

NetDiligence®

CYBER CLAIMS STUDY

2023 REPORT



SPONSORED BY



Contents

Introduction	1
Key Findings	2
An Overview of the Data.....	7
Claims by Year of Event.....	8
Incident Costs and Payouts	8
Incident and Crisis Services Costs.....	10
Business Interruption (BI) and Recovery Expense	17
Recovery Expense.....	19
Legal Costs	20
Records Exposed	21
Recordless Claims and Claims with Exposed Records.....	23
Criminal and Non-Criminal Activities.....	24
Self-Insured Retentions (SIR)	27
Causes of Loss.....	29
Ransomware	30
Business Email Compromise (BEC)	33
Hackers	34
Staff Mistakes	35
Rogue Employees	36
Third-Party Incidents	37
Sectors.....	38
Professional Services	39
Healthcare	40

Manufacturing.....	41
Financial Services.....	42
Retail.....	43
Public Entities.....	44
Claims from Canada	45
Conclusion	46
Insurance Industry Participants.....	46
Appendices	47
Revenue Size	47
Business Sector	49
Cause of Loss	54
Type of Data	59
Insights from Our Sponsors.....	63
Generative Artificial Intelligence	63
Cracking the Code: Navigating Cyber Trends.....	65
Cybersecurity Environment Remains Challenging as Business World Evolves.....	67
Nailing it.....	69
About NetDiligence®.....	71
About the Study.....	72
Contributors.....	72
Methodology.....	72

Introduction

Welcome to the thirteenth annual NetDiligence® Cyber Claims Study. This report is based on the summary statistical analysis of over 9,000 cyber claims for incidents that occurred during the five-year period 2018–2022. By comparison, the third Cyber Claims Study, published in 2013, analyzed fewer than 150 cyber insurance claims.

By the Numbers

- 9,028 claims analyzed, arising from incidents that occurred during 2018-2022
- 4,945 new and updated claims collected in 2023, from incidents occurring from 2020–2022
- 801 claims analyzed, arising from incidents occurring in 2022.
- 98% of claims (\$1.6B in total) from small to medium enterprises (SMEs) with less than \$2 billion in annual revenue
- 2% of claims (\$1.9B in total) from large companies with more than \$2 billion in annual revenue
- 2,675 claims due to ransomware, 62% of which occurred between 2020 and 2022
- 1,054 ransomware claims which provide both the ransom demand and the total incident cost
- 1,480 claims due to business email compromise, 71% of which occurred between 2020 and 2022

Preliminary Observations

- There are enormous variances in the magnitude of the loss data. The smallest claims were less than \$1,000 and the largest were over \$400M. The numbers of records exposed range from 1 to over 300M.
- There were dramatic differences between the numbers for SMEs and large companies – multiples of 10x, 50x, or more. The biggest large company in the dataset (over \$170B in annual revenue) was approximately 15 million times larger than the smallest organization (less than \$11K in annual revenue). The average large company (\$13.3B in annual revenue) was more than 140 times larger than the average SME (\$94M).
- Even though large companies represented only 2% of claims (N=174), these claims accounted for 54% of the total incident cost analyzed in the report (\$1.9B/\$3.5B).

- As has been the case every year that we have done the analysis, there was no clear correlation between the size of an organization and the magnitude of a cyber-related loss. On average, large companies experienced incidents that were up to 80 times more costly than those at SMEs. However, SMEs experienced large losses as well, with perhaps greater organizational impact – there were 254 SME claims with total incident costs >=\$1M, including 2 SME claims >\$100M.¹
- Except in the very largest incidents, there was no correlation to be found between the number of records exposed and the total cost of an incident.
- Ransomware and BEC were the two leading causes of loss. They accounted for 46% of claims during the five-year period 2018-2022, and nearly 56% in 2022.

With Appreciation

We want to sincerely thank the cyber insurers listed on page 46 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 13 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.

¹Because they are such large outliers, these two claims have been excluded from most analyses. They will be described in more detail later in this report.

Key Findings

Company Size

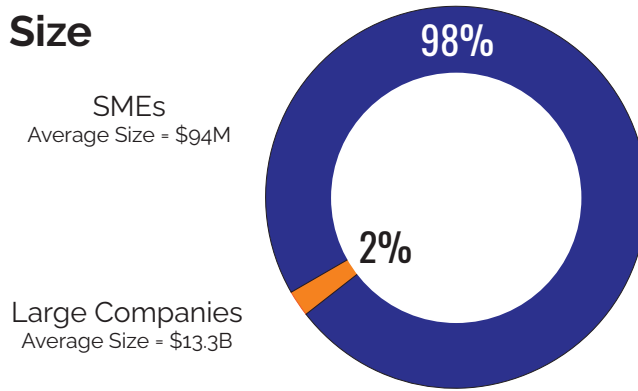


Figure 1

Average Costs for All Claims

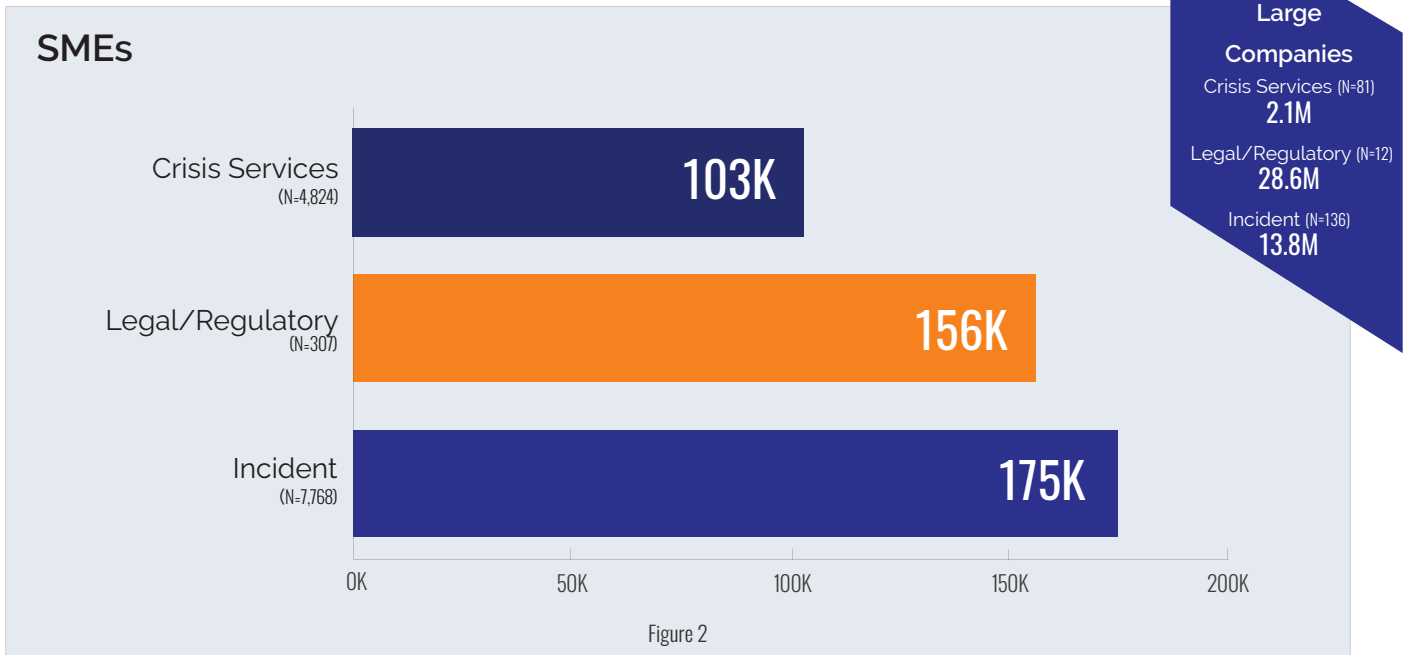


Figure 2

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 Breach Costs.

Small to Medium Enterprise (SME)

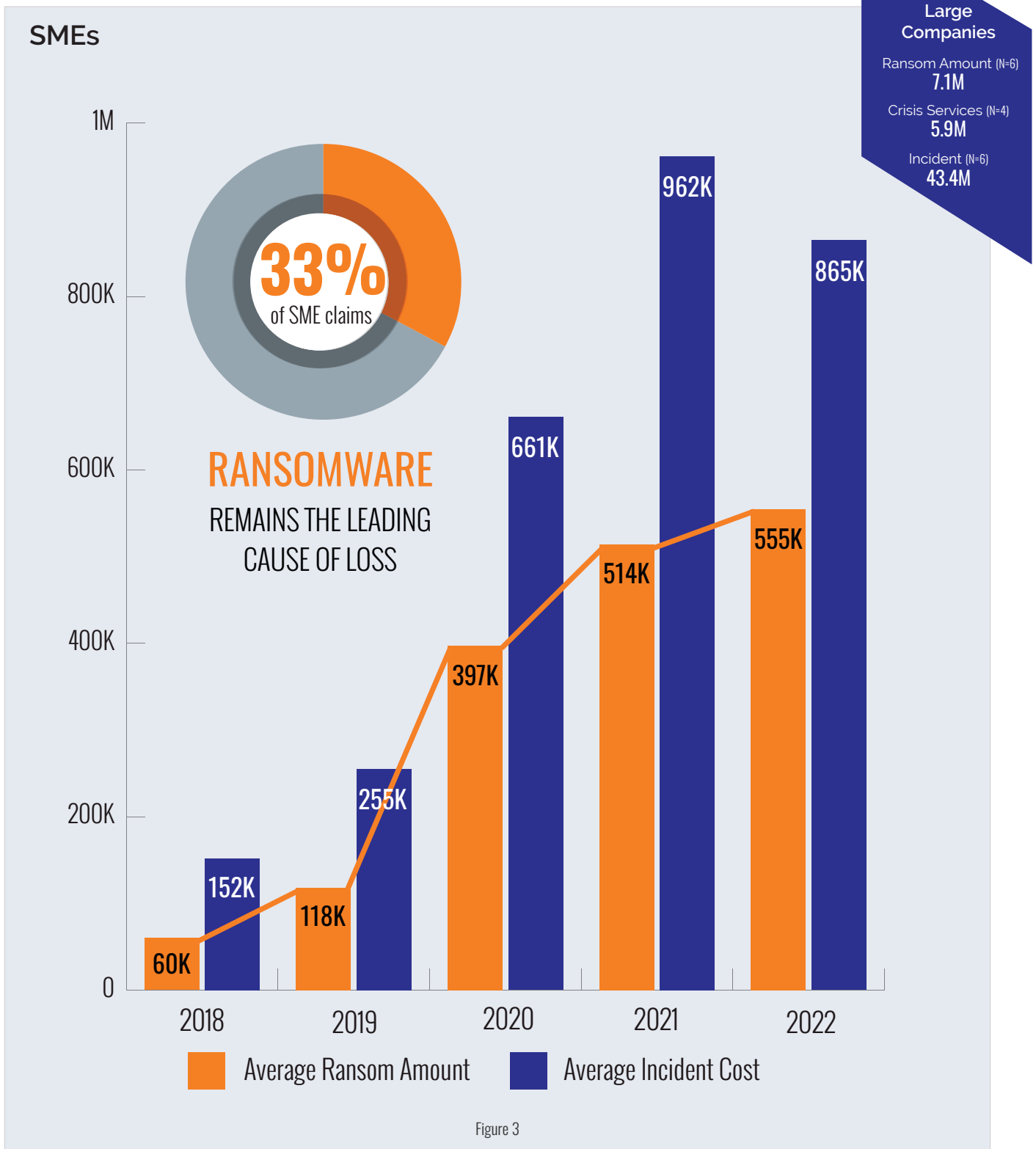
Categorized in this study as organizations with less than \$2 billion in annual revenue.

Large Company

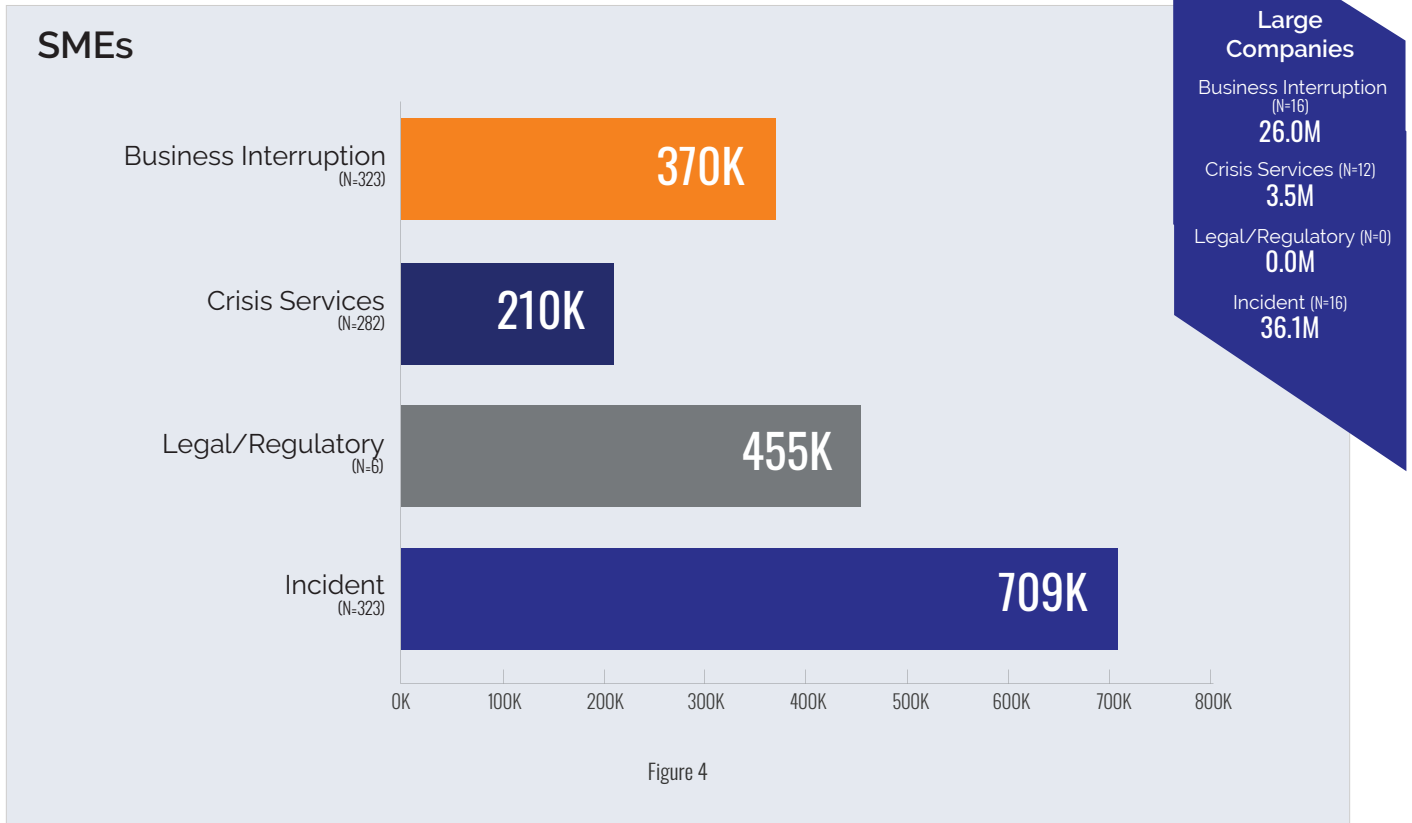
Categorized in this study as organizations with \$2 billion or more in annual revenue.

All findings are for the five-year period 2018–2022 unless otherwise noted.
NetDiligence and Breach Coach are registered trademarks of Network Standard Corporation, dba NetDiligence.

Average Costs for Ransomware



Average Costs for Business Interruption



For four consecutive years, ransomware has remained SMEs' top financial threat. We saw the two most significant SME claims occurring in 2022, affecting the manufacturing and healthcare sectors. These are concerning because they share some noteworthy similarities:

- Both claims exceeded \$100 million.
- Both claims involved ransomware as the primary threat.
- Neither company was exceptionally large (both under \$700M in annual revenue).

Additionally, the following stats show the clear financial pressure that SMEs face when dealing with a cyber incident:

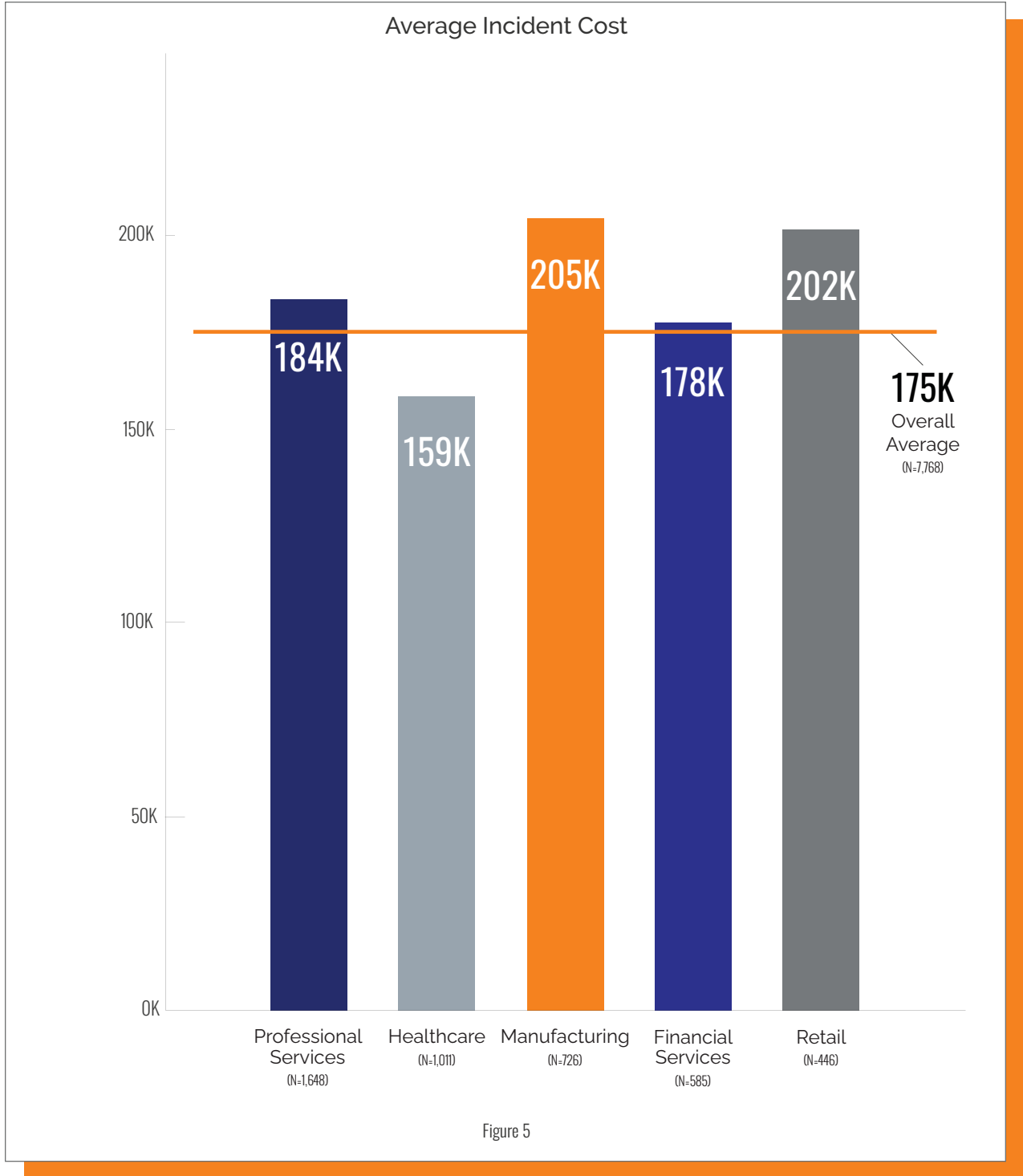
- 254 SME claims surpassed \$1 million.
- 265 SME claims fell between \$500,000 and \$1 million.
- SMEs' average cost for business interruption alone was \$370K.
- While SMEs' average incident cost dipped slightly from 2021 to 2022, average ransom payments rose from \$514K to \$555K.

These trends emphasize the urgency for organizations to establish robust incident response plans to mitigate cyber threats' financial and operational impacts. It is clear that the time for SMEs to prepare for potential cyberattacks is now.

Mark Greisiger, President & CEO, NetDiligence

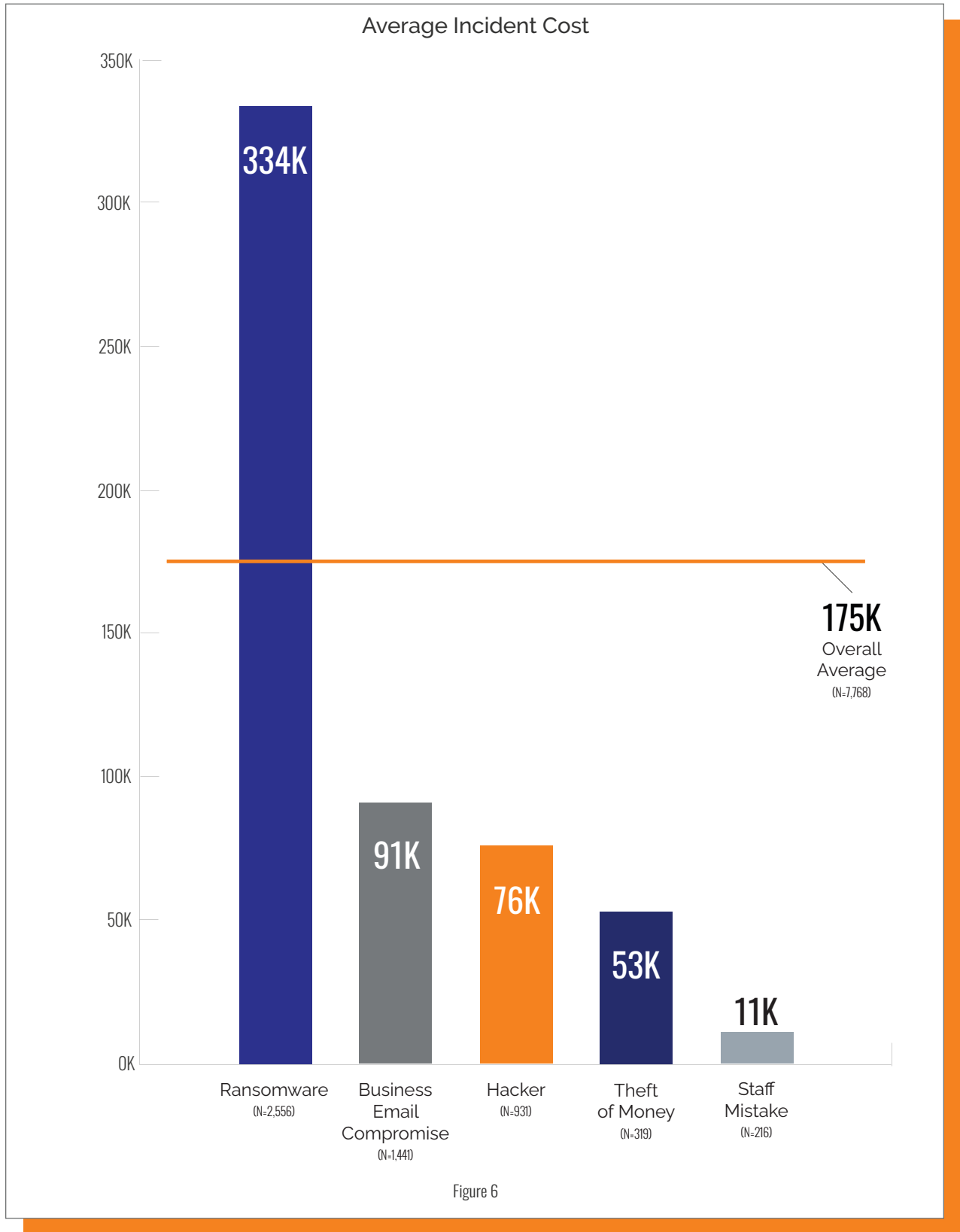
Business Sector

Top 5 by Number of Claims – SMEs



Cause of Loss

Top 5 by Number of Claims – SMEs



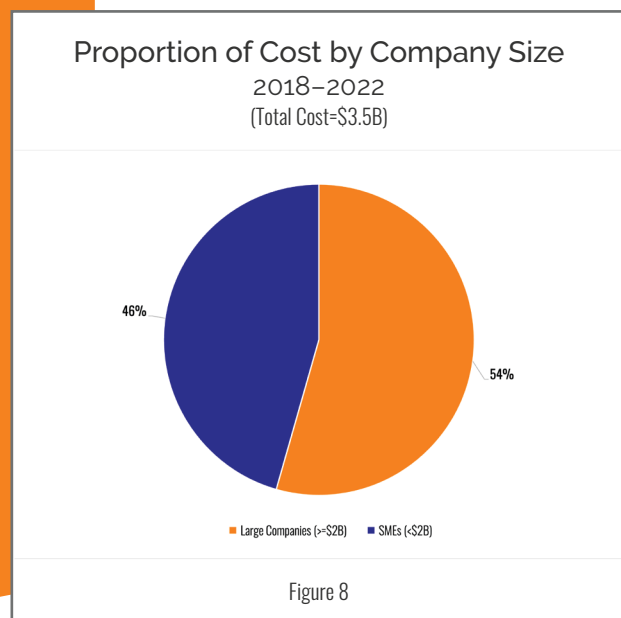
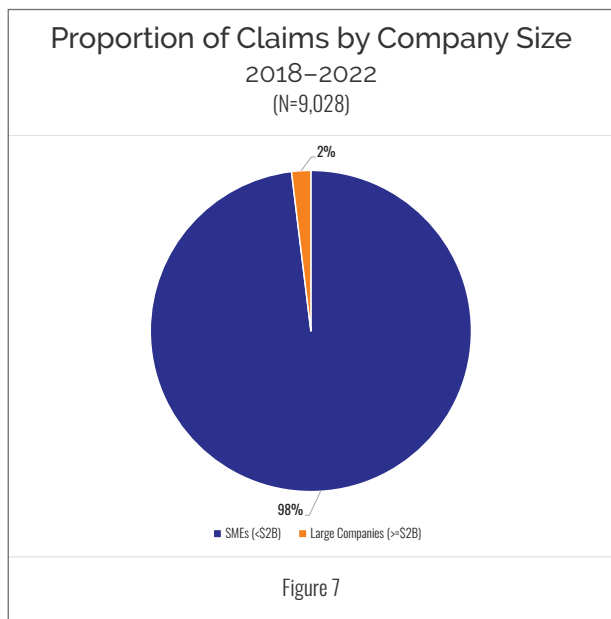
An Overview of the Data

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 \$170B. As indicated earlier, the dataset is overwhelmingly weighted with claims from smaller companies. This can dilute the findings for large companies; at the same time, large companies can function as outliers that skew the findings for small organizations.

For that reason, the dataset has been divided into two categories based on the size of the insured entity. Organizations with less than \$2B in annual revenue have been defined as small to medium enterprises (SMEs), while those with greater than \$2B in annual revenue have been defined as large companies.

A large percentage (63%) 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 \$11K to \$1.9B. The average was \$94M. SMEs accounted for 98% of claims but only 46% of total incident cost.
- Large Companies: annual revenue ranged from \$2B to more than \$170B. The average was \$13.3B. Large companies accounted for only 2% of claims but 54% of total incident cost.



The 2023 Cyber Claims Study found no clear correlation between the size of an organization and the magnitude of a cyber-related loss. It indicated, however, that SMEs experiencing larger losses may incur greater organizational impact. This is consistent with the experience of the Constangy Cyber Team. We manage responses to thousands of data security incidents on an annual basis, primarily with SMEs but with many large companies as well. We have found hundreds of variables that determine the impact of an incident, few of which are restricted to the size of an organization. The key for incident response professionals is to identify and manage, if possible, variables that control impact – recognizing some may have a disproportionate organizational impact on SMEs.

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

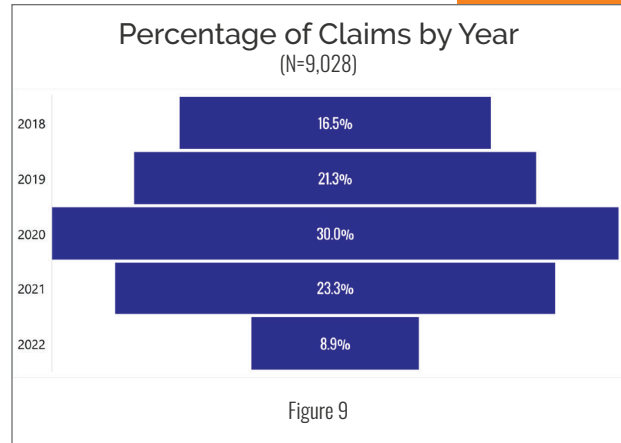
Claims by Year of Event

The scope of this study is 9,028 incidents that occurred from 2018 to 2022. The distribution of incidents by year is depicted in Figure 9.

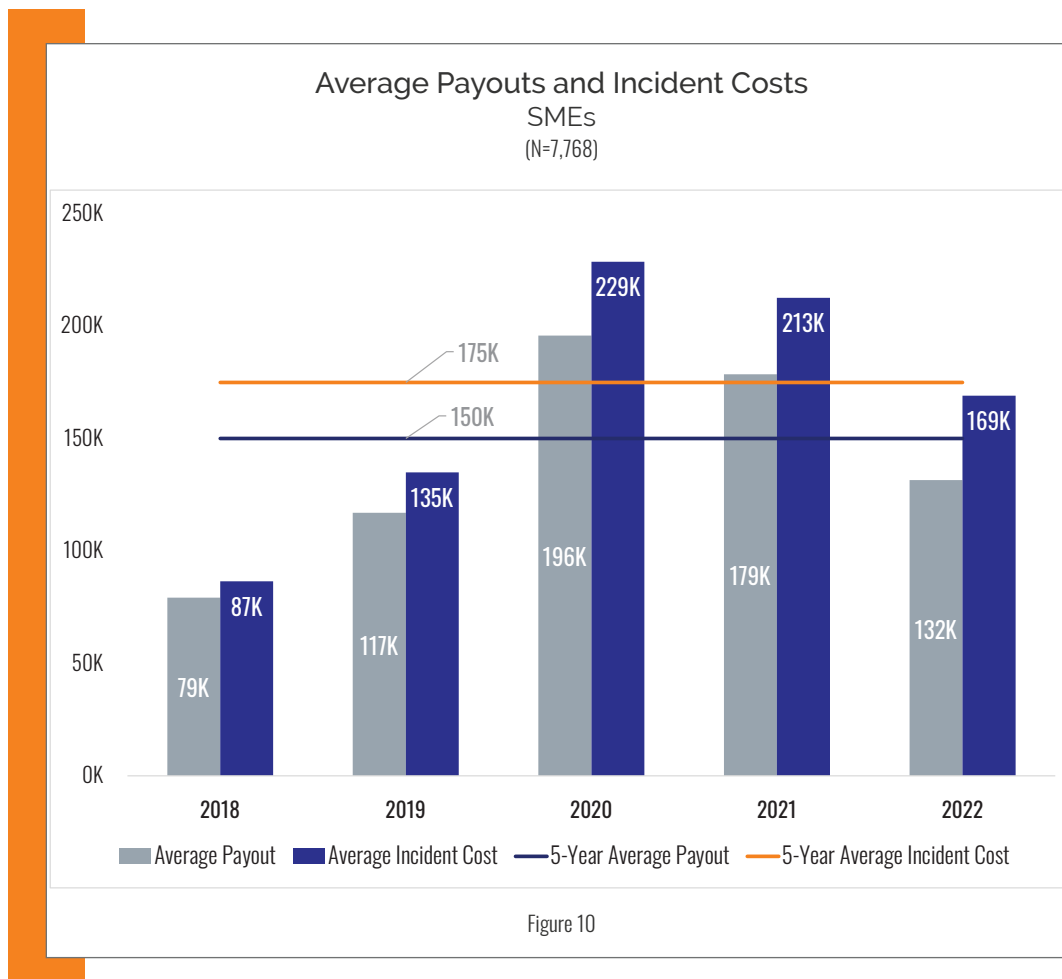
Demographic analyses have been based upon all 9,028 claims. Cost analyses have been based upon the 7,906 claims that reported incident costs >=\$1,000.

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

Detailed analyses of these four categories can be found below.



Incident Costs and Payouts



Study participants were asked to provide information about both the amount of money paid on a claim and an estimate of the total cost of the incident, including any SIR and other costs incurred that may have been excluded due to the terms of the policy.

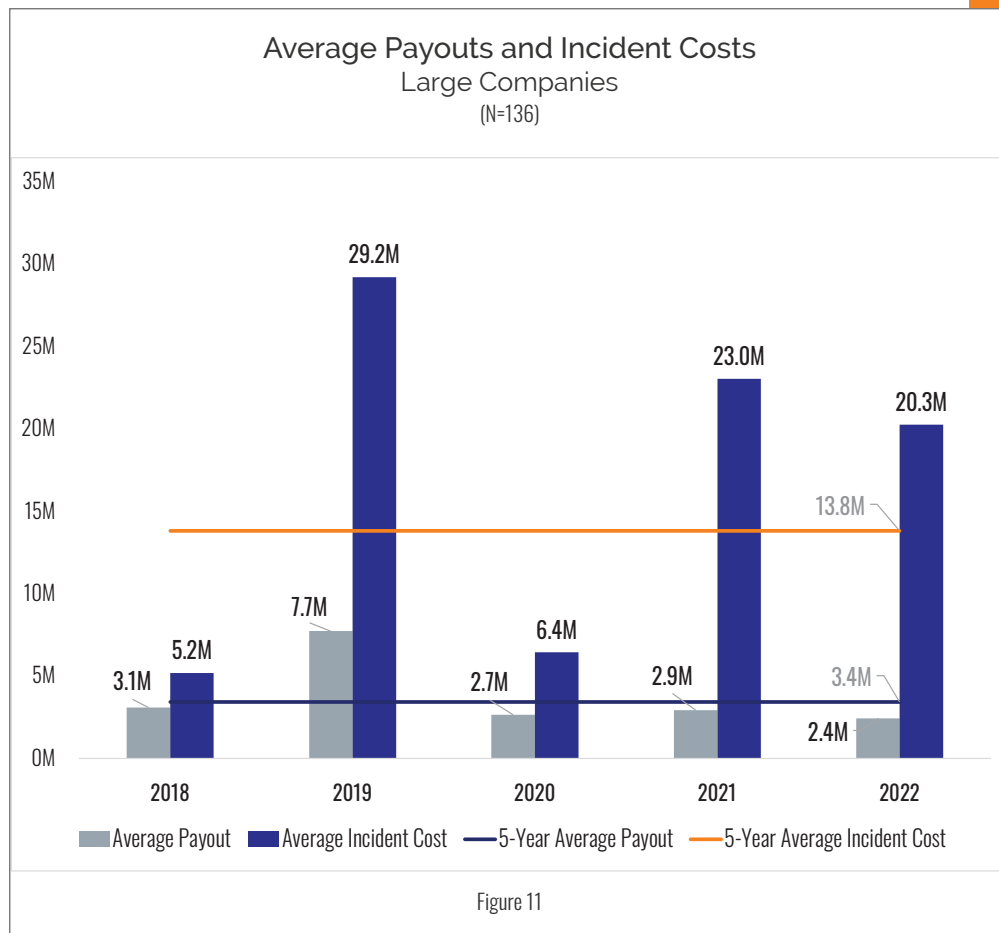
There were 254 SME claims over \$1M, and another 265 claims between \$500K and \$1M. The largest SME claims occurred in 2022 (>\$100M). These incidents happened in the manufacturing and healthcare sectors. Both involved ransomware with very large ransoms and extremely large business interruption losses (>\$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 (>\$400M). Between 2018 and 2022, there were 9 claims at large companies with over \$50M in total incident cost, and another 8 claims with between \$25M and \$50M in total incident cost.

Payouts for organizations of all sizes represented 47% of the total incident cost. For SMEs, the five-year payout was 85% of the total incident cost. At large companies, this number was 25%.

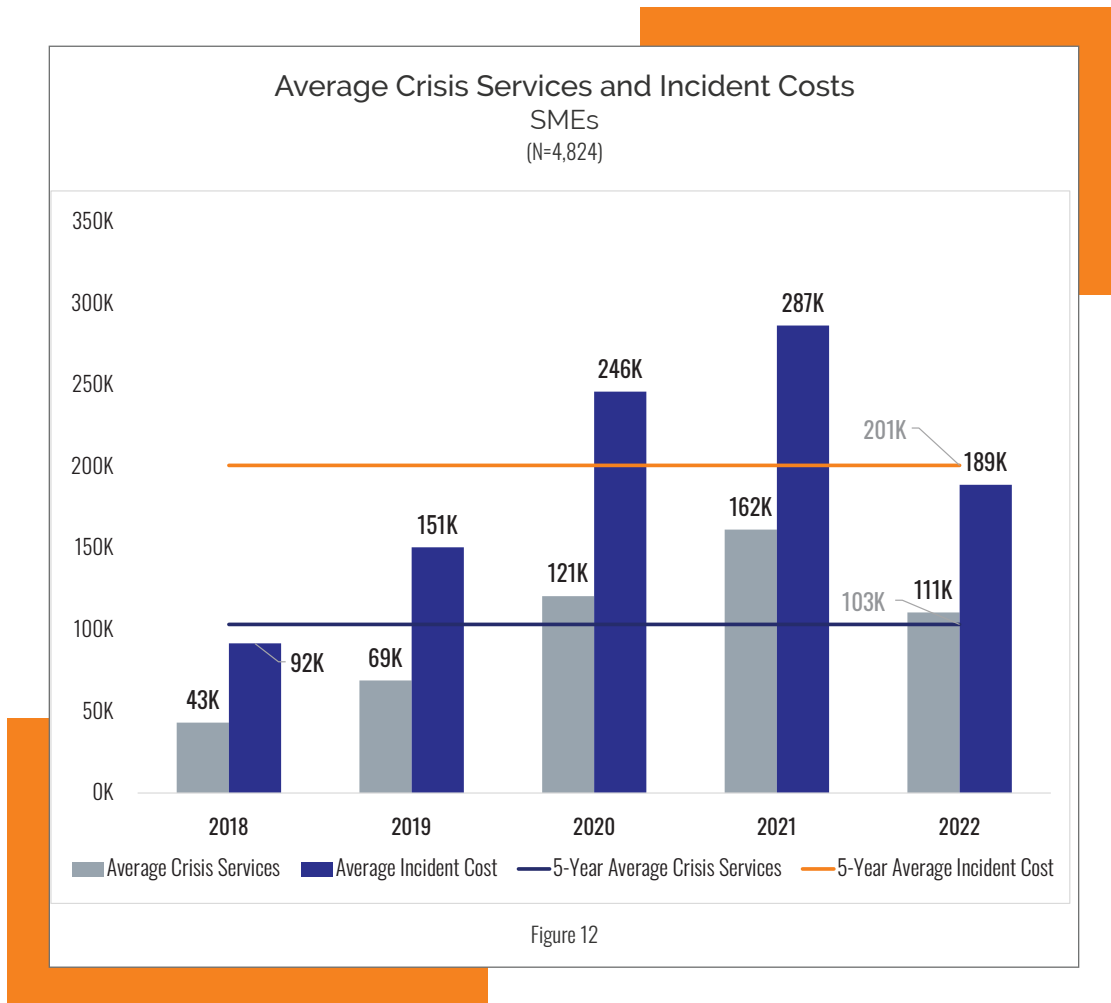
Figure 10 (above) and Figure 11 (below) provide the year-by-year average and the five-year average payout amount and total incident costs for both SMEs and large companies.

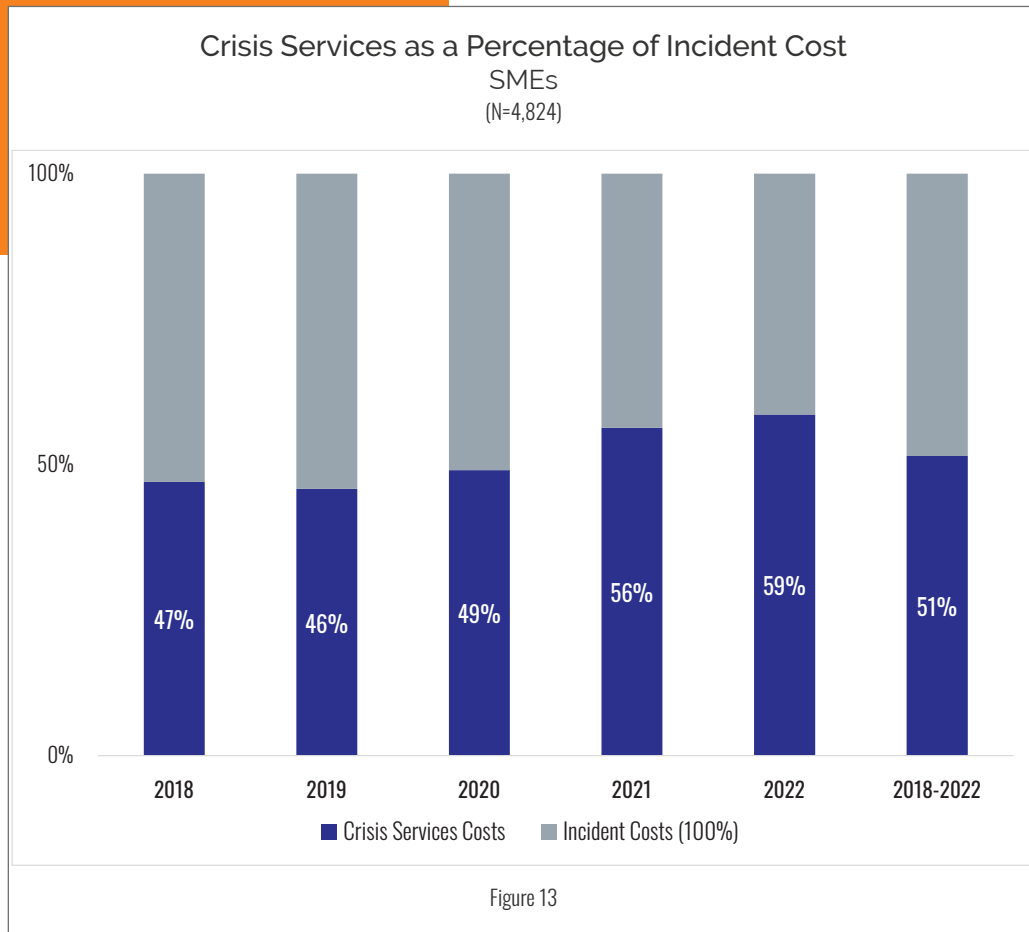


Incident and Crisis Services Costs

For all organizations, crisis services costs ranged from less than \$100 to more than \$15M. Incident costs, inclusive of self-insured retention (SIR), ranged from less than \$1,000 to more than \$400M. The averages were influenced by some very expensive claims (see above). Not every claim involves a crisis services element. This is why the "N" values on the graphs may vary.

At SMEs, the average crisis services cost ranged from \$43K in 2018 to \$162K in 2021. The dip in 2022 is most likely because we have been collecting 2022 data for only one year. Crisis services costs for SMEs, on average, comprise about 51% of total incident costs.





It's integral to support the largest growth segment with actionable security findings - SMEs! Basic economics tells us that smaller companies generally have fewer resources to spend on securing themselves, which is clear in this claims study. SMEs need our help to understand where they should invest. As trusted security professionals, we have a very important role to play in keeping this industry healthy. For some insureds, that means knowing when to reach out to help them and how to be helpful in those moments with use of scalable solutions. By creating transparency in the underwriting process, staying relevant throughout the policy period, and remaining trustworthy resources to insureds, we are doing our part to keep this industry thriving.

Aaron Aanenson, Cyber Insurance Sales and Thought Leader, Bitsight

Figures 14 and 15 depict the average crisis services costs by individual component, as well as the percentage of total crisis services costs that each component represents. During the five-year period, forensics accounted for 25% of the total and legal guidance accounted for another 9% of the total.

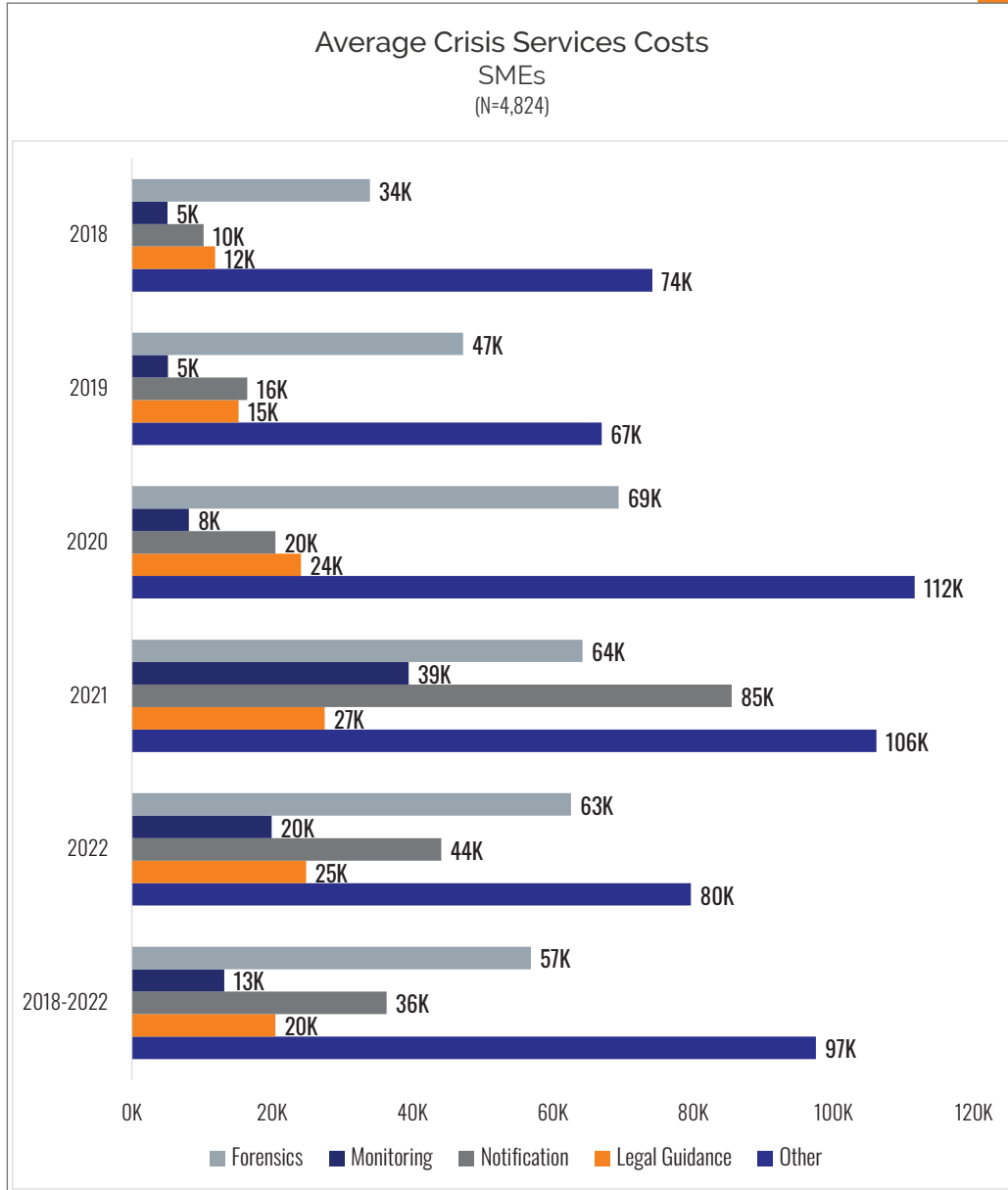
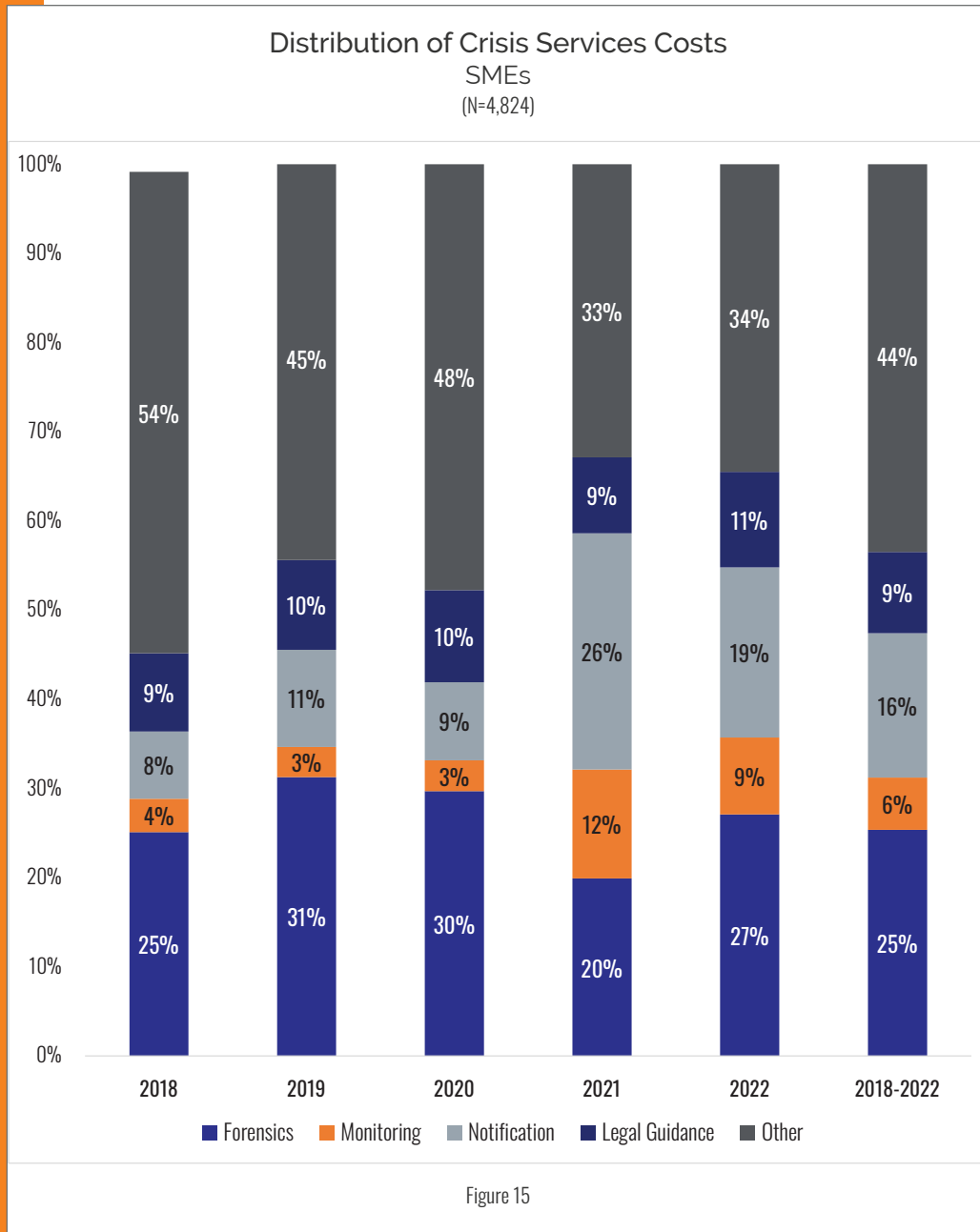
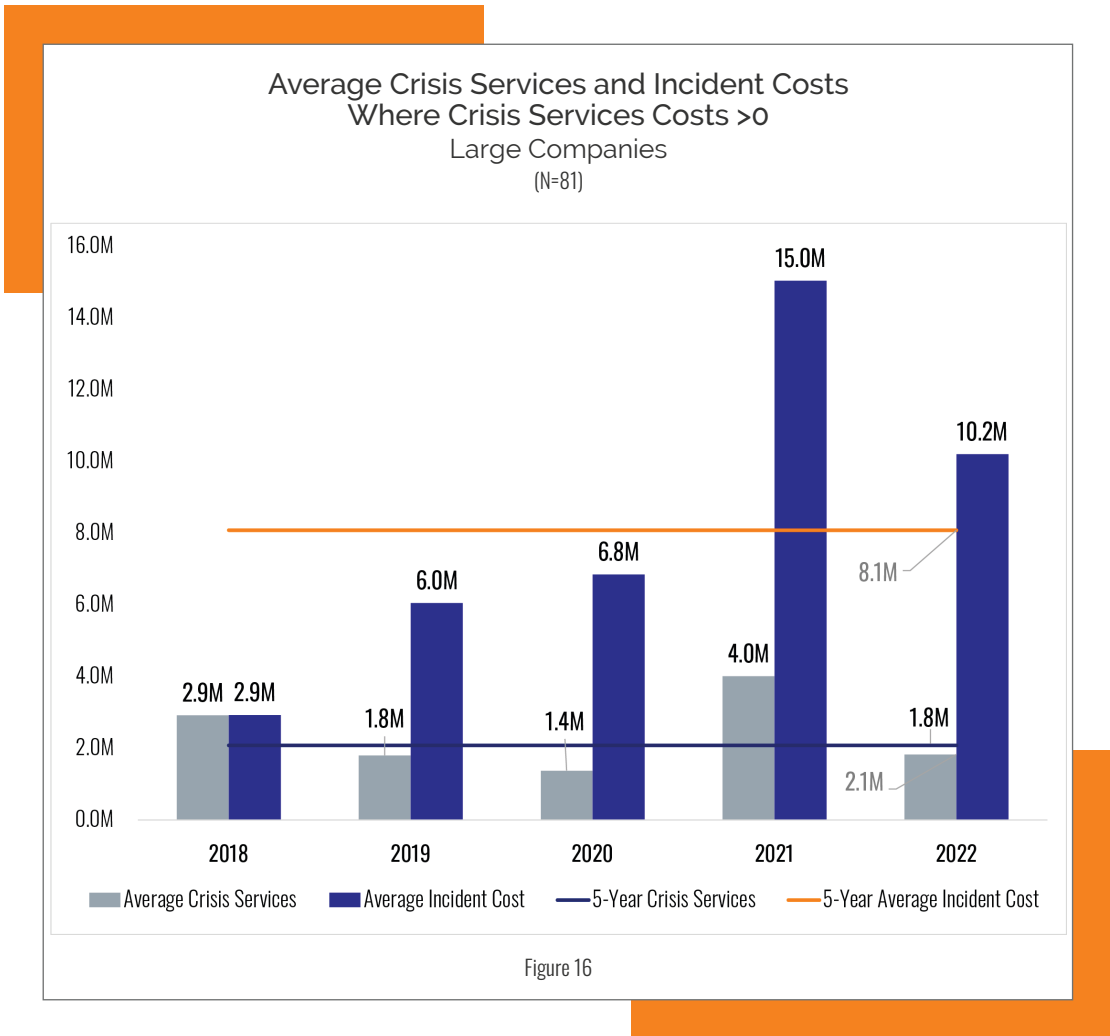


Figure 14



At large companies, there was an outlier event in 2021 that caused a spike in the average crisis services and incident costs. From year to year, there was quite a bit of variability in both the average crisis services costs and the incident costs, with average incident costs ranging from \$2.9M to \$15M.

Crisis services costs accounted for 20% to almost 100% of incident cost year-over-year, and 26% over five years, which are about the same proportions as the previous five-year period (27% from 2017-2021).



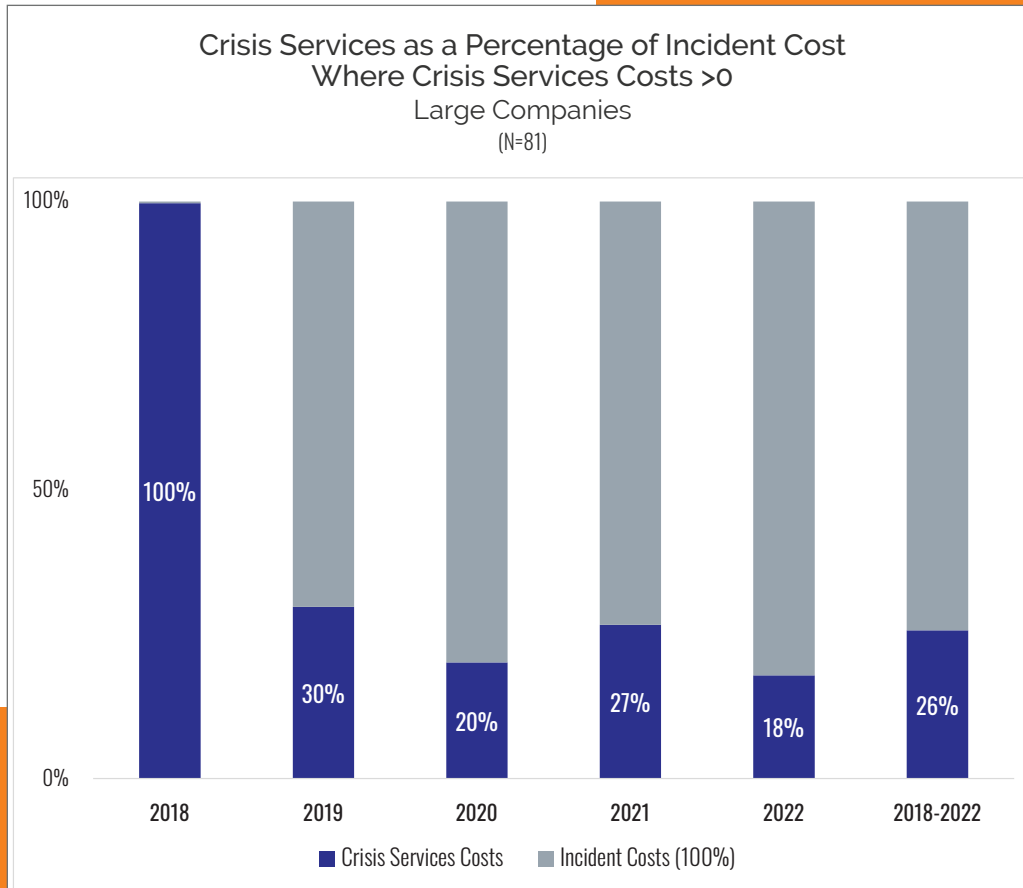


Figure 17

Notification costs periodically reflect the source of additional liability. Every person notified of a data security incident is a potential plaintiff in a class action lawsuit. We have defended class actions resulting from data breaches in which plaintiffs were part of an "over-notified" population. If unnecessary notification costs are eliminated, the potential resulting liability can be proportionately mitigated.

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

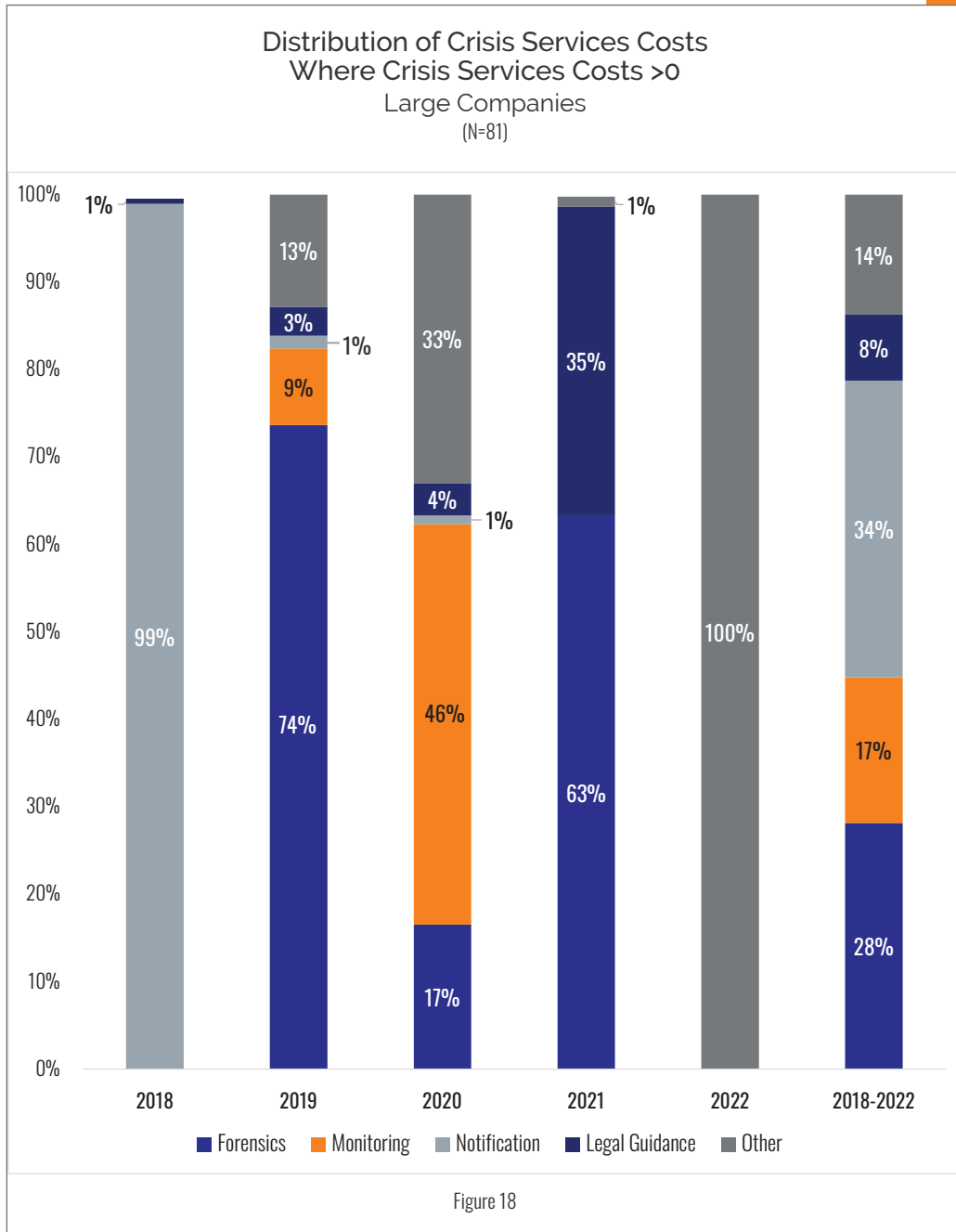


Figure 18 depicts the percentage of total crisis services costs of each crisis services component. Year over year, there is much variability.

Business Interruption (BI) and Recovery Expense

SMEs

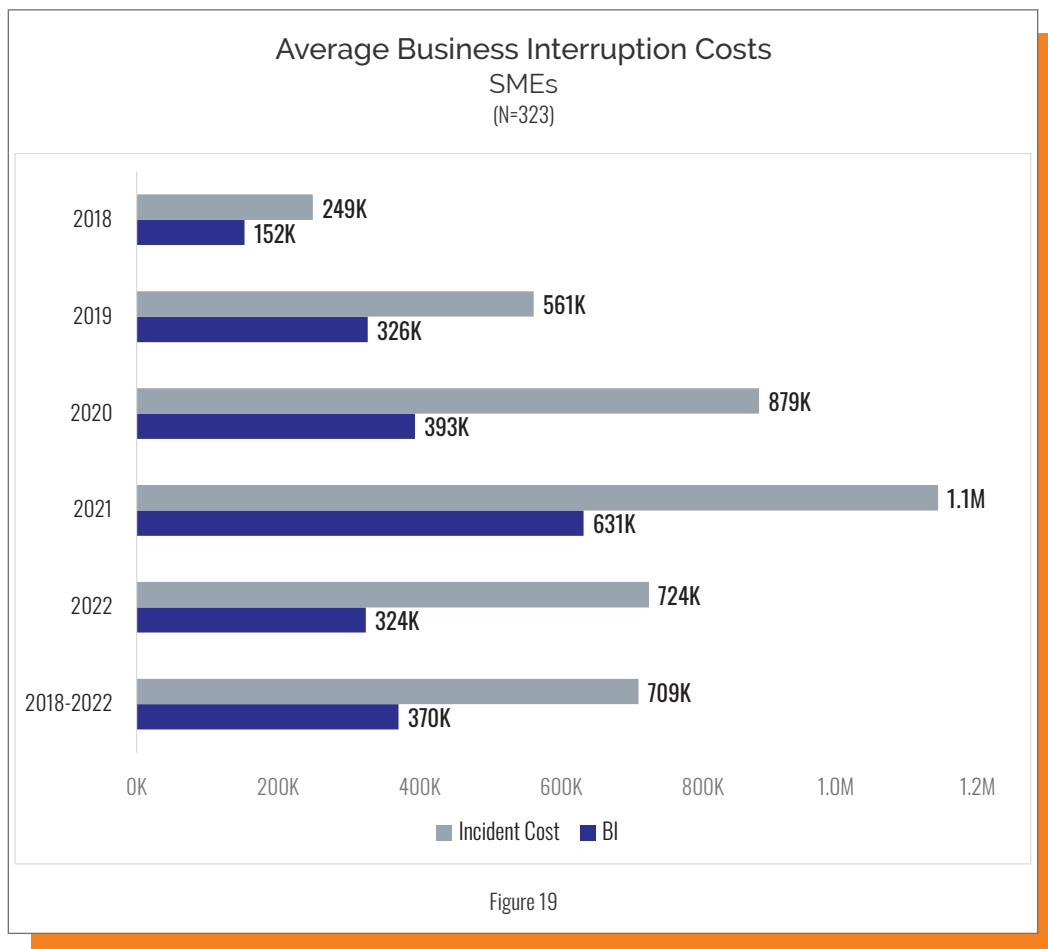
BI costs were reported for 323 incidents. Since 2018, the average BI cost and corresponding average incident cost have increased dramatically. The decrease in 2022 shown in the graph below is most likely a result of a smaller set of claims collected so far for 2022.

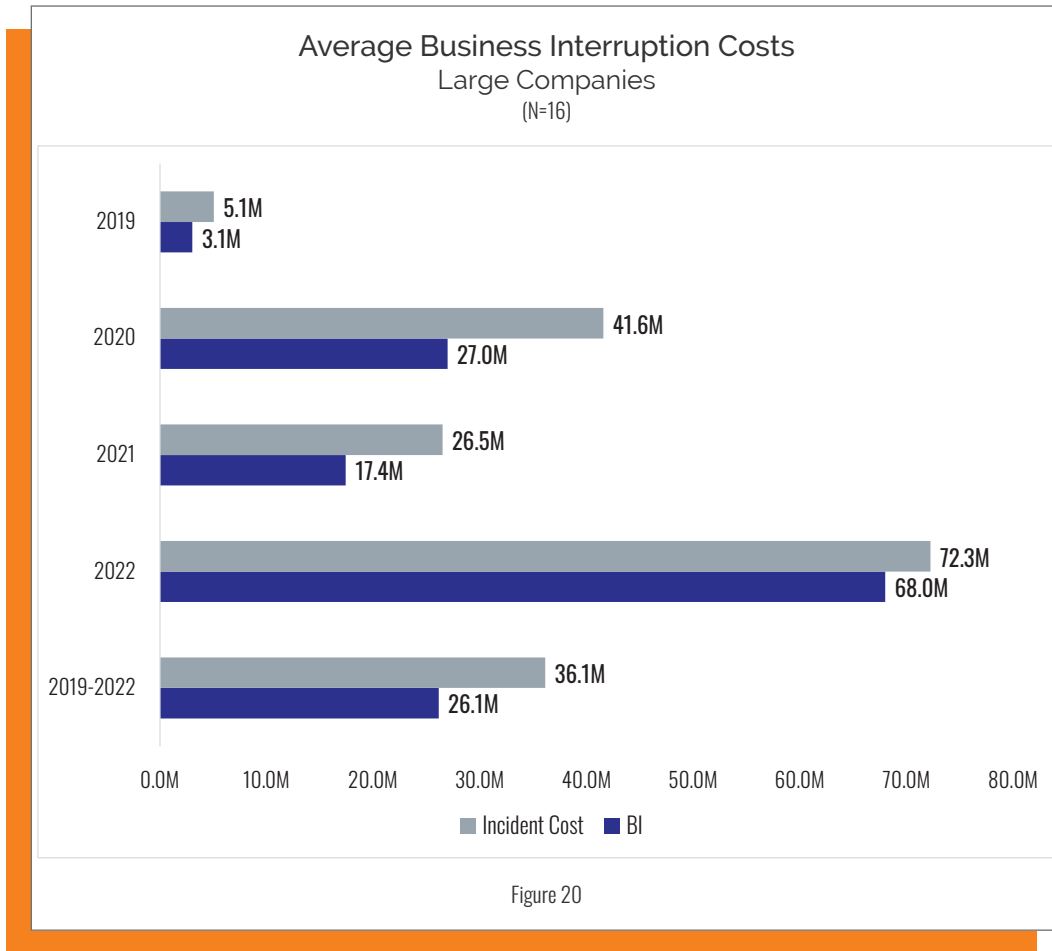
The five-year average incident cost of a claim that involved BI was over four times greater than a claim that did not involve BI. In 2022, the average claim involving BI was two and a half times greater than one that did not.

Ransomware incidents at SMEs accounted for 90% of claims with a BI component. The five-year average BI cost for ransomware incidents (ransom amount known) was \$454K. The corresponding total incident cost was \$1.01M. In 2022, these numbers were \$371K and \$1.0M, respectively.

Large Companies

Figure 20 depicts average BI and total incident cost at large companies. Even though the number of claims is small and there is quite a bit variability, the numbers are eye-opening, especially in 2022.





Business interruption and incident costs can be a formidable challenge, capable of undermining even the most robust organizations. Adaptation and preparedness are the keys to weathering the storms of uncertainty and safeguarding the future of enterprise.

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

Recovery Expense

SMEs

There were 281 claims that reported recovery expense. As Figure 21 shows, recovery expense has been steadily increasing since 2018, and the total incident cost of these events has been increasing since 2018. The average five-year incident cost of these claims is about 60% higher than incidents without recovery expense. In 2022, the incident cost was over 300% greater when recovery expense was incurred.

Ransomware incidents accounted for 85% of the claims with recovery expense reported. The five-year average incident cost of these events was 250% higher than incidents without recovery expense. In 2022, these incidents cost almost six times more.

Large Companies

There were six large company claims that reported recovery expense. Five of these were due to ransomware, and one was due to malware. The five-year average recovery expense was \$1.1M, and the average total incident cost was \$12.9M. So far, there are no claims with recovery expense in 2022. That may change next year as we collect additional data for 2022.

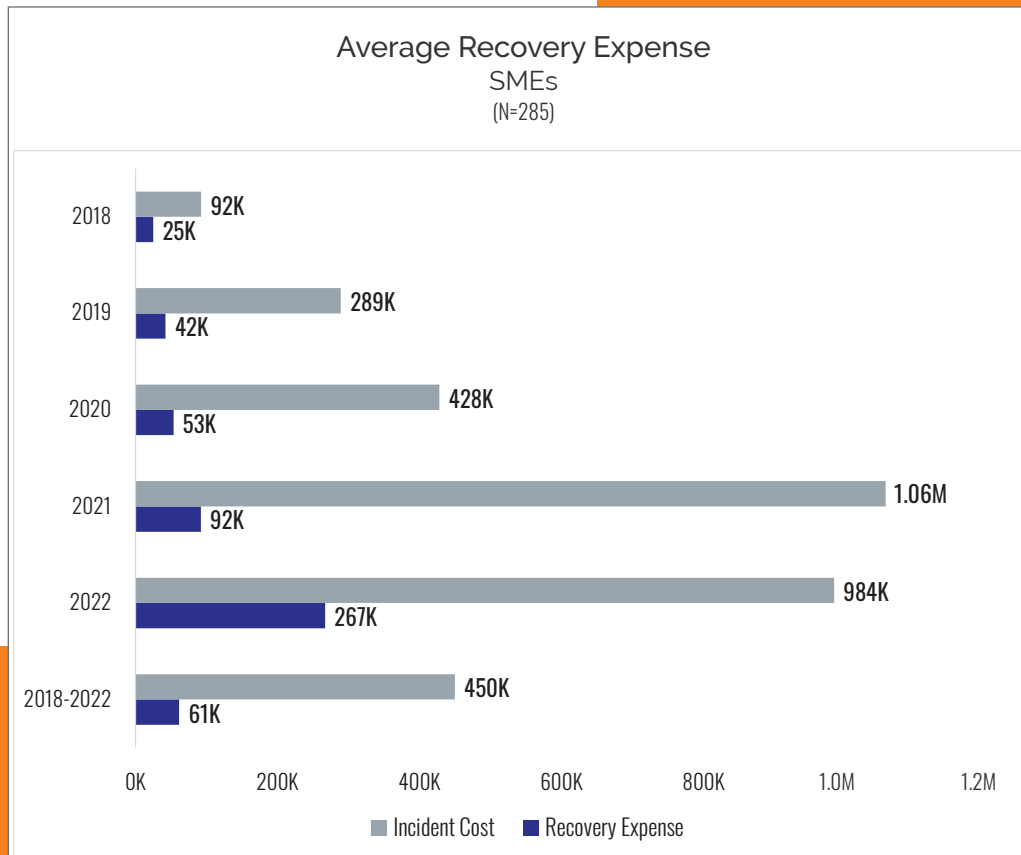


Figure 21

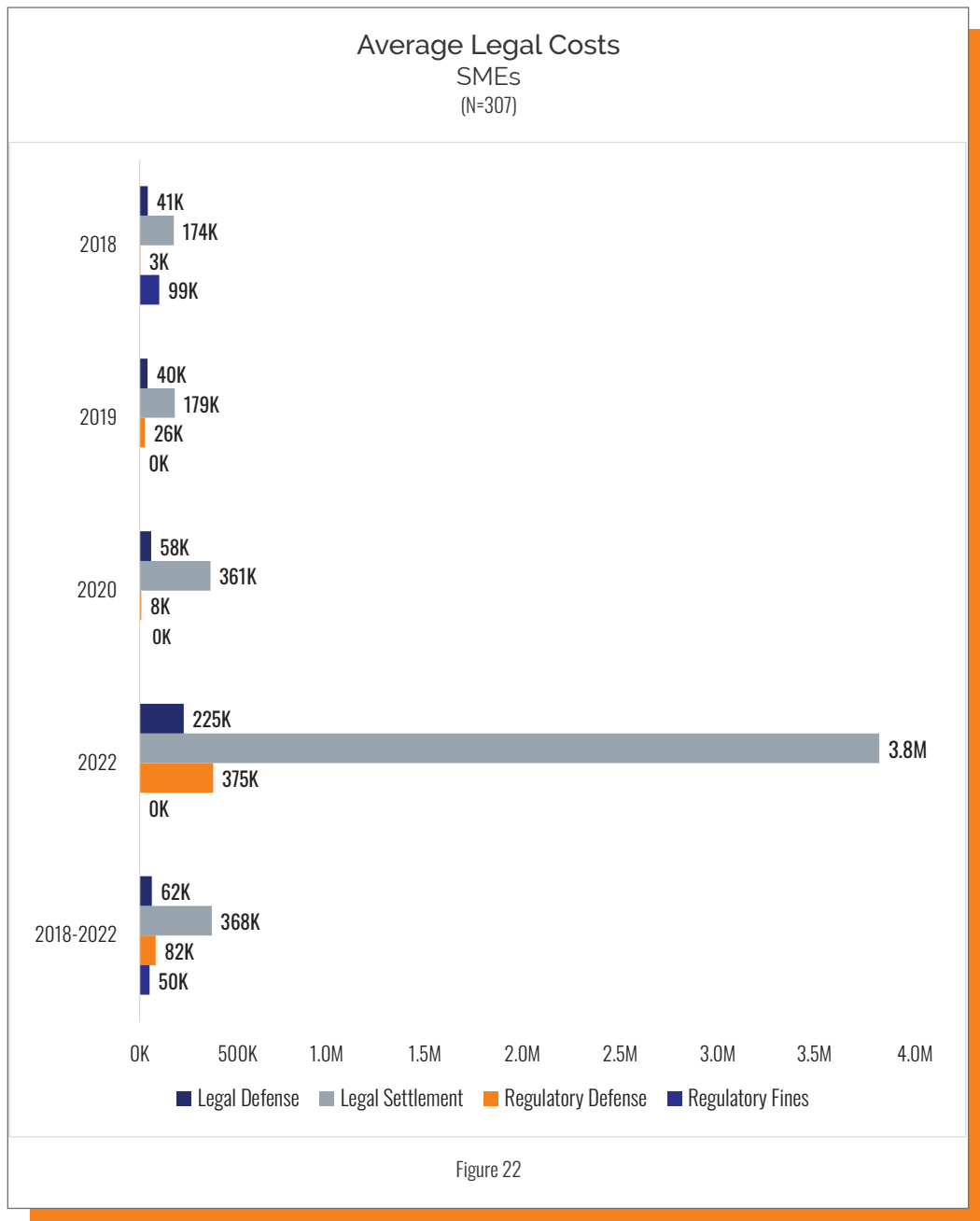
Legal Costs

SMEs

There were 307 claims in the dataset that reported at least one type of legal or litigation expense. Figure 22 depicts the yearly averages for the four categories as well as the five-year averages. There was much year-over-year variability in these costs.

Large Companies

The dataset contained 12 claims that reported at least one type of legal or litigation expense. For the five-year period, the overall average was \$5.7M, with a maximum of over \$400M (settlement). This large settlement is driving up the overall averages. Average settlement defense cost was \$890K. There was only one regulatory fine in the five-year data (\$21M).



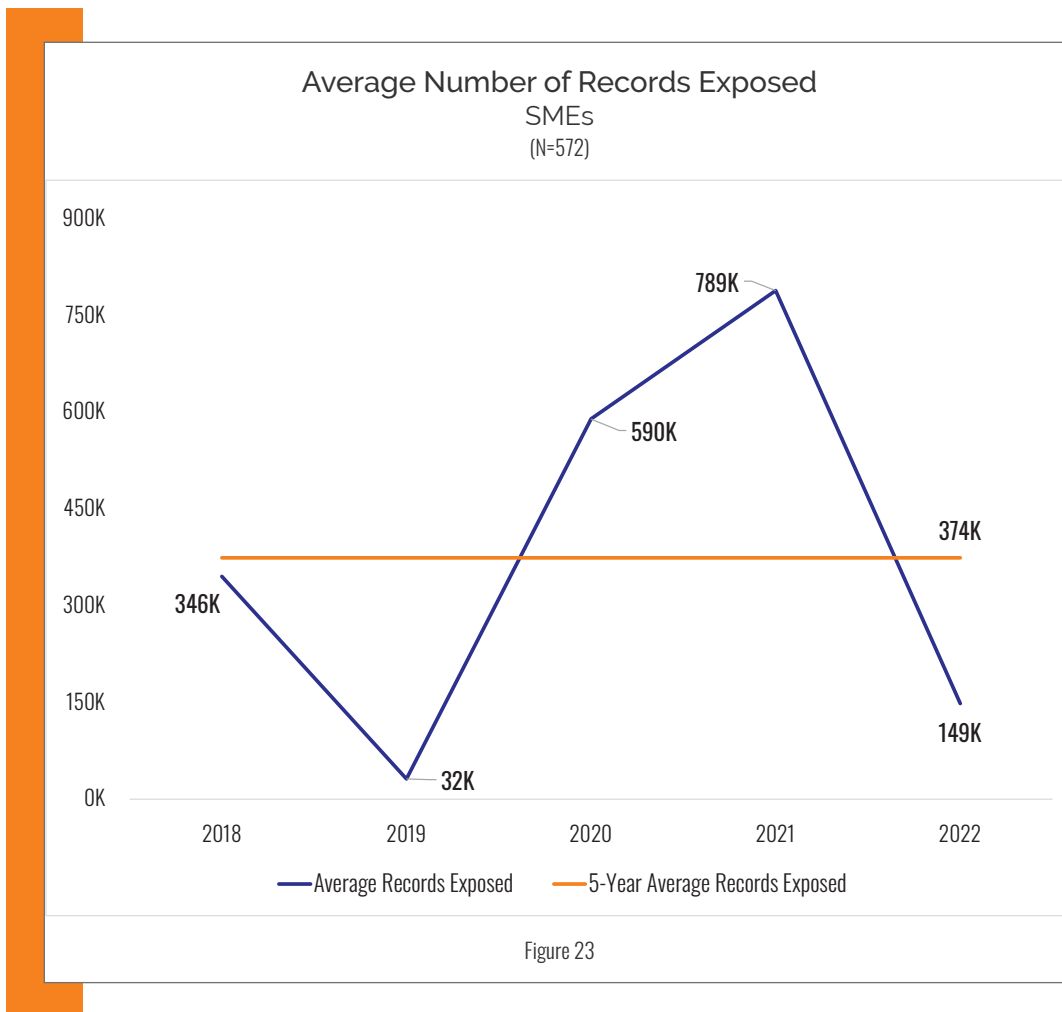
Records Exposed

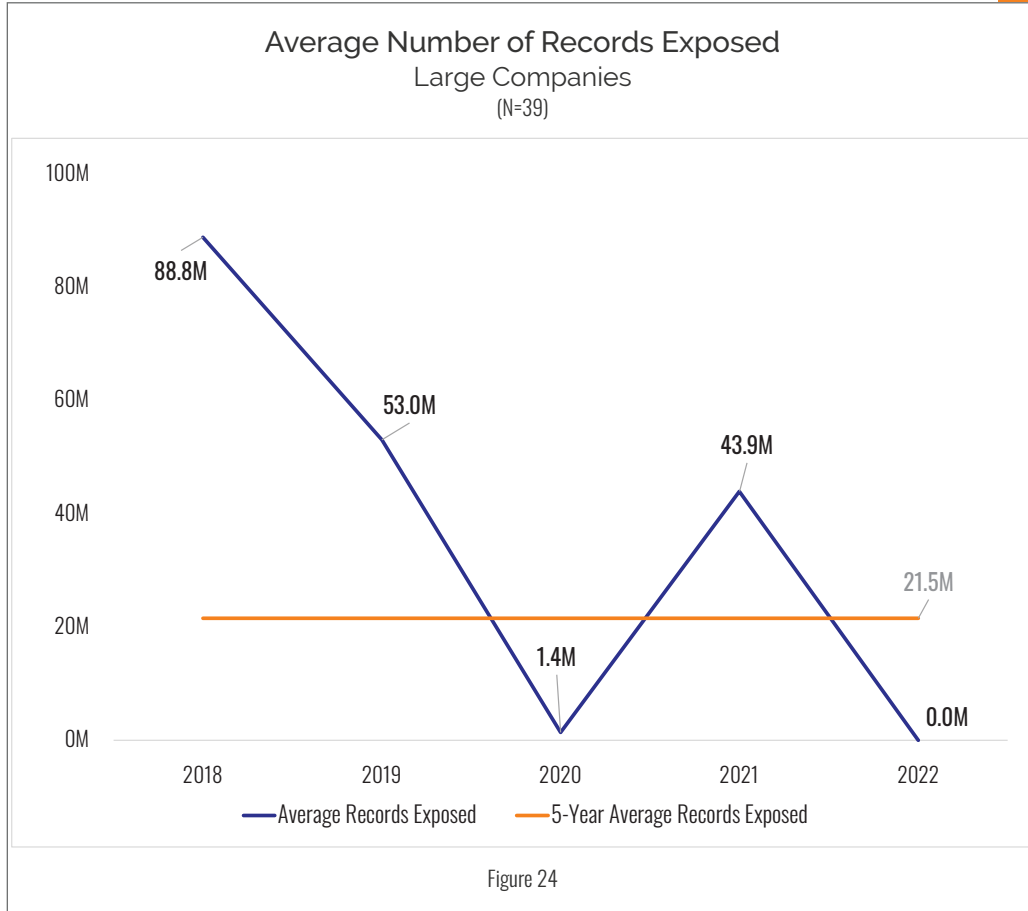
There were 611 claims that reported the number of records exposed in an incident. This represents a decrease from the previous five-year number of claims (N=755). These 611 incidents exposed over 1.0 billion records – 214M at SMEs and 840M at large companies – about the same as in last year’s report.

Figures 23 and 24 show the year-over-year and five-year average number of records exposed. There is no distinguishable pattern. As analyzed in previous NetDiligence Cyber Claims Studies, the number of records exposed does not correlate well with either the size of an organization or the total incident cost.

While we cannot say for certain why the number of claims with exposed records is decreasing, we can speculate:

- The large proportion of ransomware and BEC claims since 2020 do not involve exposed records.
- Perhaps, as we have been stressing for many years, the lack of utility of per-record metrics is causing people to be less concerned with the number of records than they used to be.



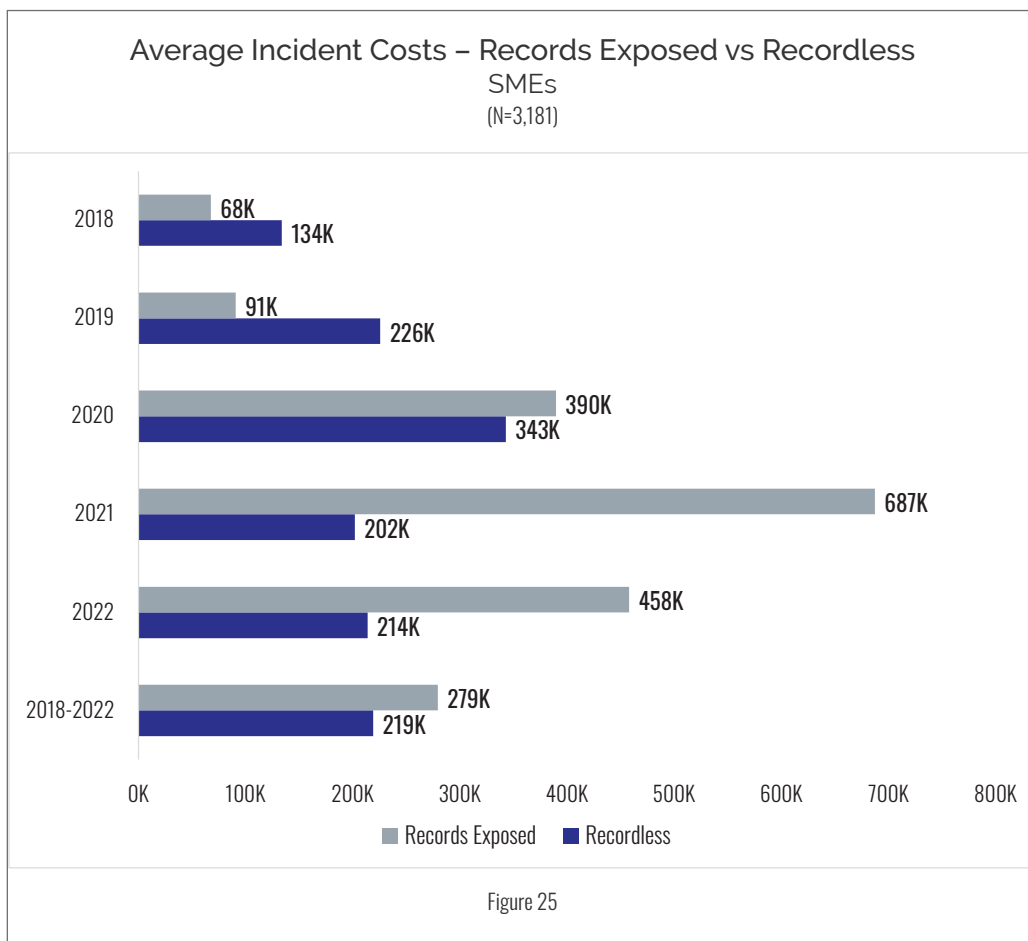


Recordless Claims and Claims with Exposed Records

"Recordless" claims are incidents that do not expose records. Ransomware, BEC, wire transfer fraud, DDoS (distributed denial of service), and theft of money accounted for most of these incidents – 86% over five years.

As Figure 25 shows, incidents that expose records are more costly than those that do not.

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 above but excluded them here.



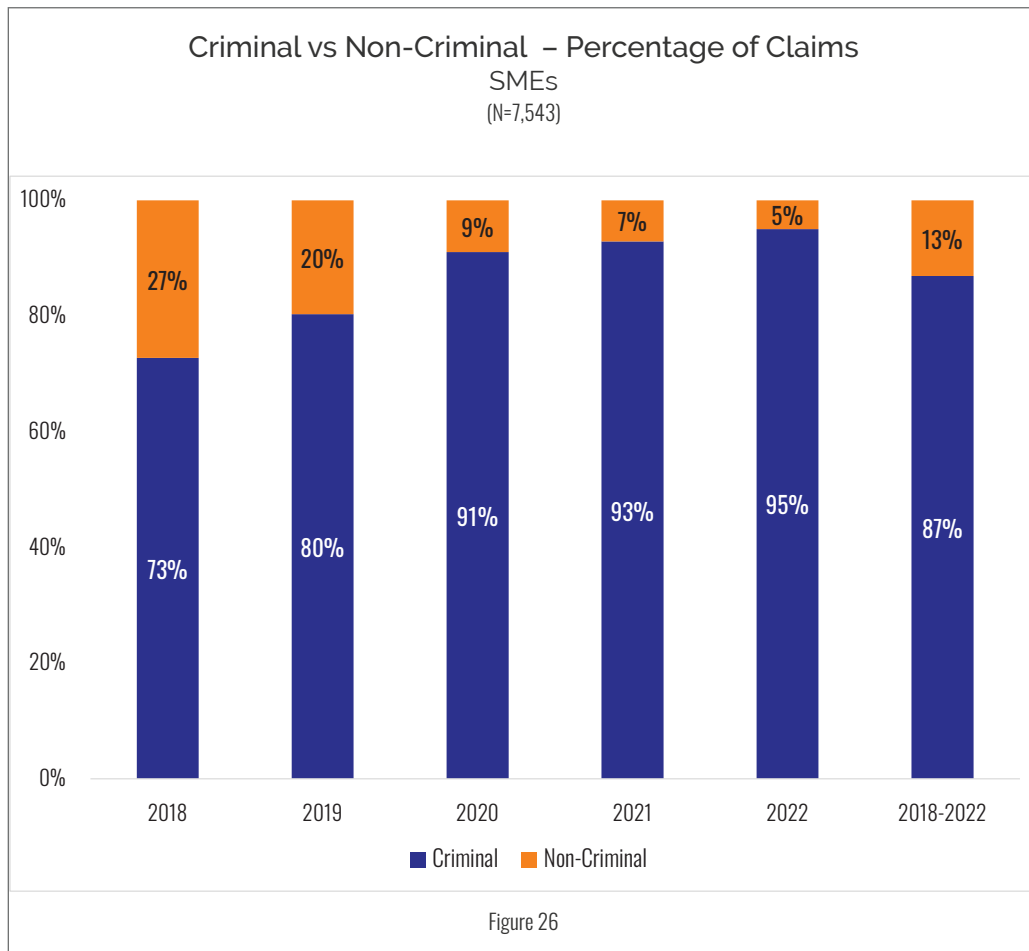
Criminal and Non-Criminal Activities

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

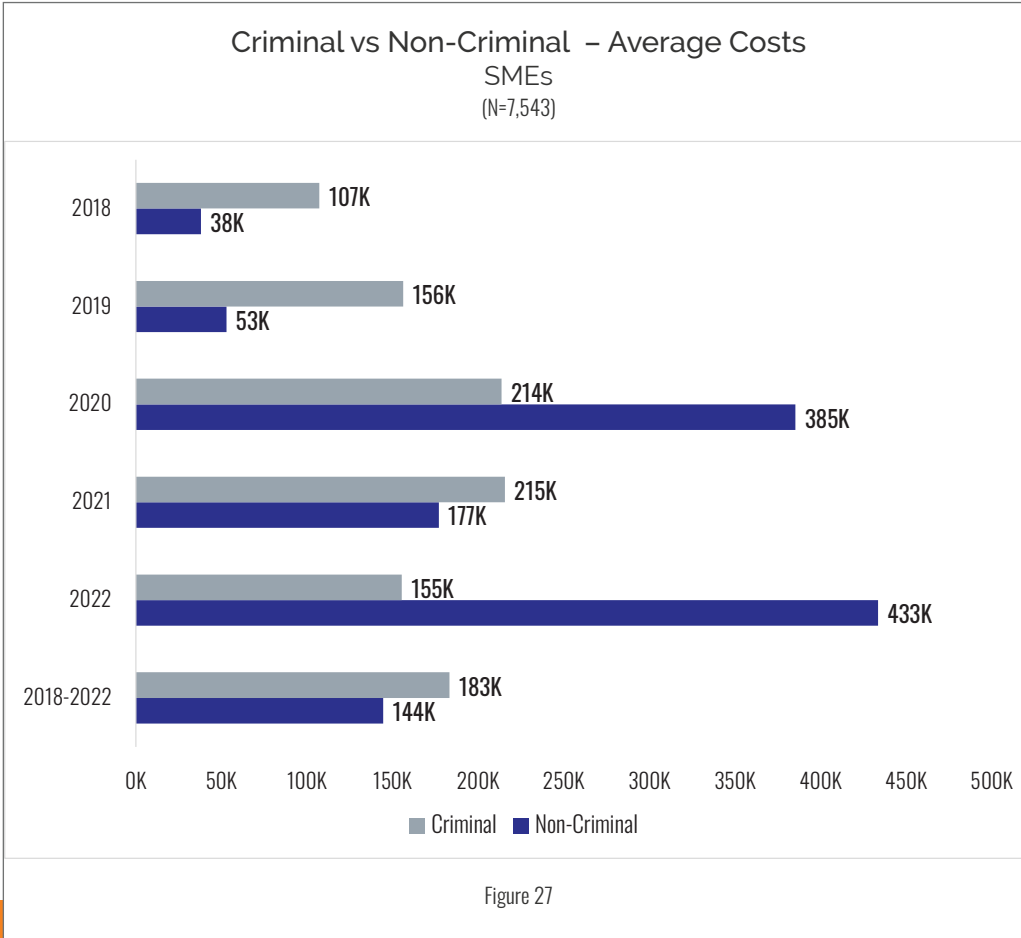
Non-criminal events include:

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



At SMEs, the proportion of claims caused by criminal activities ranged from a high of 95% in 2022 to a low of 73% in 2018. This proportion has been steadily increasing since 2018. The proportion of claims caused by non-criminal activities decreased from 7% in 2021 to 5% in 2022.

Over five years, criminal incidents at SMEs were somewhat more costly on average than non-criminal incidents. Year over year, the picture is less clear. Large events in 2020 and 2022 caused the non-criminal average cost to exceed the criminal average cost by a large margin.

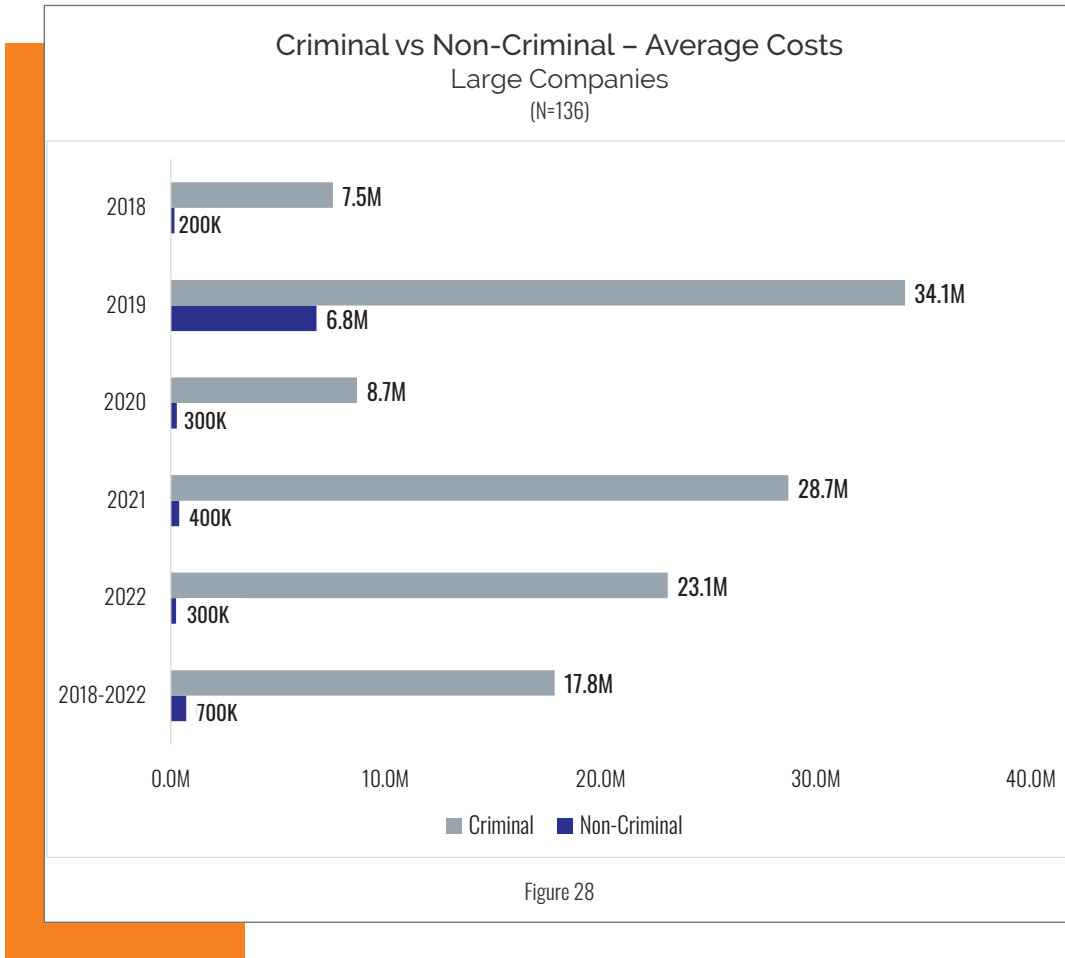


Criminal vs Non-Criminal – SMEs (N=7,543)

Time Period	Impact	Type of Activity	Average	Maximum	Total
2022	Records Exposed	Criminal	337K	3.2M	13.1M
		Non-Criminal	326K	2.8M	3.3M
	Crisis Services	Criminal	112K	3.2M	51.3M
		Non-Criminal	39K	175K	387K
	Incident Cost	Criminal	155K	10.4M	110.3M
		Non-Criminal	433K	5.1M	16.0M
2018-2022	Records Exposed	Criminal	445K	80.0M	203.8M
		Non-Criminal	98K	5.0M	10.4M
	Crisis Services	Criminal	111K	11.4M	489.9M
		Non-Criminal	21K	1.0M	7.4M
	Incident Cost	Criminal	183K	17.6M	1.2B
		Non-Criminal	144K	8.9M	142.8M

Table 1

Criminal activity was involved in 79% of incidents reported at large companies. As Figure 28 shows, the cost of criminal incidents was dramatically higher than the cost of non-criminal ones.



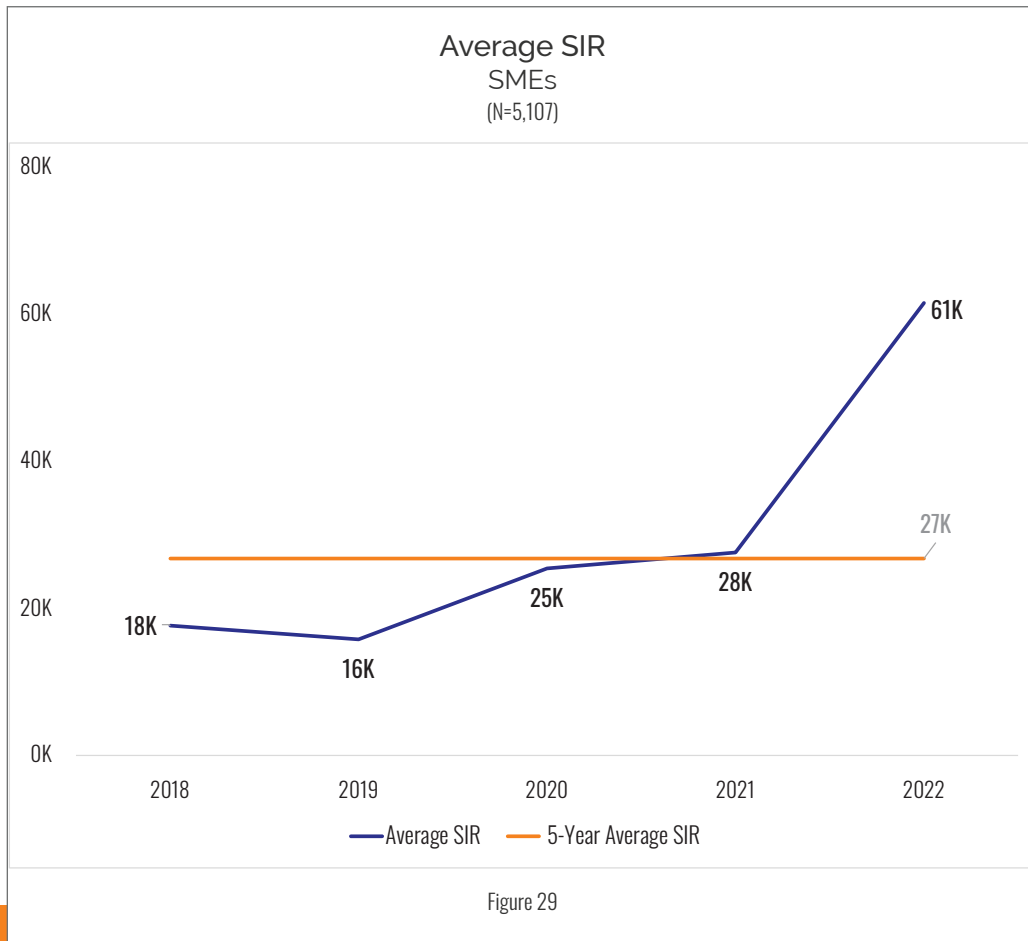
The conflict in Ukraine has had a marked impact on ransomware attacks around the world, as the parties that have traditional been behind these events are now fighting each other on the digital battlefield.

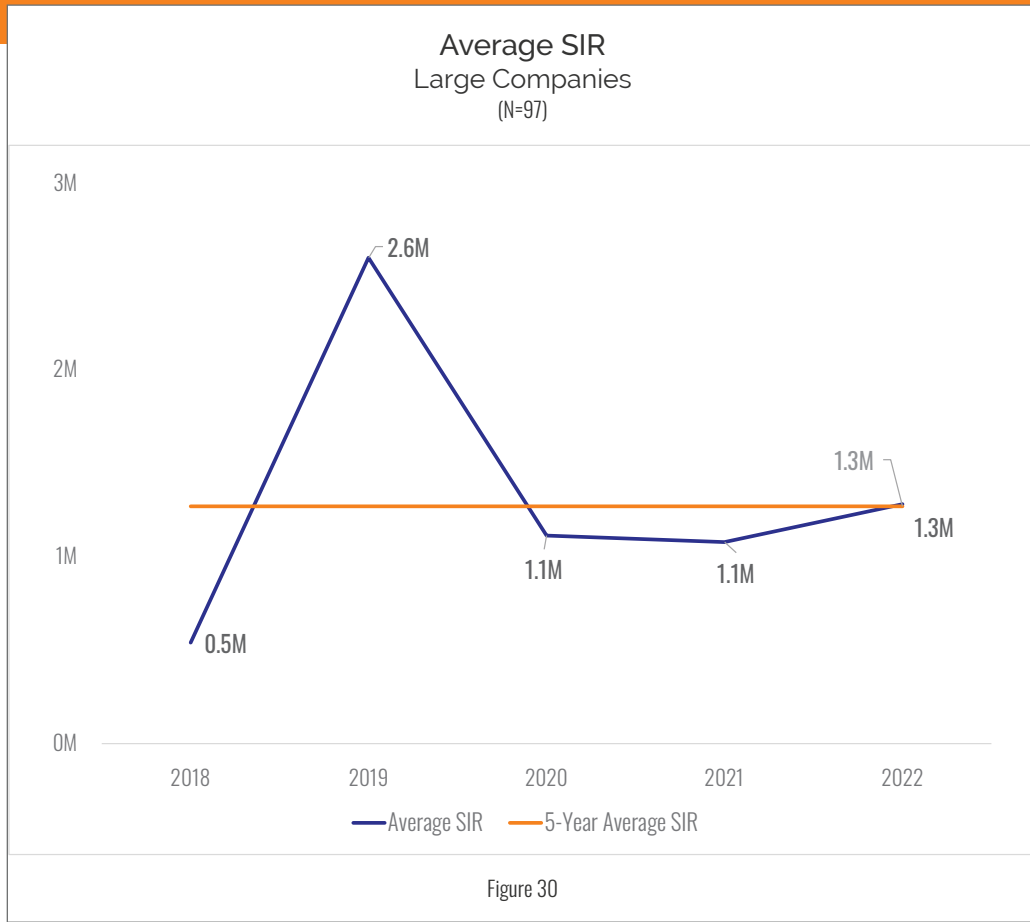
Sean Renshaw, Senior Director, Security and Privacy Risk Consulting, RSM US LLP

Self-Insured Retentions (SIR)

The dataset contained 5,107 claims for SMEs that provided an amount for SIR. These amounts ranged from \$0 to \$10M. Year-over-year averages are shown in Figure 29. Since 2019, the average SIR for SMEs has increased by almost 400%.

The dataset contained 97 claims for large companies that reported an amount for SIR. These amounts ranged from \$0 to \$10M. Year-over-year averages are shown in Figure 30. The average SIR in 2022 was 260% higher than in 2018.



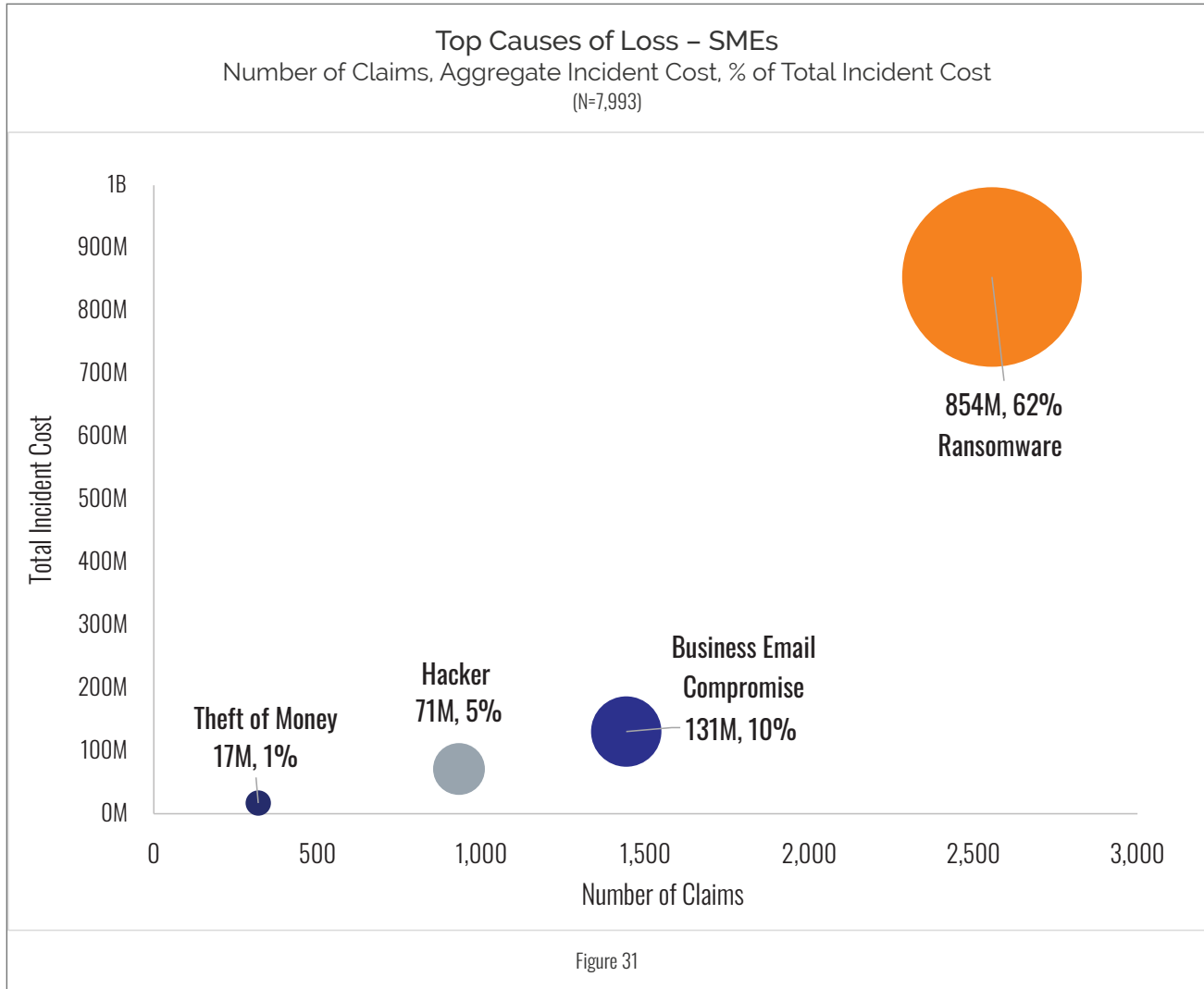


Causes of Loss

The top four causes of loss at SMEs were:

- Ransomware
- Business Email Compromise (BEC)
- Hackers
- Theft of Money

Losses in these four categories accounted for 68% of claims and 78% of total incident cost (\$1.1B). For metrics on all sectors, please see the graphs and tables in the appendices.



Ransomware

The number of ransomware incidents increased from 440 in 2018 to 628 in 2021. For 2022, the number stands at 178 so far, with additional incidents to be added to the total in the 2024 and 2025 Cyber Claims Studies.² Ransom amounts and total incident costs have also increased dramatically over the past five years.

Anecdotally, we have heard from many sources that there was a drop in the number of ransomware attacks in 2022, due in large measure to the war between Russia and Ukraine. These same sources indicated that the number of attacks increased towards the end of 2022 and into 2023.

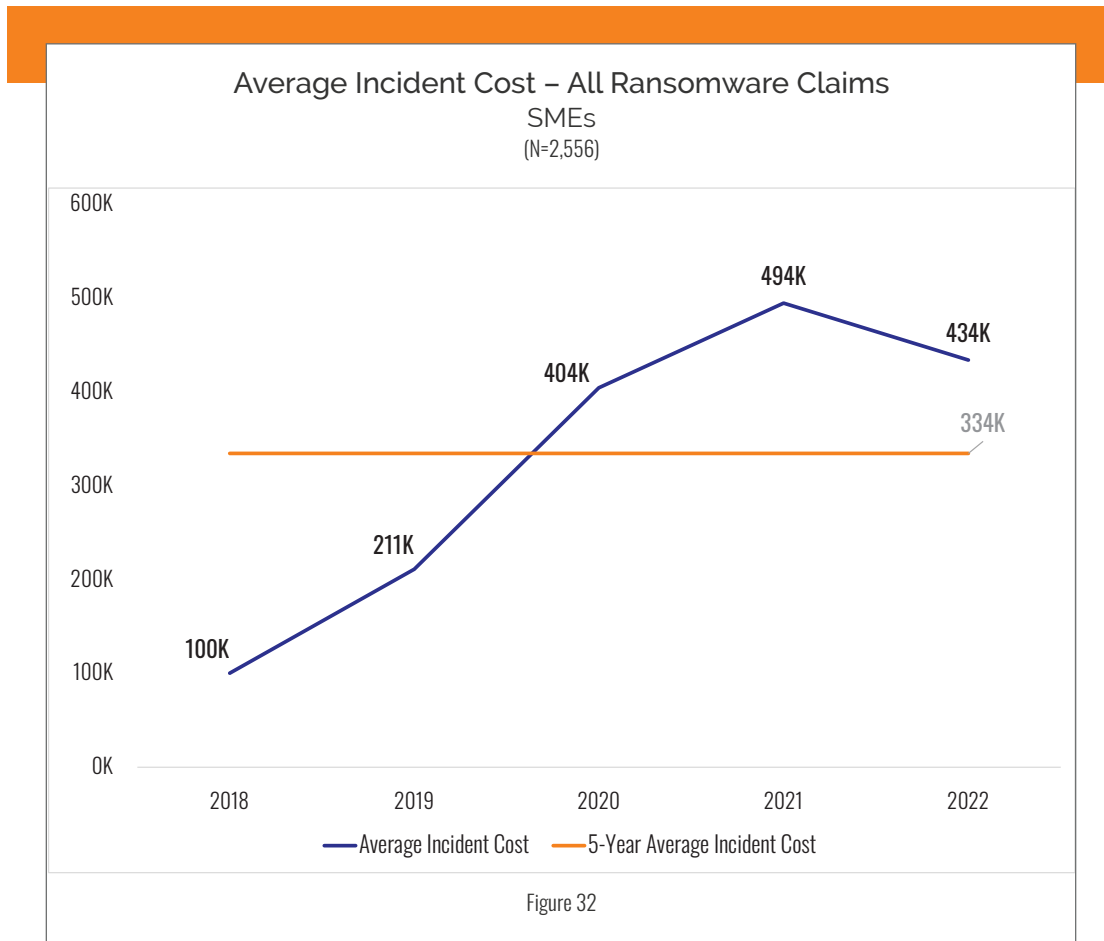
The average cost of a ransomware incident is down slightly in 2022 when compared to 2021 for both all ransomware claims and those for which the ransom paid is known. This is almost certainly due to the small number of ransomware claims collected for 2022 so far.

Our analysis looks at ransomware incidents in two ways:

- The overall cost of a ransomware event regardless of whether the amount of ransom paid was provided (over 2,500 incidents)
- The subset of ransomware events for which the ransom amount paid was known or could be estimated (over 1,000 incidents)

While both approaches provide important insight into the cost of incidents, we believe that the subset analysis provides a better picture of the costs.

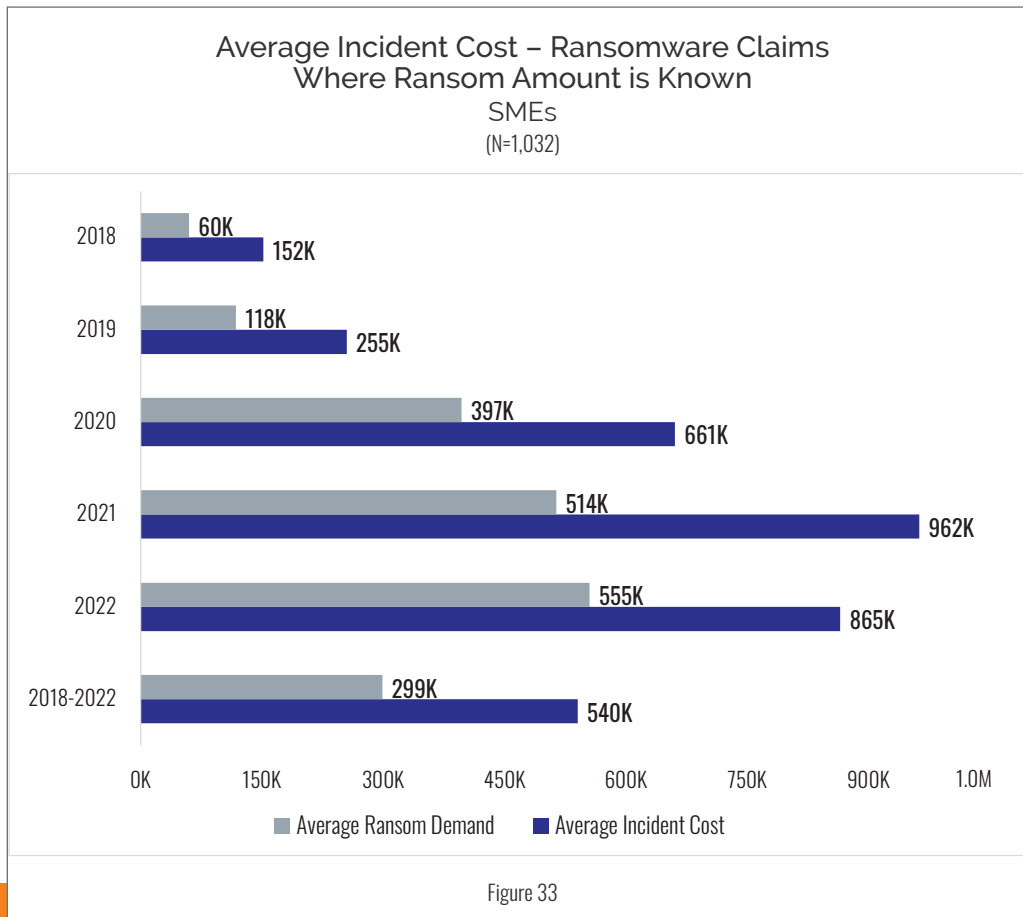
The following four figures depict both approaches, for both SMEs and large companies.



²Each year, we collect data from the three previous years. For this report (2023) we collected claims for 2020-2022. We will continue to collect claims for incidents in 2022 for two more years.

The 2023 Cyber Claims Study found the average cost of ransomware incidents down slightly in 2022 from 2021. A potential reason may be a reduction in ransom payments to prevent disclosure of stolen data. If affected consumers must be notified, the value of ransom payments to prevent disclosure of stolen information is substantially reduced because disclosure occurs through notification.

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



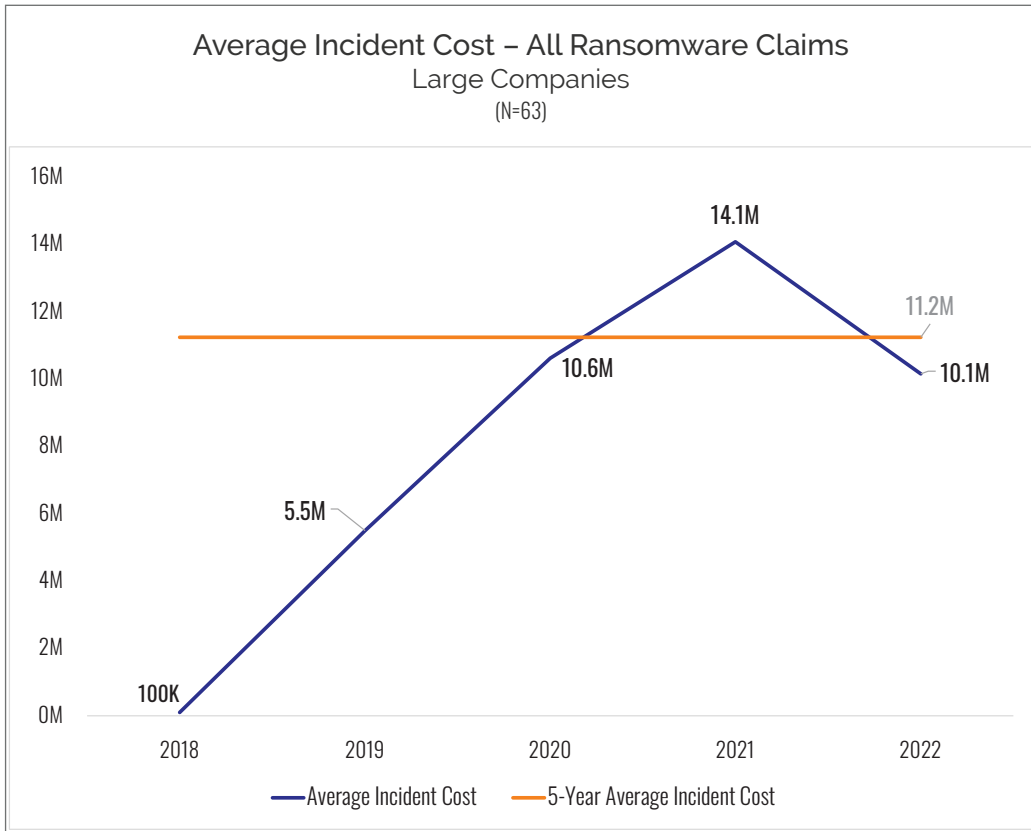


Figure 34

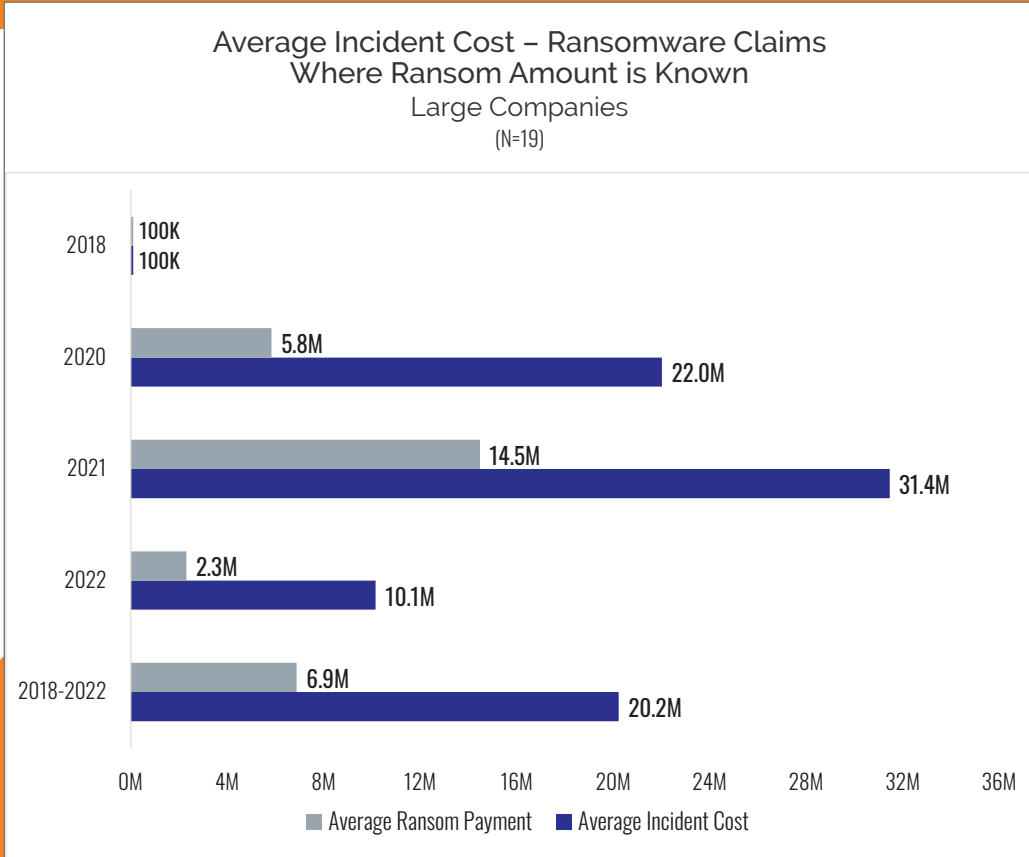
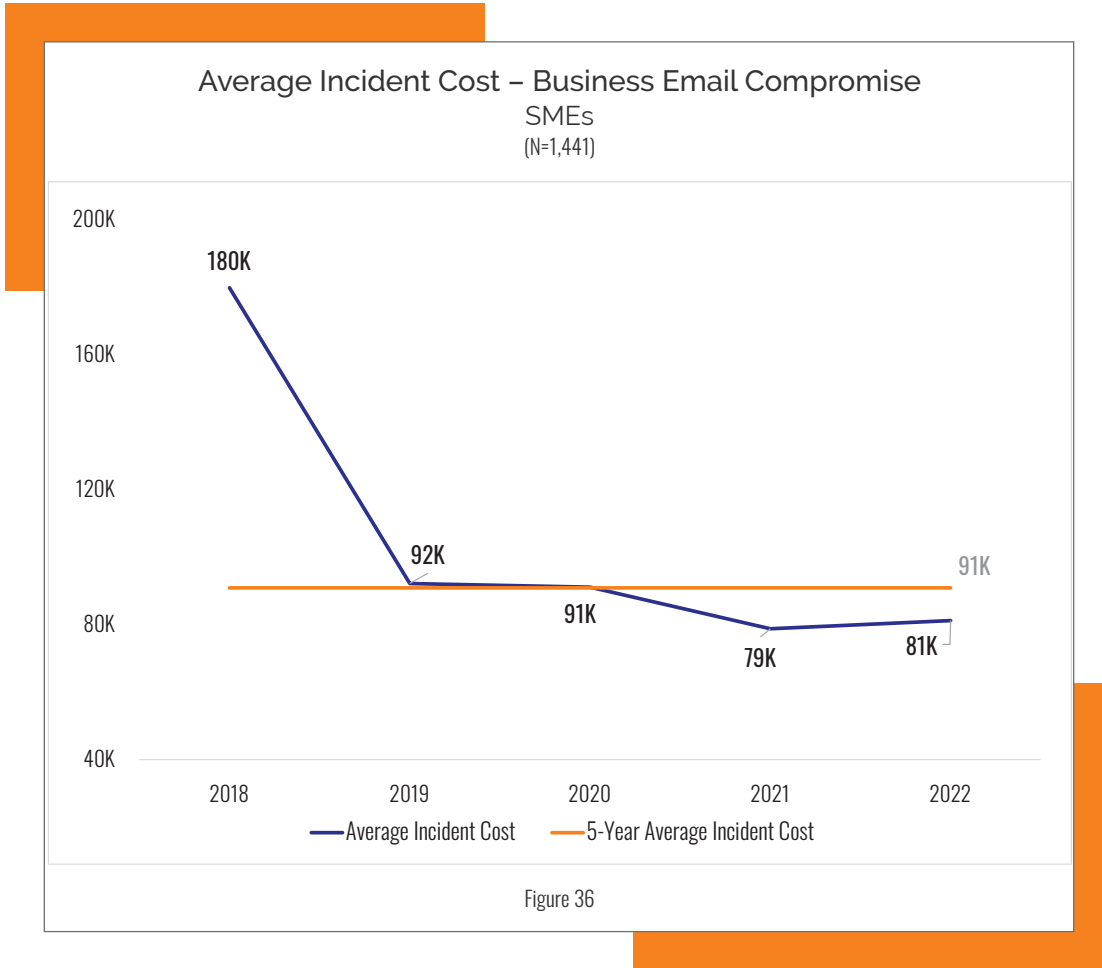


Figure 35

Business Email Compromise (BEC)

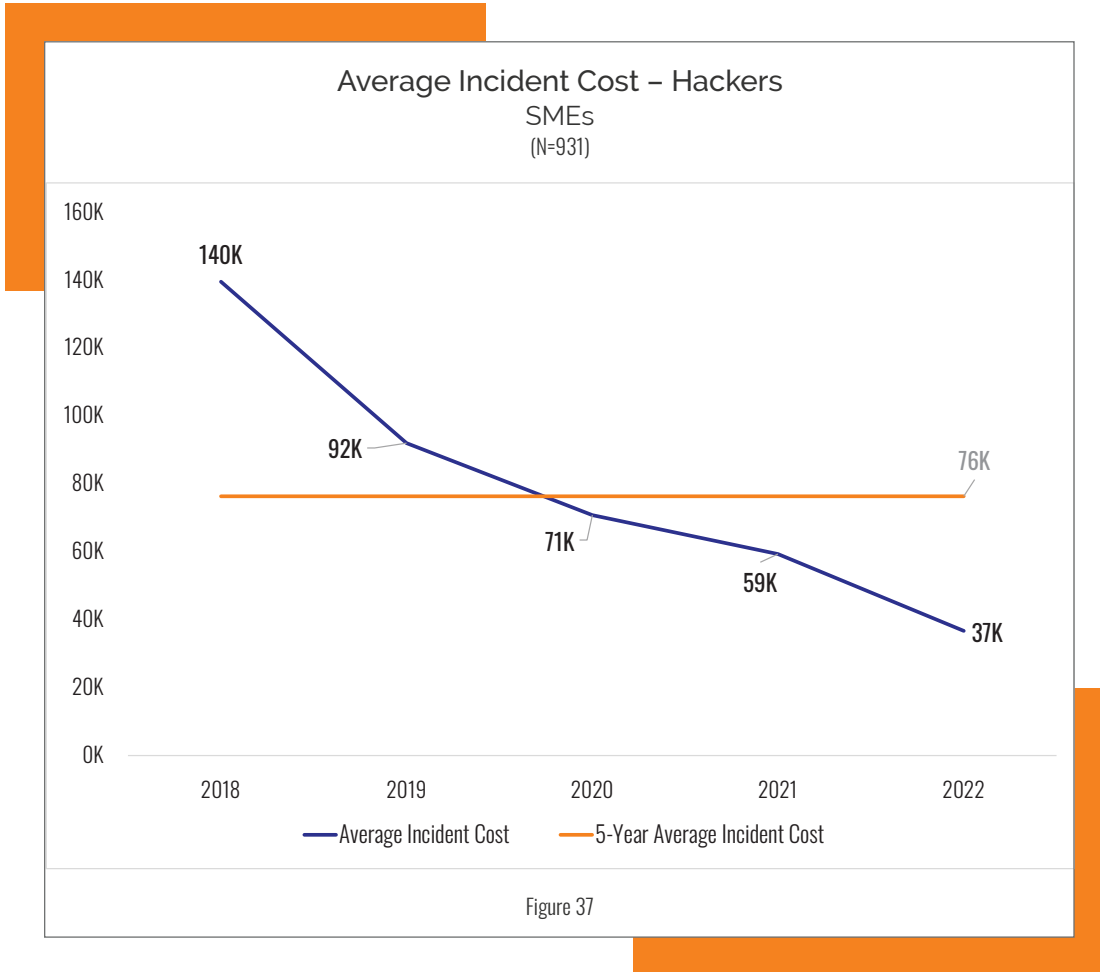
BEC was the second leading cause of loss at SMEs. The number of BEC claims increased from 74 in 2018 to almost 383 in 2021 and 257 so far in 2022. As is the case with ransomware (noted above), the number of BEC claims collected for 2022 will increase over the next two years.

The cost of BEC incidents has been dropping over the past five-years, from a high of \$180K in 2018 to \$81K in 2022.



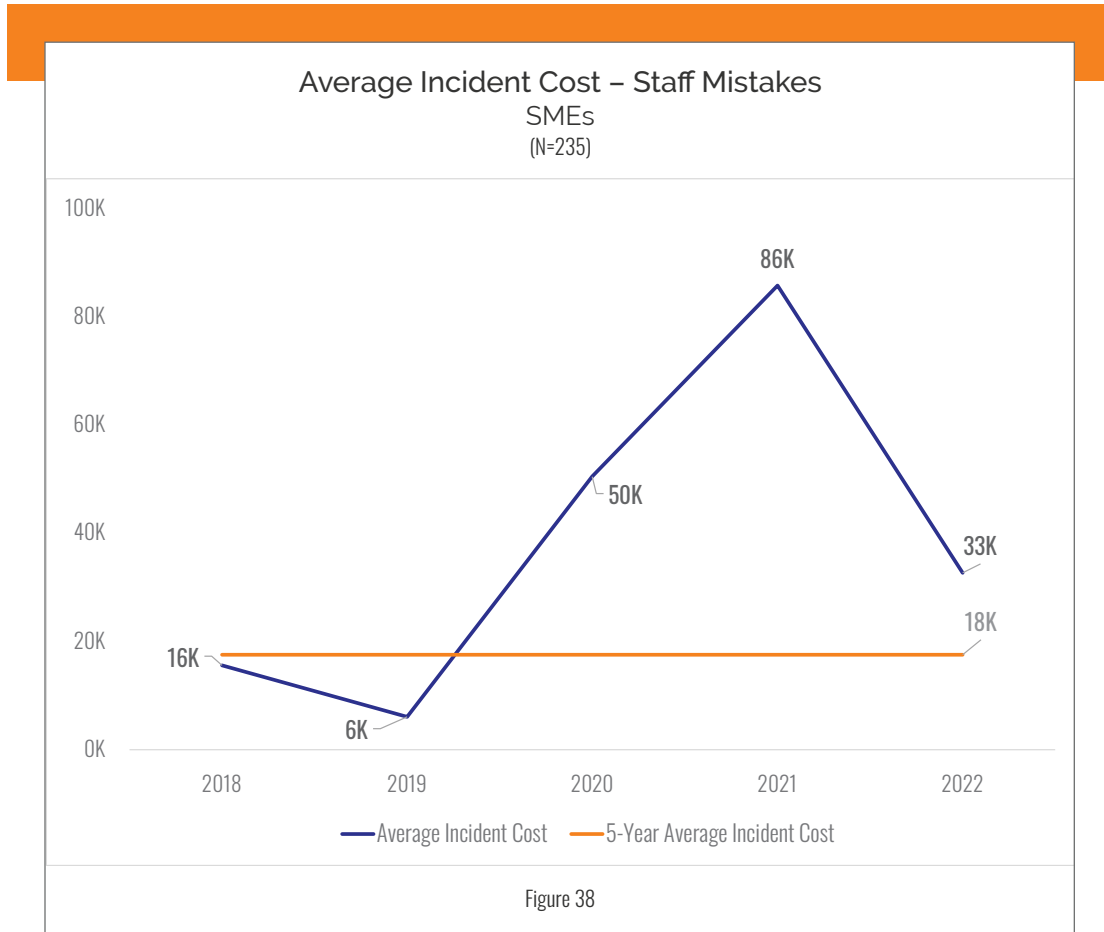
Hackers

Hackers were the third leading cause of loss at SMEs. Figure 37 tells the story. The good news here is that, based upon the five-year data, the average cost of a hacking incident has dropped since 2018 and has remained low since then.



Staff Mistakes

Staff mistakes and programming errors were still a notable cause of loss at SMEs - fortunately, not a very expensive one, as the figure below shows. The number of claims during the current five-year period (2018-2022) has decreased to 235 from 281 in last year's report.

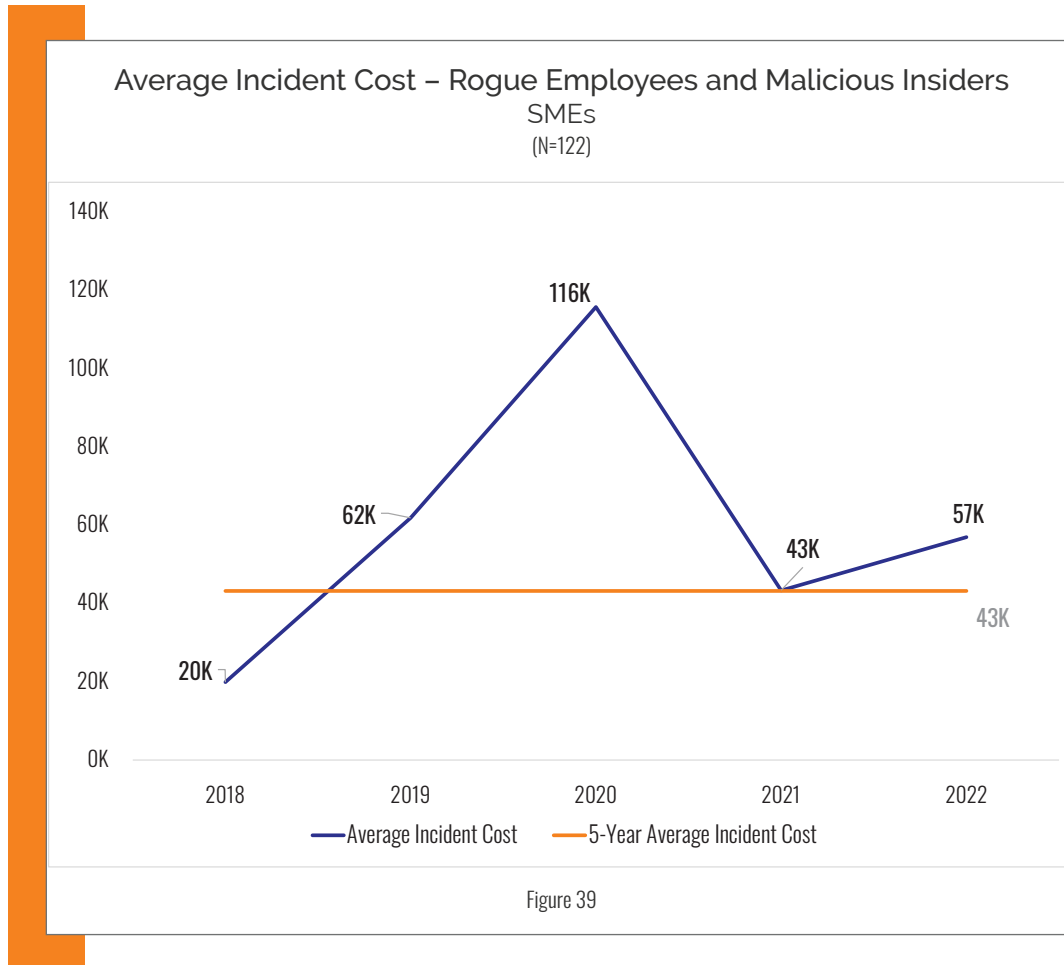


Human error will always play a significant role in data breaches. Mistakes don't take breaks. But preparedness before a breach and quick response after the inevitability of breach is how we keep the resulting chaos in check.

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

Rogue Employees

Over the past five years, much progress has been made at SMEs in dealing with malicious employees, ex-employees, and malicious insiders. From an average incident cost of \$116K in 2020, the numbers have dropped quite a bit. We will look again next year to see if this trend continues.



Insider threats have been an ongoing issue in cyber for many years. In most recent months, we have seen examples on the dark web for postings to hire a "malicious" employee into a company, with the end purpose to infiltrate and steal confidential information.

Ken Stasiak, Principal, RSM

Third-Party Incidents

Third-party incidents caused by both malicious and non-malicious actors remain a notable cause of loss. Since 2019, the cost of a malicious third-party event has been much greater than a non-malicious one. As Figure 40 below shows, except for 2020, the average cost of an incident caused by a non-malicious actor

is low. Unfortunately, the cost of an incident caused by a malicious third party has been increasing since 2019, and dramatically so in 2020 and 2021. As we have explained several times above, the low numbers in 2022 are almost certainly due to the small number of claims collected so far.

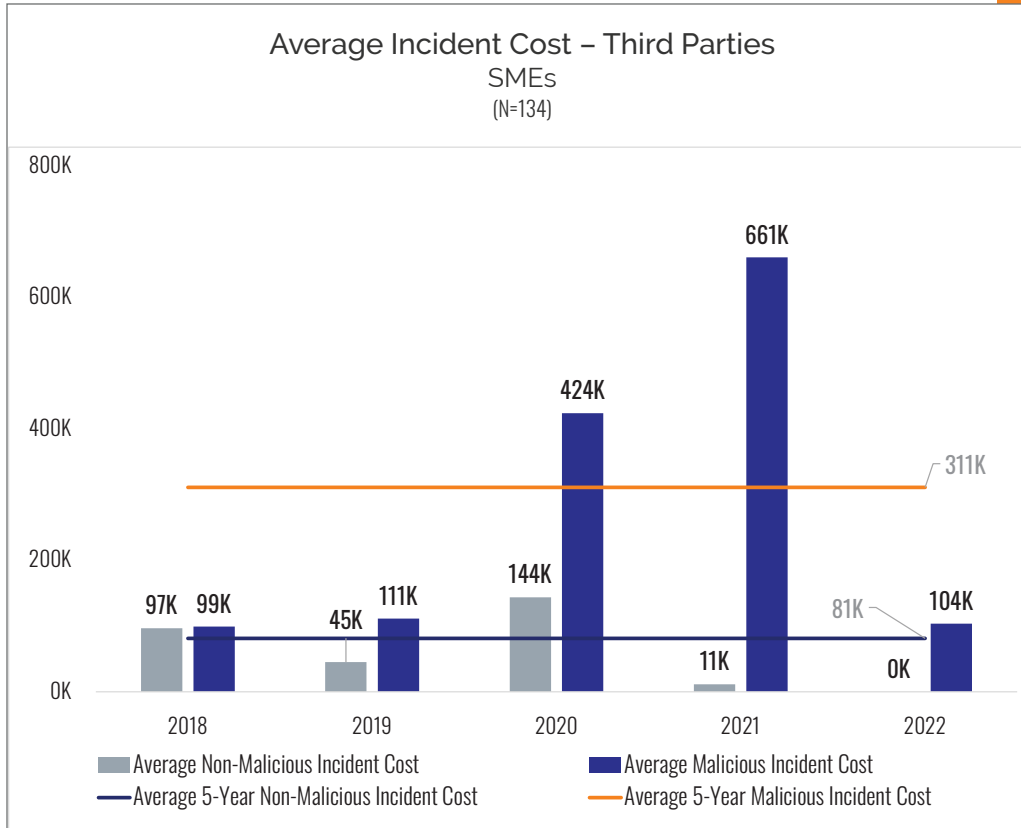


Figure 40

Third-party breaches are uninvited guests crashing through back doors. They slip through weak points, showing us the tight walk between staying safe and moving forward. This is why quick response matters.

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

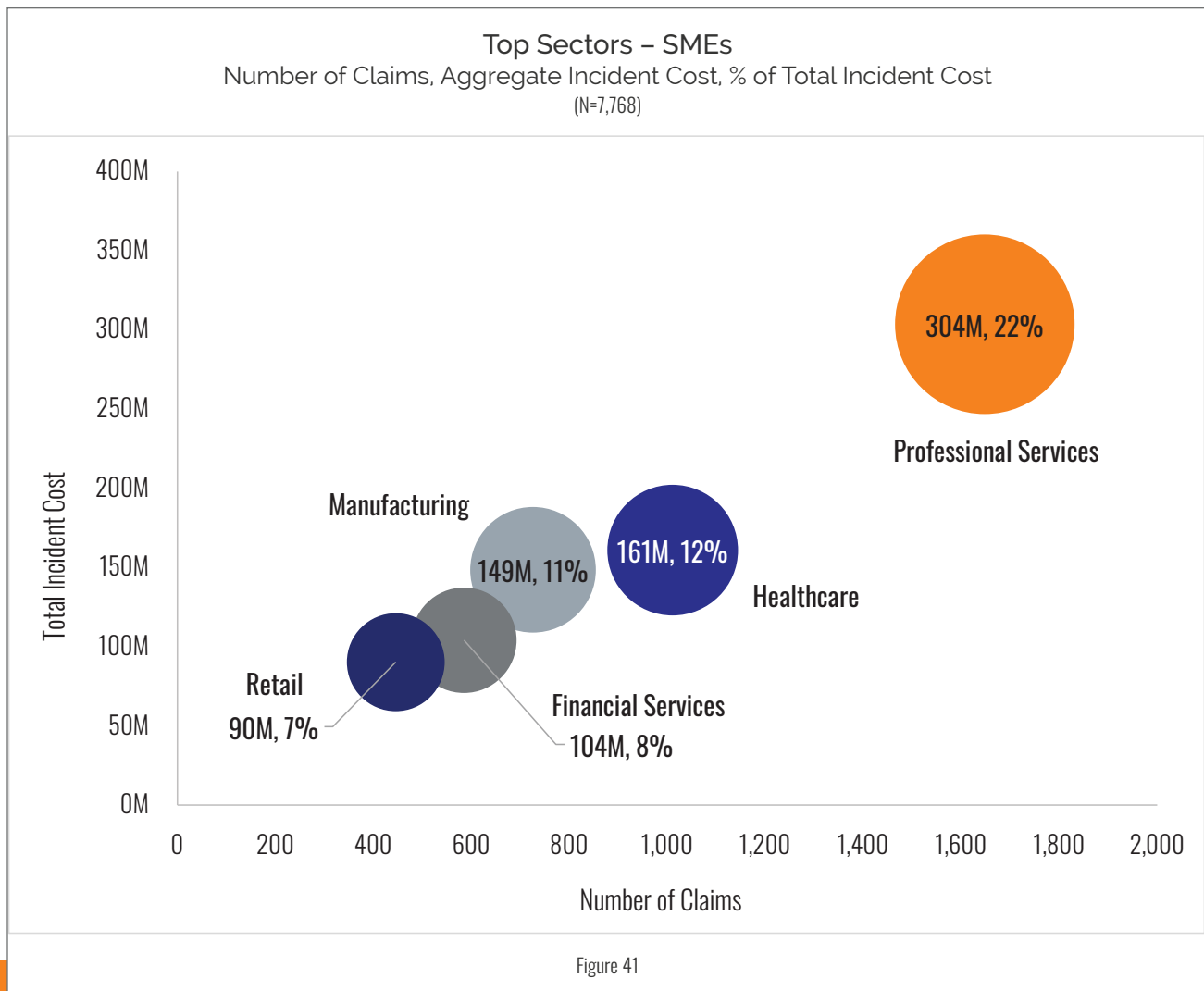
Sectors

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 57% of all claims and 60% of total incident costs 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 a look at 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.



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 about the same as in last year's report: \$51M and \$1.5B, respectively.

Professional services claims accounted for 21% of all claims and 22% of total incident costs at SMEs. Total incident costs ranged from \$1K to almost \$9M. The top causes of loss were the same as in last year's report: ransomware, BEC, and hackers.

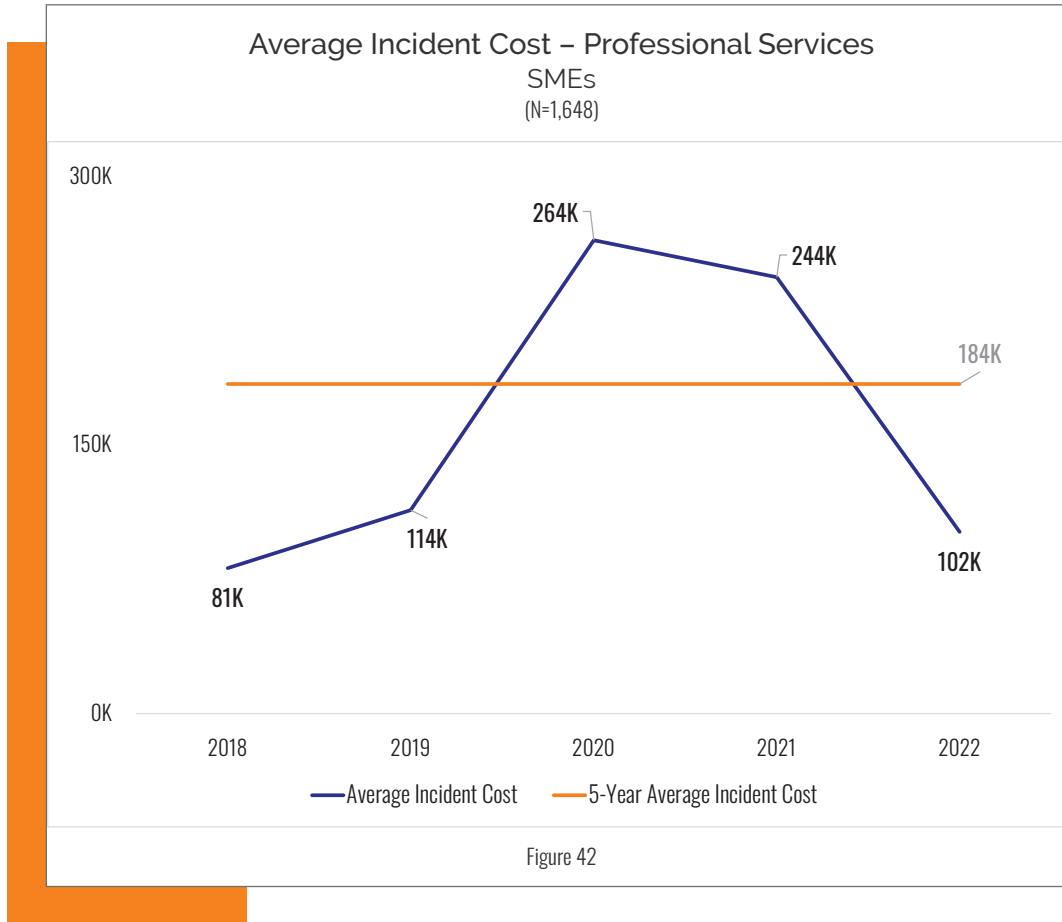


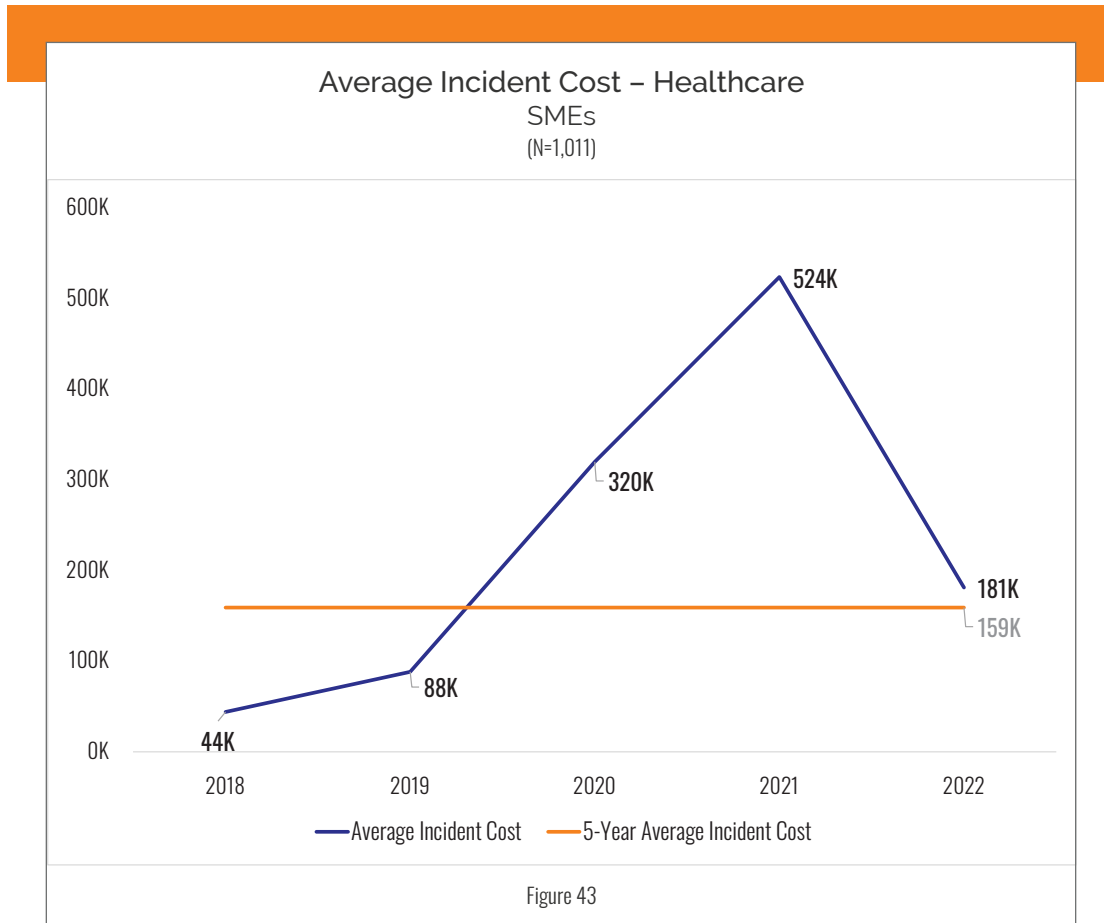
Figure 42 shows the year-over-year and five-year average incident cost for this sector.

Healthcare

The average annual revenue of organizations in the healthcare sector was \$99M (maximum=\$1.95B).

Healthcare claims accounted for 13% of all claims and 12% of incident costs at SMEs. Total incident costs ranged from \$1K to over \$17M. The top causes of loss were ransomware, BEC, and hackers – no change from last year.

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



The 2023 Cyber Claims Study found the average cost of third-party incidents to be increasing, and healthcare to be one of the most affected sectors. These two findings, when combined, reflect the reality that healthcare organizations require a disproportionately higher number of vendors to provide their various services. Proper management of liability through vendor contracts may reduce these costs.

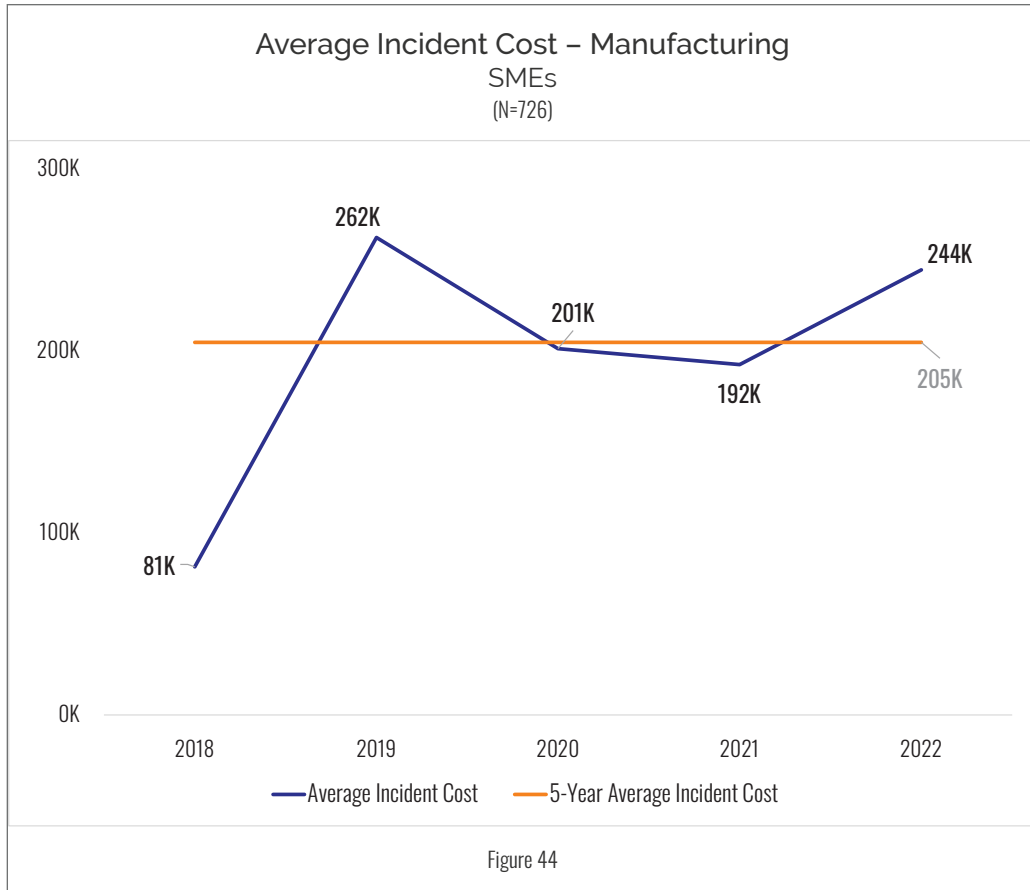
Lindsay B. Nickle, Partner & Vice-Chair, Constangy Cyber Team

Manufacturing

The average annual revenue of organizations in the manufacturing sector was \$115M (maximum=\$1.8B).

Manufacturing claims accounted for 9% of all claims and 11% of incident costs at SMEs. Total incident costs ranged from \$1K to \$7M. The top causes of loss were ransomware, BEC, and hackers.

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

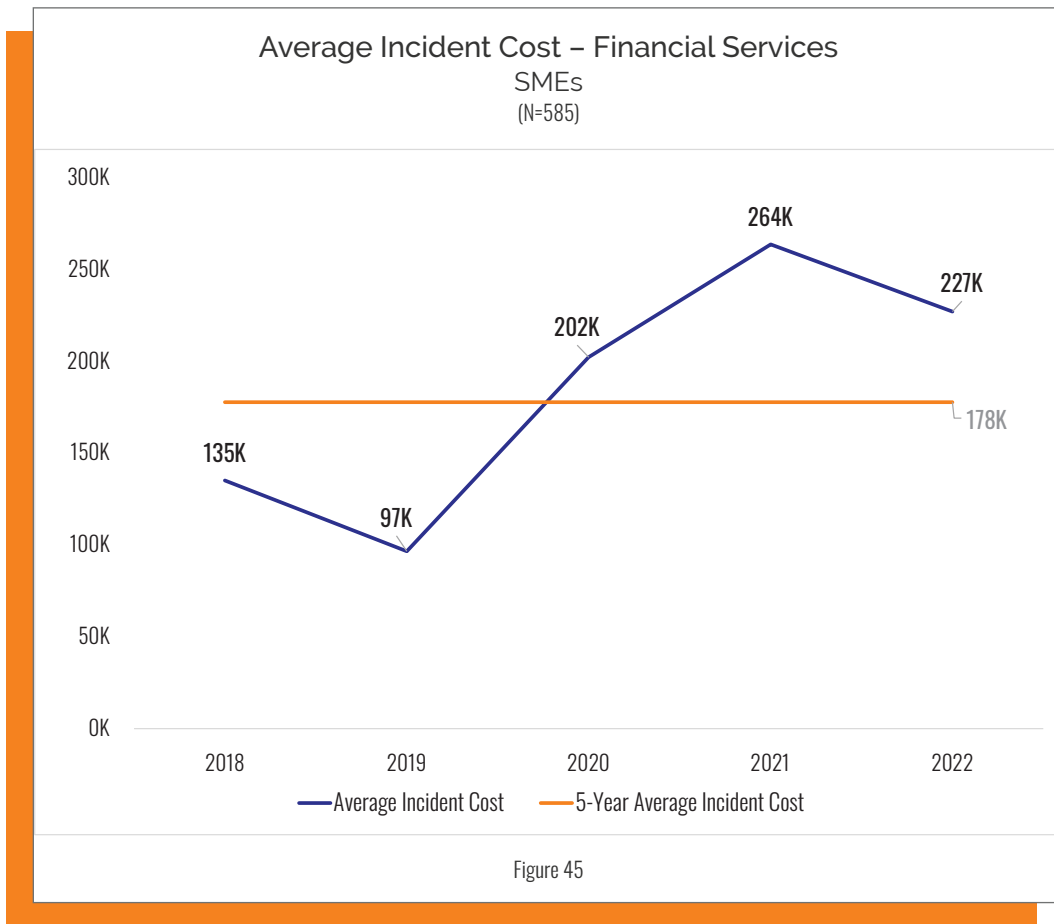


Financial Services

The average annual revenue of organizations in the financial services sector was \$88M (maximum=\$1.4B).

Financial services claims accounted for 8% of all claims and 8% of incident costs at SMEs. Total incident costs ranged from \$1K to \$4.7M. The top causes of loss were unchanged from last year: BEC, ransomware, and hackers.

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

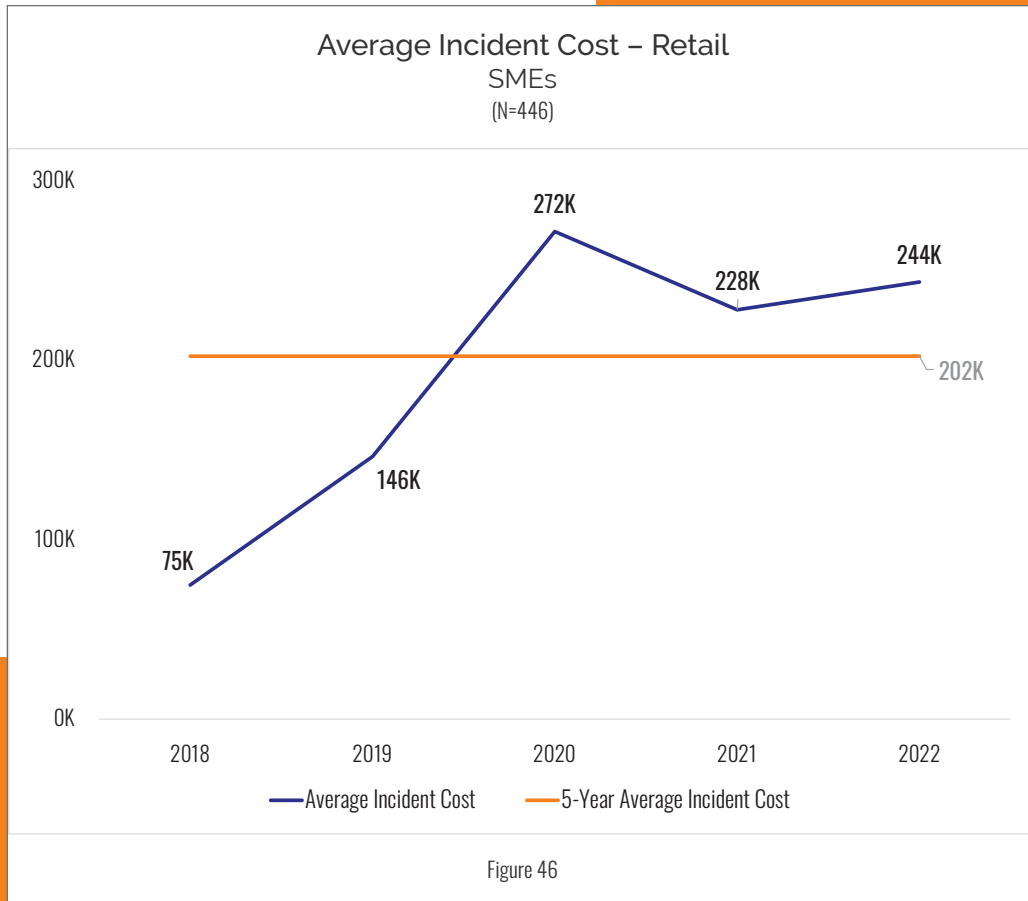


Retail

The average annual revenue of organizations in the retail sector was \$107M (maximum=\$1.6B).

Retail claims accounted for 6% of all claims and 7% of incident costs at SMEs. Total incident costs ranged from \$1K to \$7.5M. The three top causes of loss were ransomware, BEC, and hackers.

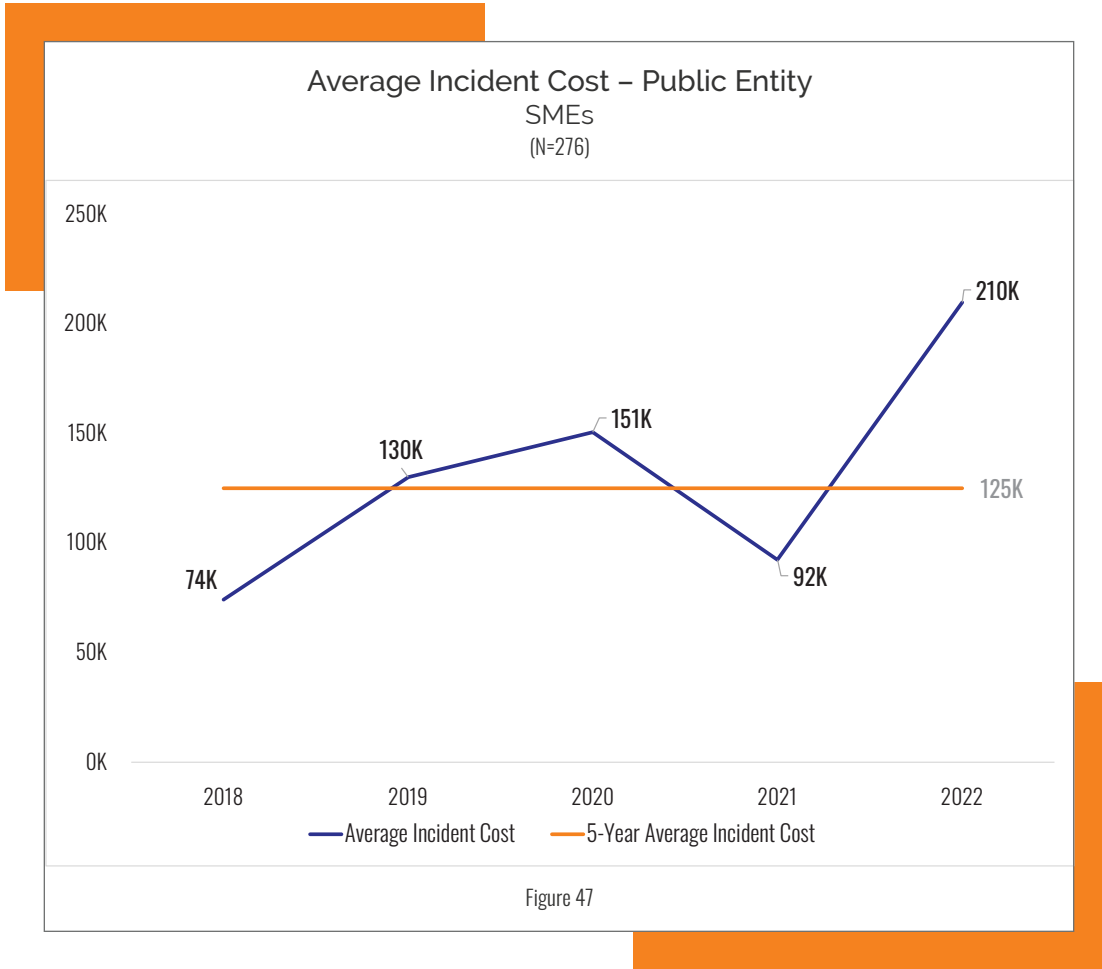
Figure 46 shows the year-over-year and five-year average incident cost for this sector.



Public Entities

The average annual revenue for public entities was \$83M (maximum=\$883M). Claims from public entities represent about 4% of all claims and 3% of total incident cost.

Average incident costs have gone up and down since 2018, with an upward trajectory in 2022. Top causes of loss were ransomware, BEC, and malware/virus.



Claims from Canada

Although there was a relatively small number of claims for incidents in Canada (2% of total submissions), these incidents represent an important subset of the dataset.

The average annual revenue of a Canadian organization in this study was 302M USD (maximum=5.0B USD).

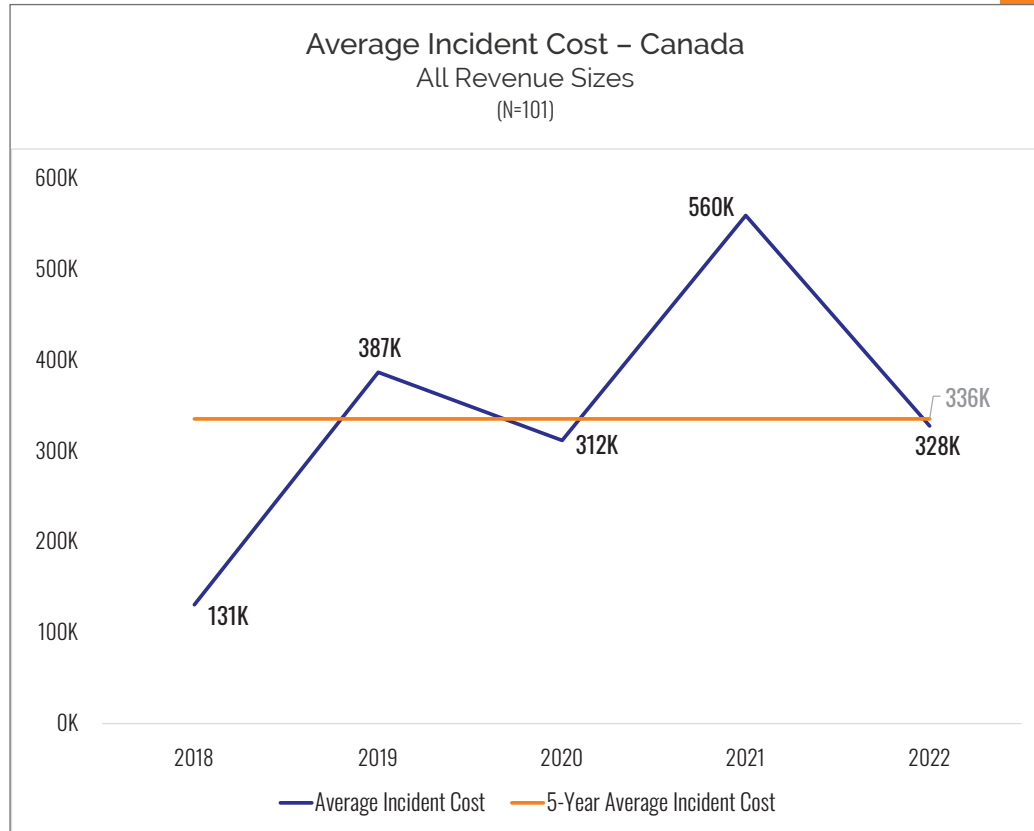


Figure 48

Ransomware continues to be one of top cyber threats to Canadian businesses, more so to the small and mid-size businesses. We are also seeing a shift in the execution of this attack, as attackers are prioritizing stealing sensitive information and then following up with the ransomware attack.

Tushar Kapoor, Director Security and Privacy, RSM Canada

Canada
Top Causes of Loss 2018-2022

Cause of Loss	Claims	Average Incident Cost
Ransomware	40	596K
Business Email Compromise	20	173K
Hacker	14	117K
Staff Mistake	8	43K
Malware/Virus	5	52K
Wire Transfer Fraud	5	615K

Table 2

Conclusion

For thirteen 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 4,000 claims. The result has been a comprehensive dataset of cyber claims incidents, including their causes and monetary impacts.

As more and more insurers and brokers have participated in this study and have shared even

more claims and more information about each claim, the value of the study has continued to increase. For the benefit of the industry overall, all underwriters are encouraged to participate in next year's NetDiligence Cyber Claims 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 2023 study.

At-Bay

Allied World

Association of Washington Cities

AXA XL

Beazley

Berkley Cyber Risk Solutions

CFC

CNA

Crum & Forster

Great American Insurance

Hiscox

Intact Insurance

Liberty Mutual

Markel

Sompo International

Tokio Marine HCC

Travelers - US

Travelers - Canada

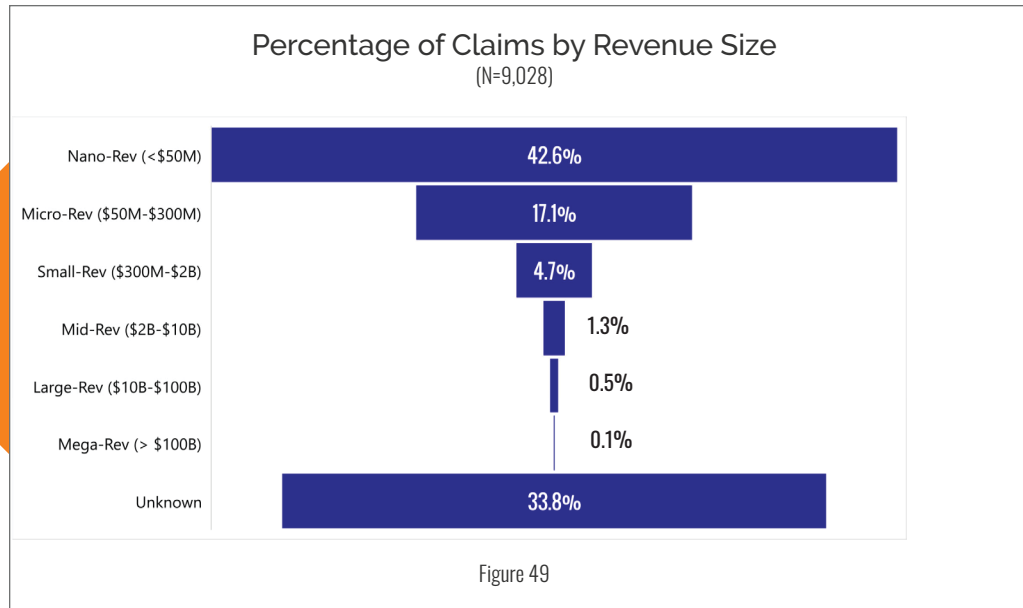
Insurers: We invite you to join this elite group of participating companies. We'll be starting next year's study in January. Contact us at cyberclaims@netdiligence.com.

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, plus crisis services costs and total incident cost.

As was mentioned previously, SMEs (companies with annual revenue less than \$2B) account for 98% of the claims analyzed and 46% of total incident cost. Large companies (companies with annual revenue greater than \$2B) account for only 2% of the claims analyzed but 54% of total incident cost.



Incident Cost by Revenue Size
Claims >= \$1K
2018-2022

Revenue Size	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Nano-Rev (<\$50M)	3,647	1K	124K	5.2M	452.8M	20%	1	6
Micro-Rev (\$50M-\$300M)	1,430	1K	294K	11.4M	420.5M	19%	3	5
Small-Rev (\$300M-\$2B)	365	3K	995K	17.6M	363.3M	16%	4	4
Mid-Rev (\$2B-\$10B)	95	1K	3.8M	60.0M	362.3M	16%	5	3
Large-Rev (\$10B-\$100B)	34	18K	12.6M	65.8M	428.3M	19%	6	2
Mega-Rev (>\$100B)	3	10.6M	35.2M	55.0M	105.6M	5%	7	1
Unknown	2,326	1K	53K	2.3M	123.6M	5%	2	7

Table 3

Average Crisis Services Costs by Revenue Size
Claims >= \$1K
2018-2022

Revenue Size	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Nano-Rev (<\$50M)	43K	5K	31K	17K	73K	80K	6
Micro-Rev (\$50M-\$300M)	77K	16K	37K	25K	135K	161K	5
Small-Rev (\$300M-\$2B)	197K	96K	156K	85K	179K	382K	4
Mid-Rev (\$2B-\$10B)	273K	21K	1.0M	53K	730K	863K	3
Large-Rev (\$10B-\$100B)	5.6M	10.0M	647K	2.4M	923K	5.6M	1
Mega-Rev (>\$100B)	0K	0K	0K	0K	0K	4.9M	2
Unknown	39K	5K	9K	10K	112K	37K	7

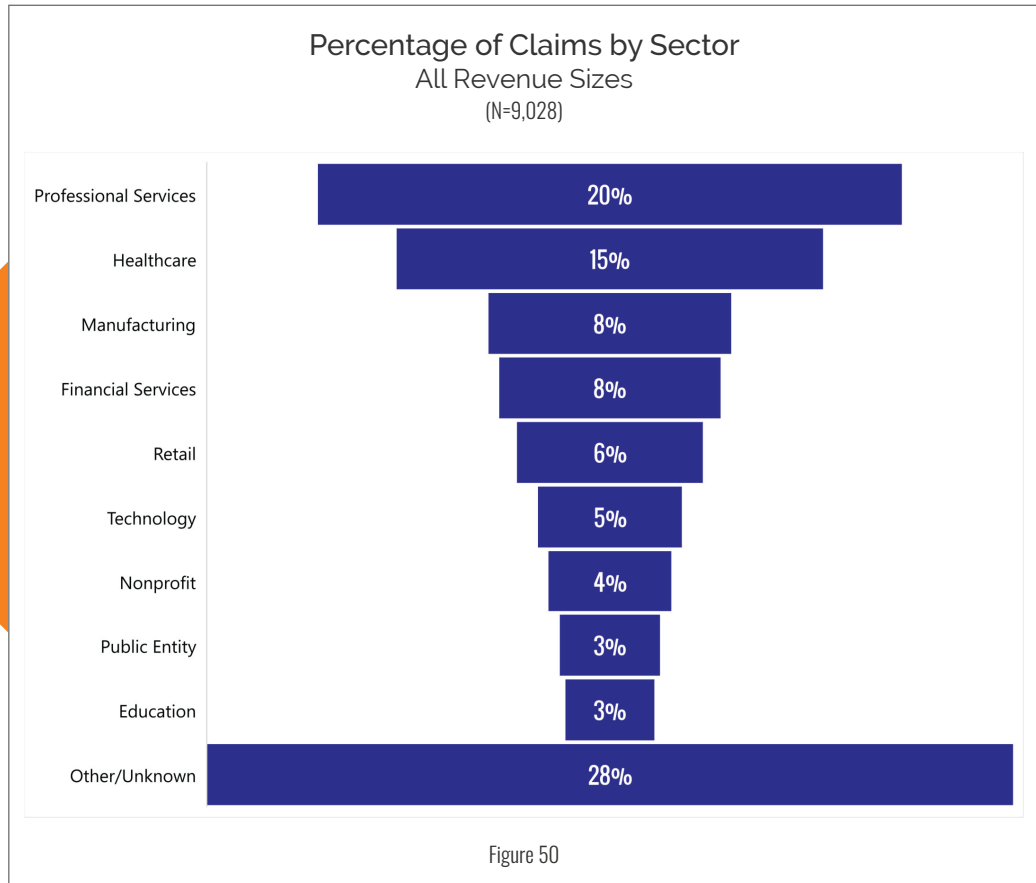
Table 4

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
- Other
- Professional Services
- Public Entity
- Restaurant
- Retail
- Technology
- Telecommunications
- Transportation

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



Incident Cost by Sector – SMEs 2018-2022								
Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Education	236	2K	126K	2.0M	29.7M	2.2%	10	16
Energy	31	13K	651K	15.0M	20.2M	1.5%	15	1
Entertainment	37	4K	215K	2.6M	7.9M	0.6%	14	7
Financial Services	585	1K	178K	4.7M	104.0M	7.6%	5	11
Gaming & Casino	4	20K	160K	532K	639K	0.0%	18	13
Healthcare	1,011	1K	159K	17.6M	160.9M	11.8%	3	14
Hospitality	113	2K	158K	2.6M	17.9M	1.3%	12	15
Manufacturing	726	1K	205K	7.2M	148.5M	10.9%	4	8
Media	43	8K	336K	4.2M	14.5M	1.1%	13	4
Nonprofit	342	1K	100K	2.9M	34.3M	2.5%	8	18
Other	1,732	1K	70K	4.9M	121.4M	8.9%	1	19
Professional Services	1,648	1K	184K	8.9M	303.5M	22.3%	2	10
Public Entity	276	2K	125K	2.3M	34.5M	2.5%	9	17
Restaurant	25	2K	298K	5.2M	7.4M	0.5%	17	5
Retail	446	1K	202K	7.5M	90.2M	6.6%	6	9
Technology	366	1K	601K	17.6M	219.8M	16.2%	7	2
Telecommunications	26	18K	369K	5.0M	9.6M	0.7%	16	3
Transportation	120	1K	292K	6.1M	35.0M	2.6%	11	6
Unknown	1	168K	168K	168K	168K	0.0%	19	12

Table 5

Average Crisis Services Costs by Sector – SMEs
2018-2022

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Education	65K	6K	13K	18K	103K	97K	10
Energy	184K	1K	3K	43K	117K	230K	2
Entertainment	36K	10K	34K	23K	34K	54K	18
Financial Services	61K	47K	53K	23K	104K	114K	6
Gaming & Casino	47K	0K	0K	3K	3K	51K	19
Healthcare	62K	9K	106K	17K	97K	91K	11
Hospitality	47K	3K	13K	14K	82K	88K	12
Manufacturing	54K	3K	8K	21K	88K	106K	9
Media	44K	1K	3K	18K	160K	129K	5
Nonprofit	55K	5K	13K	19K	70K	78K	14
Other	48K	2K	6K	14K	85K	78K	15
Professional Services	54K	4K	29K	22K	123K	110K	7
Public Entity	55K	20K	10K	20K	140K	107K	8
Restaurant	39K	9K	56K	16K	85K	71K	16
Retail	53K	1K	40K	22K	59K	85K	13
Technology	93K	8K	18K	38K	84K	182K	4
Telecommunications	42K	201K	348K	37K	72K	251K	1
Transportation	65K	6K	5K	44K	154K	213K	3
Unknown	0K	0K	44K	25K	0K	68K	17

Table 6

Incident Cost by Sector – Large Companies 2018-2022								
Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Agriculture	1	5.0M	5.0M	5.0M	5.0M	0.3%	11	9
Education	5	58K	742K	2.4M	3.7M	0.3%	8	13
Energy	1	5.0M	5.0M	5.0M	5.0M	0.3%	11	10
Financial Services	26	2K	22.0M	350.0M	572.7M	39.4%	1	2
Healthcare	20	5K	10.9M	60.0M	218.7M	15.1%	2	5
Hospitality	4	1.4M	15.4M	40.0M	61.4M	4.2%	9	3
Manufacturing	15	29K	10.6M	55.0M	159.2M	11.0%	5	6
Other	20	18K	5.7M	65.8M	113.4M	7.8%	2	8
Professional Services	8	139K	3.3M	13.2M	26.7M	1.8%	7	11
Public Entity	1	2.5M	2.5M	2.5M	2.5M	0.2%	11	12
Retail	11	1K	14.9M	111.0M	164.0M	11.3%	6	4
Technology	19	46K	6.3M	60.0M	120.4M	8.3%	4	7
Telecommunications	1	425.0M	425.0M	425.0M	425.0M	29.3%	11	1
Transportation	4	200K	370K	598K	1.5M	0.1%	9	14

Table 7

Average Crisis Services Costs by Sector – Large Companies 2018-2022							
Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Education	172K	31K	108K	50K	123K	299K	10
Financial Services	7.5M	0K	0K	24K	0K	2.0M	6
Healthcare	145K	0K	988K	65K	501K	622K	9
Hospitality	0K	10.0M	0K	0K	0K	10.0M	1
Manufacturing	452K	14K	5K	783K	28K	1.9M	7
Other	310K	39K	2.3M	131K	52K	2.3M	5
Professional Services	139K	0K	0K	0K	75K	3.4M	2
Public Entity	1.1M	0K	647K	84K	2K	1.8M	8
Retail	335K	0K	14K	3.0M	1.3M	2.5M	4
Technology	3.0M	0K	0K	30K	3.5M	2.5M	3
Transportation	0K	0K	0K	0K	100K	100K	11

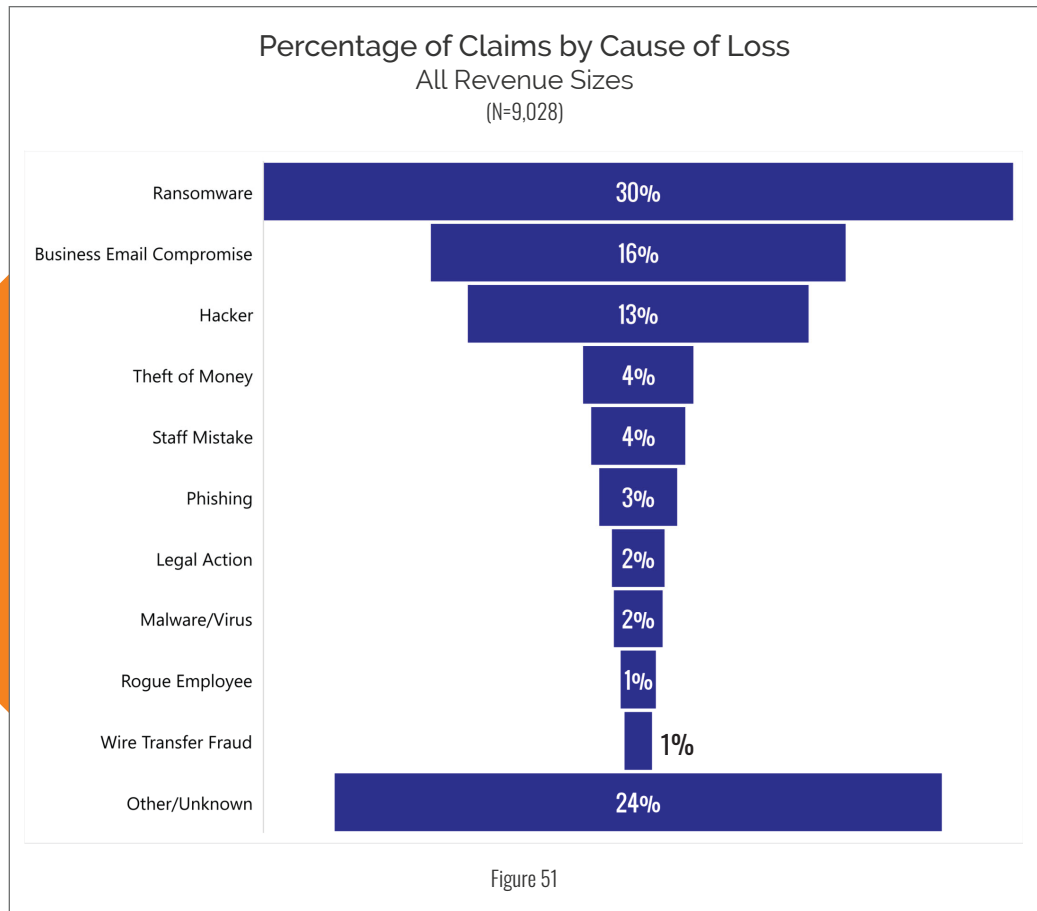
Table 8

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
- Other
- 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
- Unknown
- Wire Transfer Fraud
- Wrongful Data Collection

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



Incident Cost by Cause of Loss – SMEs 2018-2022								
Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	1,441	1K	91K	3.4M	131.0M	9.6%	2	13
Hacker	931	1K	76K	7.5M	71.1M	5.2%	3	15
Legal Action	52	2K	152K	4.2M	7.9M	0.6%	14	11
Lost/Stolen Laptop/Device	90	1K	26K	356K	2.3M	0.2%	13	21
Malware/Virus	167	2K	86K	1.0M	14.3M	1.1%	10	14
Negligence	1	450K	450K	450K	450K	0.0%	23	2
Other	710	1K	172K	8.9M	122.3M	9.0%	4	8
Paper Records	17	1K	12K	57K	208K	0.0%	16	23
Phishing	203	1K	60K	401K	12.2M	0.9%	9	17
Privacy Breach	19	1K	177K	1.9M	3.4M	0.2%	15	7
Programming Error	10	4K	153K	515K	1.5M	0.1%	19	10
Ransomware	2,556	1K	334K	17.6M	854.0M	62.8%	1	4
Rogue Employee	111	1K	32K	403K	3.6M	0.3%	11	19
Social Engineering	4	11K	167K	383K	666K	0.0%	20	9
Staff Mistake	216	1K	11K	157K	2.3M	0.2%	8	24
System Glitch	13	4K	215K	933K	2.8M	0.2%	17	6
Theft of Money	319	1K	53K	1.1M	17.0M	1.2%	6	18
Third-Party	1	31K	31K	31K	31K	0.0%	23	20
Trademark/Copyright Infringement	3	111K	1.5M	4.1M	4.6M	0.3%	21	1
Unauthorized Access	2	9K	14K	20K	29K	0.0%	22	22
Wire Transfer Fraud	94	3K	279K	1.9M	26.2M	1.9%	12	5
Wrongful Data Collection	11	5K	335K	2.0M	3.7M	0.3%	18	3
Cyber Event - unspecified	572	1K	108K	2.4M	62.0M	4.6%	5	12
Unknown	225	1K	74K	1.7M	16.6M	1.2%	7	16

Table 9

Average Crisis Services Costs by Cause of Loss – SMEs
2018-2022

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	34K	8K	15K	22K	55K	64K	6
Hacker	46K	6K	47K	26K	12K	70K	4
Legal Action	10K	5K	6K	21K	130K	41K	10
Lost/Stolen Laptop/Device	21K	1K	1K	6K	25K	13K	16
Malware/Virus	27K	1K	57K	11K	80K	53K	8
Negligence	0K	0K	0K	0K	0K	0K	N/A
Other	28K	10K	18K	13K	29K	34K	12
Paper Records	0K	0K	5K	6K	0K	9K	18
Phishing	30K	4K	14K	15K	0K	43K	9
Privacy Breach	17K	2K	1K	5K	0K	17K	15
Programming Error	29K	0K	0K	5K	3K	26K	14
Ransomware	80K	32K	66K	26K	143K	186K	2
Rogue Employee	50K	1K	6K	9K	93K	27K	13
Social Engineering	9K	0K	1K	4K	102K	83K	3
Staff Mistake	9K	6K	4K	4K	5K	5K	19
System Glitch	61K	14K	11K	37K	45K	68K	5
Theft of Money	31K	1K	9K	12K	53K	40K	11
Unauthorized Access	0K	0K	0K	0K	0K	0K	N/A
Wire Transfer Fraud	0K	0K	0K	0K	0K	0K	N/A
Wrongful Data Collection	1K	0K	0K	8K	0K	9K	17
Cyber Event - unspecified	18K	2K	0K	21K	73K	56K	7
Unknown	33K	0K	0K	28K	32K	197K	1

Table 10

Incident Cost by Cause of Loss – Large Companies
2018-2022

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	14	18K	338K	1.4M	4.7M	0.3%	3	10
Hacker	14	55K	41.8M	350.0M	585.3M	31.1%	3	1
Lost/Stolen Laptop/Device	1	32K	32K	32K	32K	0.0%	11	12
Malware/Virus	4	54K	1.6M	5.7M	6.3M	0.3%	6	6
Other	10	22K	872K	4.7M	8.7M	0.5%	5	7
Paper Records	1	5K	5K	5K	5K	0.0%	11	14
Phishing	1	179K	179K	179K	179K	0.0%	11	11
Programming Error	1	2.5M	2.5M	2.5M	2.5M	0.1%	11	5
Ransomware	65	1K	19.1M	425.0M	1.2B	66.2%	1	2
Rogue Employee	2	55K	6.6M	13.2M	13.2M	0.7%	7	3
Staff Mistake	17	2K	19K	250K	325K	0.0%	2	13
Wire Transfer Fraud	2	125K	838K	1.6M	1.7M	0.1%	7	8
Wrongful Data Collection	2	249K	5.6M	11.0M	11.2M	0.6%	7	4
Unknown	2	32K	739K	1.4M	1.5M	0.1%	7	9

Table 11

Average Crisis Services Costs by Cause of Loss – Large Companies
2018-2022

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	93K	39K	9K	71K	645K	336K	7
Hacker	4.0M	10.0M	4.6M	224K	313K	4.4M	2
Lost/Stolen Laptop/Device	19K	0K	0K	13K	0K	32K	10
Malware/Virus	312K	0K	4.5M	162K	83K	1.5M	5
Other	0K	0K	1.0M	21K	38K	543K	6
Programming Error	1.1M	0K	647K	84K	2K	1.8M	4
Ransomware	2.2M	23K	38K	917K	1.3M	3.3M	3
Rogue Employee	9K	0K	13K	33K	0K	5.0M	1
Staff Mistake	0K	0K	0K	5K	0K	5K	12
Wire Transfer Fraud	0K	0K	0K	0K	75K	75K	9
Wrongful Data Collection	0K	0K	0K	199K	0K	199K	8
Unknown	0K	0K	0K	0K	7K	7K	11

Table 12

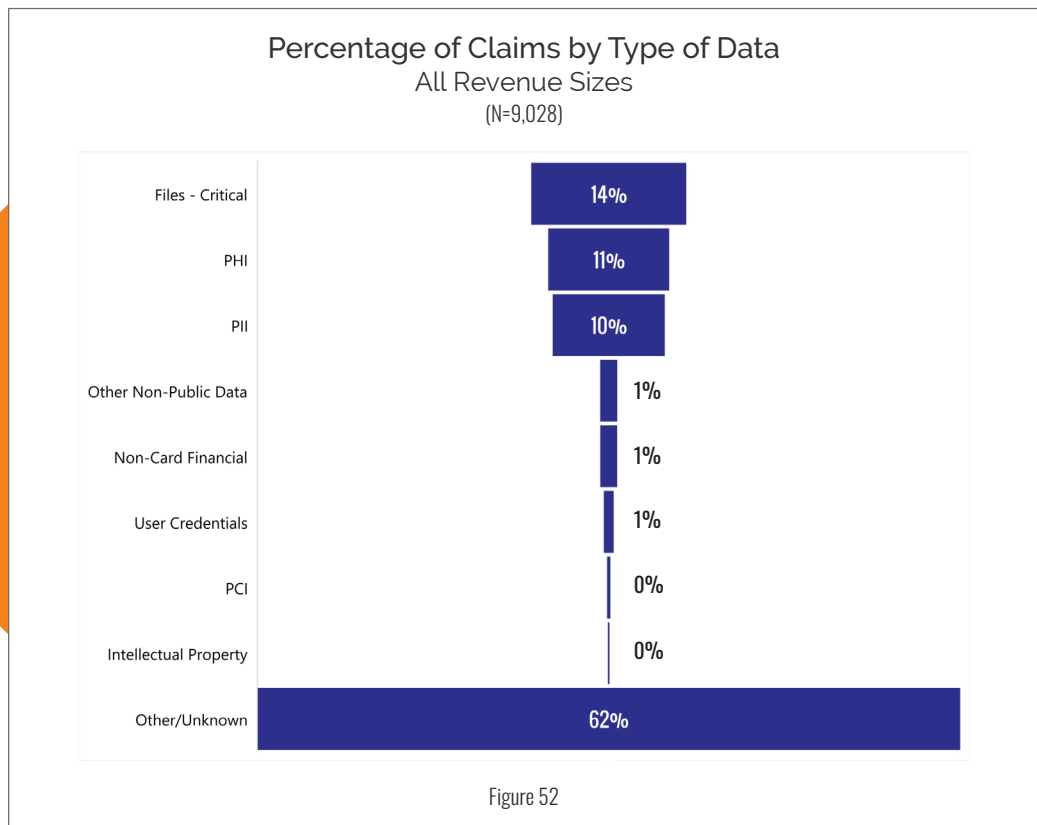
Type of Data

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

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

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.



Incident Cost by Type of Data – SMEs 2018-2022								
Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Files - Critical	1,173	1K	205K	7.4M	239.9M	17.6%	2	10
Intellectual Property	7	3K	768K	4.1M	5.4M	0.4%	12	3
N/A	183	2K	130K	1.9M	23.9M	1.8%	5	11
Non-Card Financial	121	2K	274K	4.7M	33.1M	2.4%	6	6
Other	30	6K	1.1M	17.6M	33.0M	2.4%	9	1
Other Non-Public Data	106	1K	607K	10.4M	64.3M	4.7%	7	4
PCI	24	1K	252K	2.3M	6.0M	0.4%	10	8
PHI	669	1K	206K	17.6M	137.6M	10.1%	4	9
PII	745	1K	347K	15.0M	258.8M	19.0%	3	5
Trade Secrets	3	250K	972K	2.1M	2.9M	0.2%	13	2
User Credentials	56	1K	268K	3.9M	15.0M	1.1%	8	7
Email - unspecified	21	3K	71K	0.2M	1.5M	0.1%	11	13
Unknown	4,630	1K	116K	8.9M	538.6M	39.6%	1	12

Table 13

Average Crisis Services Costs by Type of Data – SMEs 2018-2022							
Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Files - Critical	54K	6K	31K	15K	67K	90K	10
Intellectual Property	159K	0K	0K	7K	521K	175K	4
N/A	19K	2K	3K	9K	59K	51K	13
Non-Card Financial	86K	397K	36K	37K	53K	130K	7
Other	169K	8K	1.5M	168K	199K	446K	1
Other Non-Public Data	140K	3K	17K	59K	52K	205K	3
PCI	96K	7K	21K	100K	25K	172K	5
PHI	83K	26K	128K	22K	93K	116K	8
PII	99K	13K	52K	34K	86K	166K	6
Trade Secrets	134K	0K	0K	109K	6K	236K	2
User Credentials	80K	6K	13K	27K	47K	95K	9
Email - unspecified	22K	0K	2K	17K	157K	52K	12
Unknown	45K	4K	13K	16K	110K	90K	11

Table 14

Incident Cost by Type of Data – Large Companies
2018-2022

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Files - Critical	7	58K	13.9M	55.0M	97.1M	5.2%	5	5
Intellectual Property	2	24K	640K	1.3M	1.3M	0.1%	9	10
N/A	5	32K	1.4M	5.0M	6.8M	0.4%	6	9
Non-Card Financial	3	103K	117.1M	350.0M	351.4M	18.7%	8	1
Other Non-Public Data	8	1K	1.8M	13.2M	14.6M	0.8%	4	8
PCI	2	25.0M	25.5M	26.0M	51.0M	2.7%	9	3
PHI	16	22K	11.2M	60.0M	178.6M	9.5%	3	6
PII	54	2K	17.2M	425.0M	926.8M	49.3%	1	4
User Credentials	5	77K	27.4M	111.0M	136.9M	7.3%	6	2

Table 15

Average Crisis Services Costs by Cause of Loss – Large Companies
2018-2022

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Files - Critical	278K	0K	0K	46K	13K	1.4M	6
Intellectual Property	1.1M	14K	0K	103K	0K	1.2M	7
Other Non-Public Data	150K	0K	0K	21K	1K	1.5M	5
PCI	15.0M	0K	0K	11K	0K	7.5M	1
PHI	45K	0K	1.0M	77K	526K	1.6M	4
PII	1.6M	3.3M	1.2M	370K	889K	2.2M	3
User Credentials	137K	0K	0K	133K	0K	269K	8
Unknown	2.3M	31K	55K	1.0M	1.2M	2,987K	2

Table 16

Generative Artificial Intelligence

Should Cyber Insurance Mitigate the Risk?

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

Artificial Intelligence, as reflected in various mathematical theorems, has existed as a concept for centuries. It was first referenced by the term Artificial Intelligence or "AI" in 1956 during a conference of scientists gathered to discuss how human intelligence could be automated through computer code. The conference fostered the development of a revolutionary computer program known to automate human reasoning: Logic Theorist. It ultimately proved numerous mathematical theorems in Principia Mathematica and identified shorter proofs for some of them.

Although certain mathematical theorems associated with economists, mathematicians, philosophers, and other intellectual leaders attracted societal attention through the ages, the 20th century experienced an extraordinary wave of excitement and accomplishment stemming from the concept now referenced as AI. As much as AI has been heralded as contributing to the advancement of agriculture, communication, education, entertainment, finance, healthcare, and transportation, the world has not experienced the type of excitement, or hype, that surrounds generative AI.

Generative AI is a type of AI that can generate new content. Generative AI uses deep learning algorithms, a type of machine learning, to analyze patterns and arrangements in large data sets. It utilizes this information to create new outputs that resemble, in form and structure, the analyzed data sets. Generative AI products primarily pertain to audio, code, design, images, music, text, and video, and have substantial use cases across business sectors. The use of generative AI can significantly increase the speed at which any one of these types of products is created, enhancing the apparent quality in the process.

Generative AI products include Chat GPT, which was developed by OpenAI and became the fastest growing consumer application product ever recorded when released on November 30, 2022. Within its first two months it gained over 100 million users and inspired Microsoft to invest \$10 billion in OpenAI. It now experiences over 1.6 billion monthly visits to its website. Its popularity caused entities like Google and Meta to accelerate their development of competing products.

The extraordinary growth of Chat GPT use depicts the potential transformative effect of generative AI.

When used to create new text, "writer's block" no longer exists. By infusing prompts and subject matter guidance, academicians are accelerating "their" ability to publish – with the content of books being written by generative AI. Musicians, as gifted as they may be, are significantly enhancing "their" ability to create new music – with new music being created by generative AI. While this process will create challenges pertaining to identification of genuine authorship, attribution and types of infringement, those challenges pale in comparison to the devastating effects that will be caused by the malicious use of generative AI. If we simply focus on its use in information security – to defeat security controls – it is easy to envision devastating effects on information systems, business models, and even entire business sectors.

It is critically important that businesses quickly initiate both administrative and operational planning for the use of generative AI. Administrative planning pertains to policies that govern the way in which deliverables such as audio, computer code, architectural design, images, music, text and/or video are reviewed, edited, and otherwise used for business purposes. New sections of employee manuals will likely address how generative AI may be used for employment-related purposes, to address data privacy and client confidentiality concerns, and to outline penalties for unauthorized uses. Operational planning pertains to policies and procedures necessary to create a safe environment for the use of generative AI. This planning is necessary to determine whether measures should be taken to mitigate the risk that generative AI applications may pose to other documents, programs, applications, and systems within a network.

Given the powerful nature of generative AI applications, they are a high value target of malicious actors. If corrupted, they could have a devastating effect on networks in which they reside. It may therefore merit consideration to segment, "sandbox," or otherwise separate devices on which they reside from the network. If their hosting devices are segmented, post-generative AI deliverables could potentially be scanned with certain security tools in an attempt to prevent malicious code from infecting anything outside the segmented device. The worst-case scenario is the corruption of a generative AI production environment with malicious code. Unfortunately, the corruption of

significant production environments has happened too many times to not plan for the possibility – remember SolarWinds?

What can or should cyber insurance carriers do to mitigate the risk of generative AI use? Should underwriters assess the risk of generative AI use? Should they require the application of administrative and/or operational policies to mitigate the risk of a data privacy or security incident? Is the risk of an adverse event significant enough that cyber insurance carriers should consider limiting coverage for events in which the insured's use of generative AI is found to have contributed to damages and/or losses? The cyber insurance industry has experienced enough to know that these questions need to be addressed. While the beneficent use of generative AI may facilitate extraordinary advancements that benefit humanity, its malicious use will have proportionately devastating consequences.

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.



Cracking the Code: Navigating Cyber Trends

Insider Insights from Experian

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

Emerging cyber trends: A snapshot

The cyber landscape never rests. I've seen cybersecurity evolve at breakneck speed and continue to mount, with each new development bringing a fresh sense of urgency.

Three trends are front and center, each deserving immediate attention:

- Surge in third-party breaches
- Persistent healthcare sector targeting
- Human error as a recurring breach cause

Preparedness is the only way forward. More on that later, but first, let's get into the most alarming trend.

The standout trend: Third-party breaches are rising

Third-party breaches are reshaping cybersecurity. Also known as supply chain attacks, these breaches expose user data linked to subsidiaries of the breached parent company. They happen when your sensitive data is compromised through the back door of a trusted vendor.

Consider the scope of these breaches: the MOVEit breach affected over 700 known organizations, impacting more than 45 million individuals ([DataBreachToday](#)). The GoAnywhere attack exposed data from more than 130 organizations within just 10 days ([SC Media](#)). The SolarWinds breach impacted over 18,000 customers ([U.S. Government Accountability Office](#)). These instances serve as reminders that no organization, regardless of size or industry, is immune to the threat. Hackers aren't slowing down either. The [Identity Theft Resource Center](#) notes, "Supply chain attacks are a favored attack vector for cyber attackers," and 98% of organizations had at least one breached vendor in the past two years.

To comprehend how much of a problem these attacks are, consider how they magnify the scale of people attacked:

- **Nexus of attacks:** A successful breach gives hackers access to data across multiple organizations, amplifying the fallout.
- **Exploiting vulnerabilities:** Exploited weakness leads to compromised data and operational disruptions.
- **Changing landscape:** At Experian, our workload has undergone a seismic shift. Third-party breaches, once a fractional third of our work, now command over half of our services.

For firms facing breaches impacting their clients, a seamless solution for efficiently notifying and managing response is crucial and requires a coordinated effort to protect the affected parties. This is where an automated workflow proves invaluable, enabling efficient management of business-to-business (B2B) and business-to-consumer (B2C) breaches.

Healthcare: An ongoing target

Shifting the focus to healthcare, a clear and troubling trend emerges. Healthcare remains a perennial favorite target for cyber-attacks for the fifth consecutive year. The numbers don't lie—40-45% of the breaches we handle at Experian are linked to healthcare.

The sector's vulnerability is evident, with 707 breaches exposing nearly 50 million records in a [2022 IBM and Ponemon study](#). The financial toll is high; the same study showed that the average healthcare incident costs over \$10 million.

Human error: A recurring Achilles' heel

Another recurrent theme is the pivotal role of human error. This is the root cause of a whopping 90% of attacks we handle. This category encompasses a range of missteps, from Business Email Compromises to wire transfer errors and staff-related mistakes. Unfortunately, this trend has only worsened with time.

The path forward: Preparation is the key to resilience

Acknowledging the threats and adopting proactive measures are vital steps to securing your organization's future. In case of a breach, a timely response is paramount to mitigate the damage.

How Experian Data Breach steps up

Amid these challenges, Experian Data Breach emerges as a beacon of support, armed with innovative solutions and unwavering commitment. Here's how we're making a difference:

- 1. Third-party solution:** We have an automated solution for vendor events to allow their clients to Opt-in/Opt-out to a shared solution, saving time and reducing costs of consumer response.
- 2. Client satisfaction:** We take pride in our 80 Net Promoter Score (NPS) from monthly client surveys. This is a testament to our dedication to being easy to do business with.
- 3. Call center:** Our capacity—handling 5.5 million calls this year-to-date alone—underscores our preparedness for large-scale incidents.
- 4. Notification:** Experian services large-scale notifications—handling over 22 million email and 40 million mail notifications (from the period September 2022 – August 2023).

To recap

Emerging cyber trends demand unwavering vigilance and strategic preparation. Third-party breaches, healthcare vulnerabilities, and human errors are pivotal areas requiring targeted solutions. Experian Data Breach is poised to provide tailored support and guidance on this journey.

About Experian

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



Cybersecurity Environment Remains Challenging as Business World Evolves

Companies must stay vigilant as new threats emerge

by Sean Renshaw, Senior Director, Security and Privacy Risk Consulting, RSM US LLP

The cybersecurity threat environment continues to evolve as businesses contend with various threats related to geopolitical risks, uncertain economic conditions, and lingering effects of the COVID-19 pandemic. Threats can come from many different directions, so companies need to understand where their potential vulnerabilities exist and act quickly to address them.

We know no company is immune to a breach, and attackers are relentless in finding exposures to attack. That often means focusing on smaller and mid-sized companies that may not have the resources and control strength as larger organizations.

However, there is some good news: despite increasing pressure from threat actors, RSM US LLP research shows that the number of reported breaches is down as organizations appear to take cybersecurity challenges more seriously. According to the [2023 RSM US Middle Market Business Index Cybersecurity Special Report](#), 20% of middle market executives experienced a data breach within the last year, a slight drop from 22% in last year's survey.

Despite the decline, that is still a large number. Companies cannot afford to relax and must continue to focus on identifying emerging risks, refining cybersecurity strategies and closing any potential control gaps.

The ripple effect of pandemic changes

When the pandemic struck, many organizations rapidly shifted to a remote work approach that represented a seismic shift from the traditional office environment and required a new technology foundation focused on more extensive productivity software and cloud storage.

With this transition, companies have had to become more tech savvy and adopt a new way of running the business. Many companies have become more digital and now resemble tech firms in many ways, and that approach requires more focus on cybersecurity resources.

Increased focus on cybersecurity protections

As this digital shift progressed, companies moved infrastructure to the internet and the cloud, and threat actors took advantage of low-hanging fruit as compromises increased. But as digital strategies have evolved, protective strategies have also improved.

For example, the RSM US MMBI survey found a sharp increase in the number of middle market companies with a dedicated security and privacy function, as well as a significant increase in the number of people responsible for data security and privacy that now report directly to the CEO. These adjustments show that companies understand the ongoing commitment required to address ongoing cybersecurity challenges.

In addition, more companies are taking advantage of managed security services strategies to bolster protective measures. Increased innovation has created a considerable strain on internal resources that may not always have extensive experience managing emerging tools and platforms, creating potential cybersecurity gaps.

Further, the tight labor market has made qualified cybersecurity resources more difficult to attract and retain. With these obstacles in mind, a managed services approach enables companies to take advantage of supplemental qualified cybersecurity resources that can scale up or down quickly as business needs dictate.

More challenges ahead?

Companies need to keep an eye on the evolving talent market and evaluate the best strategy to deploy and manage cybersecurity resources. They generally have two options for structuring cybersecurity functions: develop in-house talent and procure the necessary tools and technology or leverage a vendor or external advisor in an aforementioned managed services strategy.

As the tasks necessary from cybersecurity resources become more complex and demand for personnel continues to drive costs up, managed services or a hybrid approach with a mix of internal and external assets should be a consideration for an effective security posture.

Over time, the structure of cybersecurity disciplines will also need to evolve. With companies utilizing varying cloud strategies, and critical tools such as identity and access management emerging to control permissions for a growing amount of technology solutions and platforms, a cybersecurity framework must be fluid and updated seamlessly as threats and new protective measures materialize.

A proactive approach

The cybersecurity environment will only require more attention moving forward as new digital investments become necessary and new threats emerge.

Companies can no longer afford to be reactive as threats become apparent; instead, they must continue to progress in developing proactive strategies that are nimble enough to address potential vulnerabilities before they become breaches.

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](#).



Nailing it.

by Aaron Aanenson, Cyber Insurance Sales and Thought Leader, Bitsight

It's that time of year when we actively await the results of last year's performance in the cyber insurance industry. Reports of gross written premium rankings, loss ratio performance, and regular commentary from the industry leaders who oversee it all captivate us as we try to balance the forces that drive our industry. As I review the trends in the NetDiligence 2023 Cyber Claims Report, one thing is clear - managing growth in a responsible manner requires trust and faith in our ability to adequately predict the future and price it accordingly. Over the past year, I've been pleased by the progress that we've made collectively to set the bar higher for underwriting, increase transparency in the process broadly, and continue to attract new insureds to grow the market. As carriers, brokers, and (now) even reinsurance companies have combed through Bitsight data, there's been broad agreement that poor security performance is predictive of cyber claims. As the industry continues to lean on this information to inform underwriting requirements, I am encouraged that we have the information the industry needs to grow in a healthy fashion, and that we continue to invest and improve it.

But not so fast! As we've experienced in the past, we know there will be years that aren't as healthy as 2022. The truth is that our industry continues to grow at a record pace while we manage a changing and challenging threat landscape. It seems an impossible task to grow this industry at this pace, but it is one that is well-served by scalable technology solutions. I am invigorated by the positive independent reports that we receive from brokers, carriers, and reinsurers who study the correlation of Bitsight's data to their claims. The predictive power it holds allows our talented underwriter community to focus more attention on their deals, rather than on their risk assessments. And for those new to the industry, it allows them an easier onramp to sell more insurance faster.

Another key to keeping this industry thriving will be to support the largest growth segment with actionable security findings - our beloved SMEs! Basic economics tells us that smaller companies generally have fewer

resources to spend on securing themselves, which is clearly represented in the results of this claims study. SMEs need our help to understand where they should invest - and who better to make those recommendations than the very companies that witness the claims firsthand? As trusted security professionals, we have a very important role to play in keeping this industry healthy. For some insureds, that means knowing when to reach out to help them and how to be helpful in those moments with use of scalable solutions. In many cases, underwriters have access to more risk information than the insured does. Think about it - without tools to automate the process, merely getting a sufficient view of third-party risk would be a full time job at some companies, and that's only a fraction of the information underwriters use to evaluate risk. By creating transparency in the underwriting process, staying relevant throughout the policy period, and remaining trustworthy resources to insureds, we are doing our part to keep this industry thriving.

But we can do even more. To start, we can share more risk data with insureds. Based on the claims correlation studies that have been conducted with Bitsight's data, we know that patching cadence is - hands down - the leading predictor of breach. Other studies, including one recently released by [Akamai](#), found that a 143% increase in ransomware victims between Q1 2022 and Q1 2023 was driven primarily by vulnerability exploitation. This leads me to believe that access control and port security has improved, and attackers are now relying more often on technical vulnerabilities to compromise their victims. With endless new critical vulnerabilities discovered daily, insureds - and especially SMEs - can use our help. If security vulnerabilities are uncovered during underwriting, we owe it to our insureds to share that information with them. And hopefully, they can even receive ongoing access to such valuable information throughout the policy lifecycle. As insureds continue to expect more services from their carriers, there continue to be more solutions available to them.

As I reflect on the year gone by and the challenges that this market faced in 2020, I am very proud of the hard work that this community put in to drive us in a better direction. As we look forward, let's remember what led to those difficult times and lean on each other as trusted leaders, underwriters, and practitioners to share our solutions to complicated challenges as we continue to grow this market in a healthy and sustainable way.

About Bitsight

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT

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

The eRiskHub® is a white-label cyber risk management portal that helps both insurers and their clients combat cyber losses. This Software-as-a-Service (SaaS) offering provides tools and resources to help clients understand their exposures, harden their cyber defenses, and respond effectively to a cyber incident. Our mobile-friendly, flexible platform can be branded, customized, and delivered to any domain. Plus, it's scalable! Start small and increase your license as you grow. You can also add content for other geographic regions as you expand globally.

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 2024, you will find us in Miami Beach, Toronto, San Diego and Philadelphia.

Contact Us

For more information, visit us at netdiligence.com, email us at management@netdiligence.com or call us at 610.525.6383.



About the Study

Contributors

Risk Centric Security, LLC.

A special thank you also 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.

Other

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

- Dave Chatfield – Vice President & Chief Operating Officer, NetDiligence
- Heather Osborne – Director of Global Events & Programming, NetDiligence
- Sharon Lyon – Publisher, NetDiligence
- Cait Osborne - Digital Media & Communications, NetDiligence

For more information, visit us at netdiligence.com, email us at management@netdiligence.com or call us at 610.525.6383.

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 2020, 2021 or 2022.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to 176 individuals at 103 organizations in the United States, Canada, and the United Kingdom. From this group, 18 individuals representing 17 organizations provided 4,945 analyzable new and updated claims, using the proprietary NetDiligence® claims data collection worksheet.

The 2023 report also includes data from NetDiligence studies published in 2018-2022, representing 4,083 incidents that occurred in 2018, 2019, 2020, and 2021, making a total of 9,028 claims that could be analyzed. All of these were included in the demographic analyses, and 7,906 claims with a Total Incident Cost >=\$1,000 were included in the financial analyses.

There are 8,725 claims in the dataset from US organizations, 177 claims from Canadian organizations, and 22 claims from organizations in the United Kingdom. There are also a small number of claims (<40) from organizations in Australia, EU Countries, South Africa, other countries, and organizations with a global footprint. The country was not specified in 56 claims.

When factoring in SIRs, we were able to calculate total incident costs to date for all 7,906 (100%) of the claims with total incident costs >\$1,000. 4,906 claims (54%) included an accounting of crisis services costs. 611 claims (7%) specified the number of records exposed. The number of claims reporting the number of records exposed decreased since last year due to the large number of claims for incidents that do not expose records (ransomware, social engineering, BEC, etc.) .

8,033 (89%) claims in the dataset were flagged as closed and 982 (11%) as open. The claim status was unknown for 13 claims. 5,118 (57%) claims were for primary coverage, 71 (<1%) for excess coverage, and 3,839 (43%) had an unknown, but most likely primary, coverage level.

There were 3,376 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 costs 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 costs 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 costs 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 costs 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 Costs 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.