incident caused by a malicious actor has increased dramatically since 2019. We may expect the 2023 numbers to rise as more claims are collected over the next two cycles.

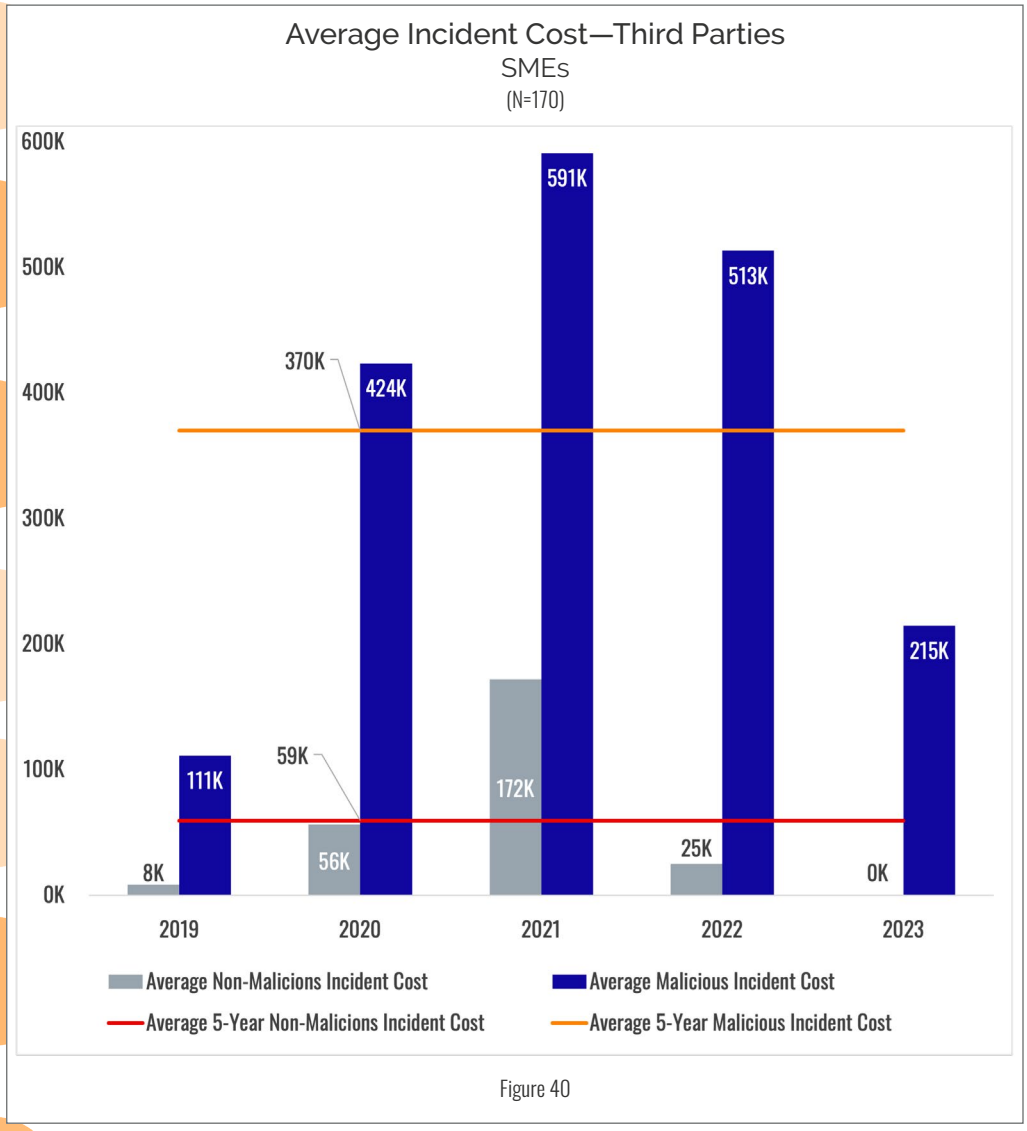


Figure 40

In today's interconnected world, a cyberattack can ripple through the supply chain, impacting not just direct partners but fourth, fifth, and even sixth-party vendors within the supply chain. Targeting the intersection of data and technology, each attack has the potential to affect thousands of businesses and millions of consumers. Adopting a concentric circle of protection is crucial. This involves three key elements rooted in awareness, rapid response, and layered defenses. Integrating these strategies helps to create a robust defense against the expansive reach of modern cyberattacks.

Michael Bruemmer, Experian

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
- Healthcare
- Manufacturing
- Financial Services
- Retail

These five sectors accounted for 52% of all claims and 59% 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 50% of Claims, 58% of All Losses

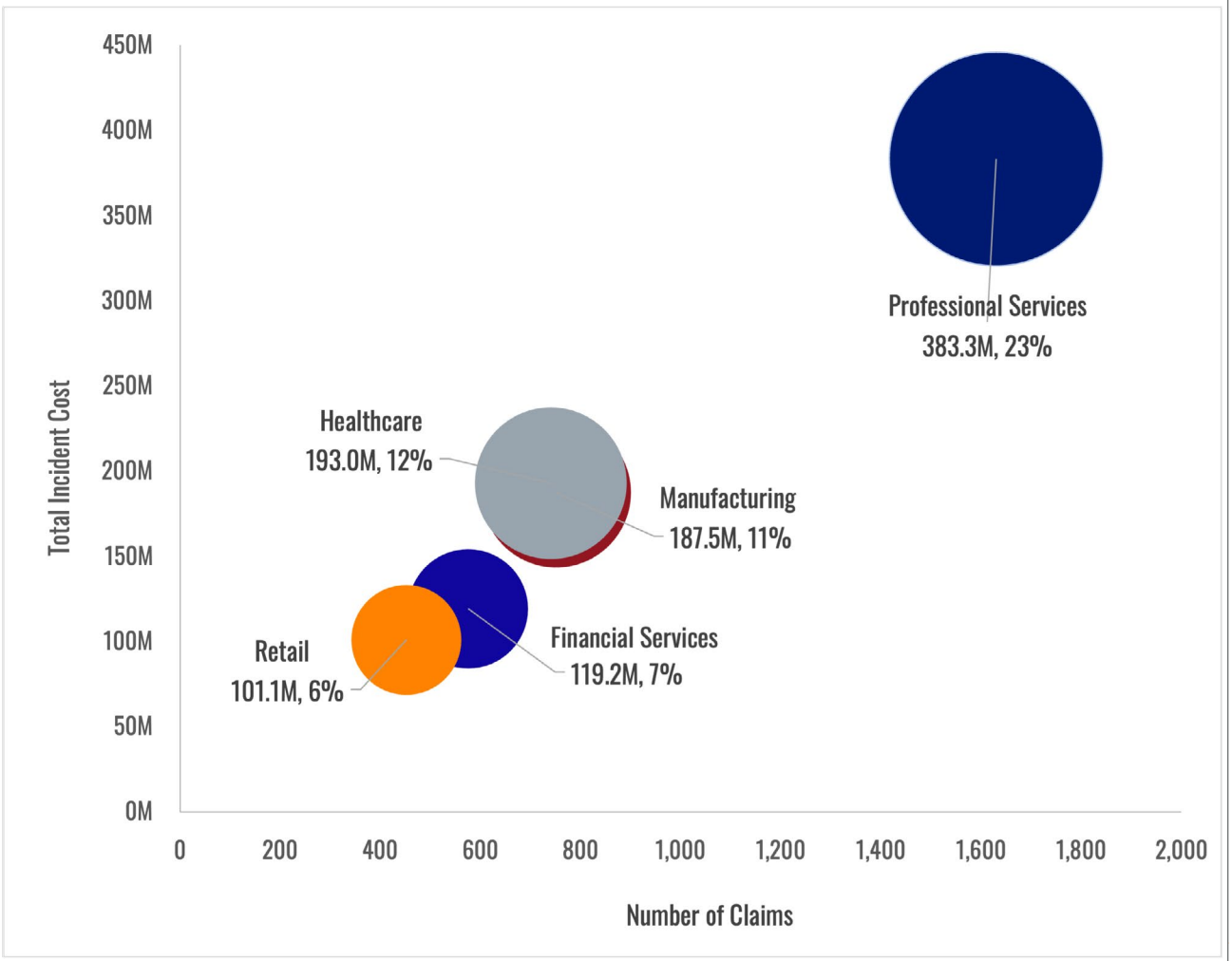


Figure 41

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: $55M and $1.5B.

At SMEs, professional services claims accounted for 20% of all claims and 23% 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 2023 Claims Study: ransomware, BEC, and hackers.

Figure 42 shows the year-by-year and five-year average incident cost for this sector.

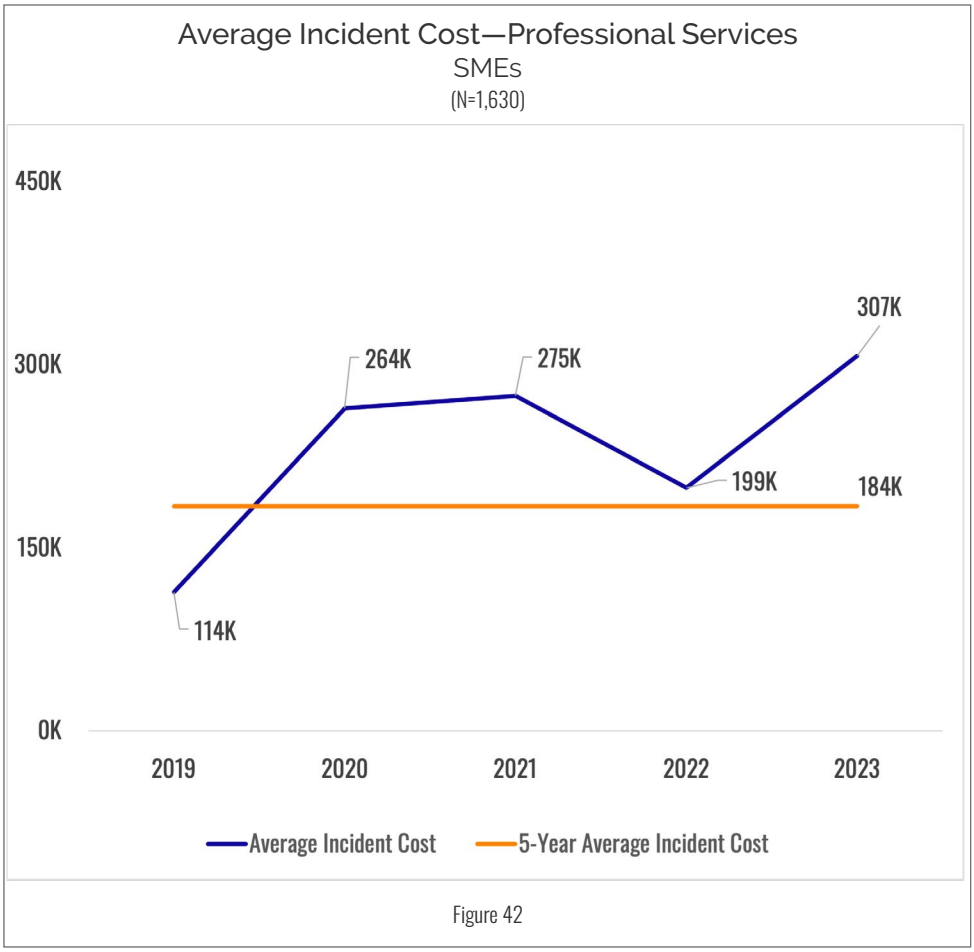
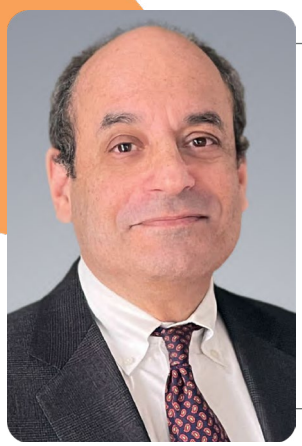


Figure 42



This study shows the resilience of cyber criminals and the inconsistency of their tactics. While increased law enforcement efforts and international cooperation have reduced the number of overall incidents, ransomware and BECs continue at a brisk pace. Attackers have more widely distributed their activities to less experienced operators, making their demands less consistent and exploits less successful. One point of consistency remains—attackers remain focused on industries with the most at risk in the event to data loss—professional services and health care.

Richard Goldberg, Partner & Vice-Chair, Constangy Cyber Team

Manufacturing

The average annual revenue of organizations in the manufacturing sector was $124M (maximum=$1.9B).

Manufacturing claims accounted for 9% of all claims and 11% of total incident cost at SMEs. Total incident cost ranged from 1K to $13.6M. The top causes of loss were ransomware, BEC, and wire transfer fraud.

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

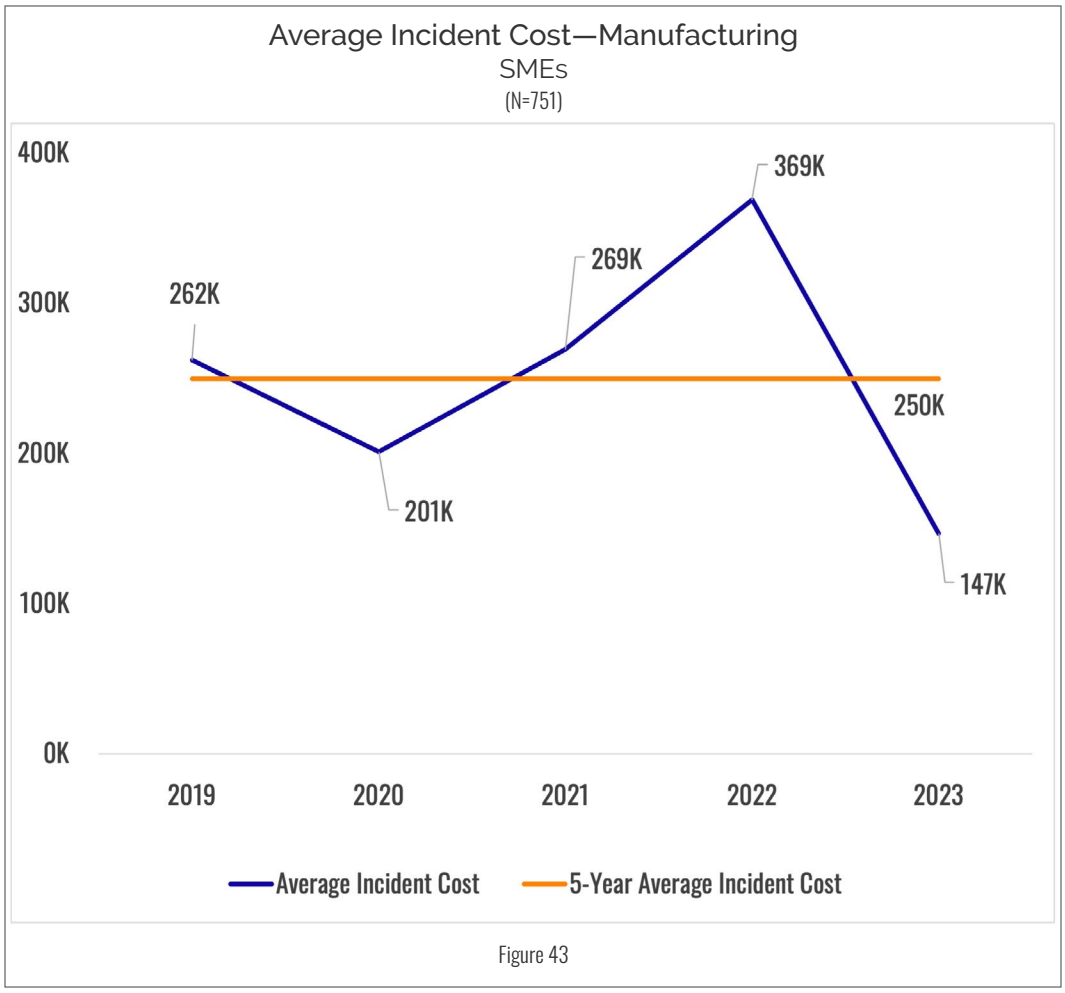


Figure 43

Healthcare

The average annual revenue of organizations in the healthcare sector was $100M (maximum=$1.95B). Healthcare claims accounted for 11% of all claims and 12% of total incident cost at SMEs.

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

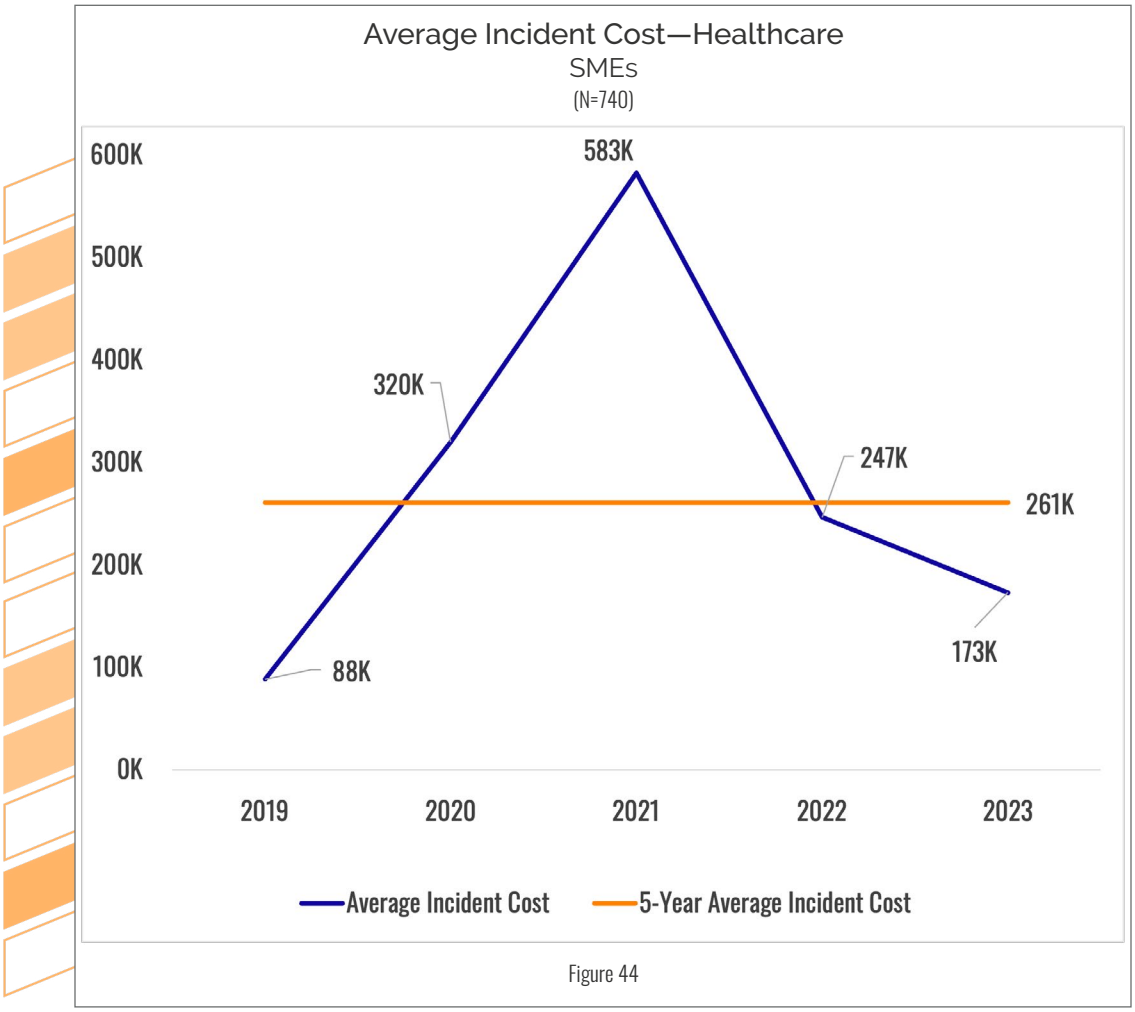


Figure 44

Financial Services

The average annual revenue of organizations in the financial services sector was $88M (maximum=$1.7B). Financial services claims accounted for 7% of all claims and 7% of total incident cost at SMEs. Total incident cost ranged from 1K to $4.8M. 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.

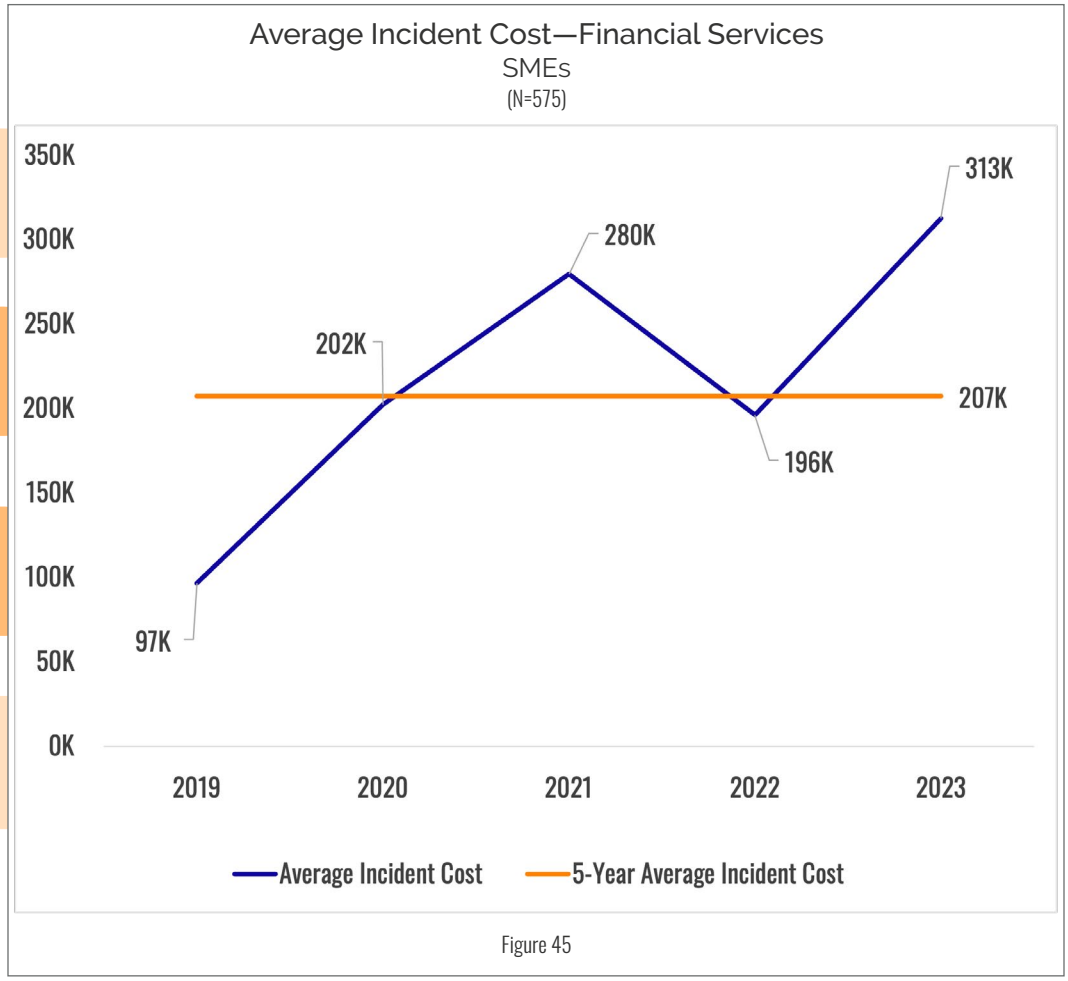


Figure 45

This study aligns with our experience in handling approximately 3,000 incidents this past year, especially as it relates to increased average legal costs. As the leader of our firm's cybersecurity litigation practice, I can report that breaches that result in large notifications are much more likely to trigger class actions than before, especially in the healthcare and financial services industries.

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

Retail

The average annual revenue of organizations in the retail sector was $121M (maximum=$1.9B). Retail claims accounted for 6% of all claims and 7% of total incident cost at SMEs. Total incident cost ranged from 1K to $7.5M. The three top causes of loss were ransomware, and BEC, hackers.

Figure 46 below shows the year-by-year and five-year average incident cost for this sector.

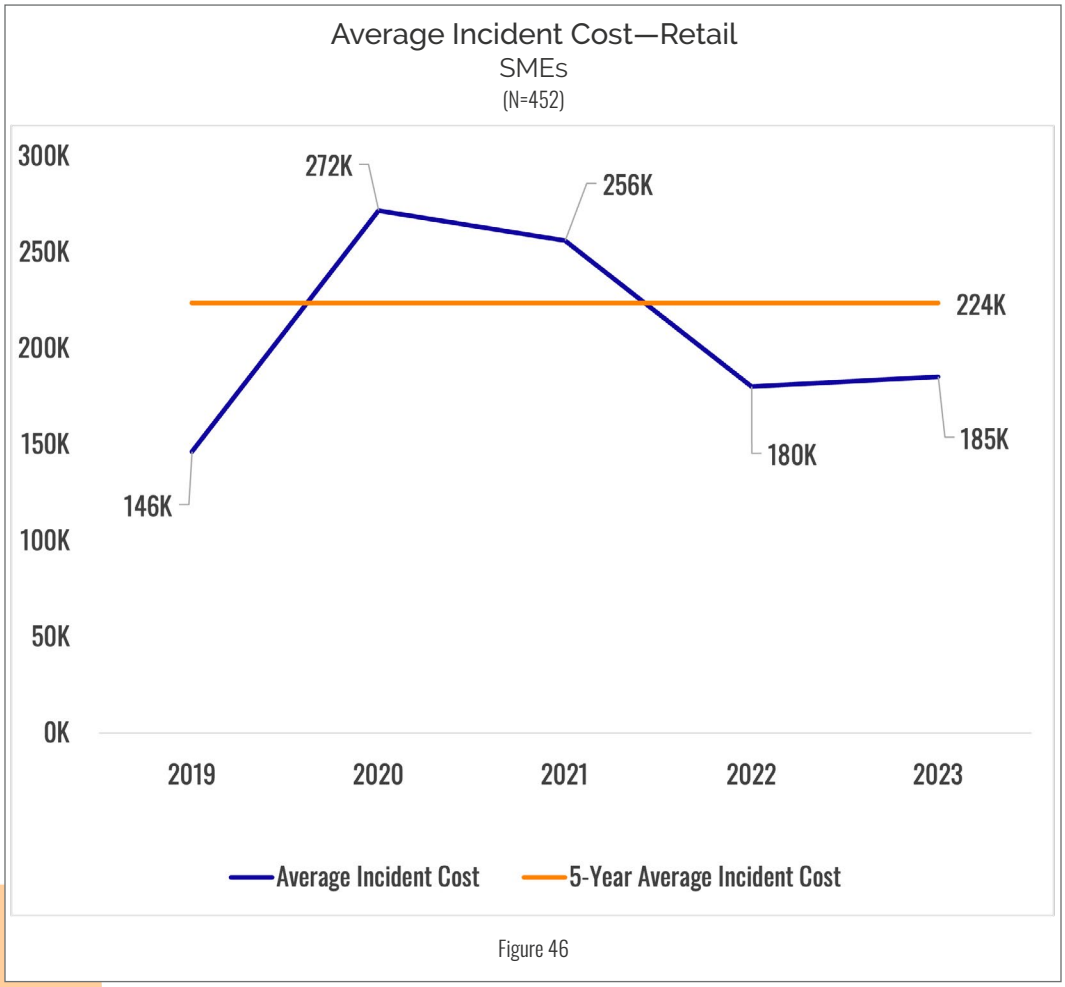


Figure 46

Public Entities

The average annual revenue for public entities was $105M (maximum=$1.2B). Claims from public entities represent around 4% of all claims and 3% of total incident cost. Total incident cost ranged from 1.5K to $2.3M. The average incident cost has been about the same each year since 2019. Top causes of loss were ransomware, BEC, and wire transfer fraud.

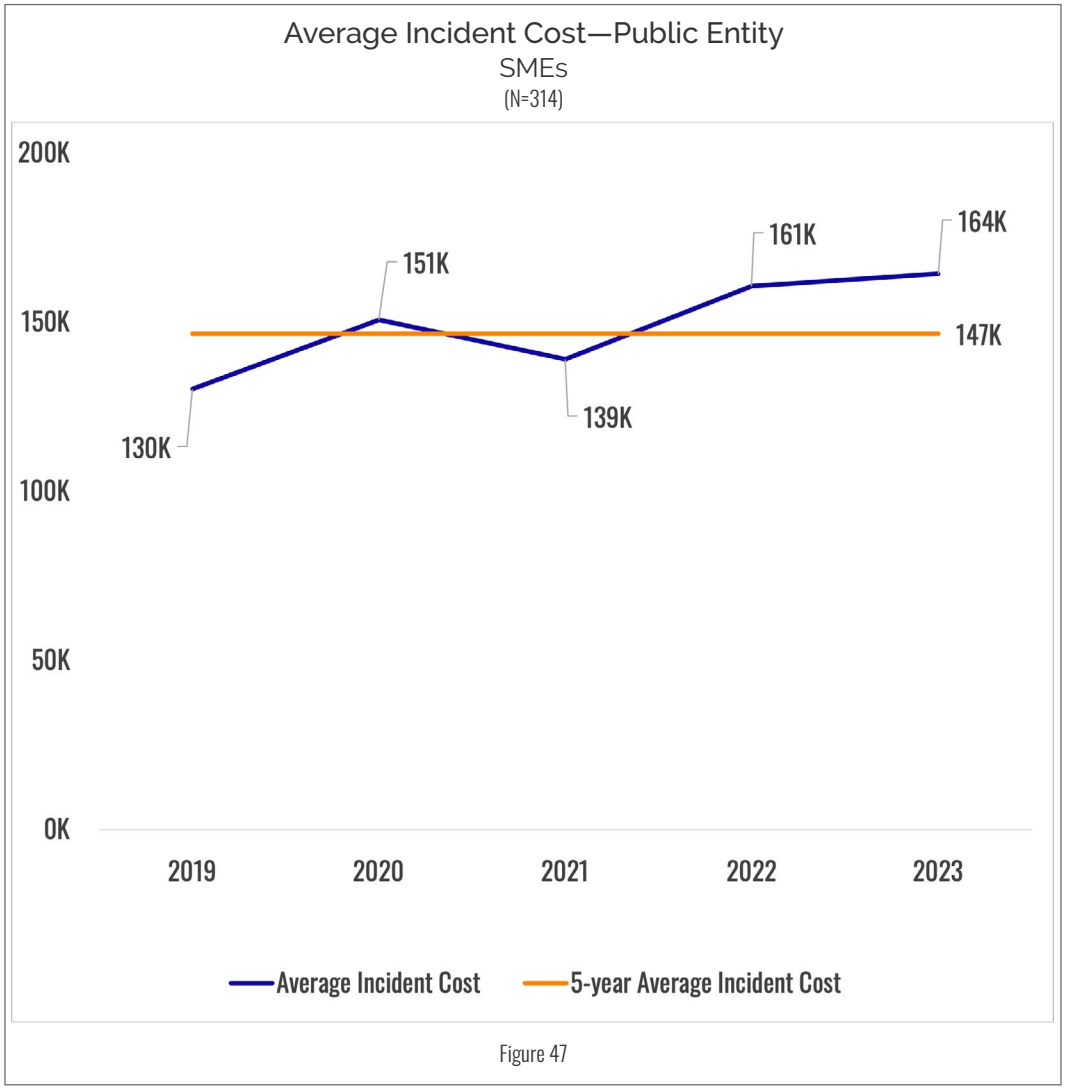


Figure 47

Claims from Canada

Although claims from Canada comprise only 1.5% of total submissions, these incidents represent an important subset of the dataset. The average annual revenue of a Canadian organization in this study was 471M USD (maximum=17B USD). The average five-year total incident cost was 584K USD (maximum=15M USD).

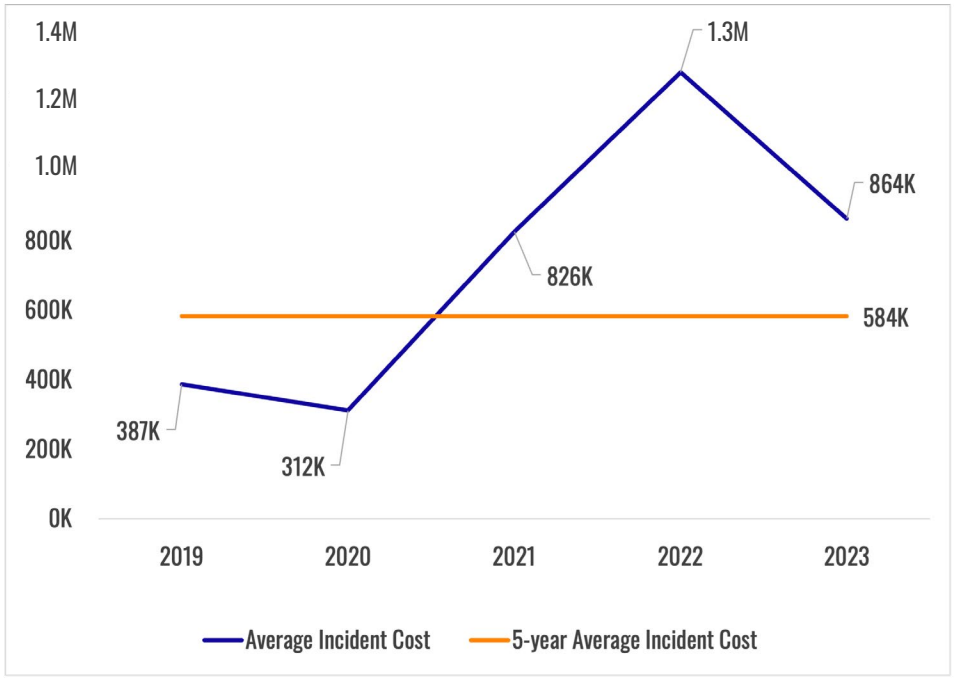


Figure 48

Canada
Top Causes of Loss
2019–2023

Cause of Loss	Claims	Average Incident Cost
Ransomware	49	1.0M
Business Email Compromise	24	150K
Hacker	15	113K
Staff Mistake	8	29K
Malware/Virus	6	533K
Wire Transfer Fraud	5	44K

Table 2

Despite the relatively low frequency of cyber incidents in Canada, the significant financial impact on high-revenue organizations highlights the urgent need for robust cybersecurity measures. Proactive risk management and incident response planning are essential to safeguard against evolving threats.

Tabish Gill, Risk Consulting Partner, RSM Canada

Conclusion

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

This year, almost 5,000 new claims were submitted. These were added to an existing dataset of over 5,500 claims. The result has been a comprehensive dataset of cyber claims incidents, including their causes and monetary impacts.

In 2024, the most insurers and brokers ever have participated in the study and have shared even more claims and more information about each claim.

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 2024 study.

At-Bay

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

AXA XL

Beazley

Berkley Cyber Risk Solutions

CFC

Cowbell

Crum & Forster

Great American Insurance Group

Intact Insurance

Liberty Mutual

Markel

Tokio Marine HCC

Travelers–US

Travelers–Canada

***Insurers**: We invite you to join this elite group of participating companies. We'll be starting next year's study in January. Contact us at cyberclaims@netdiligence.com.*

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.

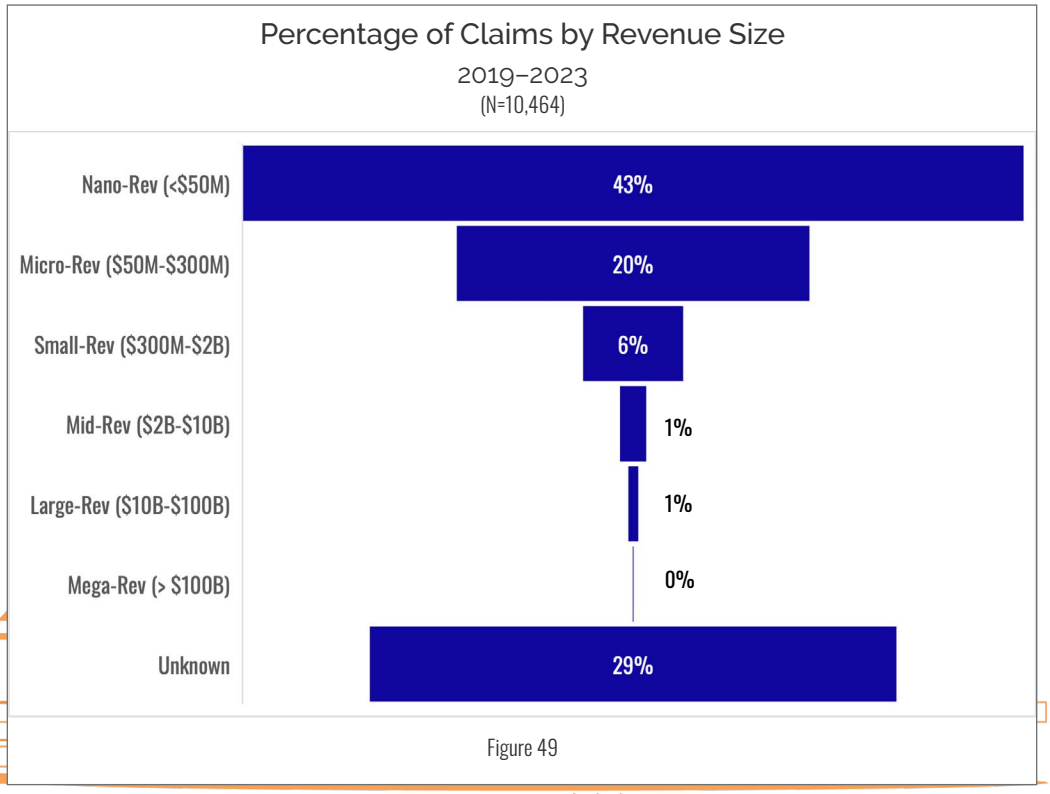


Figure 49

Incident Cost by Revenue Size
Claims ≥ $1K
2019–2023

Revenue Size	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Nano-Rev (<$50M)	3,891	1K	139K	10.4M	539.3M	14%	1	6
Micro-Rev ($50M–$300M)	1,584	1K	317K	10.4M	502.7M	13%	3	5
Small-Rev ($300M–$2B)	405	1K	1.8M	108.0M	746.8M	19%	4	4
Mid-Rev ($2B–$10B)	112	1K	4.7M	111.0M	530.6M	14%	5	3
Large-Rev ($10B–$100B)	42	10K	33.3M	503.5M	1.4B	36%	6	1
Mega-Rev (>$100B)	3	10.6M	26.1M	55.0M	78.2M	2%	7	2
Unknown	2,401	1K	50K	2.7M	120.9M	3%	2	7

Table 3

Average Crisis Services Costs by Revenue Size
Claims ≥ $1K
2019–2023

Revenue Size	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Nano-Rev (<$50M)	37K	26K	2K	16K	73K	77K	6
Micro-Rev ($50M–$300M)	74K	35K	12K	25K	137K	155K	5
Small-Rev ($300M–$2B)	238K	188K	80K	127K	307K	614K	4
Mid-Rev ($2B–$10B)	315K	991K	54K	61K	867K	1.1M	3
Large-Rev ($10B–$100B)	4.6M	1.1M	0K	2.9M	643K	5.0M	1
Mega-Rev (>$100B)	0K	0K	0K	0K	0K	4.9M	2
Unknown	8K	1K	0K	4K	101K	15K	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.

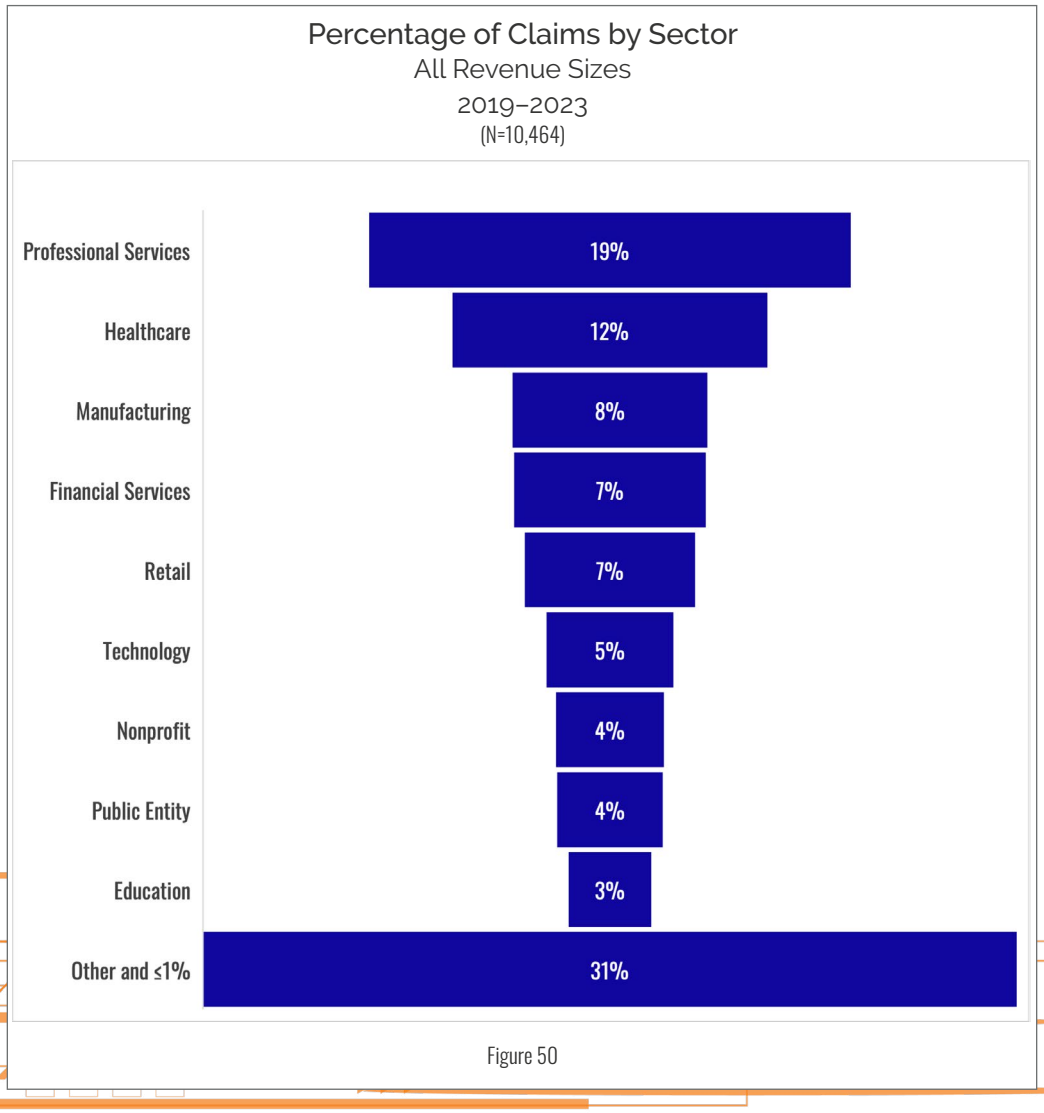


Figure 50

Incident Cost by Sector—SMEs
2019–2023

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Agriculture	1	11K	11K	11K	11K	0.0%	20	21
Education	254	2K	131K	2.0M	33.2M	2.0%	10	18
Energy	37	10K	653K	15.0M	24.1M	1.4%	15	3
Entertainment	38	4K	343K	2.6M	13.0M	0.8%	14	8
Financial Services	575	1K	207K	4.8M	119.2M	7.0%	5	14
Gaming & Casino	4	20K	160K	532K	639K	0.0%	18	16
Health services	1	267K	267K	267K	267K	0.0%	20	9
Healthcare	738	1K	261K	17.6M	192.5M	11.3%	4	10
Hospitality	116	2K	165K	2.6M	19.1M	1.1%	12	15
Manufacturing	751	1K	250K	13.6M	187.5M	11.1%	3	11
Media	52	2K	462K	5.1M	24.0M	1.4%	13	6
Nonprofit	368	1K	117K	2.9M	43.0M	2.5%	8	19
Professional Services	1,630	1K	235K	30.0M	383.3M	22.6%	2	12
Public Entity	314	2K	147K	2.3M	46.1M	2.7%	9	17
Restaurant	19	2K	579K	5.2M	11.0M	0.6%	17	4
Retail	452	1K	224K	7.5M	101.1M	6.0%	6	13
Technology	399	1K	656K	17.6M	261.7M	15.4%	7	2
Telecommunications	28	18K	934K	8.7M	26.2M	1.5%	16	1
Transportation	130	1K	418K	15.0M	54.3M	3.2%	11	7
Other	2,368	1K	65K	5.2M	154.9M	9.1%	1	20
Unknown	3	174K	537K	959K	1.6M	0.1%	19	5

Table 5

Average Crisis Services Costs by Sector—SMEs
2019–2023

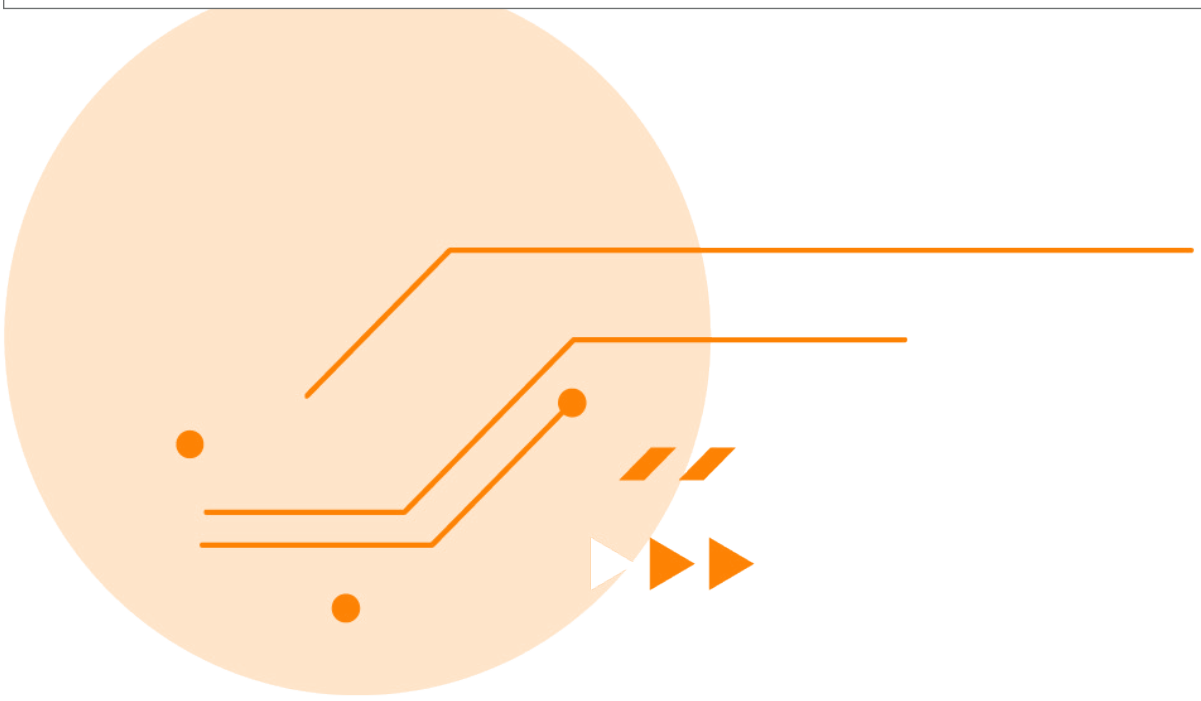
Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Agriculture	4K	0K	0K	7K	0K	11K	21
Education	59K	11K	4K	18K	115K	97K	10
Energy	154K	1K	1K	47K	100K	207K	2
Entertainment	27K	34K	2K	23K	31K	56K	17
Financial Services	59K	60K	32K	22K	126K	123K	8
Gaming & Casino	47K	0K	0K	3K	3K	51K	18
Health services	10K	0K	0K	7K	0K	17K	20
Healthcare	66K	67K	2K	21K	95K	140K	5
Hospitality	44K	8K	2K	12K	82K	80K	12
Manufacturing	56K	10K	3K	23K	87K	122K	9
Media	40K	2K	1K	15K	148K	123K	7
Nonprofit	54K	15K	2K	16K	68K	79K	13
Professional Services	51K	38K	7K	29K	169K	137K	6
Public Entity	48K	12K	5K	19K	134K	89K	11
Restaurant	42K	47K	5K	13K	61K	73K	15
Retail	39K	19K	1K	17K	58K	71K	16
Technology	78K	54K	14K	42K	87K	190K	4
Telecommunications	174K	457K	267K	57K	122K	539K	1
Transportation	58K	4K	4K	40K	154K	203K	3
Other	12K	0K	0K	4K	85K	31K	19
Unknown	0K	44K	0K	30K	0K	74K	14

Table 6

Incident Cost by Sector—Large Companies
2019–2023

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%	12	7
Education	4	226K	951K	2.4M	3.8M	0.2%	9	12
Energy	3	608K	2.4M	5.0M	7.3M	0.4%	10	11
Financial Services	30	2K	19.4M	350.0M	582.8M	29.0%	1	2
Healthcare	26	3K	9.7M	60.0M	252.4M	12.6%	2	5
Manufacturing	16	29K	10.5M	55.0M	167.4M	8.3%	5	4
Professional Services	13	72K	3.2M	13.2M	41.7M	2.1%	7	9
Public Entity	1	2.5M	2.5M	2.5M	2.5M	0.1%	12	10
Restaurant	2	10K	603K	1.2M	1.2M	0.1%	11	13
Retail	14	1K	13.6M	111.0M	190.6M	9.5%	6	3
Technology	18	46K	7.4M	60.0M	132.8M	6.6%	4	6
Telecommunications	1	503.5M	503.5M	503.5M	503.5M	25.1%	12	1
Transportation	5	200K	351K	598K	1.8M	0.1%	8	14
Other	24	18K	4.8M	65.8M	114.8M	5.7%	3	8

Table 7



Average Crisis Services Costs by Sector—Large Companies
2019–2023

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Education	192K	54K	16K	53K	123K	341K	11
Energy	449K	0K	210K	79K	50K	683K	10
Financial Services	7.5M	0K	0K	23K	0K	1.9M	5
Healthcare	101K	2.4M	94K	50K	596K	888K	8
Manufacturing	651K	5K	14K	783K	1.1M	2.4M	3
Professional Services	164K	792K	67K	106K	56K	2.1M	4
Public Entity	1.1M	647K	0K	84K	2K	1.8M	6
Restaurant	162K	415K	0K	0K	159K	736K	9
Retail	1.4M	155K	0K	4.5M	1.2M	3.4M	2
Technology	2.2M	0K	0K	500K	3.3M	6.7M	1
Transportation	0K	0K	0K	0K	100K	50K	12
Other	249K	2.3M	39K	99K	53K	1.8M	7

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.

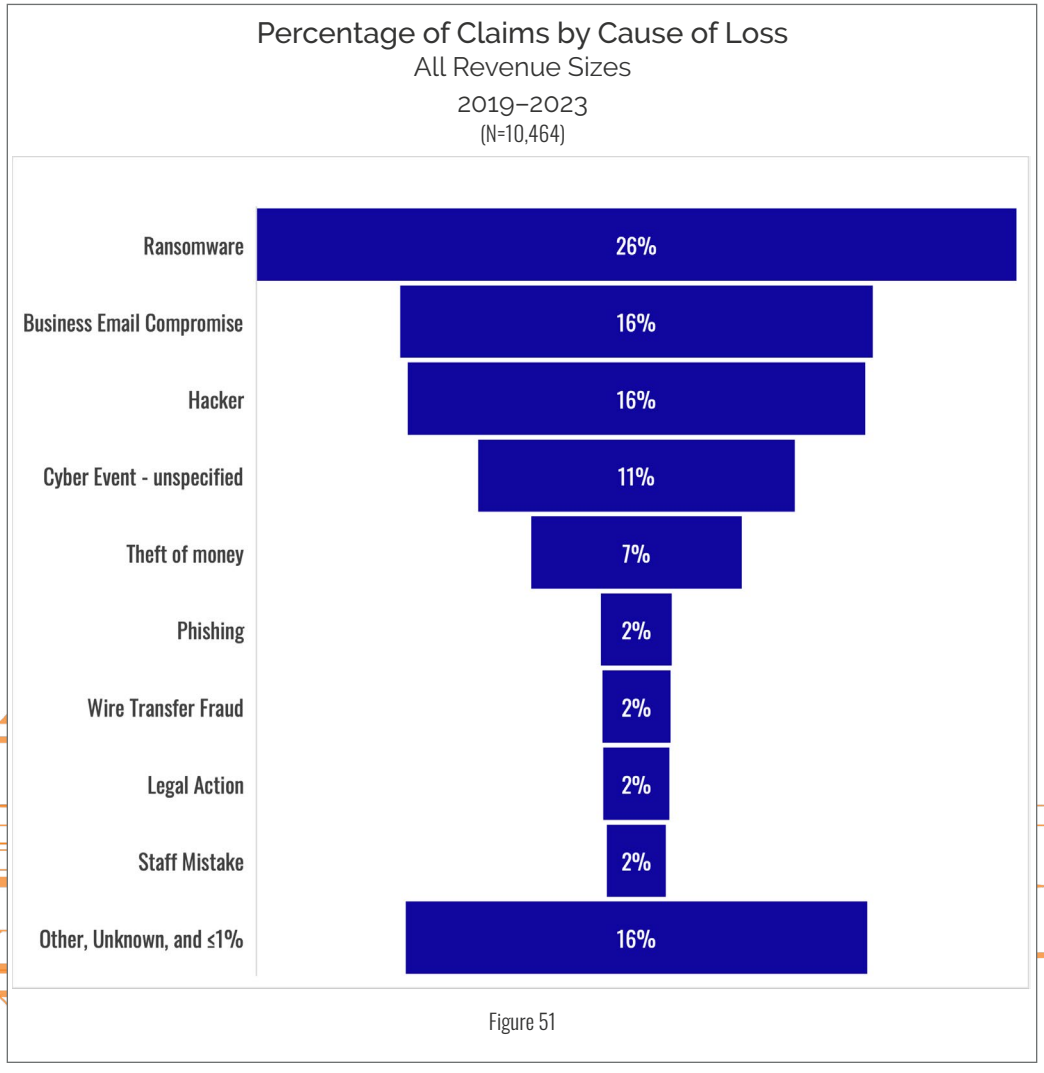


Figure 51

Incident Cost by Cause of Loss—SMEs
2019–2023

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	1,669	1K	101K	30.0M	169.3M	10.0%	2	12
Cyber Event - Unspecified	750	1K	87K	2.4M	65.2M	3.8%	4	13
Hacker	1,091	1K	78K	13.7M	85.5M	5.0%	3	15
Legal Action	60	1K	118K	4.2M	7.1M	0.4%	11	10
Lost/Stolen Laptop/Device	46	1K	37K	356K	1.7M	0.1%	13	19
Malware/Virus	141	2K	87K	1.0M	12.2M	0.7%	9	14
Negligence	1	450K	450K	450K	0.5M	0.0%	24	3
Paper Records	9	2K	24K	100K	216K	0.0%	19	20
Phishing	164	1K	61K	401K	10.0M	0.6%	8	16
Privacy Breach	16	1K	207K	1.9M	3.3M	0.2%	15	5
Programming Error	8	4K	131K	515K	1.0M	0.1%	20	9
Ransomware	2,580	1K	432K	17.6M	1.1B	65.7%	1	4
Rogue Employee	57	1K	50K	403K	2.9M	0.2%	12	17
Social Engineering	4	11K	167K	383K	666K	0.0%	21	8
Staff Mistake	136	1K	19K	463K	2.5M	0.1%	10	23
System Glitch	11	4K	113K	901K	1.2M	0.1%	18	11
Theft of Hardware	12	5K	23K	57K	277K	0.0%	16	21
Theft of Money	549	1K	44K	1.1M	24.1M	1.4%	6	18
Third Party	3	9K	23K	31K	68K	0.0%	23	22
Trademark/Copyright Infringement	4	2K	1.2M	4.1M	4.6M	0.3%	21	1
Unauthorized Access	1	9K	9K	9K	9K	0.0%	24	24
Wire Transfer Fraud	239	2K	177K	3.8M	42.2M	2.5%	7	7
Wrongful Data Collection	18	5K	765K	5.1M	13.8M	0.8%	14	2
Other	697	1K	191K	8.9M	132.8M	7.8%	5	6
Unknown	12	1K	9K	34K	105K	0.0%	16	25

Table 9

Average Crisis Services Costs by Cause of Loss—SMEs
2019–2023

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	31K	25K	7K	22K	81K	76K	4
Cyber Event - Unspecified	19K	2K	0K	4K	0K	24K	12
Hacker	22K	16K	2K	13K	19K	43K	7
Legal Action	2K	1K	1K	5K	130K	13K	16
Lost/Stolen Laptop/Device	15K	1K	0K	10K	71K	21K	13
Malware/Virus	23K	72K	1K	9K	105K	48K	5
Paper Records	0K	1K	0K	7K	0K	9K	17
Phishing	9K	3K	1K	6K	0K	17K	15
Privacy Breach	18K	1K	0K	4K	0K	18K	14
Programming Error	29K	0K	0K	5K	3K	26K	10
Ransomware	79K	53K	16K	31K	143K	209K	1
Rogue Employee	54K	9K	1K	9K	93K	38K	8
Social Engineering	9K	1K	0K	4K	102K	83K	3
Staff Mistake	8K	4K	0K	4K	4K	6K	21
System Glitch	10K	11K	14K	16K	29K	24K	11
Theft of Hardware	6K	1K	0K	6K	0K	8K	20
Theft of Money	2K	0K	0K	1K	53K	4K	22
Third Party	0K	0K	0K	0K	0K	0K	23
Trademark/Copyright Infringement	0K	0K	0K	0K	0K	0K	23
Unauthorized Access	1K	0K	0K	8K	0K	9K	18
Wire Transfer Fraud	15K	0K	0K	15K	94K	46K	6
Wrongful Data Collection	12K	0K	0K	10K	15K	119K	2
Other	17K	6K	3K	15K	38K	34K	9
Unknown	11K	0K	0K	3K	0K	8K	19

Table 10

Incident Cost by Cause of Loss—Large Companies
2019–2023

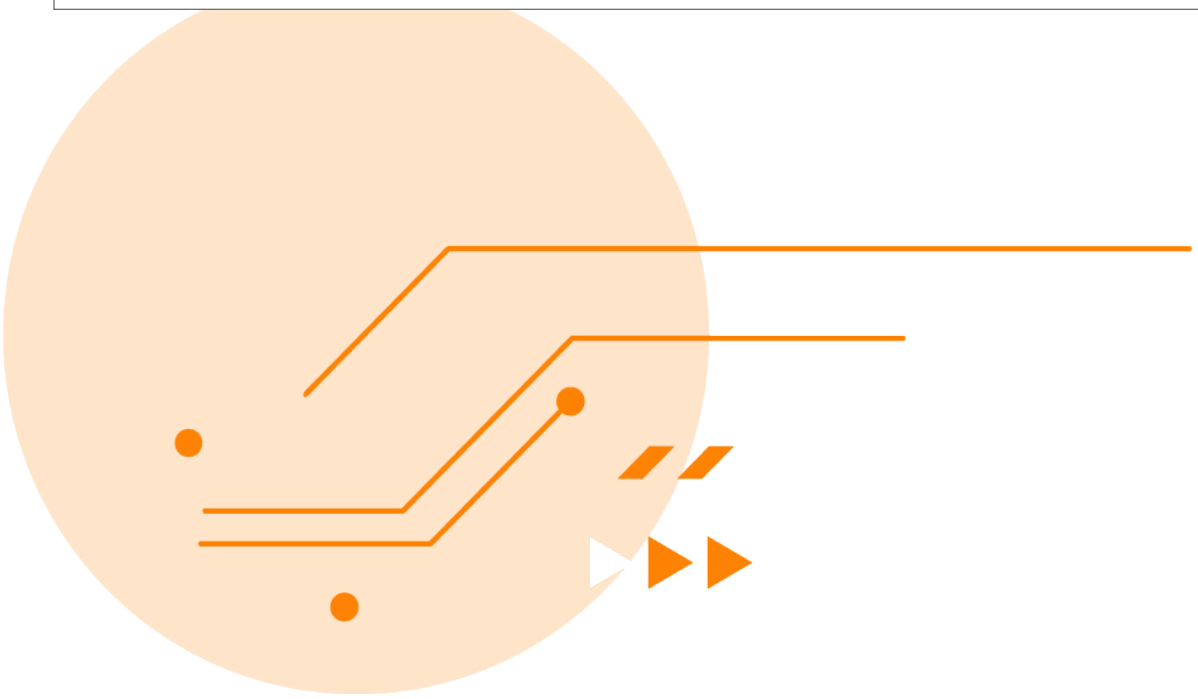
Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	13	18K	356K	1.4M	4.6M	0.2%	5	10
Cyber Event - Unspecified	1	226K	226K	226K	226K	0.0%	11	11
Hacker	15	13K	35.1M	350.0M	526.6M	26.2%	3	1
Lost/Stolen Laptop/Device	1	32K	32K	32K	32K	0.0%	11	13
Malware/Virus	3	480K	2.2M	5.7M	6.7M	0.3%	6	6
Phishing	1	179K	179K	179K	179K	0.0%	11	12
Programming Error	1	2.5M	2.5M	2.5M	2.5M	0.1%	11	5
Ransomware	81	1K	17.3M	503.5M	1.4B	69.7%	1	2
Rogue Employee	3	55K	7.1M	13.2M	21.3M	1.1%	6	3
Staff Mistake	16	2K	5K	17K	75K	0.0%	2	15
Theft of Money	2	275K	735K	1.2M	1.5M	0.1%	9	9
Wire Transfer Fraud	2	125K	838K	1.6M	1.7M	0.1%	9	8
Wrongful Data Collection	3	10K	4.0M	11.0M	12.0M	0.6%	6	4
Other	15	3K	2.1M	12.6M	31.0M	1.5%	3	7
Unknown	1	32K	32K	32K	32K	0.0%	11	14

Table 11

Average Crisis Services Costs by Cause of Loss—Large Companies
2019–2023

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	86K	9K	39K	77K	645K	358K	8
Hacker	2.7M	4.6M	0K	115K	313K	2.2M	4
Lost/Stolen Laptop/Device	19K	0K	0K	13K	0K	32K	10
Malware/Virus	448K	4.5M	0K	288K	83K	3.0M	3
Programming Error	1.1M	647K	0K	84K	2K	1.8M	5
Ransomware	1.7M	632K	79K	884K	1.1M	3.2M	2
Rogue Employee	9K	13K	0K	33K	0K	5.0M	1
Staff Mistake	0K	0K	0K	5K	0K	5K	12
Theft of Money	81K	207K	0K	0K	159K	368K	7
Wire Transfer Fraud	0K	0K	0K	0K	75K	75K	9
Other	0K	2.4M	0K	77K	56K	881K	6
Unknown	0K	0K	0K	0K	7K	7K	11

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.

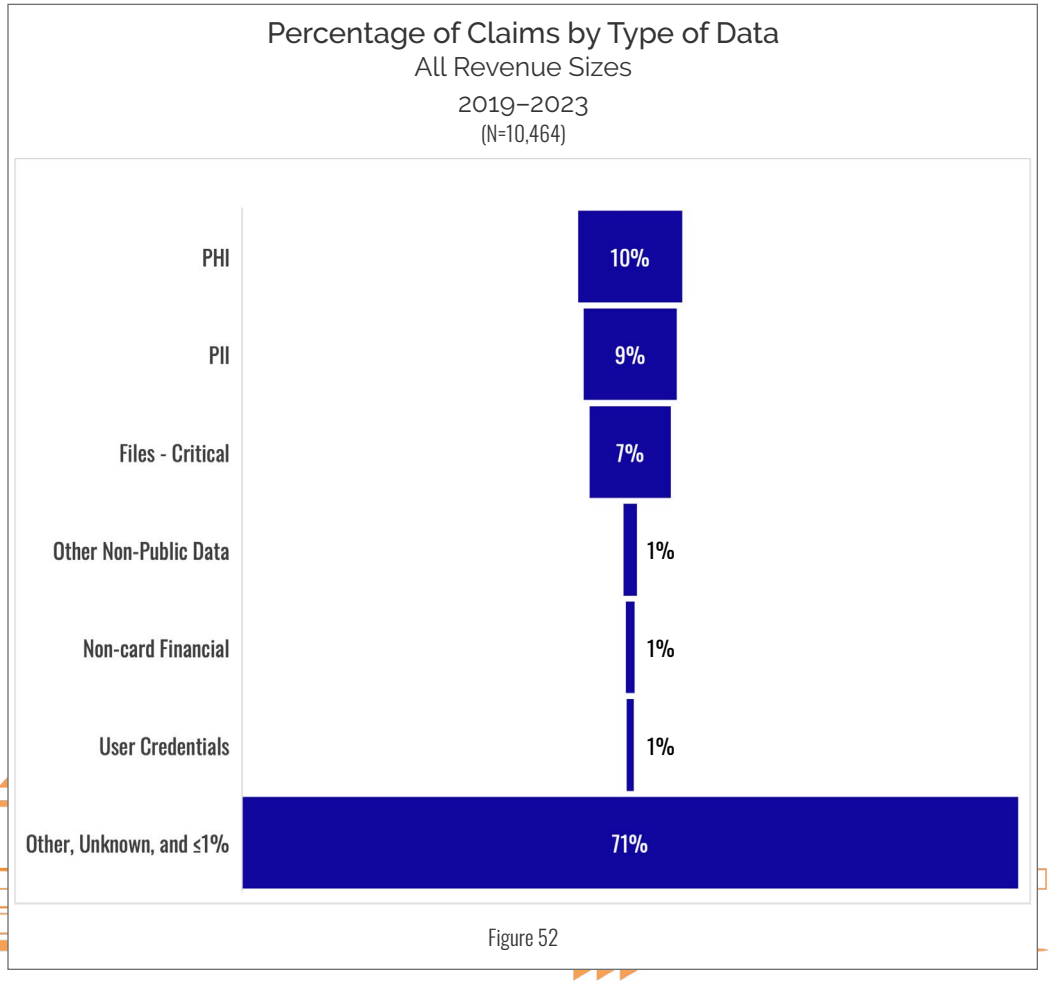


Figure 52

Incident Cost by Type of Data—SMEs
2019–2023

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Email - Unspecified	20	3K	73K	229K	1.5M	0.1%	10	14
Files - Critical	740	1K	251K	7.2M	185.7M	10.9%	3	11
Intellectual Property	6	8K	3.2M	13.6M	19.0M	1.1%	12	2
Non-Card Financial	78	2K	386K	4.7M	30.1M	1.8%	7	7
Other Non-Public Data	108	1K	803K	15.0M	86.7M	5.1%	6	5
PCI	18	1K	290K	2.3M	5.2M	0.3%	11	9
PHI	502	1K	335K	17.6M	168.1M	9.9%	4	8
PII	741	1K	508K	15.0M	376.1M	22.2%	2	6
Trade Secrets	6	250K	1.0M	2.1M	6.1M	0.4%	12	4
User Credentials	49	1K	270K	3.9M	13.2M	0.8%	8	10
Video Viewing Data	2	4.2M	4.6M	5.1M	9.3M	0.5%	14	1
Other	49	6K	1.6M	30.0M	76.4M	4.5%	8	3
N/A	260	1K	164K	5.2M	42.6M	2.5%	5	12
Unknown	5,699	1K	119K	8.9M	676.7M	39.9%	1	13

Table 13

Average Crisis Services Costs by Type of Data—SMEs
2019–2023

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Email - Unspecified	22K	2K	0K	17K	157K	52K	12
Files - Critical	60K	38K	6K	17K	66K	108K	9
Intellectual Property	316K	0K	0K	11K	521K	1,991K	1
Non-Card Financial	117K	38K	0.3M	64K	90K	190K	7
Other Non-Public Data	157K	16K	2K	62K	54K	257K	4
PCI	155K	21K	20K	121K	34K	209K	6
PHI	65K	75K	13K	27K	87K	172K	8
PII	118K	88K	17K	43K	84K	213K	5
Trade Secrets	89K	6K	1K	110K	50K	263K	3
User Credentials	70K	18K	10K	22K	41K	79K	10
Other	207K	1.2M	554K	501K	1.5M	1.3M	2
N/A	19K	1K	0K	10K	61K	46K	13
Unknown	0K	0K	0K	0K	0K	63K	11

Table 14

Incident Cost by Type of Data—Large Companies
2019–2023

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Files - Critical	6	480K	16.2M	55.0M	97.0M	4.8%	6	5
Intellectual Property	2	24K	640K	1.3M	1.3M	0.1%	8	11
Non-Card Financial	2	1.3M	175.6M	350.0M	351.3M	17.5%	8	1
Other Non-Public Data	8	0.0M	2.4M	13.2M	19.1M	0.9%	4	9
PCI	2	25.0M	25.5M	26.0M	51.0M	2.5%	8	2
PHI	20	22K	10.8M	60.0M	215.7M	10.7%	3	6
PII	60	2K	16.6M	503.5M	993.6M	49.5%	1	4
User Credentials	6	13K	22.8M	111.0M	136.9M	6.8%	6	3
Other	1	8.1M	8.1M	8.1M	8.1M	0.4%	11	7
N/A	8	25K	1.1M	5.0M	9.0M	0.4%	4	10
Unknown	43	3K	2.9M	33.5M	124.7M	6.2%	2	8

Table 15

Average Crisis Services Costs by Cause of Loss—Large Companies
2019–2023

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Files - Critical	357K	0K	0K	55K	13K	1.7M	5
Intellectual Property	1.1M	0K	14K	103K	0K	1.2M	7
Other Non-Public Data	228K	0K	0K	23K	26K	1.6M	6
PCI	15.0M	0K	0K	11K	0K	7.5M	1
PHI	59K	2.5M	0.1M	101K	607K	2.2M	2
PII	1.5M	956K	90K	569K	840K	2.1M	4
User Credentials	128K	0K	0K	99K	0K	195K	8
N/A	92K	415K	0K	4K	80K	170K	9
Unknown	1.5M	28K	10K	476K	1.4M	2.1M	3

Table 16

Underwriting Third Party Risk

Essential Cybersecurity Due Diligence

Sean B. Hoar, Chair & Partner, Cybersecurity & Data Privacy Team, Constangy, Brooks, Smith & Prophete LLP

Managing third-party risk has become an urgent priority for information security programs—and proof of risk management programs for prospective insureds is a critical part of successful underwriting programs. As our reliance on the digital environment has become almost absolute, the use of third-party providers has become proportionally essential. Businesses are increasingly forced to rely on third-party developers, manufacturers, multi-layered supply chains and service providers to manage and provide basic or business critical functions, from internet operation to email platforms, document management systems, payroll and payment processors, applications, data storage systems, and hardware to host and transmit data. This means relying on third-party operating systems, networks and hardware to be operational—and to be secure. What could go wrong?

One of the challenges in information security is the rapid growth of new technology, often exceeding human and technical means of assuring quality and security. Over 25 years ago, when I began managing investigations regarding online identity theft, payment card compromises, and intellectual property theft, information security was a nascent profession. To provide perspective: the Computer Security Act was passed by Congress in 1988. It directed the National Bureau of Standards (now the National Institute of Standards and Technology or "NIST") to work with the National Security Agency to develop standards of minimum acceptable practices. The following year, in 1989, the SANS Institute—which has become one of the world's largest cybersecurity research and training organizations—was founded. One year later, in 1990, the International Association of Computer Investigative Specialists ("IACIS")—which has become a premier international digital forensics training organization—was founded. Several years later, when I began managing investigations of "carding" cases—which later became known as data breaches—there was relatively little available forensics support. There were also relatively few information security professionals. In fact, the first widely known chief information security officer ("CISO") wasn't hired until 1994 after Citicorp (formerly Citigroup) experienced repeated intrusions from Russian hackers. Since that time, spurred by many impactful data security incidents, the information security market has experienced extraordinary growth.

This extraordinary growth highlights a major issue affecting the state of our digital environment: the chasm between information technology and information security. With the market size of information security reported to be approximately $200 billion in 2024, there are myriad economic opportunities for third-party providers to enter or remain in the market. Unfortunately, if their qualifications and/or services are deficient, it often isn't known until a data security incident occurs due to their failure to implement certain information security controls. Even reputable providers are challenged with a lack of visibility into the security of their supply chain. The following incidents recently affected thousands of organizations and millions of consumers—and highlight the depth of the problem:

- SolarWinds (compromise of network management software)
- GoAnywhere (compromise of secure managed file transfer product)
- MOVEit Transfer (compromise of secure file transfer product)
- Change Healthcare (compromise of healthcare payment processing platform)
- CDK Global (compromise of car dealership software management platform)

There is an obvious and urgent need to significantly increase due diligence about third-party risks during the underwriting process. Requiring proof of vendor management programs can substantially mitigate these risks. These programs should require vendors to provide evidence of the following:

- Risk management programs
- Information security policies and procedures (e.g., written information security policies; identity and access management policies; vulnerability and patch management processes)
- Recent security risk assessments

- Incident response, business interruption and emergency operations plans (and proof of testing)
- Attestations of critical security control deployment

These programs should also include vendor contracting protocols. In general, vendor contracts should contain the following:

- Representations and warranties of compliance with applicable data privacy laws
- Requirements to maintain administrative, physical and technical safeguards to protect data in transit and at rest (with specific requirements outlined)
- Required flow-downs under applicable laws (e.g., HIPAA, CCPA, DFARS, etc.)
- Restrictions regarding subcontracting services and location of services
- Rights to audit to confirm compliance with contractual requirements and applicable laws
- Appropriately high limitations of liability (or no limitation of liability) for high-risk claims arising from confidentiality breaches, intellectual property infringement, data security incidents and indemnification
- Indemnification triggers for negligence, willful misconduct, violations of law, data incidents and confidentiality breaches
- For mission critical services requiring proper uptime, service level agreements guaranteeing availability of services and service credits

Requiring prospective insureds to provide proof of their vendor management programs is not a panacea to potential liabilities, but it can substantially mitigate third-party risk and result in a much better underwriting product.

About Constangy, Brooks, Smith & Prophete LLP

For over 75 years, Constangy has provided workplace advice to employers. In 2023 it began providing data privacy and security services. Throughout its history Constangy has also been a diverse firm. It embraces the ABA "Resolution 113" goals to advance diversity, equity, and inclusion in the legal profession and has been recognized as one of the top law firms for diversity in each of the past seven years.

Understanding the Evolving Landscape of Cyber Threats

A Call to Action for Industry Leaders

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

As we navigate the dynamic and often alarming realm of cyber threats, it's crucial for organizations to remain grounded and strategic. Despite the ongoing evolution of cybercriminal tactics, our goal is to engage without sounding alarmist. Recent high-profile and far-reaching breaches involving National Public Data, AT&T, Ticketmaster, and Change Healthcare reveal the pressing need for vigilance.

The integration of machine learning and artificial intelligence (AI) by cybercriminals has escalated the threat landscape. These advancements enable the creation of sophisticated synthetic identities and innovative attack strategies, rendering traditional defenses increasingly ineffective. Additionally, new players and alliances are adding complexity to the cyber threat environment.

Emerging threat actors and alliances

While nation-states like China, Iran, North Korea, and Russia have long been known for sponsoring cyber activities, India's role in state-sponsored cyberattacks is rising. India's large pool of skilled IT professionals has contributed to a notable increase in cyber activities targeting adversarial countries like Pakistan and China. Recent insights suggest that threats to China are now more likely to emerge from South Asia than elsewhere.

Groups like the "Indian Cyber Force" have gained attention for their operations against foreign entities, including Canadian military and parliamentary websites. This uptick necessitates closer monitoring of irregular activities from Indian IP addresses alongside traditional bad actor nations.

Another notable player is "Scattered Spider," composed of English-speaking hackers from the US, Canada, and the UK. Their expertise in social engineering has enabled them to breach major tech firms such as Microsoft and Nvidia. Their collaboration with Russian ransomware gangs, evidenced by the September 2023 ransomware attack on MGM Resorts, highlights a troubling trend of international cyber cooperation that has led to significant financial damages.

A report from SecurityScorecard revealed that 44% of cyber incidents in 2023 were attributed to just ten threat actors. This mirrors historical patterns of alliance formation among adversaries, suggesting that today's cybercriminal networks are becoming increasingly sophisticated and coordinated.

New tactics and strategies

Recent trends show a shift towards more strategic, targeted cyberattacks. With the rise of software as a service (SaaS) and cloud platforms, attackers are now focusing on systems indirectly connected to primary targets. The ransomware attack on Change Healthcare this year, which affected millions of clients and patients, underscores the need for stringent cybersecurity measures among outsourced service providers. Vulnerabilities in the supply chain can lead directly to significant breaches.

Cybercriminals are also employing more subtle methods. Incremental data manipulation—rather than broad data theft—allows them to cause significant damage while remaining undetected. By targeting small but critical variables such as stock prices or logistics coordinates, these actors blend their malicious activities with normal operational issues, complicating detection efforts.

Moreover, the infiltration of publicly traded companies to gather insider information for market manipulation is another growing concern. In some cases, cybercriminals exploit valuable insights without breaching cybersecurity defenses, simply by posing as investors.

The role of AI in enhancing cyber threats is becoming increasingly pronounced. Cybercriminals use generative AI tools to accelerate the development of malicious code, making attacks more sophisticated and harder

to counter. The FBI has highlighted that these AI advancements are not just augmenting existing threats but are fundamentally reshaping the cybercrime landscape.

Looking forward

The cyber threat landscape of H1 2024, marked by major breaches and extensive data compromises, serves as a stark reminder of the severity of current threats. As we move through the remainder of the year, the growing sophistication and collaboration among cybercriminals suggest that the risk is escalating.

It is essential for organizations to develop robust response plans aligned with contemporary threat patterns. Effective plans not only facilitate recovery but also help in proactively addressing potential breaches. Research indicates that organizations with comprehensive cyber resilience strategies experience incidents 15% less frequently. Therefore, staying attuned to subtle security indicators and adapting to the evolving threat landscape is critical in our collective effort to mitigate cyber risks.

About Experian

Increasing Your Resiliency to Cybersecurity Incidents

Three areas of focus to minimize the impact of a potential incident

Alden Hutchison, Principal, Security & Privacy Risk, RSM US LLP

As threats continue to evolve, addressing cybersecurity challenges remains at the top of the list of priorities for middle market companies in all industries. Incidents are on the rise, as demonstrated by the record-tying number of executives reporting data breaches in the RSM US Middle Market Business Index Special Report: Cybersecurity 2024. Because of the significant costs related to addressing and remediating a data breach, companies need to proactively address potential risks within their business.

No company is immune to data breaches, but you can limit your risk exposure and the downtime and costs related to a potential attack. Below are three critical areas of focus that will strengthen your resiliency:

Assess backups: To prepare for ransomware attacks, companies need to pay close attention to their backup and recovery programs. Many companies have invested in technology but have failed to implement a program around the technology to ensure their backups are good and the restoration process is swift. Because of this, companies have often tried to restore their operations from backups following a ransomware attack and have failed because they weren't regularly practicing their recovery processes. In many cases, companies do not even have their vital systems like ERP and CRM effectively backed up, much less desktops and file servers.

Organizations can easily develop a false sense of security, thinking the backups they've deployed are effective. But when they need to deploy them in an emergency, their backups are non-functional.

Creating immutable backups is an important element of an effective cybersecurity approach, with separate files that cannot be altered or deleted. If companies allow the same admin for their production environment and backups, threat actors will simply encrypt both, significantly hampering recovery efforts.

Be aware of the human element: In business email compromise attacks, the human element is almost always the critical issue. Users can be tricked into clicking a fraudulent link in an email or authorizing an action that that they shouldn't. Threat actors are rapidly becoming more sophisticated and taking advantage of artificial intelligence to create more realistic emails and webpages that look like legitimate company pages. Criminals are even having success using advanced technology to create voice conversations and videos that seek to gain access to a network through social engineering attacks.

Companies often have a very rudimentary approach to email security, with controls that have not evolved in years and do not match current threats. With attacks on the rise, organizations need to implement more robust controls and continue educating users on current threats.

Understand systemic risks: All companies are becoming more digital; even very traditional companies and industries now operate a complex digital platform. With that structure, companies typically have a large ecosystem of service providers, vendors, cloud services and emerging technology capabilities that bring inherent risks. Additionally, data security and privacy regulations continue to change the requirements that companies need to meet. Companies must have a robust risk management program governed and managed from the board level down through the front-line employees. This ensures organizations understand their risk exposure and develop plans to minimize those known vulnerabilities.

Incidents frequently occur within critical service providers and create outages for thousands of customers. To limit those risks, companies must understand their vendors' control environment and the specific ways that they rely on each vendor to operate their business. Then, they must develop resiliency

plans to failover to another method of doing business if key functions are disrupted.

Conclusion:

In the current threat environment, all companies—regardless of size or industry—will encounter a breach attempt or a business impact from their digital ecosystem. Effectively addressing potential weaknesses is a critical element of mitigating risks and quickly recovering when these incidents occur.

About RSM US LLP

RSM's purpose is to deliver the power of being understood to our clients, colleagues, and communities through world-class audit, tax, and consulting services focused on middle market businesses. 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 environment. RSM US LLP is the U.S. member of RSM International, a global network of independent audit, tax and consulting firms with 57,000 people across 120 countries. For more information, visit rsmus.com, like us on Facebook, follow us on Twitter and/or connect with us on LinkedIn.

AI: The Double-Edged Sword in Cyber Insurance

Ben Duffy, Head of North America, KYND

Artificial Intelligence (AI) has rapidly transformed the landscape of cyber insurance, becoming a powerful tool in the hands of both defenders and attackers. As AI becomes increasingly embedded in the cyber risk landscape, insurers and underwriters face the dual challenge of assessing AI-driven threats while leveraging AI's potential to enhance their risk models and underwriting practices. Understanding how cybercriminals use AI to seamlessly penetrate business defenses is the first step for insurers to take to preempt these AI-driven threats and adapt their strategies to mitigate advanced risks.

The Rise of AI-Driven Cyberattacks and Its Impact on Insurance

AI's integration into cybercrime has given rise to a new breed of threats, where attackers deploy advanced algorithms to bypass traditional security measures. Cybercriminals are now harnessing AI to automate tasks, such as scanning for vulnerabilities, crafting personalized phishing attacks, and evading detection by adaptive malware. These capabilities, once the exclusive domain of security experts, are now being weaponized by adversaries to conduct more efficient and targeted attacks.

For insurers and underwriters, this evolution presents a significant challenge. The increasing sophistication of AI-driven cyberattacks complicates risk assessment and makes it more difficult to accurately price policies. Traditional risk models, which rely on historical data and static threat landscapes, may no longer suffice in an environment where threats are constantly evolving through AI-driven mechanisms.

One of the most concerning developments is the use of AI to create polymorphic malware. Unlike traditional malware, which remains static, polymorphic malware continuously changes its code to avoid detection by signature-based security tools. This presents a unique challenge for underwriters who must account for the heightened risk posed by such advanced threats. Policies need to be designed with an understanding that AI-enabled attacks can evade even the most sophisticated defenses, potentially leading to higher claims and increased financial exposure for insurers.

AI-Powered Social Engineering: A Growing Threat for Insureds

Another area where AI has significantly bolstered cybercriminal capabilities is in the realm of social engineering, with deepfake technology at the forefront. Deepfakes, powered by AI, allow attackers to create highly convincing audio and video content that can be used to impersonate executives, employees, or business partners. This has led to a surge in AI-driven business email compromise (BEC) attacks, where attackers use deepfakes to trick employees into transferring funds or divulging sensitive information.

For insurers, these AI-powered social engineering attacks represent a growing area of concern. The rise of such sophisticated techniques demands a reevaluation of existing coverage terms, exclusions, and limits related to social engineering fraud. Moreover, underwriters must consider how AI-driven threats impact the overall risk profile of insureds and adjust their underwriting criteria accordingly.

Leveraging AI in Risk Assessment and Underwriting

While AI's role in enabling cyberattacks is concerning, it also offers insurers and underwriters powerful tools for defense. AI-driven risk assessment models can analyze vast amounts of data to identify potential vulnerabilities and predict future risks more accurately. By integrating AI into underwriting processes, insurers can improve the precision of their risk evaluations, leading to more tailored policies and better pricing strategies.

However, the dual-use nature of AI requires a nuanced approach. Insurers must strike a balance between leveraging AI to enhance their operations and recognizing that the same technology can be used by adversaries to outmaneuver traditional defenses. This complexity underscores the need for continuous adaptation and innovation in insurance practices.

Adapting Insurance Strategies to Preempt AI-Driven Threats

To effectively combat AI-enhanced cyber threats, insurers and underwriters must adopt a proactive approach:

- Develop Adaptive Underwriting Practices: AI-driven threats are constantly evolving. Therefore, underwriting practices should be adaptive and capable of incorporating the latest threat intelligence and modeling technologies. This may involve regular updates to underwriting guidelines and the inclusion of AI-driven risk factors in policy terms.
- Promote Cyber Hygiene and Resilience among Insureds: Provide insureds with AI-powered cyber risk management solutions and best practices, like KYNDs ON and Ready programs. Striving to improve cyber hygiene and resilience, insurers can reduce the likelihood of claims and improve the overall risk profile of their portfolios.
- Collaborate with Insureds on AI Awareness: Educate insureds about the latest AI-driven social engineering tactics, including deepfakes and personalized phishing. Offering workshops or resources on recognizing these threats can help insureds mitigate their exposure and reduce the potential for costly claims.

Conclusion

The integration of AI into both cyber risk management and cybercrime has created a double-edged sword that insurers and underwriters must navigate with care. While AI offers powerful tools for enhancing risk assessment and underwriting, it also empowers adversaries to launch more complex and adaptive attacks. By understanding the dual-use nature of AI and adopting proactive approaches to cyber risk management, insurance professionals can preempt AI-driven threats and adapt their strategies to mitigate these advanced risks. The future of cyber insurance will be defined by the ability to harness AI's potential for good while staying one step ahead of those who seek to use it for harm.

About KYND

KYND is a cyber risk solutions provider dedicated to demystifying complex cyber risks, making them more manageable for insurers and their clients. Our next-generation solutions empower insurance partners to comprehensively assess, understand, and enhance their risk resilience with unprecedented ease.

Powered by its proprietary data on organizations' cyber footprint, KYND cuts through the noise and delivers superior insights into the risks that matter—those that lead to actual incidents and claims—enabling streamlined and profitable cyber underwriting as well as effective, ongoing portfolio monitoring and alerting, and proactive event response to stay ahead of emerging threats.

By combining best-in-class aggregation risk insights with bespoke, granular cyber disaster scenarios, KYND empowers insurers to more accurately evaluate and manage the accumulation and CAT exposure across their portfolios, including exposure to war and state-sponsored scenarios incorporating various war clauses, among many others.

About NetDiligence

NetDiligence® is a leading provider of Cyber Risk Readiness & Response services. We have been providing cyber risk management services and software solutions to the cyber insurance industry, both insurers and policyholders, since 2001.

Our Cyber Risk Summit conferences and our cyber advisory groups function as information exchange platforms for insurers, legal counsel, and technology specialists. This community of experts serves as the vanguard in the fight against cyber losses. We listen and learn from them. That's why our services support our insurance partners and their policyholders both proactively for cyber readiness and reactively for incident response.

Breach Response Solution with Mobile App

Breach Plan Connect® is a securely hosted solution designed to help senior managers plan for, oversee, and coordinate their organization's response to a cyber incident. Breach Plan Connect comes pre-loaded with a comprehensive incident response plan template that can be easily customized, along with detailed response playbooks for common incidents like ransomware and business email compromise. It also includes a free mobile app for convenient access and alternative means of communication if company systems are compromised.

Risk Management Portal for Insurers

To support our partners in the cyber insurance industry and beyond, NetDiligence® provides a comprehensive bespoke online platform called the eRiskHub®. This SaaS offering is the key to educating and empowering the entire cyber ecosystem from cyber insurance underwriters, claims support, and brokers to cyber policyholders and their internal staff.

Cyber Risk Assessments

NetDiligence's QuietAudit® cyber risk assessments give organizations a 360-degree view of their people, processes and technology, so they can reaffirm that reasonable practices are in place; harden and improve their data security; qualify for network liability and privacy insurance; and bolster their defense posture in the event of class action lawsuits. We offer network vulnerability scans and consultant-led assessments that are tailored to meet the unique needs of small, medium, and large organizations in all business sectors. A variety of automated online self-assessment surveys are also available for underwriting loss control and vendor risk management.

On-Site & Virtual Cyber Programs

The leading networking events for the cyber industry, NetDiligence conferences are attended by thousands of cyber insurance, legal/regulatory, and security/privacy technology leaders from all over the world. Each event features programming curated by cyber professionals and focused on current and emerging concerns in the ever-changing cyber landscape. We traditionally host four on-site conferences per year. In 2025, you will find us in Miami Beach, Toronto, San Diego and Philadelphia.

Contact Us

For more information, visit us at netdiligence.com, or email 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
- Grete Feldman, Communications Assistant

For more information, visit us at netdiligence.com, 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 2021, 2022 or 2023.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to over 200 individuals at 90 organizations in the United States, Canada, and the United Kingdom. From this group, 22 individuals representing 21 organizations provided 4,991 analyzable new and updated claims.

The 2024 report also includes data from NetDiligence studies published in 2019-2023, representing 5,473 incidents that occurred in 2019, 2020, 2021 and 2022, making a total of 10,464 claims that could be analyzed.

All of these were included in the demographic analyses. 8,436 claims with a total incident cost ≥$1,000 were included in the financial analyses. As we have noted elsewhere, two extreme outlier SME claims in excess of $100M each were excluded from most analyses.

There are 10,141 claims in the dataset from American organizations, 193 claims from Canadian organizations, and 15 claims from organizations in the United Kingdom. There are also a small number of claims from organizations in Australia, EU Countries, South Africa, other countries, and organizations with a global footprint. The country was not specified in 57 claims.

When factoring in SIRs, we were able to calculate total incident cost to date for all 8,436 (100%) of the claims with total incident cost >$1,000. 4,759 claims (45%) included an accounting of crisis services costs. 474 claims (5%) 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.) .

9,307 (89%) claims in the dataset were flagged as closed and 1,141 (11%) as open. The claim status was unknown for 16 claims. 5,535 (53%) claims were for primary coverage, 105 (<1%) for excess coverage, and 4,824 (46%) had an unknown, but most likely primary, coverage level.

There were 3,064 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 $10 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.