

NetDiligence[®]

CYBER CLAIMS STUDY
2020 REPORT



OUR SPONSORS



Contents

Introduction	1
Key Findings.....	2
An Overview of the Data.....	7
Distribution of Claims by Year of Event.....	7
Exposed Records	7
Incident Cost.....	8
Crisis Services Costs	9
Legal Defense and Settlement Costs.....	10
Regulatory Defense and Fines.....	11
PCI Fines.....	12
Business Interruption and Recovery Expense.....	13
Per-Record Cost.....	14
Recordless Claims vs Claims with Exposed Records	15
Criminal vs Non-Criminal Activities	17
A Word about Self-Insured Retentions (SIRs)	18
Crisis Services Costs by Category	19
Forensics.....	20
Credit/ID Monitoring	21
Notification	21
Breach Coach® (Legal Guidance).....	21
Other Crisis Services	21
Looking at the Data Through Different Lenses	22
Revenue Size	22
Business Sector	24
SMEs	24
Large Companies.....	27

Cause of Loss	29
SMEs	29
Large Companies	32
Insider Involvement	33
Third-Party Involvement	33
Staff Mistakes	33
Type of Data	35
SMEs	35
Large Companies	38
Taking a Closer Look at Growing Risks	40
Office Productivity Software Exploits	40
Cloud	40
Internet of Things (IoT)	41
Ransomware	42
SMEs	42
Social Engineering	45
Conclusion	47
Insurance Industry Participants	47
Insights from Our Sponsors	48
RSM	48
Experian®	50
About NetDiligence®	52
About the Study	53
Contributors	53
Methodology	53



Introduction

Welcome to the tenth edition of the NetDiligence® *Cyber Claims Study*, a decade of work. Each year the study has steadily followed the same methodology, while participants collectively have submitted enriched data. The data has allowed us to dive deeper and produce the most comprehensive report ever. Growth continues in the number of claims submitted, as well as the categories of the data analyzed.

This report includes incidents that occurred during 2015-2019. A total of 3,547 claims were analyzed, and data was distilled into over 100 categories. To compare, the fifth *Cyber Claims Study*, published in 2015, analyzed 207 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

- 3,547 claims analyzed, arising from incidents that occurred during 2015-2019
- 1,633 new claims collected in 2020, from incidents occurring from 2017-2019
- 869 claims analyzed arising from incidents occurring in 2019
- 98% of claims (\$589M in total) from Small to Medium Enterprises (SMEs) with less than \$2 billion in annual revenue
- 2% of claims (\$410M in total) from Large Companies with more than \$2 billion in annual revenue

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 companies.

Preliminary Observations

- As has been the case since the first *Cyber Claims Study* was published ten years ago, there are enormous variances in the 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, and the cost per record ranges from less than \$0.01 to over \$100K. This can lead to sizable differences between average and median costs.

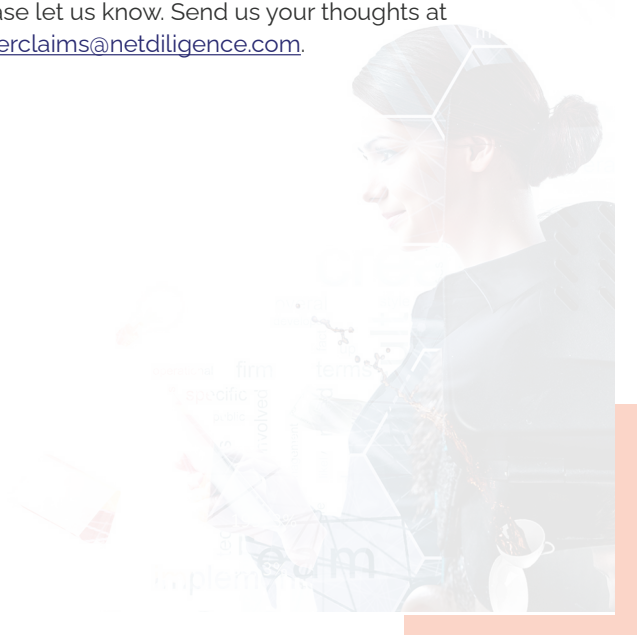
- There are often dramatic differences between the numbers for SMEs and Large Companies – multiples of 10x, 50x, or more. The biggest Large Company in the dataset (over \$30B in annual revenue) is approximately 2.7 million times larger than the smallest organization (\$11K in annual revenue). The average Large Company in the dataset (\$8B in annual revenues) is more than 80 times larger than the average SME (\$92M).
- The reverse is also true: sometimes a smaller company will experience a very expensive claim and a large company will have a claim so small 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 47 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.

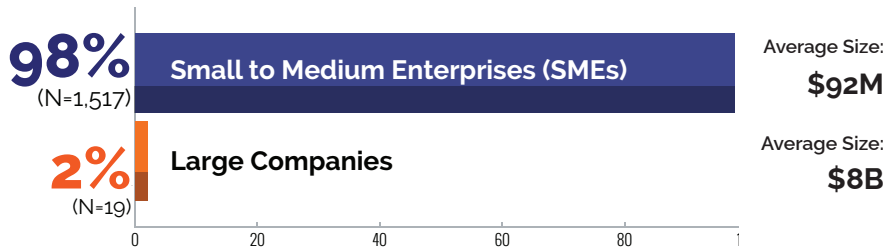
Suggestions

If you have ideas or requests for next year's study, please let us know. Send us your thoughts at cyberclaims@netdiligence.com.



Key Findings

Company Size

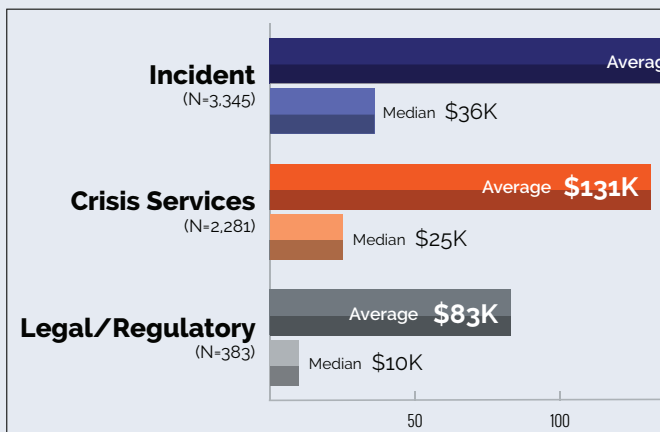


This year's report continues a painful trend as it starts to hit the mathematical extremes of the prior studies. The attacker's shift in preference to small and mid-sized organizations has become overwhelming, where the data shows that being an organization of specific size is more dangerous than being in a specific industry. The only universal constant across both large and small organizations is that incident costs continue to increase and actually appear to be accelerating.

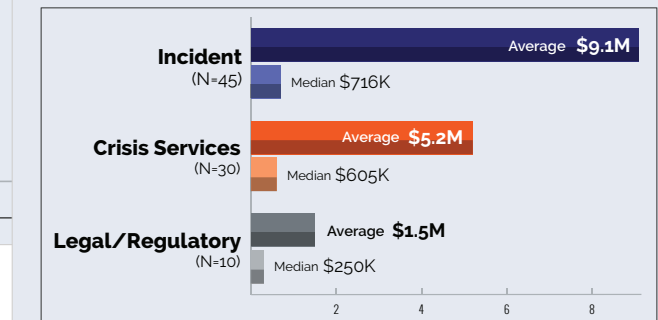
*Daimon Geopfert
National Leader,
Security and Privacy Services
RSM US*

Costs

SMEs



Large Companies



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

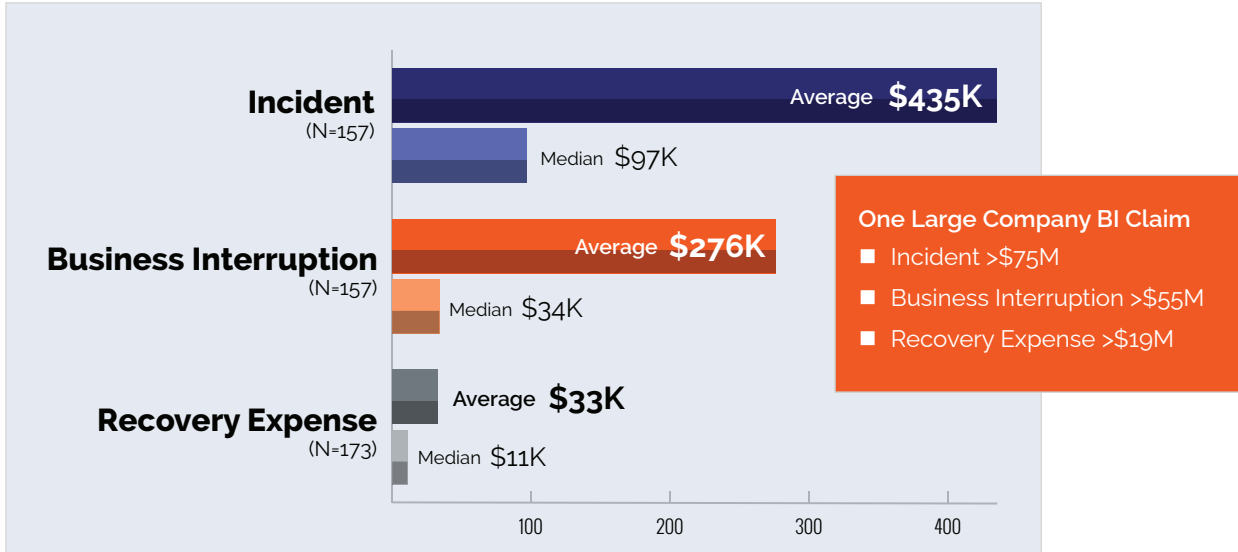
Categorized in this study as organizations with \$2 billion or more in annual revenue.

All findings are for the five-year period 2015–2019, unless otherwise noted.

NetDiligence and Breach Coach are registered trademarks of Network Standard Corporation, dba NetDiligence.

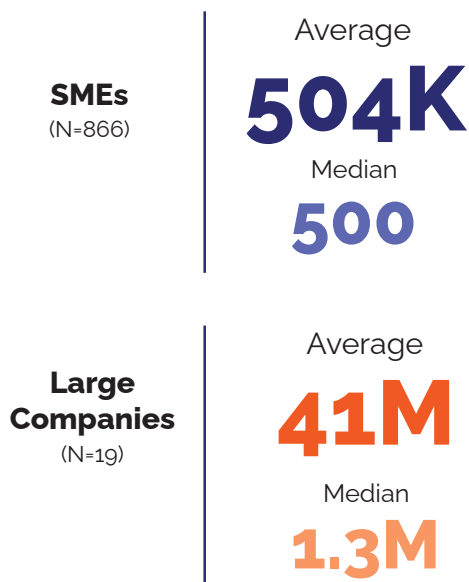
Business Interruption

SMEs

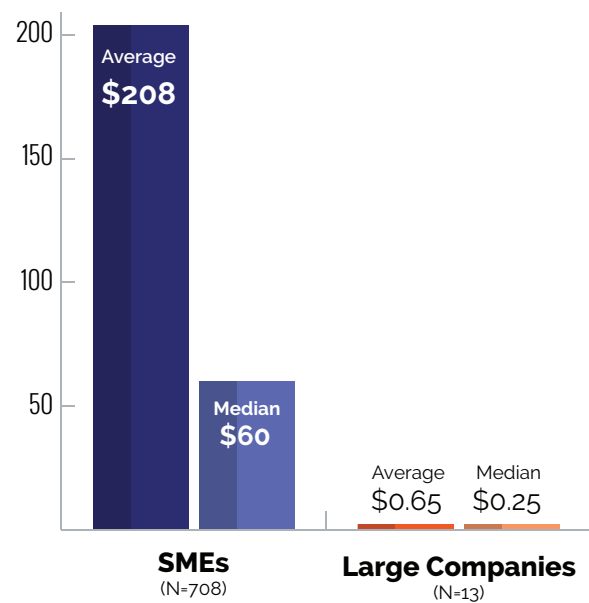


Records

Records Exposed



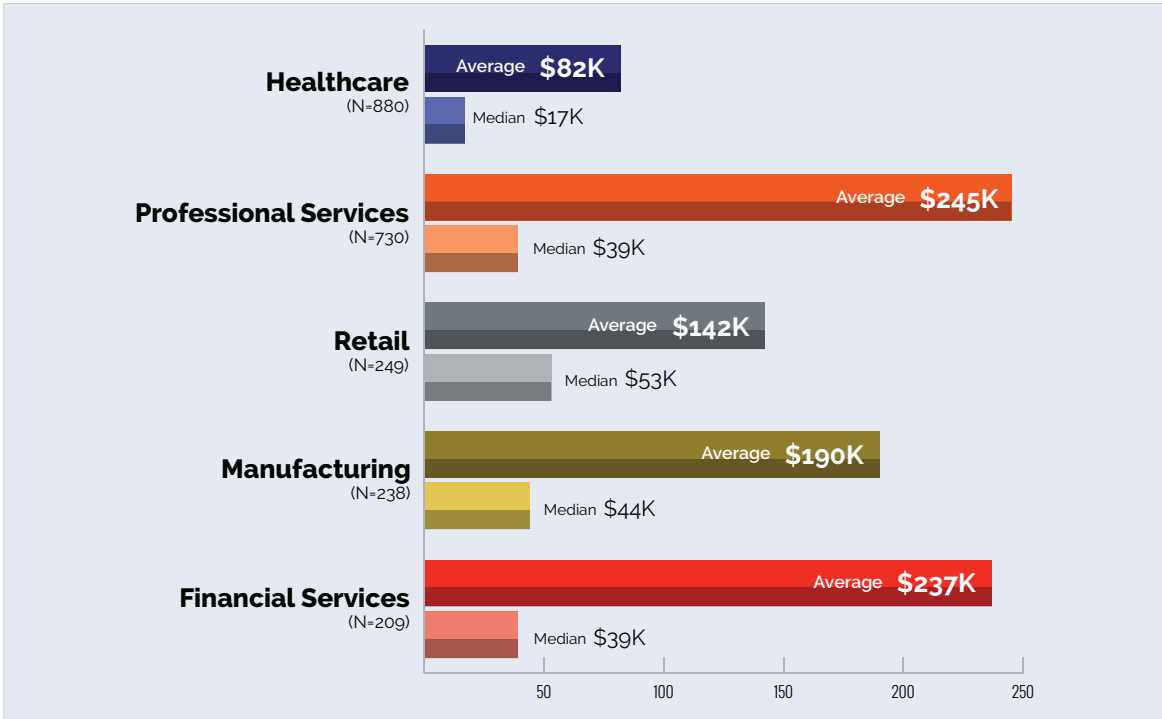
Per-Record Costs



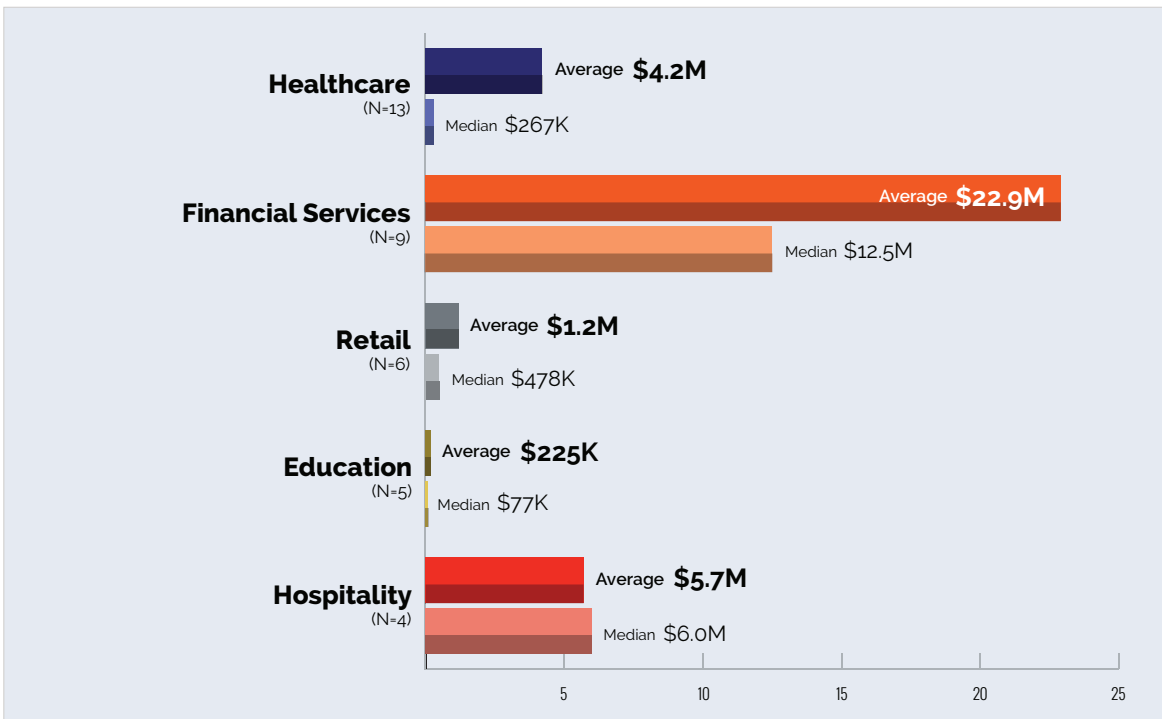
Business Sector

Top 5 by Number of Claims

SMEs



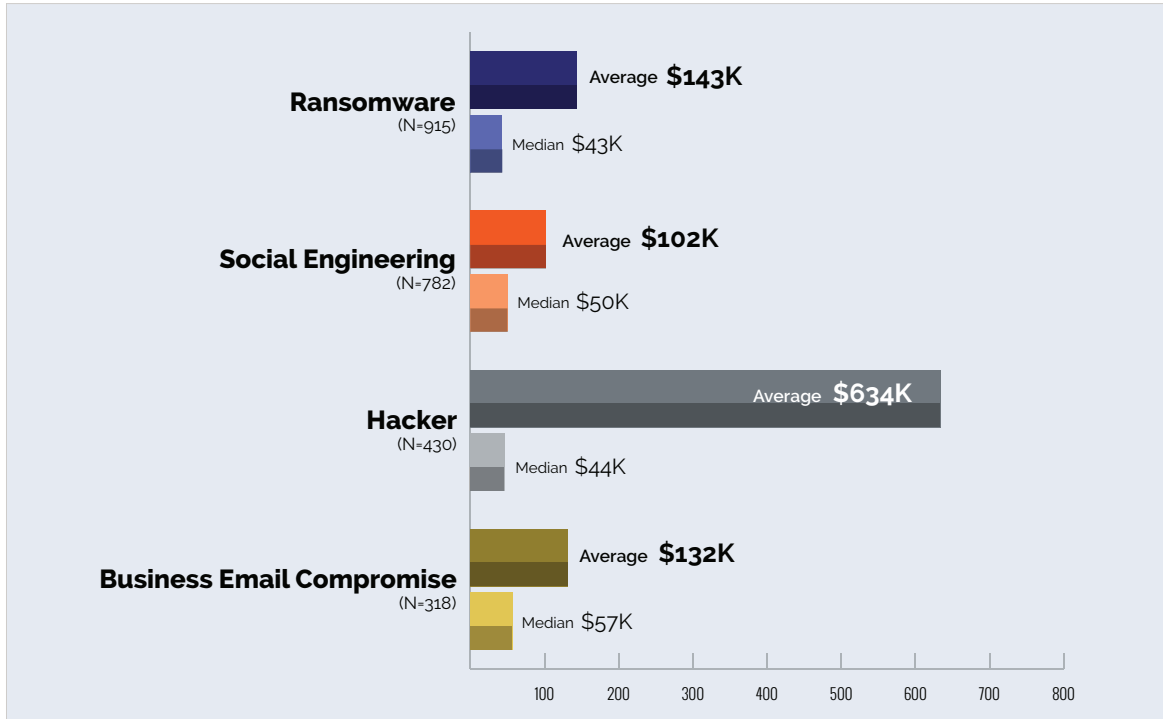
Large Companies



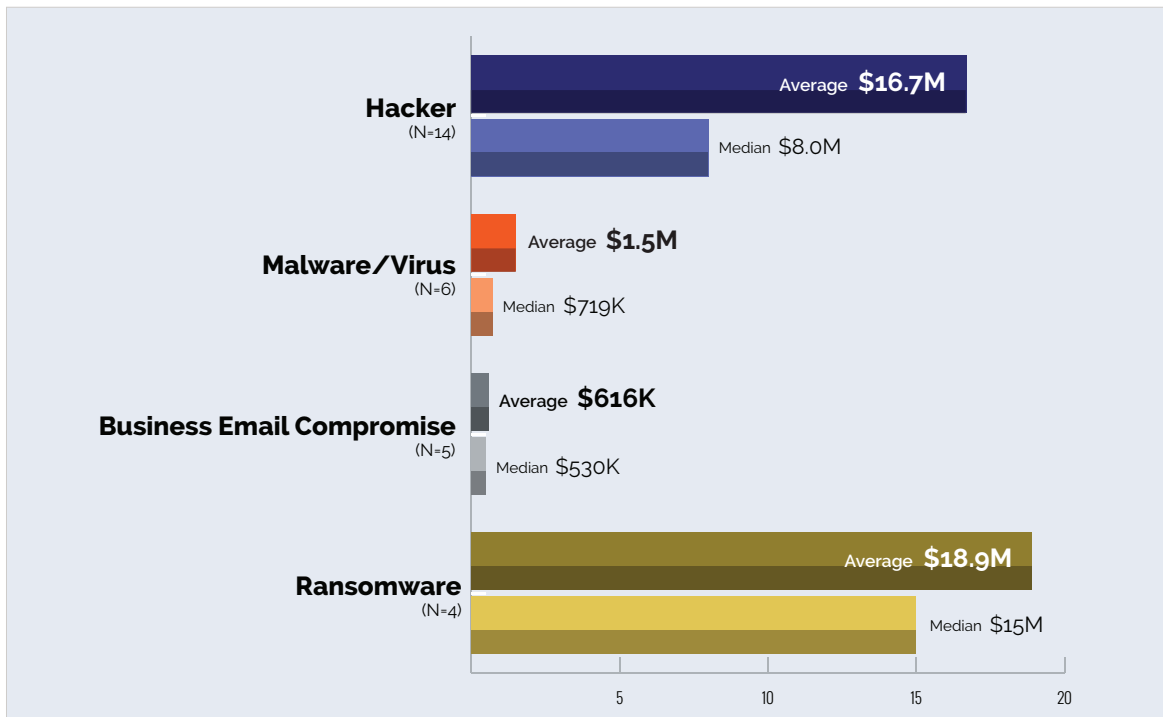
Cause of Loss

Top 4 by Number of Claims

SMEs



Large Companies



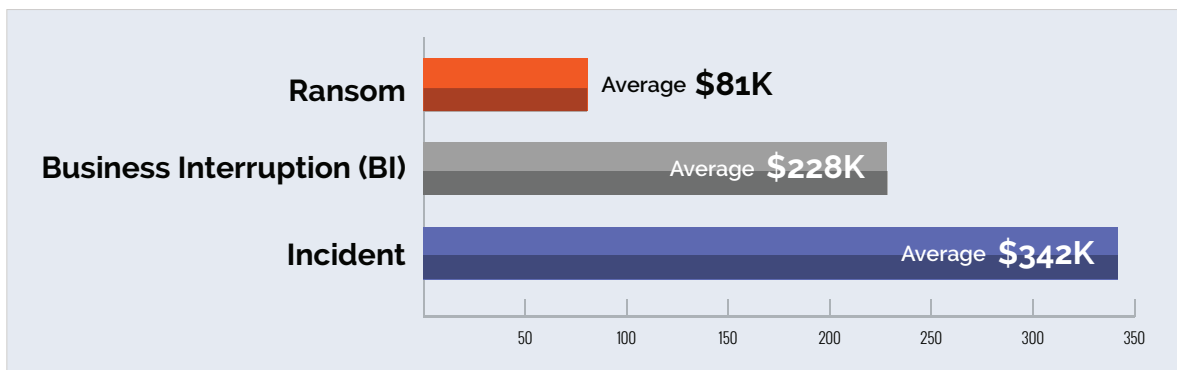
Focus on Ransomware

Leading Cause of Loss for SMEs

Average Costs by Year



Ransomware that Included Business Interruption



An Overview of the Data

The claims analyzed in this study come from companies 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 to skew the finding for small companies.

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. In most cases, analytic results for SMEs are presented separately from those for Large Companies.

A large percentage (40%) 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 \$11K to \$1.9B. The average was \$92M; the median was \$25M.
- Large Companies: annual revenue ranged from \$2B to more than \$30B. The average was \$8B; the median was \$2.9B.

These companies represent over 18 business sectors. For SMEs, the top five sectors as defined by number of claims were:

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

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

- Healthcare
- Financial Services
- Retail
- Education
- Hospitality

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

Distribution of Claims by Year of Event

The scope of this study is 3,547 incidents that occurred from 2015-2019. 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 217 in 2015 to over 1,300 in 2018 and 869 in 2019.¹

Percentage of Claims by Date of Event
2015-2019

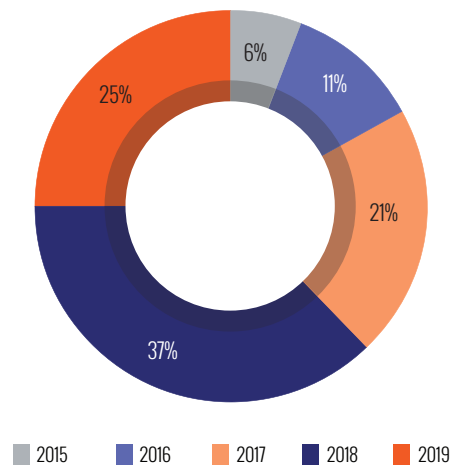


Figure 1

Exposed Records

Of the 3,547 claims in the dataset, 905 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 1.2 billion. The numbers of records exposed per claim ranged from a single record to over 300 million records. Incidents at SMEs accounted for 886 of these claims and 447 million records. Incidents at Large Companies accounted for 19 claims and 775 million records.

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 2018 and 2019, incidents at Large Companies exposed far greater numbers of records than in each of the three prior years.

¹ New claims are collected for incidents that occurred during the previous three calendar years. For the 2020 study, these were incidents in 2017, 2018, and 2019.

Large Companies exposed, on average, 80 times more records than SMEs.

Average & Median Records Exposed

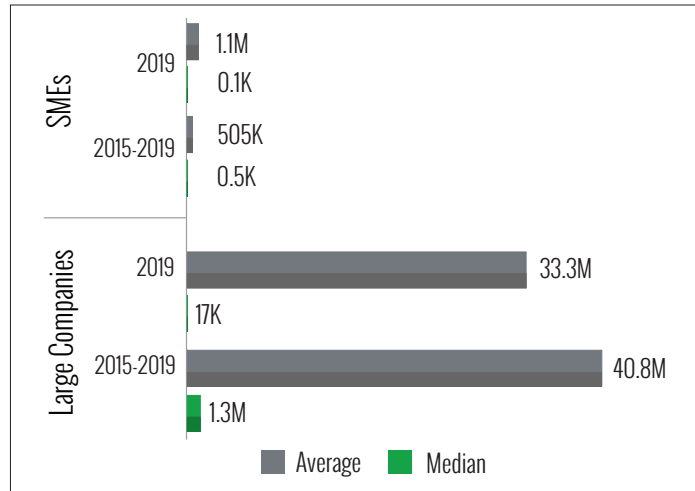


Figure 2

Figure 2 shows the average and median 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, **80 times more records** than incidents at SMEs .

Incident Cost

Incident Cost, inclusive of Self-Insured Retention (SIR), ranged from a low of \$1,000² to more than \$120M. Figure 3 depicts 2019 and five-year (2015-2019) Incident Costs for SMEs and Large Companies. Figure 4 depicts the average and median Incident Costs.

The averages were influenced by some very expensive claims. This was especially true for Large Companies, primarily because there were five claims ranging from \$6M to over \$60M in 2017 and a single claim in 2019 for almost \$100M. For SMEs, the average and median five-year Incident Costs were \$175K and \$36K, respectively. For Large Companies, the five-year numbers were \$9.1M and \$716K. The highest costs belonged to the Healthcare sector in 2015 (\$34M); Transportation in 2016 (\$81M); Professional Services in 2017 (\$120M); Hospitality in 2018 (\$60M), and Financial Services in 2019 (\$122M).

Total Incident Costs

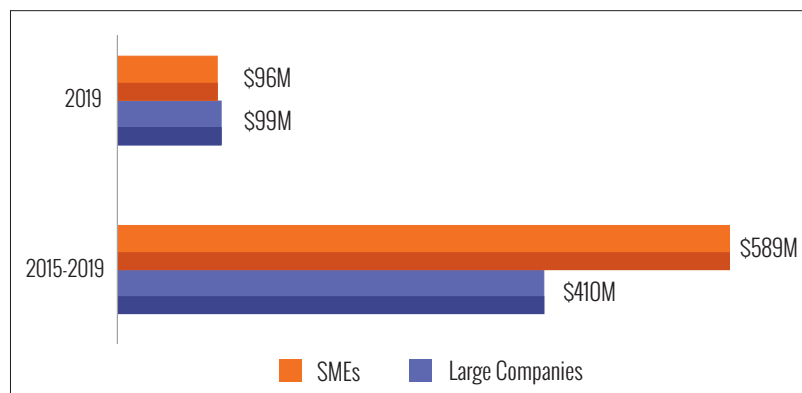


Figure 3

² A few claims for less than \$1K were excluded from the analysis.

Average & Median Incident Costs

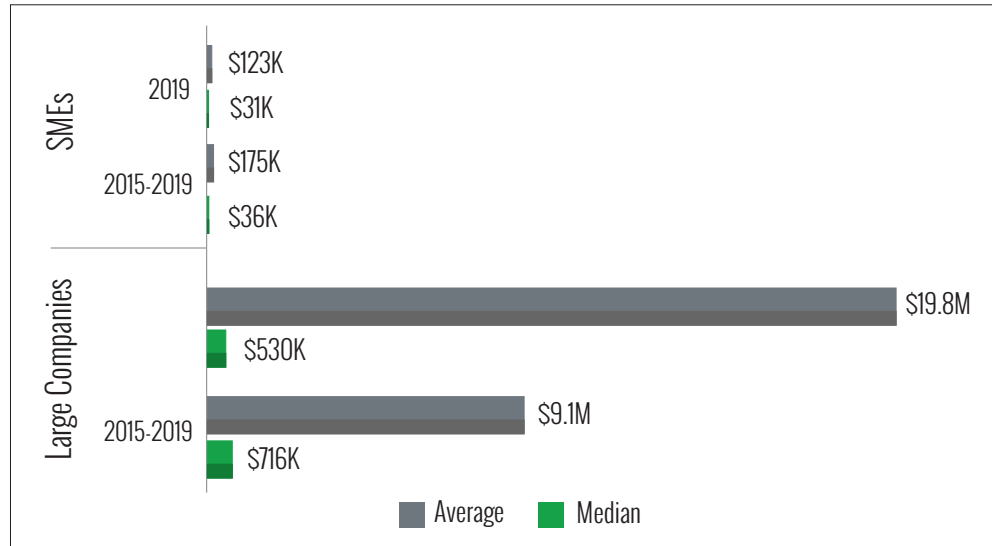


Figure 4

Crisis Services Costs

For the five-year period, Crisis Services Costs overall ranged from less than \$100 to over \$120M. In 2019, Crisis Services Costs ranged from less than \$100 to \$15M. For SMEs, 2019 had both the lowest and highest Crisis Services costs over the five-year period: from less than \$100 to \$15M. For Large Companies, the 2019 numbers ranged from \$6K to \$1.2M and the five-year numbers from \$2.6K to \$64M. Figure 5 shows the average and median Crisis Services costs for SMEs and Large Companies.

Crisis Services Costs

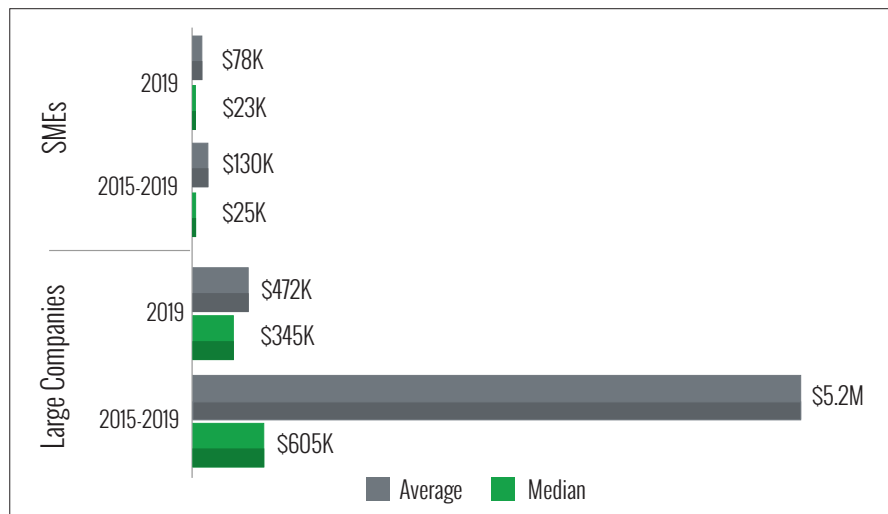


Figure 5

Legal Defense and Settlement Costs

For the five-year period, the dataset contained 339 claims with legal defense costs and 159 claims with legal settlement costs. For defense, these costs ranged from less than \$500 to \$5M. For settlement, the costs ranged from <\$500 to \$6.8M.

The costs for SMEs ranged from less than \$500 to \$5M for defense, and less than \$1K to \$6.8M for settlements. For Large Companies, the ranges for defense and settlement were \$5K to \$5M, and \$50K to \$6.5M, respectively.

Figure 6 (SMEs) and Figure 7 (Large Companies) depict the average and median costs for each category.

Legal Defense and Settlement Costs

SMEs

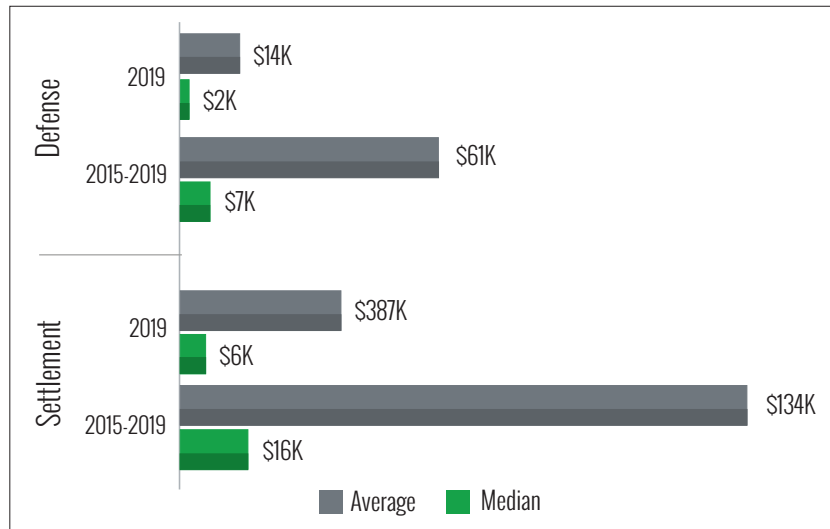


Figure 6

Large Companies

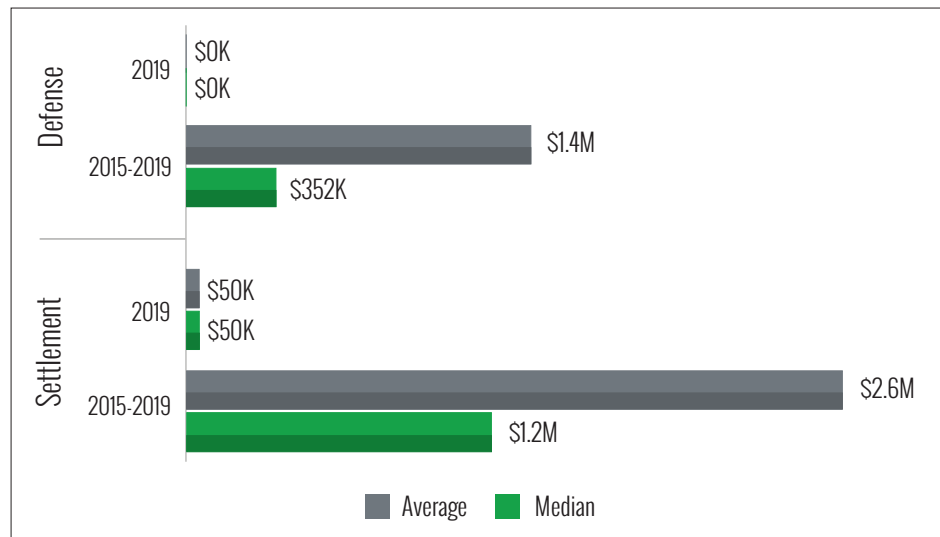


Figure 7

Regulatory Defense and Fines

For the five-year period, there were 15 claims with amounts for regulatory defense and 9 claims with amounts for regulatory fines. For defense, the amounts ranged from \$2K to \$368K. For regulatory fines, the amounts ranged from \$5K to \$3.5M.

For SMEs, these costs ranged from \$3.5K to \$368K for defense, and \$5K to \$99K for fines. For Large Companies, regulatory defense ranged from \$2K to \$250K; there was a single claim for a regulatory fine of \$3.5M.

Figure 8 (SMEs) and Figure 9 (Large Companies) depict the average and median costs for each category.

Regulatory Defense Costs and Fines

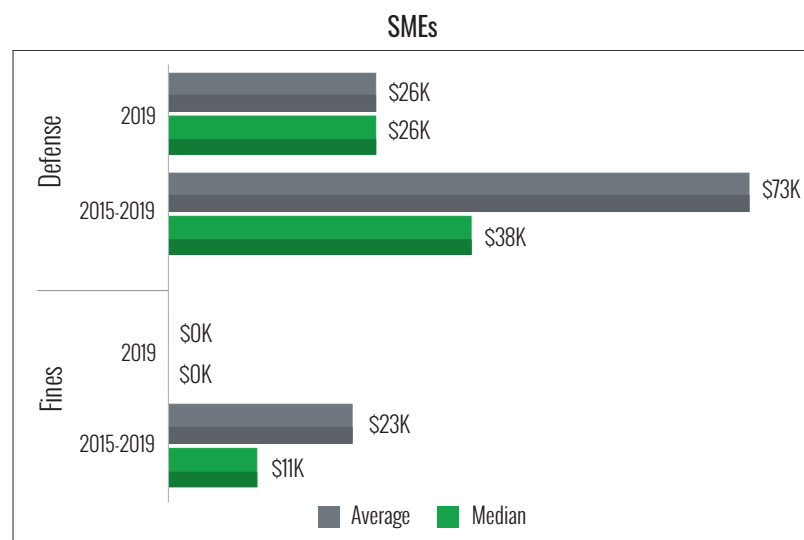


Figure 8

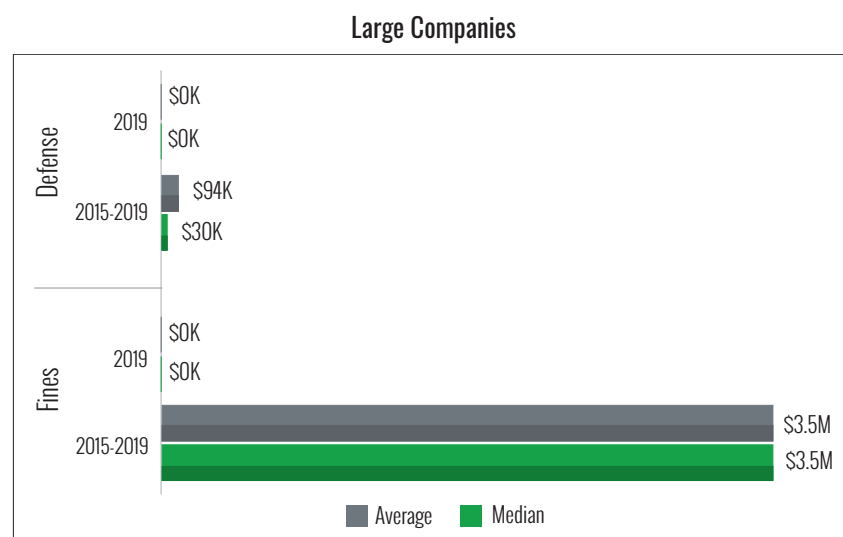


Figure 9

Note: There have been few claims for regulatory defense since 2015, and only one claim prior to 2017 for regulatory fines.

PCI Fines

Only 11 claims in the five-year data included PCI fines and no claims in 2019. The fines ranged \$21K to \$4.2M and totaled \$12M. For SMEs, there were 9 claims with PCI fines ranging from \$21K to \$4.2M. The average PCI fine was \$1.3M and the median was \$297K. For Large Companies, there were only two claims with PCI fines, one for \$25K and one for \$385K. The average and median were the same: \$205K.

PCI fines typically include costs for card brand-ordered assessments, forensic investigations, and card replacement costs. Often, they are not assessed until 12-18 months after an incident, which may explain why the dataset contains so few of them

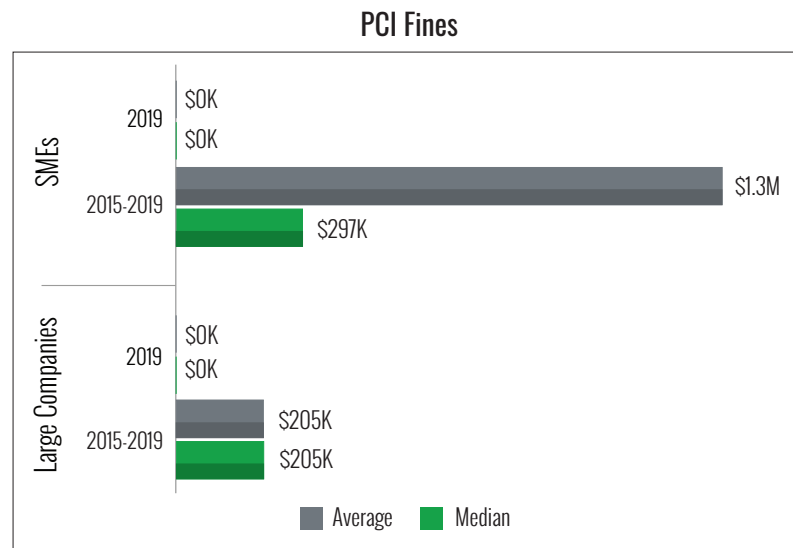


Figure 10

Business Interruption and Recovery Expense

Of the 3,547 claims in the dataset, 158 included costs for lost business income and 174 included costs for recovery expense.

The average incident cost for a BI claim was much higher than the average cost of other incidents.

At SMEs, there were 157 business interruption (BI) claims during the five-year period. The BI amounts ranged from less than \$200 to as much as \$10M. While the overall average incident cost at an SME was \$175K, the average incident cost for a BI claim was much higher - \$435K. In 2019, incidents that included some BI costs were also significantly higher on average than overall claims: \$339K vs \$123K.

Incident costs that included recovery expenses were higher in 2019 than the overall average (\$176K vs \$123K), but lower for the five-year period (\$131K vs \$175K).

There was only one Large Company claim that included these costs. It was attributed to a non-criminal network outage/system glitch. The lost income reported for that incident was \$60M; the recovery expense was \$20M.

Lost Business Income and Recovery Expense
SMEs

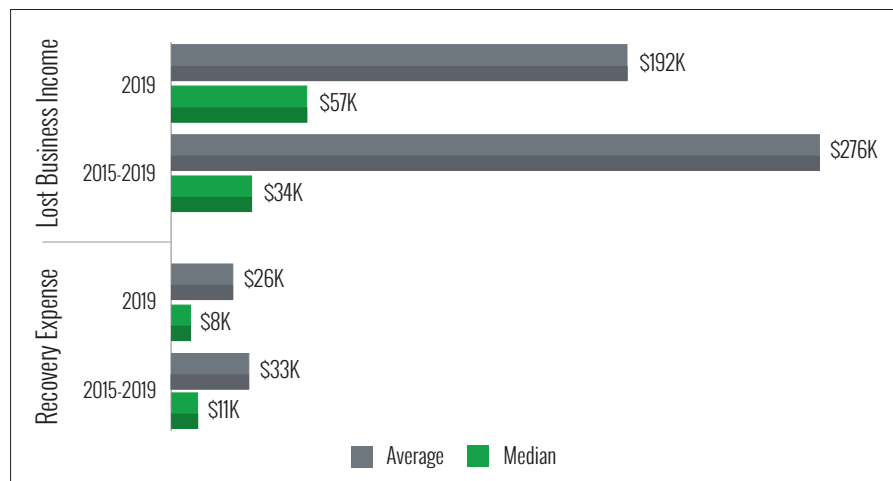


Figure 11

Per-Record Cost

Average per-record costs are heavily influenced by outliers at both ends of the spectrum. For example, the dataset contained per-record costs ranging from \$0.001 to as much as \$100K.

To understand the outsized influence of outliers, Table 1 displays per-record costs based upon 100%, 95%, 90% and 80% of the data when ranked from lowest to highest per-record costs. The results highlight the variances in the averages.

Per-Record Costs

Revenue Size	Time Period	Percent of Data	Claims	Minimum	Average	Median	Maximum
SMEs	2019	100%	98	0.01	2,609	194	99,439
		95%	92	0.78	1,140	194	13,484
		90%	88	5.85	914	194	8,802
		80%	78	7.94	584	194	3,196
	2015-2019	100%	886	0.001	1,274	60.36	100,000
		95%	840	0.58	515	60.36	9,134
		90%	796	1.24	344	60.36	5,067
		80%	708	2.41	208	60.36	1,688
Large Companies	2019	100%	3	2.72	2.85	2.72	3.12
		95%	1	2.72	2.72	2.72	2.72
		90%	1	2.72	2.72	2.72	2.72
		80%	1	2.72	2.72	2.72	2.72
	2015-2019	100%	19	0.02	0.90	0.25	3.12
		95%	17	0.03	0.82	0.25	2.72
		90%	16	0.04	0.87	0.25	2.72
		80%	13	0.05	0.65	0.25	1.97

Key: 95% = 2.5-97.5 percentiles 90% = 5th-95th percentiles 80% = 10th-90th percentiles

Table 1

For SMEs, when outliers at the top and bottom are eliminated, the average per-record cost drops dramatically.³ While the average per-record numbers have changed quite a bit since the 2019 study, the median five-year per-record costs have remained almost the same: \$59.66 in the 2019 study and \$60.36 in the 2020 study.

For Large Companies, there are fewer claims and fewer outliers to eliminate, so the ranges for average and median per-record costs are much narrower.

Note: Soft costs, such brand and reputation damage and stock price devaluation, are not collected as part of this study, and therefore are not factored in to the per-record costs presented here. Quantifying such costs, which are often excluded from cyber insurance coverage, is difficult.

³ Median values do not change. The value in the middle of a ranked list does not change, or not change much, as equal numbers of claims are dropped from the top and bottom.

Recordless Claims vs Claims with Exposed Records

More than half of the 2019 claims were for recordless incidents.

A marked shift in findings over the past couple of years is the growing prevalence of “recordless” incidents, which represent 39% of the claims in the dataset. Examples included most ransomware, distributed denial of service (DDoS), and wire transfer fraud/theft of money-related claims.

The proportion of recordless claims increased to 55 % in 2019 (58% for SMEs and 2% for Large Companies).

Recordless Claims vs Claims with Exposed Records Incident Cost

Revenue Size	Time Period	Nature of Claim	Claims	Range	Average	Median
SMEs	2019	Recordless	449	1K-3.9M	124K	48K
		Exposed Records	331	1K-25M	122K	9K
	2015-2019	Recordless	1,636	1K-20M	134K	42K
		Exposed Records	1,718	1K-120M	215K	27K
Large Companies	2019	Recordless	1	530K	530K	530K
		Exposed Records	4	6K-97M	24.7M	800K
	2015-2019	Recordless	17	3K-80M	8.1M	505K
		Exposed Records	28	5K-97M	9.8M	1.5M

Table 2

The comparative averages for Incident and Crisis Services Costs are depicted in Figure 12 for SMEs and Figure 13 for Large Companies.

Average Costs — Events with Records vs Recordless Events

SMEs

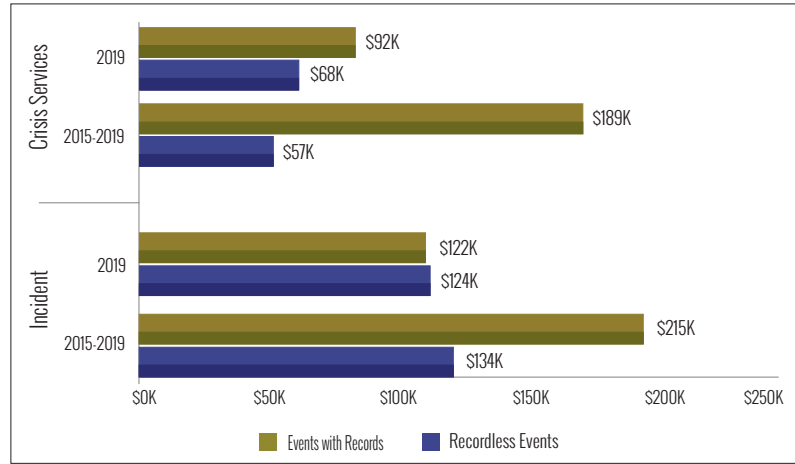


Figure 12

Large Companies

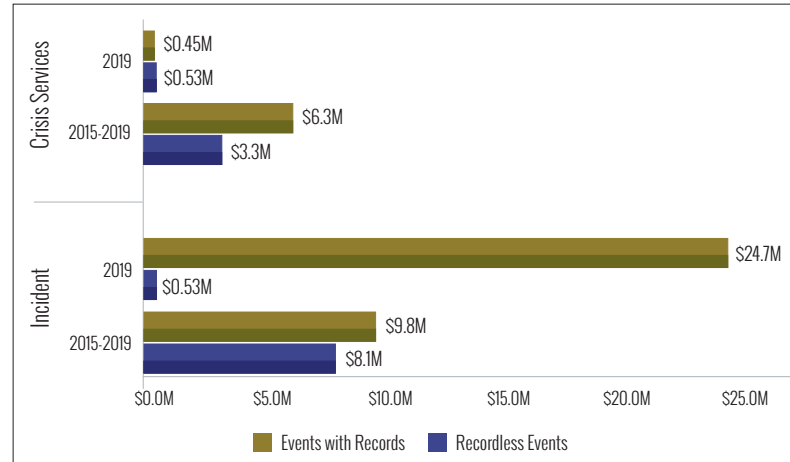


Figure 13

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, and banking/ACH fraud. Non-criminal events include staff mistakes, mishandling of paper records, improper disclosure, lost laptops, programming errors, system glitches, and legal actions.

Since 2015, the proportion of claims caused by criminal activities has ranged from a high of 82% to a low of 71%. The proportion of claims caused by non-criminal activities has been increasing slightly since 2018, to a high of 29% in 2019. This increase is due mainly to an increase in claims for staff mistakes. For more detail on Staff Mistakes, please see the section following called "Looking at the Data Through Different Lenses."

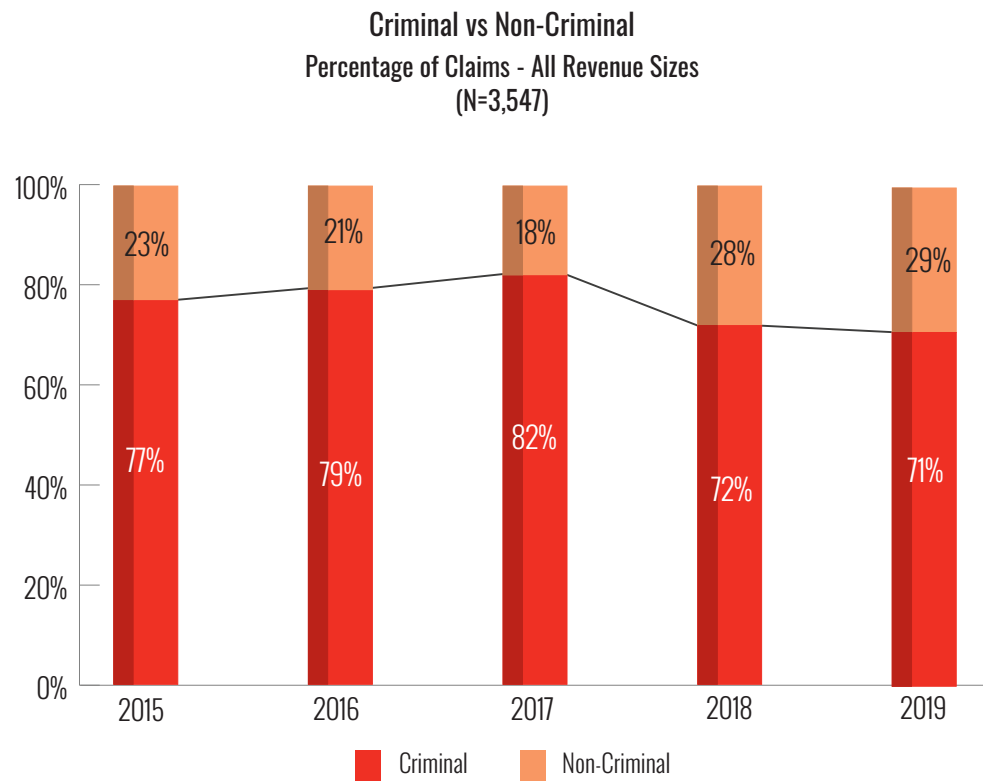


Figure 14

Average Incident and Crisis Services Costs, as well as the average number of records exposed, were all dramatically higher for criminal events. The number of incidents at Nano Revenue organizations accounted for 50% of all criminal incidents. Of the 50%, 43% were Healthcare, which spent a total of \$69M in Crisis Services.

Criminal vs Non-Criminal Financial Impact

Revenue Size	Time Period	Nature of Cost	Type of Activity	Claims	Minimum	Average	Median	Maximum	Total
SMEs	2019	Crisis Services	Criminal	423	1K	97K	33K	15M	41.1M
			Non-Criminal	112	1K	7K	2K	195K	788K
		Incident	Criminal	584	1K	156K	45K	25M	91.3M
			Non-Criminal	196	1K	23K	4K	401K	4.5M
	2015-2019	Crisis Services	Criminal	1,909	1K	151K	30K	120.2M	288.6M
			Non-Criminal	372	1K	22K	4K	679K	8.2M
		Incident	Criminal	2,587	1K	206K	44K	120.2M	532.2M
			Non-Criminal	767	1K	74K	13K	17.5M	56.4M
Large Companies	2019	Crisis Services	Criminal	4	6K	472K	345K	1.2M	1.9M
			Non-Criminal						
		Incident	Criminal	5	6K	19.8M	530K	97M	99.1M
			Non-Criminal						
	2015-2019	Crisis Services	Criminal	27	6K	5.8M	696K	64M	155.5M
			Non-Criminal	3	3K	140K	199K	218K	420K
		Incident	Criminal	37	6K	8.9M	875K	97M	327.7M
			Non-Criminal	8	3K	10.3M	250K	80M	82.6M

Table 3

A Word about Self-Insured Retentions (SIRs)

The dataset contains 1,845 claims that reported a value for SIR. Over 5 years, the value of SIR ranged from \$0 to \$15M. In 2018, SIR ranged from \$0 to \$1M.

Self-Insured Retentions

Revenue Size	Time Period	Claims	Minimum	Average	Median	Maximum
SMEs	2019	494	0	31K	10K	10M
	2015-2019	2,349	0	40K	10K	10M
Large Companies	2019	3	0	3.4M	50K	10M
	2015-2019	41	0	2.2M	500K	15M

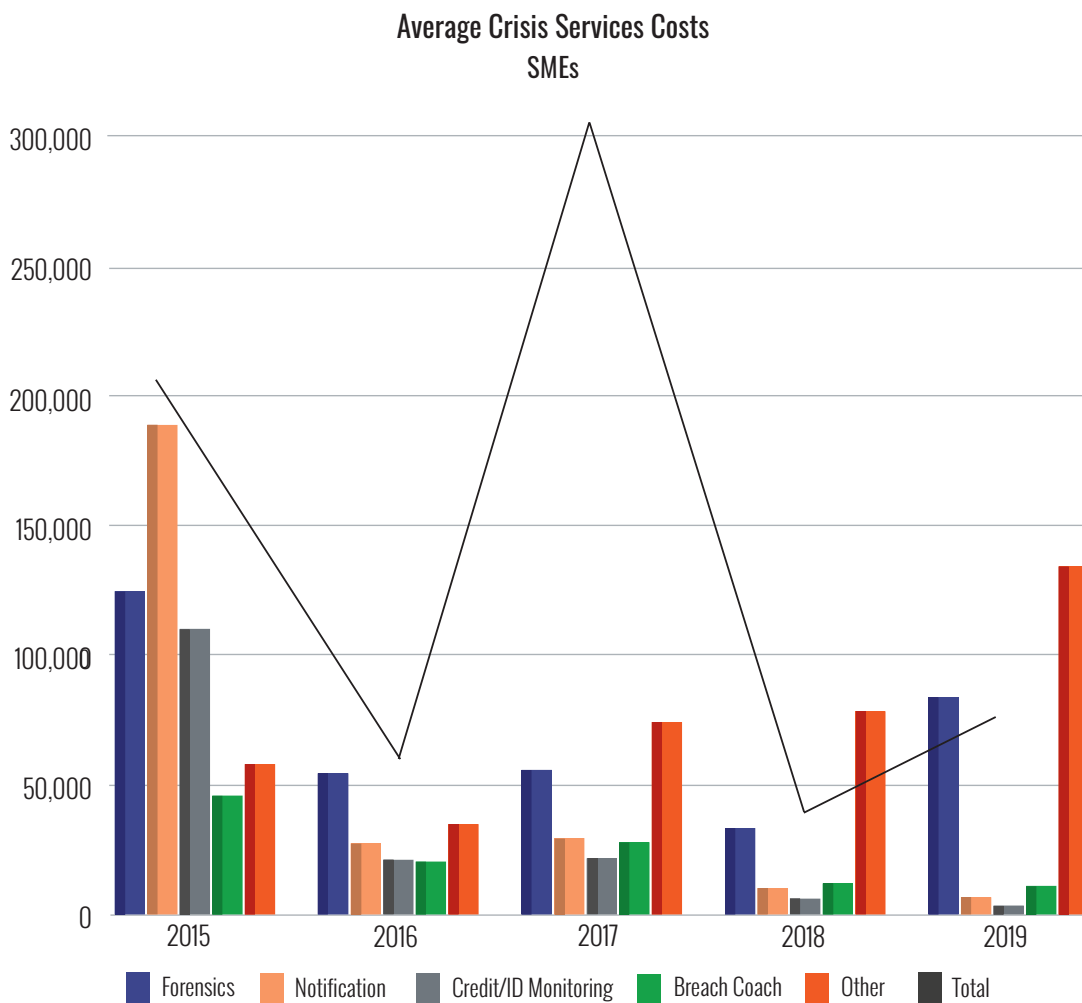
Table 4

Crisis Services Costs by Category

In addition to Total Crisis Services Costs, the dataset contains costs for five distinct categories of Crisis Services: Forensics, Credit/ID monitoring, Notification, Breach Coach® (legal guidance), and Other. Many claims reported costs in some of the categories but not in others, and many claims reported the total cost only. Therefore, Total Crisis Services costs are typically higher than the sum of the costs by category. The graph below plots the yearly average of these categories as columns, with the average Total Crisis Services costs as a line. Crisis services have been trending downward over the past five years. One potential factor in that trend may be the move by cyber carriers to include bundled breach response services as a component of their policy, thereby driving down service rates.

With the majority of companies and employees working in a virtual environment during Covid-19 and the communication challenges associated with a remote workforce, it's imperative to have a well-thought out and practiced plan that lends itself to detailed tasks and workflows, and clearly defined roles and responsibilities for quick decision-making in a time of crisis. Experian® Reserved Response is the only program that provides a real-time and live test of your end-to-end Incident Response Plan including the aspects that play out in the public – the customer response.

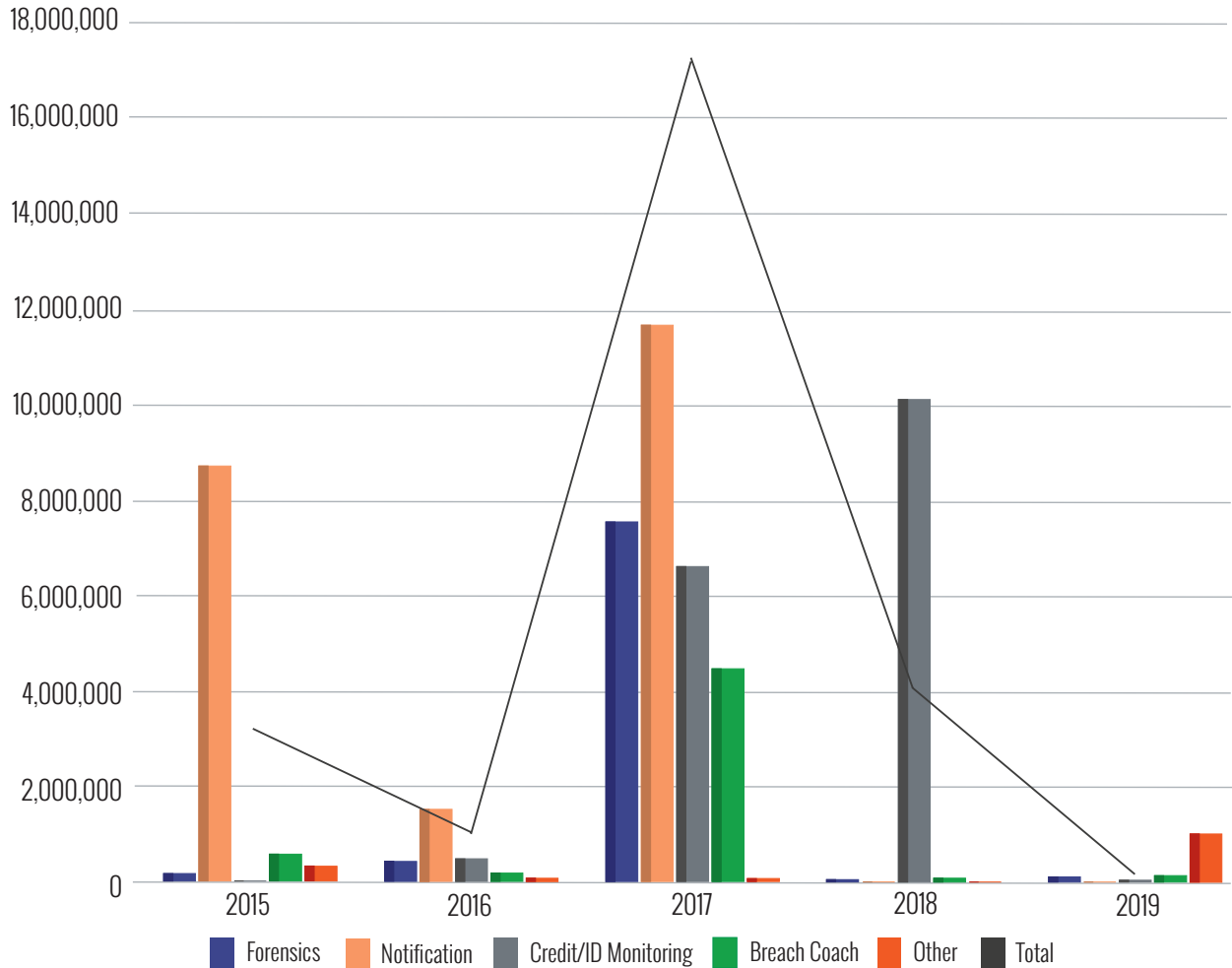
*Lisa Larson
VP of Account Development and Customer Success
Experian® Enterprise Partner Solutions*



* Includes public relations, data restoration, as well as ransom/extortion payment and fraudulent wire transfer

Figure 15

Average Crisis Services Costs
Large Companies



* Includes public relations, data restoration, as well as ransom/extortion payment and fraudulent wire transfer

Figure 16

Forensics

SMEs

In the SME space, 1,467 claims reported costs for Forensics during the five-year period. These costs ranged from less than \$100 to \$15M, with an average of \$60K and a median of \$24K. In 2019, there were 342 claims that included costs for Forensics. The range of costs remained about the same: \$500 to \$15M. The average and median costs increased to \$84K and \$28K. The \$15M cost was incurred in a claim for a hack of a healthcare institution that exposed a very large number of PII records.

Large Companies

For Large Companies, 19 claims reported costs for Forensics during 2015-2019. These costs ranged from \$18K to \$33M, with an average of \$2.5M and a median of \$267K. In 2019, based upon three claims, the cost range decreased dramatically: \$45K to \$170K. The average and median costs also decreased substantially to \$107K and \$105K. The claim for \$33M in forensics costs was due to a malware event that caused a severe disruption of the organization's network.

Credit/ID Monitoring

SMEs

Based upon 357 claims for the five-year period, Credit/ID Monitoring costs at SMEs ranged from less than \$100 to \$2.0M. The average and median costs were \$26K and \$3K. In 2019, there were 35 claims with costs from less than \$100 to \$50K. Average and median costs were \$3K and \$500, respectively.

Large Companies

Credit/ID Monitoring costs at Large Companies, based upon 7 claims for the five-year period, ranged from \$2.5K to \$13M, with an average of \$3.5M and a median of \$104K. There was only one claim for credit monitoring costs in 2019: the amount was \$39K and the Incident Cost was \$159K. The largest cost (\$13M) was incurred due to unauthorized access to systems by a hacker.

Notification

SMEs

There were 439 claims for Notification costs at SMEs during the five-year period. These costs ranged from <\$100 to \$2.9M. The average and median costs were \$42K and \$5K. In 2019, there were 53 claims. Notification costs ranged from <\$200 to \$61K with an average \$6K and a median of \$3K. The largest claims with Notification costs were all due to hackers and unauthorized access to data and/or theft of data.

Large Companies

Notification costs at Large Companies for the five-year period ranged from \$13K-\$23M, with an average of \$5.8M and a median of \$2.2M. There were no claims for Notification costs in 2019. The largest cost (\$23M) was incurred due to unauthorized access to systems by hackers.

Breach Coach® (Legal Guidance)

SMEs

There were 1,983 claims during the five-year period that included costs for legal guidance. These costs ranged from less than \$100 to \$1M, with average and median costs of \$19K and \$6K. In 2019, based upon 482 claims, these costs were between \$200 and \$582K. The average cost for legal guidance was \$11K; the median cost was \$5.5K.

Large Companies

There were 21 claims during the five-year period for legal guidance costs. These costs ranged from \$700 to \$21M, with an average of \$1.2M and a median of \$70K. In 2019, there were 4 claims for these costs, ranging from \$6K to \$360K. The average of these costs was \$133K; the median was \$83K. The largest of these costs was, once again, due to the unauthorized access to systems by hackers.

Other Crisis Services

Other Crisis Services costs encompass a broad array of expenses: PR costs, data restoration costs, recovery costs, incident response costs incurred prior to authorization from an insurance company, and even data mining. Often, a claim does not provide details regarding what constitutes the 'Other Crisis Services' expense.

SMEs

For the five-year period, there were 218 claims for Other Crisis Services expenses. These costs ranged from less than \$200 to \$2.4M. The average cost was \$82K; the median cost was \$17K. In 2019, there were 51 claims with costs ranging from \$2K to \$2.4M. The claim for \$2.4M in Other Crisis Services costs described these costs as incurred for business and IT interruption.

Large Companies

For the five-year period, there were 8 claims for Other Crisis Services costs, ranging from \$8K to \$1M. The average was \$214K and the median was \$91K. In 2019, there was one claim (\$1M) for Other Crisis Services. This expense was described as "document review."

Looking at the Data Through Different Lenses

Revenue Size

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

As was mentioned above, SMEs (companies with annual revenues less than \$2B) account for 98% of the claims analyzed, and 59% of Incident Costs (\$589M out of \$999M). Large Companies (companies with annual revenues greater than \$2B) account for only 2% of the claims analyzed but 41% of the Incident Costs (\$410M/\$999M). The tables below provide summary statistics for Incident and Average Crisis Services Costs.

**Percentage of Claims by Revenue Size
SMEs — 2019
(N=855)**

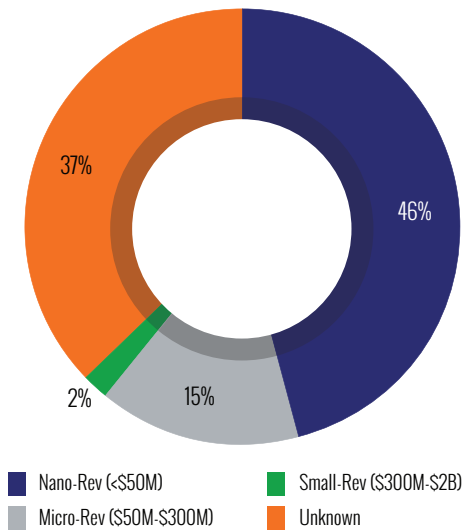


Figure 17

**Percentage of Claims by Revenue Size
SMEs — 2015-2019
(N=3,493)**

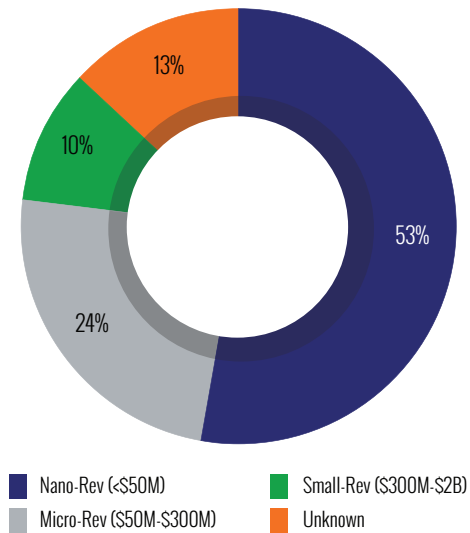


Figure 18

**Percentage of Claims by Revenue Size
Large Companies — 2015-2019
(N=54)**

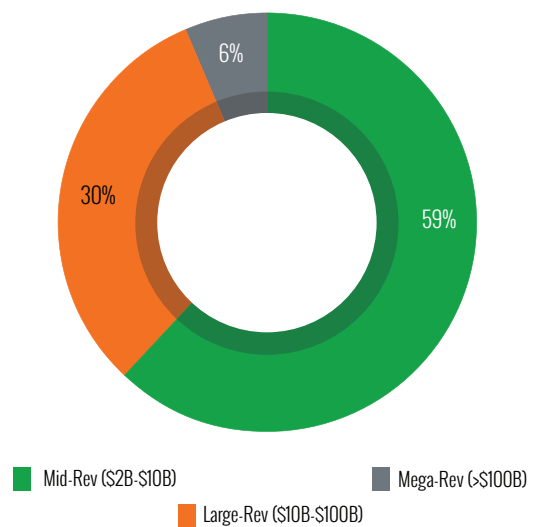


Figure 19

The tables below provide summary statistics for Incident and Average Crisis Services Costs.

**Incident Cost by Revenue Size
2015-2019**

	Revenue Size	Claims	Minimum	Average	Median	Maximum	Total
SMEs	Nano-Rev (<\$50M)	1,590	1K	91K	41K	7.1M	145.4M
	Micro-Rev (\$50M-\$300M)	594	1K	173K	62K	6.6M	102.9M
	Small-Rev (\$300M-\$2B)	199	3K	359K	105K	7.4M	71.3M
	Unknown	970	1K	211K	12K	120.2M	204.5M
Large Companies	Mid-Rev (\$2B-\$10B)	28	3K	3.6M	207K	64.0M	99.6M
	Large-Rev (\$10B-\$100B)	15	249K	20.3M	10.0M	97.0M	305.2M
	Mega-Rev (> \$100B)	3	15.0'M	23.3M	15.0M	40.0M	70.0M

Table 5

**Average Crisis Services Costs by Revenue Size
2015-2019**

	Revenue Size	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services
SMEs	Nano-Rev (<\$50M)	39K	45K	24K	18K	53K	67K
	Micro-Rev (\$50M-\$300M)	71K	72K	75K	33K	95K	122K
	Small-Rev (\$300M-\$2B)	112K	55K	34K	46K	91K	161K
	Unknown	42K	14K	8K	9K	192K	198K
Large Companies	Mid-Rev (\$2B-\$10B)	921K	6.6M	2.4M	1.3M	201K	4.0M
	Large-Rev (\$10B-\$100B)	12.0M	4.9M	10.0M	741K	306K	7.0M
	Mega-Rev (> \$100B)						

Table 6

Business Sector

Claims are categorized in one of 18 sectors, or when the sector is unknown, to an unknown sector. The table of predefined sectors can be found in the appendices.

The graphics below show the proportion of claims for 2019 as well as 2015-2019, for both SMEs and Large Companies.

As has been the case for many years, claims from the Healthcare, Professional Services, Retail, Manufacturing, and Financial Services sectors provide nearly 70% of the SME claims to be analyzed and over 80% of the Large Company claims.

SMEs

Percentage of Claims by Sector
SMEs — 2019
(N=855)

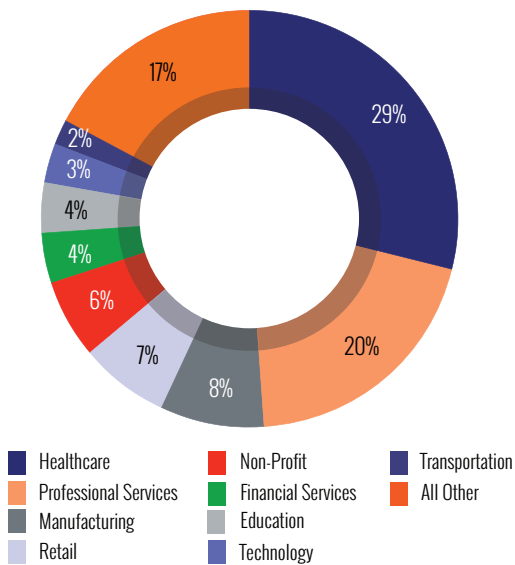


Figure 20

Percentage of Claims by Sector
SMEs — 2015-2019
(N=3,493)

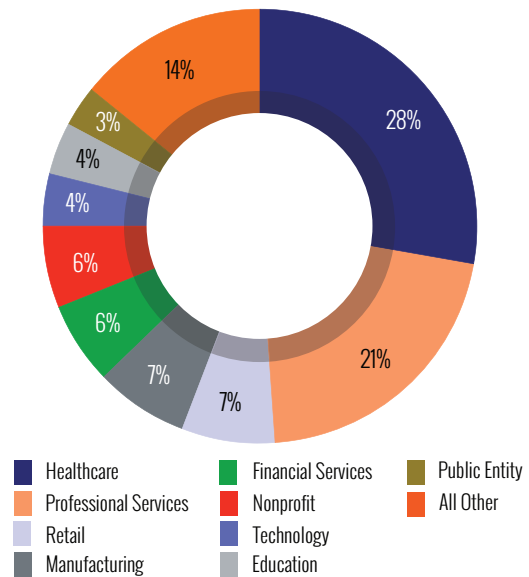


Figure 21

The following tables provide summary statistics for all the SME sectors that have been analyzed for this year's report.

Incident Cost by Business Sector
SMEs – 2015-2019

Sector	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Education - All	142	1.5K	149K	63K	1.5M	21.1M	12
Education - Higher Ed only	68	1.5K	204K	91K	1.5M	13.9M	9
Energy	22	1.5K	71K	50K	275K	1.6M	18
Entertainment	25	6.3K	151K	58K	764K	3.8M	11
Financial Services	209	1.0K	237K	39K	25.0M	49.5M	8
Gaming & Casino	5	76.3K	411K	284K	1.1M	2.1M	3
Healthcare	880	1.0K	82K	17K	7.1M	72.6M	16
Hospitality	51	6.2K	1.0M	65K	40.0M	51.7M	1
Manufacturing	238	1.1K	190K	44K	20.0M	45.3M	10
Media	15	4.5K	376K	105K	2.5M	5.6M	4
Nonprofit	189	1.2K	77K	30K	1.6M	14.6M	17
Professional Services	730	1.0K	245K	39K	120.2M	178.5M	7
Public Entity	85	1.6K	114K	57K	1.4M	9.7M	14
Restaurant	26	1.7K	62K	44K	367K	1.6M	19
Retail	249	1.7K	142K	53K	6.9M	35.3M	13
Technology	148	4.5K	280K	66K	7.4M	41.4M	6
Telecommunications	21	3.5K	346K	51K	2.3M	7.3M	5
Transportation	57	1.2K	434K	63K	17.5M	24.7M	2
Other	262	1.0K	85K	25K	4.9M	22.2M	15

*Ranking is based on Average Incident Cost

Table 7

Average Crisis Services Costs by Business Sector
SMEs – 2015-2019

Sector	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Education - All	60K	37K	9K	22K	146K	97K	10
Education - Higher Ed only	61K	57K	10K	28K	175K	121K	8
Energy	51K	4K		7K	65K	68K	14
Entertainment	92K	2K	57K	40K		98K	9
Financial Services	174K	18K	13K	22K	63K	164K	5
Gaming & Casino	361K	58K		31K		399K	1
Healthcare	37K	100K	70K	13K	115K	59K	16
Hospitality	150K	29K	26K	47K	28K	170K	4
Manufacturing	33K	9K	8K	18K	35K	48K	18
Media	50K	86K		58K	15K	90K	12
Nonprofit	66K	12K	5K	18K	37K	74K	13
Professional Services	34K	17K	10K	15K	63K	295K	2
Public Entity	47K	23K	19K	22K	88K	94K	11
Restaurant	28K	19K	10K	19K	85K	46K	19
Retail	106K	19K	13K	30K	117K	123K	7
Technology	67K	78K	48K	37K	43K	130K	6
Telecommunications	94K	22K	1K	222K	37K	254K	3
Transportation	65K	6K	3K	11K	87K	64K	15
Other	35K	21K	13K	10K	238K	49K	17

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

**Ranking is based on Average Total Crisis Services

Table 8

Large Companies

The Healthcare, Financial Services, Retail, and Education sectors account for approximately 80% of the Large Company claims in the dataset.

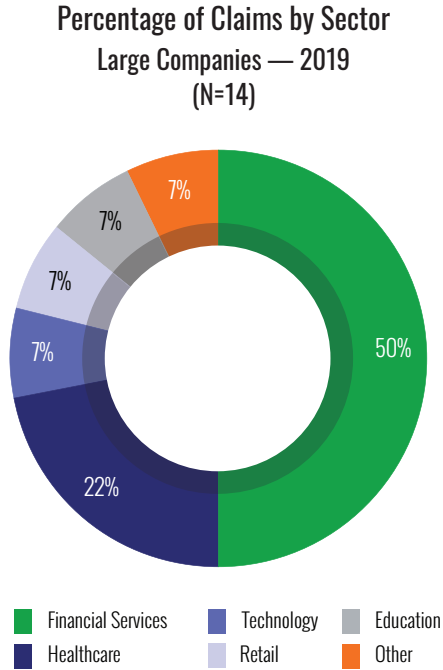


Figure 22

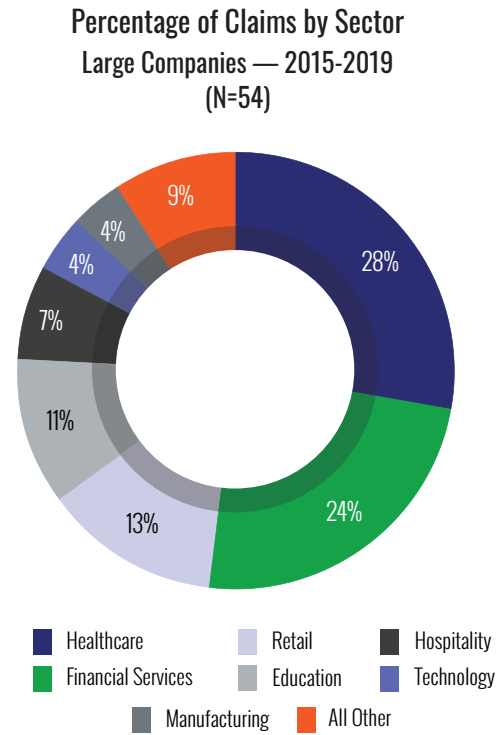


Figure 23

The tables below provide summary statistics for the Large Company sectors that have been analyzed for this year's report.

**Incident Cost by Business Sector
Large Companies – 2015-2019**

Sector	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Education - All	5	3K	225K	77K	875K	1.1M	11
Education - Higher Ed only	4	58K	280K	94K	875K	1.1M	10
Financial Services	9	6K	22.9M	12.5M	97.0M	206.0M	2
Healthcare	13	5K	4.2M	267K	15.0M	55.1M	5
Hospitality	4	738K	5.7M	6.0M	10.0M	22.7M	4
Manufacturing	2	20K	16.5M	16.5M	33.0M	33.0M	3
Public Entity	1	505K	505K	505K	505K	505K	8
Retail	6	60K	1.2M	478K	5.2M	7.1M	7
Technology	1	4.1M	4.1M	4.1M	4.1M	4.1M	6
Telecommunications	1	400K	400K	400K	400K	400K	9
Transportation	1	80.0M	80.0M	80.0M	80.0M	80.0M	1
Other	2	100K	130K	130K	159K	259K	12

*Ranking is based on Average Incident Cost

Table 9

**Average Crisis Services Costs by Business Sector
Large Companies – 2015-2019**

Sector	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Education - All	204K	60K	55K	33K		219K	8
Education - Higher Ed only	204K	60K	55K	40K		273K	7
Financial Services	2.4M	9.2M	13.0M	5.4M		8.6M	2
Healthcare	213K	6.2M	702K	124K		2.5M	4
Hospitality	280K		5.0M	866K		5.6M	3
Manufacturing	33.0M					33.0M	1
Public Entity							
Retail	1.7M			331K		1.3M	5
Technology	650K	0K		560K		605K	6
Telecommunications	18K	200K				218K	9
Other	105K	0K	39K	15K		159K	10

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

**Ranking is based on Average Total Crisis Services

Table 10

Cause of Loss

The claims in the dataset are classified by 24 distinct causes of loss.

SMEs

As the graphs below show, Ransomware and Social Engineering (BEC, Phishing, other kinds of Social Engineering) were the leading causes of loss for SMEs in 2019, and among the leaders for the five-year period of 2015-2019.

Surprisingly, during the past two years, there has been an increase in the frequency of staff mistakes of all kinds (improper handling and/or disposal of records, programming and configuration errors, and erroneous mailing and emailing of confidential records). Staff Mistakes are record less discussed in more detail in this section. Social Engineering and Ransomware are discussed later in the report in the section called "Taking a Closer Look at Growing Risks".

Percentage of Claims by Cause of Loss

SMEs — 2019
(N=855)

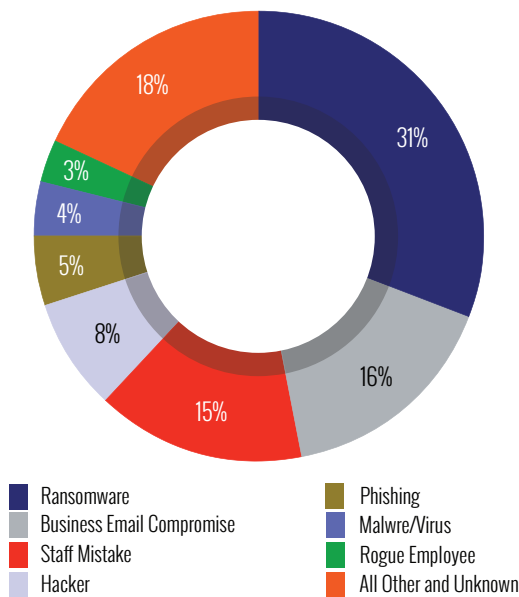


Figure 24

Percentage of Claims by Cause of Loss

SMEs — 2015-2019
(N=3,493)

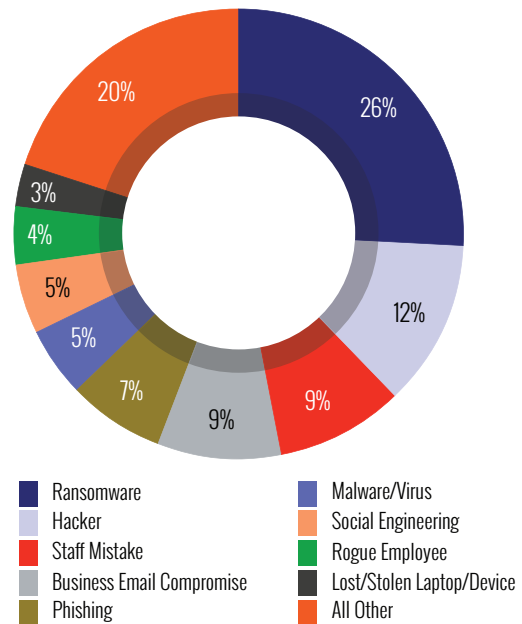


Figure 25

The following tables provide summary statistics for all the SME causes of loss that have been analyzed for this year's report.

Incident Cost by Cause of Loss
SMEs – 2015-2019

Cause	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Business Email Compromise	318	1K	132K	57K	3.4M	41.9M	9
Hacker	430	1K	634K	46K	120.2M	272.7M	2
Hacker/Malware/Virus combined	606	1K	493K	47K	120.2M	299.0M	3
Legal Action	56	3K	129K	61K	1.0M	7.2M	10
Lost/Stolen Laptop/Device combined	127	1K	50K	15K	1.5M	6.4M	17
Stolen Laptop/Device only	100	1K	50K	17K	1.5M	5.0M	18
Malware/Virus	176	1K	149K	50K	6.9M	26.3M	5
Negligence	5	5K	78K	100K	135K	389K	12
Paper Records	31	1K	47K	10K	650K	1.5M	19
Phishing	258	1K	69K	42K	666K	17.8M	15
Programming Error	20	2K	355K	52K	3.6M	7.1M	4
Ransomware	915	1K	143K	43K	20.0M	130.5M	7
Rogue Employee	161	0.1K	77K	10K	2.5M	12.3M	13
Social Engineering Combined	782	1K	102K	50K	3.4M	79.4M	11
Social Engineering (type unknown)	157	2K	71K	50K	325K	11.2M	14
Staff Mistake	344		17K	2K	779K	5.7M	23
System Glitch	12	2K	1.6M	45K	17.5M	19.4M	1
Theft of Money	10	1K	38K	40K	108K	381K	21
Third Party	15	4K	28K	17K	0.1M	0.4M	22
Trademark/Copyright Infringement	9	12K	149K	60K	468K	1.3M	6
Wire Transfer Fraud	191	1K	140K	82K	1.4M	26.8M	8
Wrongful Data Collection	2	5K	46K	46K	86K	91K	20
Other/Unknown	393	1K	56K	20K	2.8M	22.1M	16

*Ranking is based on Average Incident Cost

Table 11

Average Crisis Services Costs by Cause of Loss
SMEs – 2015-2019

Cause	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Business Email Compromise	44K	12K	14K	27K	70K	80K	7
Hacker	124K	108K	56K	32K	58K	506K	1
Hacker/Malware/Virus combined	120K	88K	48K	32K	78K	402K	2
Legal Action	23K	9K	1K	15K	67K	36K	19
Lost/Stolen Laptop/Device combined	24K	50K	14K	16K	51K	45K	15
Stolen Laptop/Device only	26K	53K	8K	16K	60K	45K	16
Malware/Virus	112K	20K	4K	33K	114K	142K	4
Negligence	6K	29K	1K	24K		44K	17
Paper Records	16K	11K	15K	14K	15K	22K	21
Phishing	43K	9K	18K	17K	24K	54K	11
Programming Error	57K	185K	133K	28K	7K	147K	3
Ransomware	37K	17K	23K	10K	92K	54K	12
Rogue Employee	57K	8K	4K	31K	13K	52K	13
Social Engineering Combined	42K	12K	16K	23K	91K	69K	9
Social Engineering (not specified)	20K	1K	1K	14K	44K	40K	18
Staff Mistake	40K	29K	15K	6K	4K	18K	22
System Glitch	68K	42K	2K	45K	100K	88K	6
Theft of Money	28K	2K	3K	29K	1K	49K	14
Third Party	23K	12K	26K	14K	1K	25K	20
Trademark/Copyright Infringement				91K		91K	5
Wire Transfer Fraud	29K	4K	7K	22K	115K	62K	10
Wrongful Data Collection				80K		80K	8
Other/Unknown	14K	3K	8K	8K	83K	17K	23

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

**Ranking is based on Average Total Crisis Services

Table 12

Large Companies

For Large Companies, the leading causes of loss were hackers, staff mistakes, malware/virus, and ransomware. Figure 26 shows the proportions of causes for the five-year period.⁴

When compared with the same causes of loss at SMEs, incidents at Large Companies were typically far more expensive. For example, Hacking incidents at Large Companies exposed an average of 84M records, with an average incident cost of nearly \$17M. Hacking incidents at SMEs exposed an average of 2M records with an average incident cost of \$616K. Even Staff Mistakes at Large Companies were over 10 times more costly than ones at SMEs.

The two tables below tell the story for Incident and Average Crisis Services Costs.

Percentage of Claims by Cause of Loss
Large Companies — 2015-2019
(N=54)

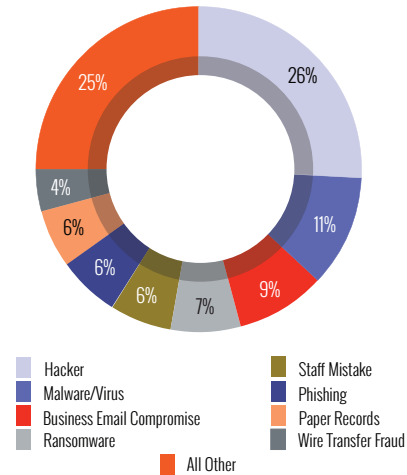


Figure 26

Incident Cost by Cause of Loss
Large Companies – 2015-2019

Cause	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Business Email Compromise (BEC)	5	77K	616K	530K	1.4M	3.1M	8
Hacker	14	60K	16.7M	8.0M	97.0M	233.4M	3
Hacker/Malware/Virus Combined	20	20K	12.1M	2.3M	97.0M	242.1M	4
Malware/Virus	6	20K	1.5M	719K	5.2M	8.7M	6
Paper Records	3	3K	36K	5K	100K	108K	14
Phishing	3	150K	190K	165K	255K	570K	12
Ransomware	4	12.8M	18.9M	15.0M	33.0M	75.8M	2
Rogue Employee	2	6K	2.1M	2.1M	4.1M	4.1M	5
Social Engineering	11	77K	522K	255K	1.5M	5.7M	9
Staff Mistake	3	250K	325K	250K	400K	650K	10
System Glitch	1	80.0M	80.0M	80.0M	80.0M	80.0M	1
Theft of Money	1	103K	103K	103K	103K	103K	13
Wire Transfer Fraud	2	505K	990K	990K	1.5M	2.0M	7
Wrongful Data Collection	1	249K	249K	249K	249K	249K	11

*Ranking is based on Average Incident Cost

Table 13

⁴ There was insufficient data to create a meaningful graph for 2019.

Average Crisis Services Costs by Cause of Loss
Large Companies – 2015-2019

Cause	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Business Email Compromise	203K	60K	47K	127K	1.0M	561K	6
Hacker	1.4M	10.9M	8.1M	4.3M	47K	9.8M	2
Hacker/Malware/Virus Combined	1.3M	10.9M	6.1M	2.4M	118K	7.2M	3
Malware/Virus	1.2M		3K	546K	189K	1.6M	4
Paper Records				3K		3K	12
Phishing		13K	104K	20K	8K	145K	10
Ransomware	33.0M	2.3M				17.6M	1
Rogue Employee	650K			283K		608K	5
Social Engineering	163K	37K	66K	94K	504K	396K	7
Staff Mistake	18K	200K				218K	8
Wire Transfer Fraud	44K			63K		107K	11
Wrongful Data Collection				199K		199K	9

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

**Ranking is based on Average Total Crisis Services

Table 14

Insider Involvement

During the five-year period, over 80% of incidents at both SMEs and Large Companies had no insider involvement. Malicious insider actions accounted for about 4.5% of claims at SMEs and 3.5% of claims at Large companies.

SME claims with unintentional insider involvement are less expensive than those overall. The average claim was \$64K and the median claim was \$7K. Sometimes, however, they can be expensive – the largest claim was over \$3M.

Malicious insider claims have been aggregated with rogue employee claims. For the analysis, please see the sections and tables for rogue employee above.

Third-Party Involvement

Very few claims in the dataset showed third-party involvement – less than 8% at SMEs and 4% at Large Companies. At SMEs, non-malicious third-party involvement accounted for 2% of claims. The average and median incident costs for these claims were relatively low: \$83K and \$21K, respectively.

Malicious third-part involvement accounted for 6% of claims at SMEs. The average and median incident costs for these claims were also relatively low: \$108K and \$53K, respectively.

The dataset contains only two claims with third-party involvement at Large Companies. One of these claims was small, less than \$5K, and one was quite large, over \$10M.

Staff Mistakes

At SMEs, staff mistakes accounted for 9% of claims. They were the third most frequent cause of loss. Fortunately, they tended to be inexpensive. During the five-year period, the average cost of a staff mistake incident was \$17K and the median was \$2K. The maximum incident cost was \$779K.

As the chart below shows, during the past two years there has been an increase in the frequency of staff mistakes of all kinds (improper handling and/or disposal of records, programming and configuration errors, and erroneous mailing and emailing of confidential records).

Claims for Staff Mistakes

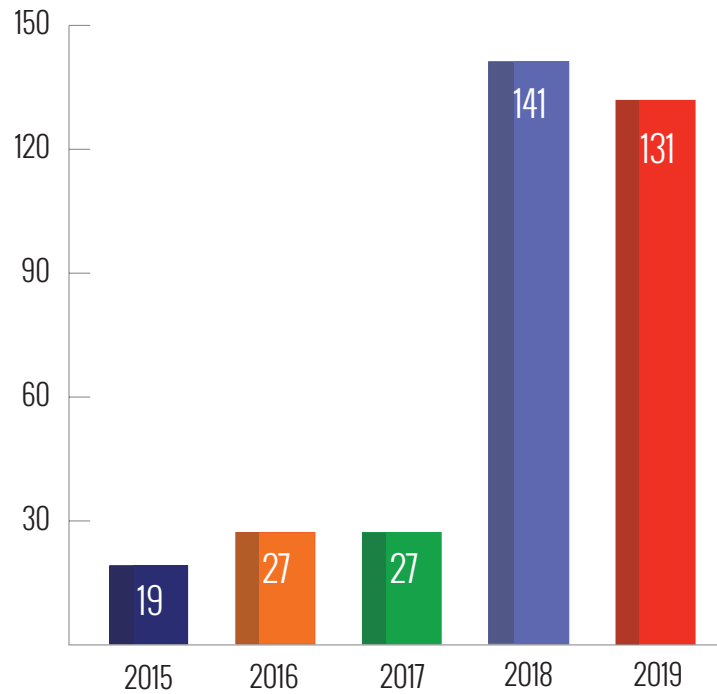


Figure 27

Staff mistakes were somewhat more prevalent at Large Companies, accounting for 14% of the claims over \$1K during the five-year period. All these claims involved inadvertent disclosures of information. They were also more costly. The average incident cost was \$250K, with a maximum incident cost of \$400K.

Costs for Staff Mistakes

Revenue Size	Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
SMEs	2019	Crisis Services	86	0.5K	3K	2K	22K
		Incident	89	1.0K	4K	2K	22K
	2015-2019	Crisis Services	221	0.1K	18K	3K	679K
		Incident	259	1.0K	22K	4K	779K
Large Companies	2019	Crisis Services	0				
		Incident	0				
	2015-2019	Crisis Services	1	218K	218K	218K	218K
		Incident	3	100K	250K	250K	400K

Table 15

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 on-card Financial, Other Non-Public, W-2 Specific, and Trade Secrets data.

Because a large percentage of incidents (ransomware, DDoS, and wire transfer fraud) do not expose records at all, two new categories were created in 2018 to capture these incidents. These categories are "Files-Critical" and "Files-Not Critical". An example of an incident with "Files-Critical" data would be a ransomware event that locked a database, system, or network deemed essential. A "Files-Not Critical" incident might involve a few desktop computers that could be restored or replaced without major impact.

The charts below depict the percentage of claims for each data type. The tables following provide summary statistics for Incident and Average Crisis Services Costs.

SMEs

Percentage of Claims by Type of Data

SMEs — 2019
(N=855)

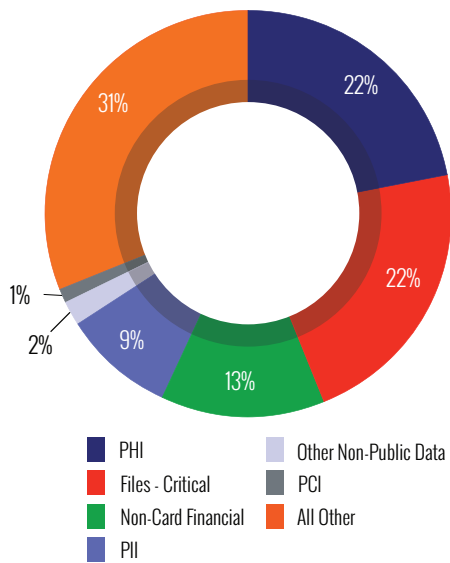


Figure 28

Percentage of Claims by Type of Data

SMEs — 2015-2019
(N=3,493)

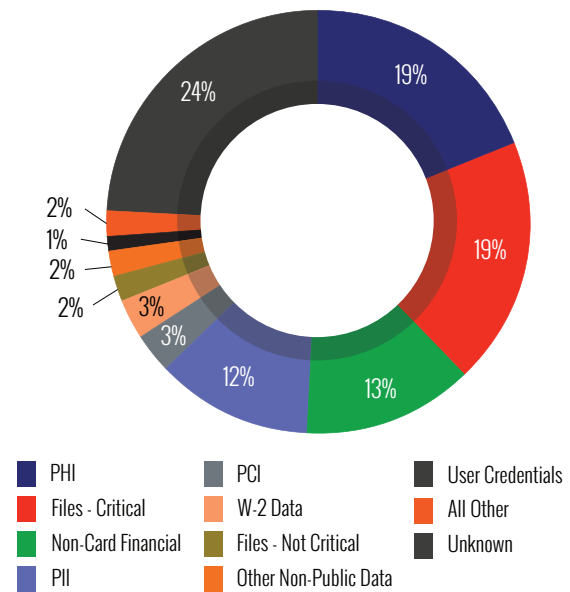


Figure 29

The following tables provide summary statistics for types of data involved in SME incidents that were analyzed for this year's report.

Incident Cost by Type of Data
SMEs – 2015-2019

Type of Data	Claims	Minimum	Average	Median	Maximum	Total	Rank*
DDoS	9	4K	283K	126K	1.6M	2.5M	4
Files - Critical	648	1K	220K	55K	20.0M	142.4M	6
Files - Not Critical	75	1K	32K	19K	183K	2.4M	15
Intellectual Property	20	3K	197K	60K	1.0M	3.9M	8
N/A	33	6K	75K	38K	800K	2.5M	10
Non-Card Financial	439	1K	372K	55K	120.2M	163.5M	2
Other Non-Public Data	72	3K	71K	33K	844K	5.1M	11
PCI	102	2K	570K	73K	25.0M	58.1M	1
PHI	582	1K	83K	10K	7.1M	48.2M	9
PII	426	1K	236K	48K	40.0M	100.5M	5
W-2 Data	100	1K	64K	39K	294K	6.4M	12
PII and W-2 Data Combined	526	1K	203K	47K	40.0M	106.9M	7
Trade Secrets	4	4K	59K	13K	208K	237K	13
User Credentials	45	4K	302K	108K	3.9M	13.6M	3
Unknown	798	1K	49K	25K	2.8M	39.1M	14

*Ranking is based on Average Incident Cost

Table 16

Average Crisis Services Costs by Type of Data
SMEs – 2015-2019

Type of Data	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
DDoS	274K	11K	5K	15K	51K	268K	3
Files - Critical	47K	24K	5K	14K	100K	70K	8
Files - Not Critical	32K	10K	50K	9K	16K	32K	14
Intellectual Property	65K			51K		58K	10
N/A	47K	24K	5K	14K	100K	70K	8
Non-Card Financial	27K	12K	5K	19K	107K	883K	1
Other Non-Public Data	30K	1K	1K	20K	13K	44K	13
PCI	436K	34K	13K	51K	164K	388K	2
PHI	55K	115K	68K	16K	146K	84K	7
PII	60K	23K	14K	34K	51K	93K	5
W-2 Data	43K	10K	29K	19K	9K	54K	12
PII and W-2 Data Combined	58K	20K	19K	31K	41K	85K	6
Trade Secrets	40K			54K		57K	11
User Credentials	72K	20K	14K	33K	44K	122K	4
Unknown	20K	10K	4K	7K	89K	21K	15

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

**Ranking is based on Average Total Crisis Services

Table 17

¹⁰ Social engineering as a cause of loss has been defined to include: social engineering, BEC, phishing, and wire transfer fraud.

Large Companies

Malicious actors focused on stealing PHI, PII, and PCI data. The average records exposed for these three were 56M, 11M, and 663K, respectively; the corresponding average Incident Costs were \$4.4M, \$16.2M, and \$2.4M.

Percentage of Claims by Type of Data
Large Companies — 2015-2019
(N=54)

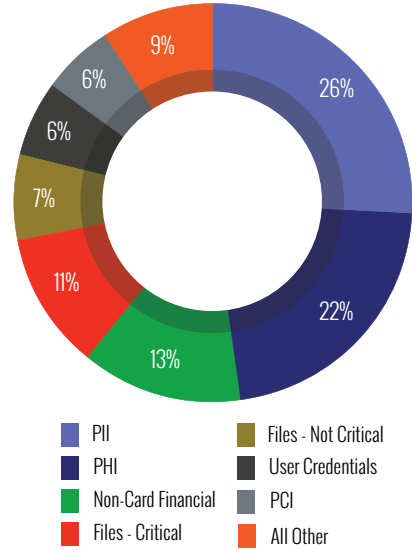


Figure 30

Incident Cost by Type of Data
Large Companies – 2015-2019

Type of Data	Claims	Minimum	Average	Median	Maximum	Total	Rank*
DDoS	1	60K	60K	60K	60K	60K	11
Files - Critical	6	58K	24.0M	7.9M	80.0M	143.8M	1
Files - Not Critical	2	3K	359K	359K	716K	719K	8
Non-Card Financial	6	103K	433K	203K	1.5M	2.6M	7
Other Non-Public Data	1	4.1M	4.1M	4.1M	4.1M	4.1M	5
PCI	3	20K	2.4M	2.0M	5.2M	7.2M	6
PHI	9	91K	4.4M	1.6M	15.0M	40.0M	4
PII	13	6K	16.2M	875K	97.0M	211.0M	2
W-2 Data	2	5K	85K	85K	165K	170K	10
PII and W-2 Data Combined	15	5K	14.1M	738K	97.0M	211.2M	3
User Credentials	2	77K	304K	304K	530K	607K	9

*Ranking is based on Average Incident Cost

Table 18

Average Crisis Services Costs by Type of Data
Large Companies – 2015-2019

Type of Data	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
DDoS	0K	0K	0K	0K	10K	10K	11
Files - Critical	11.1M	0K	0K	69K	200K	11.2M	1
Files - Not Critical	674K	0K	0K	7K	10K	349K	7
Non-Card Financial	62K	0K	0K	46K	0K	72K	10
Other Non-Public Data	650K	0K	0K	560K	0K	1.2M	6
PCI	4.0M	0K	0K	1.3M	184K	3.4M	4
PHI	195K	2.7M	1.3M	150K	560K	1.3M	5
PII	1.4M	9.6M	4.6M	4.2M	0K	10.1M	2
W-2 Data	0K	13K	104K	20K	8K	145K	9
PII and W-2 Data Combined	1.4M	7.7M	3.9M	3.5M	8K	9.2M	3
User Credentials	113K	0K	0K	191K	0K	202K	8

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

**Ranking is based on Average Total Crisis Services

Table 19



Taking a Closer Look at Growing Risks

Office Productivity Software Exploits

There are 67 office productivity-related claims in the five-year data. All were due to incidents that occurred at SMEs. These incidents were caused by exploits of Microsoft 365® (formerly called Office 365), Microsoft Outlook, and Microsoft SharePoint, as well as applications from PeopleSoft and Workday. Many of these incidents took place in cloud-based applications and infrastructure.

Criminals are attracted to these environments because one set of stolen admin-level credentials can provide access to an entire computing environment. There were victims of these exploits in almost every sector, with Professional Services (34%), Financial Services (16%), and Healthcare (10%) accounting for 60% of these claims.

Productivity Software

Revenue Size	Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
SMEs	2019	Crisis Services	12	20K	45K	29K	153K
		Incident	12	25K	61K	43K	153K
	2015-2019	Crisis Services	66	3K	111K	47K	1.3M
		Incident	68	3K	187K	58K	3.4M
Large Companies	2019	Crisis Services	0				
		Incident	0				
	2015-2019	Crisis Services	0				
		Incident	0				

Table 20

Cloud

For the past four years, study participants have been asked to note and describe any cloud-related factors involved in a claim. To date, 68 such events have been identified: 67 for SMEs and one for a Large Company.

At SMEs, cloud-related claims came from many business sectors, including Financial Services (24%), Professional Services (22%), Technology (12%), and Healthcare (10%). The majority (87%) of these claims were due to criminal acts. The primary criminal causes of loss were ransomware (27%), hackers (19%), BEC (19%), and malware/virus (10%). Non-criminal claims (13%) were caused by staff mistakes and programming errors.

Detailed descriptions of cloud-based incidents included Microsoft 365 attacks, user credential theft, hacking and data theft, and malware/viruses that exposed and/or exfiltrated data.

The claim for the Large Company involved the theft of user credentials to a cloud-based email server and cost \$530K.

Cloud

Revenue Size	Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
SMEs	2019	Crisis Services	15	2K	1.1M	60K	15.0M
		Incident	19	1K	1.6M	70K	25.0M
	2015-2019	Crisis Services	58	0.3K	371K	62K	15.0M
		Incident	67	1K	677K	80K	25.0M
Large Companies	2019	Crisis Services	1	530K	530K	530K	530K
		Incident	1	530K	530K	530K	530K
	2015-2019	Crisis Services	1	530K	530K	530K	530K
		Incident	1	530K	530K	530K	530K

Table 21

Internet of Things (IoT)

Since 2018, study participants have been asked to note if a claim involved IoT devices. The devices in these claims included cell phones, laptops, printers, and credit card terminals . After three years of asking this question, only 24 claims have been submitted for IoT-related events. All 24 incidents occurred at SMEs.

Retail, Manufacturing, Professional Services, Nonprofits, and Financial Services were the sectors with the largest numbers of claims. The leading causes of loss were BEC, Lost/Stolen Devices, Ransomware, and Malware/Viruses.

As the table below shows, IoT claims have not been extremely costly. The most expensive claim (\$130K) was due to BEC. The attack vector (the IoT device) was not specified.

Internet of Things (IoT)

Revenue Size	Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
SMEs	2019	Crisis Services	15	7K	30K	22K	90K
		Incident	19	8K	30K	22K	90K
	2015-2019	Crisis Services	58	6.6K	39K	31K	90K
		Incident	67	8K	44K	34K	90K
Large Companies	2019	Crisis Services	0				
		Incident	0				
	2015-2019	Crisis Services	0				
		Incident	0				

Table 22

Ransomware

Ransomware claims (N=920) account for over 25% of the claims in the dataset. All but four came from SMEs. The total cost for the four incidents at Large Companies was over \$15M.

SMEs

The number of ransomware claims has increased dramatically since 2015, from 19 in 2015 to 301 in 2018, and 263 in 2019. The ransom amounts have been increasing, as well. In 2018, the average ransom amount was \$72K. In 2019, it had increased to \$175K. In 2018, ransom amounts crossed the \$1M threshold for the first time. In 2019, they crossed the \$3M threshold.

Ransomware Overall SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Ransom	108	1K	175K	26K	3.7M
	Crisis Services	219	0.4K	80K	45K	2.5M
	Incident	263	1K	169K	60K	3.9M
2015-2019	Ransom	317	0.2K	81K	12K	3.7M
	Crisis Services	766	0.4K	54K	29K	2.5M
	Incident	915	1K	143K	43K	20.0M

Table 23

Ransom amount was reported for only about one-third of the claims (N=317). The analysis of these claims shows higher total incident costs than those overall (\$196K vs \$143K), and much higher incident costs in 2019 (\$275K vs \$169K).

Ransomware – Ransom Amount Known SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Ransom	108	1K	175K	26K	3.7M
	Crisis Services	96	2K	81K	52K	790K
	Incident	108	10K	275K	100K	3.9M
2015-2019	Amount	317	0.2K	81K	12K	3.7M
	Crisis Services	279	1K	58K	32K	911K
	Incident	317	3K	196K	61K	6.6M

Table 24

Ransoms were flagged as “not paid” in 64 claims. Organizations chose not to pay for a variety of reasons. Usually, but not always, recovery was possible from backups or from the reverse engineering of a decryption key. Sometimes, however, attempts at recovery from backups failed, resulting in an expensive data re-creation effort.

Organizations that chose not to pay the ransom experienced lower average Incident Costs both overall and in 2019. Since ransoms were not paid, the amount of ransom demanded was not usually provided.

Ransomware – Ransom Not Paid
SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Crisis Services	6	25K	88K	93K	157K
	Incident	6	23K	156K	118K	491K
2015-2019	Crisis Services	57	1K	54K	39K	295K
	Incident	64	3K	183K	44K	6.6M

Table 25

There were 121 ransomware claims during the five-year period and 22 claims in 2019 that had a Business Interruption (BI) cost element. In general, the costs of these incidents were much higher than those of overall ransomware incidents. In 2019, the average ransom demand for these kinds of incidents was \$453K, more than double the overall average demand for that year.

Ransomware – Incidents with Business Interruption Loss
SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Ransom	6	4K	453K	252K	1.5M
	Crisis Services	14	0.4K	93K	71K	304K
	Business Interruption	22	0.1K	215K	98K	1.7M
	Recovery Expense	4	2K	42K	33K	100K
	Incident	22	4K	373K	143K	2.9M
2015-2019	Ransom	38	0.3K	123K	22K	1.5M
	Crisis Services	87	0.4K	57K	31K	345K
	Business Interruption	121	0.1K	228K	28K	5.1M
	Recovery Expense	34	1K	58K	14K	500K
	Incident	121	4K	342K	85K	6.6M

Table 26

Almost half of the ransomware incidents occurred at organizations with less than \$50M in annual revenue. Assuming that most of the SMEs with unknown revenues were Nano-Rev organizations, the proportion is over 80%. The table below shows clearly that the average costs increased linearly given the size of the organization.

Ransomware by Revenue Size
SMEs

	Claims	Ransom Amount	Crisis Services	Total Incident Cost
Nano-Rev (<\$50M)	409	56K	55K	95K
Micro-Rev (\$50M-\$300M)	122	148K	106K	303K
Small-Rev (\$300M-\$2B)	27	499K	125K	733K
Unknown	356	23K	28K	98K

Table 27

Every business sector experienced ransomware incidents. The top 4, ranked by the number of claims, are show in table 27 below. The top 4, ranked by the average Incident Cost, are show in table 28. Though not listed, the Healthcare, Professional Services, and Financial Services sectors all experienced average Incident Costs that were <\$110K, putting them in the bottom half of all sectors.

Ransomware by Sector
Ranked by Number of Claims – Top 4
SMEs – 2015-2019

	Claims	Ransom Amount	Crisis Services	Total Incident Cost
Healthcare	312	26K	35K	107K
Professional Services	200	43K	50K	88K
Manufacturing	65	305K	47K	490K
Retail	50	82K	48K	130K

Table 28

Ransomware by Sector
Ranked by Average Incident Cost – Top 4
SMEs – 2015-2019

	Claims	Ransom Amount	Crisis Services	Total Incident Cost
Manufacturing	65	305K	47K	490K
Entertainment	2	152K	84K	480K
Technology	31	142K	94K	221K
Education	29	219K	83K	202K

Table 29

Social Engineering

Social Engineering was the second most frequent cause of loss in our analysis. As we wrote in the 2019 Cyber Claims Study, social engineering may be generally defined as "malicious action that causes a deviation from standard operating procedures or policies and subsequent losses by the organization." Very often, this was accomplished through highly-skilled persuasion by bad actors against organizational employees who failed to recognize such threats. Because social engineering, BEC, phishing, and banking fraud (including wire transfer and ACH) are categories with considerable potential overlap, data is provided for the combined categories, as well as BEC and banking fraud as separate categories.

Terms

Social Engineering

Malicious action that causes a deviation from standard operating procedures or policies and subsequent losses by the organization.

Business Email Compromise (BEC)

A well-researched, well crafted, highly personalized attack. Criminals invest considerable time and research into the wording and tone of fraudulent emails to obtain their desired outcomes.

Phishing

Indiscriminate and impersonal attacks and campaigns - mass emails sent in hope of snaring a small percentage of victims.

Banking Fraud

Almost always involves some type of social engineering, most typically BEC, but also phishing.

Social engineering can be accomplished by electronic means as well as face-to-face encounters. Examples include email solicitations, phone calls from a fake help desk, and the presentation of counterfeit credentials or badges to gain physical entry to a restricted space.

There were 785 claims caused by social engineering in the five-year period. Only three of these came from Large Companies. All three involved BEC, and two resulted in wire transfer fraud. The average Incident Cost was over \$700K and the highest cost was \$1.4M.

There were 782 social engineering incidents at SMEs: 318 involved BEC, 258 Phishing, and 143 unspecified social engineering. There were also 191 claims involving banking/ACH/wire transfer fraud, almost all of which had a social engineering/BEC attack vector.

From the data detailed below, it is clear that in 2019 fraud, crisis services, and total incident costs declined in virtually every category, when compared to the five-year averages.

Social Engineering Overall SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Crisis Services	85	0.1K	62K	27K	659K
	Incident	174	1K	88K	41K	2.3M
2015-2019	Crisis Services	408	0.1K	69K	32K	1.3M
	Incident	782	1K	102K	50K	3.4M

Table 30

Business Email Compromise (BEC)

SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Crisis Services	62	0.2K	72K	31K	659K
	Incident	133	1K	101K	47K	2.3M
2015-2019	Crisis Services	215	0.2K	81K	39K	1.3M
	Incident	318	1K	132K	57K	3.4M

Table 31

Phishing

SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Crisis Services	20	0.1K	33K	15K	153K
	Incident	37	1K	43K	19K	262K
2015-2019	Crisis Services	155	0.1K	54K	24K	641K
	Incident	258	1K	69K	42K	666K

Table 32

Banking/ACH/Wire Transfer Fraud

SMEs

Time Period	Nature of Cost	Claims	Minimum	Average	Median	Maximum
2019	Fraud Amount	82	1K	79K	50K	800K
	Crisis Services	25	0.2K	35K	24K	136K
	Incident	87	1K	85K	47K	800K
2015-2019	Fraud Amount	167	1K	125K	68K	1.0M
	Crisis Services	80	0.2K	62K	24K	479K
	Incident	191	1K	140K	82K	1.4M

Table 33



Conclusion

With this tenth edition of the *Cyber Claims Study*, NetDiligence continues to raise the bar for understanding and presenting comprehensive loss analysis for cyber insurers and other key stakeholders. For ten 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 – five years of claims data and more granular analysis, delving into more categorizations and details of the data. Over 1,600 new claims were submitted this year, a large increase over last year, and added to an existing dataset of almost 2,000 claims. The result is a comprehensive, representative, and objective dataset of cyber claims incidents, including their causes and monetary impacts, in existence.

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.

RSM

Cyberthreats continue to evolve, and companies must be prepared

COVID-19 demonstrates how quickly risks can change

As the NetDiligence report so clearly highlights, middle market companies have increasingly become the primary targets for cybercriminals, with an already high number of incidents rising incrementally each year. In fact, [the 2020 RSM US Middle Market Business Index Cybersecurity Special Report](#) found that 18% of middle market C-suite executives claimed that their company experienced a data breach in the last year, up from 15% in 2019.

For the second straight year, RSM's survey found that more than half of middle market executives surveyed indicated there will likely be an attempt to illegally access their organization's data in 2020. To put this in perspective, this only accounts for incident types that involve access to regulatory protected data. If other incident types such as ransomware and business email compromise (BEC) were taken into account, the percentages would be drastically higher.

At the same time, the RSM MMBI survey found that 95% of middle market executives claim that they are confident in their current security stance, a 2% increase from last year. Yet the NetDiligence and MMBI studies show that the midmarket has become the almost exclusive focus of many attackers, and the total number of attacks and damages continues to rise. Many C-level executives believe that the number of attacks directed toward them will increase, so it is difficult to understand how organizations' confidence in their security controls has only escalated year over year.

U.S. midmarket organizations appear to be falling into the subtle trap of the "bad things only happen to others" mindset. They see how much time, effort and money they spend on improving their security controls so they assume they must be more resilient. However, they do not take into account that attackers are constantly improving their skills as well, and the next wave of attacks always seems to be something that was unexpected and unaccounted for during the deployment of the new defenses. It is a traditional arms race that has yet to show any sign of slowing down.

Threats can pivot quickly, and middle market protective controls sometimes fail to keep up; early 2020 is a prime example of how quickly threats can change as bad actors take advantage of new

vulnerabilities. As COVID-19 spread across the world and became a global pandemic, cybercriminals deployed persistent campaigns that capitalized on the uncertainty and fear related to the coronavirus. In some cases, they took advantage of reduced cybersecurity measures because of the surge in employees working from home.

Lawmakers have warned that the coronavirus pandemic has made the United States more vulnerable than ever to a serious [cyberattack](#) due to the increased attention paid to that instead of cybersecurity. These vulnerabilities are especially relevant to the middle market, where protections are simply not able to reach the level of those used by government organizations or large international businesses. Threat actors are seeking attractive targets, and the reality is that nearly every company is at risk.

In the response to the COVID-19 pandemic, resources have shifted across the middle market, potentially taking attention away from security to focus on sustainability. In addition, employees using home networks can break the chain of security controls that have been developed within internal networks.

Phishing attempts represent the most prevalent method of attack during the COVID-19 pandemic. Emails are designed to look like they have guidance or advice from a company resource, or a legitimate organization, such as the World Health Organization or the Centers for Disease Control and Prevention. These messages attempt to coax recipients to click on a link or an attachment that launches malware to steal IDs and passwords that could lead to stolen company data.

Criminals have become very sophisticated, developing fake charities, and registering websites that seem closely aligned with COVID-19 news, relief or treatment. Their business is deception, and unfortunately, people will succumb to the tactics, especially in a time of crisis.

"Attackers will always try to utilize scenarios that will make it most likely that targets will interact with their malicious emails, and leveraging disasters has unfortunately been one of their preferred methods," said Daimon Geopfert, RSM principal and leader, national security, privacy and risk. "When people are stressed and afraid, they are not as likely to use critical

thinking, and this leads to a significantly increased failure rate of basic social engineering training where someone would ask 'do I know the sender?' or 'was I expecting this message.'"

These phishing scams are also leading to ransomware attacks, as attackers gain control of a company's network or steal company or customer records, and demand payment for their return.

Middle market companies are largely confident in their existing controls, likely because of increases in cyber insurance policies, training and dedicated resources to manage cybersecurity. But disaster responses are a unique scenario and often result in a new world of threats and demands on potentially strained resources. Even with a sharper focus on cybersecurity protections, it's difficult to stay ahead of threat actors.

The COVID-19 pandemic has caused several cybersecurity challenges; it emphasizes how quickly criminals can strike and adjust strategies to take

advantage of potential vulnerabilities. Middle market companies must be ready for any scenario by proactively communicating the risks, emphasizing where predators may be lurking and adjusting security policies as necessary—such as in remote working scenarios that may extend beyond the pandemic.

About RSM

RSM US LLP is the leading provider of audit, tax and consulting services focused on the middle market, with 13,000 people in 86 offices in the U.S. and Canada. It is a licensed CPA firm and the U.S. member of RSM International, a global network of independent audit, tax and consulting firms with more than 43,000 people in more than 120 countries. RSM uses its deep understanding of the needs and aspirations of clients to help them succeed. For more information visit <https://rsmus.com/>.





Experian®

COVID-19 has accelerated trends in the data breach industry amidst fast-tracking trends in the economy.

Without question, the coronavirus crisis has hastened economic trends. Many businesses and industries have slowed down, while others have shuttered altogether. On the home front, work-from-home orders and lockdowns have significantly boosted e-commerce and digital payments, and shoppers continue to shop online as a safety measure. The pandemic has also created an opportunity for cybercrime, including data theft and identity fraud, with cybercriminals exploiting easy access to crucial consumer information on the dark web.

The amount of data at risk is more significant than ever, with millions of students logging on to school and employees accessing company-issued devices, videoconferencing, and other collaboration tools. Then, there are the vulnerabilities of established cybersecurity challenges, such as employees opting not to use VPN software, downloading consumer-facing networks, and engaging in other behaviors to maximize their data and system experiences that could pose security risks. Once people sign off from their work-from-home responsibilities, they again turn to the internet to shop, socialize, and stream entertainment, presenting increased security concerns, such as phishing and malware.

All of this activity has resulted in telling cybercrime trends. According to industry sources, the first nine months of 2020 saw a reported 30% decrease in data breaches than in 2019. However, that doesn't necessarily correlate to fewer breaches. Despite this trending data, Experian is on track for another record year of breaches ahead with over 5,100 events creating demand for Experian's data breach resolution services. The pandemic pulled attention and resources elsewhere, and the actual number could be similar to prior years, even if there have been delays in discovery and reporting. What's more, the number of records exposed in the first six months of 2020, were reportedly more than double the billions of records exposed during 2019. The vast majority of these exposed records came from three data breaches, but even if you set those larger events aside, the average number of records exposed per breach increases. The net: the amount of at-risk data is greater as previously compromised information lead to ransomware, phishing, and brute force attacks.

COVID's Impact on Data Breaches

In addition to data theft and compromise trends, the pandemic has also inadvertently fast-tracked lessons in data breach response, especially the connection between faster response, spread prevention and increased containment. If there is a common theme emerging from the pandemic, it's this: Countries that respond earlier and aggressively experience better responses. Another lesson that's emerged: the importance of practicing. It's been reported that a U.S. pandemic playbook was created by the previous government administration but was discontinued and defunded. One could argue that if the U.S. had drilled down on logistics and distribution, it could have identified opportunities for improvement in its supply chain. Currently, we still see insufficiencies in supply chain SLAs, surging demand for test kits, uncertain impact with no guarantee or turnaround, and conflicting timelines on when the vaccine will be widely-available in distribution.

Don't Fail Your Response

The pandemic response has revealed lessons in why responses fail.

- **Lesson #1:** Not budgeting leads to poor results. Like the pandemic, many companies and security teams don't have a budget in place for a consumer response plan.
- **Lesson #2:** Planning alone is insufficient. Even the best plans could fail if they are not put through the paces. To fully prepare for an incident, companies should undergo drills and live event simulations. This will confirm that their breach plan is free of gaps, their technology is ready for high traffic, and their teams align on critical issues, including consumer-facing communications.
- **Lesson #3:** No sense of impact or wave estimate. Many companies believe their chances of being impacted by a data breach are slim. The reality and certainty of a data breach should be every security executive's priority. Knowing the maximum number of data records and consumers that could be breached is key. Also, it is crucial to guarantee infrastructure and staff expected to service

customers with SLAs. Do you have dedicated resources on-deck to quickly notify the public and the appropriate call center capabilities to accommodate consumer demand?

- **Lesson #4:** Timely response is critical. Data breaches create havoc well beyond the initial intrusion. Failing to respond quickly and appropriately can cause significant damage, including brand harm, customer migration, regulatory scrutiny, fines, class-action lawsuits, and executive termination.

Customers don't want to hear that their PII was part of a data breach, but how you respond can avoid customer flight if it does happen. Experian's 2019 Data Breach Consumer Survey Report revealed that if customers are breached, they want to know about it quickly – within 24 hours if the data breach was financial-related. The only way to respond that quickly is to have a response plan in place.

To help businesses minimize the severe consequences of a data breach, Experian® Reserved Response was developed to help businesses minimize the severe consequences of a data breach. Our solution makes it possible for clients to build, practice, and simulate a comprehensive breach response plan and guarantees—with service-level agreements—the quality of response, assistance from an experienced workforce, infrastructure, and quick dissemination of notifications to affected parties. Experian® Reserved Response can be an indispensable resource. With identity theft resolution agents, clients get access to a team of industry experts to help them navigate identity theft insurance claims, canceling bank accounts, updating medical records, and more.

With Experian® Reserved Response, cyber insurers can realize 25-35% lower notification, call center, and identity theft protection costs. Here's what else you should know:

- **Coverage counts:** 100% of Experian® Reserved Response clients have cyber insurance
- **Proven track record:** We have never missed an SLA for Experian® Reserved Response clients
- **Proactive results:** Over the last five years, Experian® Reserved Response clients experience 15% fewer notifiable data breach events versus Emergency Response clients

A proper and proactive breach plan response is critical, especially in our current environment.

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 seventeen 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.



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 a variety of consultant-led assessments that are tailored to meet the unique needs of small, medium, and large organizations in all business sectors.

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. NetDiligence also offers a variety of virtual programs that are free of charge to attendees and qualify for CE/CLE credits.

Contact Us

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

NetDiligence®

About the Study

Contributors

Risk Centric Security, Inc.

A special thank you also goes to Heather Goodnight-Hoffmann, cofounder and President, and Patrick Florer, cofounder and Chief Technology Officer of Risk Centric Security, who performed the data collection and data analysis, and provided material support in the writing and editing of the report. Risk Centric Security offers research, analysis, and reporting services, as well as state-of-the-art quantitative risk analysis and training for risk and decision analysis. For more information, visit www.riskcentricsecurity.com.

Other

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

- Heather Osborne – Director of Global Events & Programming, NetDiligence
- Sharon Lyon – Publisher, NetDiligence

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

Methodology

For this study, we invited the major underwriters and carriers of cyber liability insurance to submit claims information based on the following criteria:

- The incident occurred in 2017, 2018, or 2019.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to 137 individuals at 81 organizations in the United States, Canada and the United Kingdom. From this group, 18 individuals representing 16 organizations provided 1,663 analyzable new claims, using the proprietary NetDiligence® claims data collection worksheet.

The 2020 report also includes data from NetDiligence® studies published in 2015-2018, representing 1,914 incidents that occurred in 2015, 2016, 2017 and 2018. After the elimination of claims that

were less than \$1,000, the combined dataset included 3,399 incidents, each one, a data Incident insurance claim. This number represents a 75% increase in the number of claims analyzed compared to last year.

There are 3,488 claims in the dataset from American organizations, 11 claims from Canadian organizations, and 26 claims from organizations in the United Kingdom. There are also a small number of claims from organizations in Australia, Germany, Ireland, South Africa, and organizations with a global footprint (less than 4 each). The country was not specified in 11 claims.

When factoring in SIRs, we were able to calculate total data Incident Costs to date for all 3,499 (100%) of the analyzable claims in the dataset. In addition, 905 claims (26%) specified the number of records exposed and 2,311 claims (66%) included an accounting of Crisis Services Costs. The number of claims reporting records has not increased greatly since last year due to the large number of claims for incidents that do not expose records (ransomware, social engineering, BEC, etc.)

We calculated Per Record costs for all claims where the number of records exposed was provided (N=905). We made separate calculations for SMEs (less than \$2B in annual revenues) and Large Companies (greater than \$2B in annual revenues). For each group, we calculated the average and median Per Record costs for 100%, 95%, 90% and 80% of claims, discarding outliers from the bottom and top 2.5%, 5%, and 10% of the ranked data. The results of these calculations can be found in Table 1 (above).

3,062 (86%) of the claims in the dataset were flagged as closed, 466 (13%) as open and 19 (1%) as unknown claim status. 1,942 (55%) of the claims were for primary coverage, 31 (1%) for excess coverage and 1,574 (44%) had an unknown, but most likely primary coverage level.

There were 1,069 claims in the dataset for which the revenue size of the organization was unknown. After comparing the distribution of their incident costs to those of SMEs and Large Companies, the decision was made to include these claims in SME group.

Readers should keep in mind the following:

- Our sampling, although large, is a subset of all incidents. Some of the data points are lower than other studies because we focus on claims payouts and total costs for specific incident-related expenses and do not factor in other financial impact, including in-house investigation and administrative expenses, customer defections, opportunity loss, etc.

- There is no attempt here to consider whether claims associated with the same incident appear more than once in the data set. Given the fact that claims are anonymized when they are sent to us, there is no possible way for us to know this. We believe that the number of duplicated claims, though not zero, is very small.
- We are not privy to the terms of the cyber insurance policies governing the claims provided to us. Apart from SIR, we have no insight into specific exclusions, limits, or sub-limits that might be involved. For this reason, the reader is advised to consider the costs reported as a lower bound – i.e., we know that a given Incident has costs at least \$X, but cannot say how much more than this amount.
- 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 \$15 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 13% of the claims submitted for this study remain ‘open’. Therefore, aggregate costs as presented in this study include “payouts to-date” and “incident costs to-date”. It is virtually certain that additional payouts will be made on some of the claims in the dataset and therefore the costs in this study are almost certainly understated.

