

NetDiligence[®]

CYBER CLAIMS STUDY

2021 REPORT



OUR SPONSORS



Contents

Introduction.....	1
Key Findings.....	2
An Overview of the Data.....	7
Claims by Year of Event.....	7
Crisis Services and Incident Costs.....	7
Distribution of Crisis Services Costs.....	10
Business Interruption and Recovery Expense.....	13
SMEs.....	13
Large Companies.....	14
Legal Costs.....	14
Exposed Records.....	15
Recordless Claims versus Claims with Exposed Records.....	17
Criminal vs Non-Criminal Activities.....	18
Self-Insured Retentions (SIRs).....	20
Topics of Special Interest.....	21
Company Size and Loss Magnitude: Does Size Really Matter?.....	21
Top Causes of Loss at SMEs.....	22
Ransomware.....	23
Top Affected Sectors.....	25
Claims from Public Entities.....	26
Claims from Canada.....	27
Conclusion.....	28
Insurance Industry Participants.....	28

Appendices29

- Revenue Size.....29
- Business Sector.....31
- Cause of Loss.....34
- Type of Data.....37

Insights from Our Sponsors.....40

- RSM – Ransomware-as-a-Service (RaaS): A new business model for cyber criminals.....40
- Experian® – The Cyber-Demic: Why Data Breach Preparedness Is in Hyperdrive, How We Got To Herd Inevitability and The Only Path Forward.....42
- Guidewire – Hiding in Plain Sight: Towards Now-Gen Cyber Risk Underwriting.....44
- Beckage – This year’s study demonstrates that every enterprise must consider its ability to withstand cyberthreats.....46

About NetDiligence®48

About the Study.....49

- Contributors49
- Methodology.....49



Introduction

Welcome to the eleventh annual NetDiligence® *Cyber Claims Study*. Each year the study has grown, from fewer than 100 claims in 2011 to almost 6,000 claims in 2021. This large number of claims has allowed us to explore the data more thoroughly and produce the most comprehensive report ever. Growth continues in the number of claims submitted, as well as the in categories of the data analyzed.

This report includes incidents that occurred during the five-year period 2016–2020. A total of 5,797 claims was analyzed. By comparison, the sixth *Cyber Claims Study*, published in 2016, analyzed fewer than 200 cyber insurance claims. While many of the categories over the last five years have remained the same, the data has changed, sometimes dramatically.

By the Numbers

- 5,797 claims analyzed, arising from incidents that occurred during 2016–2020
- 3,000 new claims collected in 2021, from incidents occurring from 2018–2020
- 1,423 claims analyzed arising from incidents occurring in 2020
- 99% of claims (\$537M in total) from Small to Medium Enterprises (SMEs) with less than \$2 billion in annual revenue
- 1% of claims (\$727M in total) from Large Companies with more than \$2 billion in annual revenue
- Almost 1,500 claims due to ransomware, 55% of which occurred in 2019 and 2020
- 557 ransomware claims which provide both the ransom demand and the total incident cost

To present more accurate pictures of the business impact of cyber events on smaller versus larger organizations, findings for SMEs are often presented separately from findings for large companies¹.

Preliminary Observations

- As has been the case since the first *Cyber Claims Study* was published eleven years ago, there are enormous variances in the magnitude of the loss data. The smallest claims are less than \$1,000 and the largest are over \$120M. The numbers of records exposed range from 1 to over 300M.

- There are often dramatic differences between the numbers for SMEs and Large Companies – multiples of 10x, 50x, or more. The biggest Large Company in the dataset (over \$30B in annual revenue) is approximately 2.7 million times larger than the smallest organization (less than \$15K in annual revenue). The average Large Company in the dataset (\$11B in annual revenues) is more than 130 times larger than the average SME (\$84M).
- As will be discussed in the report, there is no clear correlation between the size of an entity and the magnitude of a cyber-related loss. Sometimes a smaller organization will experience a very expensive claim (>\$100M) and a large organization will have a claim so small (less than \$5,000) that it makes one wonder why the claim was filed in the first place. In fact, the most expensive incident during the five-year period occurred at an SME.

With Appreciation

We want to sincerely thank the cyber insurers listed on page 28 for their support of this report and their dedication to industry education. Many of them have contributed to this research every year for 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.



¹ Given the small number of claims for Large Companies, analysis is not always meaningful and so findings are usually presented for SMEs only.

Key Findings

Company Size

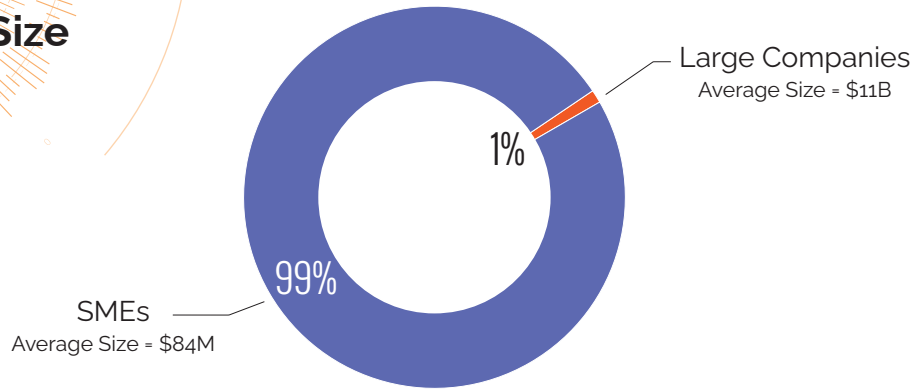


Figure 1

Average Costs for All Claims

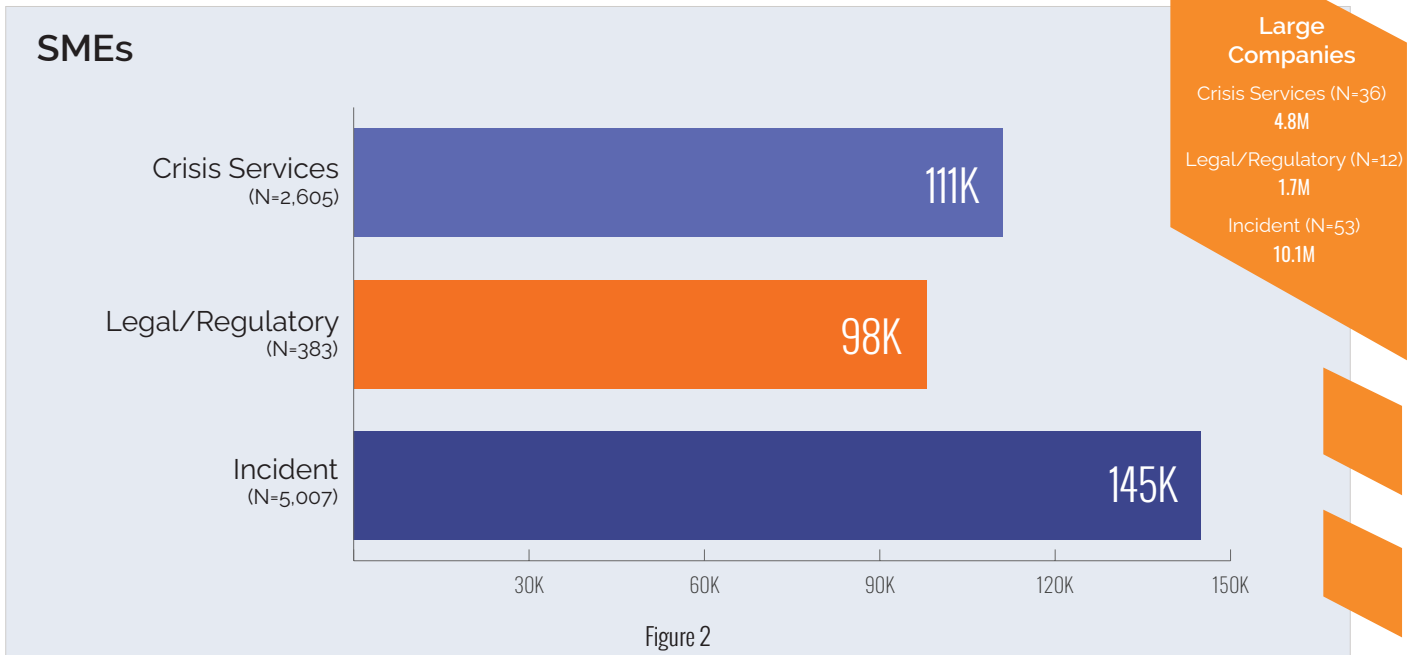


Figure 2

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)

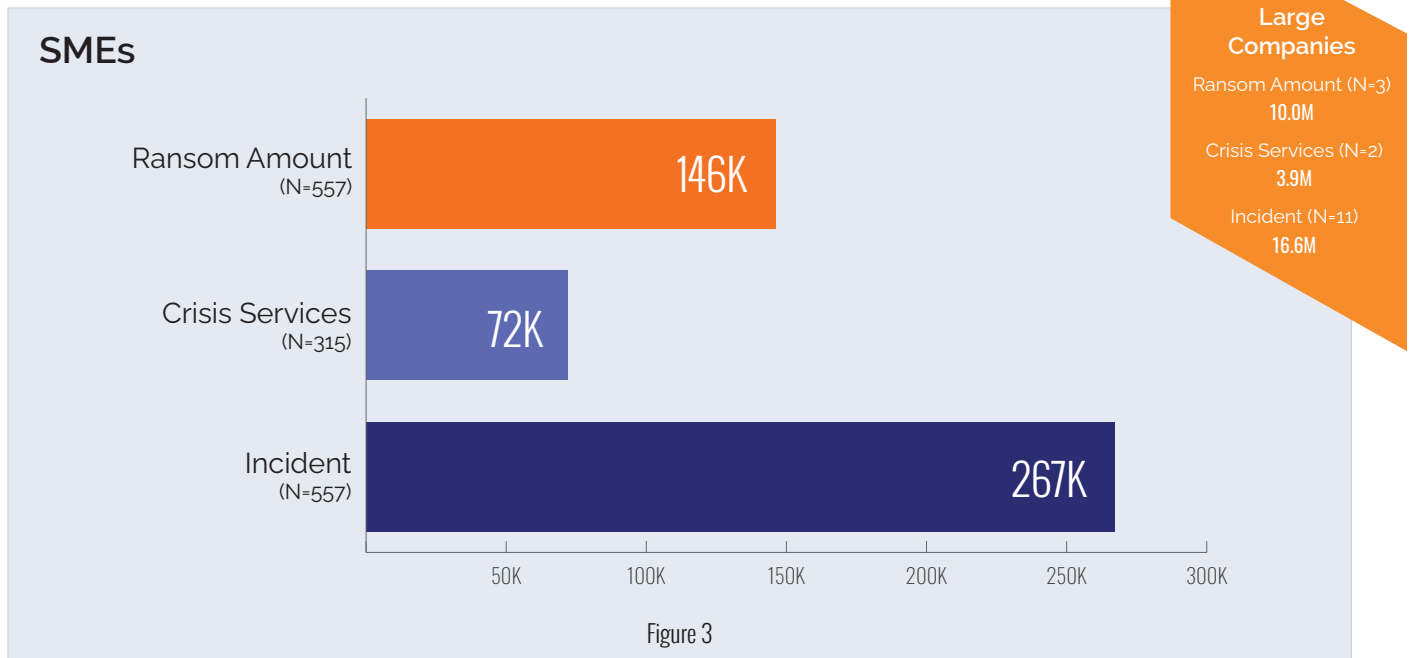
Categorized in this study as organizations with less than \$2 billion in annual revenue.

Large Company

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

All findings are for the five-year period 2016–2020 unless otherwise noted.
NetDiligence and Breach Coach are registered trademarks of Network Standard Corporation, dba NetDiligence.

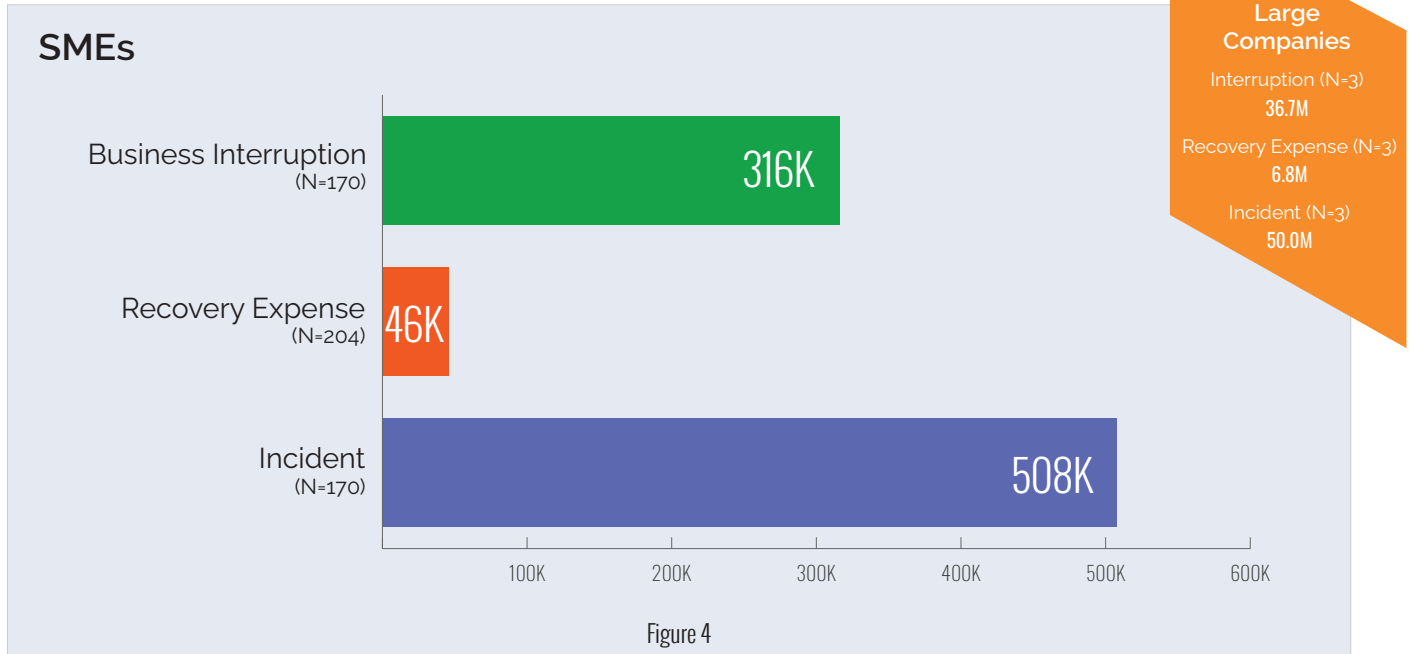
Average Costs for Ransomware



Ransomware is not slowing down or letting up. Readiness is a necessary lifeline to survive in this Cyber-demic environment. Experian® Reserved Response is the only program that offers a proven path forward that delivers live drills, a scalable infrastructure, and a guarantee to mitigate brand damage, customer migration, regulatory scrutiny, and executive termination because of a failed data breach response.

Michael Bruemmer
Experian® Data Breach Resolution

Average Costs for Business Interruption



The significant upward trend in BI claims and costs demand risk prevention guidance throughout the policy lifecycle: from initial binding/renewal, through to continuous monitoring during the policy period, and finally with the collection of more robust incident claims data that relates back to frontend risk control guidance.

Erin Kenneally
Guidewire, Director, Cyber Risk Analytics

Business Sector

Top 5 by Number of Claims – SMEs

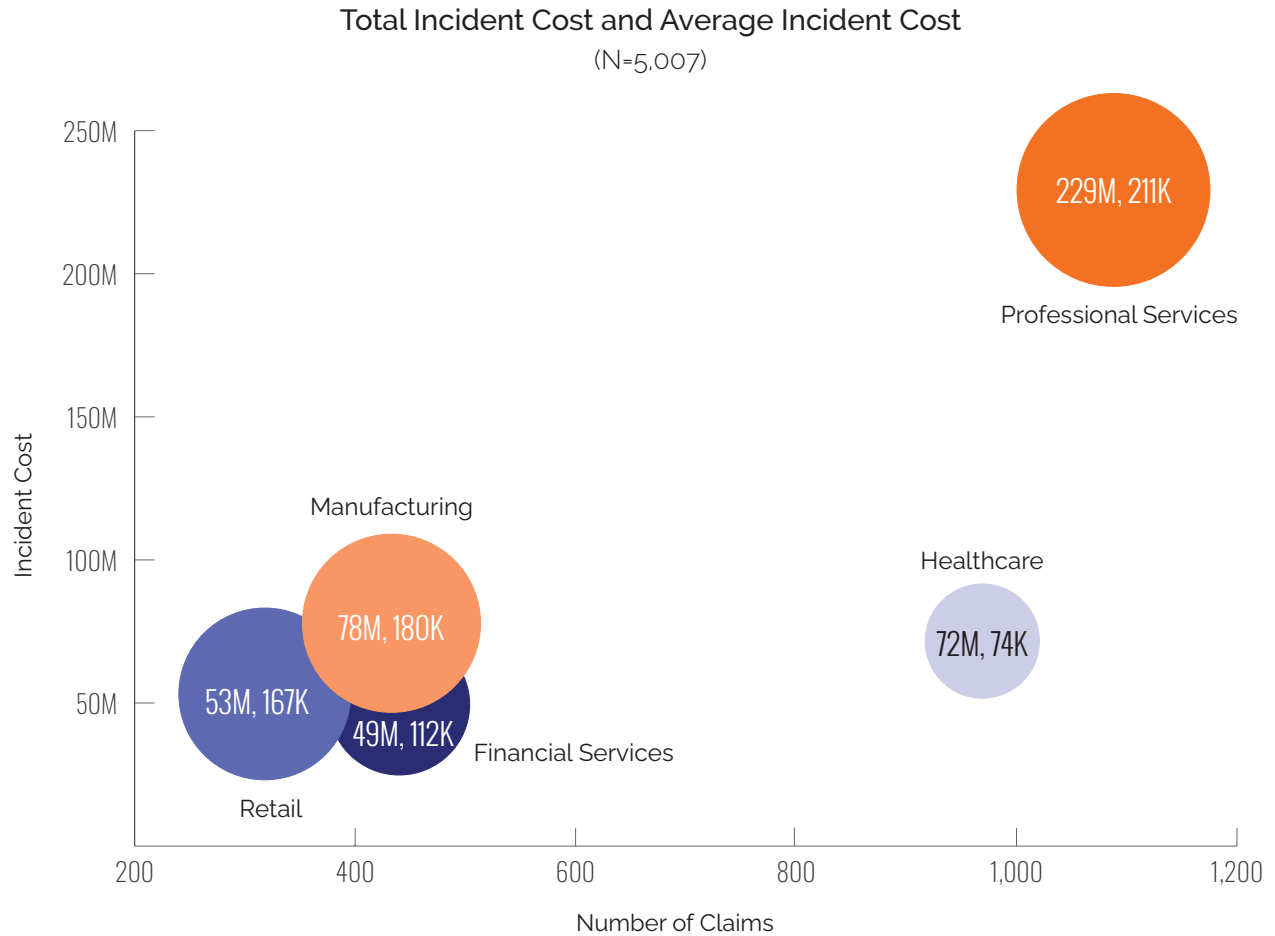


Figure 5

Every enterprise must consider its ability to withstand cyberthreats, comply with an increasingly complicated constellation of state, federal, and international regulations, and prepare to respond to incidents now.

Jennifer Beckage
Founder, Beckage

Cause of Loss

Top 5 by Number of Claims – SMEs

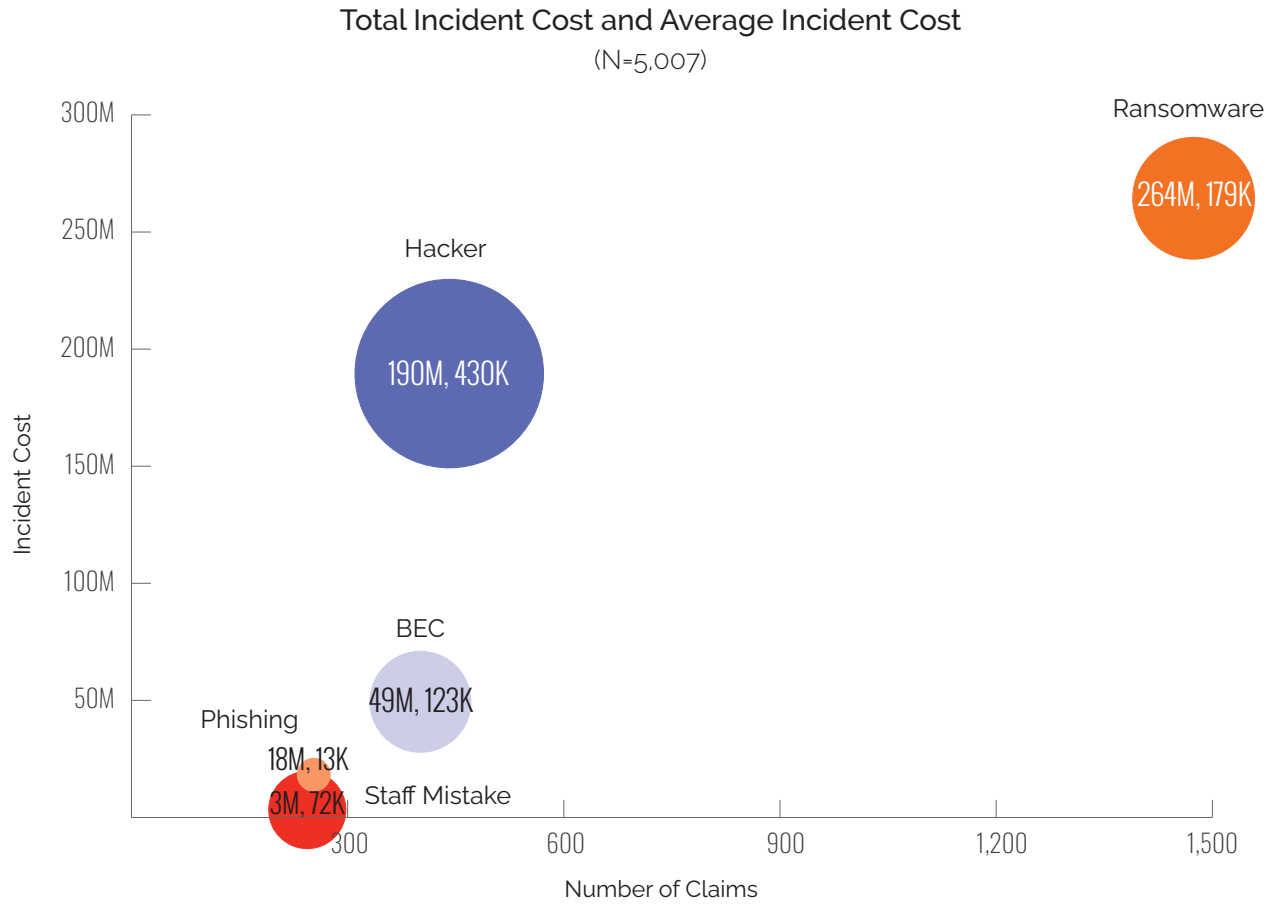


Figure 6



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 \$30B. 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 (64%) 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 \$84M.
- Large Companies: annual revenue ranged from \$2B to more than \$30B. The average was \$11B.

These companies represent more than 18 business sectors.

For SMEs, the top five sectors as defined by number of claims were:

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

For Large Companies, the top five sectors as defined by number of claims were:

- Healthcare
- Technology
- Financial Services
- Retail
- Education

Additional analysis by Business Sector and Revenue Size appear later in this report.

Claims by Year of Event

Percentage of Claims by Date of Event
(N=5,797)

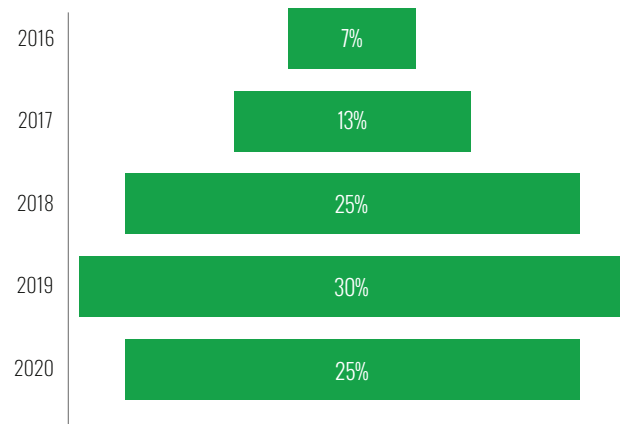


Figure 7

The scope of this study is 5,797 incidents that occurred from 2016-2020. The distribution of claims over this five-year period is depicted in Figure 1. The number of claims collected and analyzed per year has increased from almost 400 in 2016 to over 1,700 in 2019 and 1,400 in 2021.²

Crisis Services and Incident Costs

For all organizations, Crisis Services costs ranged from less than \$100 to more than \$120M. Incident cost, inclusive of Self-Insured Retention (SIR), ranged from less than \$1,000³ to more than \$120M. The averages were influenced by some very expensive claims. At SMEs, there were six claims in 2017 with total incident cost of more than \$5M, one of which exceeded \$100M. At Large Companies, there were ten claims ranging from \$15M to \$100M.

At SMEs, Crisis Services costs in 2020 averaged \$113K (ranging from less than \$100–\$2.1M). Total incident cost averaged \$286K (\$1K–\$7.6M). For the five-year period, Crisis Services costs averaged \$111K (ranging from less than \$100–\$120M). The average incident cost during this time frame was \$165K (ranging from less than \$1,000–\$120M).

² New claims are collected for incidents that occurred during the previous three calendar years. For the 2021 study, these were incidents in 2018, 2019, and 2020.

³ A few claims for less than \$1K were excluded from the analysis.

Average Crisis Services and Incident Costs – SMEs

(N=5,007)

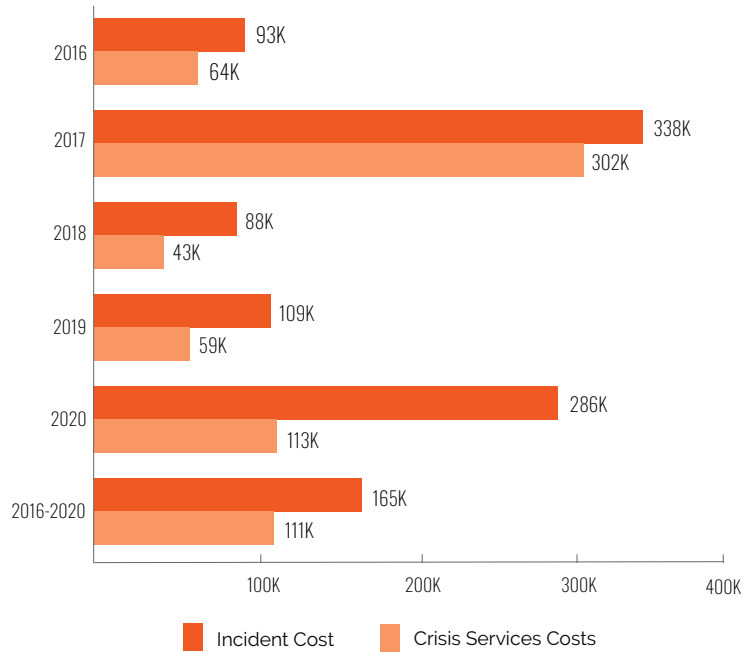


Figure 8

For Large Companies in 2020, Crisis Services costs averaged \$2.3M (ranging from less than \$5K-\$7.3M). The average incident cost in 2020 was \$10.4M (\$55K-\$55M). Over five years, the average was \$7.6M (ranging from less than \$5K-\$100M).

Average Crisis Services and Incident Costs – Large Companies

(N=53)

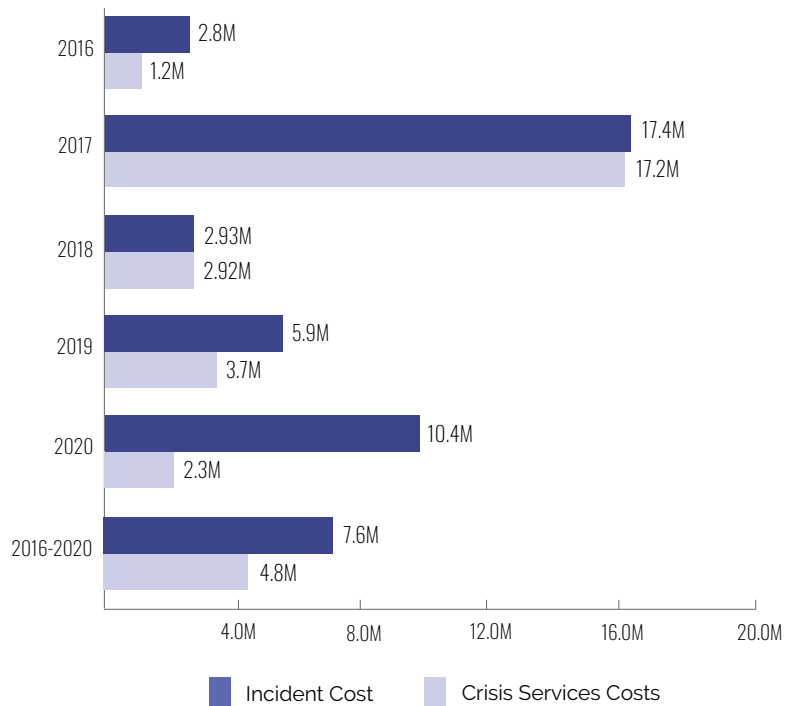


Figure 9

For all organizations, Crisis Services costs ranged from less than \$100 to more than \$120M.

The following two graphs depict Crisis Services costs as a percentage of total incident cost. These percentages are quite variable, going from 39% to 89% for SMEs and from 22% to 100% for Large Companies. The extent to which Crisis Services costs are a significant component of total incident cost is entirely dependent upon the nature of the incident. Many ransomware and banking fraud incidents do not utilize Crisis Services, whereas complex hack and malware/virus incidents often incur significant Crisis Services costs.

Crisis Services as a Percentage of Incident Cost – SMEs

(N=5,007)

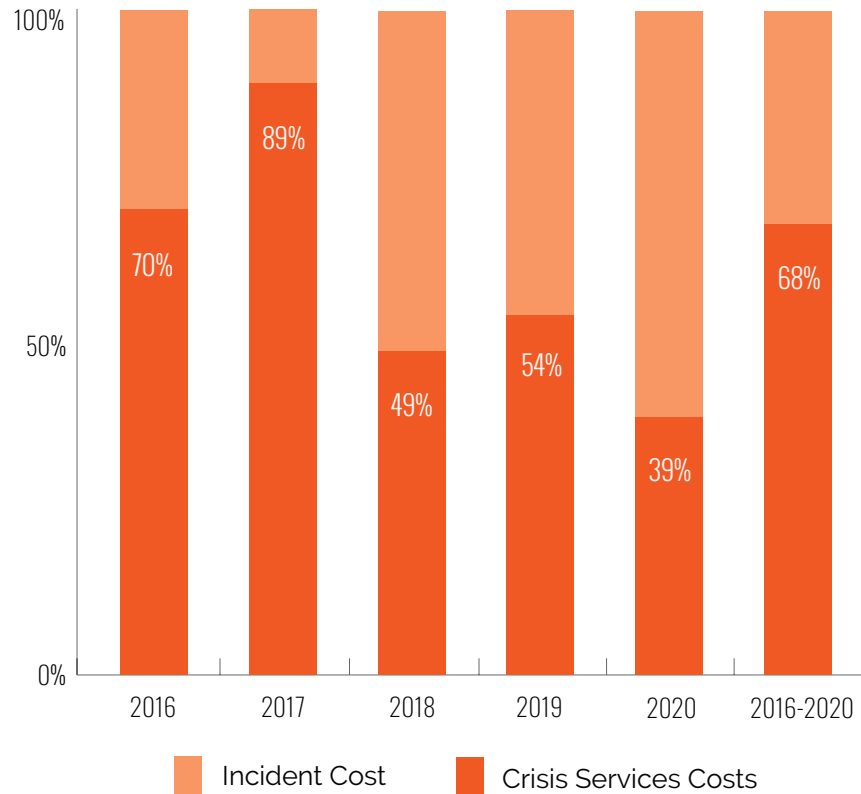


Figure 10

Crisis Services as a Percentage of Incident Cost – Large Companies
(N=53)

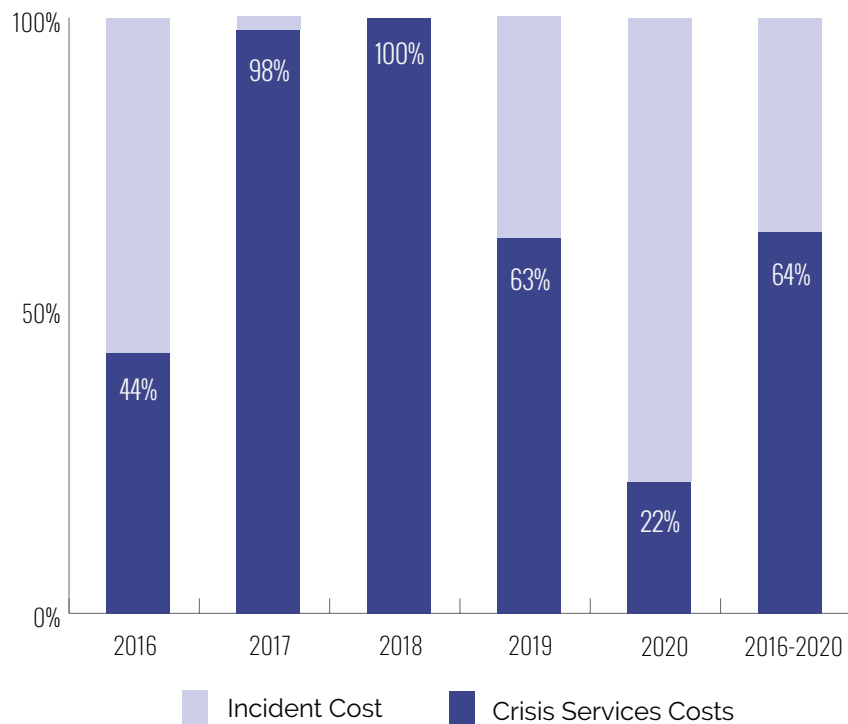


Figure 11

Distribution of Crisis Services Costs

The following graphs depict the year-by-year average individual Crisis Services costs for SMEs, as well as the year-by-year and five-year percentage distribution of individual Crisis Services costs⁴ for both SMEs and Large Companies. Incidents that expose records usually have significant costs in all categories. Ransomware and wire transfer fraud events often have no forensics, monitoring, or notification costs.

Figure 6 displays the average cost of each individual crisis service. Forensic services and Other crisis services have the highest average in each of the five years.

At SMEs, the percentage of forensics and legal guidance costs is fairly uniform, ranging from 47%–53% for forensics and 17%–27% for legal guidance. Monitoring costs are negligible and notification costs range from 1%–11%.

At Large Companies, the distribution of Crisis Services costs can be quite variable and heavily dependent upon not only the type of incident but also one or two mega-events.

⁴ Forensics costs typically include the cost of incident response services. However, when the victim organization engages an incident response company to negotiate and pay a ransom, forensics costs will sometimes include the cost of the ransom. Other crisis services costs typically include public relations costs. However, some insurers put ransom amounts and even data recovery in this category.

Average Crisis Services Costs – SMEs
(N=2,605)

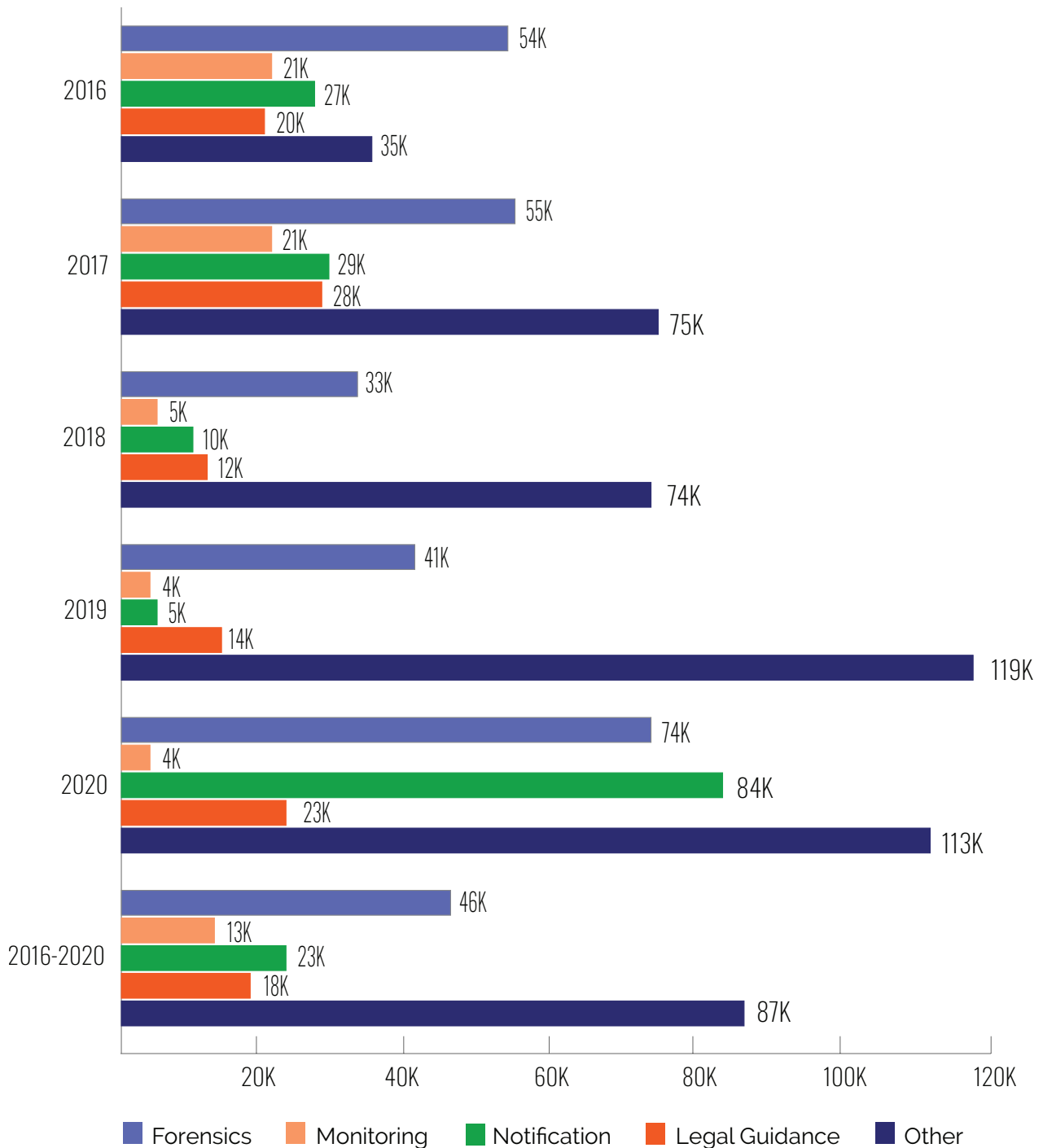


Figure 12

⁴ Forensics costs typically include the cost of incident response services. However, when the victim organization engages an incident response company to negotiate and pay a ransom, forensics costs will sometimes include the cost of the ransom. Other crisis services costs typically include public relations costs. However, some insurers put ransom amounts and even data recovery in this category.

Distribution of Crisis Services – SMEs
(N=2,605)

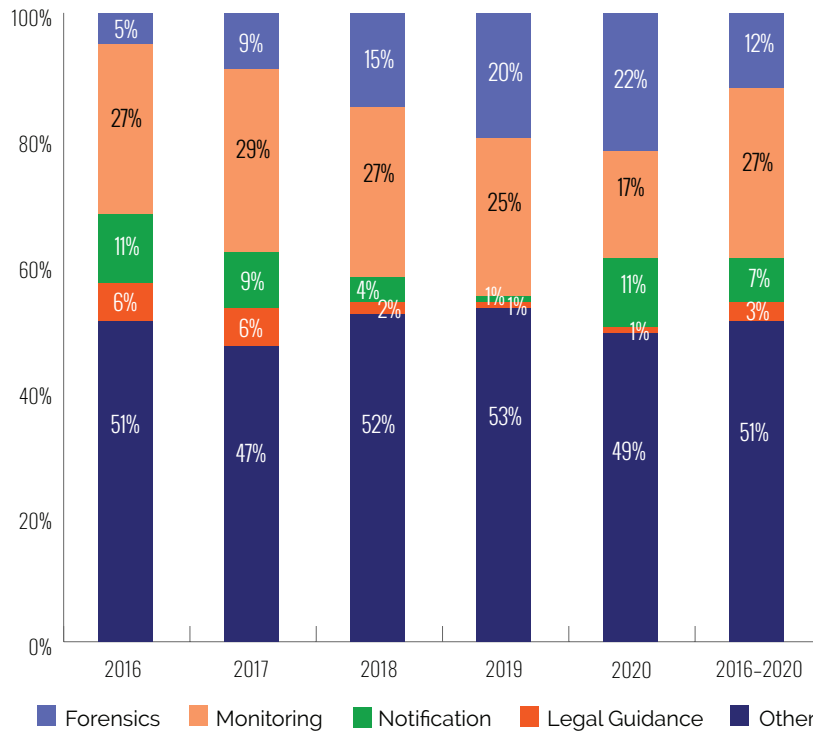


Figure 13

Distribution of Crisis Services – Large Companies
(N=36)

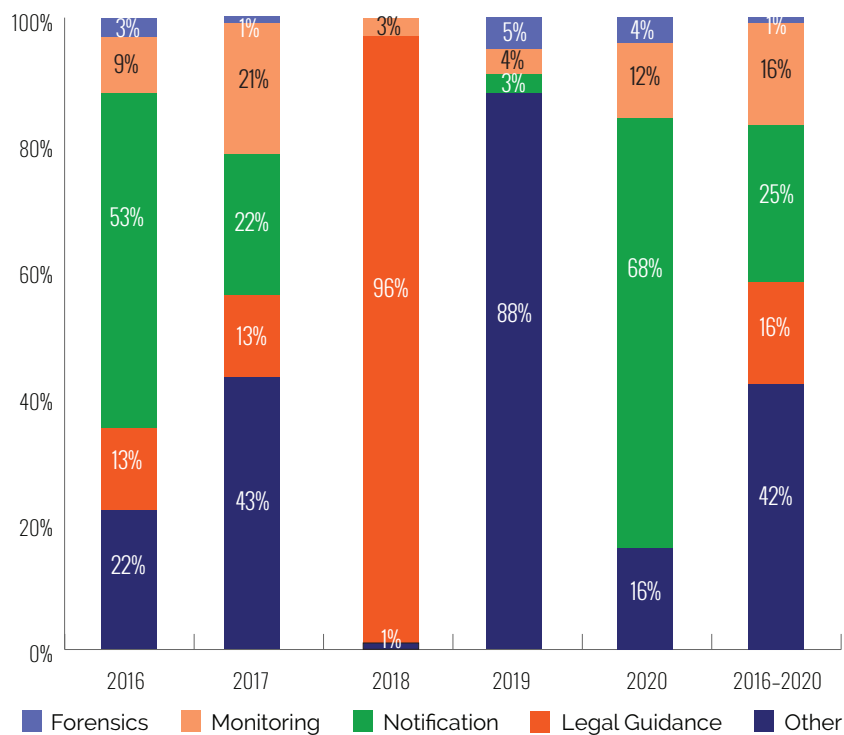


Figure 14

Business Interruption and Recovery Expense

SMEs

Of the 5,716 claims at SMEs, 170 included costs for business interruption (BI) and 204 included costs for recovery expense. Only 49 claims incurred both BI and recovery expense.

Overall, BI costs in 2020 averaged \$446K (\$3,500-\$3M). The total incident cost for these claims averaged \$898K (\$25K-\$3.1M). For the five-year period, the average BI costs were \$316K (<\$150 to \$10M). Total incident cost averaged \$508K (\$4K to \$17.5M). In 2020 and over five years, the average incident cost with BI is significantly higher than the overall average incident cost for the same periods.

Ransomware incidents accounted for 79% of the claims with a business interruption loss, followed by malware/virus (9%) and hacking (5%) incidents. The remaining claims (7%) were due to rogue employees, system glitches, and other/unknown causes of loss.

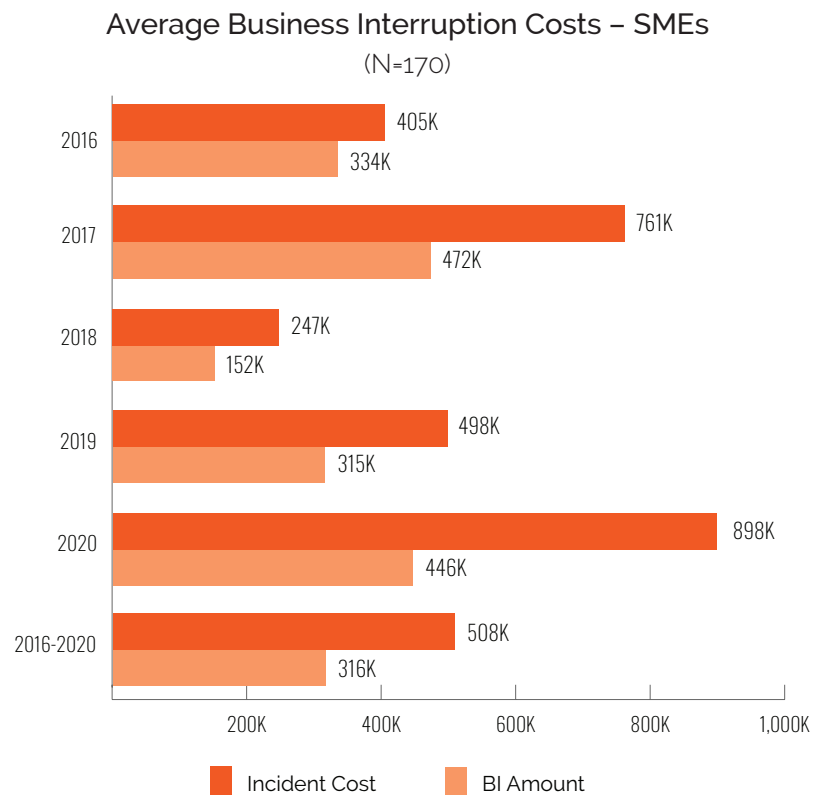


Figure 15

Recovery expense in 2020 averaged \$103K (less than \$1,700-\$1.6M). The total incident cost for these claims averaged \$412K (\$8K-\$1.7M). For the five-year period, these costs averaged \$46K (less than \$200-\$1.6M). The five-year average incident cost for a claim with recovery expense was \$181K (\$1,500-\$3.9M).

Ransomware incidents accounted for 81% of the claims with a recovery expense loss, followed by hacking (7%) and malware/virus (5%) incidents. The remaining claims (7%) were due to rogue employees, staff mistakes, system glitches, and other/unknown causes of loss.

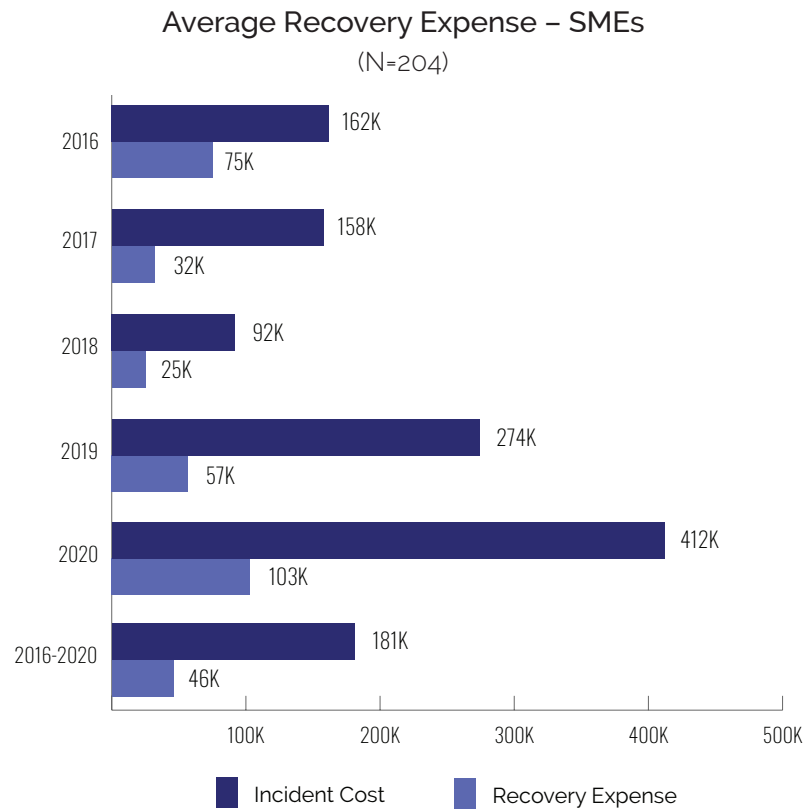


Figure 16

Large Companies

There were only five Large Company claims that included BI and/or recovery expense. Three of these involved ransomware, one involved malware, and one very large claim was caused by a system glitch/network outage. In 2020, these claims averaged a BI loss of \$25M. The total incident cost averaged \$35M. Over five years, the BI loss averaged \$37.7M and the total incident cost averaged \$50M. In 2020, the average recovery expense was \$133K and the average total incident cost was \$4M. The five-year incident amounts were \$6.8M and \$29.3M, respectively.

Legal Costs

In this year's report, we have combined the four categories of litigation cost—Legal Damages Defense, Settlement, Regulatory Defense, and Regulatory Fines—into a single category of Legal Costs.

There were 385 claims for legal costs from SMEs. In 2020, these costs ranged from less than \$500 to \$5.2M (average=\$411K). Over five years, these costs ranged from less than \$100 to \$6.8M (average=\$98K). At Large Companies, there were 13 claims for legal costs. In 2020, the total costs ranged from \$500K to \$8M (average=\$4.2M) and the five-year costs ranged from less than \$2K to \$8M (average=\$1.6M).

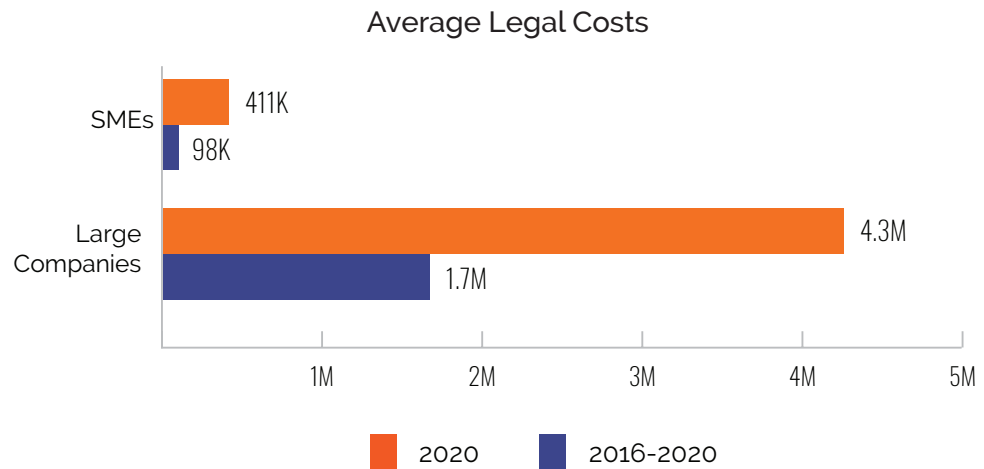


Figure 17

Exposed Records

Of the 5,797 claims in the dataset, 895 were for incidents that constituted some form of a data privacy incident, and thus exposed records. The total number of records exposed in these incidents was greater than 1.1 billion. The numbers of records exposed per claim ranged from a single record to over 300 million records. Incidents at SMEs accounted for 872 of these claims and 355 million records. Incidents at Large Companies accounted for 23 claims and 724 million records.

Incidents at Large Companies exposed, on average, 85 times more records than incidents at SMEs.

The average number of records exposed varies substantially from year to year for both SMEs and Large Companies. This is primarily because mega-incidents drive up the averages. In 2017 and 2020, incidents at SMEs exposed far greater numbers of records than in each of the other years. In 2018 and 2019, incidents at Large Companies exposed far greater numbers of records than in other years.

Figure 12 shows the average number of records exposed. These averages are dramatically different for SMEs and Large Companies. For the five-year period, incidents at Large Companies exposed, on average, 85 times more records than incidents at SMEs.

Average Number of Records Exposed – SMEs

(N=840)

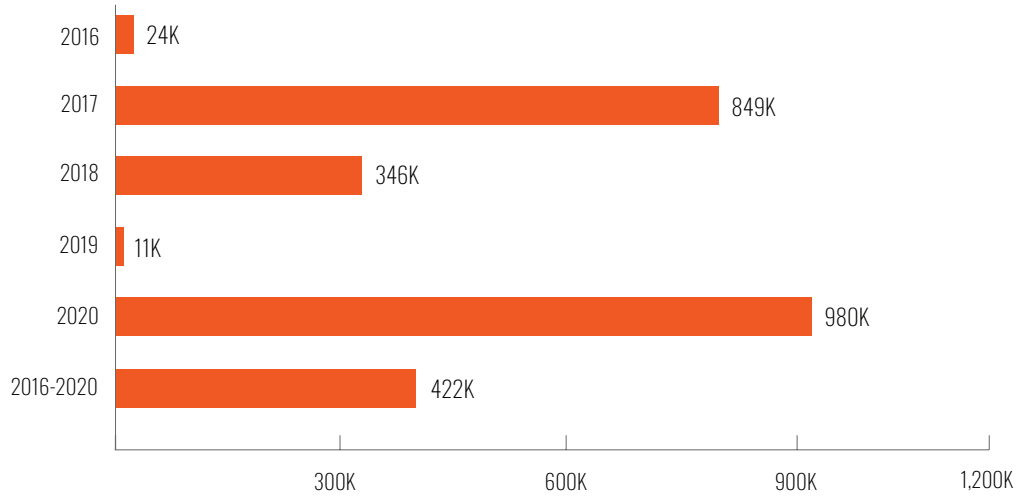


Figure 18

Average Number of Records Exposed – Large Companies

(N=20)

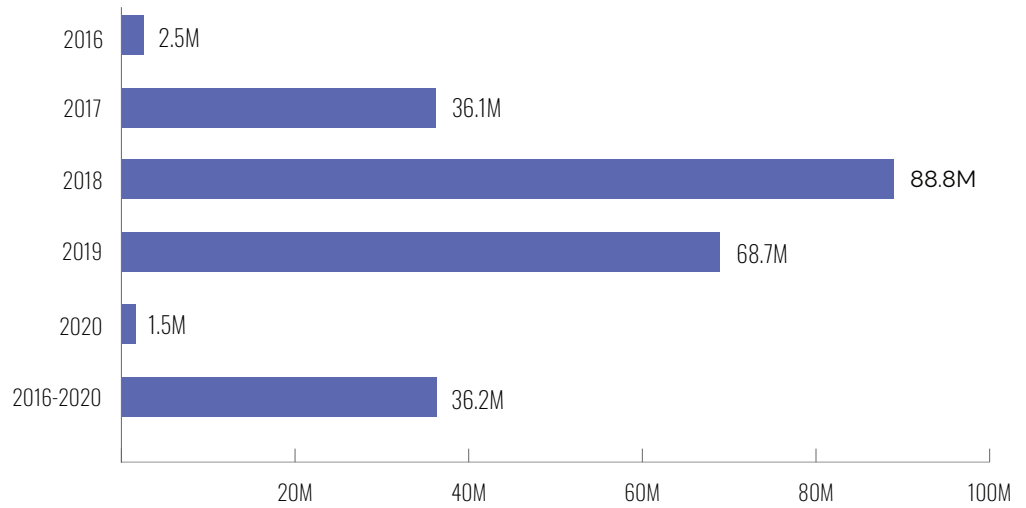


Figure 19

Recordless Claims versus 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) account for most of these incidents. In last year's report, recordless incidents accounted for 55% of claims in 2019 and 39% of claims over five years. In this year's report, these incidents account 70% in 2020 and 37% of claims over five years. This large increase in the proportion of recordless incidents is primarily due to the increased number of ransomware claims in 2020.

Average Incident Cost – Records Exposed vs Recordless – SMEs

Records Exposed (N=3,132); Recordless (N=1,875); Combined (N=5,007)

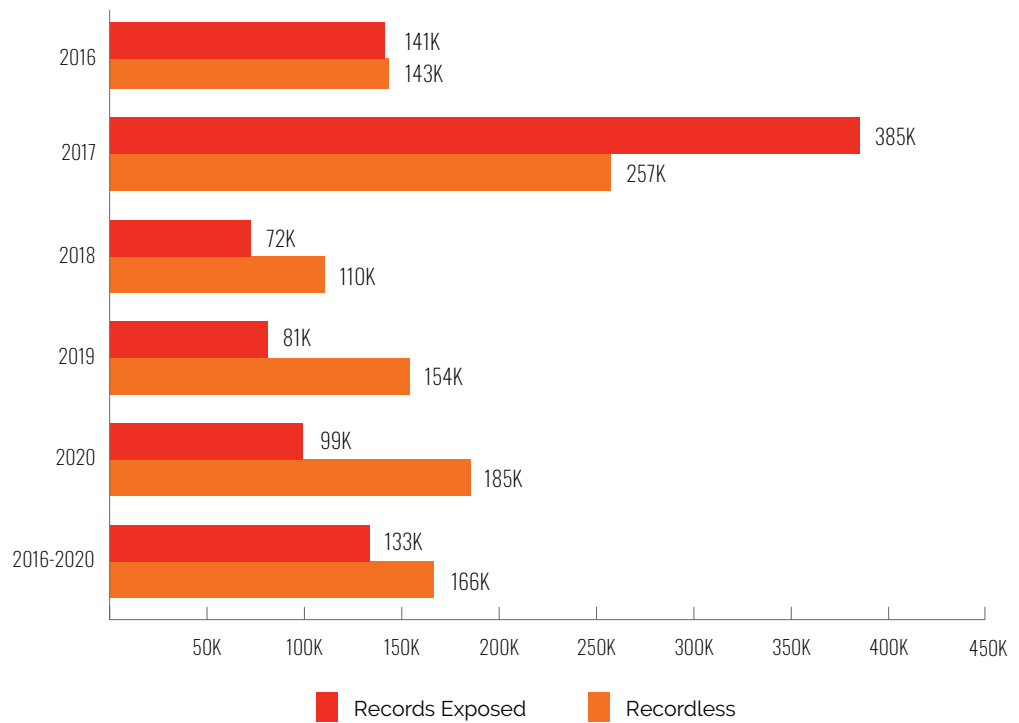


Figure 20

Criminal vs Non-Criminal Activities

Criminal incidents 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

Since 2016, the proportion of claims caused by criminal activities has ranged from a high of 83% to a low of 69%. The proportion of claims caused by non-criminal activities decreased from 28% in 2019 to 17% in 2020.

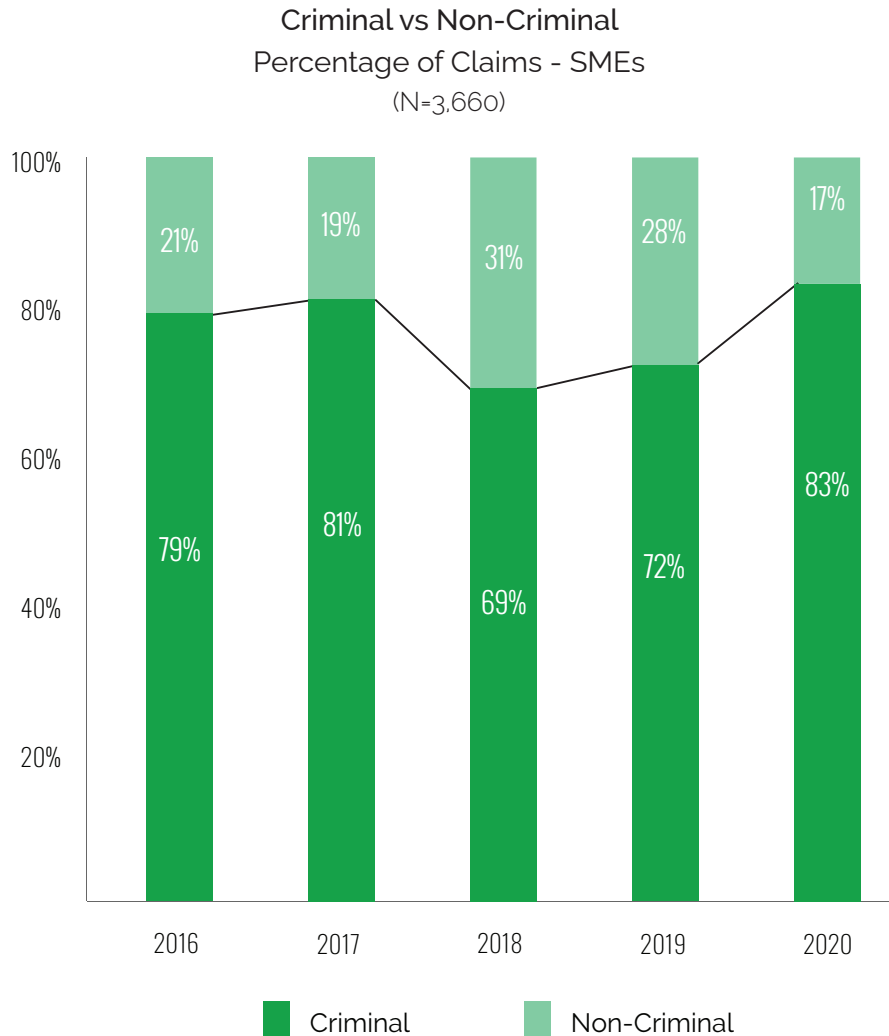


Figure 21

Criminal vs Non-Criminal
Average Incident Cost - SMEs
(N=3,660)

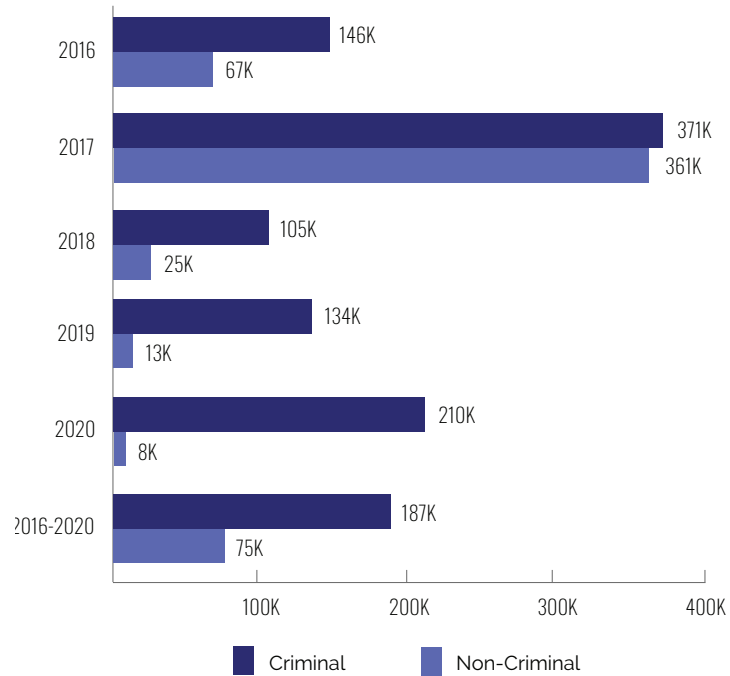


Figure 22

Average Incident and Crisis Services costs, as well as the average number of records exposed, were all dramatically higher for criminal events.

Criminal vs Non-Criminal – SMEs

Time Period	Impact	Type of Activity	Minimum	Average	Maximum	Total
2020 Criminal (N=611) Non-Criminal (N=25)	Records Exposed	Criminal	3	1M	30M	33.3M
		Non-Criminal	0.4K	4K	8.5K	8.9K
	Crisis Services	Criminal	0.1K	116K	2.1M	23M
		Non-Criminal	0.1K	8K	26K	41K
	Incident Cost	Criminal	1K	210K	7.5M	128.4M
		Non-Criminal	1K	9K	64K	233K
2016-2020 Criminal (N=3,241) Non-Criminal (N=419)	Records Exposed	Criminal	2	519K	143M	347.7M
		Non-Criminal	2	40K	1.8M	6.8M
	Crisis Services	Criminal	0.1K	97K	120.2M	41.1M
		Non-Criminal	0.1K	19K	540K	5.6M
	Incident Cost	Criminal	1K	187K	120.2M	606.3M
		Non-Criminal	1K	75K	17.5M	31.6M

Table 1

Self-Insured Retentions (SIRs)

The dataset contains 3,520 claims from SMEs that reported a value for SIR. Over five years, the size of SIR ranged from \$0 to \$10M. In 2020, SIR at SMEs ranged from \$1K to \$250K. The maximum SIR in 2020 dropped to \$250K, from \$350K in 2019 and \$500K in 2018.

Self-Insured Retentions (SIRs) – SMEs

	Claims	Minimum	Average	Maximum
2020	908	1K	14K	250K
2016–2020	3,520	0	28K	10M

Table 2

The following chart displays the average SIR for each of the previous five years as well as the five-year average. Since 2017, there has been a dramatic decrease in the average SIR.

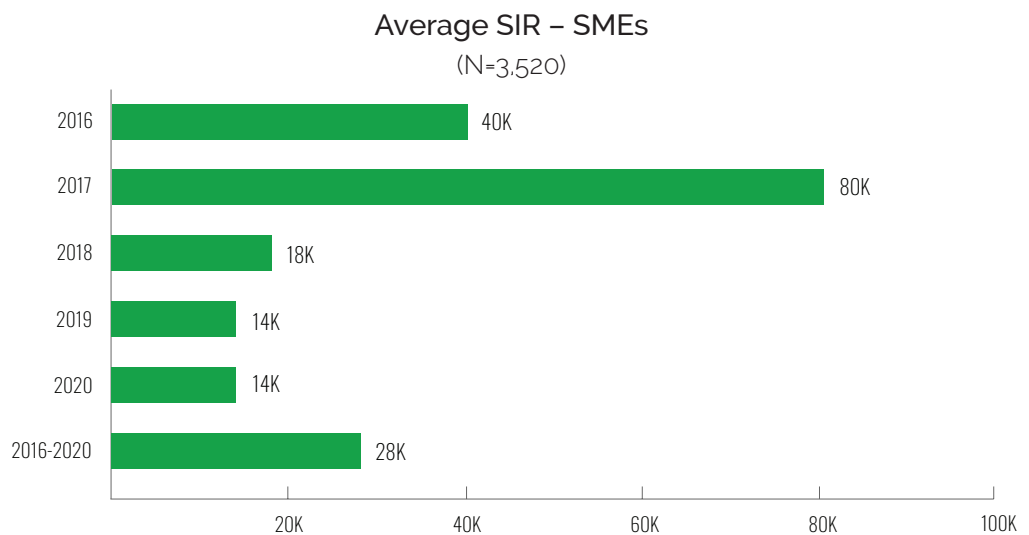


Figure 23



Topics of Special Interest

Company Size and Loss Magnitude: Does Size Really Matter?

Four 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 65% 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 really no correlation at all ($R^2 < 0.0992$). For large companies, there is some, but not much,

correlation ($R^2 < 0.3364$). One of the largest incidents in the dataset occurred at a small enterprise and one of the smallest at a very large one.

There are probably many reasons for this, most importantly the equalizing effect of cheaper and more powerful hardware. Other factors include the omnipresence of the internet, the availability of fast, inexpensive connectivity, and massive amounts of cheap storage in the cloud and on premises. 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 vs Annual Revenue – SMEs

(N=3,130)

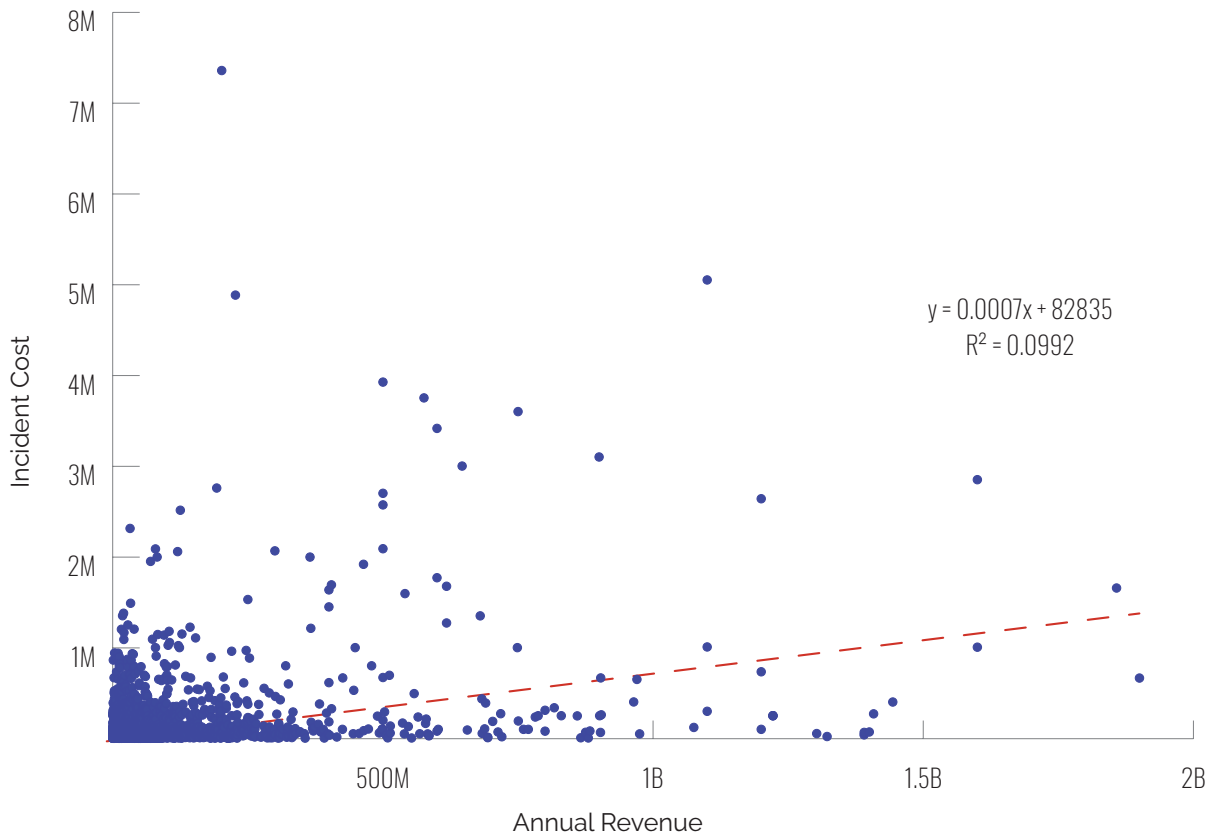


Figure 24

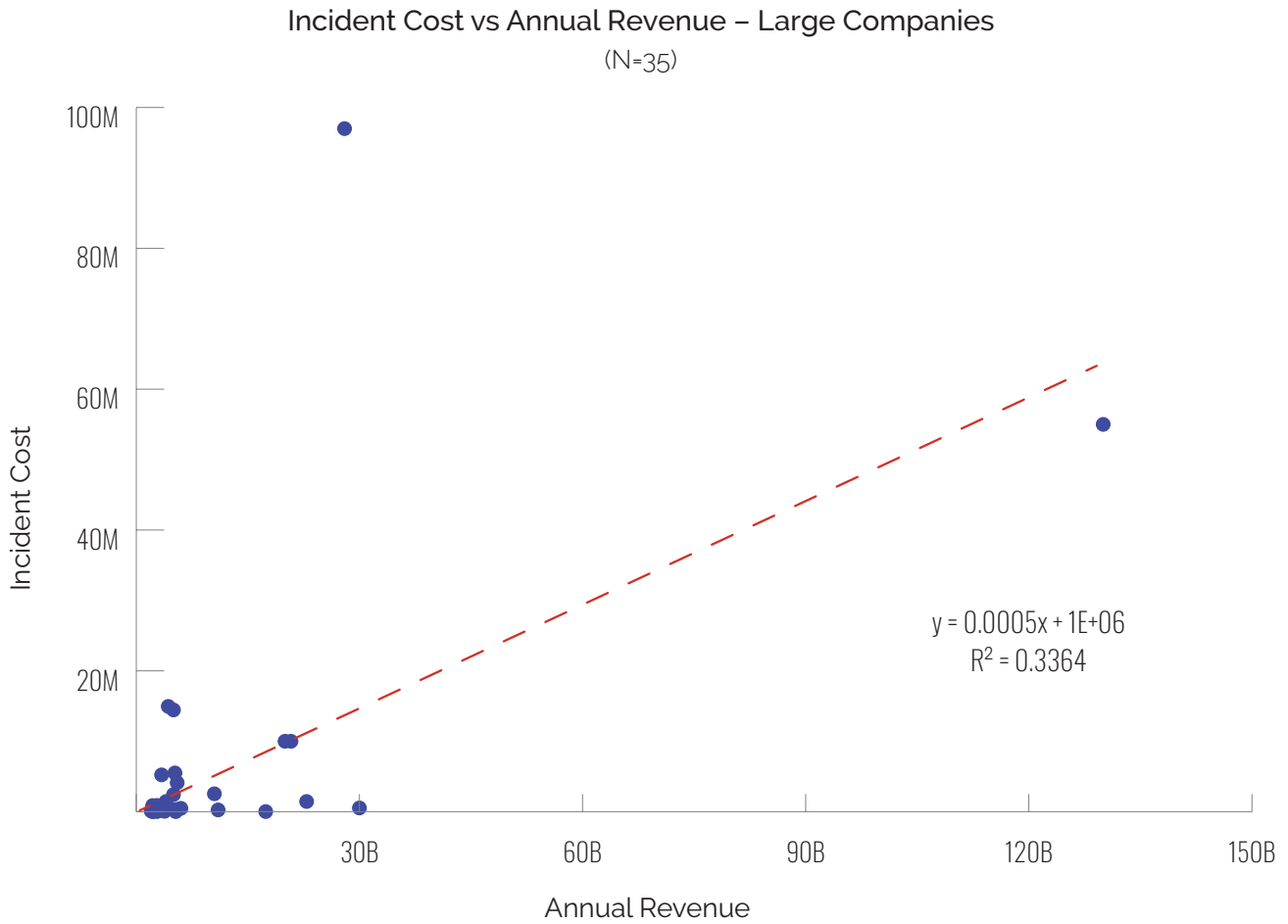


Figure 25

Top Causes of Loss at SMEs

As measured by the number of claims over five years, the top five causes of loss at SMEs were:

- Ransomware
- Hackers
- Business email compromise
- Staff mistakes
- Phishing

Losses in these five categories accounted for 70% of claims and 80% of total incident cost (\$525M). For metrics on all sectors, please see the graphs and tables in the appendices.

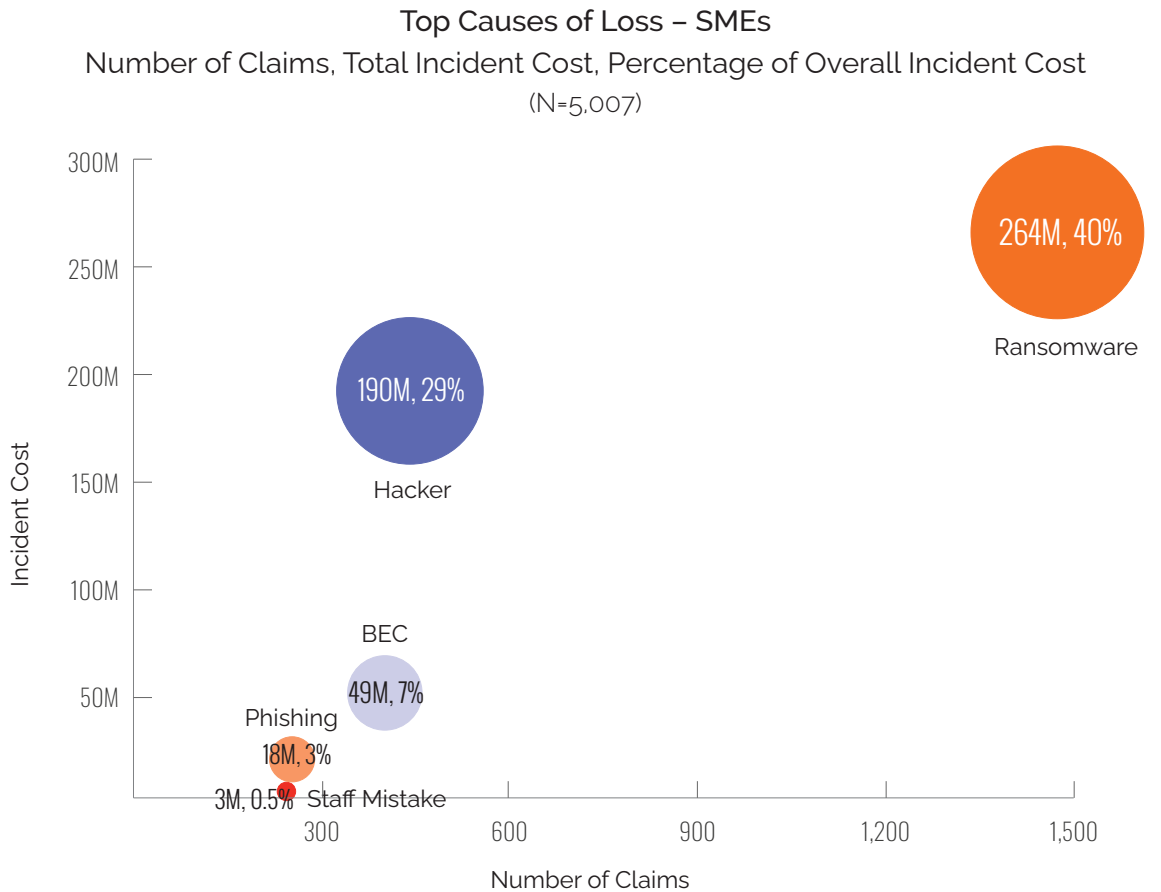


Figure 26

Ransomware

As we all know, ransomware claims have snowballed since 2018–2019. From year to year, the NetDiligence data shows a significant increase in the number of ransomware claims and in the costs of ransomware incidents. From reading the news about events at Colonial Pipeline, Kaseya, the NBA, and many other entities, we know that things have become even worse in 2021⁵.

Ransomware accounts for the largest number of claims in the five-year data (N=1,474). Ransom demands and total incident cost average \$146K (less than \$200–\$3.7M) and \$179K (\$1K–\$20M), respectively.

Ransom amounts and incident cost were provided for only a subset⁶ of claims (N=557). We have focused on these claims because we believe that they provide a better understanding of the claims experience. When viewed in this way, the average ransom amount and range of incident cost do not change, but the average incident cost is substantially higher.

This year's report further confirms the growing impact of ransomware attacks on both small to medium businesses and large organizations. Based on what we're seeing in the marketplace, ransomware threats are only becoming more frequent, and threat actors are becoming more sophisticated by leveraging criminal business models like Ransomware-as-a-Service (RaaS). We expect these numbers to continue to trend in an upward direction unless organizations focus on putting appropriate defensive controls and processes in place.

Tauseef Ghazi
National Leader, Security and Privacy Risk Consulting, RSM

⁵ NetDiligence has not yet collected data for incidents in 2021.

⁶ See the methodology section for a discussion of missing and mismatched data.

Average Cost of Ransomware – SMEs
(N=557)

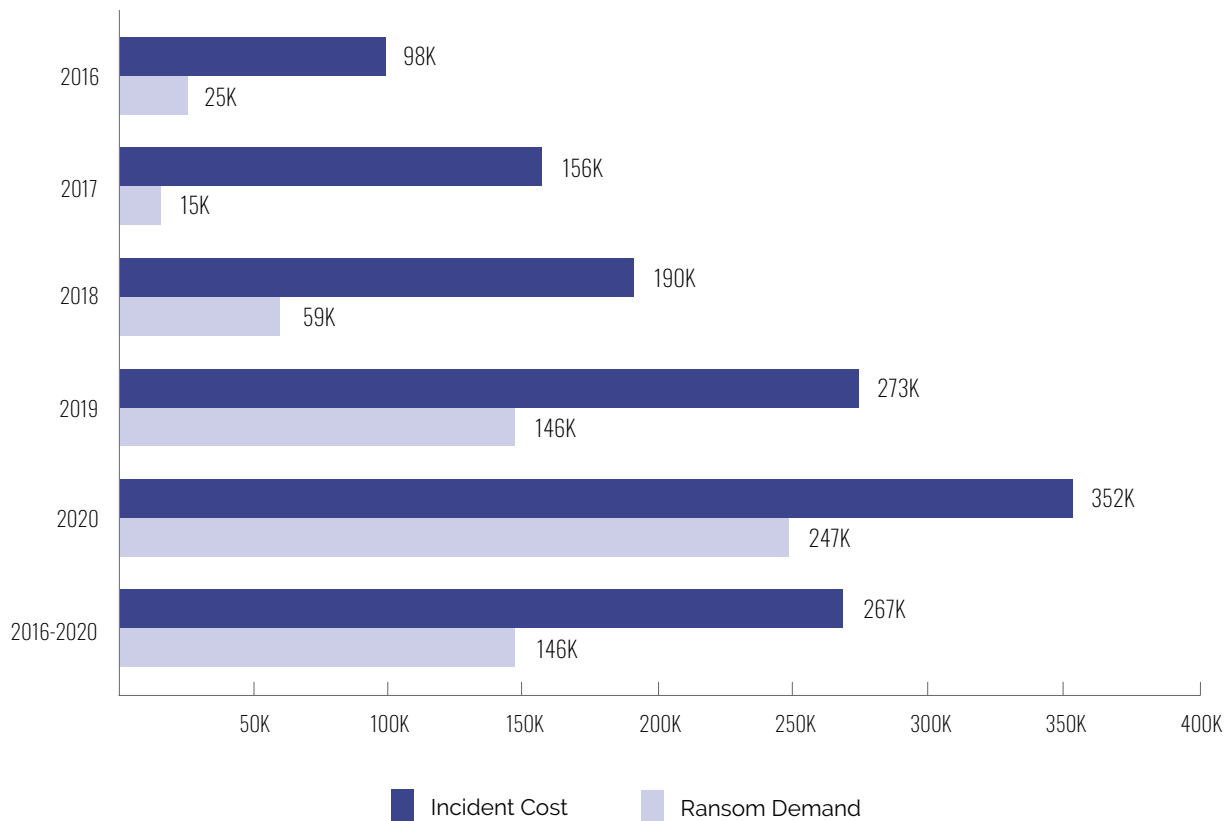


Figure 27

Some victim organizations choose not to pay a ransom. What happens then? Sometimes, but not very often, backups have not been infected and sufficient recovery is possible. Some organizations just bite the bullet and perform a data recovery process. Increasingly, victims elect not to pay ransoms because there is a good chance that the decryption keys will not work.

There is a small subset of claims which noted that the victim chose not to pay a ransom demand. For most of these, we do not know what the ransom demand was because it was not paid and therefore was not provided. The total incident cost for these events averaged \$308K (\$15K–\$2.1M) in 2020 and \$247K (\$2.5K–\$6.6M) over five years (not much less than the averages in Figure 21).

As noted above, ransomware incidents accounted for 79% of the claims with a business interruption loss. BI costs in ransomware incidents in 2020 ranged from \$3,500–\$3M and averaged \$489K. The total

incident cost of these incidents ranged from less than \$25K–\$3.1M and averaged \$975K. BI costs over five years ranged from less than \$200–\$5.1M and averaged \$275K. Total incident cost ranged from \$4.6K–\$6.6M with an average of \$433K.

Ransomware incidents accounted for 81% of the claims with a recovery expense loss. Recovery expense in ransomware incidents in 2020 ranged from \$1,700–\$613K and averaged \$107K. The total costs of these incidents ranged from less than \$8K–\$1.7M and averaged \$427K. Recovery expense over five years ranged from less than \$200–\$613K and averaged \$49K. Total incident cost ranged from less than \$1,500–\$3.9M with an average of \$181K.

The increasing frequency and loss magnitude caused by ransomware incidents is a huge concern for insurers and organizations. NetDiligence has published two Spotlight reports on ransomware (2020 and 2021), and will very likely publish another one in the near future.

Top Affected Sectors

As measured by the number of claims over five years, the following sectors accounted for 70% of claims and 74% of total incident cost (\$535M):

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

These sectors have been at the top of the list for many years now because they represent valuable and easy targets for criminals. 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.

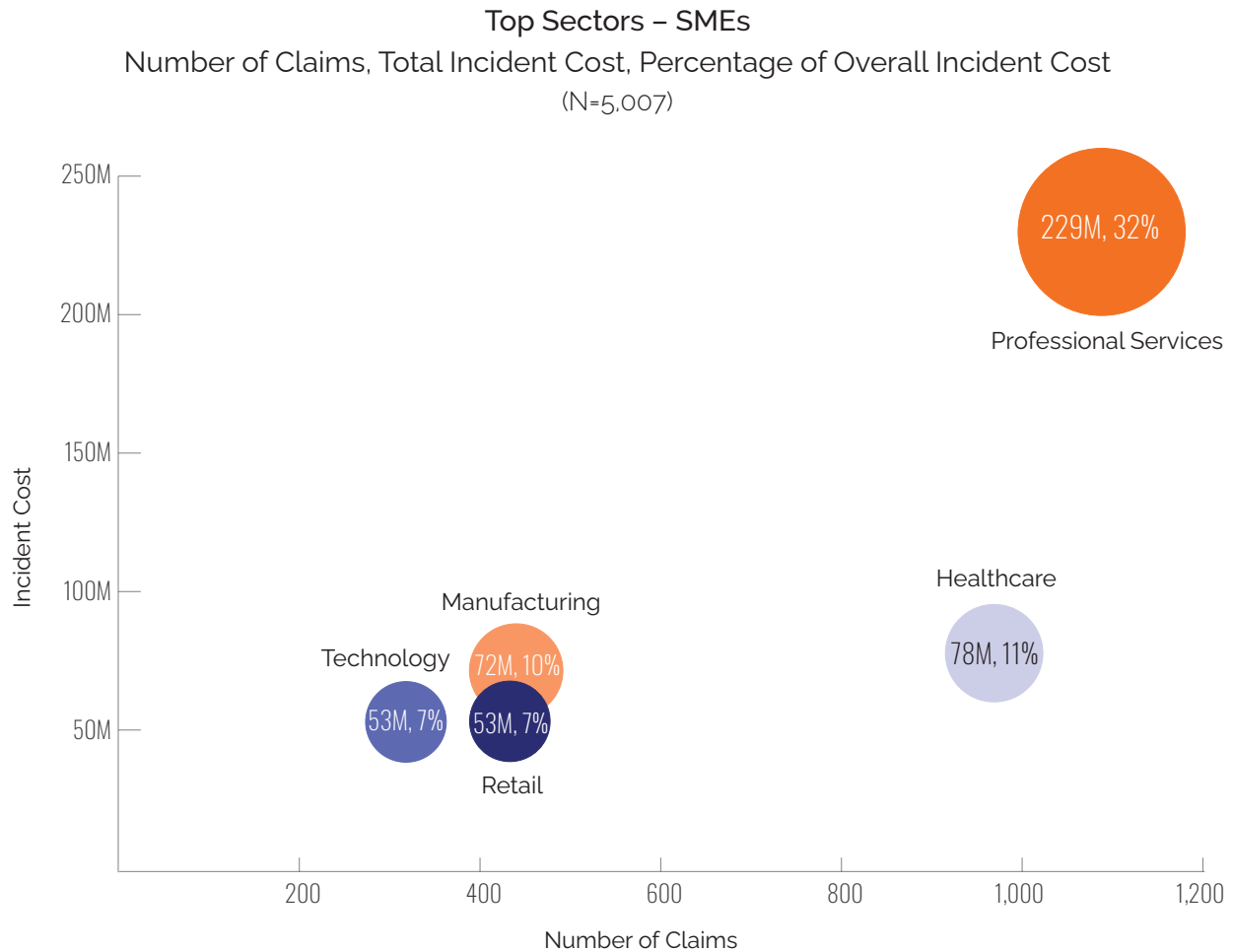


Figure 28

Claims from Public Entities

The average Public Entity claim for Crisis Services costs in 2020 was \$76K (\$7K–\$236K). The average incident cost was \$239K. The corresponding five-year averages were \$95K (less than \$200–\$790K) and \$156K (\$1.8K–\$1.4M), respectively.

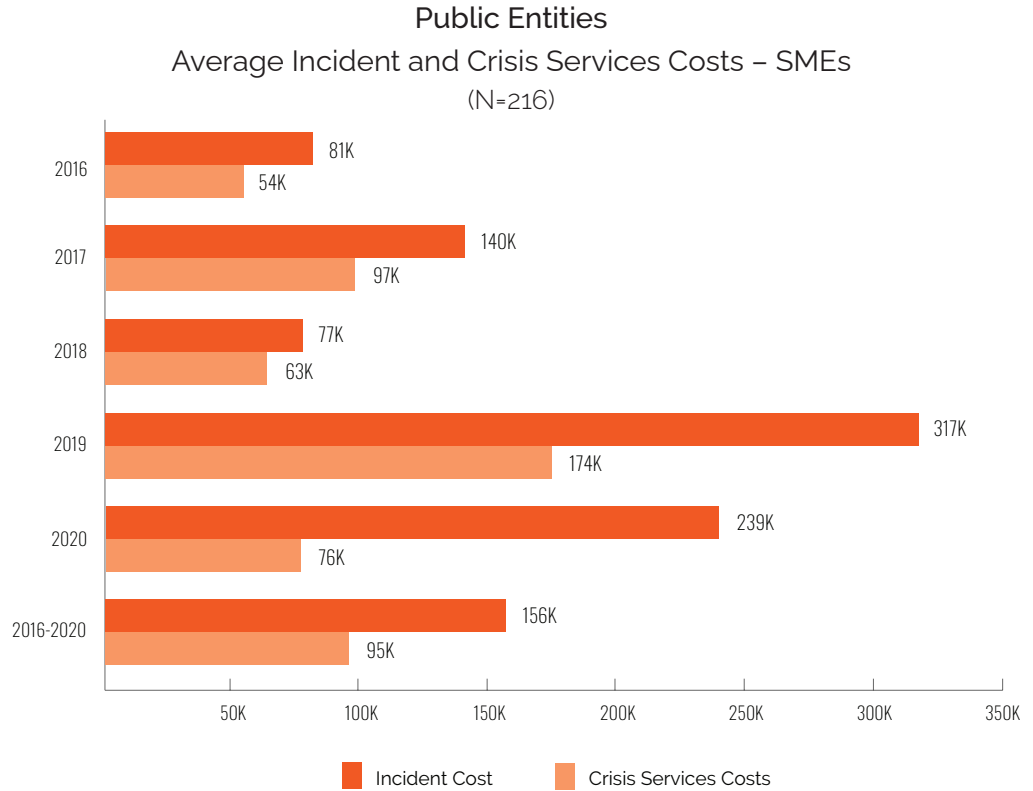


Figure 29

Public Entities
Top Causes of Loss 2016-2020 – SMEs

Cause of Loss	Claims	Average Incident Cost
Ransomware	72	157K
Hacker	23	83K
Staff Mistakes	16	17K
Business Email Compromise	14	200K

Table 3

Claims from Canada

The average Canadian claim for Crisis Services in 2020 was \$144K (from less than \$100–\$1.1M). The average incident cost was \$310K (\$1.1K–\$2.1M). The corresponding five-year averages were \$163K (less than \$100–\$3.8M) and \$237K (\$1.1K–\$3.8M), respectively.

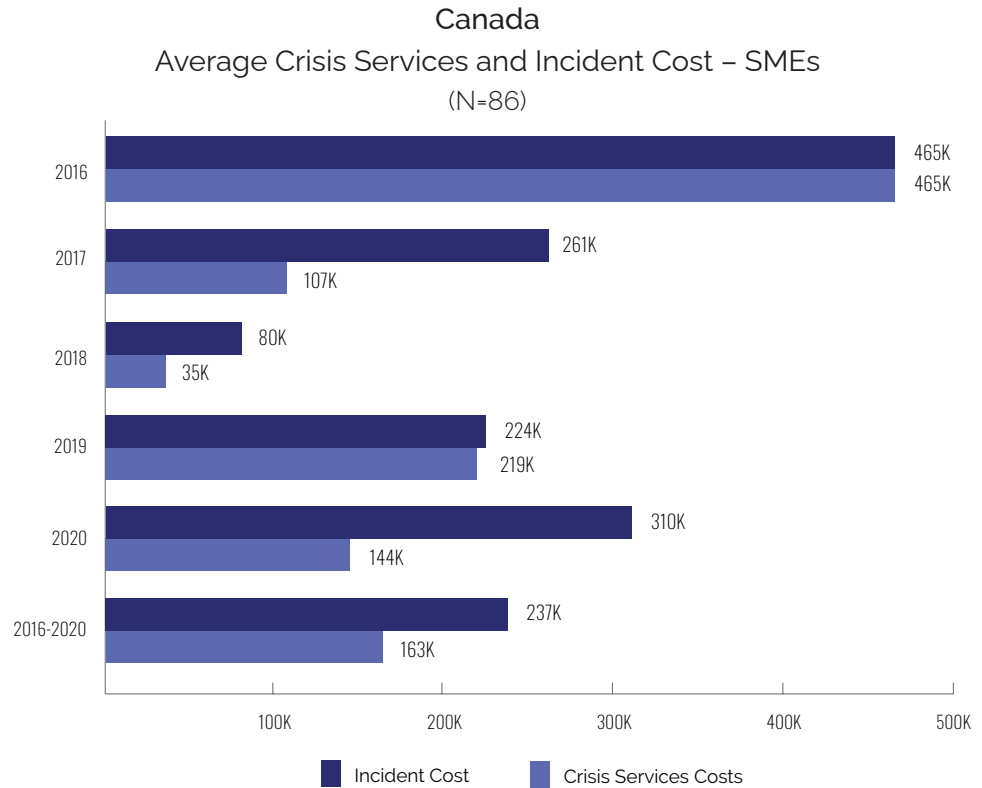


Figure 30

Canada
Top Causes of Loss 2016-2020 – SMEs

Cause of Loss	Claims	Average Incident Cost
Ransomware	33	393K
Business Email Compromise	17	178K
Hacker	10	115K
Staff Mistake	6	23K

Table 4

7 Canadian claim amounts were provided in CAD. These amounts were converted to USD as of December 31st of the year of each incident.

Conclusion

With this eleventh edition of the Cyber Claims Study, NetDiligence continues to raise the bar for presenting and understanding comprehensive loss analysis for cyber insurers and other key stakeholders. For eleven years, these studies have represented the gold standard in the cyber insurance space and, arguably, in the entire cybersecurity space. No other studies provide more or better evidence-based information.

This year's study includes more data and more targeted findings than ever before including the first data analysis of Canadian claims. 3,000 new claims were submitted this year, an almost 50% increase over last year. These were added to an existing dataset of over 2,700 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 participated in this study and shared even more claims and more information about each claim, the value of the study has continued to increase. For the benefit of the industry overall, all underwriters are encouraged to participate in next year's NetDiligence study. All participating insurers are encouraged to share a larger percentage of their cyber claims, especially those for companies with more than \$2B in annual revenue. As participation in the study expands in these two ways, its findings will be richer and more representative of changing market conditions.

Insurance Industry Participants

Over the years, many insurance companies have contributed claims data for this study. We thank them all, as without their participation this study would not be possible. Special thanks go to the following companies for contributing a significant number of new claims for analysis and inclusion in the 2020 study.

AXA XL

Beazley

Berkley Cyber Risk

CFC Underwriting

Chubb

Great American Insurance

Hiscox

Markel

Philadelphia Insurance Companies

QBE

Sompo International

Swiss Re

Tokio Marine HCC

Travelers

United States Liability Insurance

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

Appendices

Revenue Size

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

As was mentioned previously, SMEs (companies with annual revenue less than \$2B) account for 99% of the claims analyzed, and 61% of total incident cost. Large Companies (companies with annual revenue greater than \$2B) account for only 1% of the claims analyzed but 39% of total incident cost.

Percentage of Claims by Revenue Size

SMEs – 2016–2020

(N=5,716)

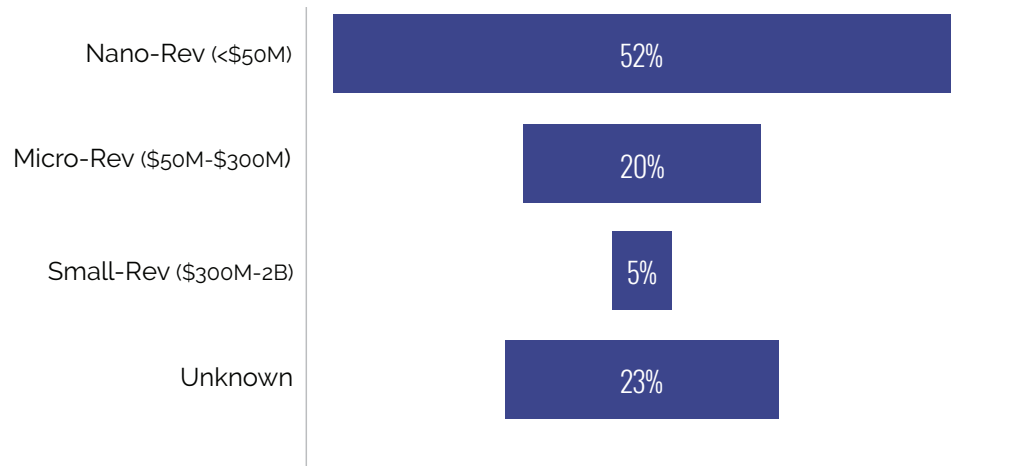


Figure 31

Incident Cost by Revenue Size

SMEs – 2016–2020

	Claims	Minimum	Average	Maximum	Total	Rank*
Nano-Rev (<\$50M)	2,651	1K	88K	6.7M	232.8M	4
Micro-Rev (\$50M-\$300M)	971	1K	172K	7.5M	167.4M	3
Small-Rev (\$300M-\$2B)	223	3K	478K	7.4M	106.7M	1
Unknown	1,162	1K	189K	120.2M	220.0M	2

*Rank based on Average Incident Cost

Table 5

Average Crisis Services Costs by Revenue Size
SMEs – 2016–2020

	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis	Rank*
Nano-Rev (<\$50M)	35K	11K	14K	15K	45K	53K	4
Micro-Rev (\$50M-\$300M)	64K	26K	43K	33K	116K	110K	3
Small-Rev (\$300M-\$2B)	120K	27K	66K	44K	143K	209K	1
Unknown	43K	8K	12K	10K	177K	189K	2

*Rank based on Total Crisis Services Cost

Table 6

Business Sector

Claims are categorized into one of 18 sectors. As has been the case for many years, claims from the Professional Services, Healthcare, Financial Services, Manufacturing, and Retail sectors provide over 65% of the SME claims in the dataset.

The graphic below shows the percentage of SME claims by sector for 2016–2020.

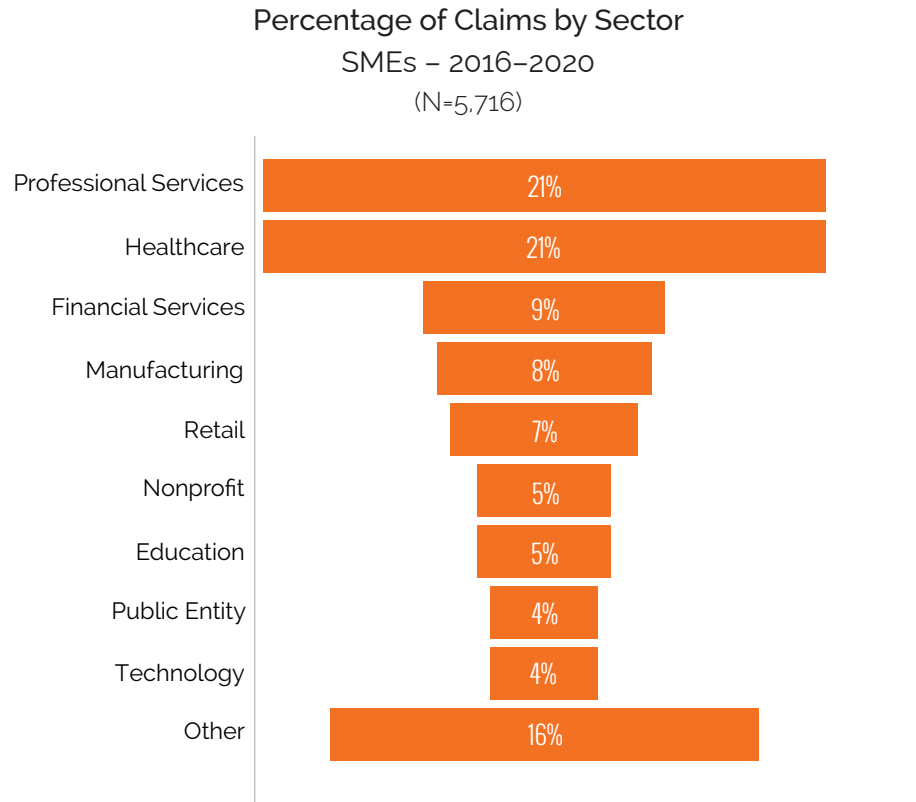


Figure 32

The following two tables list important metrics for claims in each sector. Table 7 provides a summary of total incident cost. Table 8 provide a summary of Crisis Services costs.

Incident Cost by Sector
SMEs - 2016-2020

Sector	Claims	Minimum	Average	Maximum	Total	Rank*
Education	229	1K	118K	1.5M	27.1M	10
Energy	20	11K	89K	390K	1.8M	15
Entertainment	20	4K	110K	548K	2.2M	13
Financial Services	440	1K	112K	5.0M	49.4M	11
Gaming & Casino	6	18K	202K	532K	1.2M	6
Healthcare	969	1K	74K	6.6M	71.6M	16
Hospitality	86	2K	159K	2.6M	13.7M	9
Manufacturing	433	1K	180K	20.0M	77.9M	7
Media	37	2K	214K	2.5M	7.9M	4
Nonprofit	271	1K	65K	1.2M	17.6M	17
Other	580	1K	104K	4.9M	60.4M	14
Professional Services	1,088	1K	211K	120.2M	229.3M	5
Public Entity	216	2K	111K	1.4M	24.1M	12
Restaurant	23	2K	63K	376K	1.4M	18
Retail	318	2K	167K	7.5M	53.2M	8
Technology	180	2K	296K	7.4M	53.4M	3
Telecommunications	25	4K	300K	2.3M	7.5M	2
Transportation	66	1K	412K	17.5M	27.2M	1

*Rank is based on Average Incident Cost

Table 7

Average Crisis Services Costs by Sector
SMEs - 2016-2020

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other*	Total Crisis Services	Rank**
Education	64K	9K	38K	22K	128K	99K	7
Energy	52K		6K	10K	65K	70K	10
Entertainment	32K	92K	3K	33K		64K	13
Financial Services	41K	10K	13K	21K	61K	68K	11
Gaming & Casino	132K		6K	31K	3K	159K	3
Healthcare	34K	20K	26K	10K	83K	36K	18
Hospitality	79K	18K	36K	33K	28K	101K	6
Manufacturing	34K	7K	8K	23K	40K	77K	9
Media	34K		86K	22K		52K	16
Nonprofit	47K	13K	6K	15K	46K	55K	15
Other	44K	4K	11K	12K	188K	58K	14
Professional Services	35K	8K	11K	15K	85K	271K	1
Public Entity	46K	19K	20K	20K	97K	95K	8
Restaurant	30K	7K	16K	18K	85K	48K	17
Retail	104K	14K	47K	33K	121K	134K	4
Technology	73K	45K	83K	32K	88K	129K	5
Telecommunications	89K	1K	22K	204K	37K	241K	2
Transportation	73K	8K	3K	14K	0K	66K	12

* Includes public relations, data restoration, and sometimes ransom payment, and fraudulent wire transfer

**Ranking is based on Average Crisis Services

Table 8

Cause of Loss

Claims in the dataset are classified by 24 distinct causes of loss. As the graphs below show, ransomware, hackers, BEC, staff mistakes, and phishing were the leading causes of loss for 2016–2020.

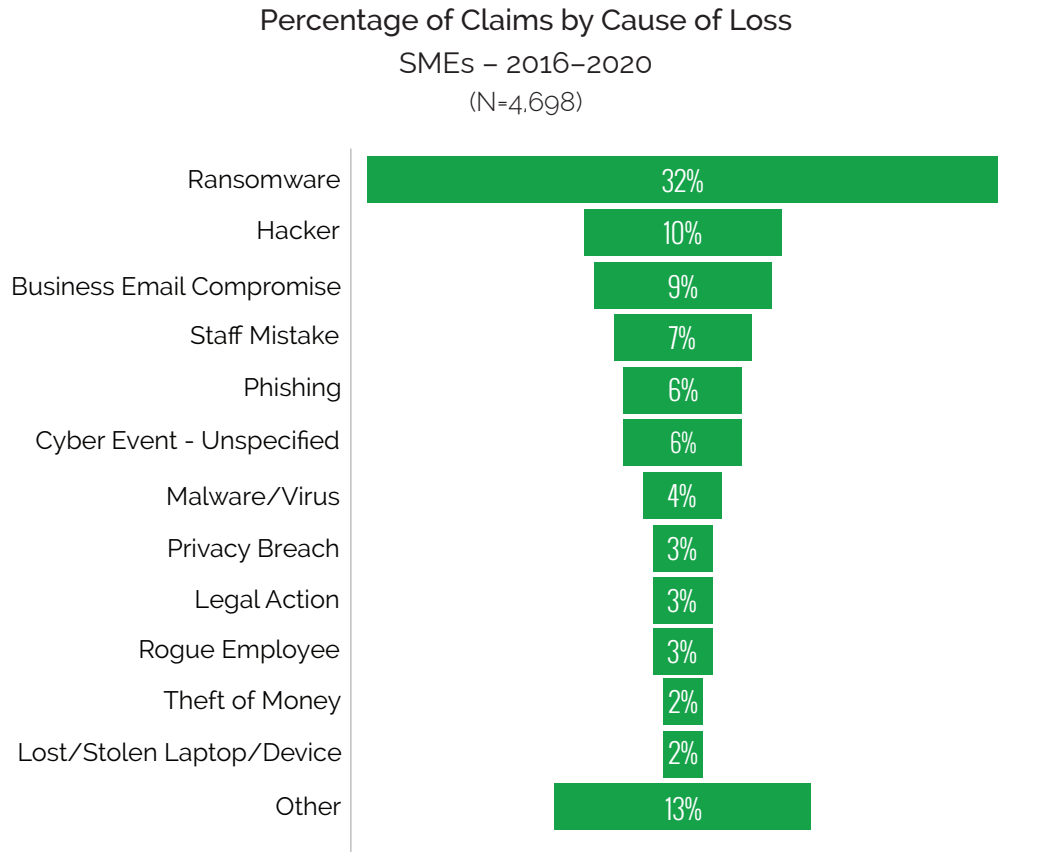


Figure 33

The following two tables tell the story for incident and Crisis Services costs based on cause of loss.

Incident Cost by Cause of Loss
SMEs - 2016-2020

Cause of Loss	Claims	Minimum	Average	Maximum	Total	Rank*
Business Email Compromise	401	1K	123K	3.4M	49.4M	8
Cyber Event (unspecified)	160	2K	100K	860K	15.9M	11
Hacker	441	1K	430K	120.2M	189.5M	2
Legal Action	52	3K	90K	661K	4.7M	13
Lost/Stolen Laptop/Device	69	1K	57K	1.5M	3.9M	18
Malware/Virus	168	2K	160K	6.9M	26.9M	7
Negligence	4	5K	63K	121K	253K	16
Paper Records	28	1K	40K	650K	1.1M	20
Phishing	253	1K	72K	666K	18.2M	14
Privacy Breach	33	1K	13K	51K	415K	25
Programming Error	16	4K	348K	3.6M	5.6M	3
Ransomware	1,474	1K	179K	20.0M	264.4M	5
Rogue Employee/ Malicious Insider	136	1K	91K	2.5M	12.4M	12
Social Engineering - All	716	1K	114K	3.4M	81.8M	9
Staff Mistake	244	1K	13K	284K	3.2M	24
System Glitch	13	4K	1.5M	17.5M	19.5M	1
Theft of Hardware	44	1K	16K	100K	0.7M	23
Theft of Money	54	1K	102K	1.1M	5.5M	10
Third Party	8	5K	33K	76K	264K	21
Trademark/Copyright Infringement	8	12K	166K	468K	1.3M	6
Unauthorized Access	1	20K	20K	20K	20K	22
Wire Transfer Fraud	58	9K	289K	1.9M	16.8M	4
Wrongful Data Collection	3	5K	42K	86K	126K	19
Other	377	1K	58K	2.8M	21.9M	17
Unknown	974	1K	69K	2.0M	67.3M	15

*Rank based on Average Incident Cost

Table 9

Average Crisis Services Costs by Cause of Loss
SMEs - 2016-2020

Cause of Loss	Forensics	Monitoring	Notification	Legal Guidance	Other*	Total Crisis Services	Rank**
Business Email Compromise	42.7K	15K	13K	30K	88K	79K	8
Cyber Event (unspecified)	43.1K	1K	8K	8K		50K	13
Hacker	44.5K	12K	43K	30K	28K	398K	1
Legal Action	24K	3K	7K	17K	67K	39K	16
Lost/Stolen Laptop/Device	20K	10K	73K	14K	117K	46K	14
Malware/Virus	105K	2K	30K	32K	116K	142K	2
Negligence	6K	1K	20K	24K		41K	15
Paper Records	16K	3K	4K	11K	20K	13K	22
Phishing	46K	20K	10K	17K	24K	56K	12
Privacy Breach	17K	1K	2K	5K		16K	21
Programming Error	37K	300K	278K	21K		123K	3
Ransomware	45K	20K	19K	12K	102K	72K	9
Rogue Employee/Malicious Insider	64K	5K	7K	34K	19K	57K	11
Social Engineering-All	42K	16K	12K	25K	91K	71K	10
Staff Mistake	51K	7K	6K	5K	4K	10K	23
System Glitch	78K	2K	81K	40K	54K	87K	6
Theft of Hardware	8K	0K	1K	4K	50K	7K	24
Theft of Money	18K	0K	18K	14K		30K	18
Third Party	23K	36K		12K	1K	28K	19
Trademark/Copyright Infringement				91K		91K	4
Wire Transfer Fraud	15K	5K		15K	141K	91K	5
Wrongful Data Collection				80K		80K	7
Other	15K	8K	6K	9K	83K	19K	20
Unknown	22K	6K	1K	11K	34K	32K	17

* Includes public relations, data restoration, and sometimes ransom payment, and fraudulent wire transfer

**Ranking is based on Average Crisis Services

Table 10

Type of Data

For incidents that expose data, it is important to understand the type of data that was exposed or stolen. Statutes in each state of the United States, the GDPR in the European Union, and laws in many other countries require notification and other actions when certain types of data have been exposed.

Personally Identifiable Information (PII), Private Health Information (PHI), and PCI data (payment cards) are the three types of data familiar to most people. However, claims can be classified with 13 other types of data, including non-card financial, other non-public, W-2 specific data, and trade secrets.

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 chart below depicts the percentage of claims for each data type. The tables provide summary statistics for incident and Crisis Services costs.

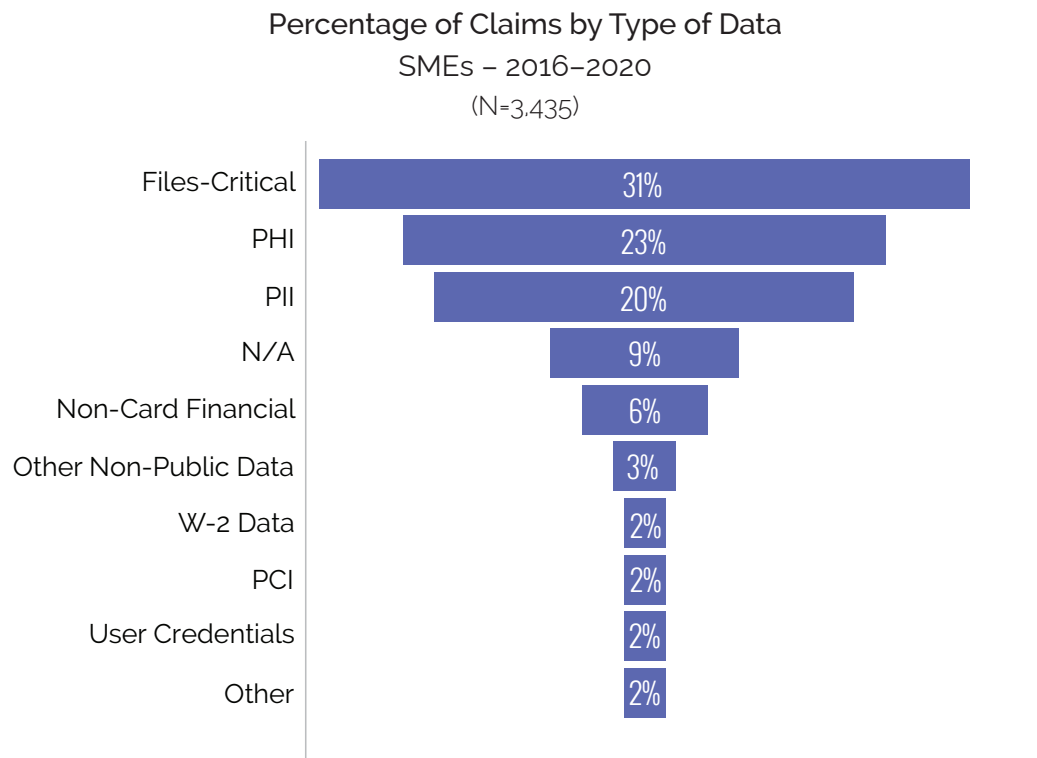


Figure 34

Incident Cost by Type of Data
SMEs - 2016-2020

Type of Data	Claims	Minimum	Average	Maximum	Total	Rank*
DDoS	5	4K	85K	183K	427K	10
Email (unspecified)	14	3K	78K	200K	1.1M	11
Files-Critical	1,023	1K	231K	20.0M	236.1M	5
Intellectual Property	20	3K	178K	1.2M	3.6M	6
N/A	304	1K	91K	1.9M	27.7M	9
Non-Card Financial	193	1K	764K	120.2M	147.5M	1
Other	11	6K	386K	1.1M	4.2M	2
Other Non-Public Data	82	2K	154K	3.1M	12.6M	8
PCI	76	2K	340K	6.9M	25.9M	3
PHI	627	1K	64K	2.1M	40.0M	13
PII	538	1K	156K	7.5M	83.8M	7
Trade Secrets	4	4K	59K	208K	237K	15
Unknown	1,966	1K	63K	2.8M	124.2M	14
User Credentials	59	1K	231K	3.9M	13.6M	4
User Online Tracking	1	25K	25K	25K	25K	16
W-2 Data	84	2K	68K	294K	5.7M	12

*Rank based on Average Incident Cost

Table 11

Average Crisis Services Costs by Type of Data
SMEs -2016-2020

Type of Data	Forensics	Monitoring	Notification	Legal Guidance	Other*	Total Crisis	Rank**
DDoS	38K			8K	4K	36K	14
Email (unspecified)	38K		2K	38K	157K	156K	3
Files-Critical	53K	22K	23K	17K	95K	88K	8
Intellectual Property	130K			28K	521K	148K	4
N/A	32K	5K	4K	10K	45K	42K	13
Non-Card Financial	28K	8K	13K	20K	114K	974K	1
Other	63K			4K	276K	146K	5
Other Non-Public Data	41K	3K	1K	41K	18K	57K	11
PCI	189K	11K	28K	50K	175K	218K	2
PHI	45K	20K	35K	12K	85K	49K	12
PII	57K	11K	27K	32K	79K	94K	6
Trade Secrets	40K			54K		57K	10
Unknown	26K	3K	10K	7K	89K	27K	15
User Credentials	73K	15K	18K	29K	45K	92K	7
User Online Tracking	15K				10K	25K	16
W-2 Data	46K	29K	11K	20K	9K	57K	9

* Includes public relations, data restoration, and sometimes ransom payment, and fraudulent wire transfer

**Rank based on Average Crisis Services

Table 12



Ransomware-as-a-Service (RaaS): A new business model for cyber criminals

Threat actors are selling their ransomware secrets to less sophisticated criminals, resulting in an explosion of new cyberattacks.

by RSM

Ransomware has become the most significant cybersecurity threat today, impacting large multinational organizations to the smallest of entities. A ransomware attack represents a low-risk, high-reward opportunity for criminals, as little effort is required to access sensitive information and demand bounties that can significantly harm businesses—especially small- to medium-sized companies. [The RSM US Middle Market Business Index 2021 Cybersecurity Special Report](#) found that 42% of middle-market executives know of a company that has been a target of a ransomware attack, and 11% of executives indicated that they experienced more than one attack in 2020. In the current environment, inaction is not an option, and companies must take proactive steps to address expanding and evolving ransomware risks.

To add to the evolving threat landscape, cyber criminals have taken advantage of the exponential growth of Ransomware-as-a-Service (RaaS), a service model where sophisticated threat actors develop and sell ransomware platforms to other threat actors. Now, cyber criminals no longer need to be highly technical to launch a cyberattack into an organization, so ransomware attacks are rapidly increasing.

How does the RaaS model work?

- The RaaS model provides the purchaser with extensive training, reference materials and malicious code that can be used to launch a ransomware attack. Here are some key takeaways for understanding how RaaS works:
- RaaS providers typically use several different purchase models:
 - Subscription: The RaaS provider receives a predetermined cryptocurrency payment for a finite period of usage.

- Affiliate: The RaaS provider receives a recurring fee plus a percentage of the ransom payment.
- Purchase: The RaaS provider sells a “kit” to the purchaser.
- The attacks leverage well-established hacking tools (i.e., Mimikatz), while employing current vulnerability and penetration testing tools (i.e., Cobalt Strike).
- These attacks are designed to not only exploit well-known, existing vulnerabilities, but also take advantage of new zero-day vulnerabilities.
- Threat actors have developed elaborate social engineering and intelligence-gathering methods with the intention of causing significant devastation for a victim when a ransomware attack is launched.

How to protect your organization from ransomware attacks

The reality is that ransomware will continue to be an ongoing threat to organizations, and there is no way to completely remove the risk of ransomware. However, the following actions can help reduce the potential success of an attack:

- **Stay informed about new vulnerabilities:** The National Institute of Standards and Technology (NIST) published information to help protect against threats and recover from a potential ransomware attack. In addition, the US-CERT—CISA regularly posts updates on new vulnerabilities and attacker tactics, techniques and procedure (TTP) trends.
- **Make sure you have backups:** It is important to have backups not just for business continuity and disaster recovery, but also to be able to restore critical data if a ransomware attack occurs. The

trusted, age-old 3-2-1 backup rule will help protect backups from attackers. Don't forget that attackers also work nights, weekends and holidays, so you should have regular and frequent backups.

- **Implement advanced endpoint detection and antivirus protection:** While attackers use established TTPs, they are also attacking new vulnerabilities and constantly updating their toolset. Have a robust and properly configured defense system in place to identify and minimize potential attacks before they gain traction and impact your environment.
- **Have an incident response plan:** Develop a strategy that outlines how your organization will respond if you suffer an attack. A ransomware situation is a chaotic event; the longer it takes you to respond to an attack, the more costly it will be.

Ransomware has always been a concern, but the rapidly changing threat landscape is increasingly impacting companies of all types and sizes. Every organization should create a security approach that includes strategies to both prevent and remediate ransomware attacks. A strong security plan can limit financial exposure and reduce downtime.

About RSM

RSM is the leading provider of audit, tax and consulting services focused on the middle market, with nearly 13,000 professionals in 83 U.S. cities and four locations in Canada. It is a licensed CPA firm and the U.S. member of RSM International, with 48,000 people in more than 120 countries. For more information, visit <https://rsmus.com/>.



The Cyber-Demic: Why Data Breach Preparedness Is in Hyperdrive, How We Got To Herd Inevitability and The Only Path Forward.

by Experian®

There's no polite way to say this, so I'll make it plain.

The threat of a ransomware cyberattack is not only real; it's here and causing damage by the second, with no end in sight. At this stage of the lawless pay-or-else game, no organization is safe from the devastating financial impacts, regulatory issues, and brand damage of this malware-driven virus. Despite best efforts to prevent it from rising, like the rampant Delta variant, ransomware is raging out of control, posing extreme risks and breaching unsuspecting and unprepared barriers.

What We Know

In the first half of 2021 alone, we saw a 102% increase in ransomware attacks from the year before, according to data released from the cybersecurity firm, Check Point Software. As three cybersecurity threat reports put it, "Attackers have doubled down on ransomware and phishing –with some tweaks—while deep fakes and disinformation are set to become major threats in the future." Even more troubling, with data compromises up 38% over the first quarter of 2021, the Identity Theft Resource Center predicts that if the trend continues, the year could end with data compromises reaching an all-time high.

The hard truth: we are beyond the tipping point of herd inevitability.

Getting hit by a ransomware attack can be summed up in two words: when and how. Gone are the days of "if." Studies and reports show that more ransomware events are happening, and the costs to respond to them are increasing. The outlook is not positive, but there is light in the tunnel.

The Only Path Forward is Preparedness

Ransomware is ripping through all industries, stressing systems, and causing brand harm. Every entity must be ready to unleash an agile and effective response to protect its reputation, customers, and future in these unpredictable times.

At Experian, we've seen the impact of attacks play out firsthand. So far this year, we're up to 6,000 breaches serviced, up nearly 1,000 from 2020. Having managed more than 55,000 breaches over almost 20 years, we also see ransomware attacks getting more complex. Here's what we know:

- 1. It's taking 20% longer to execute** a consumer response.
- 2. Hackers are getting more sophisticated** in their payment scheme, demanding double extortion money: a first fee to access the data and another to keep it off the dark web. Sometimes they get bolder and ask for three disbursements. The stakes are higher from a company response point of view, too, with ransomware attacks requiring more complex involvement from multiple resources, from crisis public relations and legal to forensics and the C-suite.
- 3. All of this activity adds up** in additional costs to plan for and respond to events. In the end, it amounts to higher regulatory fines, customer flight, and brand damage.

Experian handles many data breach cases, and we know that 7 of 10 breaches involve ransomware. As highlighted in this year's Cyber Claims Study, our work also confirms that an organization's size doesn't mean, by any account, that their claim will be small. We also learned that spending on preparedness could save money, and more, in the long run.

Proper preparedness is the only path forward because, again, an attack is just a matter of time.

With Experian® Reserved Response, cyber insurers can be ready, not hasty. With policy costs up 15-17%, being prepared means saving money; 25% less if consumer response is needed. With major providers exiting cyber policies, insurers can benefit from Experian's referral model for lower costs. Being prepared with Experian also means getting:

- **Guaranteed Service:** Our program includes built-in penalties for missing incident response SLAs
- **Speed and Custom Responses:** You won't get cookie-cutter service with our 24/7 dedicated U.S.-based call center support
- **Yearly Readiness Planning and Live Drills:** A ransomware attack is no time to wing it. Our clients are prepared to respond rapidly.
- **Small Business Solutions:** Guaranteed solutions for affected populations of up to 1 million

Data Breach Response

- **Notification:** Quickly notifies affected individuals within federal and any state data breach laws. Includes letters and address verification.
- **Enhanced Call Center:** Dedicated, 24/7 U.S.-based call center support to service impacted customers.
- **Identity Protection:** Offers Experian IdentityWorks® to help customers maintain security and peace of mind.
- **Identity Restoration:** U.S.-based Fraud Resolution Agent to guide customers through recovery.

Ransomware is here for the long haul. Experian Reserved Response and Data Breach Resolution are the best ways to fight it.

About Experian® Data Breach Resolution

Experian® Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach via the proprietary Experian® Reserved Response program and also mitigate consumer risk following breach incidents. With more than nineteen years of experience, Experian has successfully serviced some of the largest and highest-profile data breaches in history. The group offers swift and effective incident management, notification, call center support and fraud resolution services while serving millions of affected consumers with proven credit and identity protection products. For more information, visit www.experian.com/databreach and follow us on Twitter @Experian_DBR.



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

by Erin Kenneally, Director, Cyber Risk Analytics, Guidewire

Risk Underwriting Self Help: Closing the Data & Analytics Feedback Loop

Take a gander at any report, paper or article on the state of cyber insurance during its entire multi-decade existence and you'll find at least one universal bellyaching: there is a lack of incident loss data upon which to reliably assess insurance risks and calculate premiums.

Myth busted: the problem is not lack of data, rather, it is under-extraction of insights from the actuarial data that has been generated around cyber incidents. Specifically, there is a facet of incident data that promises to drive better underwriting but which insurers have left on the proverbial cutting room floor: post-incident digital forensics.

Heretofore the industry has mined incident data monolithically and superficially for its firmographics and insurable impacts, which in turn have bounded risk selection and pricing. The industry has overlooked a key data and analytical feedback loop whose closure would move insurers beyond the self-perpetuated actuarial Groundhog Day. Digital forensics & incident response (DFIR) data about incident attack vectors and controls deficiencies collected in the post-incident claims process will evolve the quality of risk correlation and causation and enrich the frontend underwriting of cyber risk.

The Tail Wagging the Dog: Legal Privilege

There are two main dynamics that impede inclusion of DFIR data into the actuarial record and stifle improved underwriting: misaligned insurer-law firm data governance, and disjointed business process.

Cyber carriers are positioned to collect DFIR data and utilize it to inform frontend risk underwriting yet remain largely abstracted from the data because of how they structure the incident response process. Insurers cover the cost of forensic incident response in the

wake of breaches and govern the relationship between policyholders and response firms.

Significantly, however, cyber insurers commonly appoint law firms to manage the incident response functions and workflow. This practice strategically and deliberately leverages attorney-client privilege or work product doctrine to prevent third party liability and E&O exposure that may arise if causal details from the DFIR report were otherwise discoverable during litigation proceedings. The goldmine of who, what, when, where, why, and how that is extracted in the DFIR process is nevertheless often left entombed within the ore of firmographic and loss figures associated with the claim.

The economic justification for deferring to avoidance of potential liability cost to the detriment of continuous-loop analytics and ex ante risk reduction has grown frail. Wielding attorney-client privilege to shield access to DFIR data is a vestige of an era when cyber policies were liability-centric and losses were driven by third party litigation following a data breach.

Present day losses and risk transfer needs of cyber compromised companies are skewing more heavily toward business income, interruption (BI) and recovery costs that flow from technical compromise, largely as a result of the ransomware epidemic.

Disjointed Insurance Business Processes

The business process issue for many cyber insurers is not a function of authority over IR data, but rather, structuring and processing more robust claims data to inform underwriting. So even if carriers were to exercise their governance authority to acquire better data from the IR process, the cyber incident details, metadata, and more granular forensics may not be integrated into legacy database schema and tables to close the loop with front-end risk analyses.

Unhiding What's in Plain Sight

While there is variability across IR documentation, the lack of carrier-driven standards and the expanded role of insurers in proactive risk reduction argue that smart engineering of IR data for claims should take a cue from infosec industry data standards. Innovative infosec and DFIR firms are embracing the VERIS and Mitre ATT&CK frameworks, so it's logical that these should be the connective tissue for carriers who seek to effectuate that learning and insight.

If IR and claims are classified in this way an underwriter considering a cyber policy application can consult its corpus of VERIS/ATT&CK-classified claims to augment its assessment of likelihood and severity of the applicant's cyber losses.

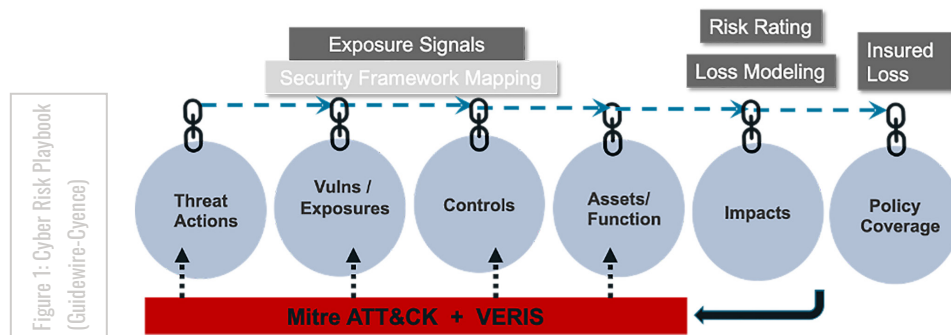
Now-Gen Cyber Underwriting: Building a More Robust Cyber Risk Playbook

Now-generation cyber underwriting requires going beyond indemnifying, pooling, and diversifying risks at the policy level to proactively managing insureds' cyber risk at the technical and governance levels.

Continuously looping backend DFIR data for frontend underwriting offers many advantages, including: reduced risk visibility bias, certainty of semantic and syntactic standards, harnessing untapped claims insights, closing the gap between pricing and value, and enhanced understanding of controls efficacy.

About Guidewire

Guidewire is the platform P&C insurers trust to engage, innovate, and grow efficiently. We combine digital, core, analytics, and AI to deliver our platform as a cloud service. More than 400 insurers, from new ventures to the largest and most complex in the world, run on Guidewire. For more information, contact us a info@guidewire.com.



For the full version of this article, see: https://success.guidewire.com/Whitepaper-HidinginPlainSightTowardsNow-GenCyberRiskUnderwriting_Registration.html

This year's study demonstrates that every enterprise must consider its ability to withstand cyberthreats

by Beckage

With the exponential rise in cybercrimes and new national attention to ransomware, the eleventh edition of NetDiligence's Cyber Claims Study is more relevant than ever. Since 2011, this survey has provided unparalleled insight into the shifting cybersecurity landscape. The analysis of almost 6,000 claims in this year's study serves as a stark reminder of the growth in cyberthreats in recent years, and the expansion of attacks across industry sectors and businesses of all sizes.

At Beckage, our data security and privacy professionals rely on this study for its evidence-based assessment of the trends in the field where we are working on a day-to-day basis. Each year, the study offers a wide lens, capturing the experience of businesses and organizations of all sizes, similar to the clients that we guide through data security incidents. Its analysis of past claims allows us to analyze and assess what's coming next.

This year, the study reflects the well-documented increase in cybercrimes and provides a critical analysis that enterprises of every size should carefully consider. Cyber incidents have not just increased in number, the number of exploited small- and medium-sized enterprises (SMEs) has also vastly expanded. Smaller business size does not translate into fewer consequences, as the study found no clear correlation between the size of a claimant organization and the magnitude of loss related to the incident.

When NetDiligence began this crucial study in 2011 with an analysis of less than 100 cyber claims, there were fewer threats, and many small businesses were less reliant on e-commerce, cloud storage, and constant connectivity to manage and grow their business operations. Now, nearly every organization has become a potential target for exploitation and no company should expect that its size can provide insulation from attacks.

In today's economy, SMEs are often just as reliant on well-connected business ecosystems as large corporations. Accelerated by the COVID-19 pandemic, SMEs need to leverage virtual communication platforms and remote access. Many are sophisticated in their use of personal data, and thus may store large amounts of sensitive information in the cloud or on premise. At the same time, SMEs may not perceive the need for resources to harden their data security environment and compliance programs.

The findings of this year's study demonstrate that every enterprise must consider its ability to withstand cyberthreats, comply with an increasingly complicated constellation of state, federal, and international regulations, and prepare to respond to incidents now.

The study's analysis does not, however, focus only on the challenges that exist or the threats that continue to grow. Instead, its assessment of the most prevalent incidents can help SMEs prioritize a roadmap to increasing their data security posture and privacy policies.

Importantly, the study found that 70% of claims and 80% of total incident costs for SMEs resulted from just five categories of incidents: ransomware, other hacker attacks, business email compromise, staff mistakes, and phishing. Among these, ransomware was the most prevalent incident for SMEs, accounting for 79% of claims with a business interruption loss and 81% with a recovery expense loss.

Based on prior experience and resources like this study, data security and privacy professionals at firms like Beckage have insight regarding what threats are most likely to occur, can assist organizations in preventing incidents before they happen, create business continuity and response plans to minimize loss, and guide SMEs strategically through each step following an incident.

While the headlines often focus on the incident facing large organizations like Colonial Pipeline or JBS Foods, the NetDiligence's Cyber Claims Study goes much deeper. Its findings again demonstrate the prevalence of threats for enterprises across all industries, regardless of size – and the need for every organization to incorporate data security as a fundamental business priority.

About Beckage

Beckage is a women-owned law firm focused on technology, data security, and privacy. Our attorneys counsel clients on matters pertaining to data security and privacy compliance, litigation and class action defense, incident response, government investigations, technology intellectual property, and emerging technologies. Our lawyers are technologists, tech business owners, CISAs, CISOs, former regulators, and certified privacy professionals. Learn more at [Beckage.com](https://www.beckage.com).

Beckage
Legally Focused. Technology Driven.

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. 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, London, 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 insurance to submit claims information based on the following criteria:

- The incident occurred in 2018, 2019, or 2020.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to 144 individuals at 87 organizations in the United States, Canada, and the United Kingdom. From this group, 21 individuals representing 19 organizations provided 3,000 analyzable new claims, using the proprietary NetDiligence® claims data collection worksheet.

The 2021 report also includes data from NetDiligence® studies published in 2017-2020, representing 2,797 incidents that occurred in 2016, 2017, 2018, and 2019. After the elimination of claims that were less than \$1,000, the combined dataset included 5,060

incidents, each one, a data Incident insurance claim. This number represents a 50% increase in the number of analyzable claims compared to last year.

There were 5,580 claims in the dataset from American organizations, 163 claims from Canadian organizations, and 25 claims from organizations in the United Kingdom. There were also a small number of claims (N=23) from organizations in Australia, Germany, India, Ireland, Mexico, South Africa, Sweden, and organizations with a global footprint. The country was not specified in 6 claims.

When factoring in SIRs, we were able to calculate total Incident cost to-date for 5,060 (100%) of the claims in the dataset in which the total loss was less than or equal to \$1,000. Of these claims, 860 (17%) specified the number of records exposed (greater than one record) and 2,641 claims (52%) included an accounting of Crisis Services costs. The number of claims reporting records decreased somewhat last year due to the large number of claims for incidents that did not expose records (ransomware, social engineering, BEC, etc.). The overall percentage of claims reporting records decreased by nine percentage points (26% to 17%) for the same reason.

For the first time, we did not calculate per-record costs. Per-record cost has been a controversial metric since it was introduced more than 10 years ago by the Ponemon Institute. In previous reports, we presented per-record costs as percentiles of the total distribution of per-record costs: averages from 100%, 95%, 90%, and 80% of the claims for which a per-record cost could be calculated. We have found that even this approach is not useful. Consequently, we no longer provided this analysis.

4,874 (84%) of the claims in the full dataset (N=5,797) were flagged as closed, 907 (15.7%) as open, and 16 (0.3%) as unknown claim status. 3,293 (56.8%) of the claims were for primary coverage, 32 (0.6%) for excess coverage, and 2,472 (42.6%) had an unknown, but most likely primary, coverage level.

There were 1,322 claims in the full dataset for which the revenue size of the organization was unknown. After comparing the distribution of their incident cost to those of SMEs and Large Companies, the decision was made to include these claims in the SME group.

Readers should keep in mind the following:

- Our sampling, although large, is a subset of all incidents. Some of the data points are lower than other studies because we focus on claim 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.

- The NetDiligence data collection form includes approximately 50 fields per claim. Half of these fields captures demographic information: incident date, country, company size, sector, cause of loss, type of data, and incident description, etc. The other half captures loss data: SIR, Crisis Services including forensics, monitoring, notification, legal counsel, and other crisis services, legal costs and regulatory fines, PCI fines, business interruption loss and recovery expense, and total payout and incident cost.
- We have a significant issue of missing data, for the following two reasons.
 1. Not every claim involves each of the data elements that we ask for. For example, ransomware and staff mistake claims do not usually involve exposed records, whereas most hacking and malware/virus claims do; wire transfer fraud claims do not involve ransoms, and often do not incur any Crisis Services costs.
 2. Not every participant can or does provide us with every data element we ask for. The output format of many insurers' claims systems is not always easily aligned with our data collection form.

This means that we often have to perform subset analyses in which we calculate results in what we describe as an "apples-to-apples" approach. Two of these kinds of analyses involve ransomware and business interruption. The ransomware example follows:

- We have over 1,500 ransomware claims but know the ransom demand for fewer than 600 of these. The average 5-year incident cost for these 1,500 claims is \$179K. However, when you include only the 600 claims for which the ransom is known, the average 5-year incident cost rises to \$267K. If you further limit the analysis to ransomware claims with a business interruption loss, the total 5-year incident cost rises to \$432K.

- So, what is the incident cost of a ransomware event? All three answers are correct. The one you choose depends upon the question you are trying to answer.
- There is no attempt here to consider whether claims associated with the same incident appear more than once in the dataset. 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 as a lower bound; i.e., we know that a given Incident cost at least \$X, but cannot say how much more cost (than this amount) was actually incurred.
- Having said that, beginning in 2017, we asked 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 approximately 16% of the claims submitted for this study remain 'open'. Therefore, aggregate costs as presented in this study include "payouts to-date" and "incident cost to-date". It is virtually certain that additional payouts will be made on some of the claims in the dataset and therefore

