NetDiligence®

CYBER CLAIMS STUDY

2022 REPORT

RSM

experian

GUIDEWIRE

THEBECKAGEFIRM

Contents

Introduction 1

Key Findings 2

An Overview of the Data 7

- Claims by Year of Event 7
- Incident Costs and Payouts 8
- Incident and Crisis Services Costs 10
- Business Interruption (BI) and Recovery Expense 18
- Recovery Expense 20
- Legal Costs 21
- Records Exposed 22
- Recordless Claims and Claims with Exposed Records 24
- Criminal and Non-Criminal Activities 25
- Self-Insured Retentions (SIR) 28

Causes of Loss 29

- Ransomware 30
- Business Email Compromise (BEC) 33
- Hackers 35
- Wire Transfer Fraud, including BEC 36
- Staff Mistakes 37
- Rogue Employees 38
- Third Party Incidents 39

Sectors 40

- Professional Services 41

Healthcare 42
Manufacturing 43
Financial Services 44
Retail 45
Public Entities 46
Claims from Canada 47
Conclusion 48
Insurance Industry Participants 48
Appendices 49
Company Size and Loss Magnitude: Does Size Really Matter? 49
Revenue Size 51
Business Sector 53
Cause of Loss 57
Type of Data 61
Insights from Our Sponsors 64
Cyber resiliency: The art of bending, not breaking 64
Business, Interrupted 66
Hiding in Plain Sight: Towards Now-Gen Cyber Risk Underwriting – 2.0 68
Leveraging Innovative Solutions to Prevent Data Security Incidents 70
About NetDiligence® 72
About the Study 73
Contributors 73
Methodology 73

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.

© 2022 NetDiligence®

Key Findings

Company Size

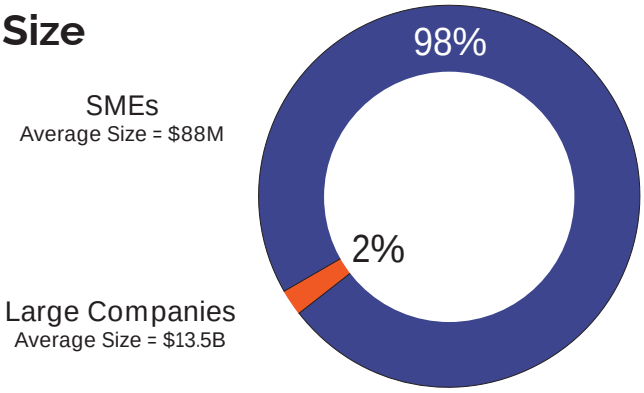


Figure 1

Average Costs for All Claims

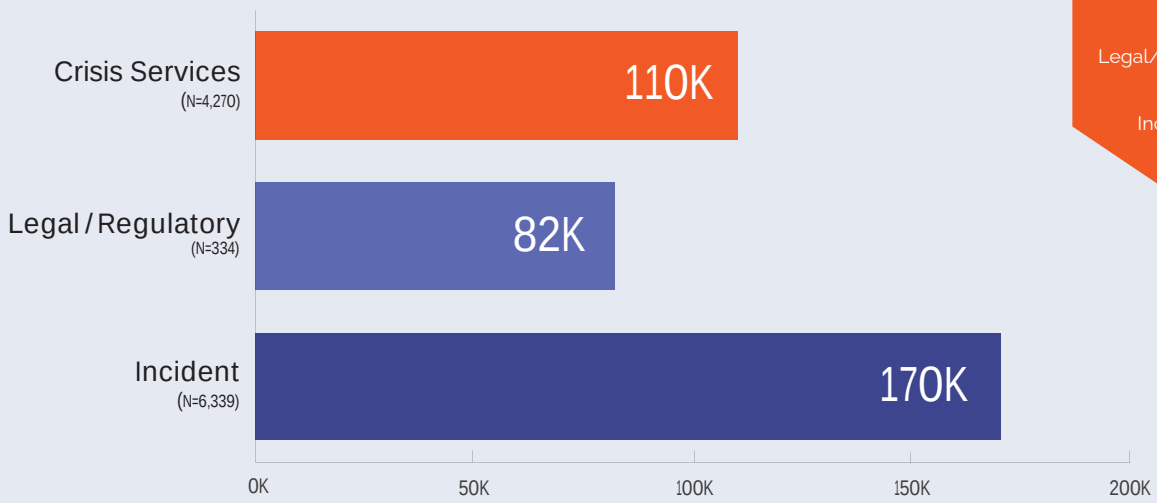


Figure 2

Crisis Services (N=51)
4.1M
Legal/Regulatory (N=11)
3.1M
Incident (N=72)
15.4M

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)

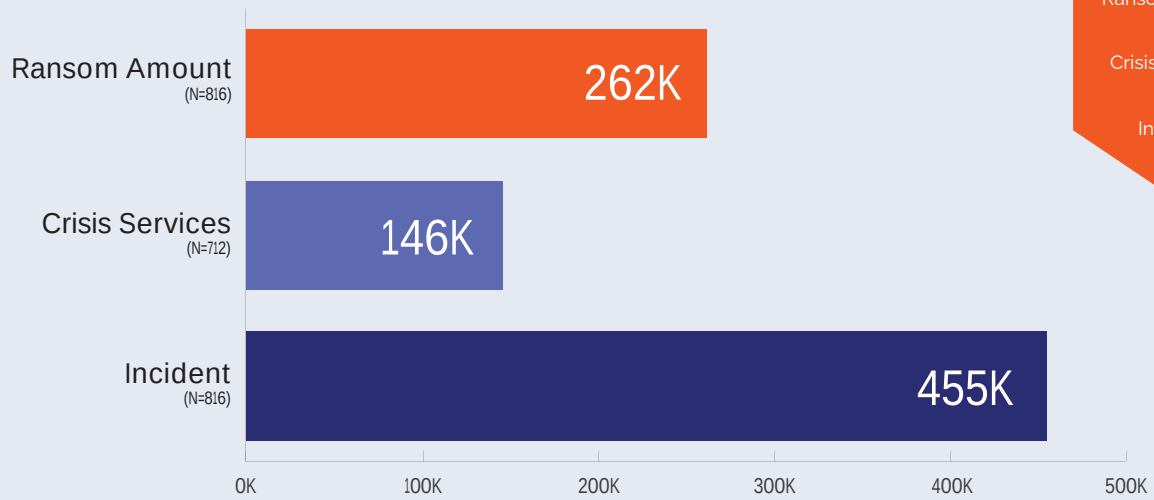
Categorized in this study as organizations with less than $2 billion in annual revenue.

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.

Average Costs for Ransomware



Ransom Amount (N=9)
8.6M
Crisis Services (N=8)
2.2M
Incident (N=9)
12.8M

Figure 3

or 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

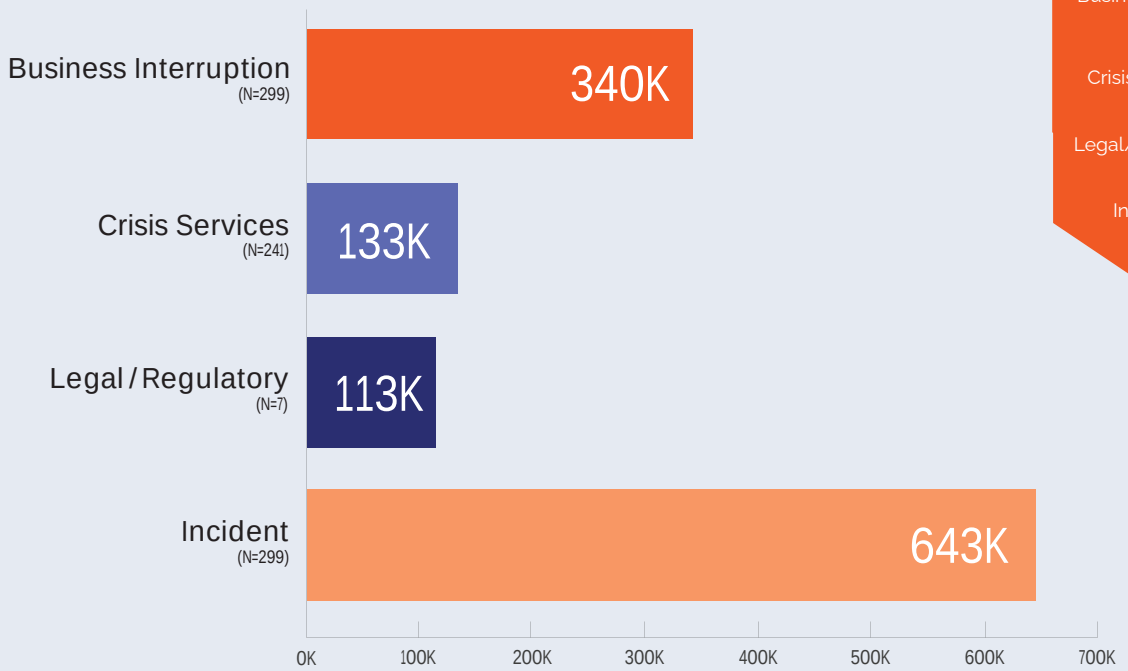


Figure 4

Business Interruption (N=10) 16.5M
Crisis Services (N=9) 2.1M
Legal/Regulatory (N=0) 0.0M
Incident (N=10) 26.6M

his 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

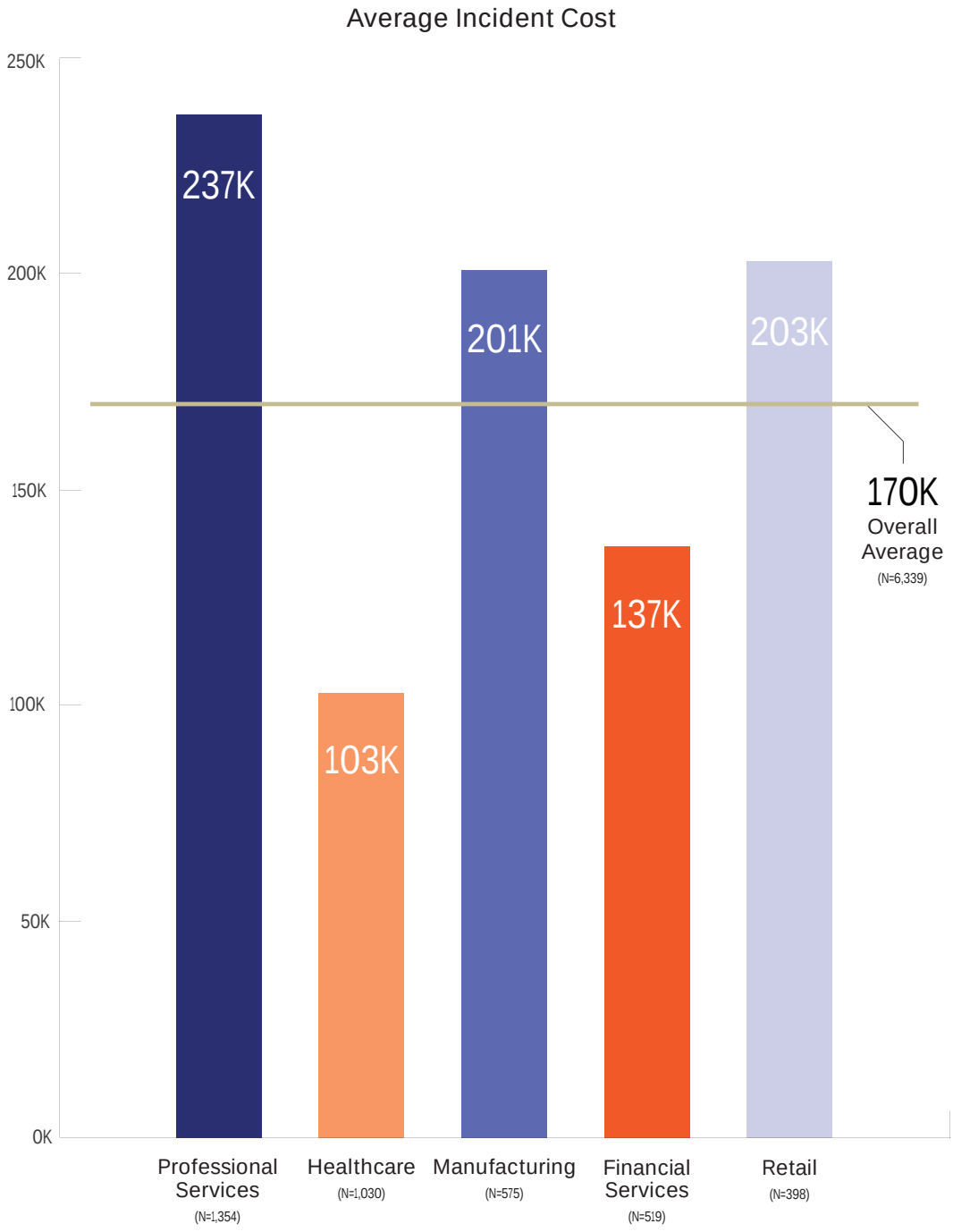


Figure 5

Cause of Loss

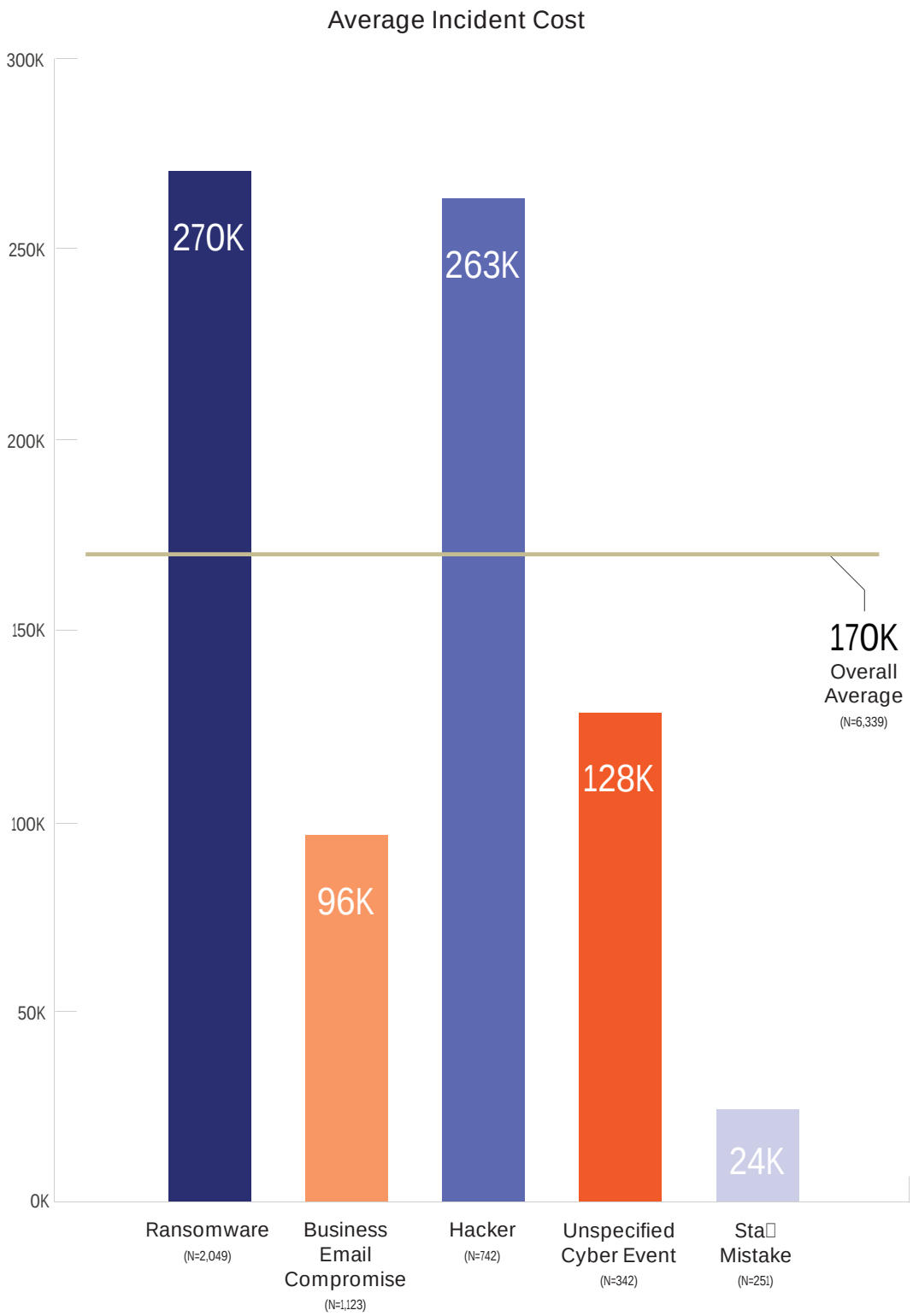


Figure 6

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)

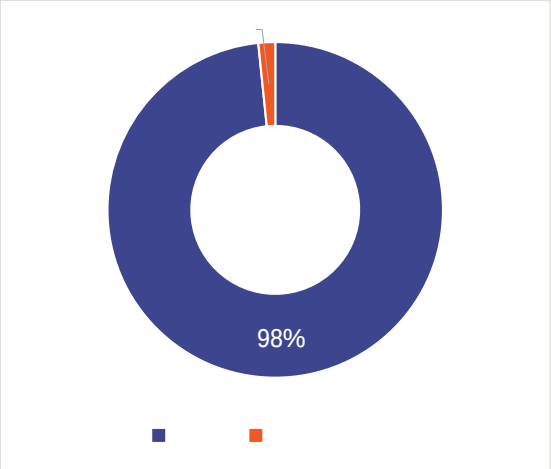


Figure 7

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

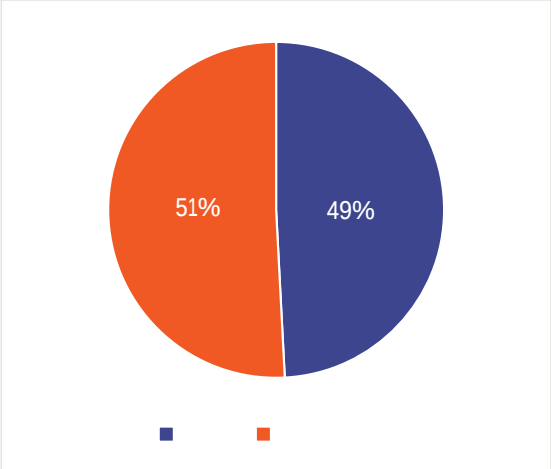


Figure 8

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)

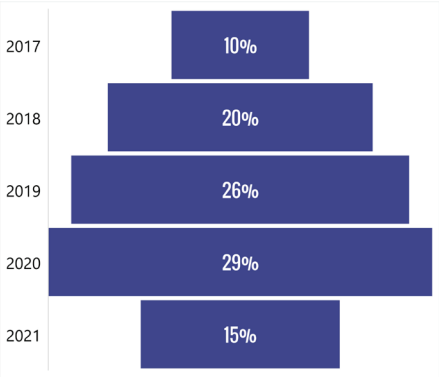


Figure 9

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%.

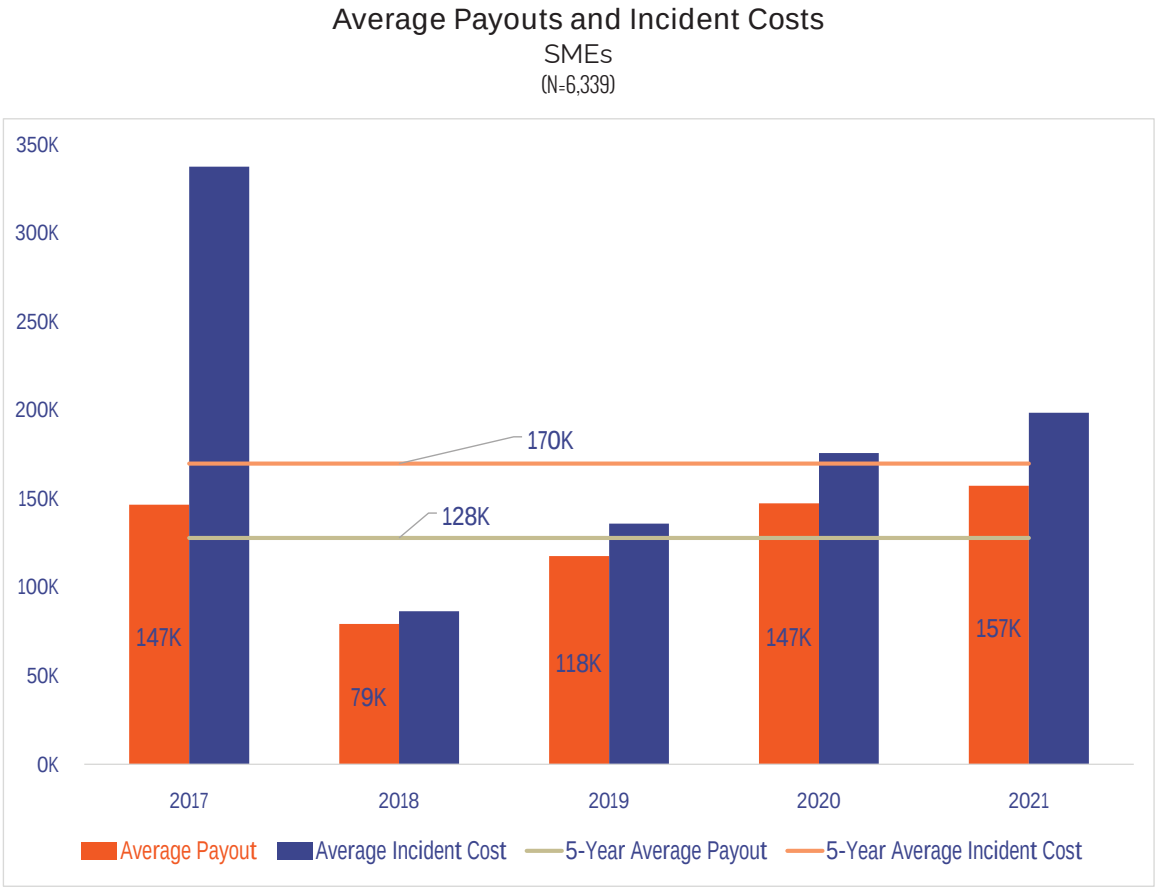


Figure 10

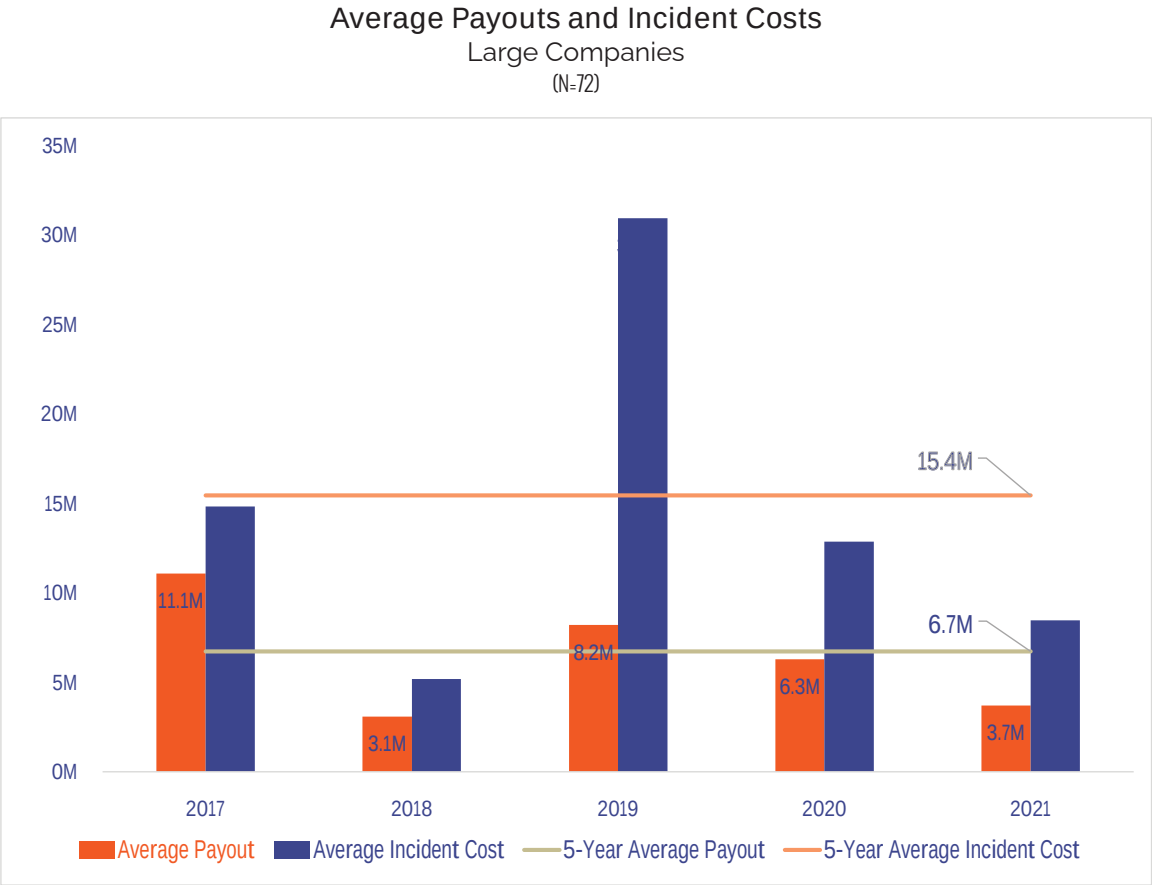

Average Payouts and Incident Costs
Large Companies
(N=72)
35M
30M
25M
20M
15M
10M
5M
0M
15.4M
6.7M
11.1M
3.1M
8.2M
6.3M
3.7M
2017
2018
2019
2020
2021
Average Payout
Average Incident Cost
5-Year Average Payout
5-Year Average Incident Cost

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.

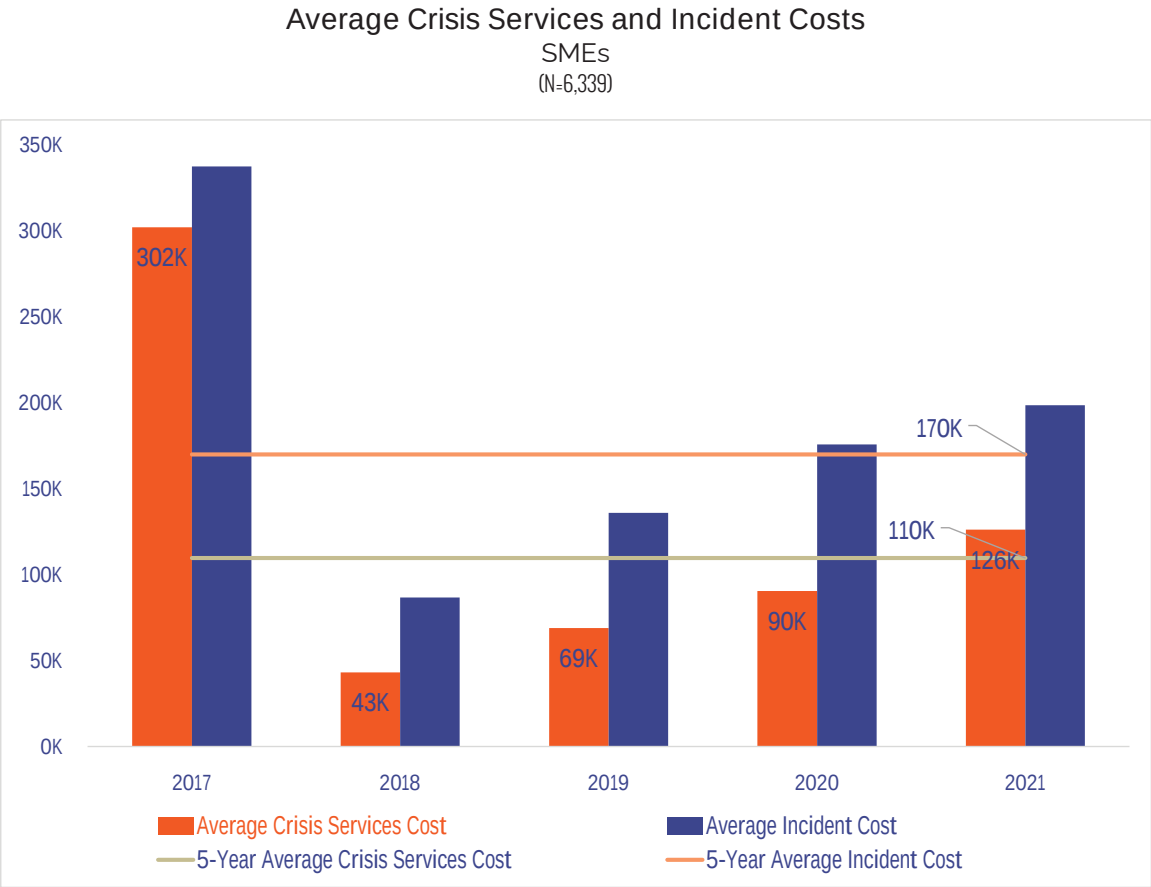


Figure 12

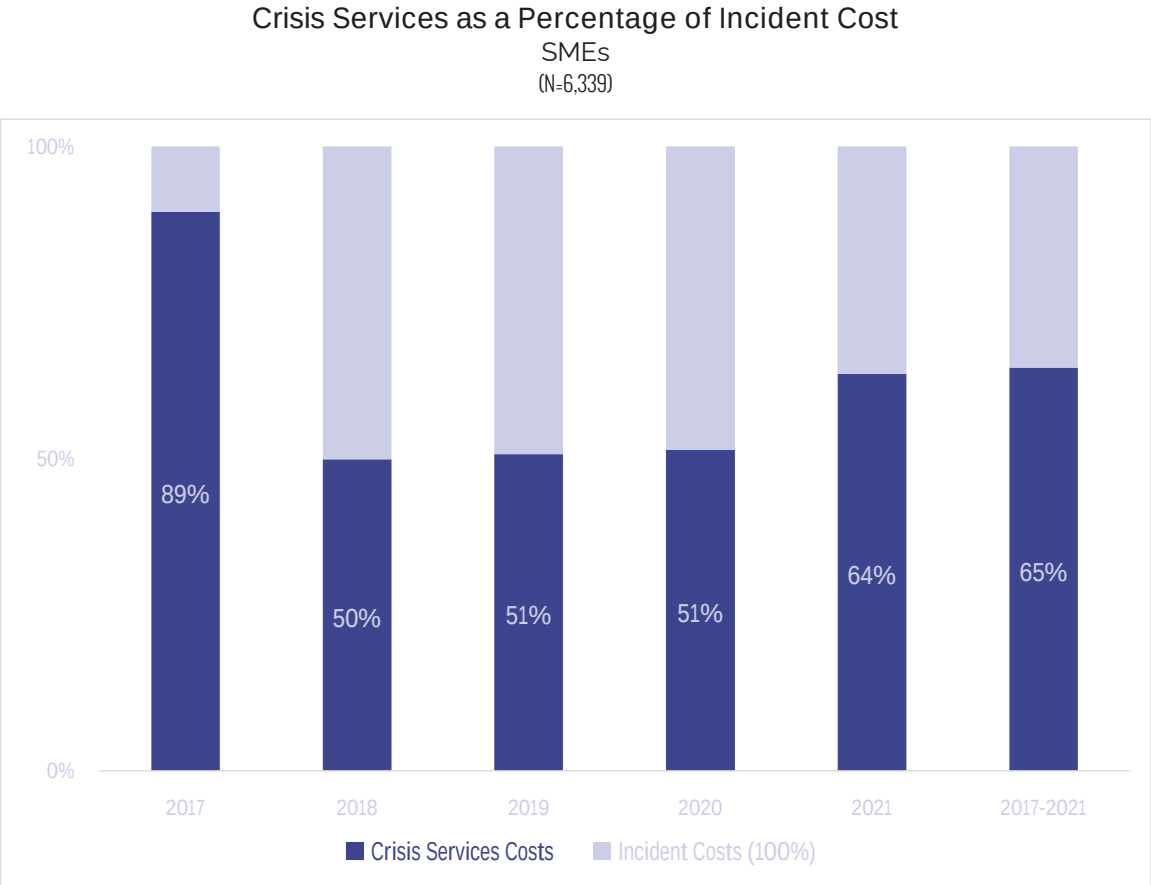


Figure 13

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.

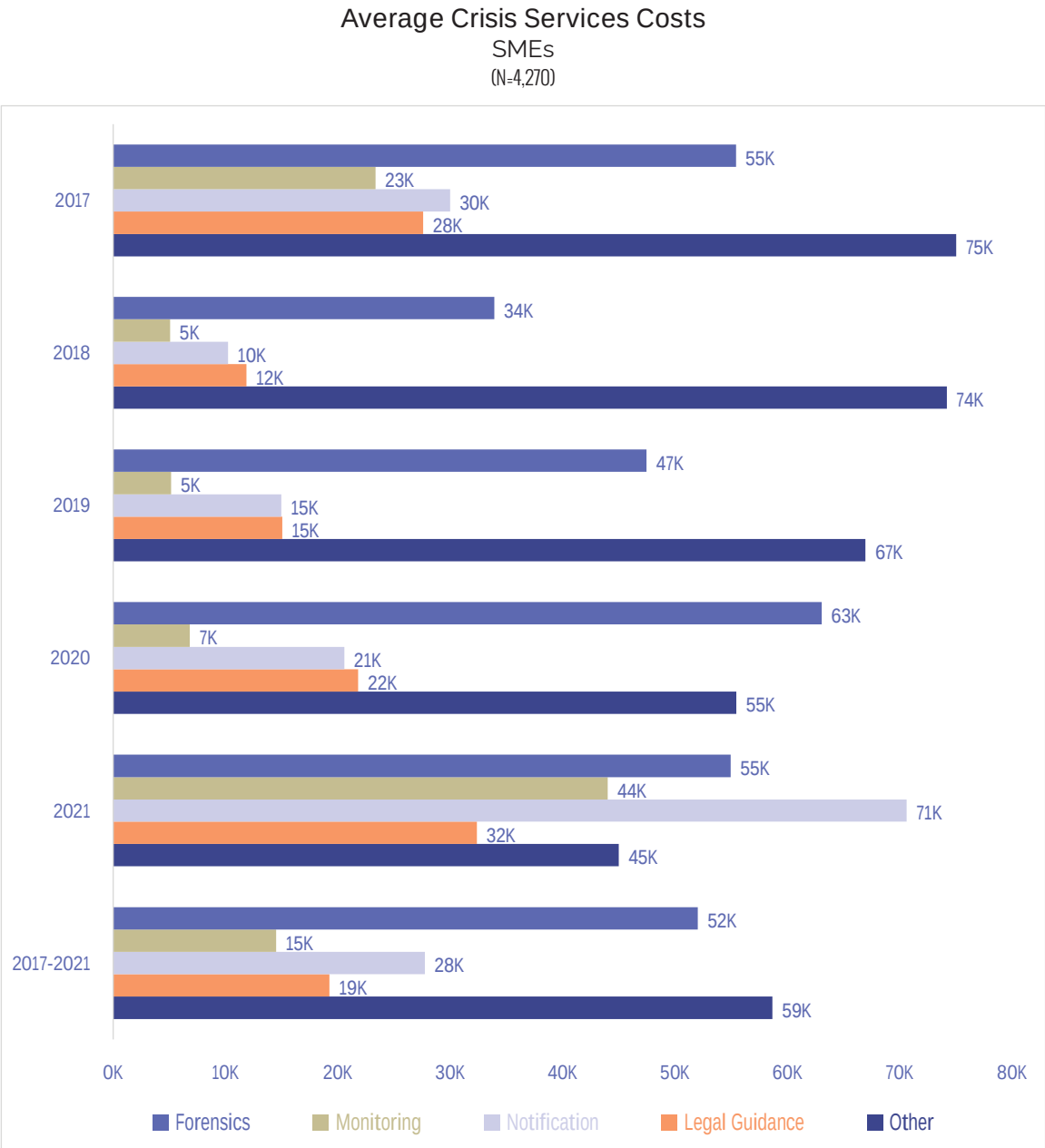

Average Crisis Services Costs
SMEs
(N=4,270)
2017
55K
23K
30K
28K
75K
2018
34K
5K
10K
12K
74K
2019
47K
5K
15K
15K
67K
2020
63K
7K
21K
22K
55K
2021
55K
44K
71K
32K
45K
2017-2021
52K
15K
28K
19K
59K
0K
10K
20K
30K
40K
50K
60K
70K
80K
Forensics
Monitoring
Notification
Legal Guidance
Other

Figure 14

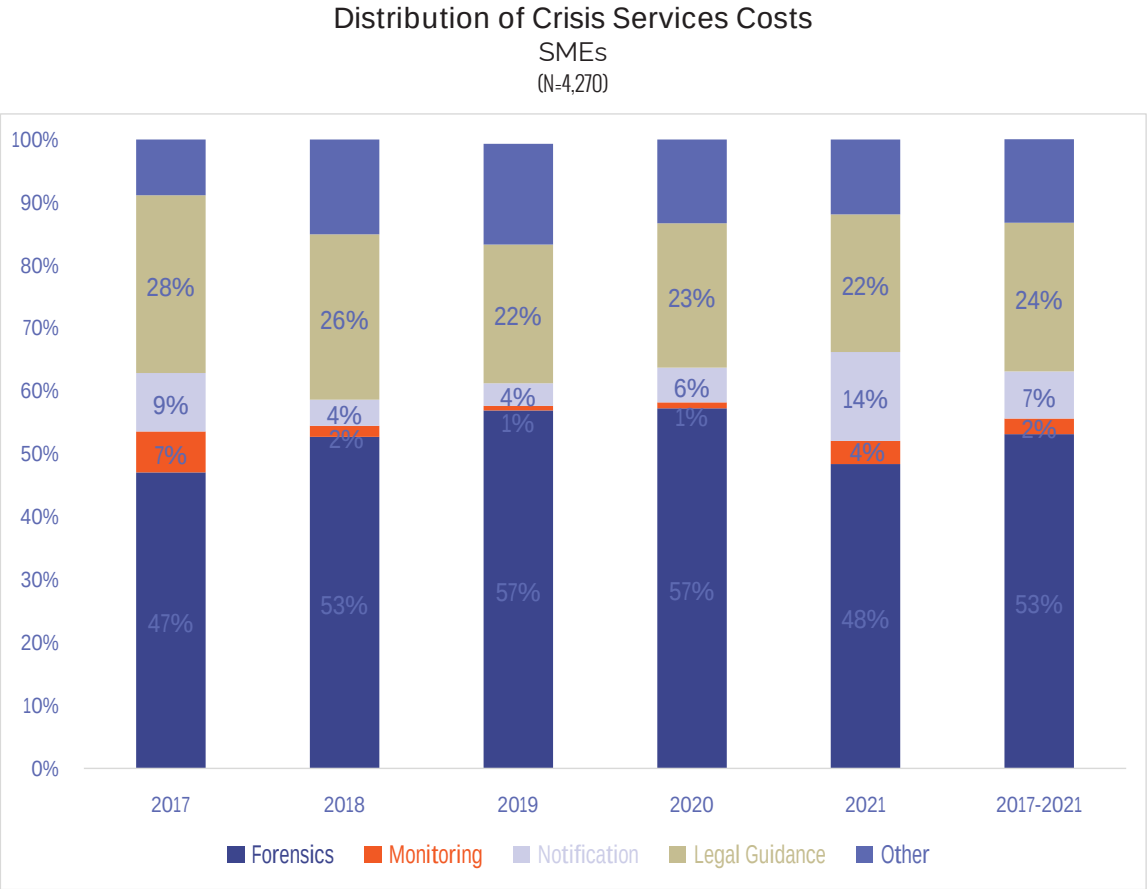


Figure 15

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.

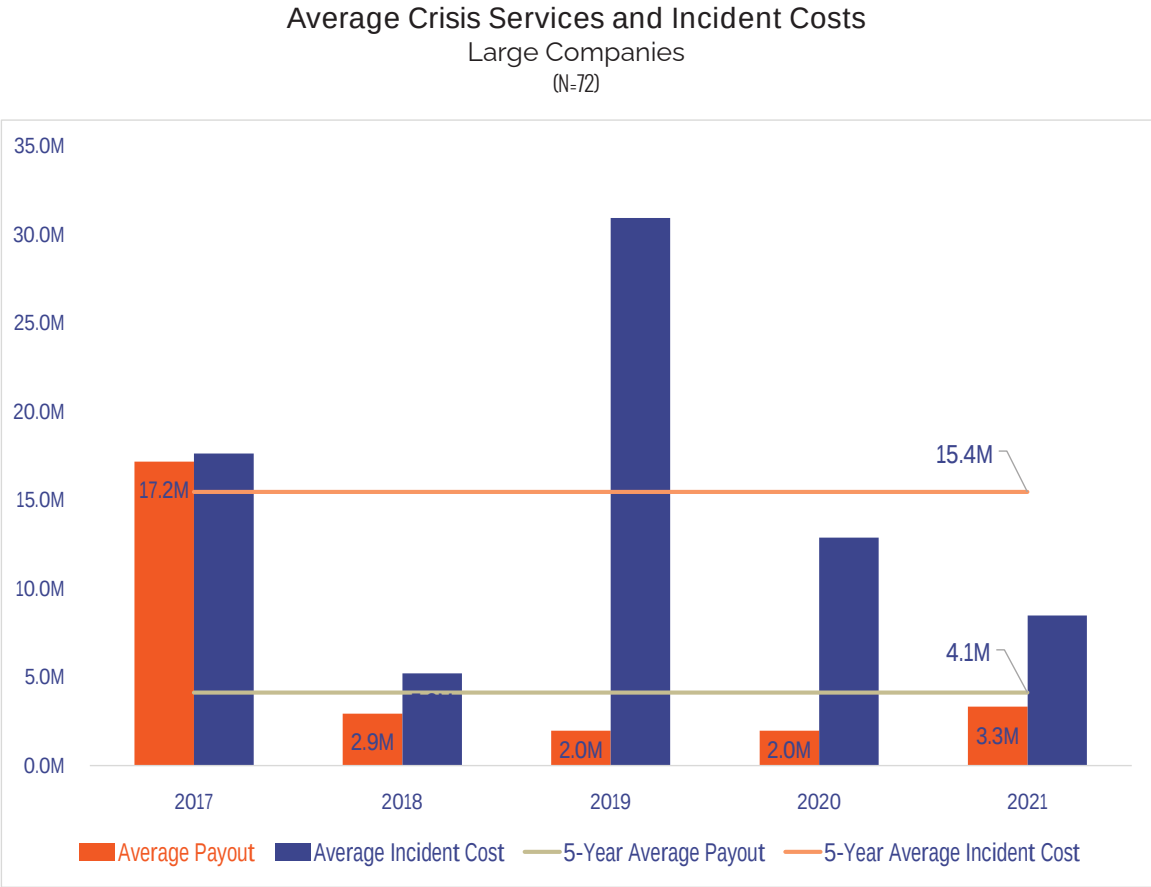

Average Crisis Services and Incident Costs
Large Companies
(N=72)
35.0M
30.0M
25.0M
20.0M
15.0M
10.0M
5.0M
0.0M
17.2M
2.9M
2.0M
2.0M
3.3M
15.4M
4.1M
2017
2018
2019
2020
2021
Average Payout
Average Incident Cost
5-Year Average Payout
5-Year Average Incident Cost

Figure 16

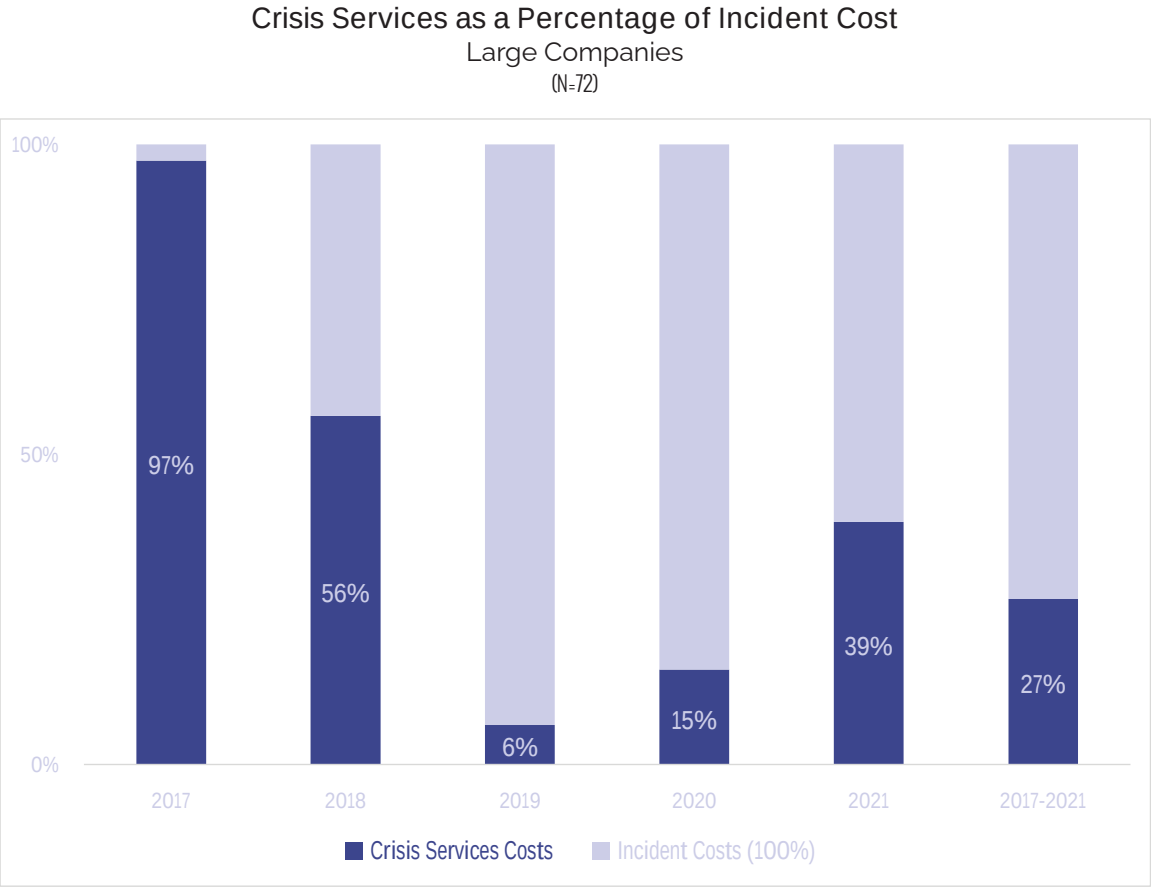


Figure 17

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.

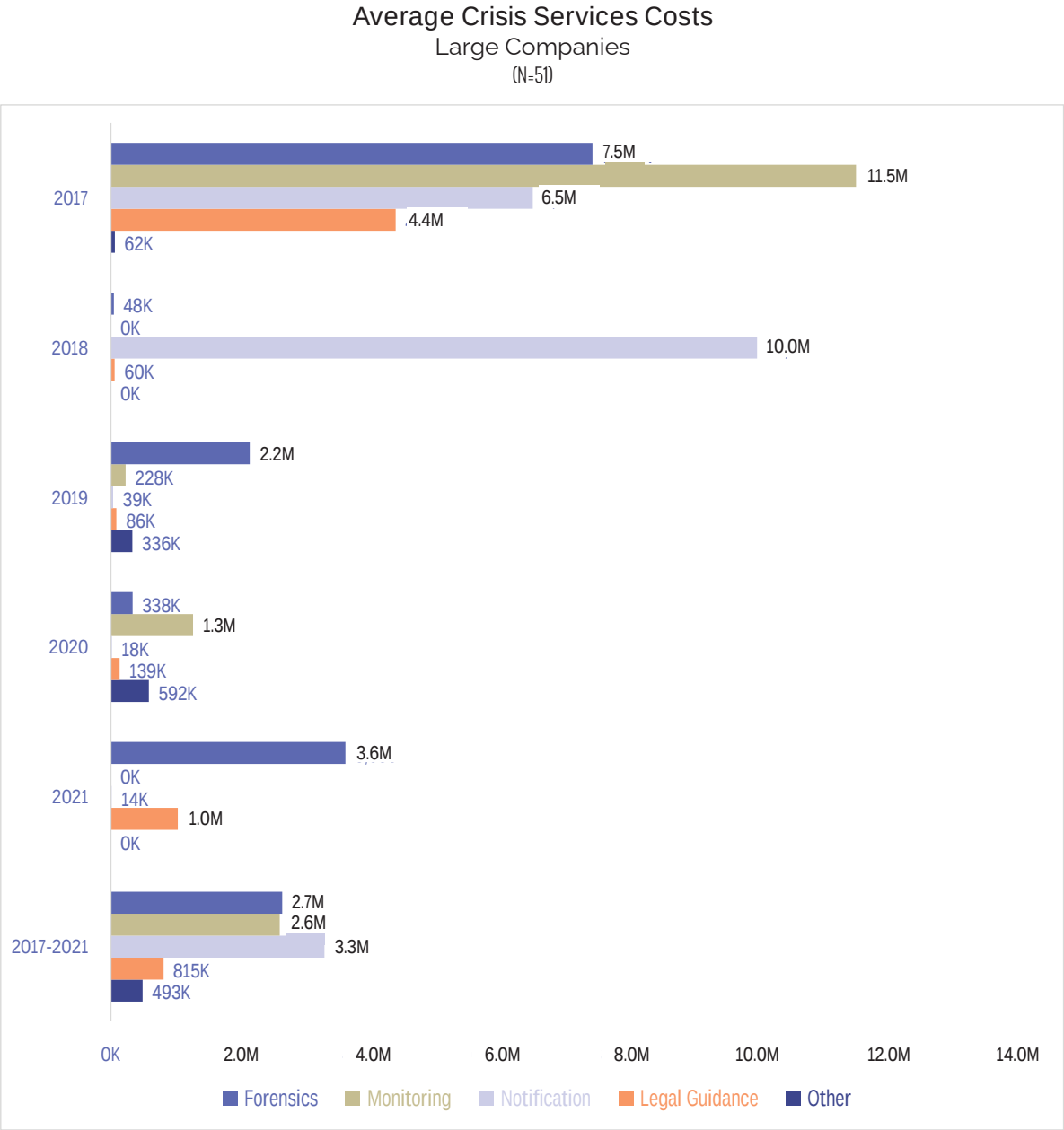

Average Crisis Services Costs
Large Companies
(N=51)
2017
7.5M
11.5M
6.5M
4.4M
62K
2018
48K
0K
10.0M
60K
0K
2019
2.2M
228K
39K
86K
336K
2020
338K
1.3M
18K
139K
592K
2021
3.6M
0K
14K
1.0M
0K
2017-2021
2.7M
2.6M
3.3M
815K
493K
0K
2.0M
4.0M
6.0M
8.0M
10.0M
12.0M
14.0M
Forensics
Monitoring
Notification
Legal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

Figure 18

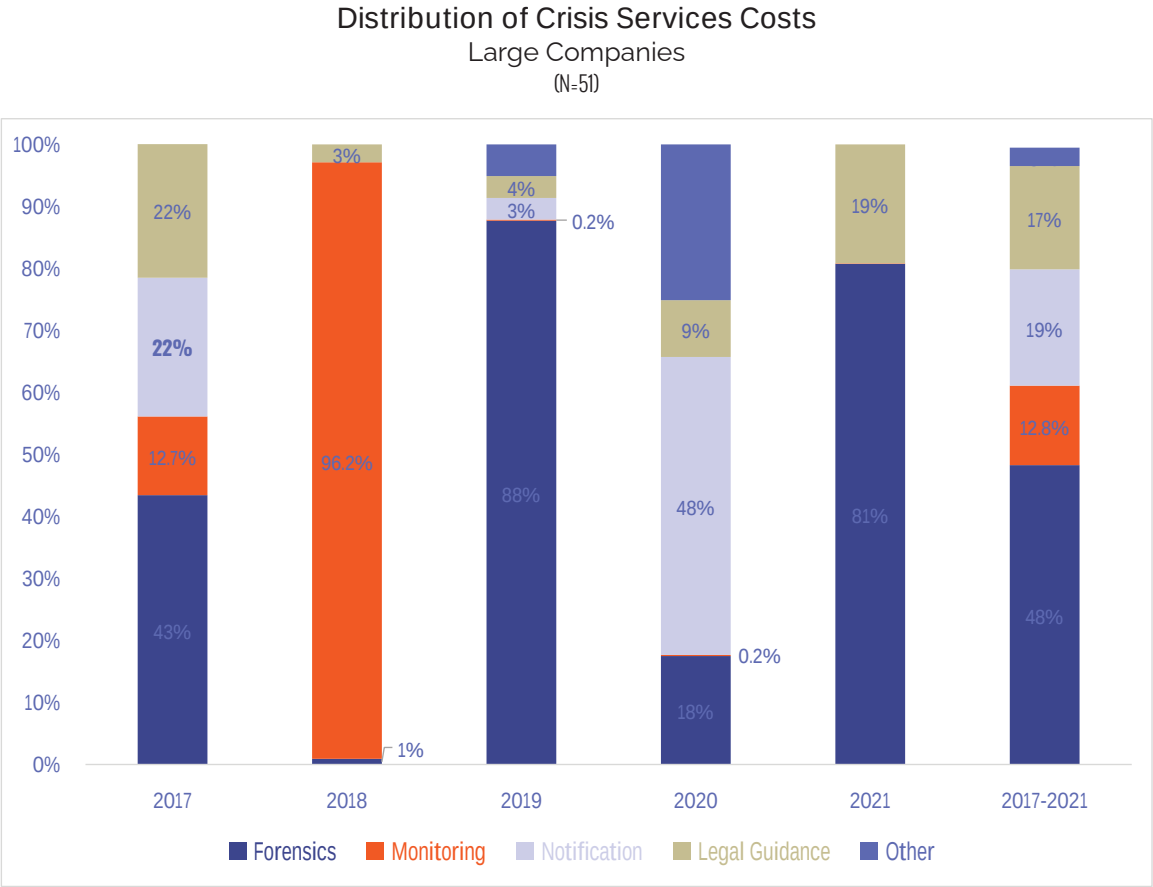

Distribution of Crisis Services Costs
Large Companies
(N=51)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
22%
22%
12.7%
43%
3%
96.2%
1%
4%
3%
0.2%
88%
9%
48%
0.2%
18%
19%
81%
17%
19%
12.8%
48%
2017
2018
2019
2020
2021
2017-2021
Forensics
Monitoring
Notification
Legal Guidance
Other

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.

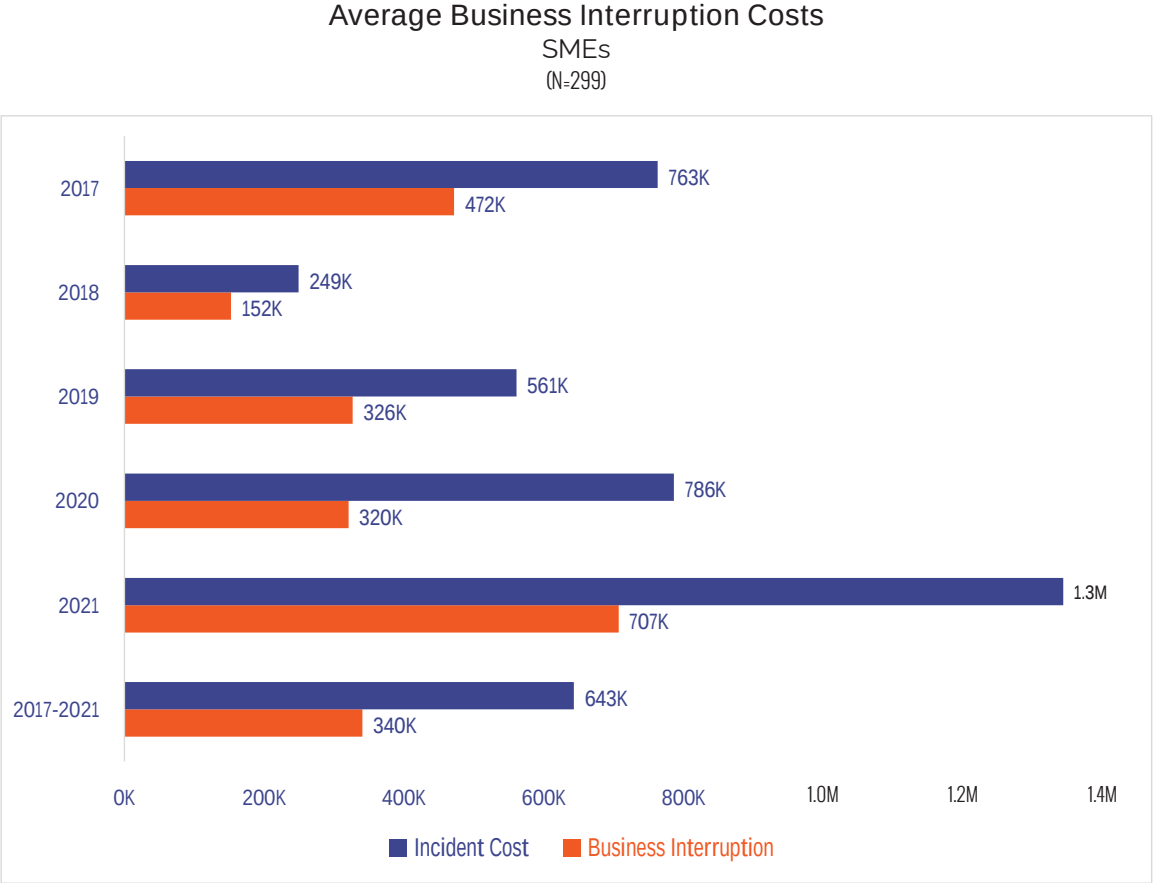


Figure 20

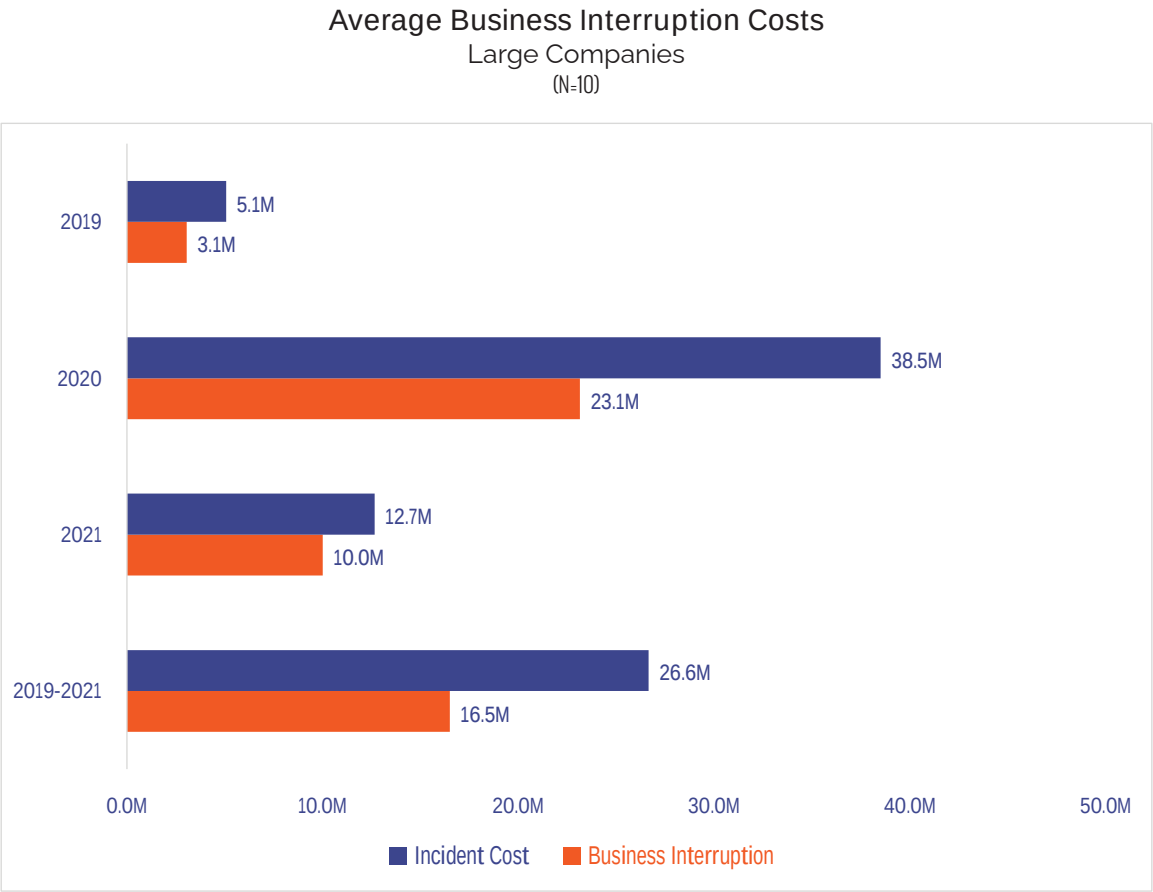

Average Business Interruption Costs
Large Companies
(N=10)
2019
5.1M
3.1M
2020
38.5M
23.1M
2021
12.7M
10.0M
2019-2021
26.6M
16.5M
0.0M
10.0M
20.0M
30.0M
40.0M
50.0M
Incident Cost
Business Interruption

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.

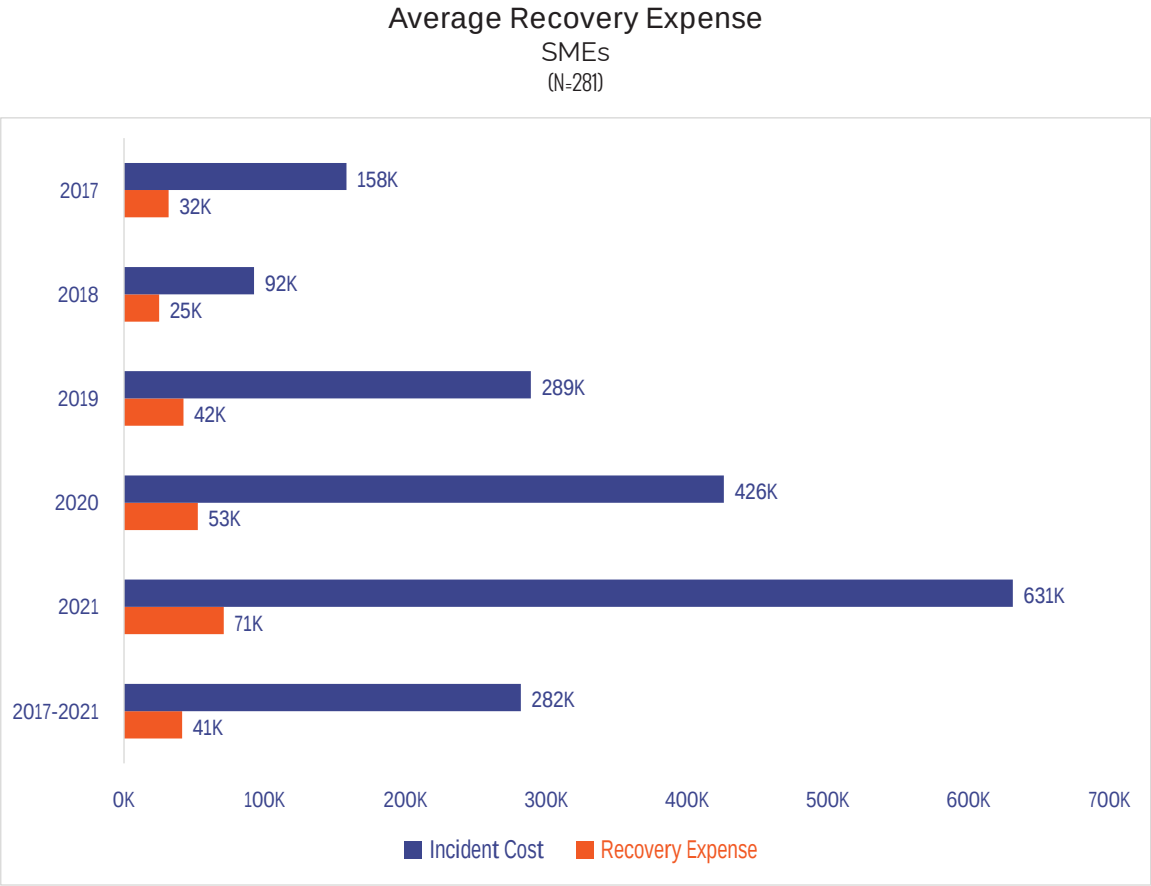


Figure 22

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.

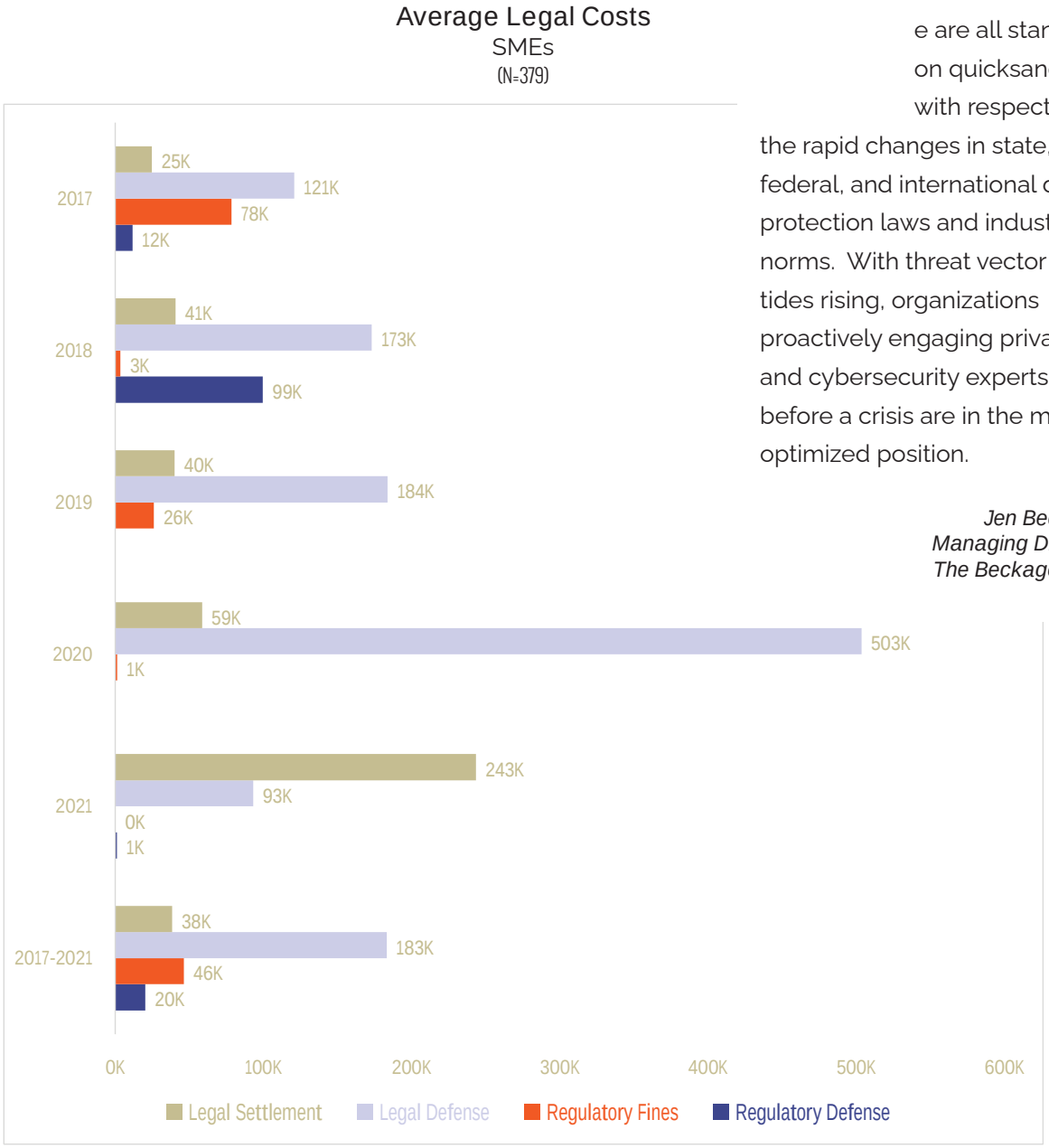


Figure 23

e 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.

Average Number of Records Exposed
SMEs
(N=732)

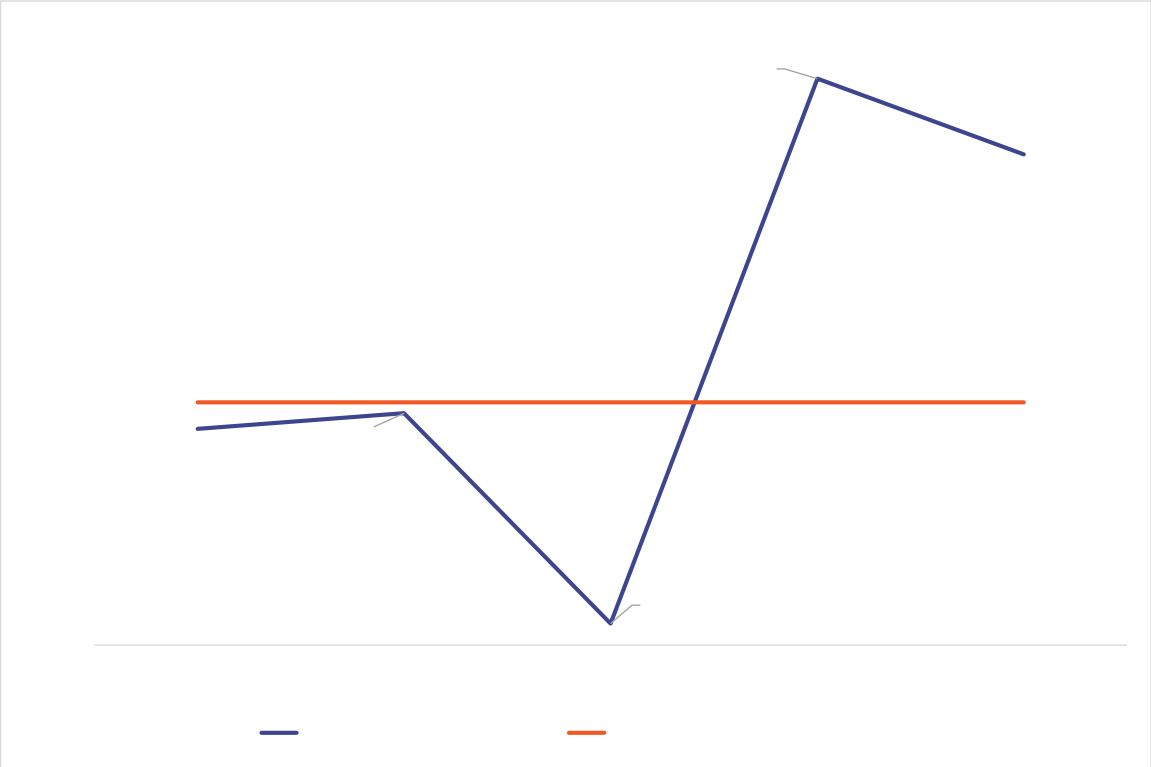


Figure 24

e'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)

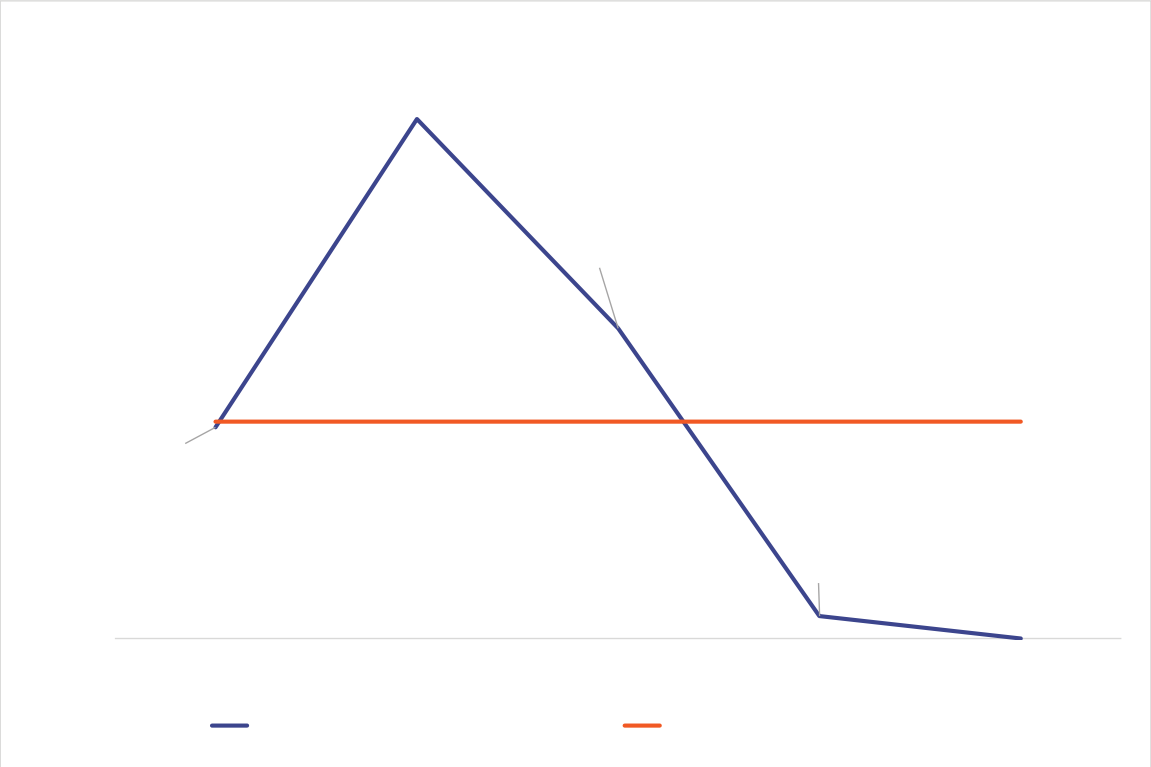


Figure 25

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.

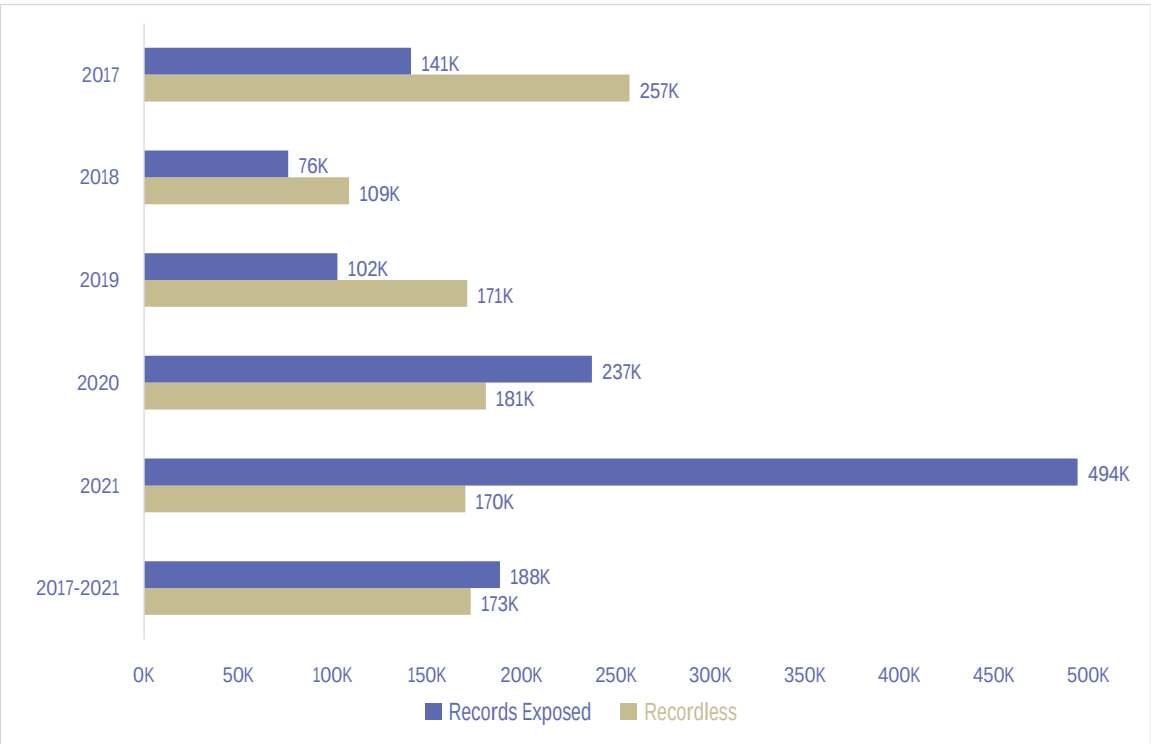


Figure 26

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%.

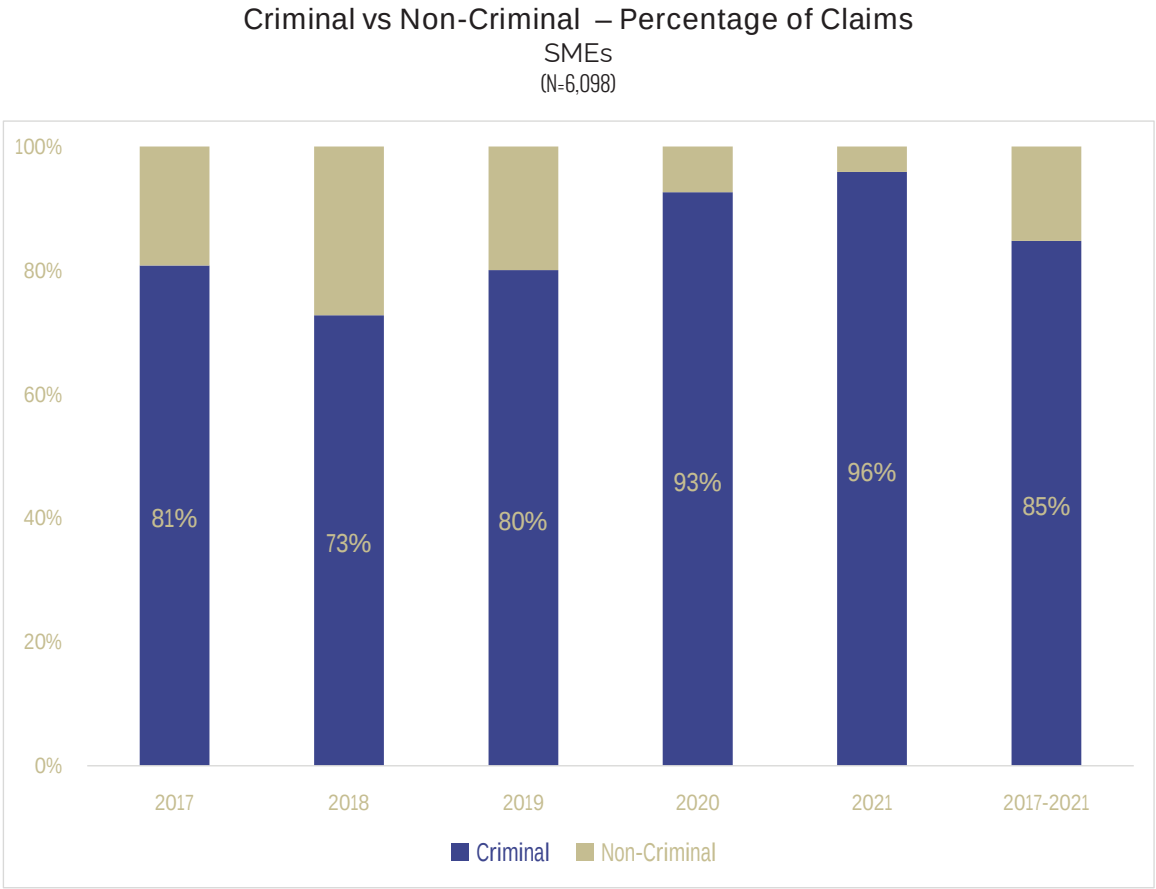


Figure 27

Criminal vs Non-Criminal – Average Costs

SMEs
(N=6,098)

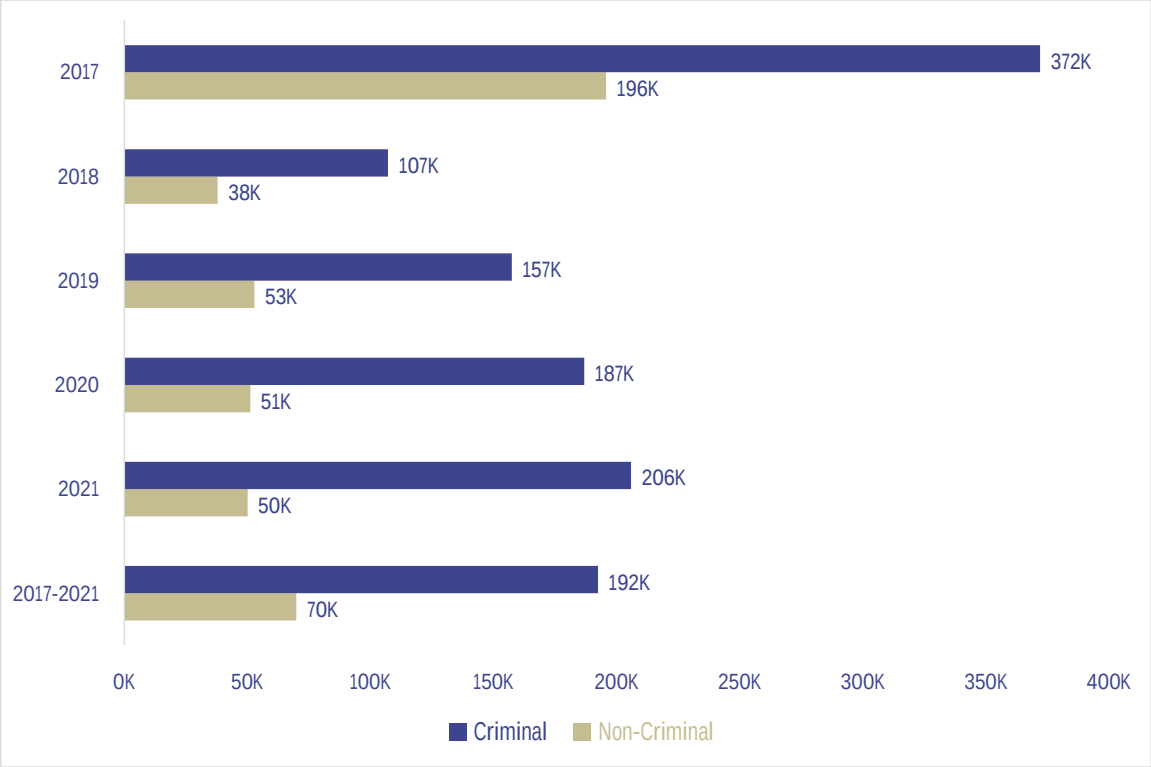


Figure 28

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.

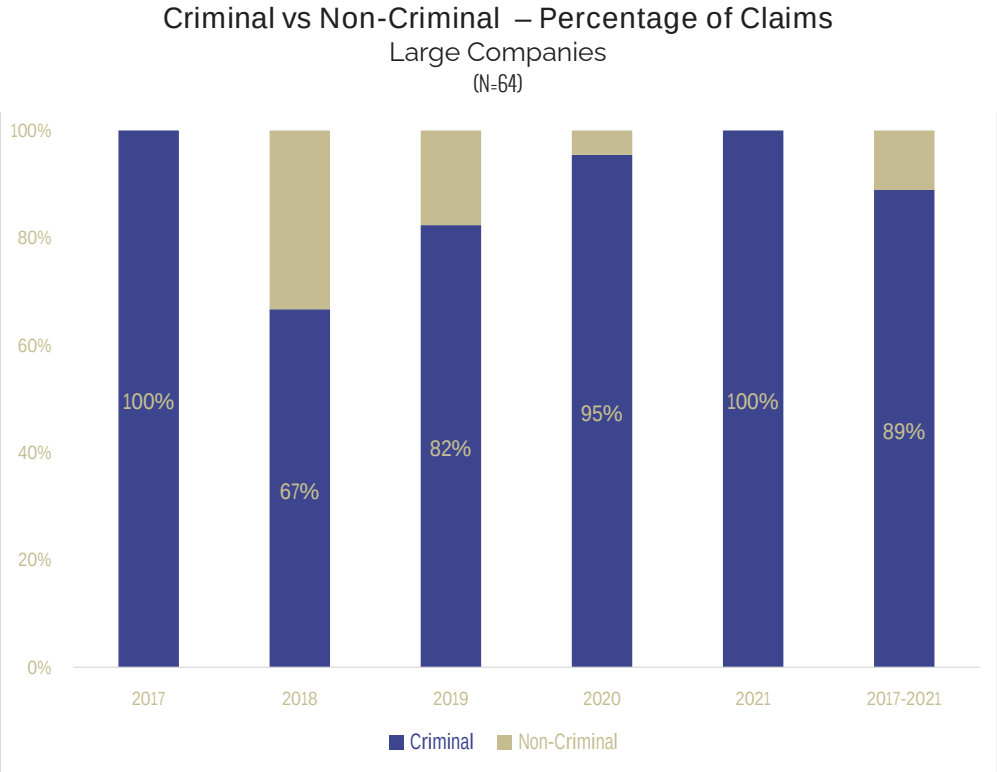


Figure 29

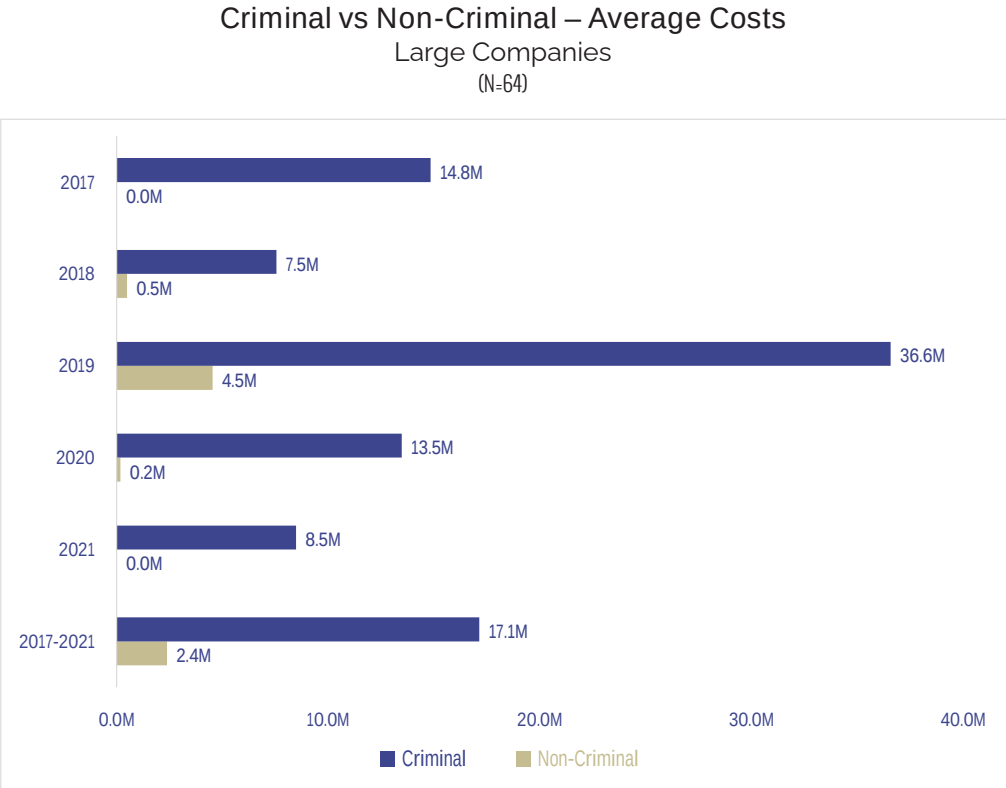


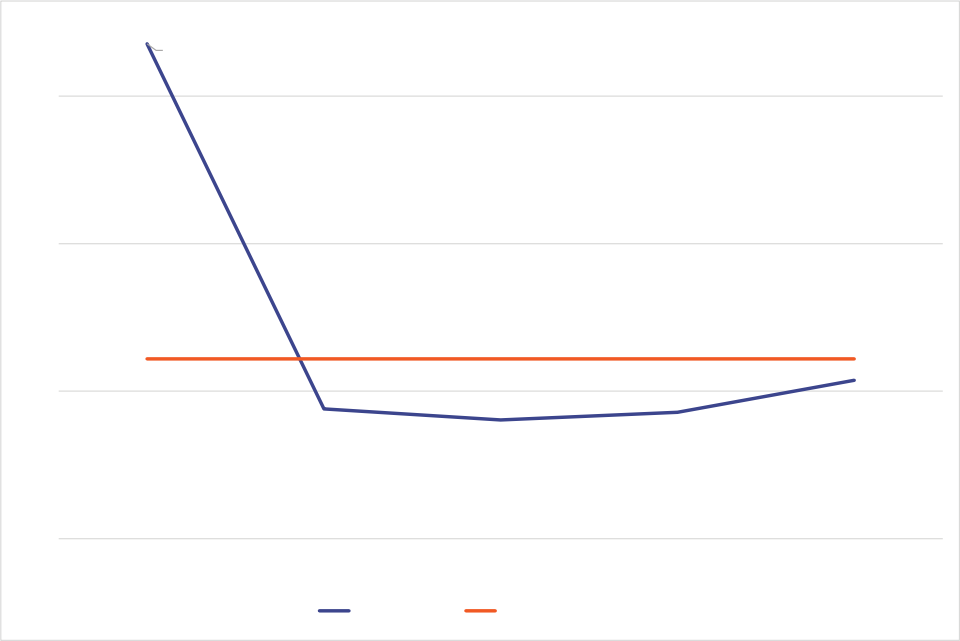
Figure 30

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.

Average SIR
SMEs
(N=4,343)



Large Companies
(N=64)

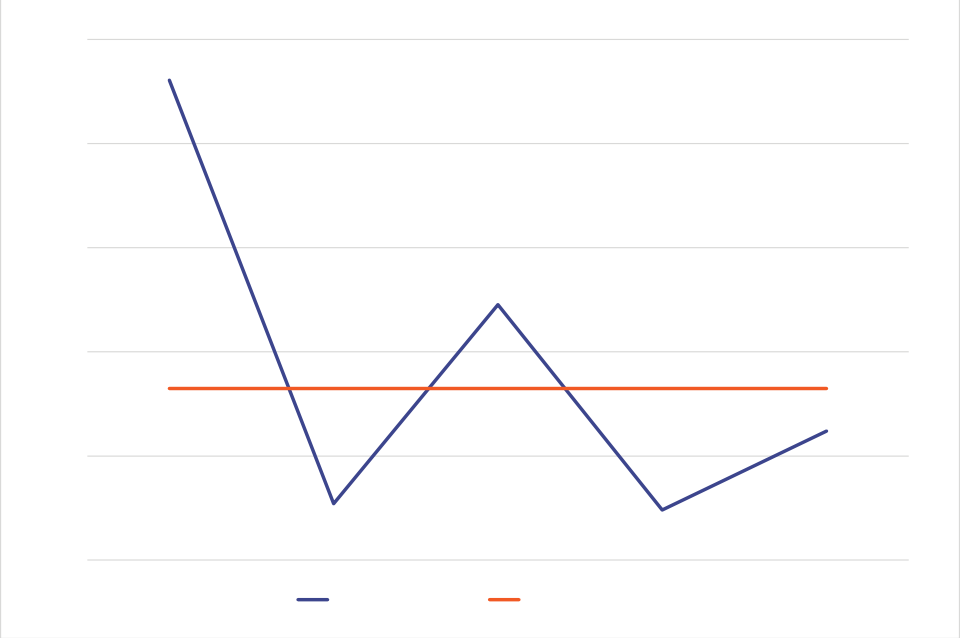


Figure 31

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)

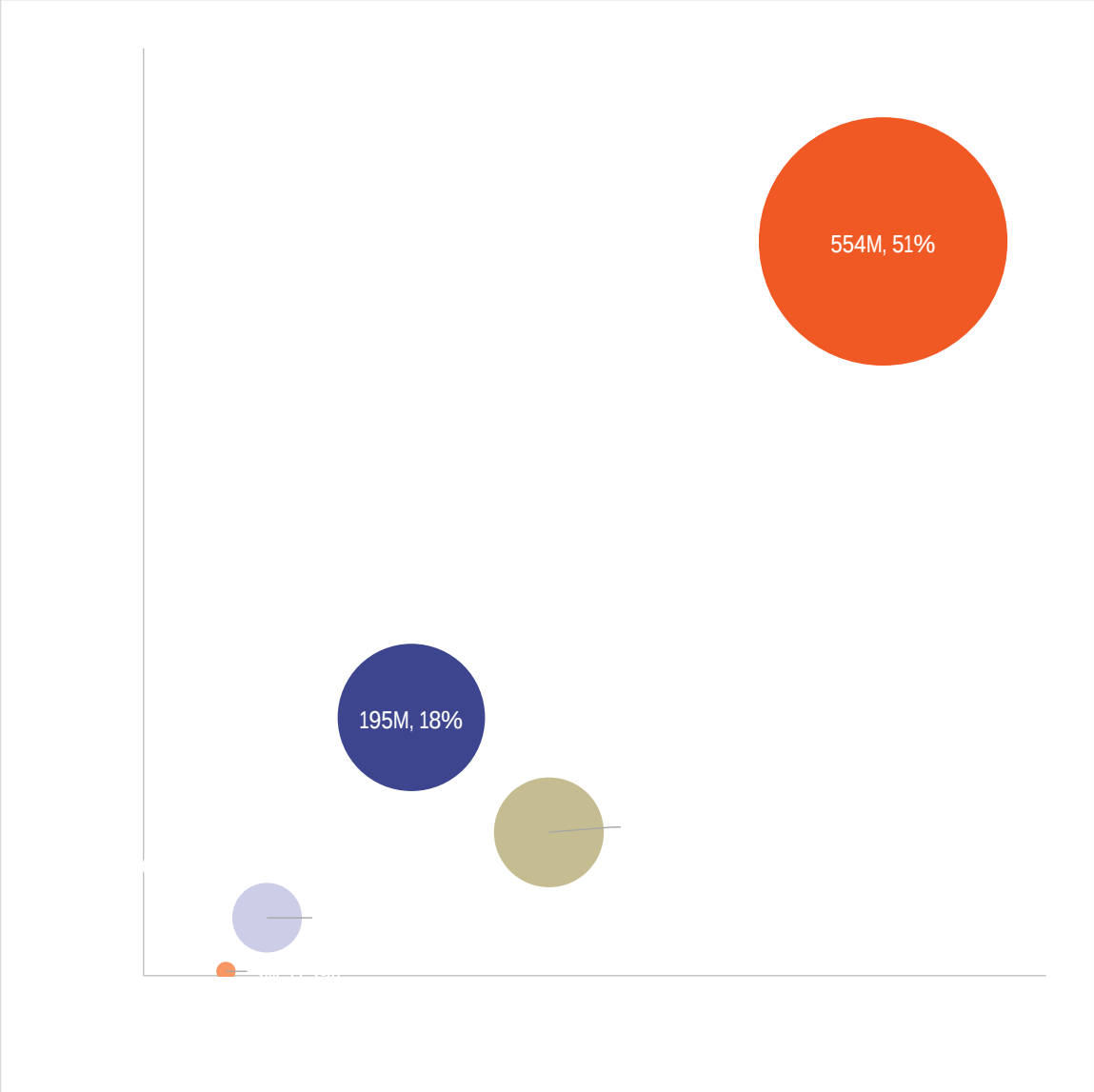


Figure 32

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.