NetDiligence®
CYBER CLAIMS STUDY
2022 REPORT

RSM experian GUIDEWIRE THEBECKAGEFIRM

Contents

Introduction

Welcome to the twelfth annual NetDiligence® *Cyber Claims Study*. This report is based upon the summary statistical analysis of almost 7,500 cyber claims for incidents that occurred during the five-year period 2017–2021. By comparison, the sixth *Cyber Claims Study*, published in 2016, analyzed fewer than 200 cyber insurance claims.

By the Numbers

- 7,439 claims analyzed from incidents that occurred during 2017–2021
- 3,403 new and updated claims collected in 2022, from incidents occurring from 2019–2021
- 1,119 claims analyzed arising from incidents occurring in 2021
- 98% of claims ($1.08B in total) from Small to Medium Enterprises (SMEs) with less than $2 billion in annual revenue
- 2% of claims ($1.1B in total) from Large Companies with more than $2 billion in annual revenue
- 2,123 claims due to ransomware, 45% of which occurred in 2020 and 2021
- 825 ransomware claims which provide both the ransom demand and the total incident cost
- 1,153 claims due to business email compromise (BEC), 57% of which occurred in 2020 and 2021

Preliminary Observations

- There are enormous variances in the magnitude of the loss data. The smallest claims were less than $1,000 and the largest are over $300M. The numbers of records exposed range from 2 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 $150B in annual revenue) was approximately 15.5 million times larger than the smallest organization (less than $15K in annual revenue). The average Large Company ($13.5B in annual revenues) was more than 150 times larger than the average SME ($88M).
- Even though Large Companies represented only 2% of claims (N=120), these claims accounted for 51% of the Total Incident Cost analyzed in the report ($1.1B/$2,1B).
- 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 90 times more costly than those at SMEs. However, SMEs experienced large losses as well, with perhaps greater organizational impact – there were 149 SME claims with Total Incident Costs >$1M.
- 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 business email compromise were the two leading causes of loss. They accounted for 44% of claims during the five-year period 2017–2021, and nearly 50% in 2020 and 2021.

With Appreciation

We want to sincerely thank the cyber insurers listed on page 48 for their support of this report and their dedication to industry education. Many of them have contributed to this research every year for more than 10 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

Company Size

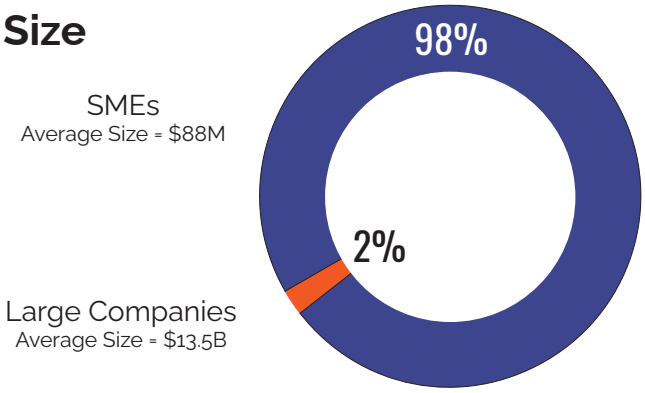


Figure 1

Average Costs for All Claims

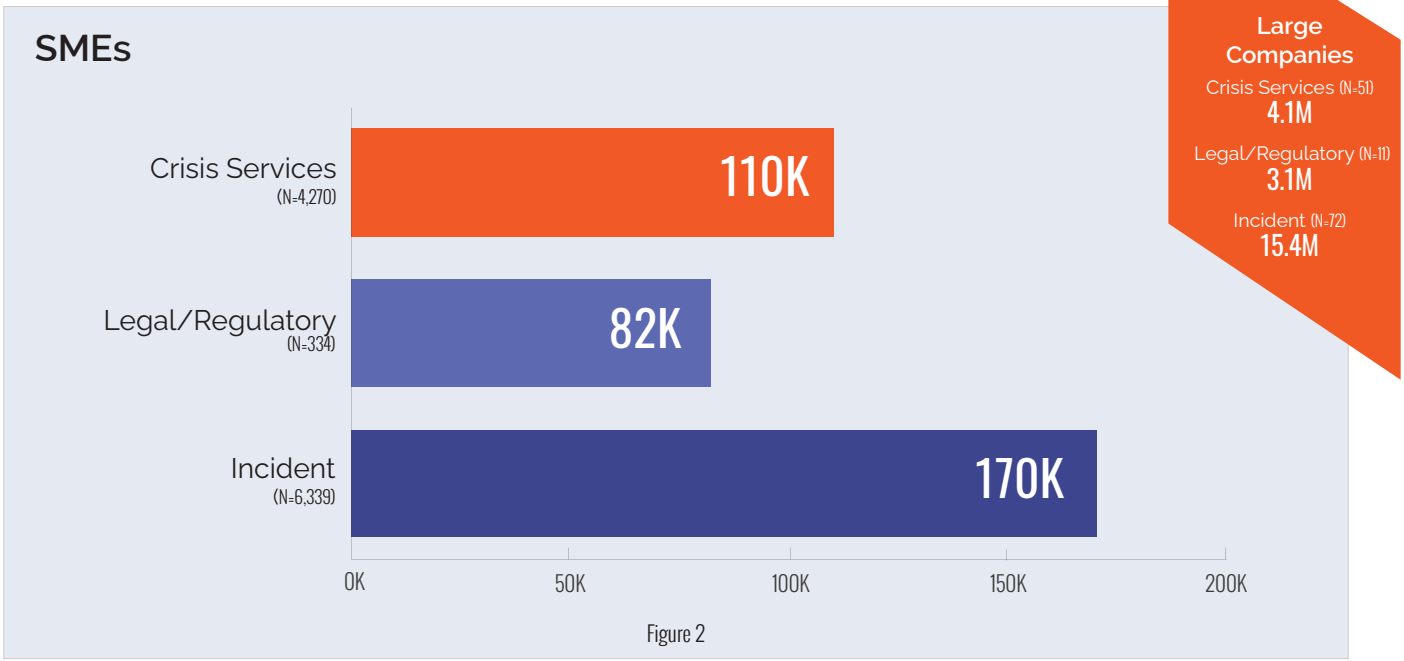


Figure 2

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 2017–2021 unless otherwise noted.
NetDiligence and Breach Coach are registered trademarks of Network Standard Corporation, dba NetDiligence.

 Version 1.0

Average Costs for Ransomware

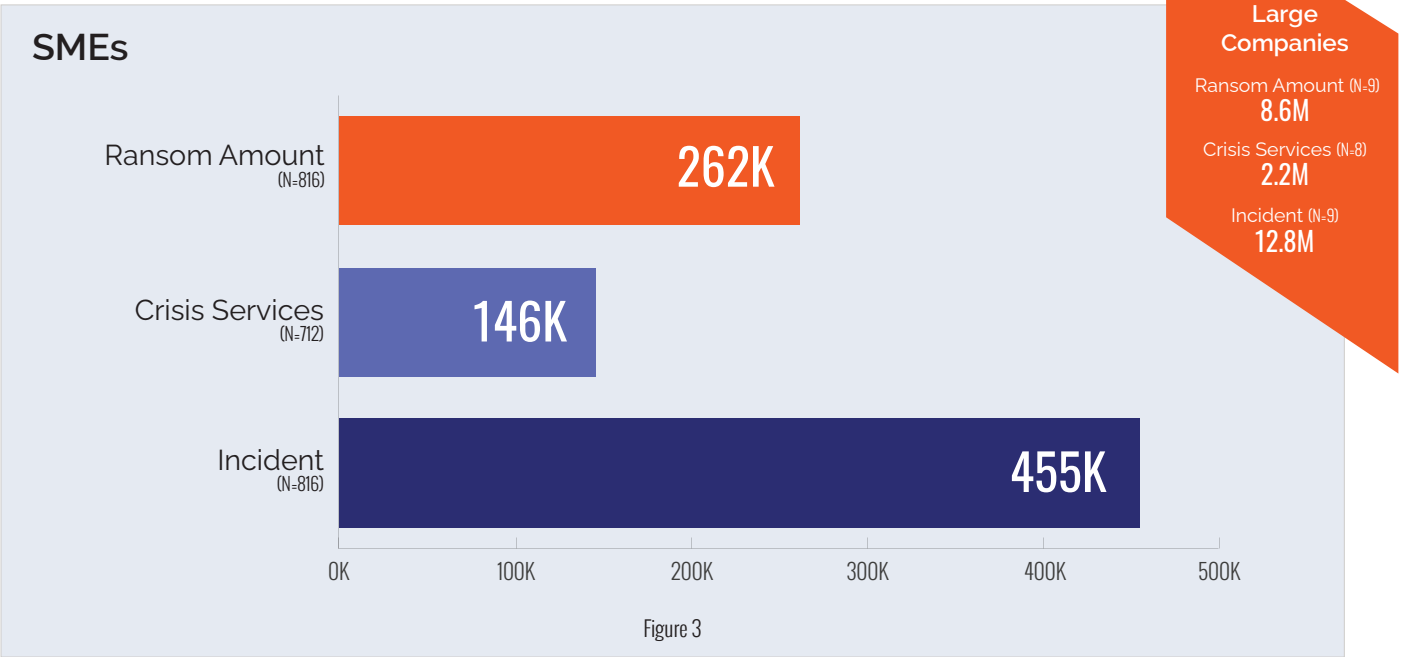


Figure 3

For the third year in a row, ransomware is the leading cause of loss for SMEs. Furthermore, the overall business interruption cost of a ransomware incident has significantly grown over that time period. It is a crucial time for SMEs to protect themselves by implementing preventative measures such as MFA and EDR.

Equally important, we have learned from the cyber insurance community that all sectors must be vigilant about putting in place an actionable incident response plan with hotlines to the insurance carrier's Breach Coach® and IR experts. Ransomware, along with business email compromise (BEC), will likely remain the primary cyber threats. However, we have seen first-hand that when organizations have the tools and planning in place to respond quickly and efficiently, they can minimize both the cost and the disruption to their business.

Mark Greisiger
President
NetDiligence®

Average Costs for Business Interruption

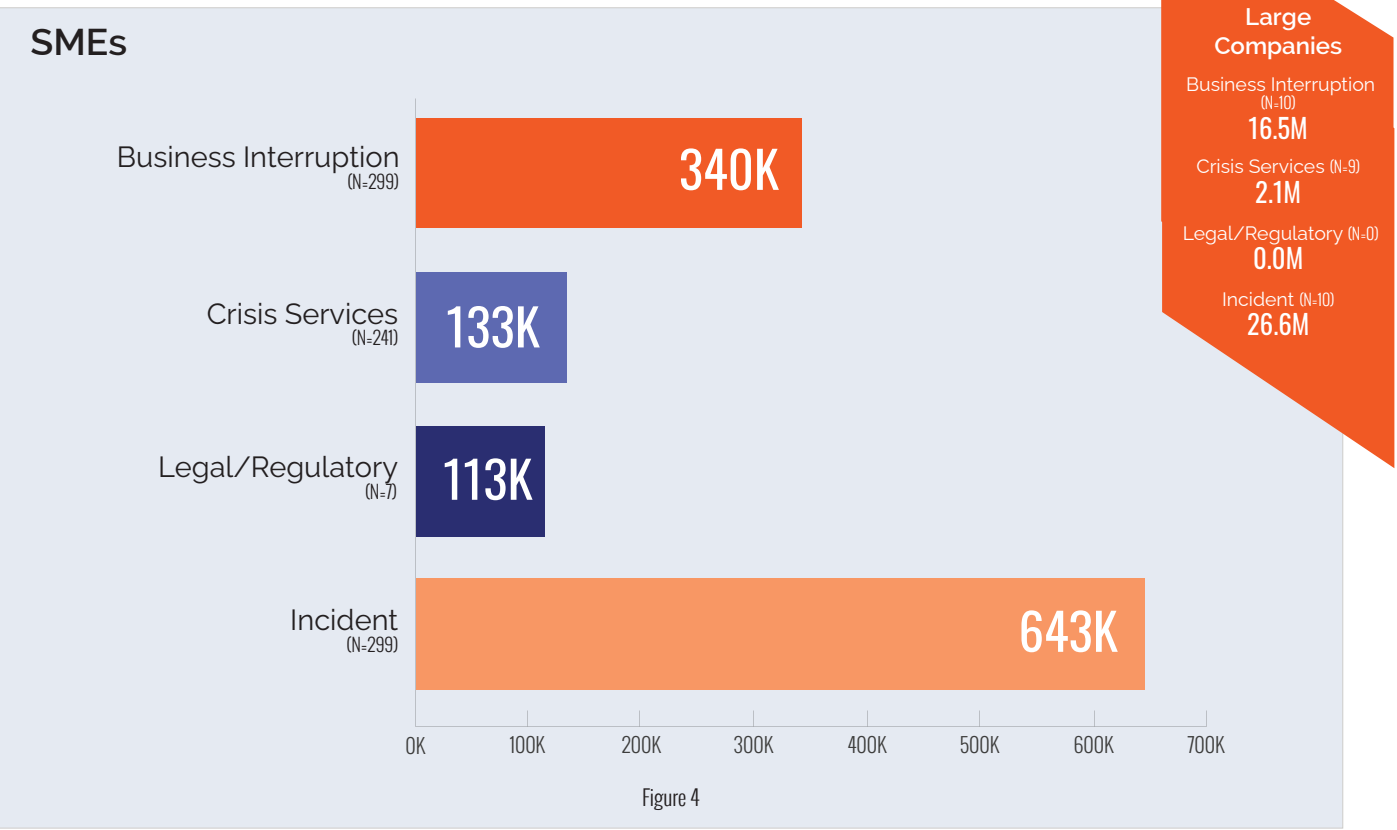


Figure 4

This year's study makes it clear that the cost of a cybersecurity incident and its timely recovery can vary depending on an organization's incident response and resiliency plans. Organizations with a robust and tested cyber resiliency plan will potentially mitigate the risk of longer interruptions and high recovery costs, reducing the overall impact to the business. The idea is not only to recover, but to recover expeditiously–which can only be accomplished with a proper cyber resiliency and crisis management plan.

Tauseef Ghazi
National Leader, Security and Privacy Services
RSM US

Business Sector

Top 5 by Number of Claims – SMEs

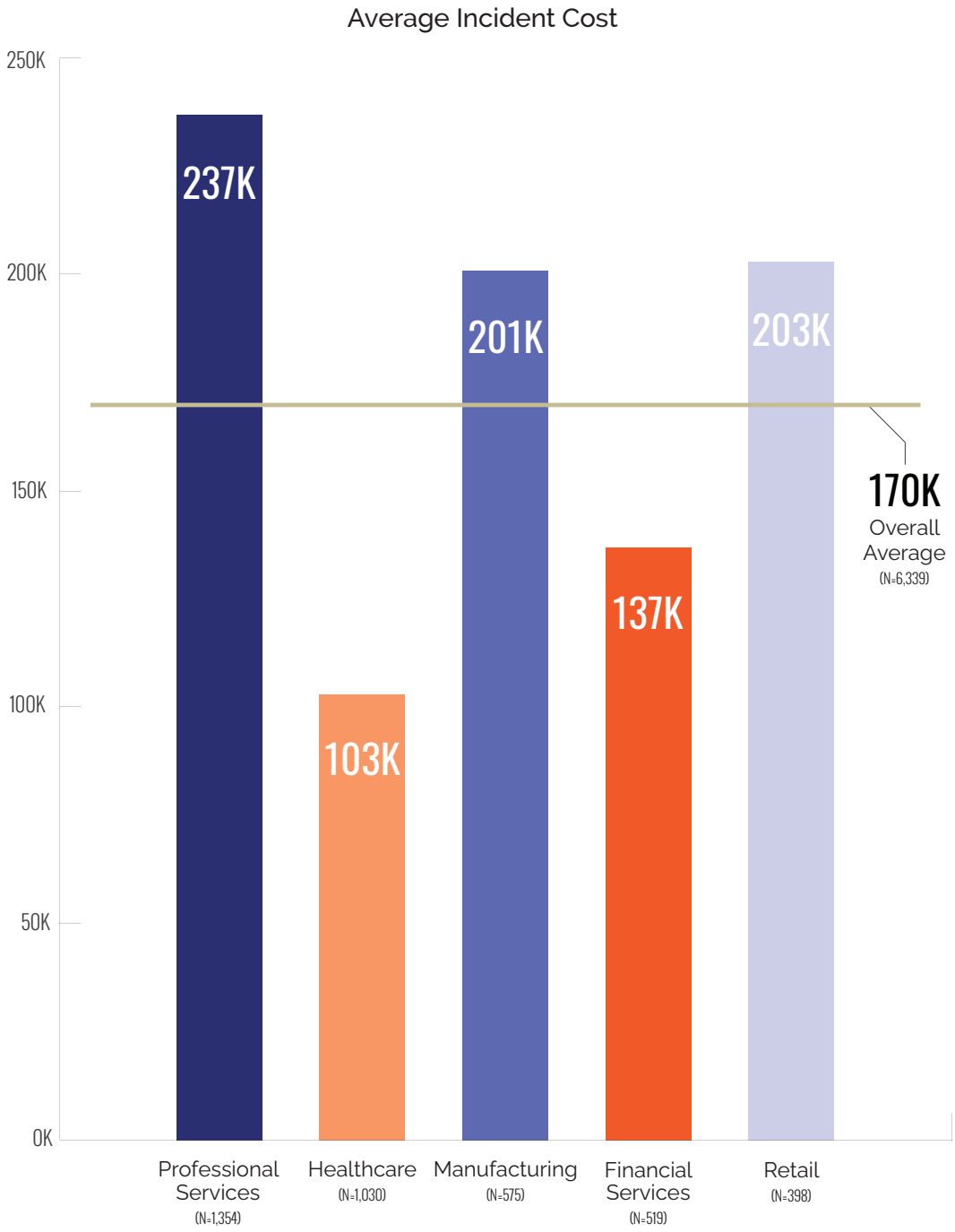


Figure 5

Cause of Loss

Top 5 by Number of Claims – SMEs

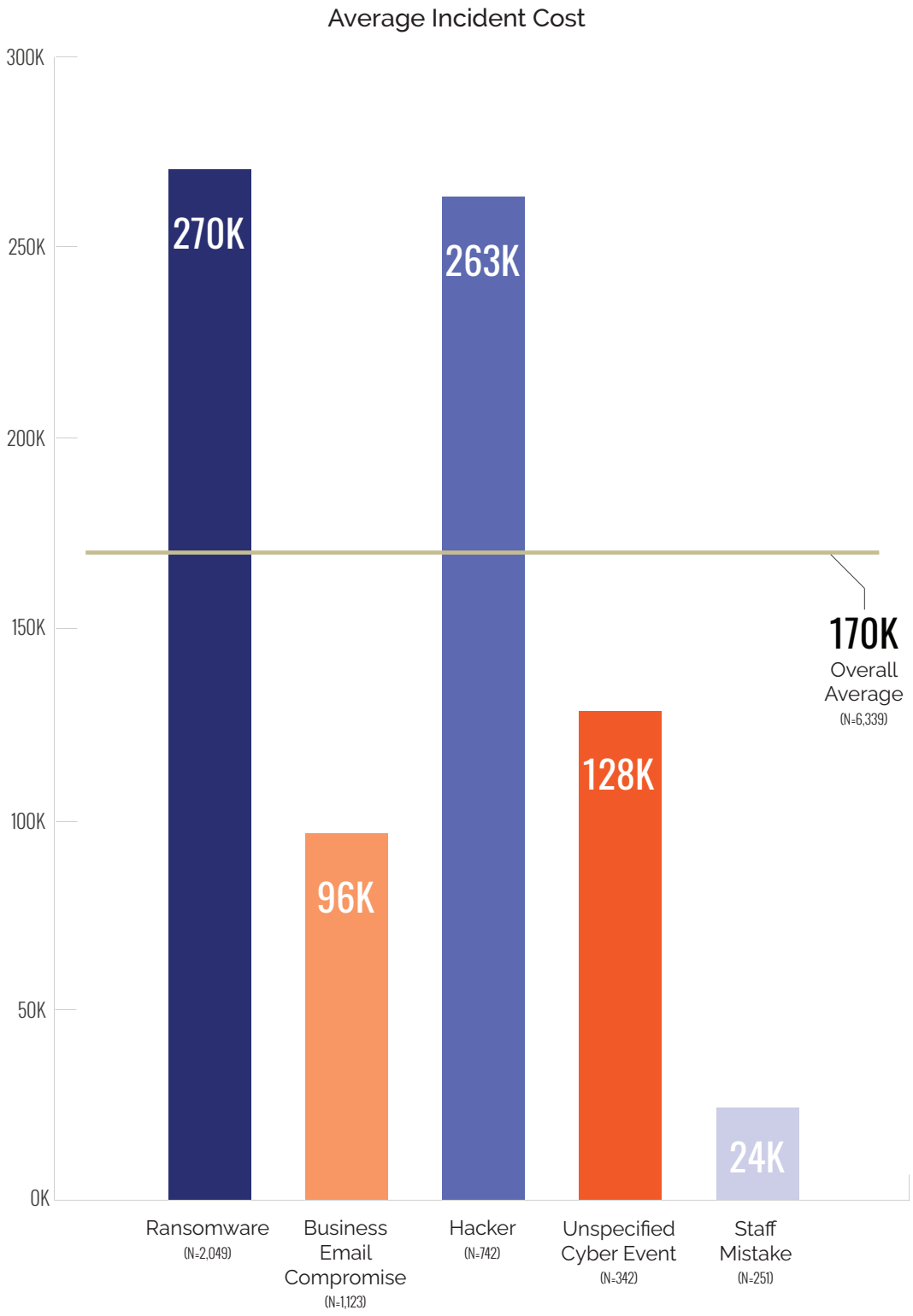


Figure 6

An Overview of the Data

The claims analyzed in this study come from organizations of all sizes, the smallest with less than $15K in annual revenue and the largest with over $150B. As indicated earlier, the dataset is overwhelmingly weighted with claims from smaller companies. This can dilute the findings for large companies, while 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 (70%) 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 $15K to $1.9B. The average was $88M. SMEs accounted for 98% of claims but only 49% of Total Incident Cost.
- Large Companies: annual revenue ranged from $2B to more than $150B. The average was $13.5B. Large companies accounted for only 2% of claims but 51% of Total Incident Cost.

Proportion of Claims
2017–2021
(N=7,439)

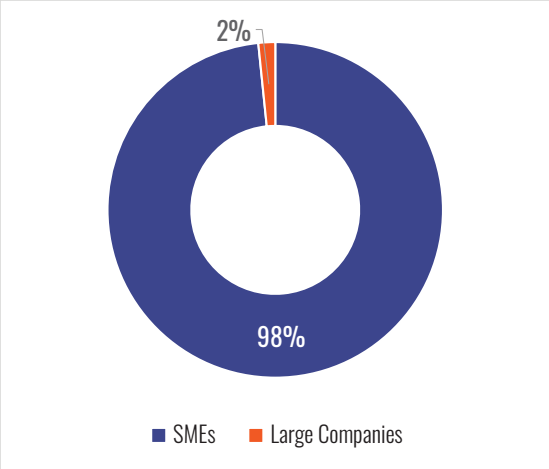


Figure 7

Proportion of Cost
2017–2021
(N=7,439)

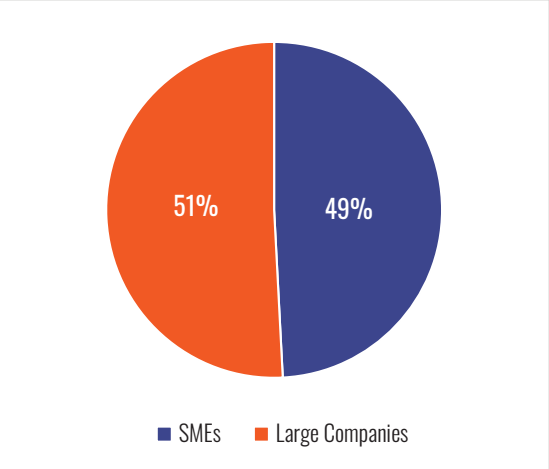


Figure 8

Claims by Year of Event

The scope of this study is 7,439 incidents that occurred from 2017 to 2021. The distribution of incidents by year is depicted in Figure 9.

Demographic analyses have been based upon all 7,439 claims. Cost analyses have been based upon the 6,622 claims that reported Incident Costs >=$1,000.

The claims analyzed in this report come from incidents at organizations in seven revenue groupings, 18 business sectors, 25 causes of loss, and 10 types of data.

Percentage of Claims by Year
(N=7,349)

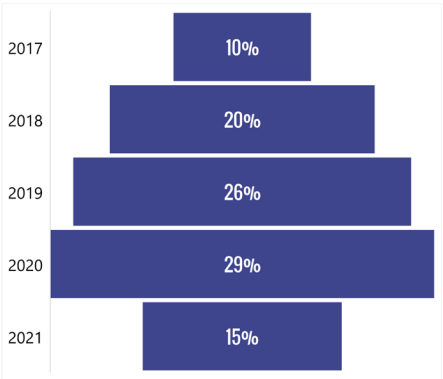


Figure 9

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. The following figures provide the year-by--year average and the five-year average payout amount and Total Incident Costs for both SMEs and Large Companies.

For SMEs, the largest incident occurred in 2017 (>$100M). The largest incident at a Large Company happened in 2019 (>$300M).

Payouts represented 70-80% of the Total Incident Cost. For SMEs, the five-year payout was 75% of the Total Incident Cost. At Large Companies, this number was 45%.

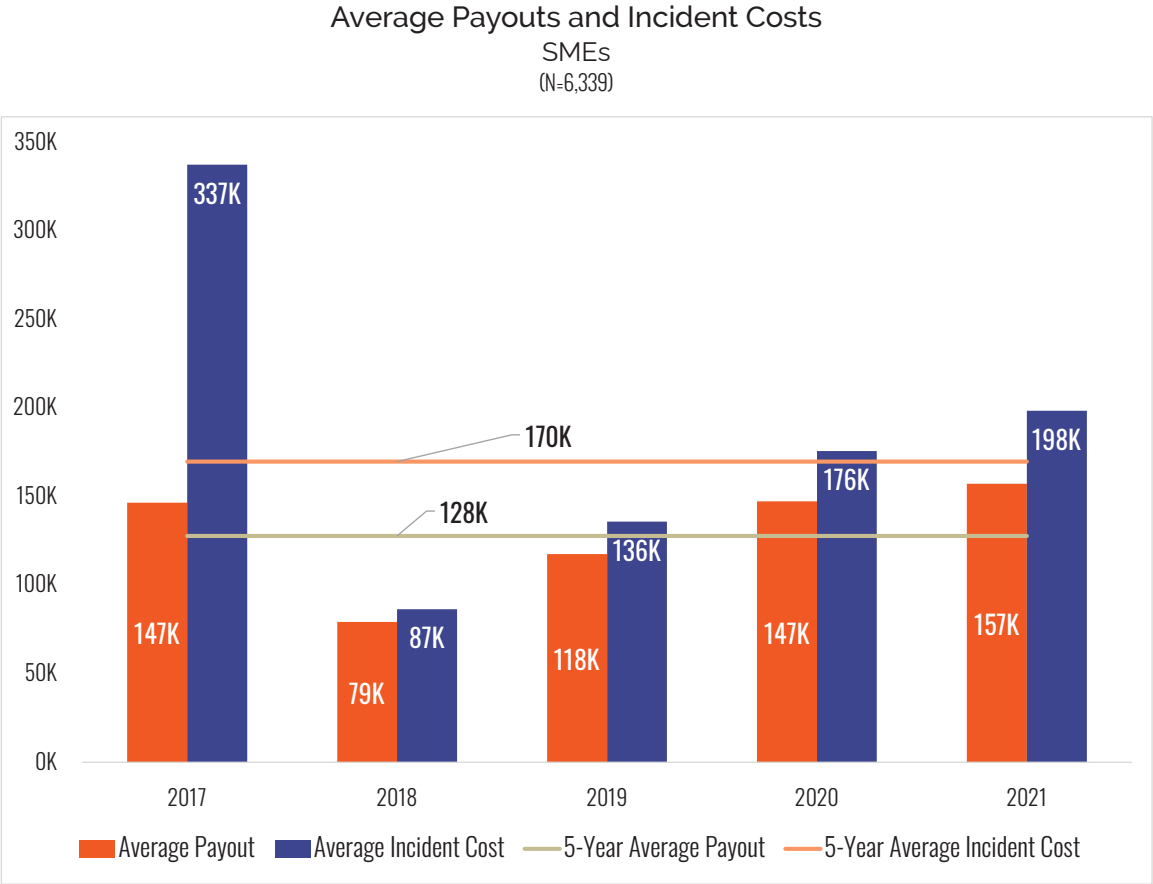


Figure 10

Average Payouts and Incident Costs
Large Companies
(N=72)

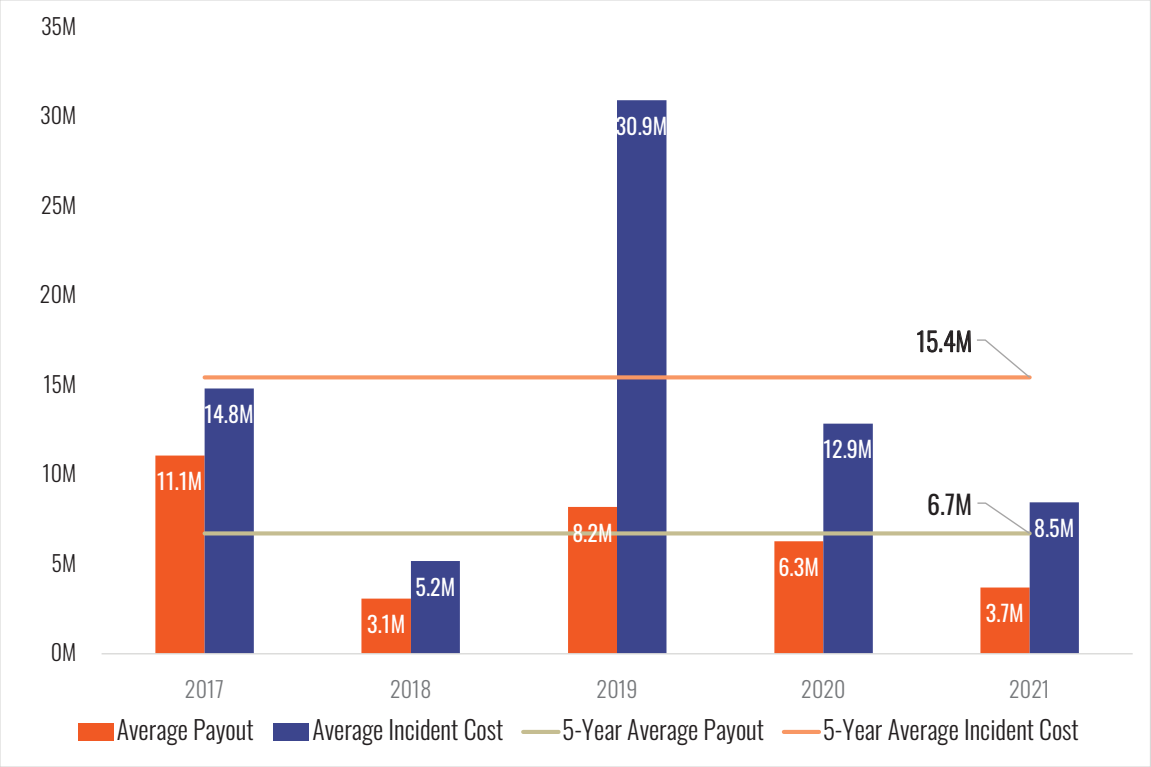


Figure 11

Incident and Crisis Services Costs

For all organizations, Crisis Services Costs ranged from less than $100 to more than $120M. Incident Costs, inclusive of Self-Insured Retention (SIR), ranged from less than $1,000 to more than $300M. The averages were influenced by some very expensive claims. At SMEs, there were twelve claims in 2017-2021 with Total Incident Cost of more than $5M, one of which exceeded $100M. At Large Companies, there were thirty claims ranging from $5M to over $300M.

At SMEs, there was a large outlier event in 2017 that caused a spike in the average Crisis Services and Incident Costs. Since 2018, the averages for both costs have been steadily increasing. Year over year, Crisis Services Costs ranged from 50% to 89% of Incident Cost. Over five years, these costs accounted for 65% of Total Incident Cost.

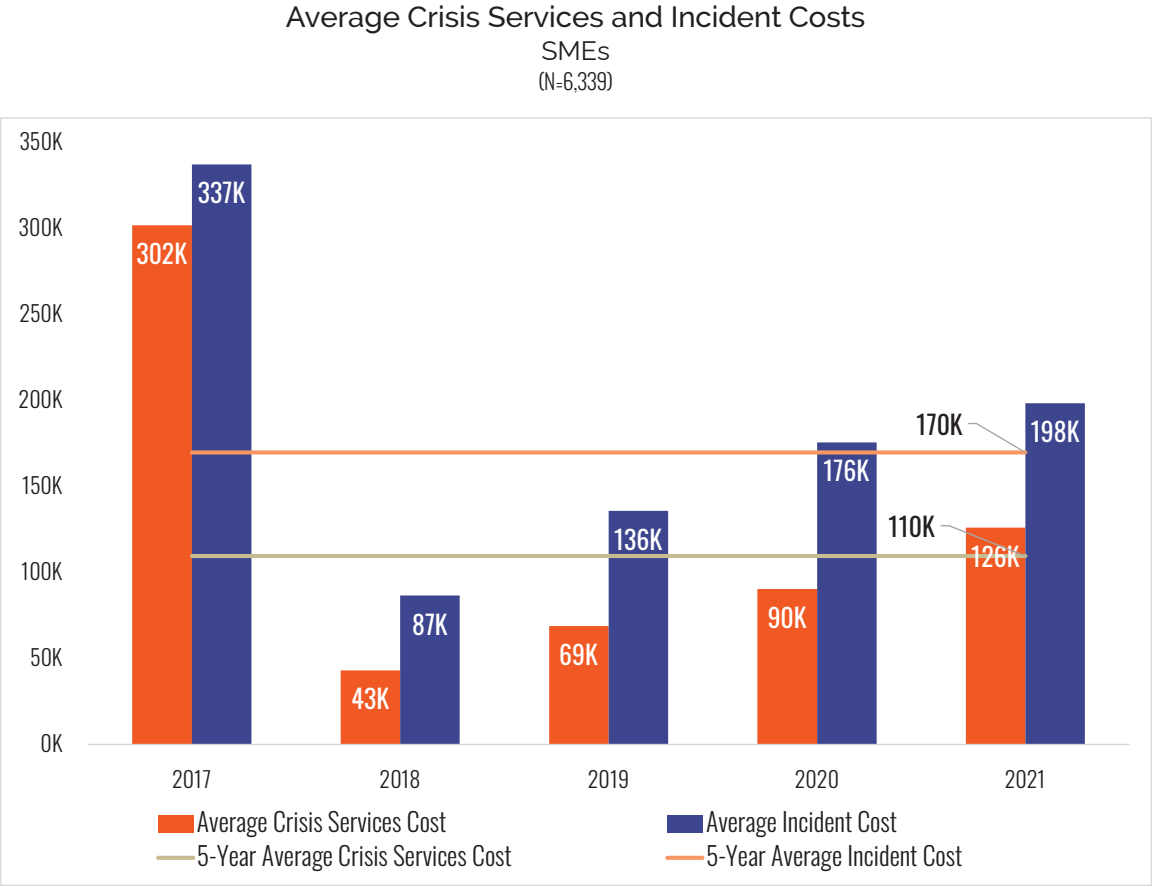


Figure 12

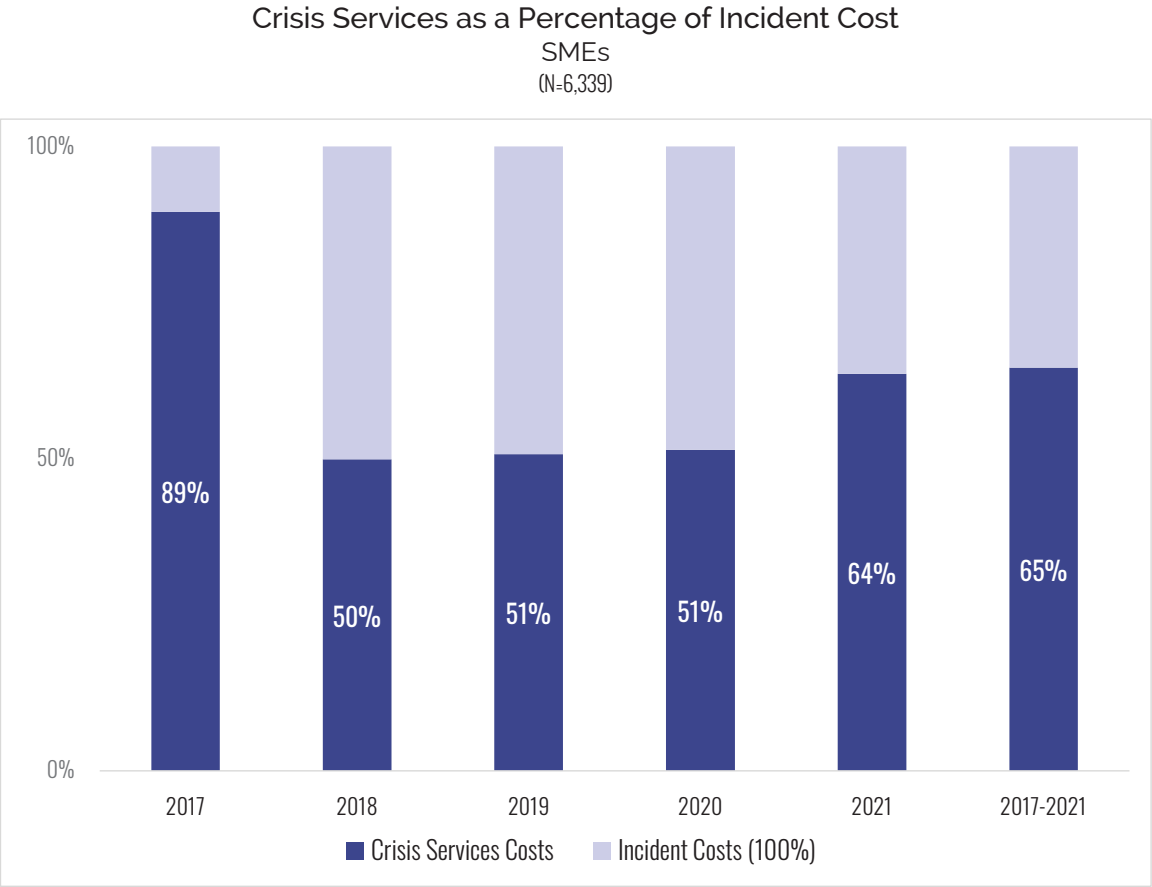


Figure 13

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. Forensics accounted for 53% of the total and Legal Guidance accounted for another 24% of the total.

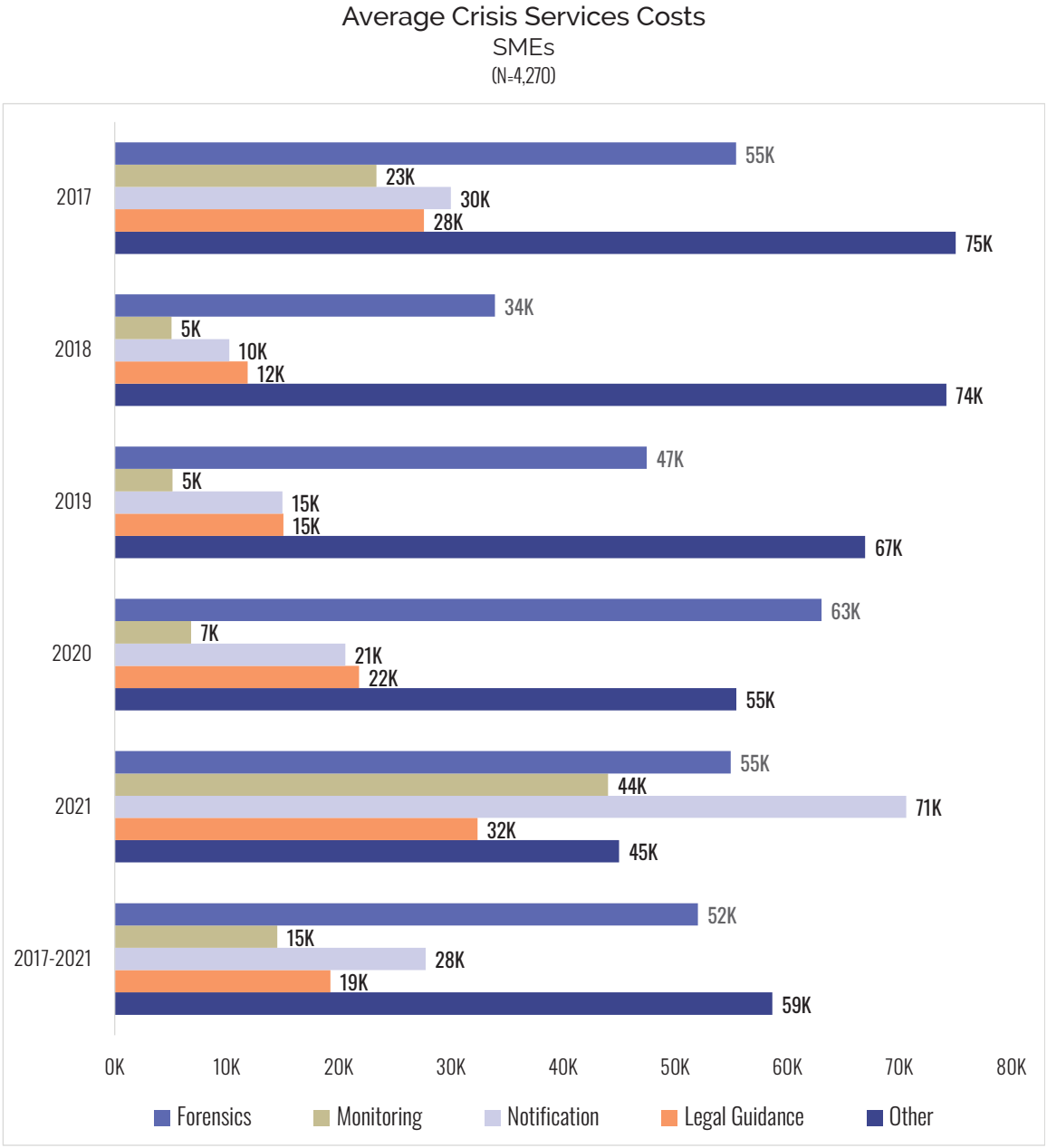

Average Crisis Services Costs
SMEs
(N=4,270)
2017
55K
23K
30K
28K
75K
2018
34K
5K
10K
12K
74K
2019
47K
5K
15K
15K
67K
2020
63K
7K
21K
22K
55K
2021
55K
44K
71K
32K
45K
2017-2021
52K
15K
28K
19K
59K
0K
10K
20K
30K
40K
50K
60K
70K
80K
Forensics
Monitoring
Notification
Legal Guidance
Other

Figure 14

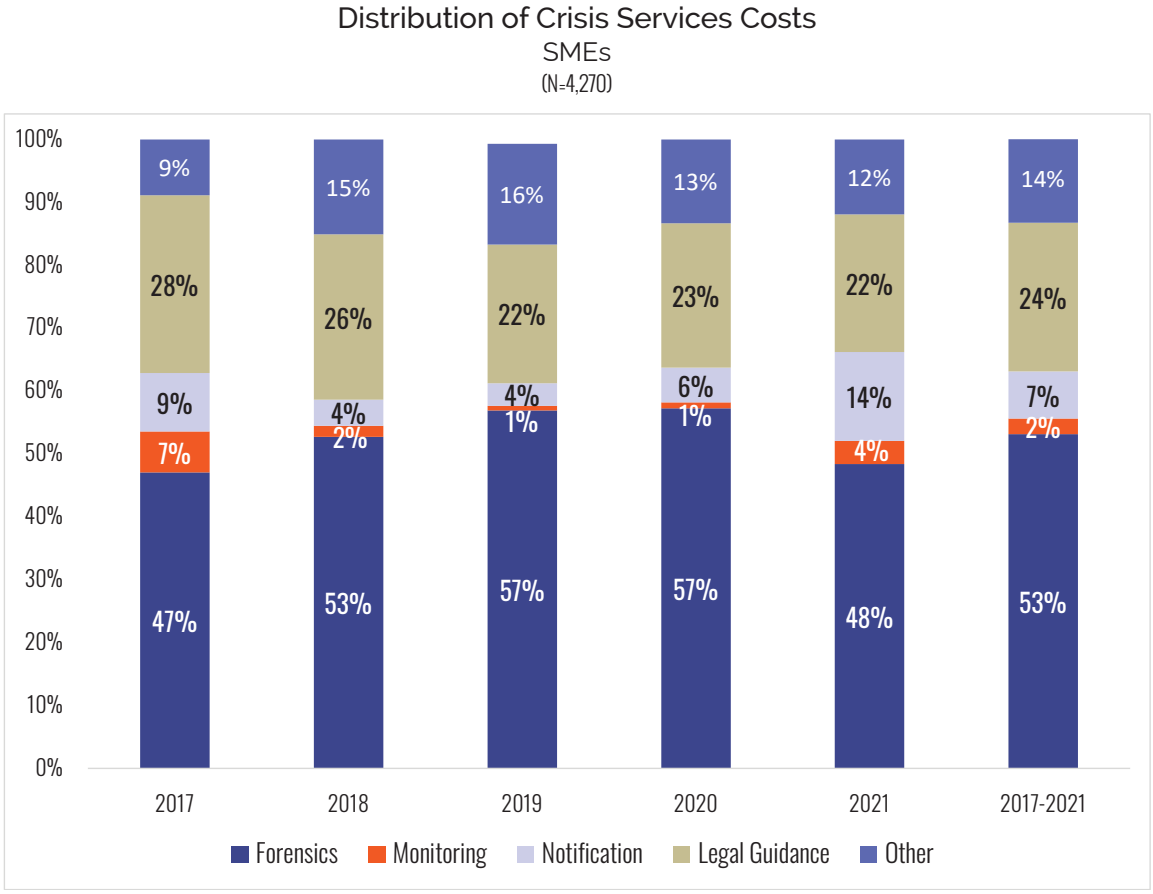


Figure 15

At Large Companies, there was an outlier event in 2019 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 Incident Costs ranging from $5.2M to $30.9M

Crisis Services Costs accounted for 6% to 97% of Incident Cost year-over-year, and 27% over five-years.

Average Crisis Services and Incident Costs
Large Companies
(N=72)

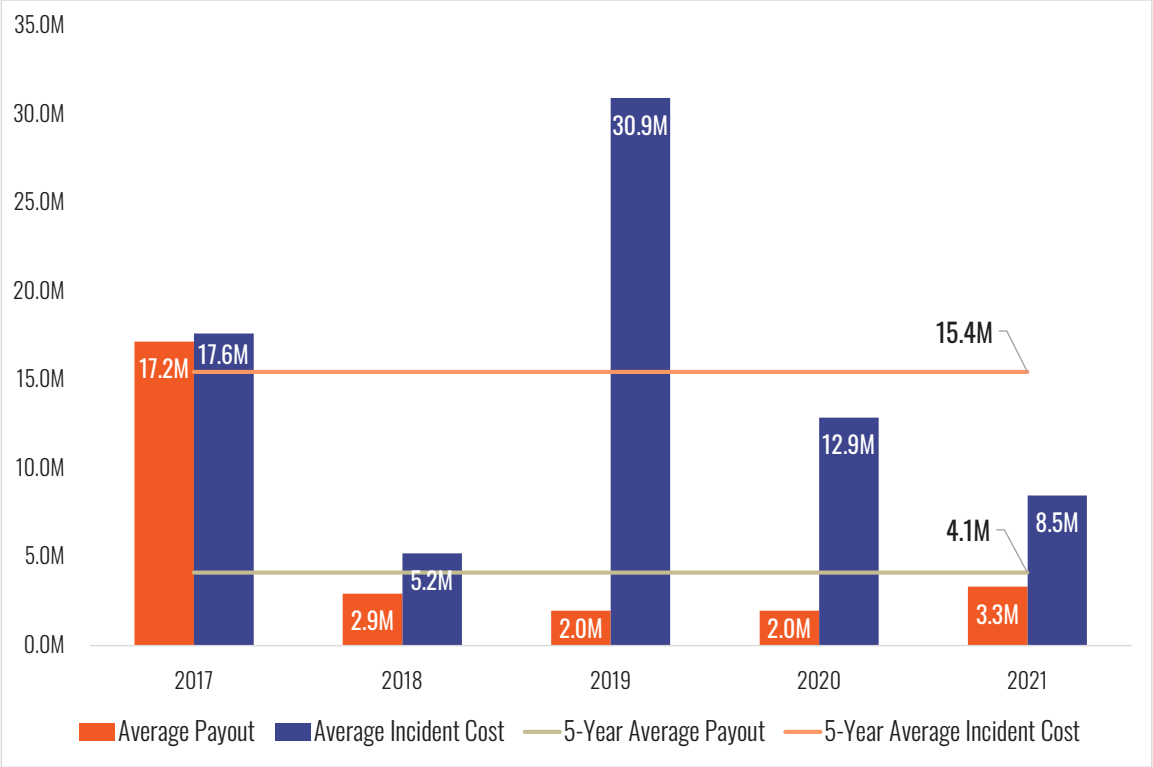


Figure 16

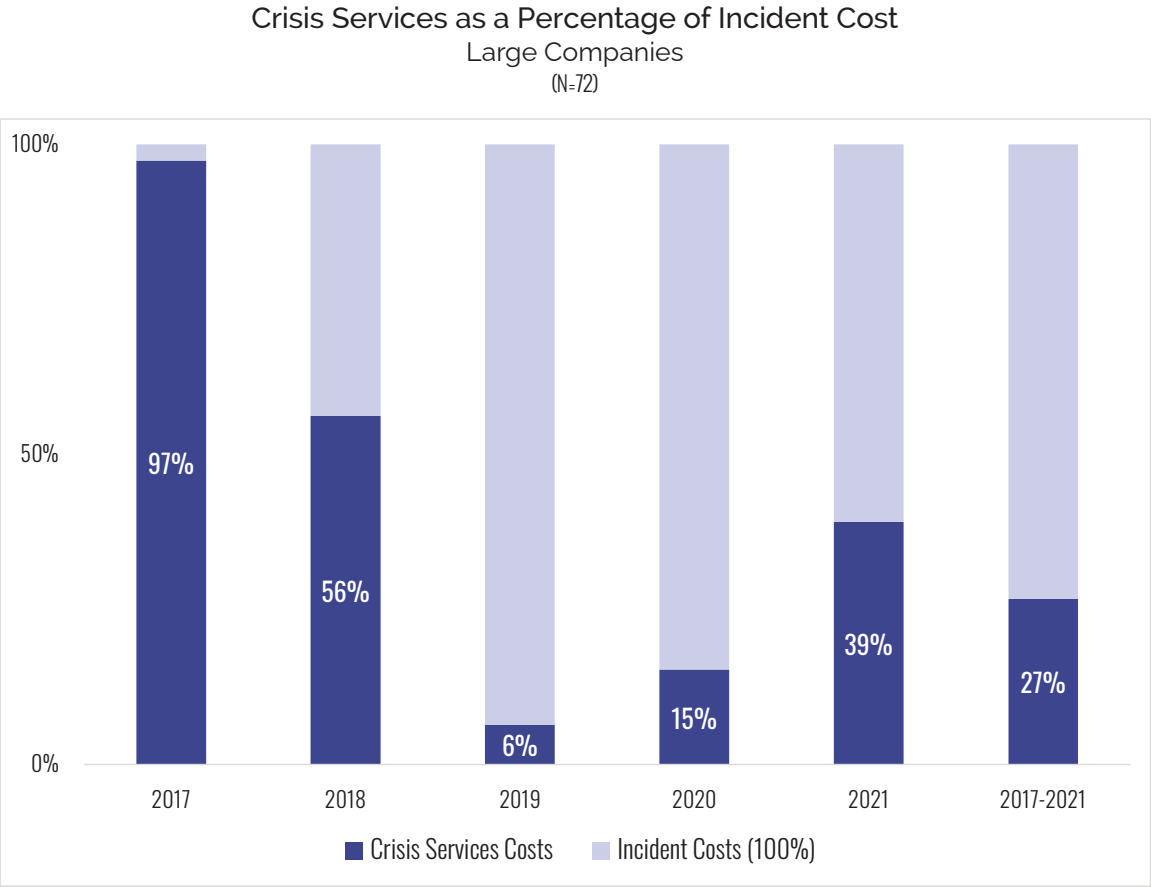


Figure 17

Figure 18 depicts the percentage of total of each crisis services component. Year over year, there is much variability. Over five-years, Forensics accounted for 48% of the total. Notification and Legal Guidance accounted for 19% and 17%, respectively.

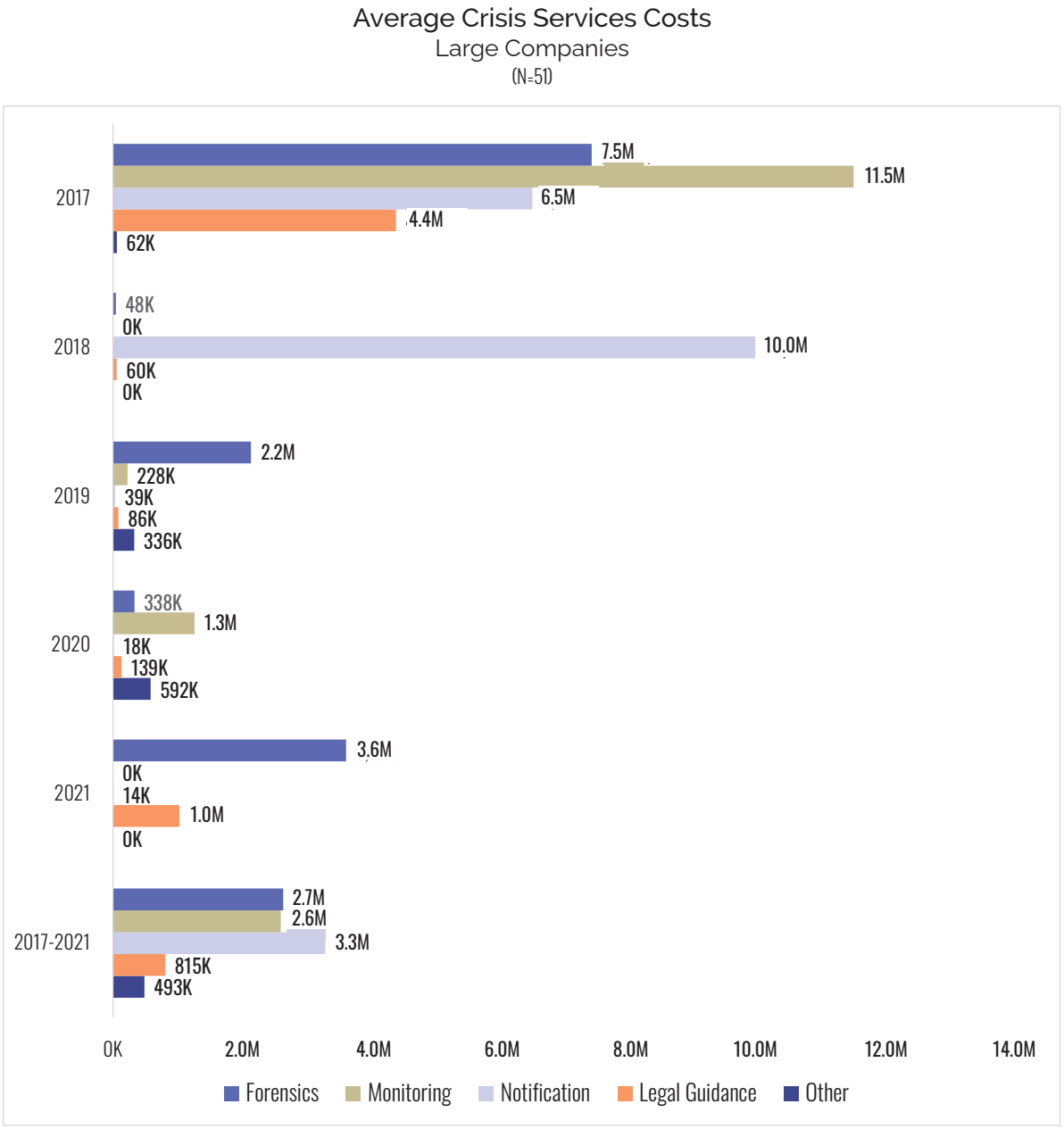

Average Crisis Services Costs
Large Companies
(N=51)
2017
7.5M
11.5M
6.5M
4.4M
62K
2018
48K
0K
10.0M
60K
0K
2019
2.2M
228K
39K
86K
336K
2020
338K
1.3M
18K
139K
592K
2021
3.6M
0K
14K
1.0M
0K
2017-2021
2.7M
2.6M
3.3M
815K
493K
0K
2.0M
4.0M
6.0M
8.0M
10.0M
12.0M
14.0M
Forensics
Monitoring
Notification
Legal Guidance
Other

Figure 18

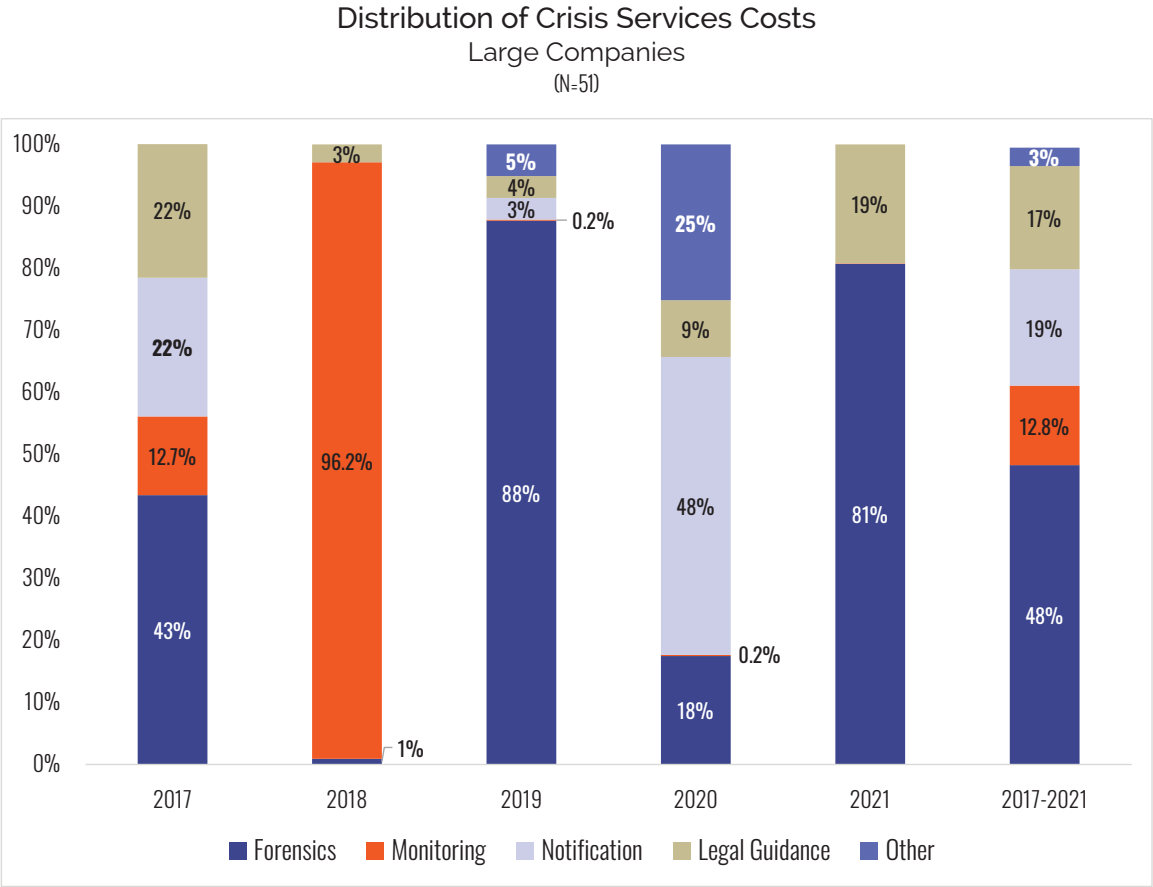

Distribution of Crisis Services Costs
Large Companies
(N=51)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
22%
22%
12.7%
43%
3%
96.2%
1%
5%
4%
3%
0.2%
88%
25%
9%
48%
0.2%
18%
19%
81%
3%
17%
19%
12.8%
48%
2017
2018
2019
2020
2021
2017-2021
Forensics
Monitoring
Notification
Legal Guidance
Other

Figure 19

Business Interruption (BI) and Recovery Expense

SMEs

BI costs were reported for 299 incidents. Since 2018, the average BI cost and corresponding average Incident Cost have increased, dramatically since 2020.

The five-year average Incident Cost of a claim that involved BI was almost four times greater than a claim that did not involve BI. In 2021, the average claim involving BI was almost seven times greater than one that did not.

Ransomware incidents at SMEs accounted for 87% of claims with a BI component. The five-year average BI cost for Ransomware incidents averaged $321K. The corresponding Total Incident Cost was $623K. In 2021, these numbers were $756K and $1.4M, respectively.

Large Companies

Figure 21 depicts Average BI and Total Incident Cost at Large Companies. Since there are only 10 incidents in our dataset, there is not much to be said other than that the reader should be careful not to extrapolate too much from the graph.

Average Business Interruption Costs
SMEs
(N=299)

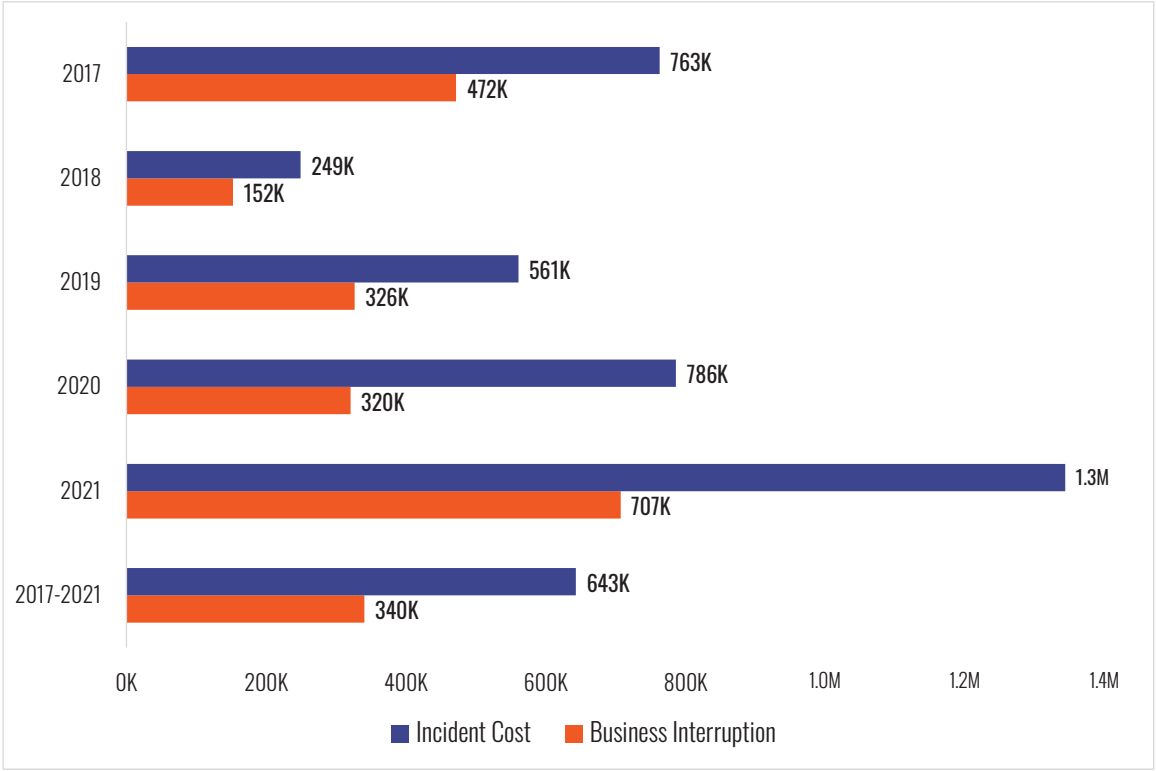


Figure 20

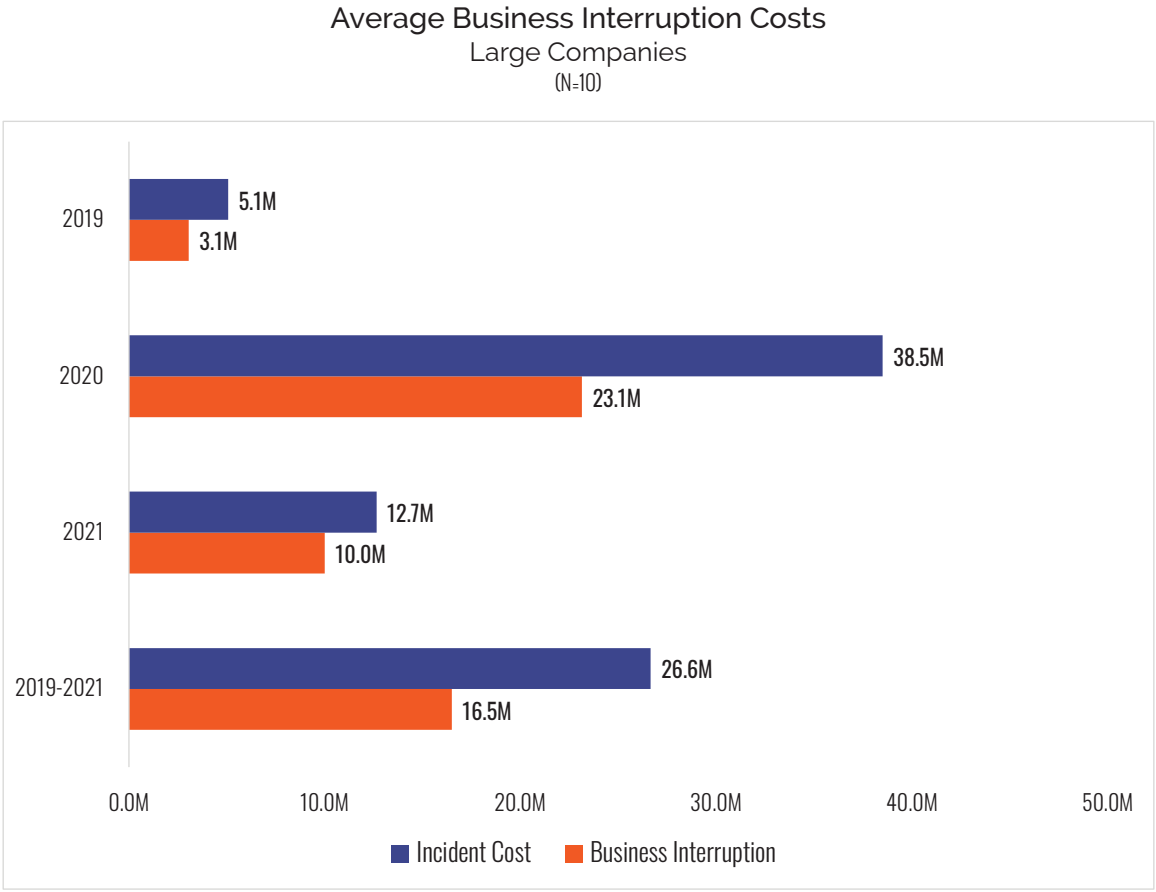

Average Business Interruption Costs
Large Companies
(N=10)
2019
5.1M
3.1M
2020
38.5M
23.1M
2021
12.7M
10.0M
2019-2021
26.6M
16.5M
0.0M
10.0M
20.0M
30.0M
40.0M
50.0M
Incident Cost
Business Interruption

Figure 21

Recovery Expense

SMEs

There were 281 claims in the dataset that reported Recovery Expense. As Figure 22 shows, Recovery Expense has been steadily increasing since 2017, 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 2021, the Incident Cost was over 300% greater when Recovery Expense was incurred.

Ransomware incidents accounted for 84% of the claims with Recovery Expense reported. The five-year average Incident Cost of these events was almost 200% higher than incidents without Recovery Expense. In 2021, these incidents cost almost four times more.

Large Companies

There were only five Large Company claims that reported Recovery Expense. Four of these were due to ransomware and one was due to malware. The five-year average recovery expense was $1.3M and the average Total Incident Cost was $9.9M. In 2021, there was only one small claim (<$25K) with a Recovery Expense listed.

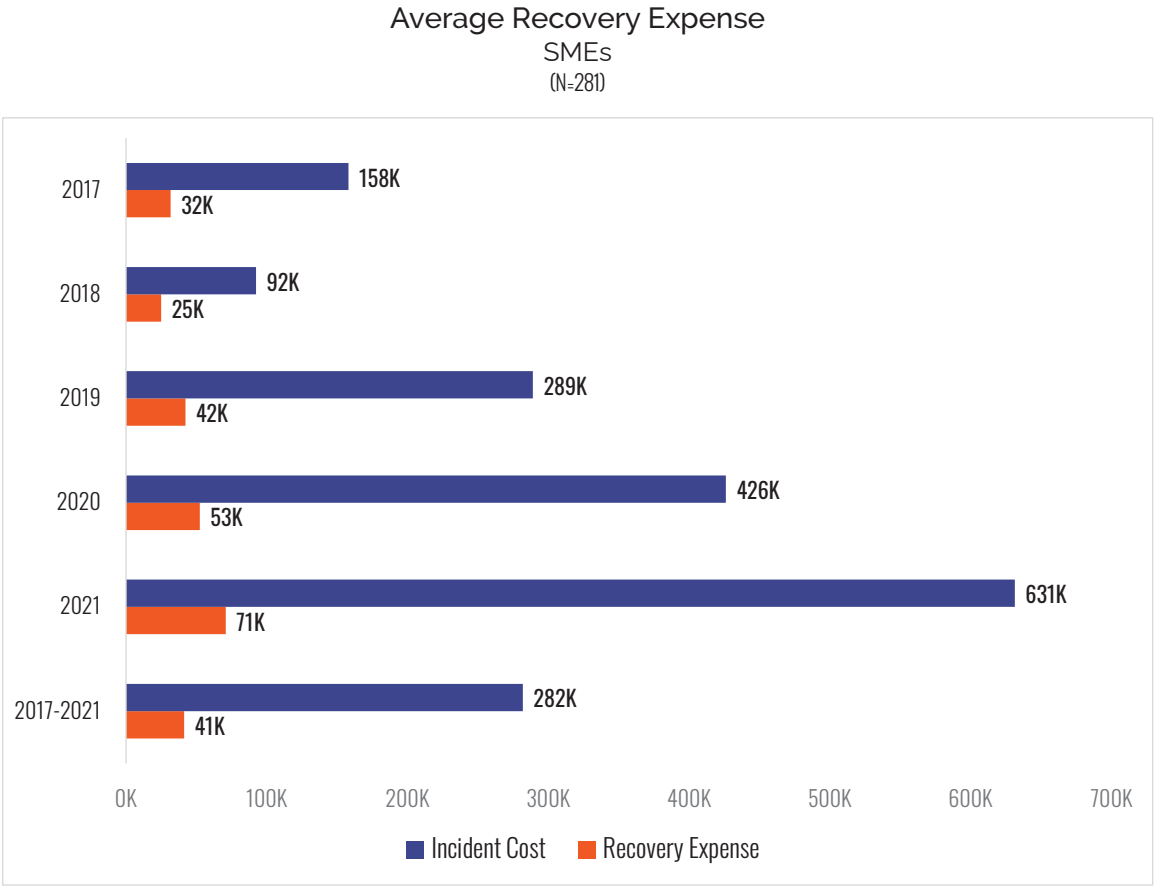


Figure 22

Legal Costs

SMEs

There were 379 claims in the dataset that reported at least one type of legal or litigation expense. Figure 23 below depicts the year-by-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 only 11 claims that reported at least one type of legal or litigation expense. For the five-year period, the overall average was $3.1M, with a maximum of $21M.

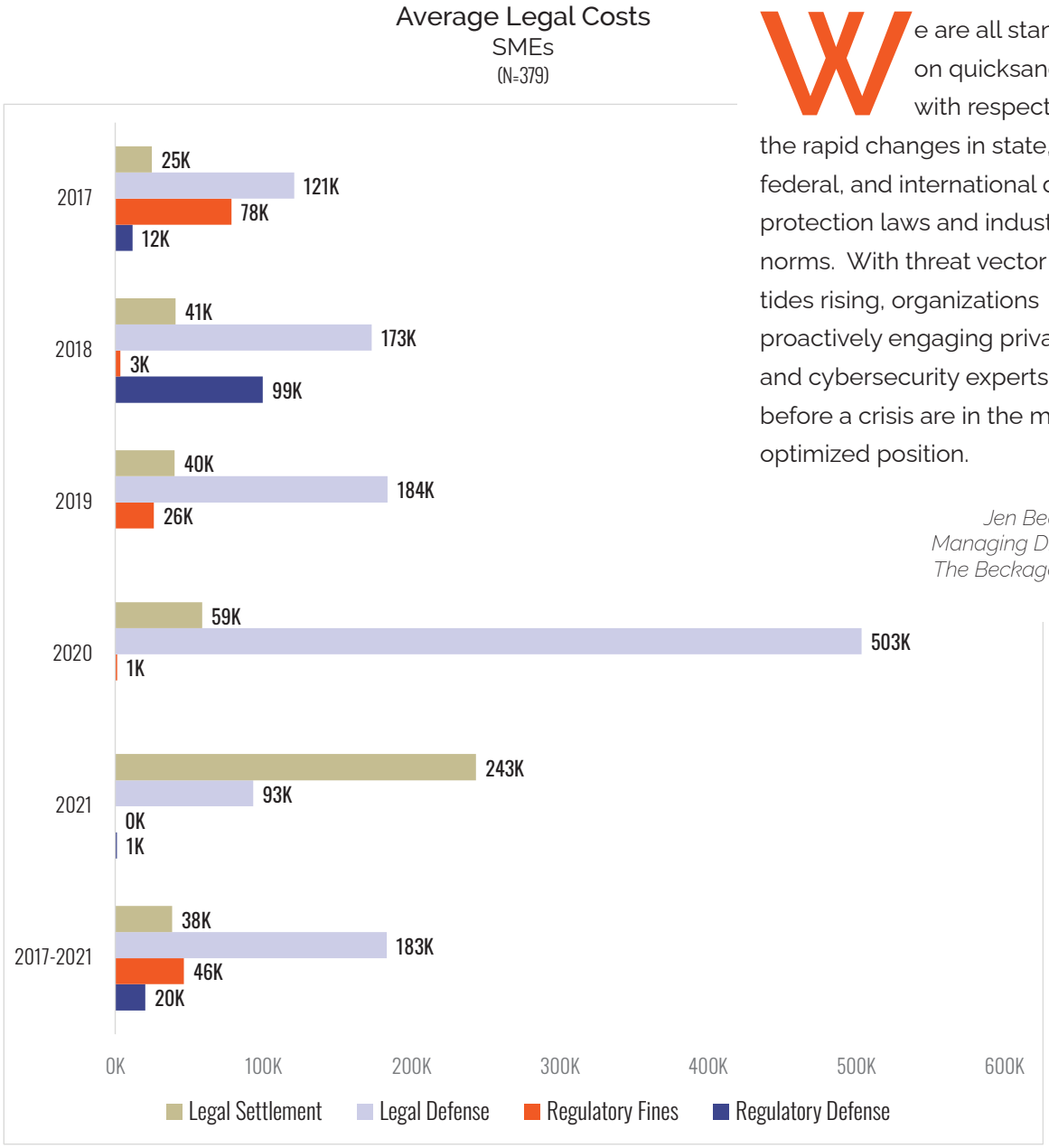


Figure 23

> We are all standing on quicksand with respect to the rapid changes in state, federal, and international data protection laws and industry norms. With threat vector tides rising, organizations proactively engaging privacy and cybersecurity experts before a crisis are in the most optimized position.
>
> *Jen Beckage*
> *Managing Director*
> *The Beckage Firm*

Records Exposed

There were 755 claims that reported the number of records exposed in an incident. This represents a decrease from the previous five-year number of claims (N=895). While we cannot say for certain why this was the case, we can speculate that it was due to the large number of Ransomware and BEC events reported in 2020 and 2021.

These 755 incidents exposed over 1.1 billion records: 265M at SMEs and 852M at Large Companies

Figures 24 and 25 show the year-over-year and five-year average number of records exposed. There is no particular pattern to be seen. As mentioned in the introduction, the number of records exposed does not correlate with either the size of an organization or the Total Incident Cost.

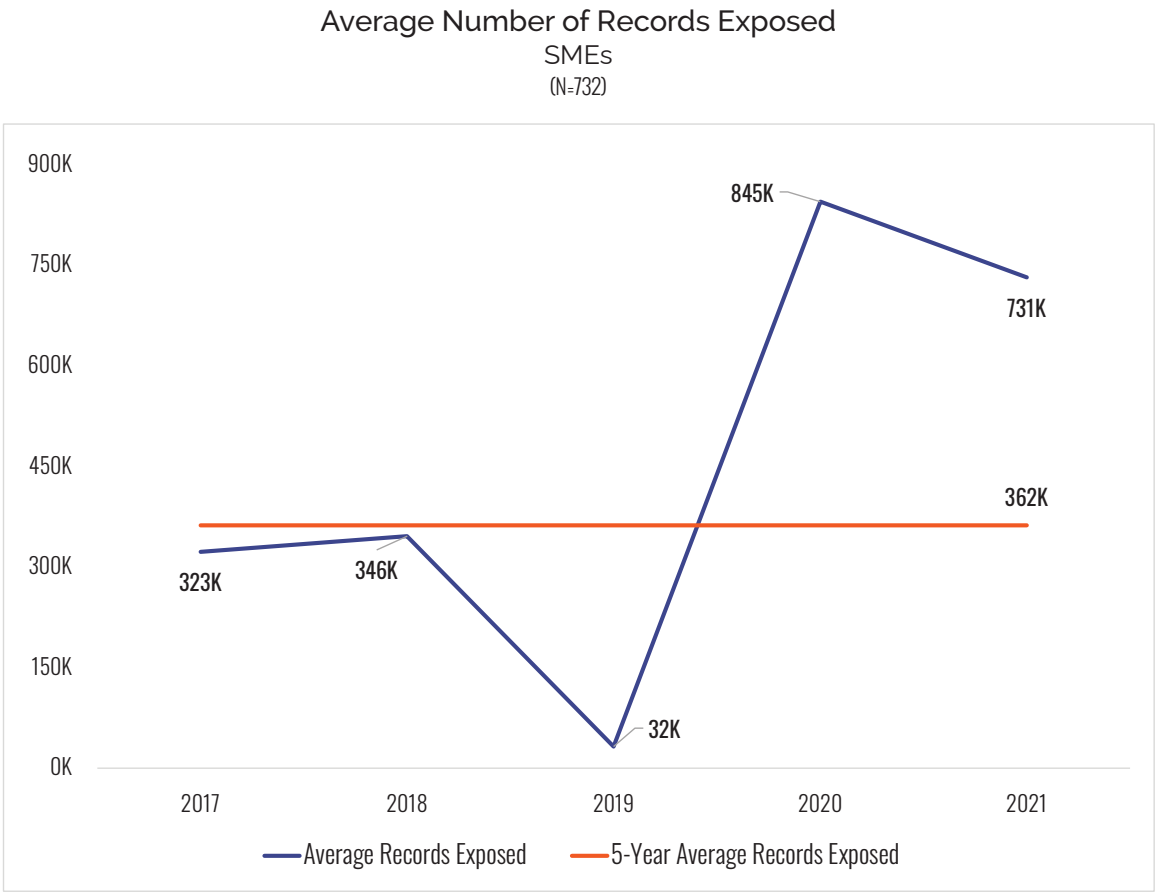


Figure 24

We're getting more last-minute notification jobs. For example, only three days before launch versus a week. Conversely, some organizations are notifying 60 days from discovery only to those who they must notify based on their event circumstances— determining the smallest affected population to inform could be why some are taking more time to notify.

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

Average Number of Records Exposed
Large Companies
(N=23)

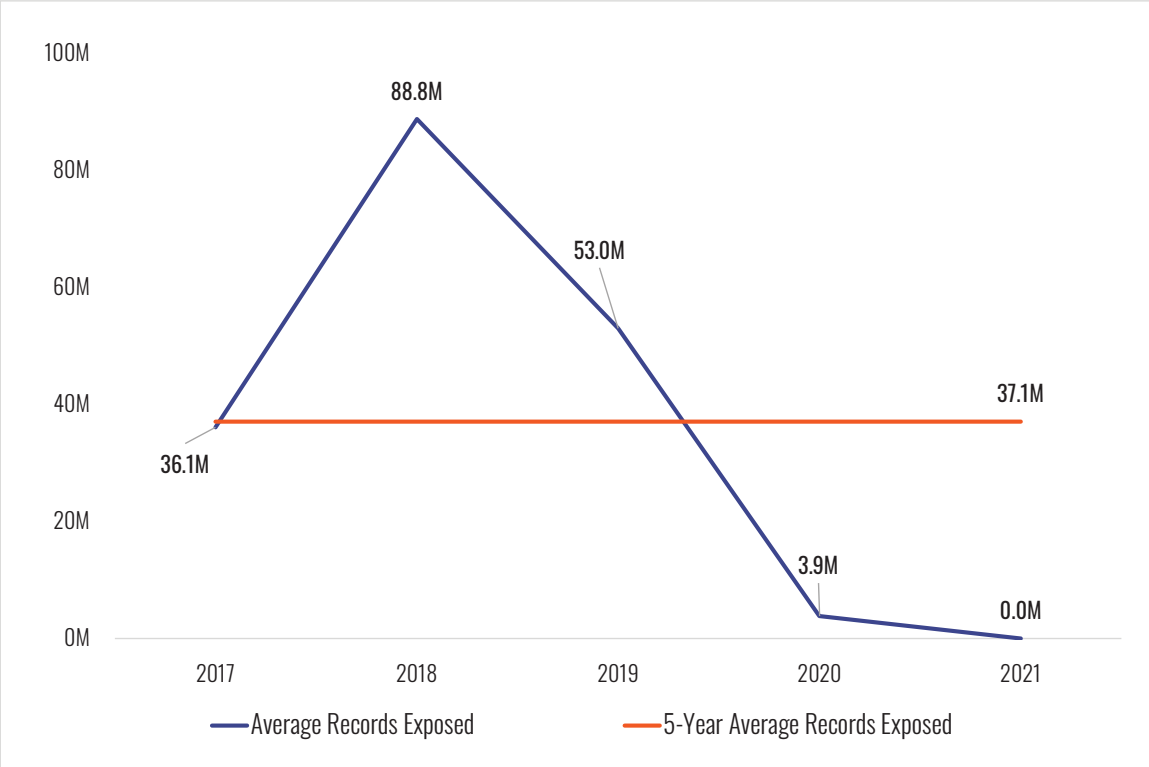


Figure 25

Recordless Claims and Claims with Exposed Records

"Recordless" claims are incidents that do not expose records. Ransomware, wire transfer fraud, business email compromise (BEC), and distributed denial of service (DDoS) accounted for most of these incidents. In this year's report, these incidents accounted for 80% in 2021 and 72% of claims over five years. This large increase in the proportion of recordless incidents was primarily due to the increased number of ransomware claims in 2020 and 2021.

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

As Figure 26 shows, incidents that expose records are more costly than those that do not.

Average Incident Costs – Records Exposed vs Recordless
SMEs
(N=4,155)

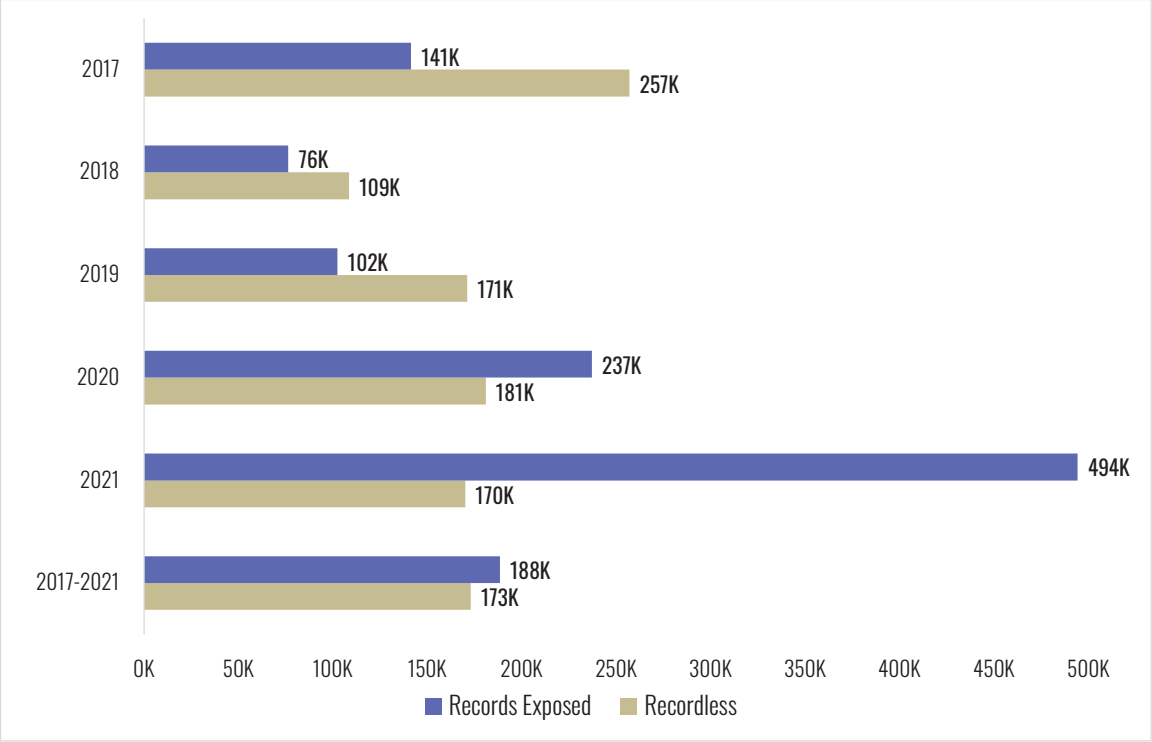


Figure 26

Criminal and Non-Criminal Activities

Criminal activities include:

- Hacking
- Ransomware
- Malware/virus
- Social engineering
- Business email compromise (BEC)
- Phishing
- Distributed denial of service (DDoS) attacks
- Stolen devices
- Theft of money by wire transfer
- 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 at SMEs caused by criminal activities ranged from a high of 96% in 2021 to a low of 73% in 2018. The proportion of claims caused by non-criminal activities decreased from 7% in 2020 to 4% in 2021.

Criminal incidents were much more costly on average than non-criminal incidents. Year over year, the difference ranged from approximately 200% to over 400%. Over five years, the difference was about 270%.

Criminal vs Non-Criminal – Percentage of Claims
SMEs
(N=6,098)

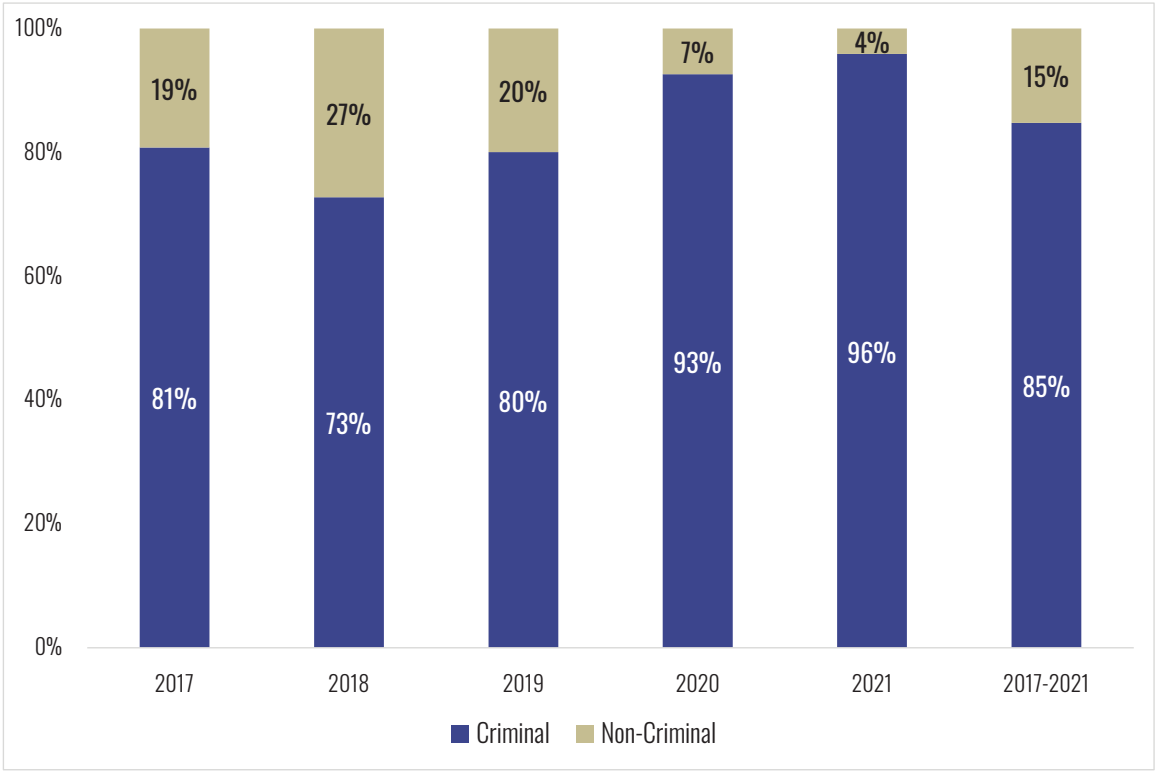


Figure 27

Criminal vs Non-Criminal – Average Costs
SMEs
(N=6,098)

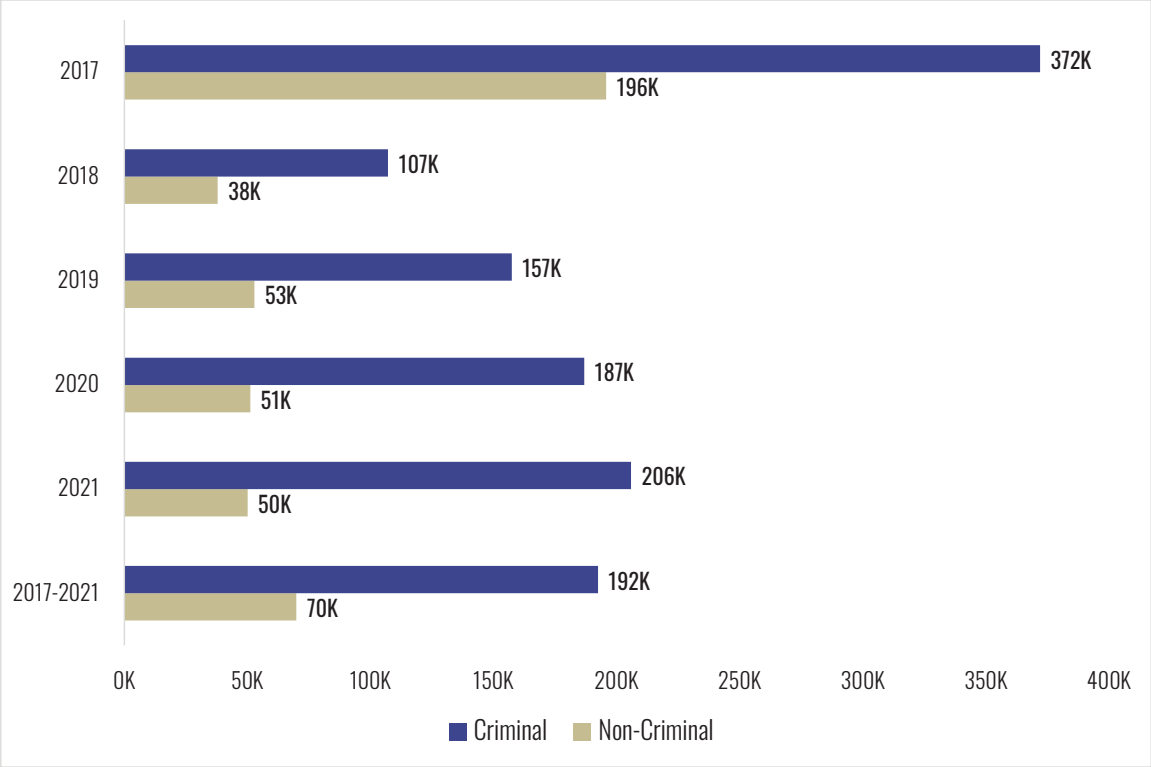


Figure 28

Criminal vs Non-Criminal – Costs
SMEs
(N=6,098)

Time Period	Impact	Type of Activity	Average	Maximum	Total
2021	Records Exposed	Criminal	668K	16.0M	37.4M
		Non-Criminal	2.5M	5.0M	5.0M
	Crisis Services	Criminal	131K	11.4M	86.6M
		Non-Criminal	36K	318K	1.2M
	Incident Cost	Criminal	206K	15.0M	200.3M
		Non-Criminal	50K	468K	2.1M
2017-2021	Records Exposed	Criminal	430K	80.0M	254.0M
		Non-Criminal	81K	5.0M	11.0M
	Crisis Services	Criminal	121K	120.2M	454.4M
		Non-Criminal	26K	1.0M	12.3M
	Incident Cost	Criminal	192K	120.2M	994.5M
		Non-Criminal	70K	17.5M	65.0M

Table 1

Criminal activity was involved in 86% of incidents reported at Large Companies. As Figure 29 shows, the cost of criminal incidents was dramatically higher than non-criminal ones.

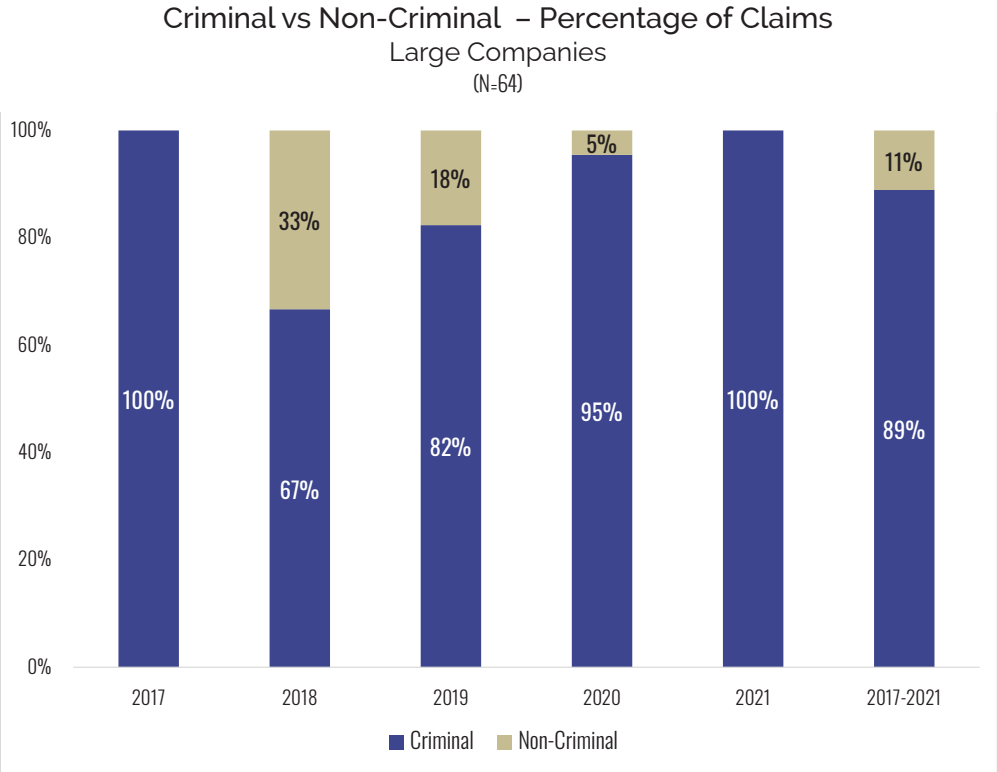


Figure 29

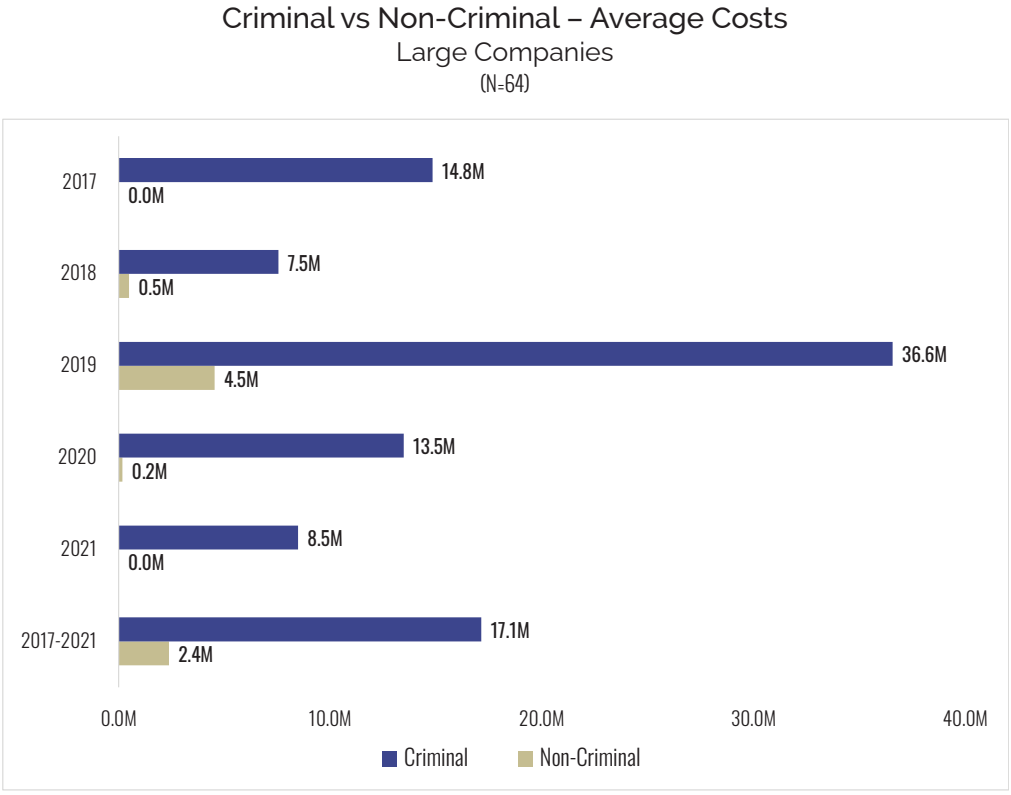
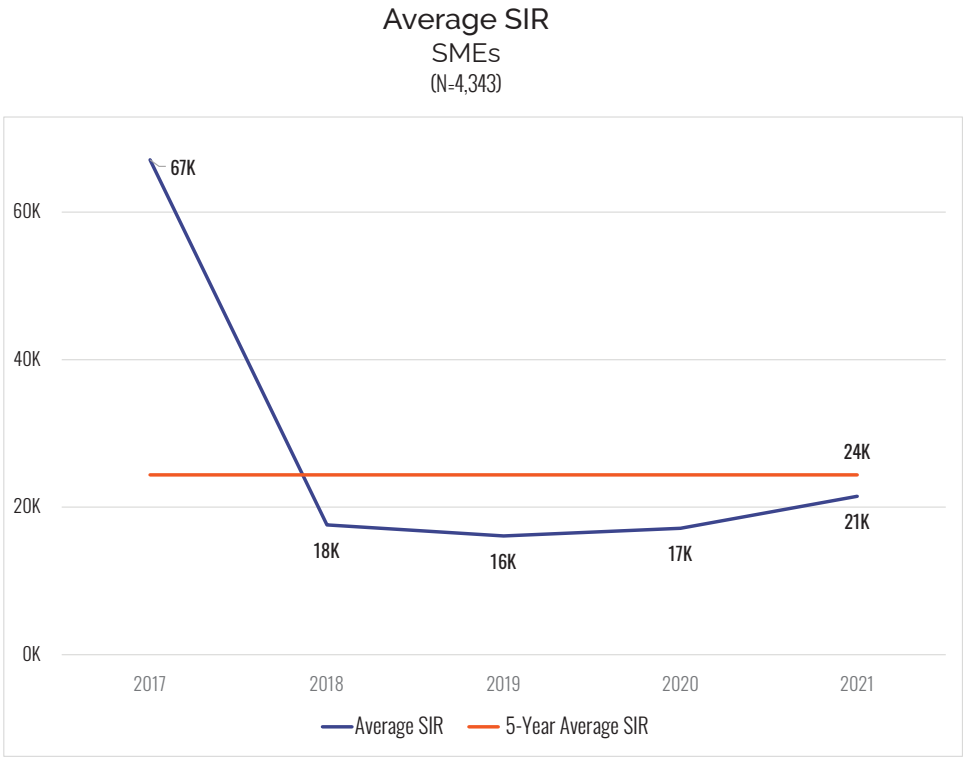


Figure 30

Self-Insured Retentions (SIR)

The dataset contained 4,343 claims for SMEs that reported a non-zero amount for SIR. These amounts ranged from <$100 to $10M.

The dataset also contained 65 claims for Large Companies that reported a non-zero amount for SIR. These amounts ranged from $5K to $10M.



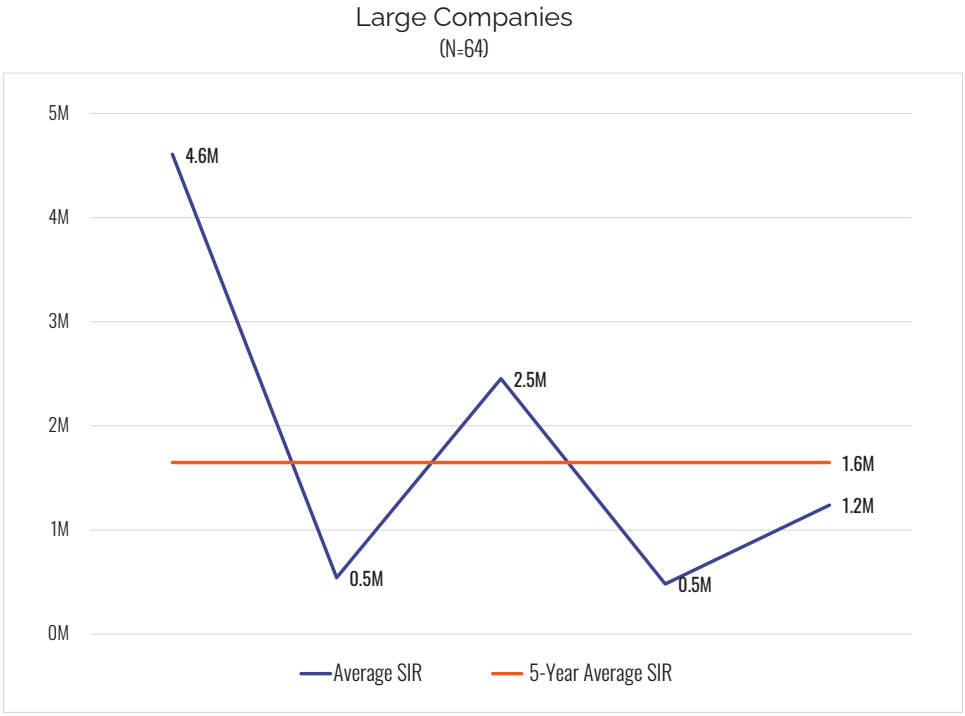


Figure 31

Causes of Loss

The top five causes of loss at SMEs were:

- Ransomware
- Business Email Compromise (BEC)
- Hackers
- Cyber Events – Unspecified
- Staff Mistakes

Losses in these five categories accounted for 71% of claims and 84% of Total Incident Cost ($901M). For metrics on all sectors, please see the graphs and tables in the appendices.

Top Causes of Loss – SMEs
Number of Claims, Total Incident Cost, % of Total Incident Cost
(N=4,343)

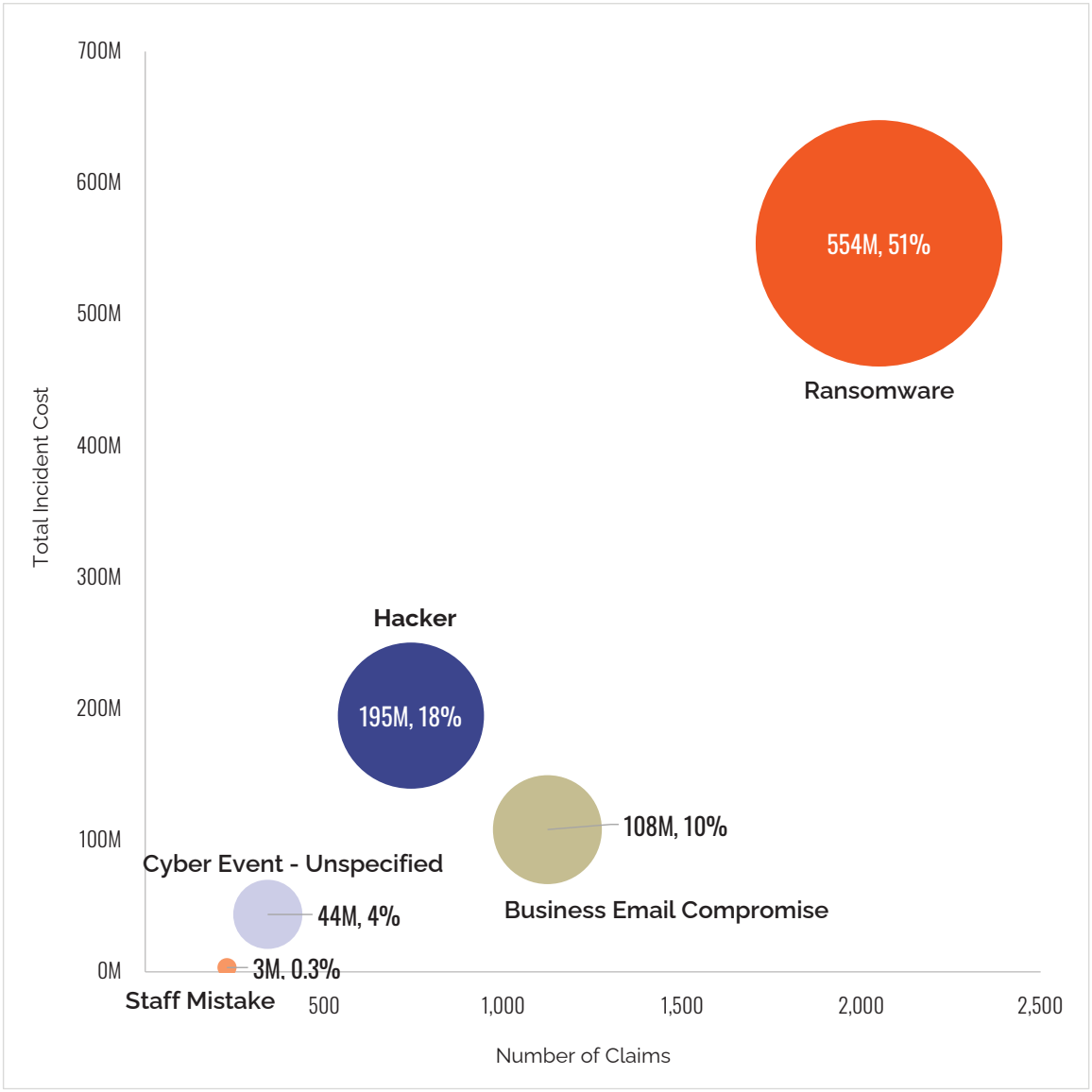


Figure 32

Ransomware

The number of ransomware incidents increased from 254 in 2017 to 559 in 2020. For 2021, the number stands at 359 so far, with additional incidents to be added to the total in the 2023 and 2024 cyber claims reports[1].

Ransom amounts and total incident costs have also increased dramatically over the past five years. Our analysis looks at ransomware incidents in two ways:

- The overall cost of a ransomware event even when the ransom amount was not provided (over 2,000 incidents)
- The subset of ransomware events for which the ransom amount is known (over 800 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 of these approaches, for both SMEs and Large Companies.

1 Each year, we collect data from the three previous years. For this report (2022) we collected claims for 2019-2021. We will continue to collect claims for incidents in 2021 for two more years.

Average Incident Cost – All Ransomware Claims
SMEs
(N=2,049)

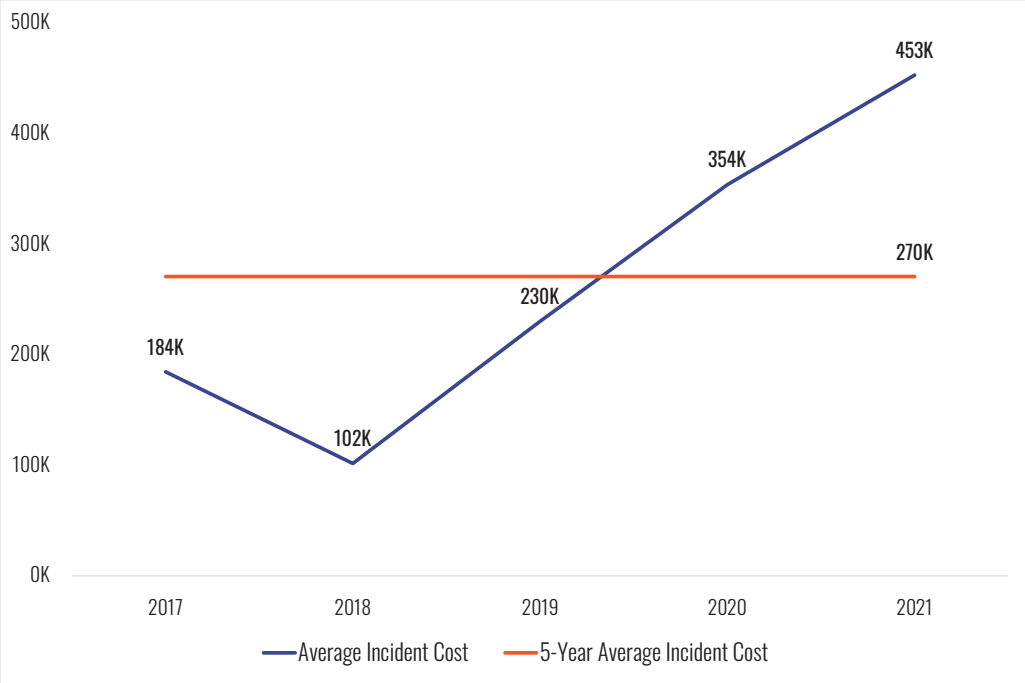


Figure 33

Average Incident Cost – Ransomware Claims where Ransom Amount is Known
SMEs
(N=816)

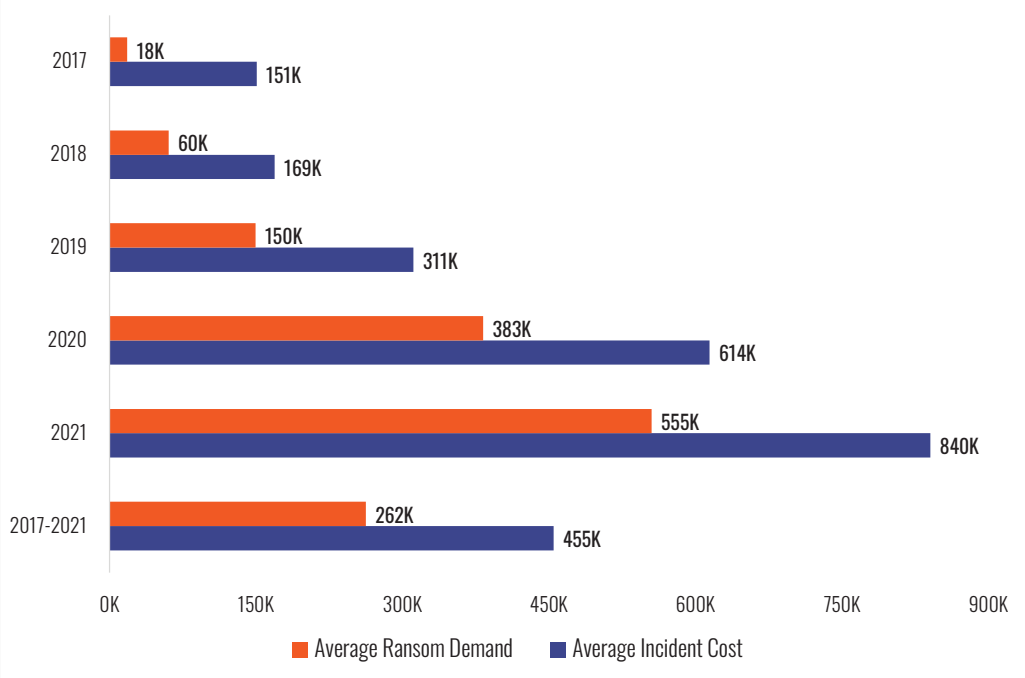


Figure 34

Average Incident Cost – All Ransomware Claims
Large Companies
(N=25)

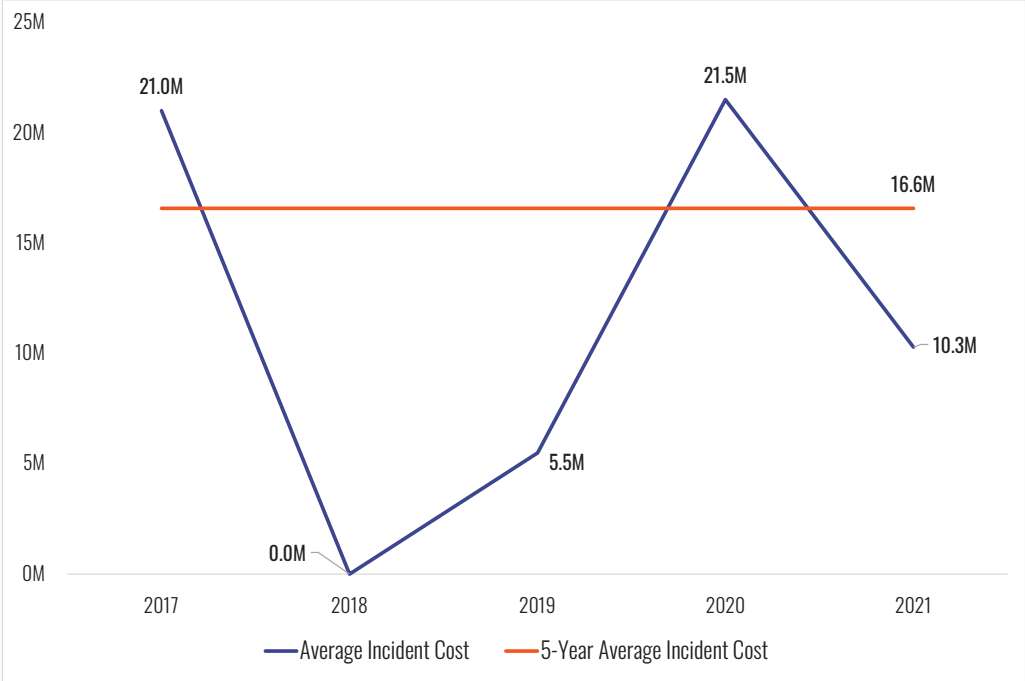


Figure 35

Average Incident Cost – Ransomware Claims where Ransom Amount is Known
Large Companies
(N=9)

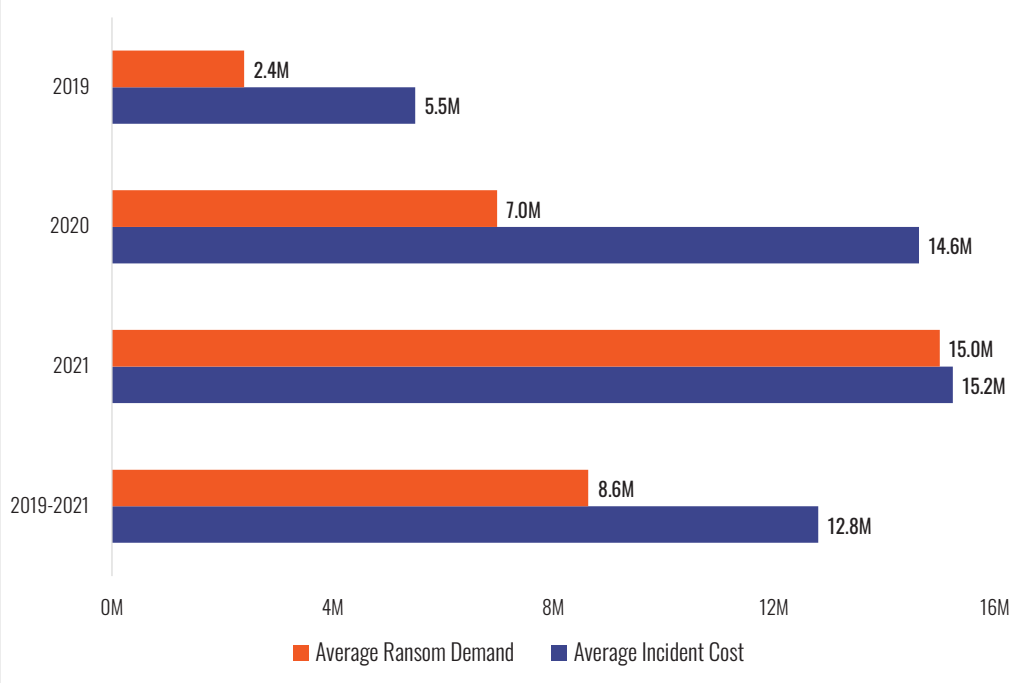


Figure 36

Business Email Compromise (BEC)

BEC was the second leading cause of loss at SMEs. The number of BEC claims increased from 80 in 2017 to almost 300 in 2021. As is the case with Ransomware (noted above), the number of BEC claims collected for 2021 will increase over the next two years.

> Business email compromise is a growing and critical attack vector which drives ransomware and data breach incidents. Noticing BEC trends over the past few years, Guidewire Cyence invested in developing new exposure signals that directly relate to this vulnerability and has embedded them into its fifth generation predictive model to support a carrier's ability to mitigate this growing threat.
>
> *Maurizio Gobbato*
> *Head of Cyber Catastrophe Modeling*
> *Guidewire*

The cost of BEC incidents has been dropping over the past five-years, from a high of $180K in 2017 to $73K in 2021.

BEC incidents are often accompanied by fraudulent wire transfers. We have identified a small subset of these claims at SMEs and have presented the year-over-year analysis in Figure 38 below.

The year-by-year average Incident Costs were much higher in this subset and the five-year average was nearly 250% higher.

Average Incident Cost – Business Email Compromise
SMEs
(N=1,123)

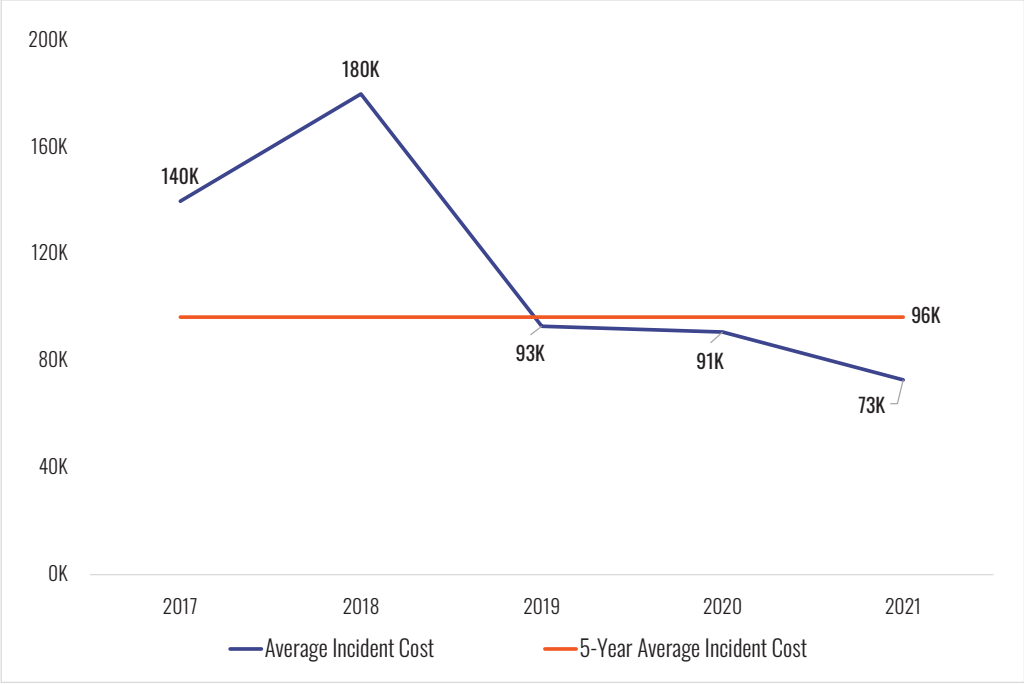


Figure 37

Average Incident Cost – Business Email Compromise with Wire Fraud
SMEs
(N=126)

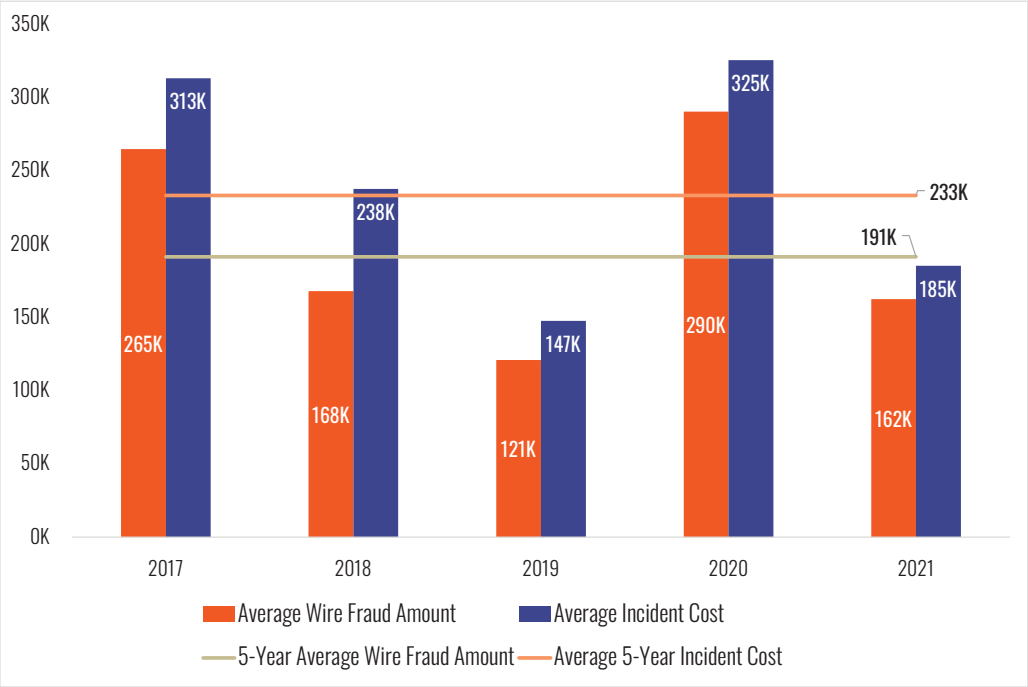


Figure 38

Hackers

Hackers were the third leading cause of loss at SMEs. Figure 39 below 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 2017 and has remained low since then.

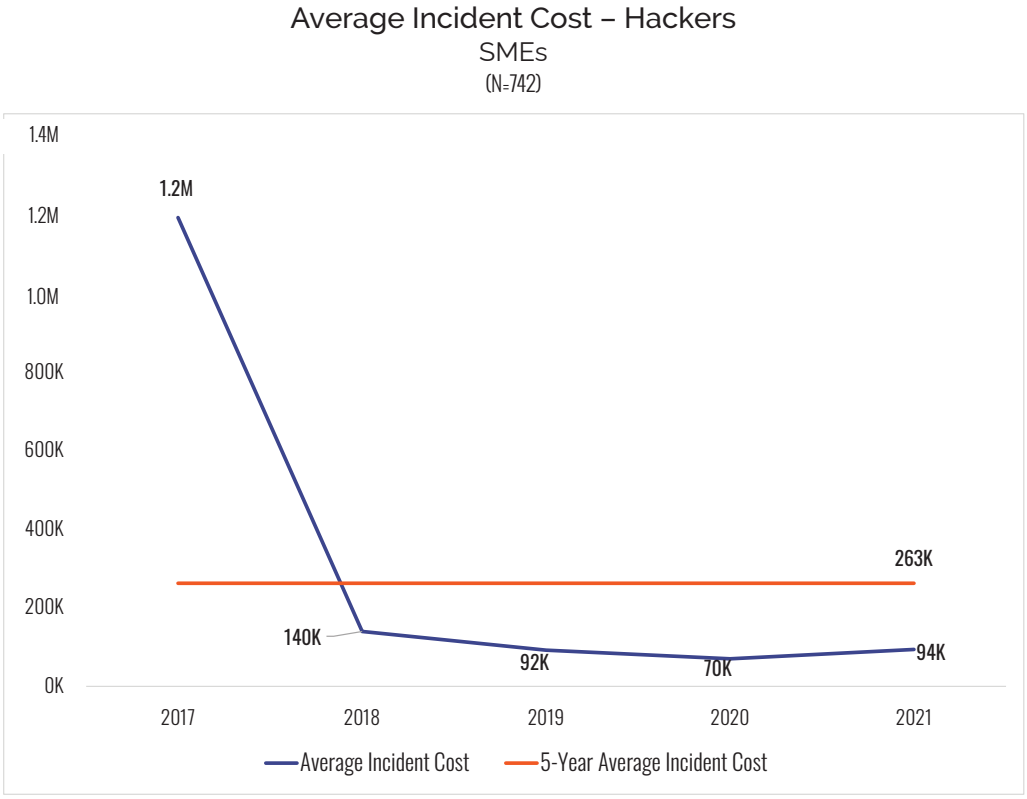


Figure 39

Wire Transfer Fraud, including BEC

Not all Wire Transfer Fraud occurs because of BEC. Figure 40 depicts the year-over-year and five-year averages for Wire Transfer Fraud of all kinds.

Apart from a spike in 2020, the numbers have not changed much since 2017.

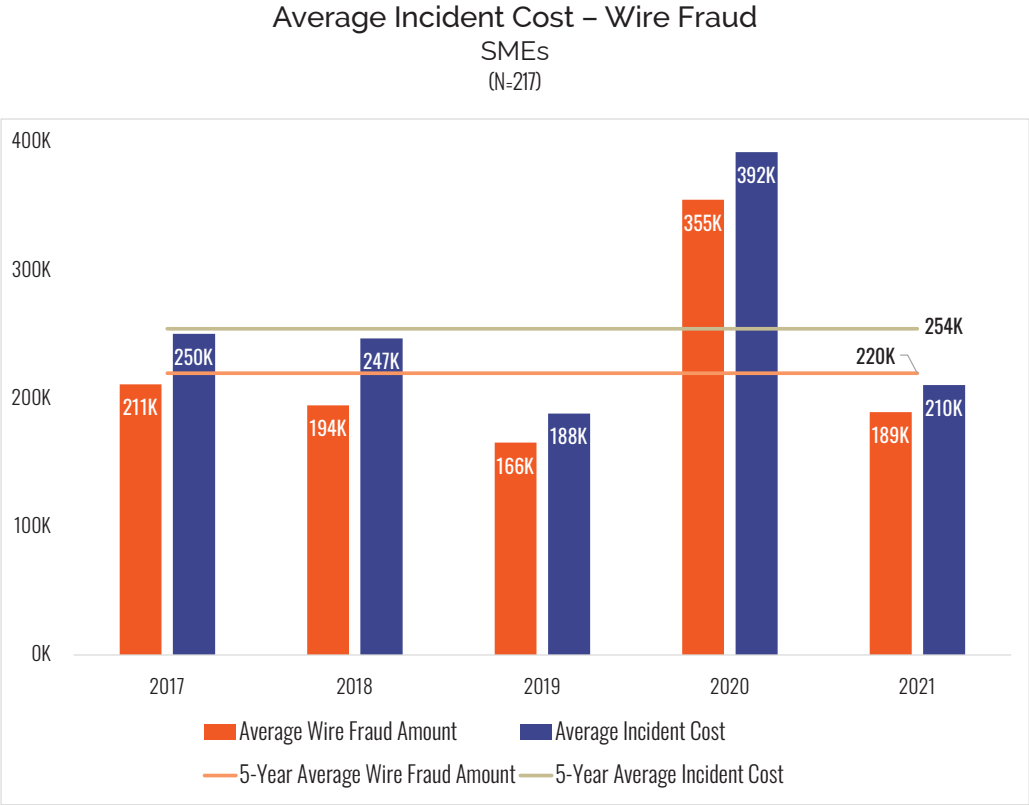


Figure 40

Staff Mistakes

Staff mistakes and Programming Errors were still a notable cause of loss at SMEs.

Fortunately, a not very expensive one, as the figure below shows.

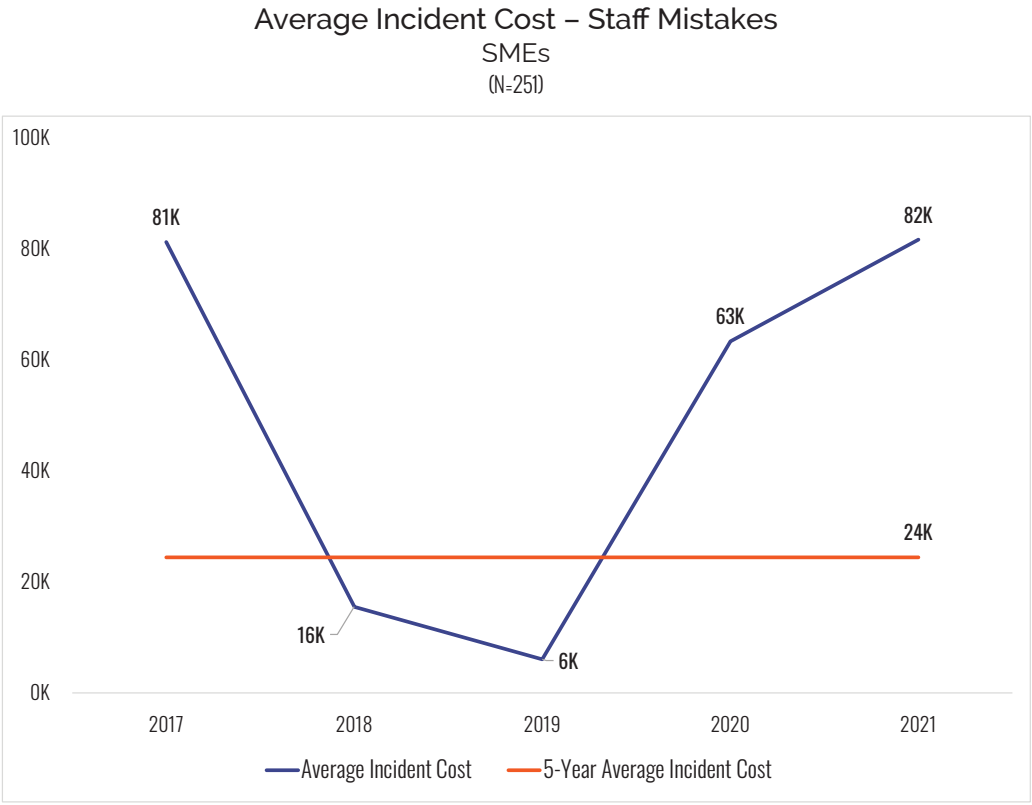


Figure 41

Rogue Employees

Over the past five years, progress has been made at SMEs in dealing with malicious employees, ex-employees, and malicious insiders.

From an average Incident Cost of $255K in 2017, and despite a spike in 2019, the numbers have dropped quite a bit. We will look again next year to see if this trend continues.

Average Incident Cost – Rogue Employees and Malicious Insiders
SMEs
(N=137)

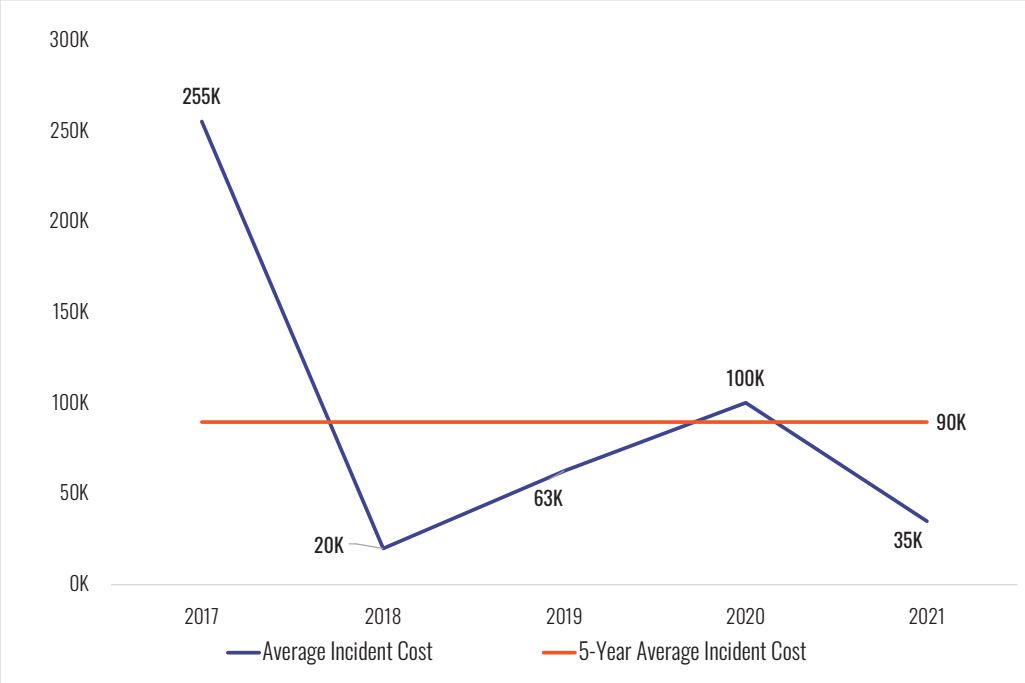


Figure 42

Third Party Incidents

Incidents caused by both malicious and non-malicious actors remain a notable cause of loss. As Figure 43 below shows, with exception of 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 2017, and dramatically so in 2020 and 2021.

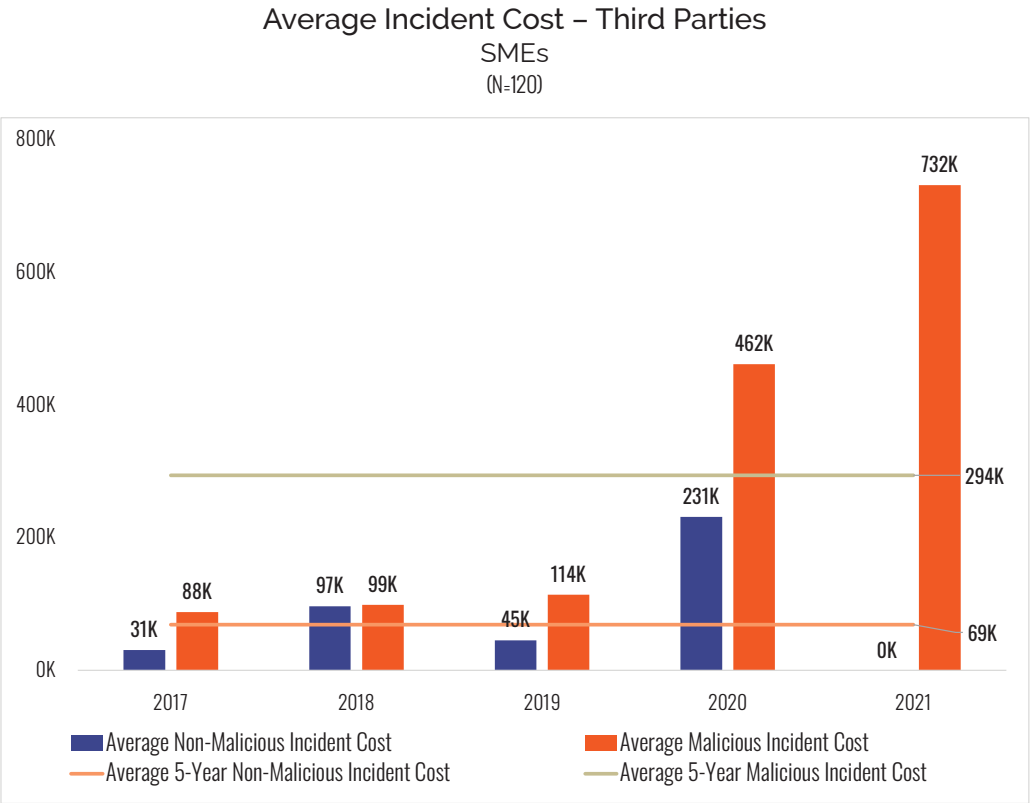


Figure 43

Sectors

As measured by the number of claims over five-years, the top five affected Business Sectors at SMEs are:

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

These five sectors accounted for 66% all claims and 65% of 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 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.

Top Sectors – SMEs
Number of Claims, Total Incident Cost, % of Total Incident Cost
(N=6,339)

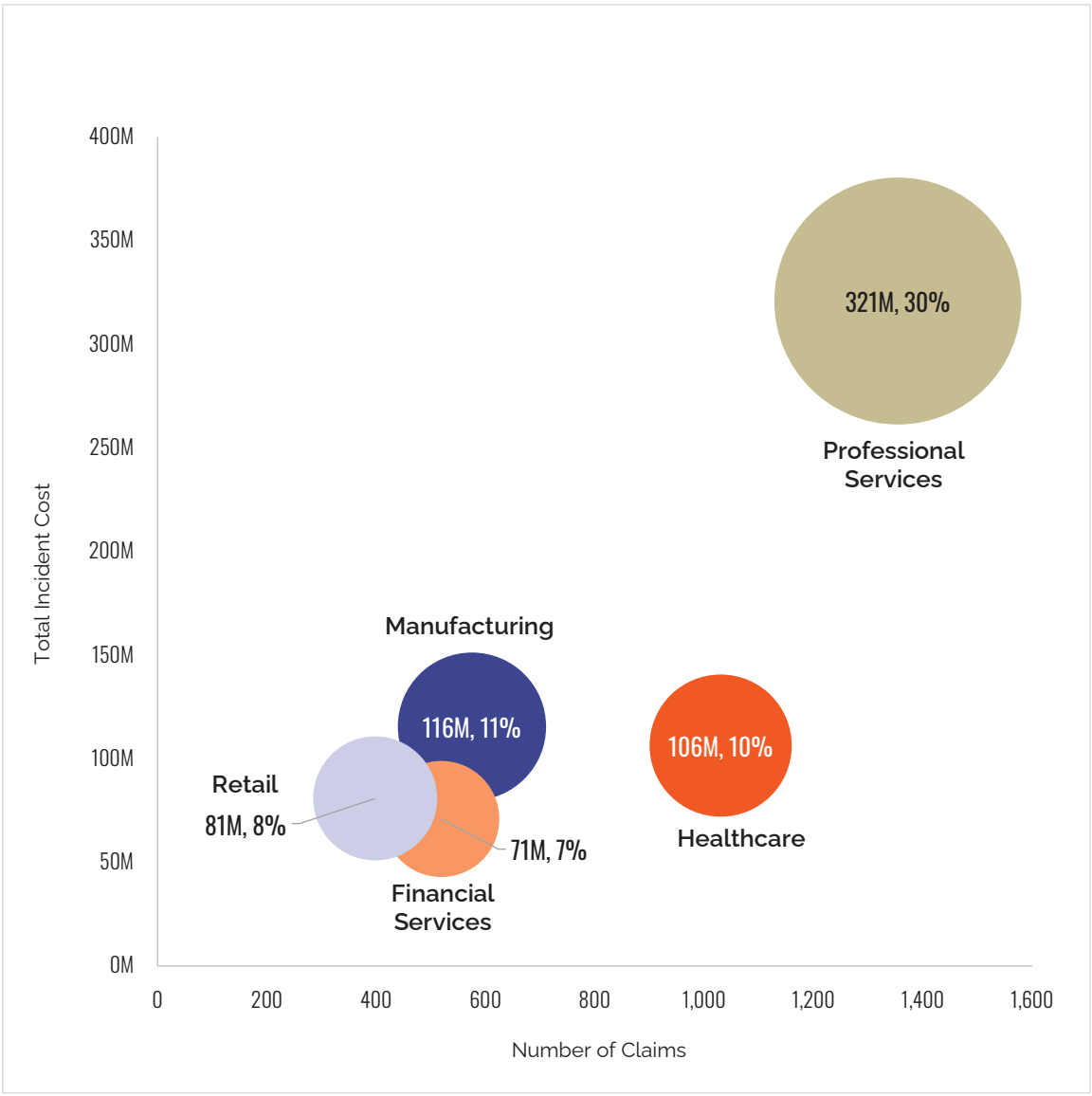


Figure 44

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 annual revenue of these firms was $51M (maximum=$1.5B).

Professional Services claims accounted for 21% of all claims and 30% of Total Incident Costs at SMEs. Total Incident Costs ranged from 1K to over $100M. The top causes of loss were Ransomware, BEC, and Hackers.

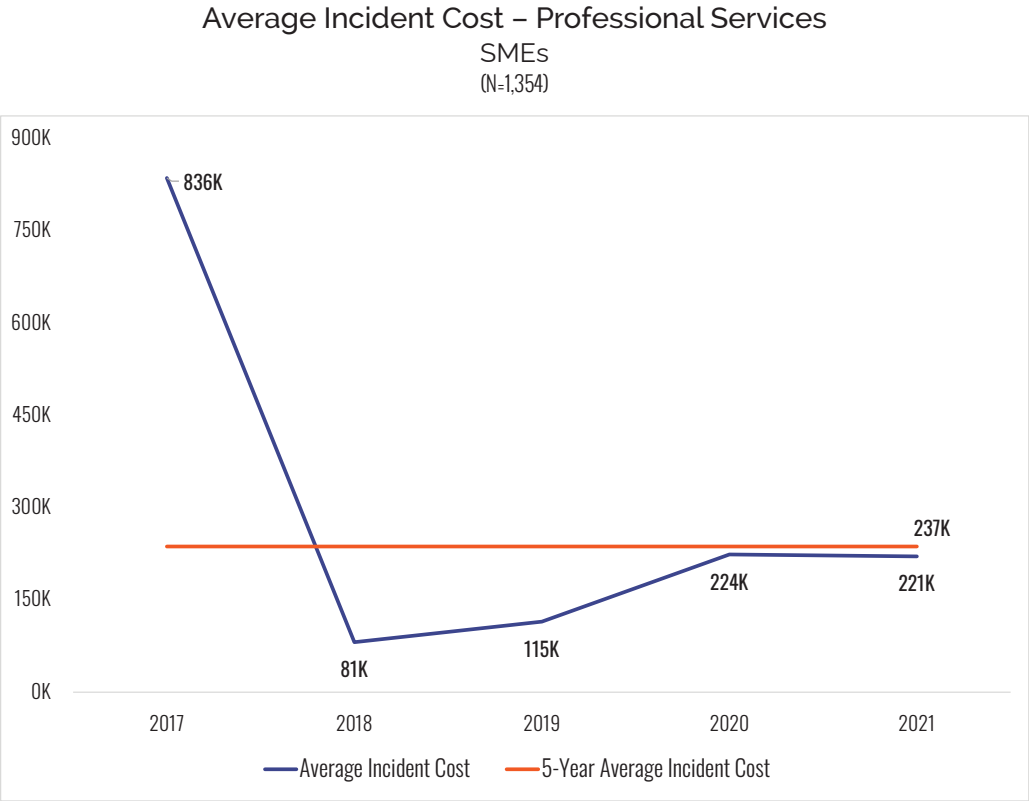


Figure 45

Healthcare

The average annual revenue of organizations in the Healthcare sector was $95M (maximum=$1.4B).

Healthcare claims accounted for 16% of all claims and 10% of Total Incident Cost at SMEs. Total Incident Costs ranged from 1K to over $11M. The top causes of loss were Ransomware, Staff Mistakes, and Hackers.

Figure 46 below shows the year-over-year and five-year average Incident Cost for this sector.

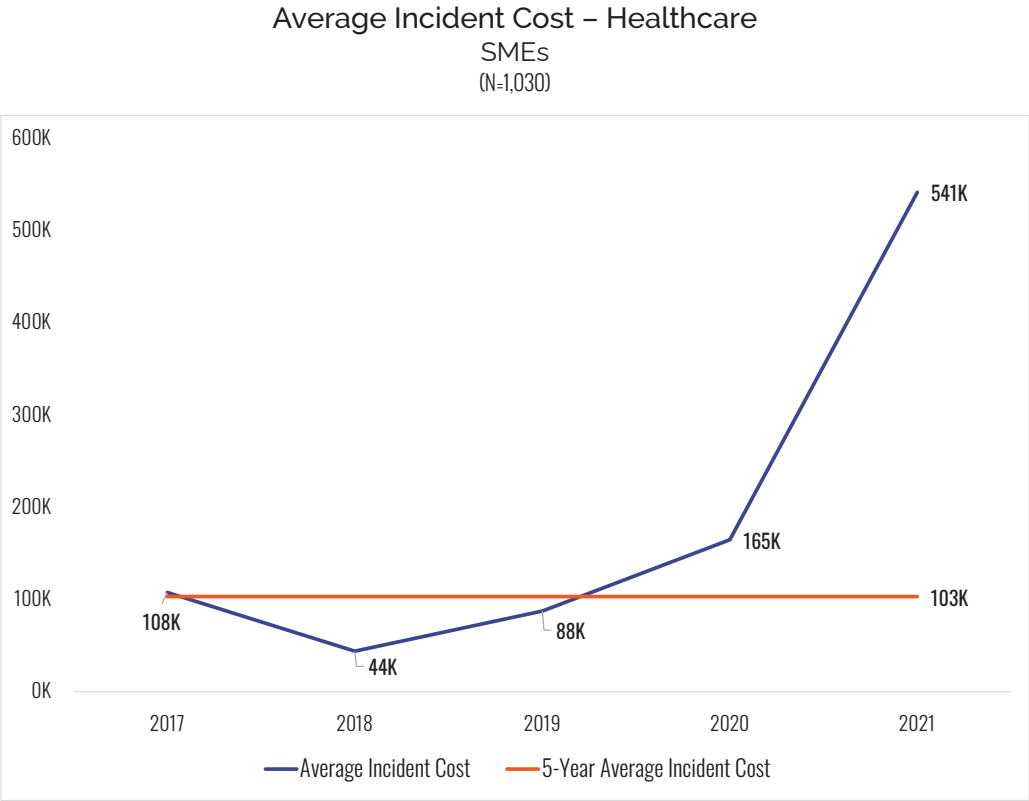


Figure 46

Manufacturing

The average annual revenue of organizations in the Manufacturing sector was $102M (maximum=$1.8B).

Manufacturing claims accounted for 9% of all claims and 11% of Total Incident Cost at SMEs. Total Incident Costs ranged from 1K to $20M. The top causes of loss were Ransomware, BEC, and Malware/Virus.

Figure 47 below shows the year-over-year and five-year average Incident Cost for this sector.

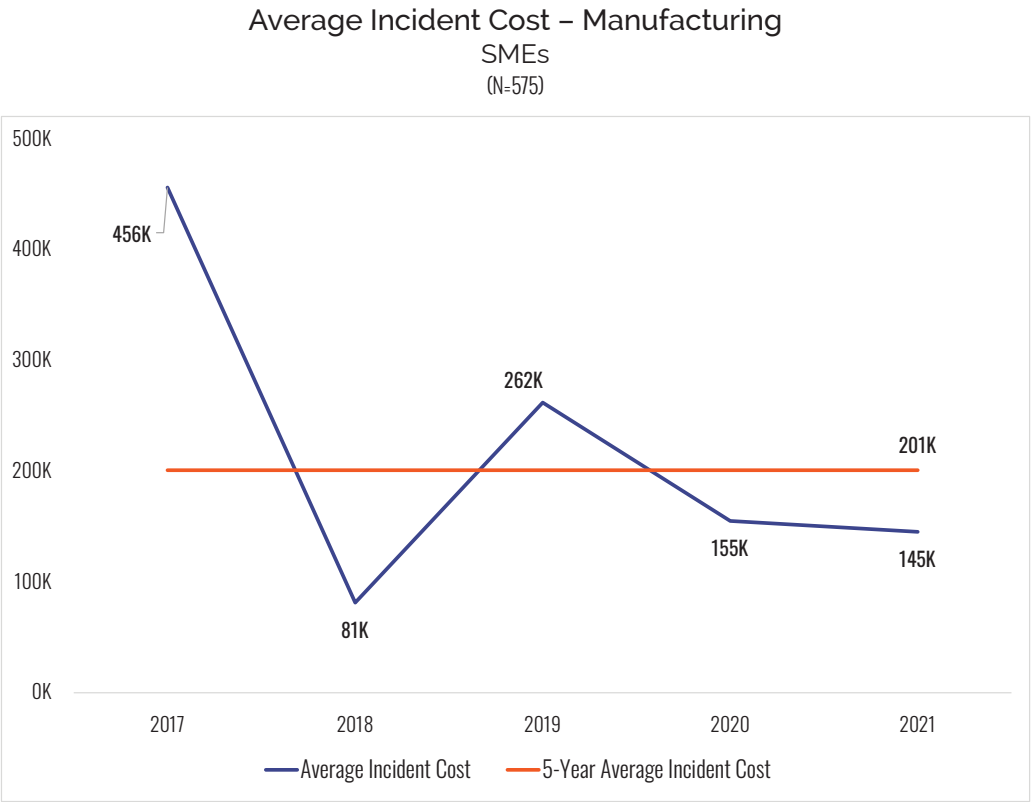


Figure 47

Financial Services

The average annual revenue of organizations in the Financial Services sector was $51M (maximum=$1.7B).

Financial Services claims accounted for 8% of all claims and 7% of Total Incident Cost at SMEs. Total Incident Costs ranged from 1K to $3.7M. The top causes of loss were BEC, Ransomware, and Hackers.

Figure 48 below shows the year-over-year and five-year average Incident Cost for this sector.

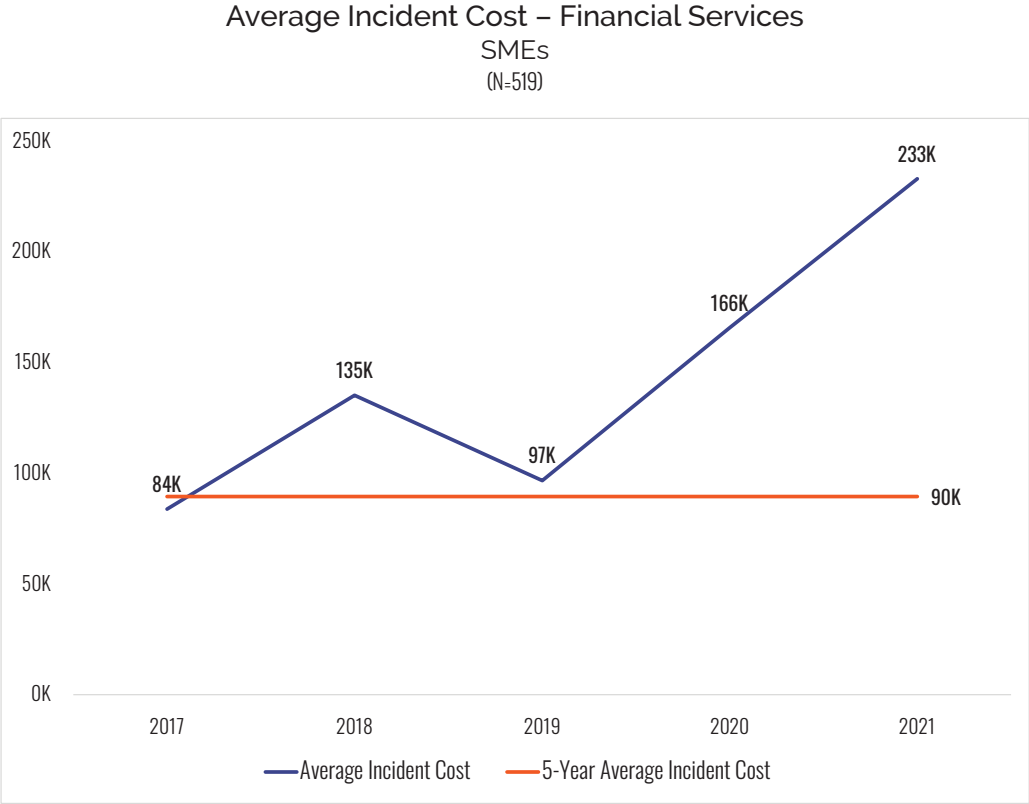


Figure 48

Retail

The average annual revenue of organizations in the Retail sector was $146M (maximum=$1.7B).

Retail claims accounted for 6% of all claims and 8% of Total Incident Cost at SMEs. Total Incident Costs ranged from 1K to $10.7M. Three of the top causes of loss were Ransomware, Hackers, and BEC.

Figure 49 below shows the year-over-year and five-year average Incident Cost for this sector.

Average Incident Cost – Retail
SMEs
(N=398)

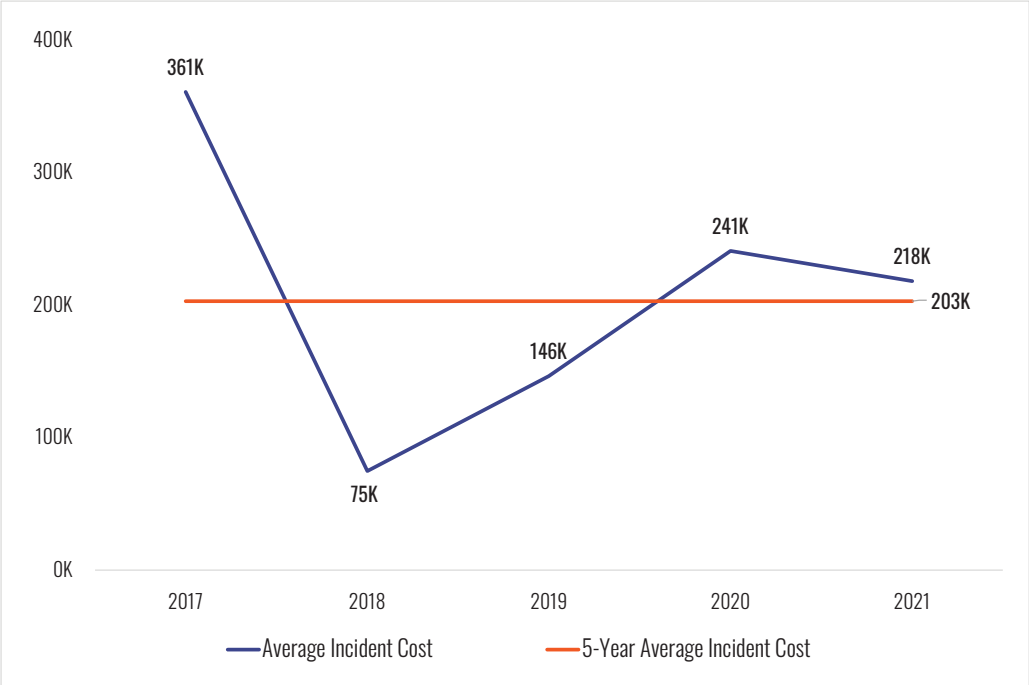


Figure 49

Public Entities

The average annual revenue for Public Entities was $94M (maximum=$909M). Claims from Public Entities represent about 3.5% of all claims and 1.5% of Total Incident Cost (N=7,439).

The average Incident Costs have gone up and down since 2017, with a downward trajectory since 2019. Top causes of loss were Ransomware, Hackers, and BEC.

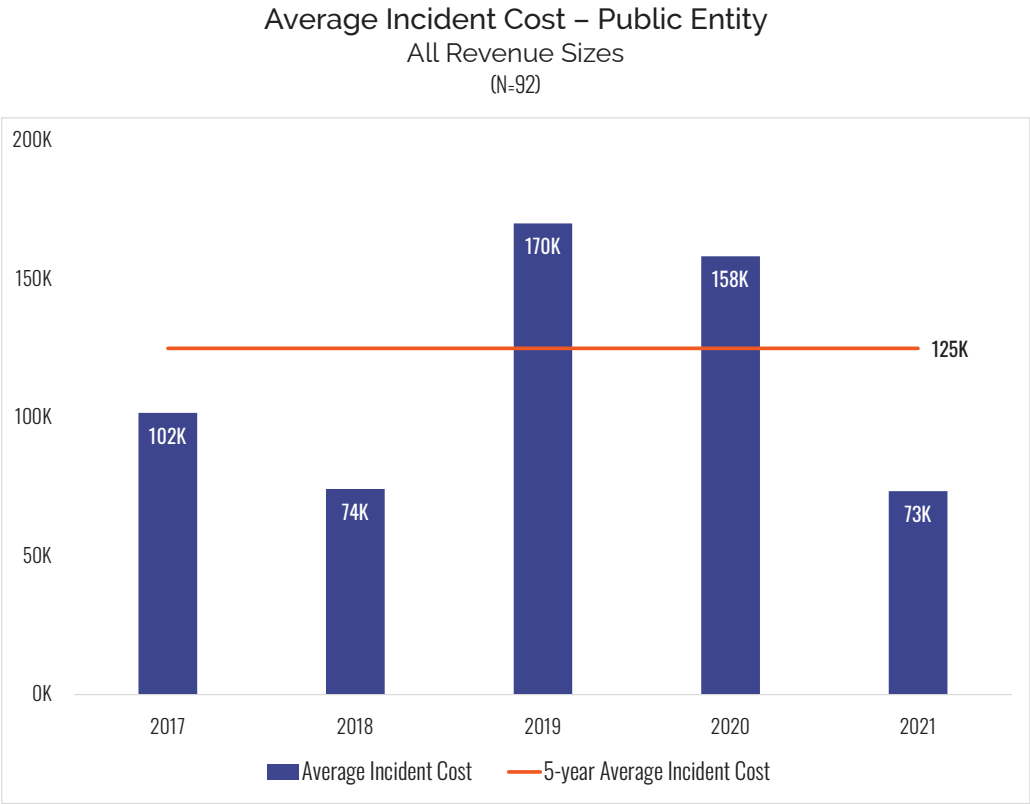


Figure 50

Claims from Canada

Although there were not a large number of claims for incidents in Canada, these incidents represent an important subset of the dataset. The average annual revenue of a Canadian organization in this study was $371M USD (maximum=1.7B USD).

Despite spikes in 2017 and 2019, the trend has been toward decreased average Incident Costs.

Average Incident Cost – Canada
All Revenue Sizes
(N=267)

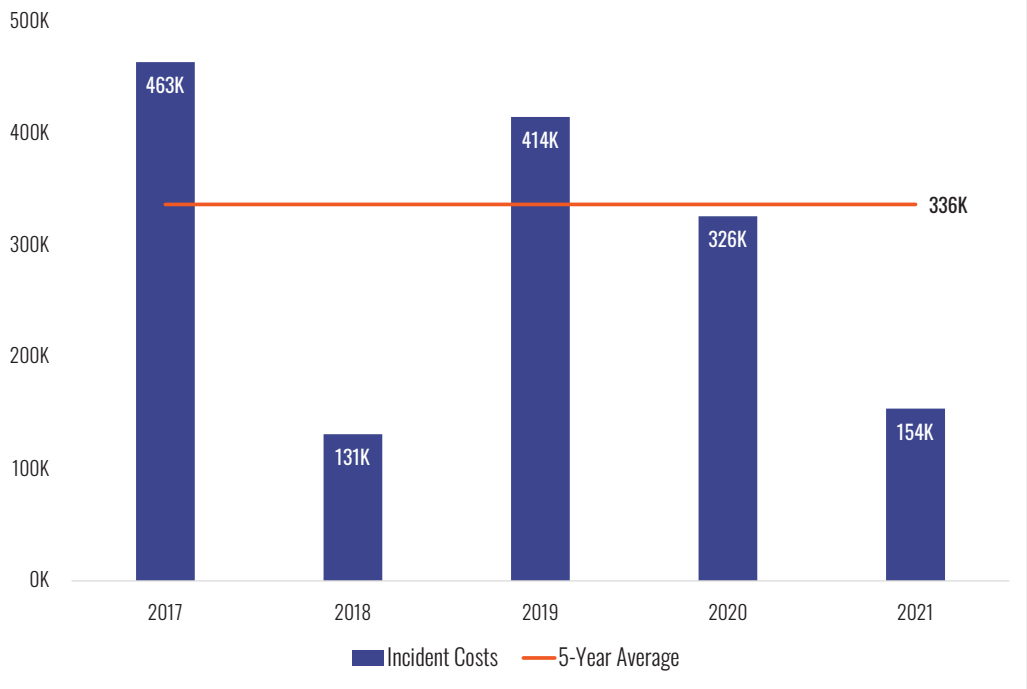


Figure 51

Canada
Top Causes of Loss 2017-2021 – SMEs

Cause of Loss	Claims	Average Incident Cost
Ransomware	35	563K
Business Email Compromise	17	181K
Hacker	11	121K
Staff Mistake	7	34K
Wire Transfer Fraud	6	759K
Malware/Virus	17	178K

Table 2

Conclusion

Once again, NetDiligence has raised the bar for understanding cyber insurance loss for both cyber insurers and other key stakeholders. This year's study includes more data and more targeted findings than ever before. This year 3,400 new claims were submitted. These were added to an existing dataset of over 4,000 claims. The result has been a comprehensive, representative, and objective dataset of cyber claims incidents, including their causes and monetary impacts.

As more and more insurers and brokers have shared more claims and more information about each claim, the value of the study has continued to increase. For the benefit of the industry overall, more underwriters are encouraged to participate and participants are urged to share are a larger percentage of their cyber claims, especially those for large companies. 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 analysis and inclusion in the 2020 study.

AIG

Allied World

AmTrust Financial Services

Ascent Insurance Solutions

At-Bay

AXA XL

Beazley

Berkley Cyber Risk

CFC Underwriting

Chubb

Chubb Canada

CNA

County Reinsurance

Crum & Forster

CUNA Mutual

Great American Insurance

Hiscox

Hylant

Intact Insurance

Liberty Mutual

Markel

Municipal Insurance Association of British Columbia

National League of Cities RISC

OneBeacon

Philadelphia Insurance Companies

QBE

Safety National

Sompo International

Swiss Re

Tokio Marine HCC

Travelers

Travelers Canada

United States Liability Insurance

Zurich NA

***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

Company Size and Loss Magnitude: Does Size Really Matter?

Five years ago, we began asking study participants to provide an estimate of the annual revenue of each claimant. At present, we have this data for about 58% of claims.

One of the questions we have tried to answer is whether there is a clear correlation between the size of the claimant organization and the magnitude of the cyber-related loss.

As the graphs below show, the short answer is no. For SMEs, there is no correlation at all (R^2<0.0992). For Large Companies, there is even less correlation (R^2<0.0024). One of the largest incidents in the dataset occurred at a small enterprise and one of the smallest at a very large one.

Why is this the case? Perhaps, and most importantly, is the equalizing effect of cheaper and more powerful computer hardware, especially mass storage both on premises and in the cloud. An individual can now carry a database of millions of people on a phone or laptop computer. Instead of a relatively small number of targets to exploit, in 2021 almost everyone on the planet has become a potential target to exploit.

Incident Cost and Organization Size
SMEs
(N=4,352)

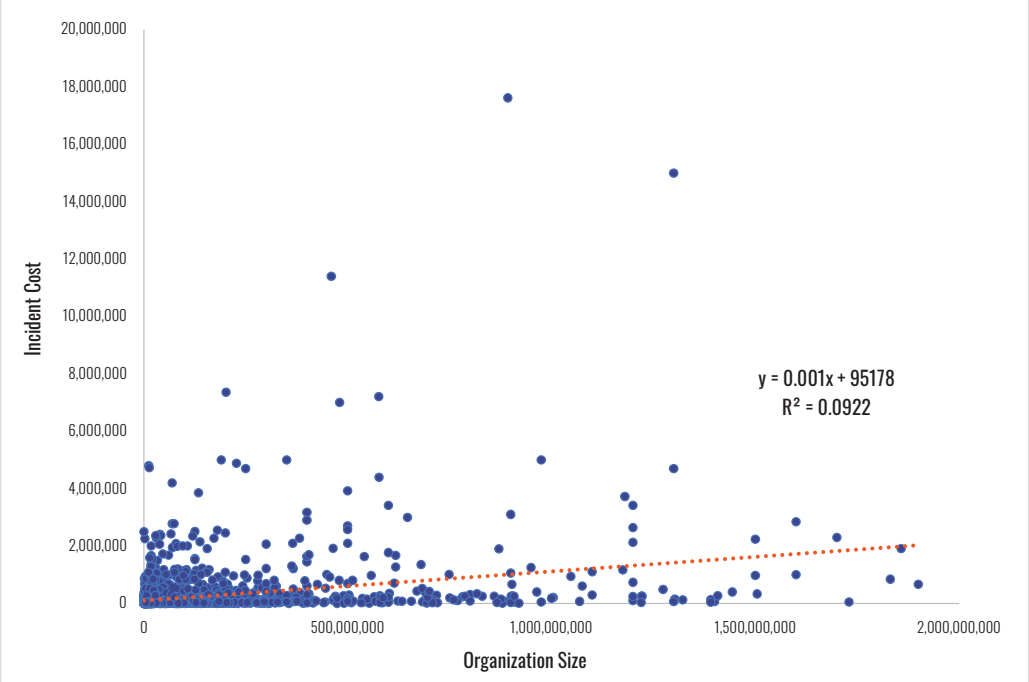


Figure 52

Incident Cost and Organization Size
Large Companies
(N=62)

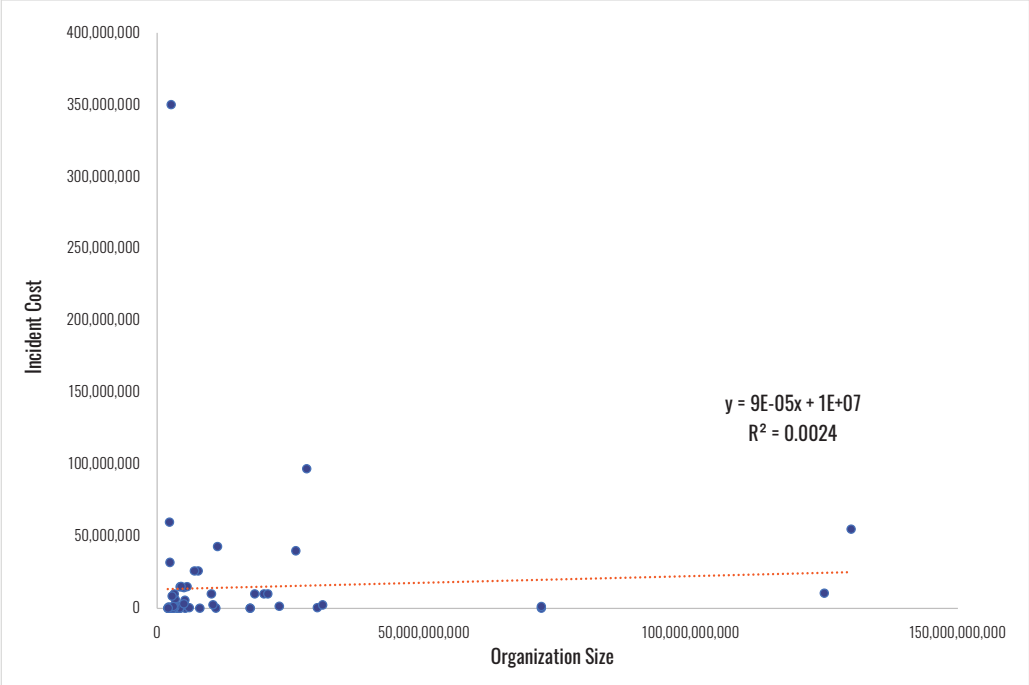


Figure 53

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.

As was mentioned previously, 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.

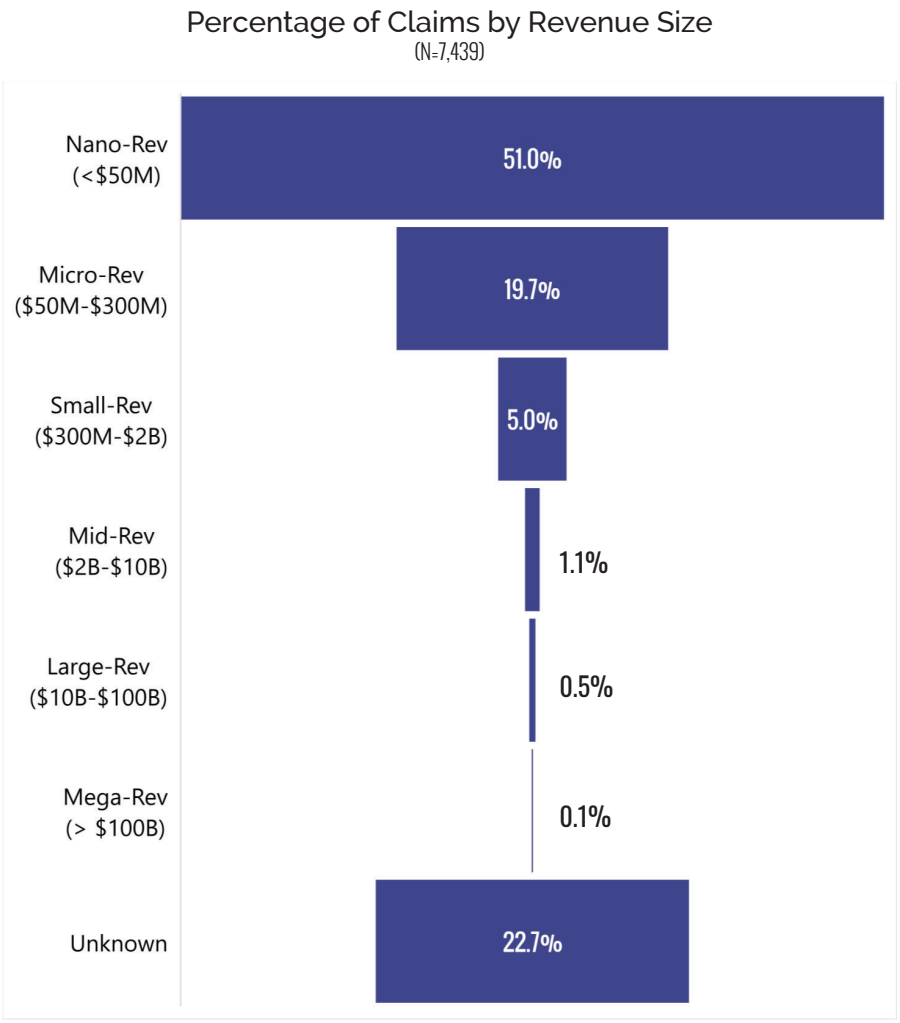


Figure 54

Incident Cost by Revenue Size

2017-2021

Revenue Size	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Nano-Rev (<$50M)	3,365	1K	105K	4.8M	354.8M	16%	1	7
Micro-Rev ($50M-$300M)	1,239	1K	223K	11.4M	276.1M	13%	3	5
Small-Rev ($300M-$2B)	272	3K	796K	17.6M	216.5M	10%	4	4
Mid-Rev ($2B-$10B)	46	5K	7.1M	64.0M	328.8M	15%	5	3
Large-Rev ($10B-$100B)	21	18K	30.8M	350.0M	647.8M	30%	6	1
Mega-Rev (>$100B)	5	10.6M	27.1M	55.0M	135.6M	6%	7	2
Unknown	1,463	1K	156K	120.2M	228.9M	10%	2	6

Table 3

Average Crisis Services Costs by Revenue Size

2017-2021

Revenue Size	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Nano-Rev (<$50M)	39K	10K	22K	16K	38K	61K	7
Micro-Rev ($50M-$300M)	66K	12K	25K	25K	72K	119K	6
Small-Rev ($300M-$2B)	176K	81K	131K	78K	117K	342K	4
Mid-Rev ($2B-$10B)	701K	2.2M	2.8M	767K	575K	2.9M	3
Large-Rev ($10B-$100B)	9.9M	10.0M	647K	1.1M	38K	7.4M	1
Mega-Rev (>$100B)						4.9M	2
Unknown	47K	8K	12K	11K	155K	194K	5

Table 4

Business Sector

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

- 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.

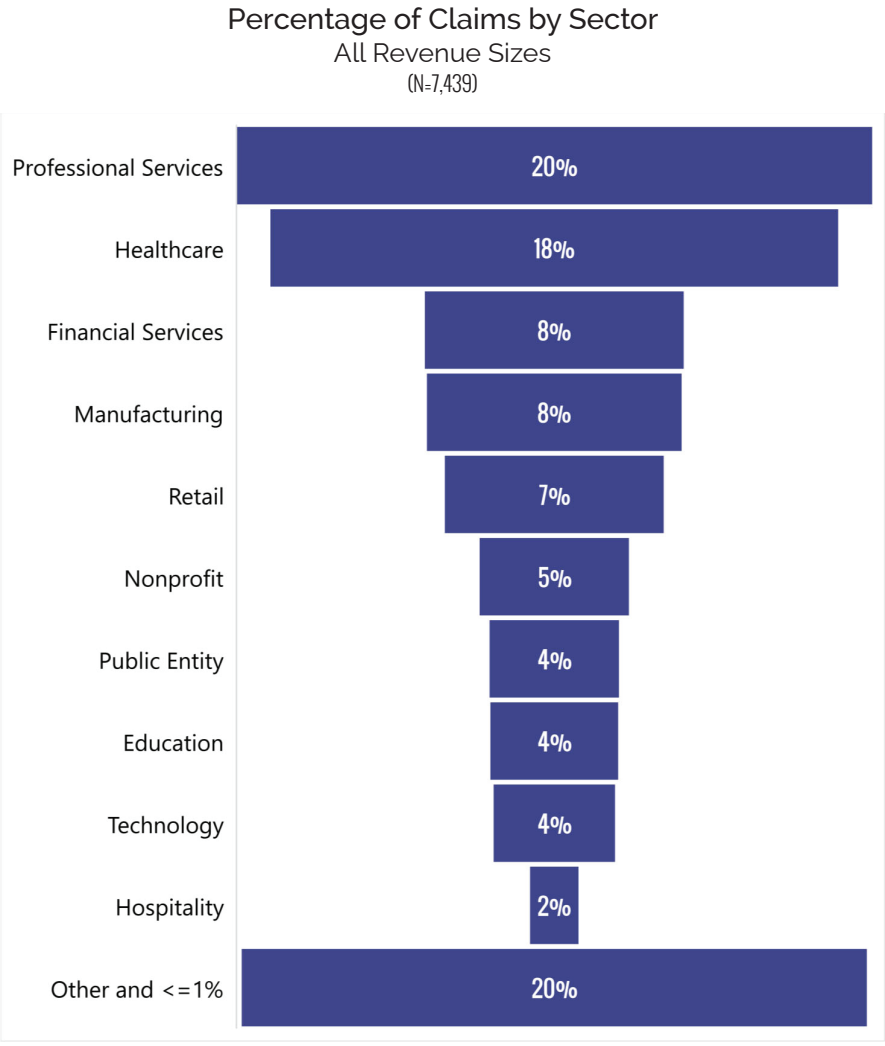


Figure 55

Incident Cost by Sector – SMEs

2017-2021

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Education	257	2K	121K	2.0M	31.0M	2.9%	9	12
Energy	25	13K	795K	15.0M	19.9M	1.8%	15	1
Entertainment	26	4K	107K	548K	2.8M	0.3%	14	14
Financial Services	519	1K	0.1M	3.7M	70.9M	6.6%	5	11
Gaming & Casino	4	20K	163K	532K	651K	0.1%	18	9
Healthcare	1,030	1K	103K	11.4M	106.4M	9.9%	3	15
Hospitality	99	5K	158K	2.6M	15.7M	1.5%	11	10
Manufacturing	575	1K	201K	20.0M	115.6M	10.7%	4	8
Media	44	5K	280K	2.5M	12.3M	1.1%	13	5
Nonprofit	307	1K	90K	2.0M	27.8M	2.6%	7	16
Professional Services	1,354	1K	237K	120.2M	320.9M	29.8%	1	6
Public Entity	266	2K	116K	2.3M	30.8M	2.9%	8	13
Restaurant	22	2K	71K	376K	1.6M	0.1%	17	18
Retail	398	1K	203K	10.7M	80.8M	7.5%	6	7
Technology	219	2K	450K	17.6M	98.5M	9.2%	10	2
Telecommunications	25	6K	312K	2.3M	7.8M	0.7%	15	4
Transportation	89	1K	448K	17.5M	39.8M	3.7%	12	3
Other	1,080	1K	86K	4.9M	93.0M	8.6%	2	17

Table 5

Average Crisis Services Costs by Sector – SMEs

2017-2021

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Education	57K	7K	23K	18K	73K	76K	10
Energy	198K	2K	4K	49K	174K	287K	1
Entertainment	40K	15K	12K	26K	7K	44K	18
Financial Services	46K	44K	19K	21K	64K	82K	9
Gaming & Casino	47K	0K	0K	21K	3K	59K	16
Healthcare	47K	21K	85K	13K	62K	73K	13
Hospitality	54K	11K	17K	22K	36K	83K	8
Manufacturing	44K	4K	9K	18K	40K	76K	11
Media	44K	1K	10K	17K	59K	73K	12
Nonprofit	49K	6K	14K	17K	52K	65K	14
Professional Services	49K	4K	13K	20K	48K	197K	3
Public Entity	50K	20K	15K	18K	85K	88K	7
Restaurant	31K	7K	16K	15K	85K	48K	17
Retail	80K	8K	34K	25K	70K	111K	6
Technology	91K	35K	41K	40K	89K	174K	4
Telecommunications	89K	1K	22K	189K	59K	247K	2
Transportation	60K	7K	4K	45K	37K	166K	5
Other	46K	3K	6K	13K	70K	61K	15

Table 6

Incident Cost by Sector – Large Companies

2017-2021

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Education	7	58K	677K	2.4M	4.7M	0.4%	5	8
Financial Services	11	24K	54,596K	350,000K	600.6M	54.0%	3	1
Healthcare	16	5K	14.6M	60.0M	233.7M	21.0%	1	3
Hospitality	4	1,446K	15,361K	40,000K	61.4M	5.5%	7	2
Manufacturing	9	20K	14,387K	55.0M	129.5M	11.6%	4	4
Professional Services	1	175K	175K	175K	175K	0.0%	9	11
Public Entity	1	2,547K	2,547K	2.5M	2.5M	0.2%	9	7
Retail	5	179K	6,703K	26.0M	33.5M	3.0%	6	5
Technology	3	47K	329K	885K	1.0M	0.1%	8	9
Transportation	1	275K	275K	275K	275K	0.0%	9	10
Other	14	18K	3,193K	14.5M	44.7M	4.0%	2	6

Table 7

Average Crisis Services Costs by Sector – Large Companies

2017-2021

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Education	229K	44K	88K	54K	116K	354K	8
Financial Services	6.0M	13.0M	23.0M	5.4M	0K	14.2M	1
Healthcare	145K	0K	988K	65K	501K	622K	7
Hospitality	0K	10.0M	0K	0K	0K	10.0M	2
Manufacturing	8.8M	14K	5K	1.3M	24K	6.8M	3
Professional Services	0K	0K	0K	0K	75K	75K	9
Public Entity	1.1M	0K	647K	84K	2K	1.8M	6
Retail	1.5M	2K	10K	367K	1.6M	2.7M	4
Technology	0K	0K	0K	30K	0K	46K	10
Other	313K	39K	2.3M	143K	67K	2.0M	5

Table 8

Cause of Loss

Claims are assigned to one of the following twenty-six 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 Hardware
- 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.

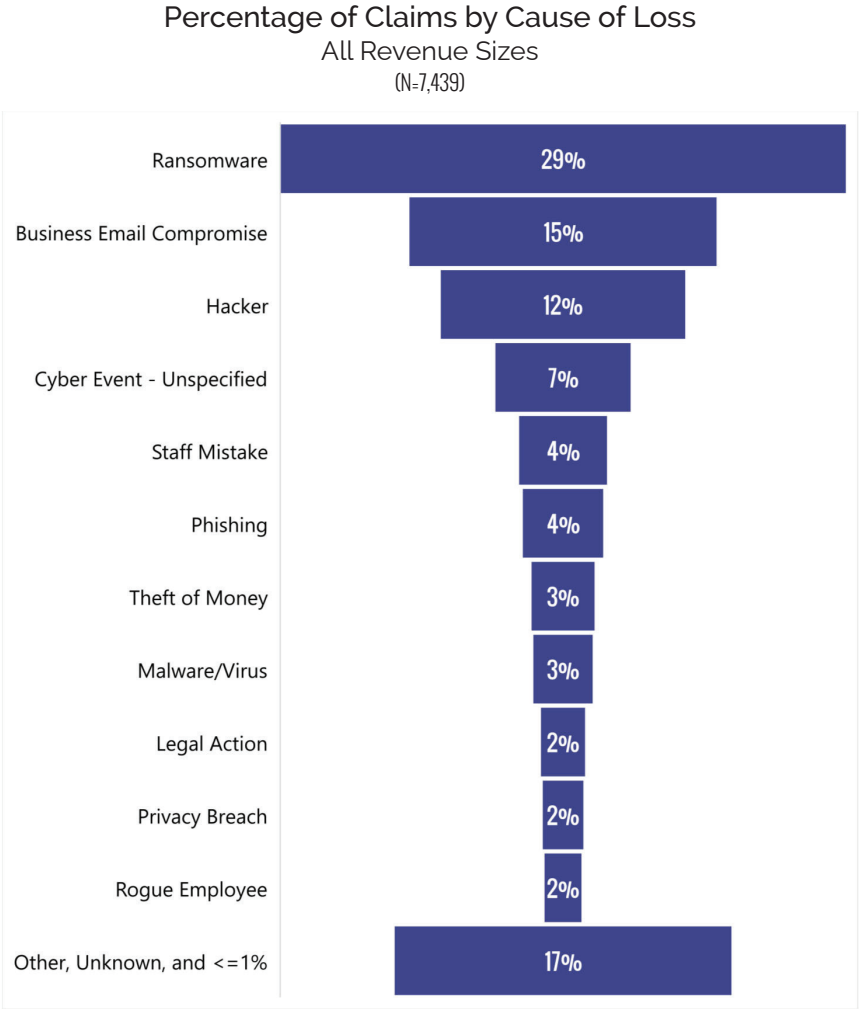


Figure 56

Incident Cost by Cause of Loss – SMEs

2017-2021

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	1,123	1K	96K	3.4M	108.2M	10.1%	2	11
Cyber Event - Unspecified	342	1K	128K	2.4M	43.7M	4.1%	5	10
Hacker	742	1K	0.3M	120.2M	194.9M	18.1%	3	6
Legal Action	46	2K	96K	946K	4.4M	0.4%	14	12
Lost/Stolen Laptop/Device	39	1K	80K	1.5M	3.1M	0.3%	15	14
Malware/Virus	214	2K	143K	10.7M	30.7M	2.9%	9	9
Paper Records	25	1K	21K	130K	516K	0.0%	17	20
Phishing	227	1K	65K	666K	14.8M	1.4%	8	16
Privacy Breach	33	1K	13K	51K	415K	0.0%	16	24
Programming Error	16	4K	148K	0.5M	2.4M	0.2%	18	8
Ransomware	2,049	1K	270K	20.0M	554.1M	51.5%	1	5
Rogue Employee	125	1K	81K	2.5M	10.2M	0.9%	11	13
Social Engineering	7	11K	149K	383K	1.0M	0.1%	20	7
Staff Mistake	228	1K	14K	284K	3.3M	0.3%	7	23
System Glitch	14	4K	1.4M	17.5M	19.6M	1.8%	19	1
Theft of Hardware	54	1K	18K	100K	993K	0.1%	13	22
Theft of Money	171	1K	62K	1.1M	10.7M	1.0%	10	17
Third Party	4	5K	33K	69K	133K	0.0%	22	19
Trademark/Copyright Infringement	4	50K	287K	468K	1.1M	0.1%	22	3
Unauthorized Access	1	20K	20K	20K	20K	0.0%	24	21
Wire Transfer Fraud	80	11K	281K	1.9M	22.5M	2.1%	12	4
Wrongful Data Collection	6	5K	0.5M	2.0M	3.1M	0.3%	21	2
Other	548	1K	54K	2.1M	29.7M	2.8%	4	18
Unknown	241	1K	70K	1.7M	16.8M	1.6%	6	15

Table 9

Average Crisis Services Costs by Cause of Loss – SMEs

2017-2021

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	36K	10K	15K	23K	66K	64K	12
Cyber Event - Unspecified	47K	1K	11K	9K	0K	55K	14
Hacker	45K	10K	50K	27K	24K	287K	2
Legal Action	19K	52K	23K	23K	67K	74K	8
Lost/Stolen Laptop/Device	28K	12K	167K	15K	218K	76K	7
Malware/Virus	66K	3K	39K	21K	97K	95K	5
Paper Records	16K	3K	3K	11K	20K	14K	21
Phishing	37K	6K	12K	17K	15K	50K	15
Privacy Breach	17K	1K	2K	5K	0K	16K	20
Programming Error	31K	300K	278K	17K	3K	107K	4
Ransomware	65K	29K	34K	19K	59K	115K	3
Rogue Employee	63K	3K	8K	34K	64K	57K	13
Social Engineering	23K	0K	1K	15K	102K	71K	10
Staff Mistake	46K	7K	6K	5K	4K	10K	22
System Glitch	54K	8K	11K	40K	54K	73K	9
Theft of Hardware	14K	0K	2K	4K	50K	9K	23
Theft of Money	30K	0K	10K	13K	0K	39K	16
Third Party	4K	69K	0K	9K	1K	31K	18
Trademark/Copyright Infringement	0K	0K	0K	91K	0K	91K	6
Wire Transfer Fraud	23K	5K	0K	27K	99K	65K	11
Wrongful Data Collection	0K	0K	0K	80K	48K	376K	1
Other	24K	5K	10K	11K	34K	28K	19
Unknown	22K	6K	1K	11K	34K	32K	17

Table 10

Incident Cost by Cause of Loss – Large Companies

2017-2021

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Business Email Compromise	11	18K	376K	1.4M	4.1M	0.4%	3	10
Cyber Event - Unspecified	1	714K	714K	714K	0.7M	0.1%	9	9
Hacker	15	55K	44.1M	350.0M	661.2M	59.5%	2	1
Lost/Stolen Laptop/Device	1	32K	32K	0.0M	0.0M	0.0%	9	14
Malware/Virus	6	20K	2,097K	6.2M	12.6M	1.1%	4	5
Paper Records	1	5K	5K	5K	5K	0.0%	9	15
Phishing	1	179K	179K	179K	179K	0.0%	9	13
Programming Error	1	2.5M	2.5M	2.5M	2.5M	0.2%	9	4
Ransomware	25	24K	16.6M	60.0M	414.4M	37.3%	1	2
Staff Mistake	1	250K	250K	250K	250K	0.0%	9	11
Theft of Money	2	103K	189K	275K	378K	0.0%	5	12
Wire Transfer Fraud	1	1.5M	1.5M	1.5M	1.5M	0.1%	9	6
Wrongful Data Collection	2	249K	5.6M	11.0M	11.2M	1.0%	5	3
Other	2	175K	741K	1.3M	1.5M	0.1%	5	7
Unknown	2	32K	739K	1.4M	1.5M	0.1%	5	8

Table 11

Average Crisis Services Costs by Cause of Loss – Large Companies

2017-2021

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Business Email Compromise	182K	47K	26K	86K	655K	396K	8
Cyber Event - Unspecified	347K	2K	6K	173K	0K	528K	7
Hacker	4.6M	11.5M	13.8M	4.3M	50K	10.8M	1
Lost/Stolen Laptop/Device	19K	0K	0K	13K	0K	32K	23
Malware/Virus	1.2M	0K	4.5M	301K	73K	2.2M	3
Programming Error	1.1M	0K	647K	84K	2K	1.8M	4
Ransomware	4.4M	0.0M	40K	469K	1.2M	4.4M	2
Wire Transfer Fraud	44K	0K	0K	63K	0K	107K	15
Wrongful Data Collection	0K	0K	0K	199K	0K	199K	10
Other	0K	0K	988K	21K	38K	543K	6

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.

Percentage of Claims by Type of Data
All Revenue Sizes
(N=7,439)

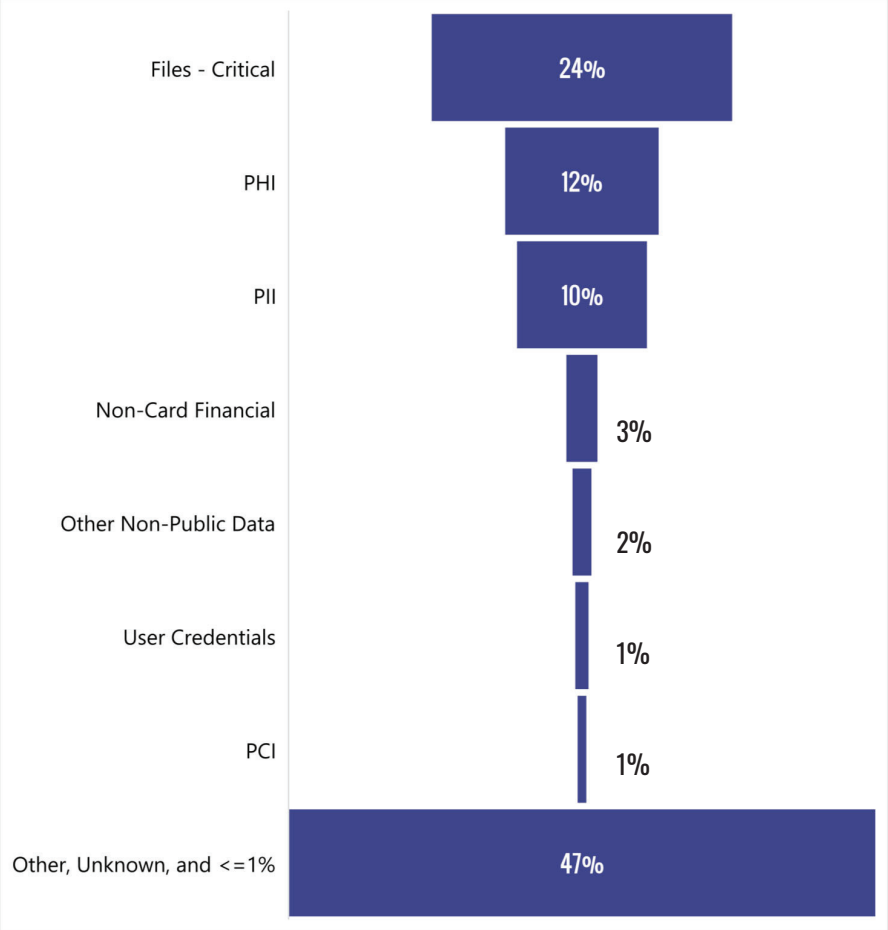


Figure 57

Incident Cost by Type of Data – SMEs
2017-2021

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Email - Unspecified	22	3K	69K	0.2M	1.5M	0.1%	10	12
Files - Critical	1,740	1K	230K	20.0M	400.5M	37.2%	2	7
Intellectual Property	10	3K	208K	1.2M	2.1M	0.2%	12	8
Non-Card Financial	173	2K	914K	120.2M	158.1M	14.7%	5	1
Other Non-Public Data	91	4K	332K	7.0M	30.2M	2.8%	7	4
PCI	49	1K	468K	10.7M	22.9M	2.1%	9	3
PHI	662	1K	141K	17.6M	93.1M	8.7%	3	9
PII	607	1K	242K	15.0M	146.7M	13.6%	4	6
Trade Secrets	3	12K	78K	0.2M	0.2M	0.0%	13	11
User Credentials	62	1K	247K	3.9M	15.3M	1.4%	8	5
Other	20	6K	485K	2.4M	9.7M	0.9%	11	2
N/A	104	2K	137K	1.9M	14.2M	1.3%	6	10
Unknown	2,796	1K	65K	2.5M	181.7M	16.9%	1	13

Table 13

Average Crisis Services Costs by Cause of Loss – SMEs
2017-2021

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Email - Unspecified	22K	0K	2K	17K	157K	52K	11
Files - Critical	55K	7K	18K	16K	52K	88K	8
Intellectual Property	159K	0K	0K	28K	521K	161K	3
Non-Card Financial	42K	243K	11K	29K	89K	1.2M	1
Other Non-Public Data	89K	3K	3K	62K	32K	139K	5
PCI	238K	13K	21K	90K	204K	315K	2
PHI	66K	25K	101K	19K	85K	103K	7
PII	80K	12K	31K	34K	73K	129K	6
Trade Secrets	40K	0K	0K	104K	0K	75K	10
User Credentials	69K	17K	21K	25K	47K	84K	9
Other	56K	0K	2K	71K	170K	158K	4
N/A	22K	13K	7K	12K	51K	42K	12
Unknown	31K	3K	8K	12K	18K	39K	13

Table 14

Incident Cost by Type of Data – Large Companies
2017-2021

Sector	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Files - Critical	12	58K	13.2M	55.0M	157.9M	14.2%	2	5
Intellectual Property	2	24K	640K	1.3M	1.3M	0.1%	9	6
Non-Card Financial	5	103K	70.6M	350.0M	353.0M	31.7%	5	1
Other Non-Public Data	3	47K	329K	885K	1.0M	0.1%	7	8
PCI	4	20K	14.3M	26.0M	57.3M	5.1%	6	4
PHI	11	249K	15.5M	60.0M	170.8M	15.4%	3	3
PII	21	5K	17.5M	97.0M	366.5M	33.0%	1	2
User Credentials	3	77K	303K	530K	909K	0.1%	7	9
N/A	2	32K	43K	55K	86K	0.0%	9	10
Unknown	9	18K	378K	1.4M	3.4M	0.3%	4	7

Table 15

Average Crisis Services Costs by Cause of Loss – Large Companies
2017-2021

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis Costs	Rank by Total Crisis Cost
Files - Critical	6.3M	34K	116K	876K	31K	6.4M	3
Intellectual Property	1.1M	14K	0K	103K	0K	1.2M	5
Non-Card Financial	62K	0K	0K	46K	0K	108K	8
Other Non-Public Data	0K	0K	0K	30K	0K	46K	9
PCI	9.5M	0K	0K	436K	62K	6.6M	2
PHI	45K	0K	988K	77K	501K	1.7M	4
PII	1.6M	5.8M	3.6M	1.9M	747K	6.8M	1
User Credentials	137K	0K	0K	133K	0K	269K	6
N/A	0K	0K	0K	5K	7K	6K	10
Unknown	202K	2K	4K	78K	75K	232K	7

Table 16

Cyber resiliency: The art of bending, not breaking

by RSM

Cyberattacks are expensive–there's no doubt about it. When a company falls victim to ransomware, not only are they hit with a ransom amount and standard crisis management services, but they can also face business interruption (BI) and recovery costs without a proper cyber resiliency plan.

According to this year's claims study, the average cost of a ransomware incident that includes BI and recovery costs is $623K for SMEs and $29.6M for large companies. Additionally, the five-year average cost of a claim that involved BI was almost four times greater than a claim that didn't involve these added expenses. The study further identified that business interruption can account for more than half of all costs associated with a cyber incident.

For all these reasons, cyber insurance carriers are scrutinizing how companies are preparing for business interruption, which has been reflected in supplemental questionnaires and rising premiums. This indicates that an organization's preparation for such an event contributes significantly to reducing risk and associated business interruption costs.

When an organization encounters a business interruption, key operational capabilities are impacted, customer expectations suffer, revenues are lost, relationships are tarnished, and the sustainability of the organization becomes quite volatile.

The traditional focus on pure IT disaster recovery mechanisms–although reliable to recover a system–are not sufficient to maintain operational capabilities during an incident, and this is becoming more and more apparent to business owners–especially SMEs. In fact, the RSM US Middle Market Business Index 2022 Cybersecurity Special Report found that 55% of middle market executives surveyed expressed concerns over interruption.

But what if cyberattacks didn't have to be so costly? What if with proper incident response (IR), disaster recovery (DR), business continuity (BC) and vulnerability management (VM) in place, you could minimize the financial impact to your business when an attack happens and also keep cyber insurance costs low?

How cyber resiliency curbs the cost of a cyberattack

Cyber resiliency can help organizations minimize the financial, operational and reputational impacts of a cyber incident. The goal of resiliency is to "bend but not break" and to maintain operational capabilities despite expected losses. In other words, a strong resiliency plan identifies the key operational capabilities that drive customer facing activities–and in turn, drive revenue–so that a potential business interruption can be avoided. These capabilities might include sustaining operational support and work in progress, maintaining customer billing and invoicing capabilities, meeting contractual and legal obligations, and more. When evaluating cyber resiliency, organizations should identify the top five to ten loss scenarios that would negatively impact customer expectations and revenue. Once identified, each loss scenario should be evaluated according to the "resiliency chain" that supports it. The resiliency chain includes the technologies, people and processes that support each scenario.

How to reduce vulnerabilities within the resiliency chain

Cyber resiliency that leads to operational continuity should represent the fusion of incident response, disaster recovery, business continuity and vulnerability management within an "assess, plan and recover" framework. Here are some ways to achieve this:

- **Internal assessments**: Organizations should perform assessments that probe the business impacts of loss scenarios then evaluate the resiliency chain. They should establish a risk register that tracks each of the gaps identified within each of the scenarios.

- **Planning exercises**: Companies should consider planning exercises that establish an integrated roadmap (IR/DR/BCP/VM). This roadmap should include but not be limited to procedure reviews, integrated tabletops, testing and program management to identify and close key gaps identified along the resiliency chain.
- **Incident response**: Traditional incident response should be revisited to ensure that it includes linkage to those business continuity, disaster recovery and vulnerability management methods, layering these into the response architecture.

What's the ROI for being more resilient?

Reducing risks through the proactive and effective mitigation of business interruption loss scenarios can translate into reducing impact to the bottom line. It is estimated that for every $1 invested in cyber resiliency, organizations save $4 in response and recovery efforts. Some of the benefits of resiliency include:

- Improved insurance rates
- A deeper understanding of how to address failure as an organization
- Improved ability to meet regulatory compliance measures
- Reduced revenue loss after a cyber incident
- Protected reputation and brand
- Improved partner/supplier relationships

About RSM

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 48,000 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.

Business, Interrupted

Breach exposure insight from the Experian front lines

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

New year, same cybersecurity problems

If you thought the 'Cyber-Demic' was over, think again.

Before I get into my 2022 study takeaways, let's recap 2021. If you recall, ransomware was running amok with a 102% increase in attacks in the first six months alone, it took 20% longer to execute a consumer response, and 7 out of 10 breaches were ransomware related. Plus, we reached breach 'herd inevitability.' I said it then, and I'll repeat it: the only path forward is preparedness. More on that later, but first, let's get into current events.

Trends we're experiencing

- Year-over-year increase in breach incidents
- Expecting to service 10% more breaches in 2022, up from 5,100 in 2021
- Third-party breaches account for 50% of our responses, up from one-third

To notify or not to notify?

That, my cybersecurity friends, is the question every legal team is asking. Breaches are still happening, but when they do, clients and forensics opt to notify only the population with the most exposed sensitive information. What's more, the Identity Theft Resource Center says about 40% of notices in the first half of 2022 didn't note the root cause, making "unknown" the top breach reason for the first time since the group began tracking this data point.

Why is this all happening?

For one, organizations are only notifying egregiously impacted populations. For instance, if the breach number is 1 million, legal teams are only notifying 25,000. Second, clients are pushing counsel to use exfiltration confirmation to back the decision. In these cases, if clients can only confirm 10% breached, they will notify 10% (or none), which we're seeing at Experian. In the last six months, out of ten companies that contacted us for a breach quote, only five chose to notify—this is not happening across the board, but it is something to watch.

Is ransomware still a 'triple' threat?

Incident responders and researchers believe ransomware threats over the past six months have decreased partly because of the Ukraine-Russian war. The Identity Theft Resource Center asserts that the collapse of cryptocurrencies is a contributing factor. However, we can all agree that ransomware remains a serious threat and is still a top cause of loss. Based on Experian's client list, ransomware is ramping up again, accounting for 60% of breaches with single, double, and even triple extortion.

Ransomware is here to stay, along with the forensics, crisis PR, and legal complexities needed to respond to it, rising stakes around regulatory fines, and customer flight escalating costs to prepare, plan and respond to the attacks.

Finally, we need to talk about third-party events

Third-party breach events are rising and should be on every cyber insurer's radar. According to the "Is Your Company Ready for a Big Data Breach" study, 50% of respondents say third parties in their supply chain caused the data breach, and virtually all—91% of respondents—say their organizations have a data breach response plan in place. Despite the risk, only about half (56%) of respondents require an audit of third parties' security procedures. But that's just the external story. That same study also reveals that only 49% of

responders said their organization purchased a data breach and cyber insurance policy.

As supply chain woes wage on, attacks are following suit. In fact, the Identity Theft Resource Center says, "Supply chain attacks, a subset of cyberattacks, continue to be a favored attack vector for cyber attackers." Another critical issue, especially for insurance policy underwriters, is third-party events deriving from software and third-party vendors. This group could benefit from a referral model by partnering with Experian to lower its cost ratios.

Our Experian Reserved Response better prepares cyber insurers' cross-departmental teams like forensics and public relations to manage a breach. Also, ERR clients benefit from a stronger security posture due to response drills, lose 25% fewer consumers, and claim fewer incidents and reportable breaches. With 19% of breaches occurring because criminals comprise a business partner, insurers must act to keep their businesses going, close third-party vendor security gaps to protect their organizations, and mitigate brand and consumer risk.

Remember

1. More third-party events are on the way. Attn: Cyber Insurers
2. Ransomware isn't going anywhere any time soon
3. Keep your eyes open. Just because you don't hear about breaches doesn't mean they are disappearing or declining; the 'declines' may be an illusion based on the notify the smallest subset trend
4. Preparedness is the only path forward for the foreseeable future

About Experian Crisis Solutions

When every minute counts, count on Experian Crisis Solutions. Powered by the nation's largest credit reporting agency, Experian Crisis Solutions creates better outcomes and unmatched value by delivering expertise, ease, and guaranteed speed when our partners need it the most. With over 15 years of experience, Experian Crisis Solutions has successfully serviced some of the largest and highest-profile breaches in history. Our turnkey solutions include Experian Reserved Response™, data breach response, crisis response management, and proven credit and identity protection products. To learn more, visit www.experian.com/databreach or email databreachinfo@experian.com.

Hiding in Plain Sight: Towards Now-Gen Cyber Risk Underwriting – 2.0

by Scott Hammesfahr, Solution Consultant, Guidewire Cyence

In last year's report, we laid out an argument against common misconceptions that "there is not enough data to underwrite cyber insurance" as well as the idea that it is not possible to share such data to "legal privilege". We made a case for focusing on collection of digital forensics & incident response (DFIR) data and connecting it to front end underwriting to create a feedback loop that can keep up with this evolving threat.

We believe these arguments are gaining acceptance across the cyber insurance market, and based on feedback from last year's report, we would like to elaborate and build on these ideas.

"There is not enough data to underwrite cyber insurance."

Gone are the days of poor reporting and low incident figures. There is a fast-expanding list of carriers and MGAs with premiums well over $100M, and leaders in this space have premiums approaching and over $1B. Since at least 2020, these portfolios have seen meaningful claims frequency, with average loss ratios above 60% - so for better or worse, there is actually *significant* claims data available. As we argued last year, in claims handling and incident response there was a considerable opportunity to get more diagnostic around incident causes. While many carriers do not share such info, we believe all carriers writing this coverage meaningfully are taking this call seriously, staffing with technical security experts and collecting incident data carefully. One public example of this is the reporting coming out of the newer generation tech-savvy MGAs which publish reports that get into detail on granular causes of losses by industry and revenue sub-segment.

"We can't share information because it is privileged!"

Legal privilege is a fundamentally liability-driven concept, yet as this year's report demonstrates, cyber risk is predominantly causing 1st party losses such as breach response, business interruption, and most unfortunately ransom, where this concept is of little relevance. In August of 2021, the White House held a cybersecurity summit, inviting policy officials, big tech, and insurers to discuss how we can better work together to tackle the challenges related to cybersecurity. One major theme was around sharing data in a consistent and organized way, to gain valuable insights and help mitigate and avoid these risks as stated by insurance participants (Citation). As an example of what this might look like, top IT service providers it's now regularly publish detailed postmortems quickly after incidents. Following this meeting, in March of 2022 the SEC proposed rules to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies." It's no wonder some of the largest rating agencies in the world, such as S&P, are renewing their focus on cybersecurity as a key risk that requires transparency for a broad set of stakeholders. Through standards setting, collaboration, aggregation, and anonymization, we hope to see continued transparency in this space.

Now-gen Cyber Risk underwriting – 2022

Top performing markets are thinking broadly about the kinds of data available to help make sense of the risk landscape and individual company risk characteristics. Incident response data is obviously key. Where incident response data falls short, the increasingly powerful and effective market-level reporting exemplified by

this NetDiligence report can help augment available data. A large opportunity for most insurers is to better manage and leverage underwriting data. This data is accurate, confidential, and is already being laboriously collected by all insurers – yet too often only used in a bespoke and ad-hoc basis, never being consolidated in a coherent way for quantitative analysis. Underwriting data can be augmented by third party data and models

In today's tight-capacity environment, 'doing' data analytics is seen as a must. But this is not a checkbox to tick off. Collecting and synthesizing a variety of risk specific and aggregated data, and effectively implementing it to make better decisions without creating an administrative burden requires tight collaboration of teams that are often siloed within insurers – IT, Data Science, Actuarial, ERM, Claims, Underwriting experts to name some of the key players.

Today's outperforming carriers are not getting lost in the fog of future potential – they are leveraging available DFIR information and their own underwriting data, as well as public reports to build best in class underwriting today.

Guidewire's analytics team delivers advanced data and risk models to support a carrier's ability to address all coverage lines, and our Cyence team is specifically focused on the cyber insurance market. We believe the market's journey is progressing, and work to support its continued growth and resiliency.

About Guidewire

Guidewire is the platform P&C insurers trust to engage, innovate, and grow efficiently. We combine digital, core, analytics to more than 500 insurers in 38 countries, from new ventures to the largest and most complex in the world. Our analytics division is comprised of Cyence for cyber risk, HazardHub for property and casualty, and Predict our flexible platform for machine learning. For more information, contact us a info@guidewire.com.

Leveraging Innovative Solutions to Prevent Data Security Incidents

by Jen Beckage, Managing Director, The Beckage Firm

The twelfth edition of NetDiligence's Cyber Claims Study illustrates the continued impact of ransomware as a leading threat and the substantial costs associated with responding to data security incidents. The Beckage Firm, a NetDiligence Platinum Breach Coach® and women-owned boutique data security and privacy law firm, relies upon the Study to help identify trends and make predictions about future data security incidents. Additionally, as a legal service provider for incident response, compliance, litigation and regulatory defense, The Beckage Firm leverages information in the Study to evaluate how claims, and related costs, can be minimized.

Although the percentage of claims by year decreased from 29% in 2020 to 15% in 2021, the costs for crisis services related to claims were still sizable in 2021. Payouts and Incident Costs appear to steadily increase from 2019-2021. The Study shows that the Average Crisis Services Costs for SMEs were substantial in 2022, as compared to 2021. Similarly, based on the Study, the Average Business Interruption (BI) Costs for SMEs were high. In fact, for SMEs in 2021, the average cost for claims involving BI was almost seven times greater than the average cost for claims that had no BI component. As expected, the Study shows that Average Incident Costs with records exposed were significantly higher than when Records were not exposed. The Beckage Firm recommends that organizations evaluate their record retention and destruction practices and find opportunities to limit that data set in a legally defensible manner.

The Study shows that ransomware is still a leading threat, and threat actors do not discriminate based on the size of the organization. SMEs are still a target, where they often have less resources or expertise to respond to such incidents. Over the last few years, the increased regulatory requirements to report ransomware payments is aimed to discourage such payments, but the Study shows that ransomware is still a leading threat. On average, criminal incidents, particularly for SMEs, were significantly more expensive than non-criminal incidents. In addition to ransomware, business email compromise (BEC) is also still a leading cause of data security incidents. Per the Study, both ransomware and BEC account for nearly 50% of the claims for 2020 and 2021.

Based on experience, The Beckage Firm notes that new laws and regulations continue to impact incident response. For example, the Study shows that in 2021, there were increased legal guidance costs for large entities, possibly due to new laws and regulations for international organizations with global data sets. The Beckage Firm monitors new and changing state and international data security and privacy laws along with geopolitical pressures. The White House made cybersecurity a top priority last year, and agencies everywhere now provide more oversight. The increase in legal and regulatory efforts requires organizations of all sizes to work hard to build up defenses, which may have made an impact on the percentage of claims by year decreasing to 15% in 2021.

The COVID pandemic played a tremendous role in the evolution of organizations' cybersecurity resilience strategy. During 2020-2021 many organizations moved to a remote or hybrid work environment fostering a digital evolution in how organizations store, transmit, and use data. While the impacts of the pandemic have somewhat slowed, the cybersecurity industry will continue to face new challenges, such as the Russia-Ukraine crisis and growing geopolitical matters. Preparation for the next crisis, whatever that might be, will remain critical.

To stay at the cutting edge of the security and technology landscape, The Beckage Firm is watching how new technologies may impact the size and volume of claims. One of the most impactful technologies is artificial intelligence (AI). The Beckage Firm focuses on

AI technologies, as these solutions may enable faster, smarter, and more robust defenses and opportunities to limit costs related to incidents. Additionally, there are ongoing evolutions of the metaverse, web3, NFTs, smart contracts, cryptocurrency, and the legal liability and opportunities related to such technologies in a limited legal landscape on such topics. As predicted by The Beckage Firm members years ago, there will also be more discussions on how quantum may impact cybersecurity in the future.

Overall, the Study shows that while the percentage of claims decreased in 2021, the average cost for claims is still substantial. The Beckage Firm, like other organizations relying on the Study, will contemplate how external factors, such as remote workforces, changes in the legal and regulatory landscape, growing data sets, larger attack surfaces, and new technologies are part of the overall picture of 2021 claims and related costs so modifications can be made going forward.

About The Beckage Firm

The Beckage Firm is a women-owned law firm that focuses on technology, data security and privacy, incident response, litigation, and regulatory inquiries. The Beckage Firm attorneys and team counsel clients on matters pertaining to data security and privacy compliance, government investigations, litigation and class action defense, incident response, technology, and emerging technologies such as Artificial Intelligence (AI). The Beckage Firm's headquarters are in New York. Learn more at TheBeckageFirm.com.

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 five on-site conferences per year, in Philadelphia, Santa Monica, Toronto, Florida, and Bermuda.

Contact Us

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

NetDiligence®

About the Study

Contributors

Risk Centric Security, Inc.

A special thank you also goes to Heather Goodnight-Hoffmann, cofounder and President, and Patrick Florer, cofounder and Chief Technology Officer of Risk Centric Security, who performed the data collection and data analysis, and provided material support in the 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:

- Heather Osborne – Director of Global Events & Programming, NetDiligence
- Sharon Lyon – Publisher, 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 2019, 2020, or 2021.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to over 150 individuals at 100 organizations in the United States, Canada, and the United Kingdom. From this group, 21 individuals representing 20 organizations provided 3,403 analyzable new claims, using the proprietary NetDiligence® claims data collection worksheet.

The 2022 report also includes data from NetDiligence® studies published in 2018-2021, representing 4,036 incidents that occurred in 2017, 2018, 2019 and 2020. After the elimination of claims that were less than $1,000, the combined dataset included 6,411 incidents, each one a cyber incident insurance claim.

There are 7,167 claims in the dataset from American organizations, 166 claims from Canadian organizations, and 27 claims from organizations in the United Kingdom. There are also a small number of claims from organizations in Australia, Germany, Ireland, South Africa, other countries, and organizations with a global footprint (less than 4 each). The country was not specified in 56 claims.

When factoring in SIRs, we were able to calculate Total Incident Costs to date for all 6,411 (100%) of the analyzable claims in the dataset. In addition, 755 claims (12%) specified the number of records exposed and 4,321 claims (67%) included an accounting of Crisis Services Costs. The number of claims reporting records decreased since last year due to the large number of claims for incidents that do not expose records (Ransomware, Social Engineering, BEC, etc.)

6,393 (86%) of the claims in the dataset were flagged as closed, 1,035 (14%) as open. 4,094 (55%) of the claims were for primary coverage, 48 (<1%) for excess coverage, and 3,297 (44%) had an unknown, but most likely primary coverage level.

There were 1,690 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 in 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 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 14% 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.