NetDiligence®

CYBER CLAIMS STUDY
2019 REPORT

OUR SPONSORS

RSM

COZEN O'CONNOR

Contents

Introduction 1

Key Findings 2

Terms 2

An Overview of the Data 6

The Insureds—Who Are They? 6

Distribution of Claims by Year of Event 6

Exposed Records 6

Breach Costs 7

Crisis Services Costs 8

Legal Defense and Settlement Costs 9

Regulatory Defense and Fines 10

PCI Fines 11

Lost Business Income and Recovery Expense 11

Per-Record Cost 12

Recordless Claims versus Claims with Exposed Records 13

A Word about Self-Insured Retentions (SIRs) 15

Taking a Closer Look at the Data 16

Crisis Services Costs by Category 16

Forensics 17

Credit/ID Monitoring 17

Notification 18

Breach Coach (Legal Guidance) 18

Other Crisis Services 18

Business Sector 19
SMEs 19
Large Companies 22
Revenue Size 25
Cause of Loss 27
SMEs 27
Large Companies 30
Criminal vs Non-Criminal Activities 32
Social Engineering, Business Email Compromise (BEC), Phishing, and Banking Fraud 34
Ransomware 36
Hacking and Malware/Virus 37
Rogue Employees and Malicious Insiders 38
Lost and Stolen Devices 38
W-2 Fraud 40
Banking Fraud 41
Distributed Denial of Service (DDoS) Attacks 41
Office Productivity Software Exploits 42
Losses Due to Non-Criminal Factors 43
Type of Data 46
SMEs 46
Large Companies 49
Personally Identifiable Information (PII) 50
Protected Health Information (PHI) 50
Payment Card Information (PCI) 51
Files–Critical & DDoS 51
Files–Not Critical 52
Non-Card Financial 52
Other Non-Public Data 53
Insider Involvement 54
Third Parties 55
Cloud 57
Internet of Things (IoT) 57

Conclusion 58

Insurance Industry Participants 59

Contributors 59

Sponsor – RSM US 60

Growing Confidence Conflicts with Rising Cyber Concerns 60

Sponsor – Cozen O'Connor 61

Cybersecurity Risk in the World of the Internet of Things 61

About NetDiligence® 62

Study Methodology 63

Introduction

Welcome to the ninth edition of the NetDiligence® *Cyber Claims Study*. This study, based on over 2,000 cyber claims, provides a comprehensive view of recent cyber claim events.

By the Numbers

- 2,081 claims analyzed, arising from events that occurred during 2014-2018
- 649 claims analyzed arising from events occurring in 2018
- Almost 1,100 new claims collected in 2018, from events occurring from 2016-2018
- 96% of claims ($357M in total) from small to medium enterprises (SMEs), i.e., organizations with less than $2 billion in annual revenue
- 4% of claims ($433M in total) from large companies, i.e., organizations with greater than $2B in annual revenue

The data from these claims has been aggregated in over 20 ways, including:

Totals, Averages, and Medians

- Breach costs
- Crisis services costs
- Legal and regulatory costs
- Per-record costs

Nature of Events

- Type of data exposed
- Business sectors affected
- Revenue size of claimants
- Causes of loss

Financial Impact of Cybercrimes

- Business interruption
- Malicious insiders
- Social engineering
- Ransomware

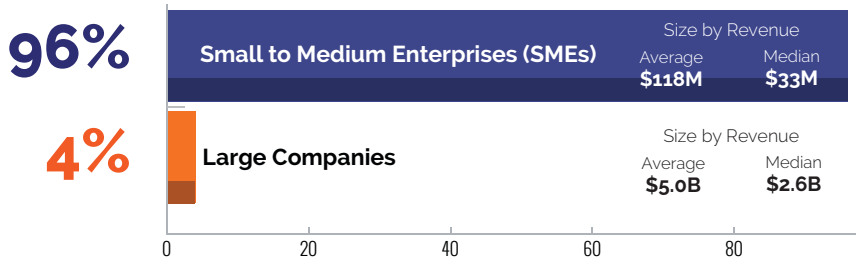
To present more accurate pictures of the business impact of cyber events on smaller versus larger organizations, findings for SMEs are often presented separately from findings for large companies.

Preliminary Observations

- As has been the case since the first *Cyber Claims Study* was published nine years ago, there are enormous variances in the data. The smallest claims are approximately $1,000 and the largest are $80M. The numbers of records exposed range from 1 to over 300M, and the overall per-record costs range from less than $0.01 to over $1.5M.
- In almost every category of the analysis, there are large variances between the average (mean) and median values. These variances are due to a small number of very large events in the dataset.
- There are often dramatic differences between the numbers for SMEs and large companies – multiples of 10x, 50x, or more. The largest company in the dataset (over $100B in annual revenue) is approximately 400,000 times larger than the smallest organization ($275K in annual revenue). The average large company in the dataset ($5B in annual revenues) is more than 40 times bigger than the average SME ($118M).
- The reverse is also true: sometimes a smaller company will have a very expensive claim and a large company will have a very small claim.

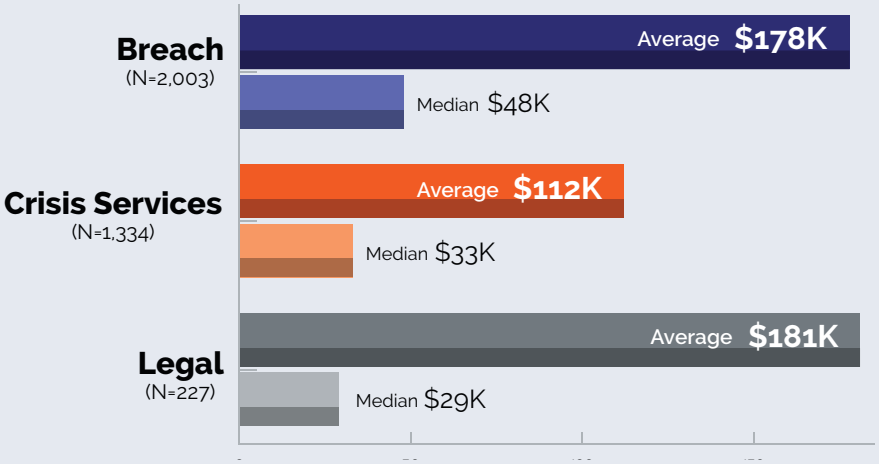
Key Findings[1]

Company Size

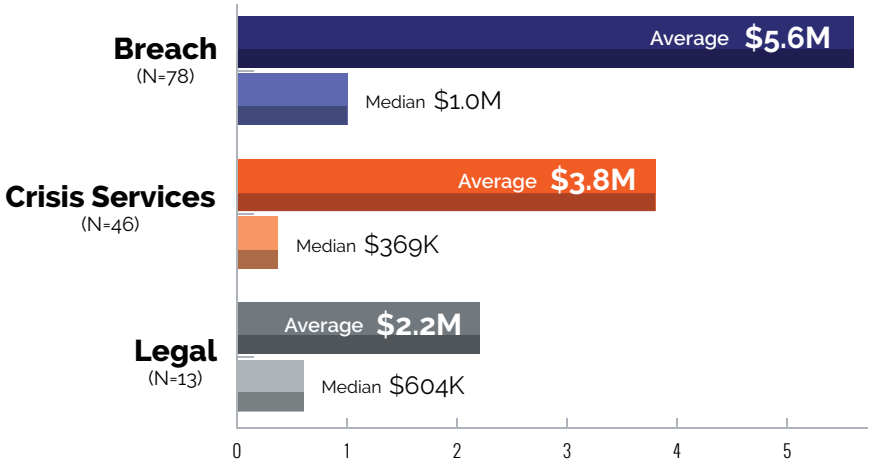


Costs

SMEs



Large Companies



Terms

Breach Coach®[2]

A qualified data security and privacy attorney who provides legal guidance for cyber incident response.

Breach Costs

All costs associated with the event that were reported by the insurer.

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

Regulatory and legal 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

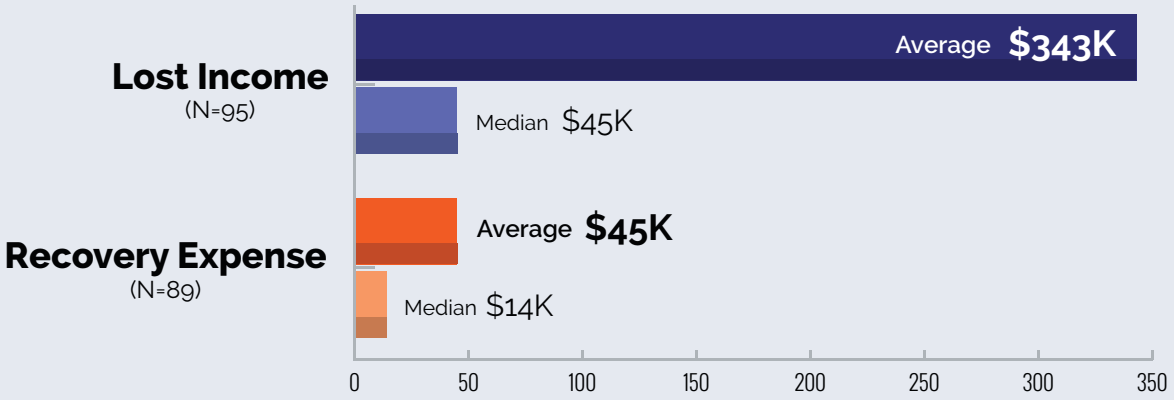
Categorized in this study as organizations with $2 billion or more in annual revenue.

[1] All findings are for the five-year period 2014-2018, unless otherwise noted

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

Business Interruption

SMEs



Records

Records Exposed

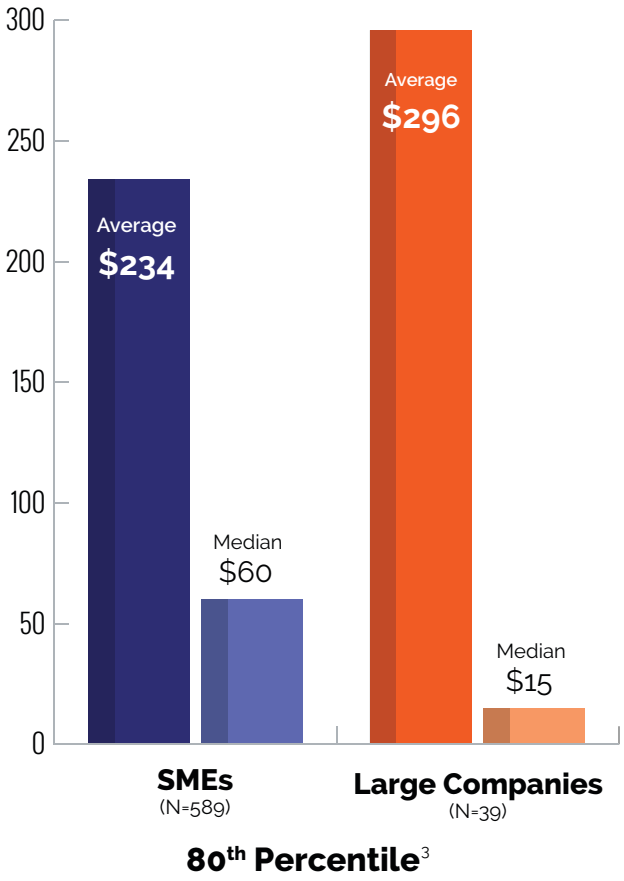
SMEs
(N=737)

Average
280K
Median
600

Large Companies
(N=50)

Average
19.6M
Median
48K

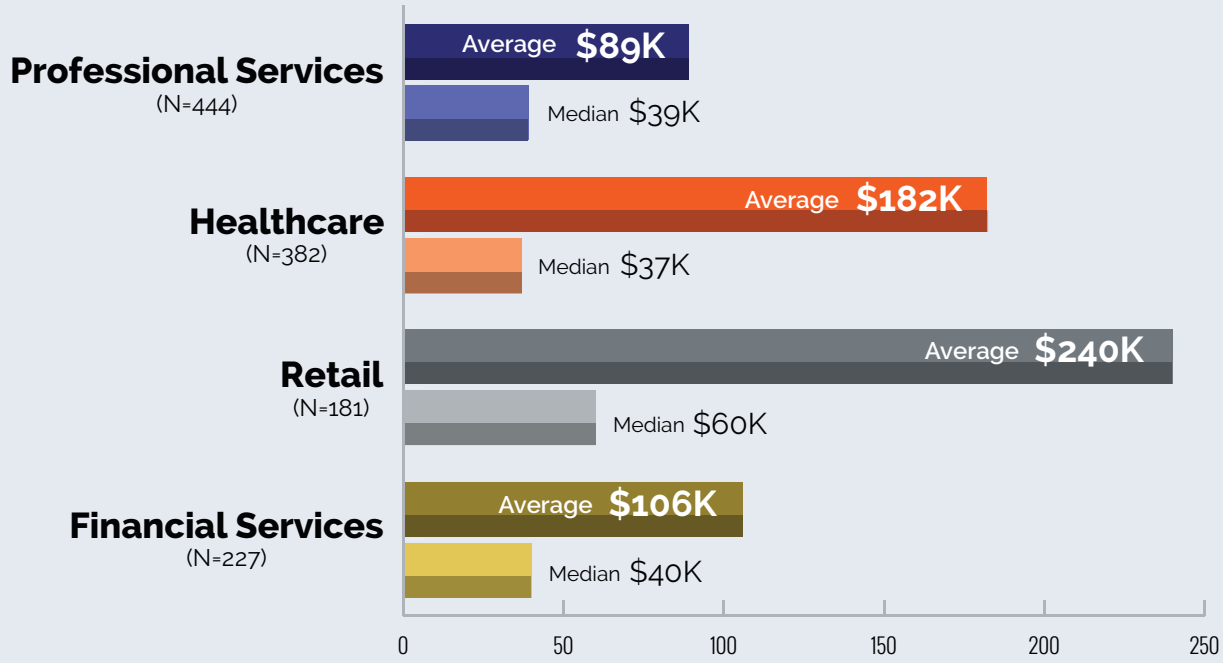
Per-Record Costs



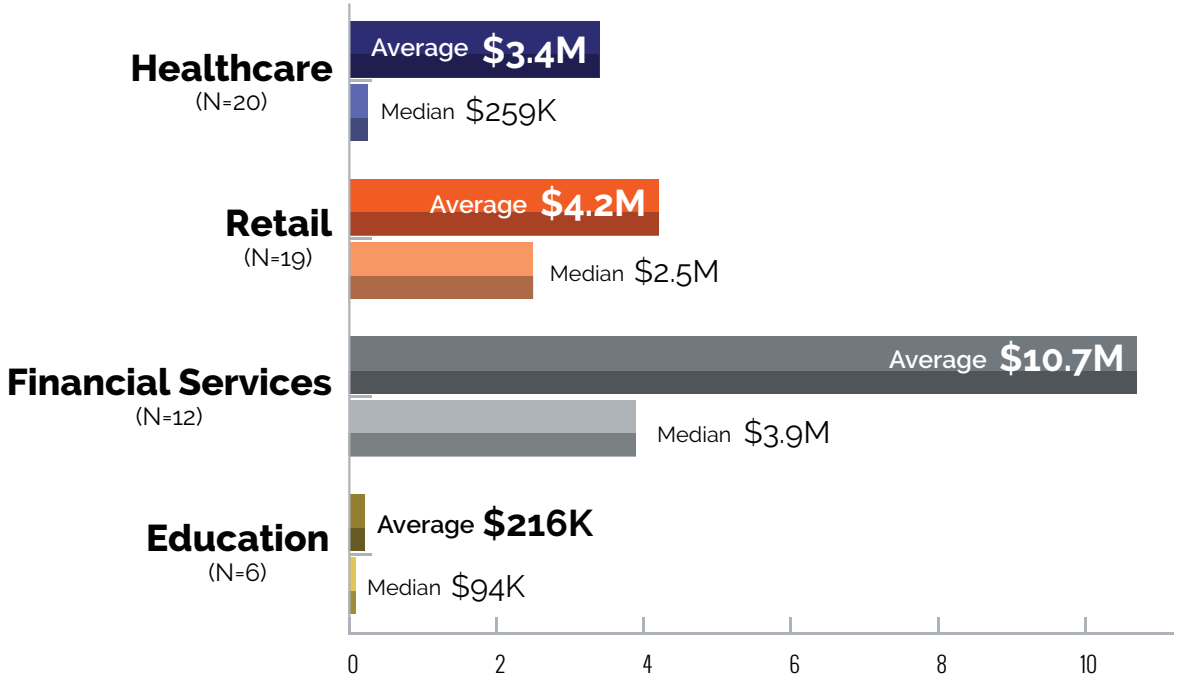
[3] 80% of events (eliminating bottom and top 10%)

Business Sector

SMEs

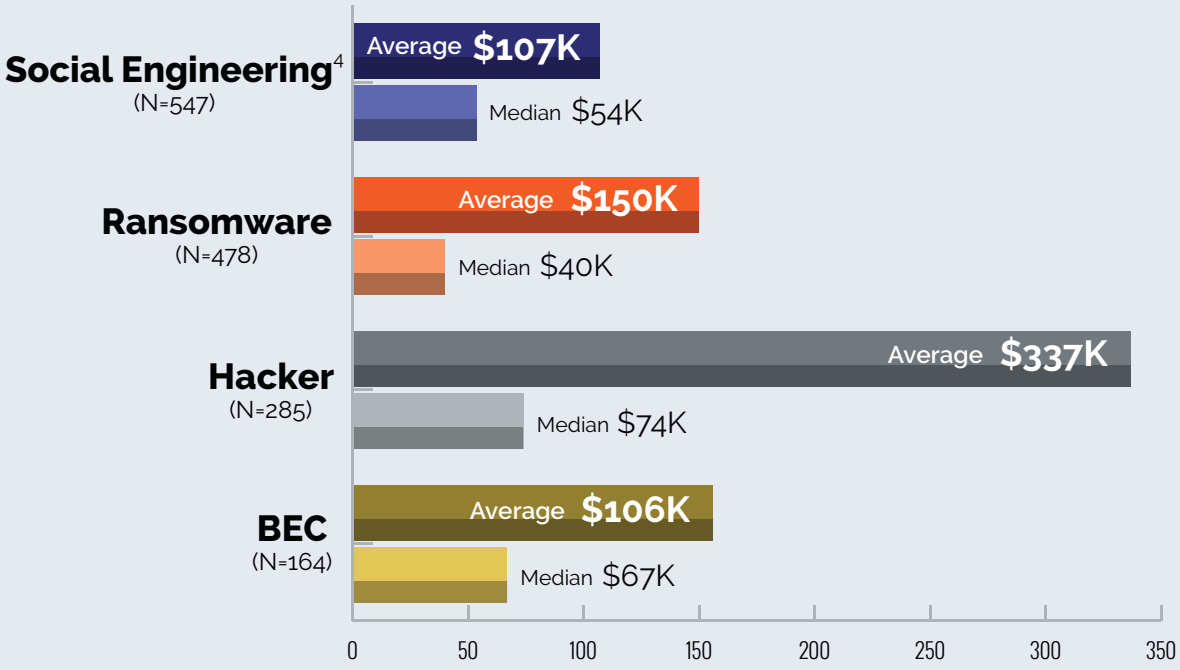


Large Companies

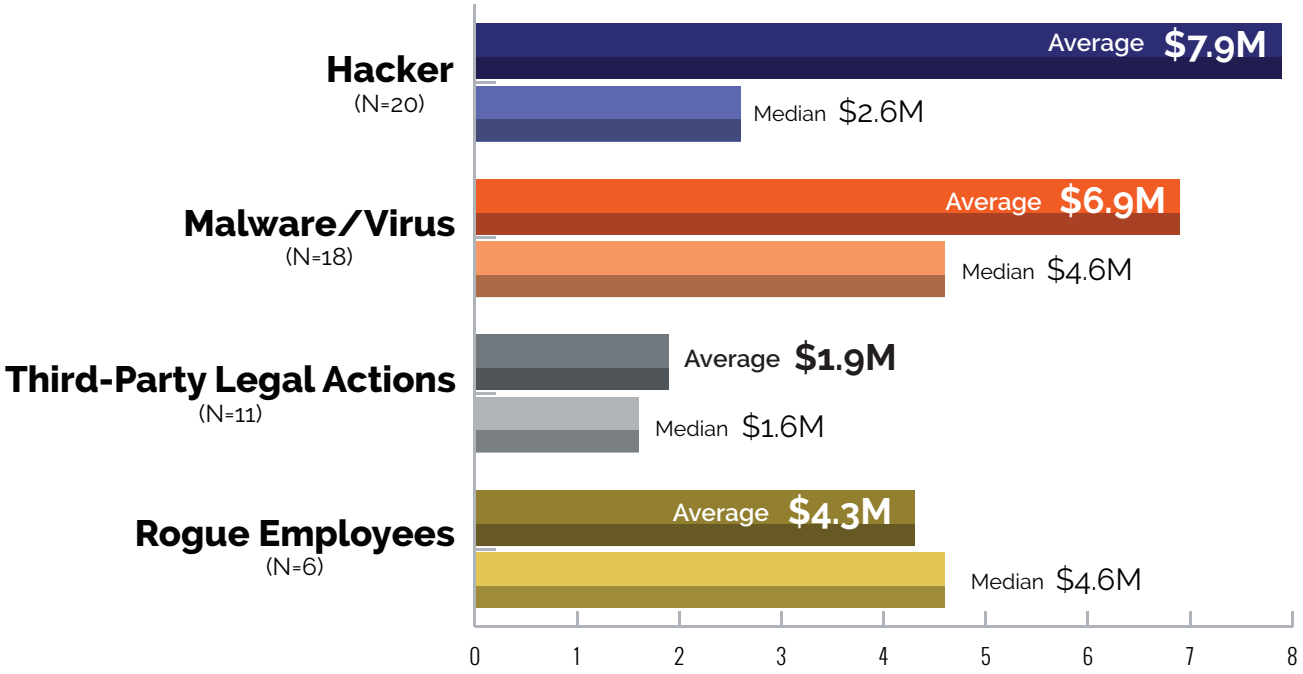


Cause of Loss

SMEs



Large Companies



[4] Social engineering includes social engineering, business email compromise, phishing, and wire transfer fraud

An Overview of the Data

The Insureds—Who Are They?

The claims analyzed in this study come from companies of all sizes – the smallest with less than $300K in annual revenue and the largest with over $100B in annual revenue.

For the first time, study participants provided estimates of the annual revenue of the insured companies. After the initial data analysis, the opportunity to divide the dataset into two categories became clear. Organizations with less than $2B in annual revenue were classified as small to medium enterprises (SMEs), while those with greater than $2B in annual revenue were classified as large companies.

Analysis of this data provides the following company demographics:

- SMEs: annual revenue ranged from $275K to $1.9B. The average was $118M; the median was $33M.
- Large Companies: annual revenue ranged from $2B to more than $100B. The average was $5B; the median was $2.6B.

These companies represent over 18 business sectors. The top 4 sectors as defined by number of claims were:

- Professional Services
- Healthcare
- Retail
- Financial Services

Additional analysis by business sector and revenue size appear later in this report.

Distribution of Claims by Year of Event

For this report, 2,081 cyber claims for events that occurred from 2014-2018 were analyzed. 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 197 in 2014 to over 600 in both 2017 and 2018.[5]

Percentage of Claims by Date of Event
2014-2018

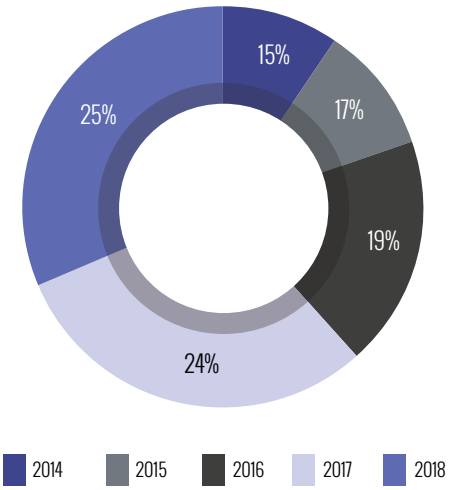


Figure 1

Exposed Records

Of the 2,081 claims in the dataset, 787 were for events that constituted some form of a data privacy breach, and thus exposed records. The total number of records exposed in these events was 1.2 billion. The numbers of records exposed per claim ranged from a single record to over 300 million. Events at SMEs accounted for 737 of these claims and 207 million records. Events at large companies accounted for 50 claims and almost 1 billion records.

The average number of records exposed varies substantially from year to year for both SMEs and large companies. This is primarily because mega-breaches, which drive up the averages, do not necessarily occur every year. In 2018, events at both SMEs and large companies had far greater numbers of records exposed than in each of the four prior years.

As Figure 2 makes clear, the average and median number of records exposed are dramatically different for SMEs and large companies. For the five-year period, events at large companies, on average, had 70 times more records exposed than events at SMEs.

[5] New claims are collected for events that occurred during the previous three years. For the 2019 study, these were events from 2016, 2017, and 2018.

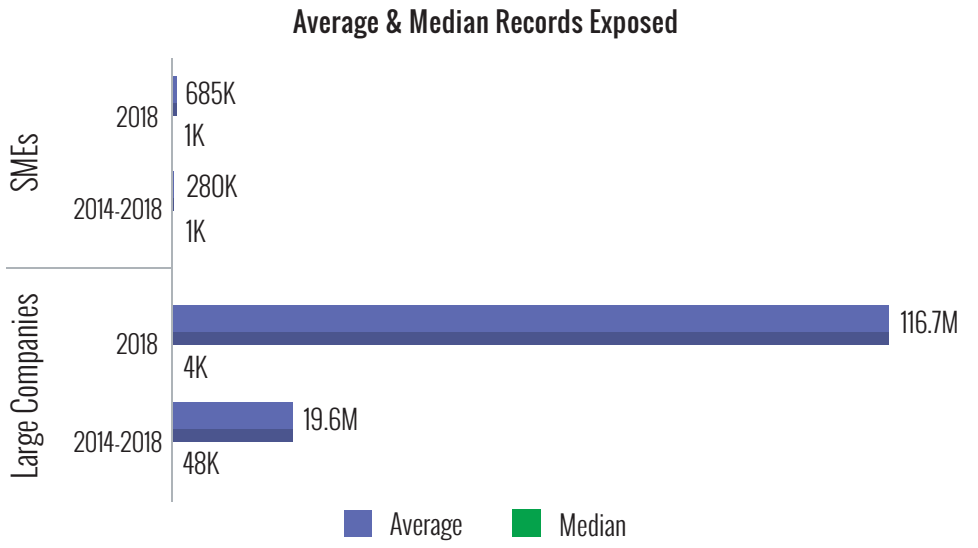


Figure 2

Breach Costs

Total Breach Costs, inclusive of Self-Insured Retention (SIR), ranged from a low of $1,000[6] to a high of $80M. Figure 3 depicts 2018 and five-year (2014-2018) total Breach Costs for SMEs and large companies. Figure 4 depicts the average and median Breach Costs.

Note that 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. For SMEs, the average and median five-year Breach Costs were $178K and $48K, respectively. For large companies, the five-year numbers were $5.6M and $1M.

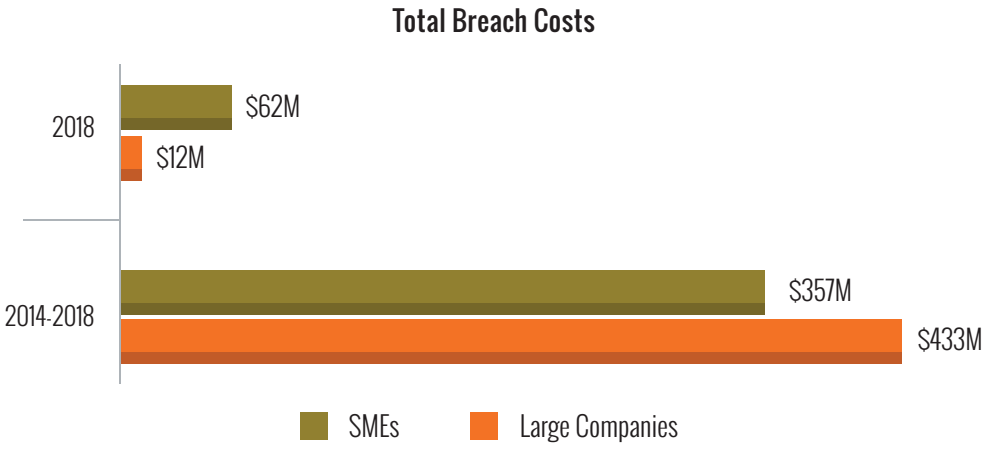


Figure 3

[6] A few claims for less than $1K were excluded from the analysis.

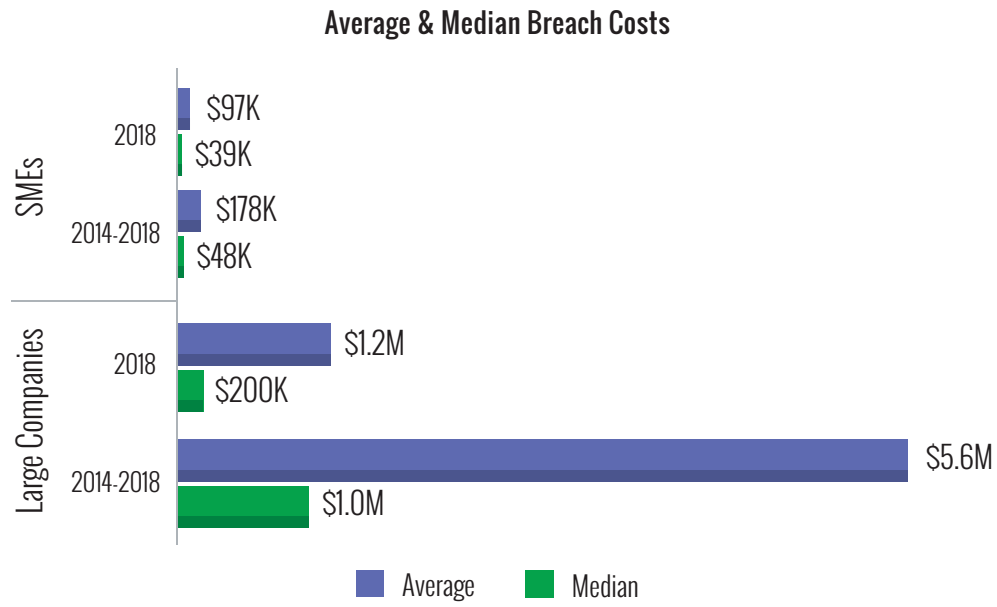


Figure 4

Crisis Services Costs

For the five-year period, Crisis Services Costs overall ranged from less than $100 to $64M per claim. In 2018, Crisis Services Costs ranged from $500 to $10M. For SMEs, the 2018 numbers were $500 to $1.3M and the five-year numbers were less than $100 to $8.2M. For large companies, the 2018 numbers were $58K to $10M and the five-year numbers were $2.6K to $64M. Figure 5 shows the average and median Crisis Services Costs for SMEs and large companies.

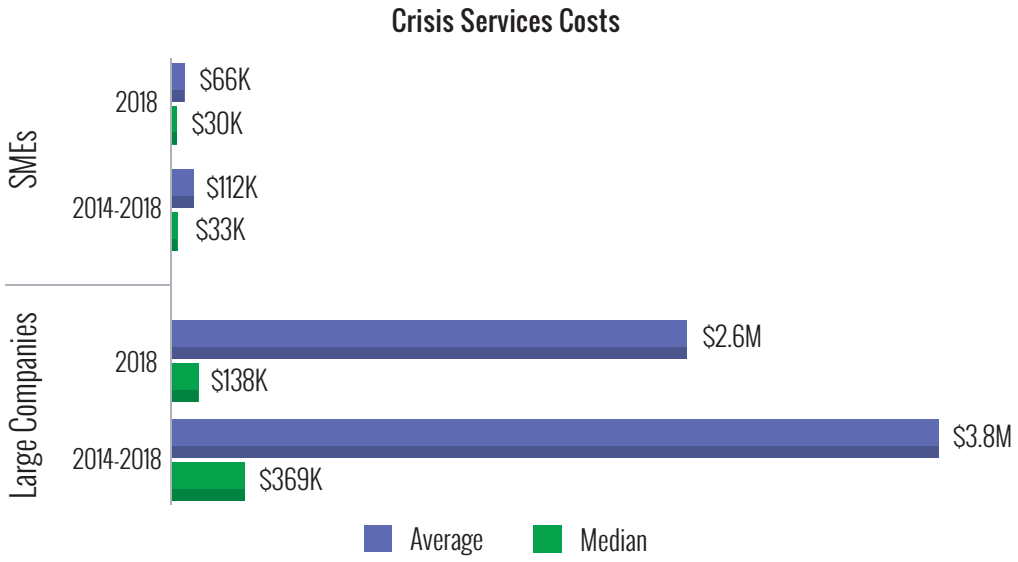


Figure 5

Legal Defense and Settlement Costs

For the five-year period, the dataset contained 189 claims with legal defense costs and 100 claims with legal settlement costs. For defense, these costs ranged from less than $500 to $5M. For settlement, the costs ranged from $1,500 to $6.8M.

The costs for SMEs ranged from less than $500 to $2.5M for defense, and $1.5K to $6.8M for settlements. For large companies, the ranges for defense and settlement were $5K to $5M, and $50K to $6.5M, respectively.

Figures 6 and 7 depict the average and median costs for SMEs and large companies, respectively.

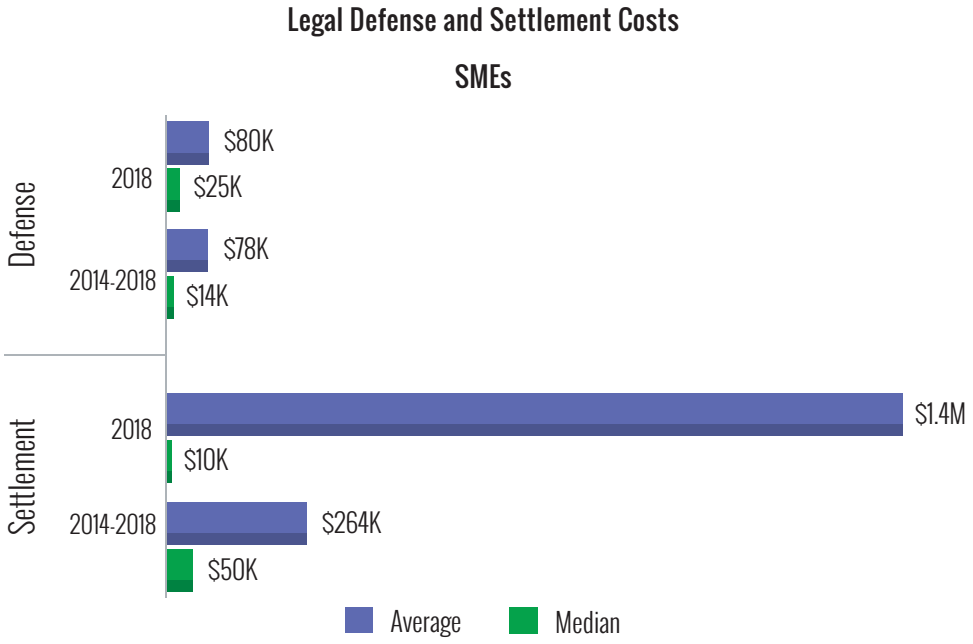


Figure 6

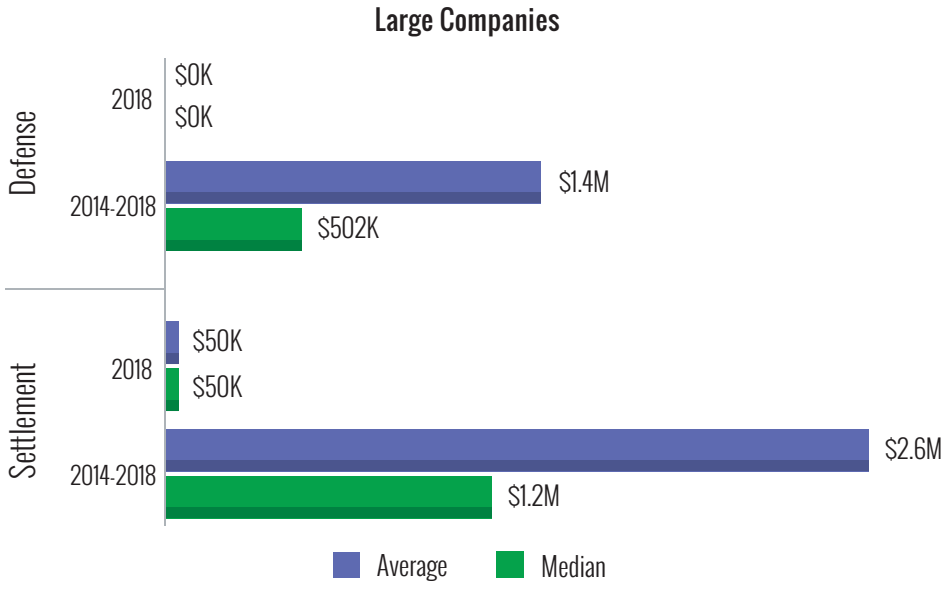


Figure 7

Regulatory Defense and Fines

For the five-year period, there were 17 claims with amounts for regulatory defense and 10 claims with amounts for regulatory fines. For defense, the amounts ranged from $2K to $5.8M. For regulatory fines, the amounts ranged from $5K to $3.5M.

Almost half of the claims that included regulatory fines were the result of a third party. A subset of those claims reported that all crisis services costs *except regulatory fines* were shared with the third party.

For SMEs, these costs ranged from $3.5K to $368K for defense, and $5K to $60K for fines. For large companies, regulatory defense ranged from $2K to $5.8M; there was a single claim for a regulatory fine of $3.5M. Figures 8 (SMEs) and 9 (large companies) depict the average and median costs for each category.

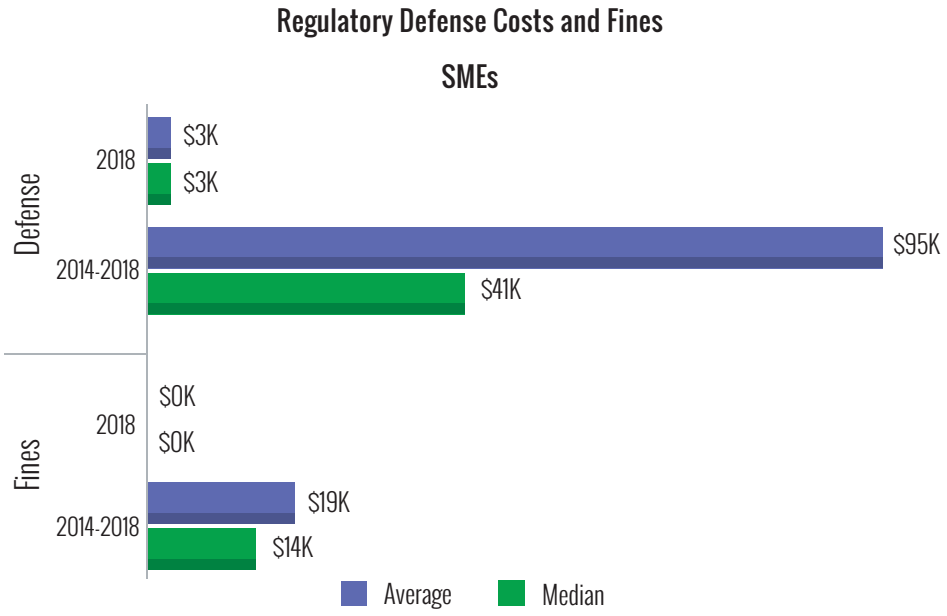


Figure 8

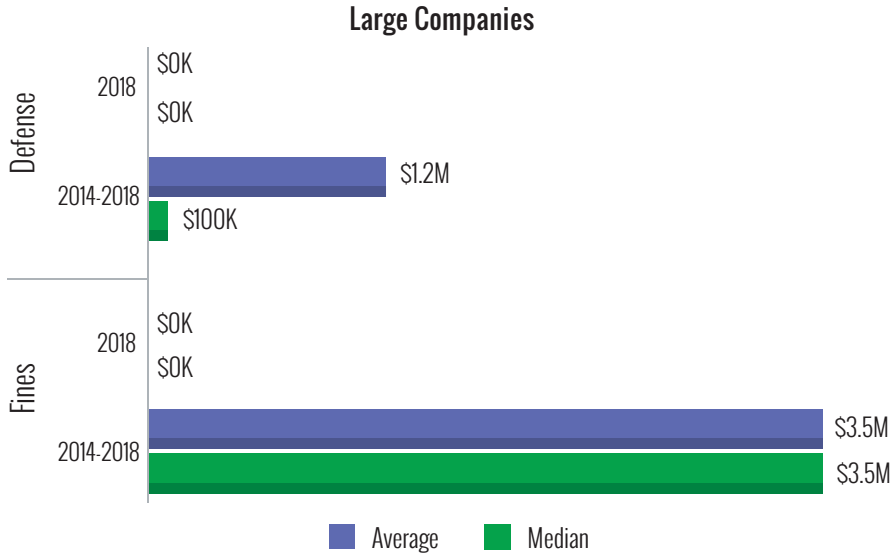


Figure 9

Note: There have been few claims for regulatory defense since 2014 and only four claims before 2017 for regulatory fines. Six of the 10 claims for regulatory fines occurred in 2017 and none occurred in 2018. However, because regulatory action often occurs many months after the triggering event these numbers could change significantly in future reports.

PCI Fines

Only 21 claims in the five-year data included PCI fines. The fines ranged $7K to $4.2M and totaled $13.7M. For SMEs, there were 19 claims with PCI fines ranging from $7K to $4.2M. The average PCI fine was $700K and the median was $68K. 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.

Point-of-sale malware and e-commerce RAM scraping impacted 71% of these claims with a financial impact for SMEs of $22M.

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 or more after an event. Sixty-two percent of the claims in this dataset are closed. The others remain open with a combined breach cost to date of $20M..

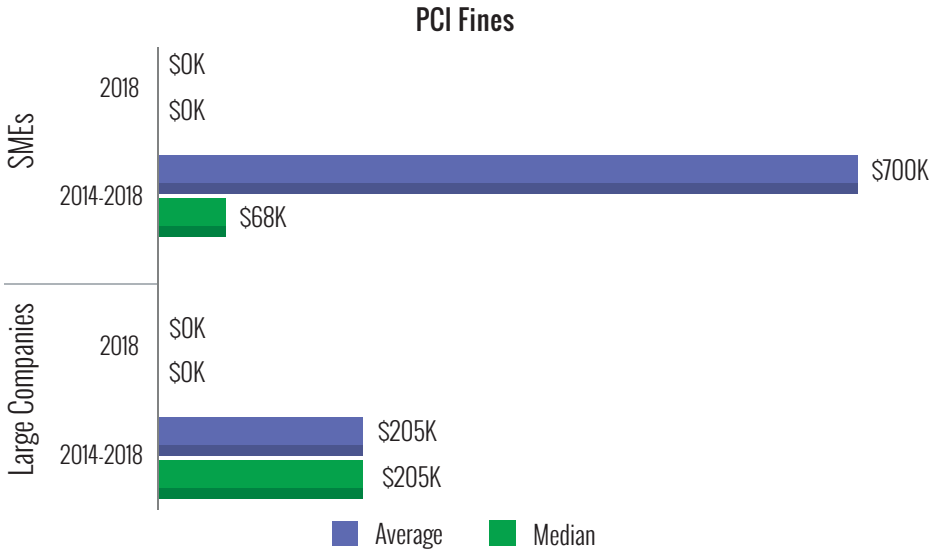


Figure 10

Lost Business Income and Recovery Expense

Of the 2,081 claims in the dataset, 96 included costs for lost business income and 90 included costs for recovery expense.

Ransomware is the most frequent cause of lost business income, accounting for almost 70% of claims. Malware/virus (15%) and hackers (9%) are the second and third most common causes of lost business income. Rogue employees, programming errors, and system glitches account for the remainder of claims for lost business income.

Ransomware is also the most frequently cited cause of recovery expense, accounting for 87% of claims. Malware/virus, hackers, rogue employees, and system glitches are the primary causes of loss in the other 13% of claims.

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 event was $60M; the recovery expense was $20M.

Lost Business Income and Recovery Expense
SMEs

Time Period	Nature of Loss	Claims	Range	Average	Median
2014-2018	Lost Income	95	1K-10M	343K	45K
	Recovery Expense	89	1K-500K	45K	14K

Table 1

Lost Business Income and Recovery Expense
SMEs

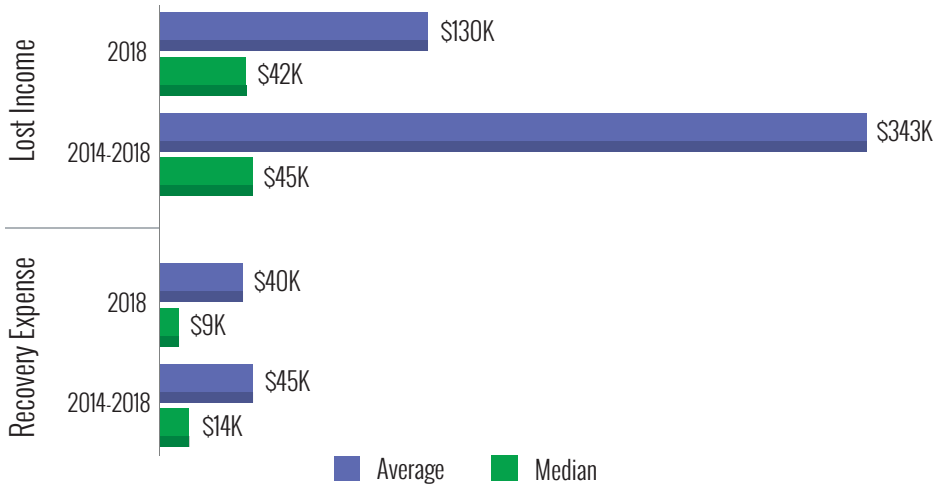


Figure 11

Per-Record Cost

Average costs per record are heavily influenced by outliers at both ends of the spectrum. For example, the dataset contained per-record costs ranging from $0.001 to more than $1.5M. The first of these involved a data breach with millions of records; the second involved a settlement for exposing the information of one person.

To understand the outsized influence of outliers, table 2 displays per-record costs based upon 100%, 95%, 90% and 80% of the data when ranked from least to greatest per-record costs. The results highlight the variances in the averages and the consistency in the medians.

Note: Soft costs, 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 coverage, is difficult and could be considered subjective.

Per-Record Costs

Revenue Size	Time Period	Percent of Data	Claims	Minimum	Average	Median	Maximum
SMEs	2018	100%	123	0.01	3,147	153	100,000
		95%	119	1.16	3,253	153	100,000
		90%	109	2.41	1,511	153	10,557
		80%	97	3.99	1,089	153	8,333
	2014-2018	100%	737	0.001	2,105	60	128,448
		95%	703	0.73	943	60	25,000
		90%	664	1.25	461	60	8,333
		80%	589	2.59	234	60	2,450
Large Companies	2018	100%	3	0.03	83,000	1.14	249,000
		95%	1	1.14	1.14	1.14	1.14
		90%	1	1.14	1.14	1.14	1.14
		80%	1	1.14	1.14	1.14	1.14
	2014-2018	100%	50	0.02	42,617	15	1,603,800
		95%	46	0.03	6,044	15	160,932
		90%	43	0.05	2,724	15	100,000
		80%	39	0.19	296	15	5,000

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

Table 2

Recordless Claims versus Claims with Exposed Records

One of the critical findings of the 2018 report was the prevalence of "recordless" events, representing 39% of claims in the dataset. Examples included most ransomware, distributed denial of service (DDoS), and wire transfer fraud/theft of money-related claims.

In 2018, the proportion of recordless claims increased to 63%. Social engineering, BEC, banking fraud, and ransomware accounted for 90% of this increase. The 2018 numbers drove the 5-year proportion of recordless claims from 39% to 48% (49% for SMEs and 23% for large companies).

The comparative averages for Breach and Crisis Services Costs are depicted in Figure 12 for SMEs and Figure 13 for large companies.

Recordless Claims vs Claims with Exposed Records Breach Costs

Revenue Size	Time Period	Nature of Claim	Claims	Range	Average	Median
SMEs	2018	Recordless	405	1K-2.6M	87K	44K
		Exposed Records	235	1K-7.4M	114K	26K
	2014-2018	Recordless	983	1K-20M	161K	45K
		Exposed Records	1,020	1K-10M	194K	50K
Large Companies	2018	Recordless	6	58K-505K	216K	200K
		Exposed Records	4	5K-10M	2.6M	176K
	2014-2018	Recordless	18	3K-80M	7.7M	380K
		Exposed Records	60	5K-64M	4.9M	2M

Table 3

Average Costs - Events with Records vs Recordless Events

SMEs

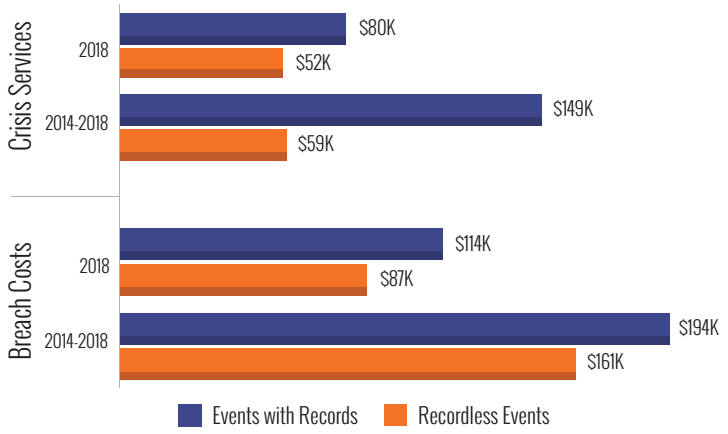


Figure 12

Large Companies

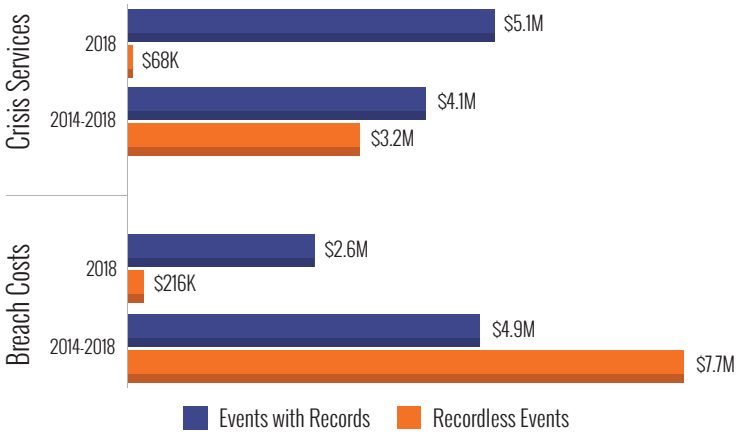


Figure 13

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	2018	575	0	16K	10K	250K
	2014-2018	1,766	0	56K	10K	10M
Large Companies	2018	10	5K	391K	150K	1M
	2014-2018	69	5K	2.6M	500K	15M

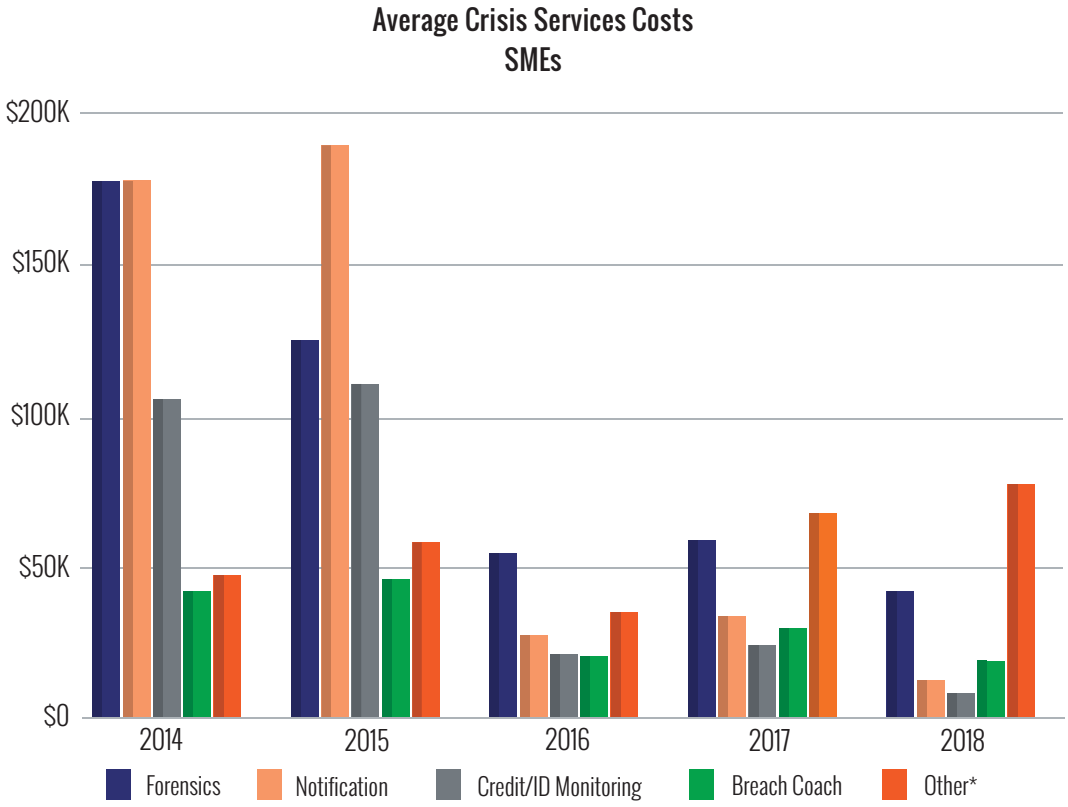
Table 4

Taking a Closer Look at the Data

Crisis Services Costs by Category

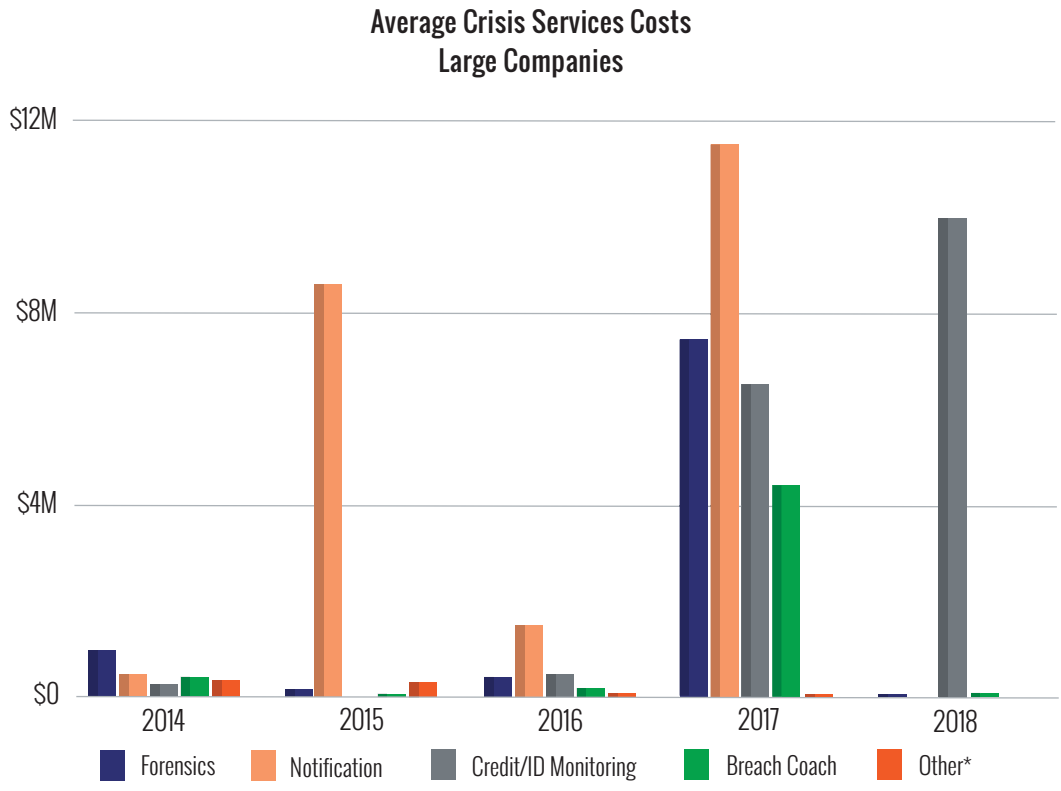
In addition to Total Crisis Services costs, the dataset contains costs for five distinct categories of crisis services: forensics, credit/ID monitoring, notification, Breach Coach (legal guidance), and other. Many claims reported costs in some of the categories but not in others, and many claims reported the total cost only. Therefore, Total Crisis Services costs are typically higher than the sum of the costs by category.

As Figures 14 and 15 illustrate, the amount spent on crisis services has 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.



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

Figure 14



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

Figure 15

Forensics

The increasing frequency of social engineering, ransomware, and wire transfer fraud claims has created two notable impacts on forensics costs. First, the dataset exposes a shift in the "accounting column" from traditional forensics to insurers' value-added bundled services. Second, bundled services enable pre-defined relationships with forensics firms that maintain large enough balances in cryptocurrency wallets to be able to pay ransoms quickly. Broadly, this helps to clarify the downward shift in forensics costs.

SMEs

In 2018, 31% of claims included forensics costs. For the five-year period, 47% of claims included forensics costs. Overall average and median forensics costs were $72K and $26K, respectively. The largest claim for forensic costs in the five-year period occurred in 2014 ($4.9M).

The average cost for forensics in 2018 dropped by almost 70% compared to the five-year average ($42K vs $72K), while the median remained virtually unchanged ($24K vs $26K). The largest claim for forensic costs in 2018 was $262K.

Large Companies

From 2014-2018, 38% of claims included forensic costs. In 2018, this percentage fell to 20%. The average and median forensic costs for the five-year period were $2M and $275K, respectively. The largest claim for forensic costs occurred in 2017 ($33M).

The average forensic costs in 2018 dropped dramatically when compared to the five-year average ($48K vs $2M), while the median dropped by a factor of 5 ($48K vs $275K). The largest claim for forensic costs in 2018 was $55K (there were only 2 large-company claims with forensics costs).

Credit/ID Monitoring

SMEs

For the five-year period, 15% of claims included credit/ID monitoring costs. Overall, the average and median credit/ID monitoring costs were $45K and $5K, respectively. The largest claim for credit/ID monitoring costs occurred in 2015 ($2M).

In 2018, the percentage of claims that included credit/ID monitoring costs fell to 6%. Average credit/ID monitoring costs in 2018 dropped by 83% compared to

the five-year average ($8K vs $45K), while the median remained unchanged ($4.5K vs $5K). The largest claim for credit/ID monitoring costs in 2018 was $75K.

Large Companies
For large companies, 21% of the claims in the five-year period included credit/ID monitoring costs. In 2018, this percentage fell to 10% (1 claim). For the five-year period the average and median credit/ID monitoring costs were $1.7M and $55K. The largest claim for credit/ID monitoring costs in the five-year period occurred in 2017 ($13M).

In the one 2018 large company claim that included credit/ID monitoring, the cost was $10M.

Large company claims that included credit/ID monitoring costs typically also included costs for other types of crisis services. For these claims, crisis services accounted for 81% of breach costs and totaled $94M.

Notification

SMEs
Approximately 17% of claims in the five-year period and 7% of claims in 2018 reported notification costs. The five-year average and median notification costs were $75K and $8K. The largest claim for notification costs occurred in 2014 ($5.5M).

The average notification cost in 2018 dropped by 84% compared to the five-year average ($12K vs $75K), while the median fell by half ($4K vs $8K). The largest claim for notification costs in 2018 was $125K.

Large Companies
In 2018, there were no large-company claims that included notification costs.

Overall, 28%of claims included notification costs. The average and median notification costs were $2.4M and $131K, respectively. The largest claim for notification costs occurred in 2017 ($23M). This outlier will affect the study's five-year numbers for several years.

Breach Coach (Legal Guidance)

SMEs
Thirty-four percent of claims in 2018 and 56% of claims in the five-year period reported Breach Coach costs. The five-year average and median Breach Coach costs were $28K and $11K. The largest claim for this cost occurred in 2017 ($1.1M).

The average Breach Coach cost in 2018 was 33% lower than the five-year average ($19K vs $28K), while the median was 25% lower ($8K vs $11K). The largest claim for this cost in 2018 was $186K.

Large Companies
Forty-two percent of claims in the five-year period and 30% of claims in 2018 reported Breach Coach costs. The five-year average and median Breach Coach costs were $954K and $70K. The largest claim for these costs occurred in 2017 ($21M).

The average Breach Coach cost in 2018 was a fraction of the five-year average ($80K vs $954K), while the median was one-third ($22K vs $70K). The largest claim for Breach Coach costs in 2018 was $199K.

Other Crisis Services

Other crisis services costs include public relations, data restoration, as well as ransom/extortion payment and fraudulent wire transfer. Given the nature of this "catch all" category, trends in costs—either upward or downward—may not be readily evident. Some variance by year can be expected.

SMEs
Eight percent of claims in the five-year period and 7% of claims in 2018 reported other crisis services costs. The five-year average and median costs were $60K and $14K. The largest claim for these costs occurred in 2015 ($1.1M).

The average other crisis services costs in 2018 was 25% higher than the five-year average ($77K vs $60K), while the median was double ($26K vs $14K). The largest claim for these costs in 2018 was $861K.

Large Companies
There were no claims in 2018 that included other crisis services costs. However, for the five-year period, 17% of large company claims included other crisis services costs. The five-year average and median costs were $218K and $20K. The largest claim for these costs occurred in 2014 ($2M).

Business Sector

In addition to the major sectors discussed in this section of the report, the dataset contains claims from multiple other sectors, including Energy, Entertainment, Gaming & Casino, Media, Restaurant, Telecommunications, and Transportation. As each of these sectors represented fewer than 2% of the claims in the dataset, they have been combined in the **All Other** category.

SMEs

Claims in the five-year dataset represent more than 18 business sectors. The top four sectors for SMEs were Professional Services, Healthcare, Retail, and Financial Services, which accounted for 59% of claims overall. In 2018, these four sectors plus Manufacturing (third place) accounted for 69% of claims.

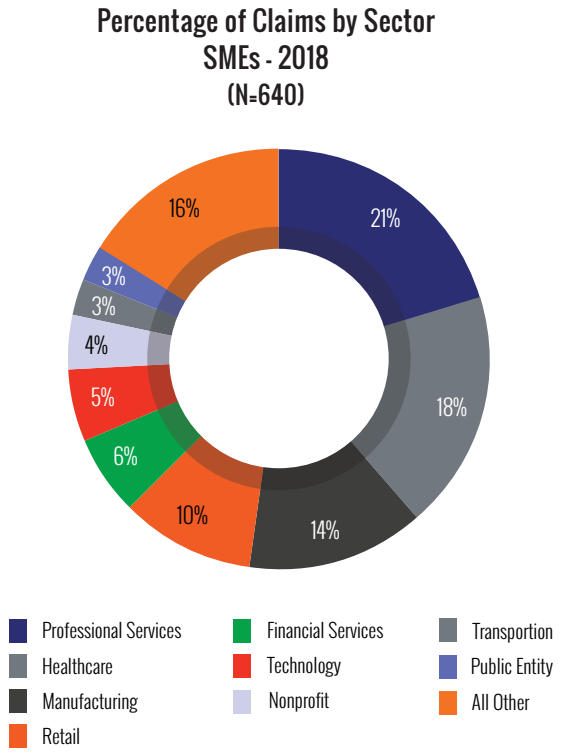


Figure 16

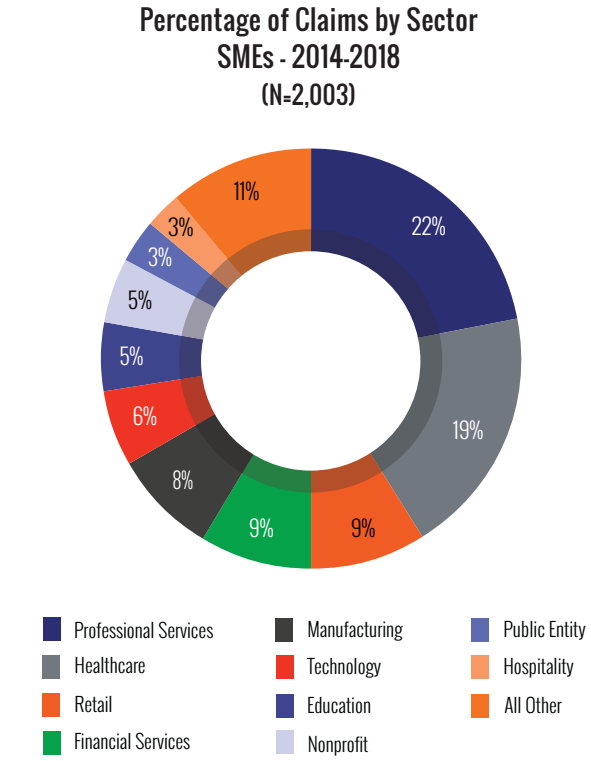


Figure 17

Table 5 below presents summary statistics and ranking for each sector based on Breach Costs. Table 6 provides the average costs for the individual components of Crisis Services, as well total Crisis Services.

Breach Costs by Business Sector
SMEs - 2014-2018

Sector	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Education	108	2K	163K	65K	1.5M	17.6M	11
Energy	20	2K	319K	50K	5.0M	6.4M	6
Entertainment	15	7K	154K	74K	764K	2.3M	12
Financial Services	171	1K	106K	40K	3.4M	18.2M	13
Gaming & Casino	6	76K	359K	284K	1.1M	2.2M	4
Healthcare	382	1K	182K	37K	9.0M	69.4M	10
Hospitality	58	6K	260K	65K	5.7M	15.1M	7
Manufacturing	163	2K	200K	44K	20.0M	32.6M	9
Media	17	5K	328K	75K	2.5M	5.6M	5
Nonprofit	97	1K	72K	20K	1.6M	7.0M	17
Professional Services	444	1K	90K	37K	3.6M	40.2M	15
Public Entity	66	3K	96K	56K	1.4M	6.4M	14
Restaurant	17	2K	68K	65K	367K	1.2M	18
Retail	181	2K	240K	60K	7.5M	43.4M	8
Technology	117	5K	455K	75K	10.0M	53.2M	3
Telecommunications	13	4K	542K	199K	2.0M	7.0M	2
Transportation	37	5K	590K	90K	17.5M	21.8M	1
Other	91	1K	81K	41K	800K	7.4M	16

*Ranking is based on average Breach Cost

Table 5

Average Crisis Services Costs by Business Sector
SMEs - 2014-2018

Sector	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Education	76K	44K	27K	26K	120K	114K	8
Energy	65K			5K	65K	73K	12
Entertainment	115K	3K	70K	39K	37K	124K	7
Financial Services	51K	27K	15K	22K	56K	78K	10
Gaming & Casino	292K	45K	12K	28K		342K	2
Healthcare	55K	198K	104K	27K	113K	157K	5
Hospitality	134K	27K	23K	48K	23K	155K	6
Manufacturing	26K	11K	7K	14K	21K	37K	18
Media	46K	59K		47K	15K	77K	11
Nonprofit	81K	6K	4K	19K	17K	71K	14
Professional Services	40K	29K	15K	19K	44K	57K	17
Public Entity	43K	23K	21K	23K	20K	72K	13
Restaurant	35K	19K	14K	26K	85K	66K	15
Retail	234K	29K	24K	38K	119K	228K	3
Technology	91K	83K	158K	53K	32K	173K	4
Telecommunications	164K	1.6M		396K	12K	533K	1
Transportation	95K	7K	5K	17K	86.9K	86.7K	9
Other	43K	33K	18K	17K	47K	62K	16

* Includes public relations, data restoration, and sometimes ransom payment and fraudulent wire transfer
**Ranking is based on average Total Crisis Services

Table 6

Professional Services

Professional Services claims comprised 22% of the five-year dataset (444 claims). Ranging from $1K to $3.6M, they accounted for 11% of total Breach Costs ($40M). Of those claims, 21% occurred in 2018 and accounted for 19% of Breach Costs for that year. The average and median costs for Professional Services claims tended to be lower than those of other sectors. The five-year average Breach Cost placed Professional Services fifteenth out of 18 sectors.

Healthcare

Healthcare claims accounted for 19% of claims in the five-year period and 19% of Breach Costs. In 2018, these claims accounted for 18% of claims and 12% of Breach Costs. When ranked by the five-year average Breach Cost, Healthcare occupied tenth place.

Financial Services

Claims in the Financial Services sector accounted for 9% of claims in the five-year period and 5% of Breach Costs. In 2018, they accounted for only 6% of claims, but 10% of Breach Costs. When ranked by the five-year average Breach Cost, Financial Services occupied thirteenth place.

Retail

Retail claims accounted for 9% of claims in the five-year period and 12% of Breach Costs. In 2018, they constituted 10% of claims, but only 7% of Breach Costs.

Retail placed eighth when ranked by the five-year average Breach Cost.

Education and Higher Education

Claims in Education accounted for 5% of claims in the five-year period and 5% of the Breach Costs. In 2018, this sector accounted for less than 3% of claims and 5% of Breach Costs. When ranked by average Breach Cost, Education occupied eleventh place.

Higher Education Only

Higher Education accounted for 57% of claims in the Education sector (same percentage as the 2018 study). Of interest however, is that for the five-year period, average Crisis Services Costs were 34% higher in this sub-sector ($141K vs $114K) and average Breach Cost was 24% higher than costs for the Education sector overall ($215K vs $163K). For 2018, average Crisis Services Costs were 5% lower for this sub-sector ($102K vs $107K), while average Breach Costs were 33% higher ($251K vs $189K).

Manufacturing

The Manufacturing sector has been increasingly targeted by cyber criminals. The proportion of claims from this sector has increased from 9% in the 5-year period to 14% in 2018. Social engineering and ransomware claims in the Manufacturing sector rose to 85% in 2018, up from 71% for the 5-year period.

Apart from a very large claim ($20M), 5-year average Breach Costs ($200K) and average Crisis Services Costs ($37K) rank fairly low among SME sectors, ninth and eighteenth, respectively. Average Breach Costs in 2018 dropped to $75K while average Crisis Services Costs remained the same at $37K.

Large Companies

The dataset contained 78 claims filed by large companies. These companies operated in 15 different business sectors. In 2018, the top four sectors for large companies were Healthcare, Retail, Education, and Public Entity. Historically, however, Public Entity has not occupied a top spot and is therefore absent in Figure 19. For the five-year period, the top four sectors for large companies were Healthcare, Retail, Financial Services, and Education.

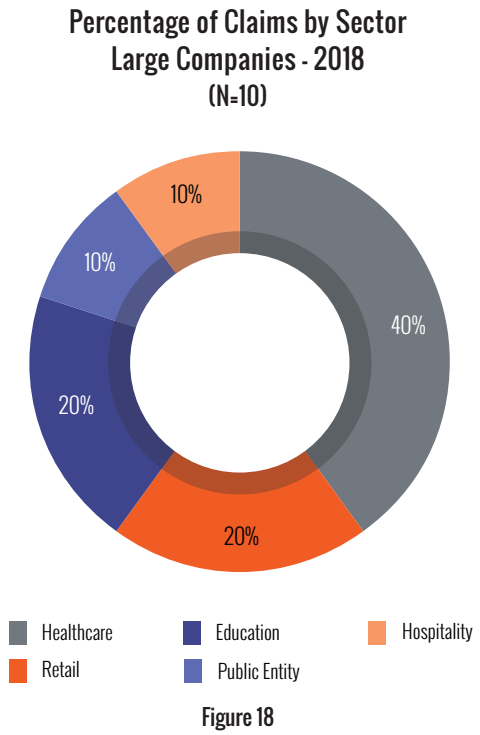


Figure 18

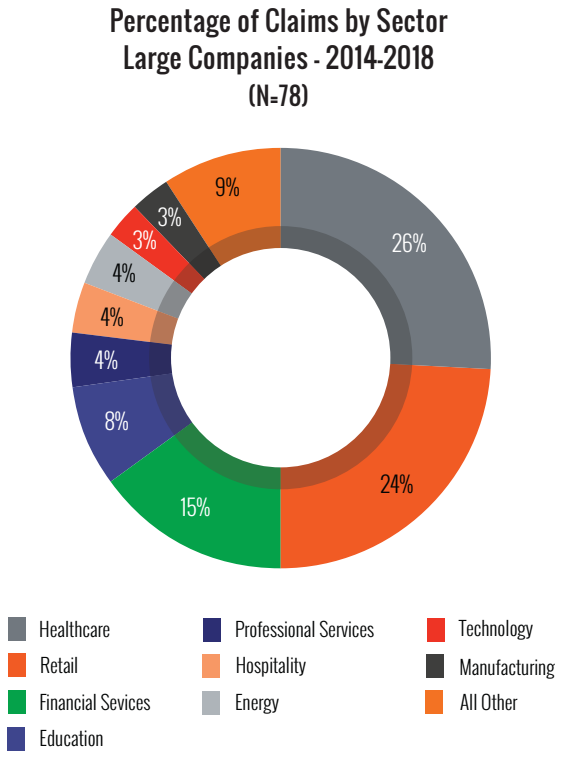


Figure 19

Table 7 below presents summary statistics and ranking for each sector based on Breach Costs. Transportation companies experienced the highest average Breach Costs, followed Manufacturing, Financial Services, and Retail. Healthcare organizations ranked seventh in average Breach Costs.

Breach Costs by Business Sector: Large Companies - 2014-2018

Sector	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Education	6	3K	216K	94K	875K	1.3M	13
Energy	3	2.5M	4.2M	5.0M	5.0M	12.5M	6
Financial Services	12	72K	10.7M	3.9M	64.0M	128.7M	3
Gaming & Casino	1	80K	80K	80K	80K	80K	14
Healthcare	20	5K	3.4M	259K	15.0M	68.3M	7
Hospitality	3	738K	4.2M	2.0M	10.0M	12.7M	5
Manufacturing	2	20K	16.5M	16.5M	33.0M	33.0M	2
Nonprofit	1	13K	13K	13K	13K	13K	15
Professional Services	3	332K	3.1M	2.7M	6.2M	9.2M	8
Public Entity	1	505K	505K	505K	505K	505K	10
Retail	19	60K	4.2M	2.5M	16.8M	80.5M	4
Technology	2	1.0M	2.6M	2.6M	4.1M	5.1M	9
Telecommunications	1	400K	400K	400K	400K	400K	11
Transportation	1	80.0M	80.0M	80.0M	80.0M	80.0M	1
Other	3	100K	219K	234K	322K	656K	12

*Ranking is based on average Breach Cost

Table 7

Table 8 provides the average costs for individual components of Crisis Services, as well total Crisis Services. Due to a single very large claim, the highest average for total Crisis Services costs occurred in the Manufacturing sector. The following three highest averages occurred in the Financial Services, Professional Services, and Healthcare sectors.

Average Crisis Services Costs by Business Sector
Large Companies - 2014-2018

Sector	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Education	192K	60K	55K	31K	4K	211K	10
Financial Services	3.2M	5.7M	7.4M	7.2M		12.5M	2
Gaming & Casino	50K			10K		60K	11
Healthcare	322K	2.8M	286K	79K	64K	2.4M	4
Hospitality	280K		5.0M	866K	306K	4.1M	7
Manufacturing	33.0M					33.0M	1
Nonprofit				11K		11K	12
Professional Services	2.3M	69K	5K	402K	13K	3.1M	3
Retail	1.1M	277K	200K	797K	299K	1.8M	5
Technology	650K			560K		1.2M	6
Telecommunications	18K	200K				218K	9
Other	217K	18K	7K	28K		258K	8

* Includes public relations, data restoration, and sometimes ransom payment and fraudulent wire transfer
**Ranking is based on average Total Crisis Services

Table 8

Healthcare

Healthcare claims accounted for 26% of claims in the five-year period and 16% of Breach Costs. In 2018, these Healthcare accounted for 40% of claims but only 5% of Breach Costs. When ranked by the five-year average Breach Cost, Healthcare occupied seventh place.

Retail

Retail claims accounted for 24% of claims in the five-year period and 19% of Breach Costs. In 2018, they constituted 10% of claims, but only 3.5% of Breach Costs. Retail placed fourth when ranked by the five-year average Breach Cost.

Financial Services

The Financial Services sector accounted for 15% of claims in the five-year period and 29% of Breach Costs. In 2018, there were no Financial Services claims for large companies. When ranked by the five-year average Breach Cost, Financial Services occupied third place.

Other

In 2017, malware caused a very expensive ($33M) network outage in the Manufacturing sector. The largest claim in 2018 occurred in the Hospitality sector: $10M in Crisis Services due to a hacking incident.

Revenue Size

In the five-year period from 2014-2018, 96% of claims came from SMEs and 4% of claims from large companies. Because claims from organizations of unknown annual revenue had cost distributions similar to SMEs, they were included in SME analyses.

As might be expected, there were very large differences in Breach Costs and Crisis Services Costs for organizations on opposite sides of the $2B annual revenue threshold.

Figures 20 and 21 present a more granular look at the revenue size of SMEs with claims in 2018 and the five-year period, respectively. There were very few large-company claims in 2018, but a more granular view of revenue size for the five-year period is presented in Figure 22.

Percentage of Claims by Revenue Size
SMEs - 2018
(N=640)

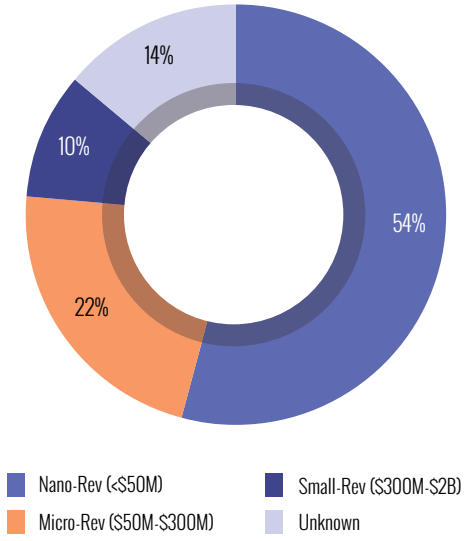


Figure 20

Percentage of Claims by Revenue Size
SMEs - 2014-2018
(N=2,003)

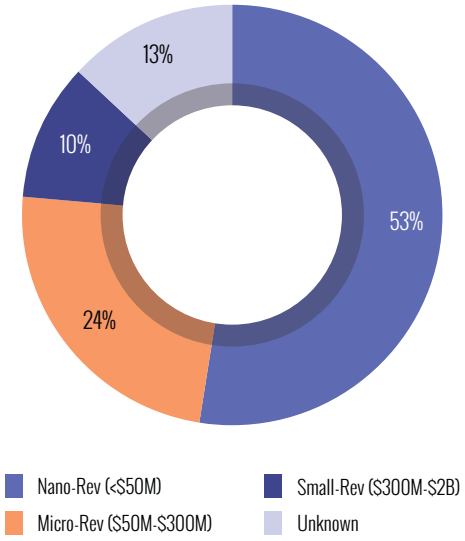


Figure 21

Percentage of Claims by Revenue Size
Large Companies - 2014-2018
(N=78)

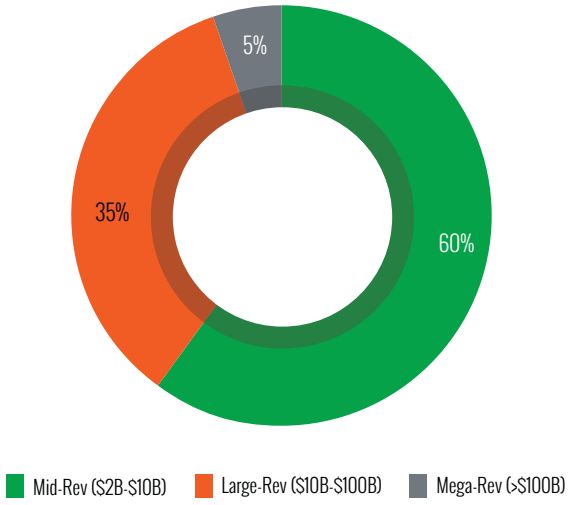


Figure 22

There was a 30-fold difference in average Breach Costs between SMEs and large companies, and a 20-fold difference in median costs. For SMEs, average Breach Costs were $178K vs $5.6M for large companies. For median Breach Costs, the numbers were $48K vs $1M.

The tables below present total Breach Costs and average Crisis Services Costs for SMEs and large companies, as well as more detailed numbers based on revenue size. Note that average Breach Costs increased as the size of the company increased, from $103K for Nano-Rev to $11M for Mega-Rev companies.

In virtually every category of crisis services, costs also differed dramatically between SMEs and large companies. Costs were 20 to 30 times more for large companies in every category except other crisis services costs.

Breach Costs by Revenue Size
2014-2018

Revenue Size	Claims	Minimum	Average	Median	Maximum	Total
SMEs	2,003	1K	178K	48K	20.0M	356.8M
Nano-Rev (<$50M)	1,056	1K	103K	38K	7.5M	109.0M
Micro-Rev ($50M-$300M)	476	1K	183K	61K	6.6M	87.2M
Small-Rev ($300M-$2B)	210	3K	419K	116K	10.0M	88.1M
Unknown	262	1K	278K	35K	20.0M	73.0M
Large Companies	78	3K	5.6M	1.0M	80.0M	433.1M
Mid-Rev ($2B-$10B)	46	3K	2.9M	261K	64.0M	133.7M
Large-Rev ($10B-$100B)	27	249K	9.4M	5.0M	80.0M	254.9M
Mega-Rev (> $100B)	4	2.5M	11.0M	13.2M	15.0M	44.0M

Table 9

Average Crisis Services Costs by Revenue Size
2014-2018

	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services
SMEs	72K	75K	45K	28K	60K	112K
Nano-Rev (<$50M)	43K	54K	27K	22K	48K	74K
Micro-Rev ($50M-$300M)	81K	77K	81K	41K	34K	132K
Small-Rev ($300M-$2B)	197K	96K	78K	44K	67K	238K
Unknown	77K	108K	40K	21K	162K	128K
Large Companies	2.0M	2.4M	1.7M	954K	218K	3.8M
Mid-Rev ($2B-$10B)	911K	1.8M	1.2M	914K	46K	2.8M
Large-Rev ($10B-$100B)	9.0M	4.1M	5.2M	1.3M	189K	6.9M
Mega-Rev (> $100B)	2.5M	1.0M	1.7M	532K	2.0M	4.1M

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

Table 10

Cause of Loss

SMEs

Social engineering[7], ransomware, hackers, and malware/viruses were the leading causes of loss in this year's report. Social engineering and ransomware occupied the top spots in 2018 and for the five-year period.

The increasing prevalence of social engineering claims was quite obvious: 48% in 2018 versus 30% for the five-year total. The distribution of SME claims by cause of loss is presented in Figures 23 and 24.

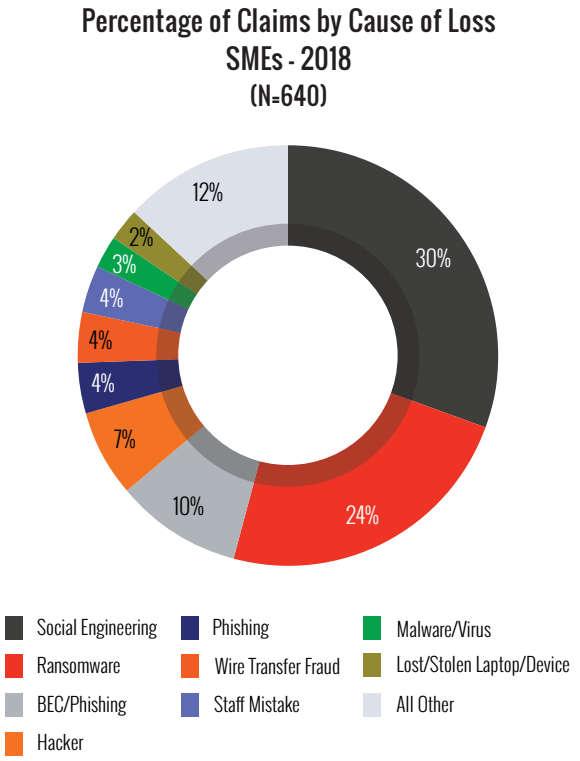


Figure 23

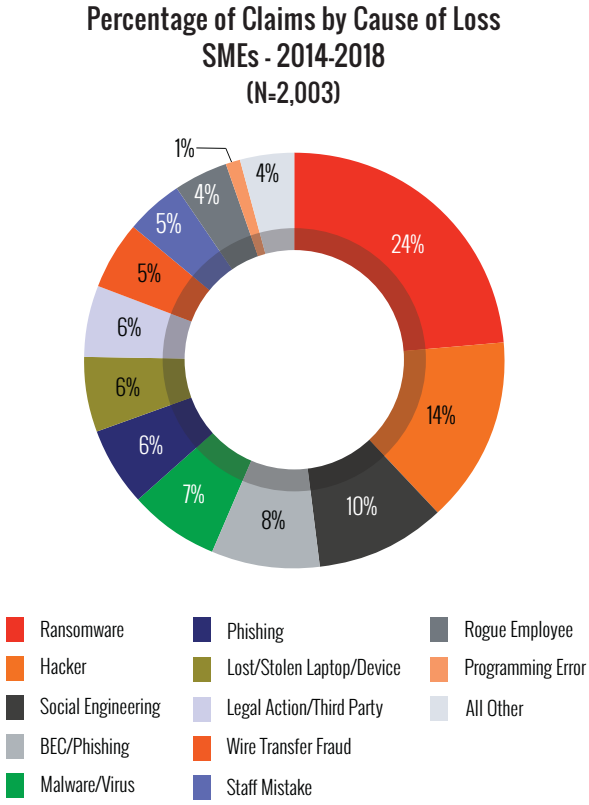


Figure 24

Table 11 below presents summary statistics and ranking based on Breach Costs for each cause of loss. Table 12 provides the average costs for the individual components of Crisis Services, as well total Crisis Services for each cause.

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

Breach Costs by Cause of Loss
SMEs - 2014-2018

Cause	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Business email compromise (BEC)	164	4K	156K	67K	3.4M	25.6M	7
Hacker	285	1K	337K	74K	7.4M	96.1M	2
Legal action/Third party	112	3K	241K	51K	10.0M	27.0M	5
Lost/stolen laptop/device	95	2K	76K	27K	1.5M	7.2M	15
Malware/Virus	142	2K	308K	70K	9.0M	43.7M	3
Negligence	7	5K	58K	27K	135K	0.4M	18
Paper records	23	3K	69K	25K	650K	1.6M	16
Phishing	133	1K	80K	37K	1.1M	10.6M	17
Programming error	24	2K	305K	63K	3.6M	7.3M	4
Ransomware	478	1K	150K	40K	20.0M	71.6M	9
Rogue employee	80	1K	151K	60K	2.5M	12.1M	8
Social engineering[8]	547	1K	107K	54K	3.4M	58.6M	12
Staff mistake	120	1K	78K	25K	2.5M	9.4M	14
System glitch	10	2K	1.9M	79K	17.5M	19.3M	1
Theft of money	9	2K	123K	67K	470K	1.1M	11
Trademark/Copyright infringement	9	12K	149K	60K	468K	1.3M	10
Wire transfer fraud	106	4K	180K	105K	1.4M	19.1M	6
Wrongful data collection	1	86K	86K	86K	86K	86K	13

*Ranking is based on average Breach Cost

Table 11

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

Average Crisis Services Costs by Cause of Loss
SMEs - 2014-2018

Cause	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Business email compromise (BEC)	49K	14K	17K	26K	99K	83K	7
Hacker	138K	157K	84K	47K	52K	247K	2
Legal action	23K	18K	26K	16K	7K	33K	18
Lost/stolen laptop/device	31K	66K	24K	25K	46K	75K	9
Malware/Virus	146K	184K	141K	42K	129K	249K	1
Negligence	6K	24K	1K	24K		37K	16
Paper records	8K	13K	21K	27K	15K	35K	17
Phishing	57K	14K	28K	18K	39K	68K	12
Programming error	57K	125K	107K	32K	7K	140K	3
Ransomware	33K	17K	26K	11K	30K	46K	15
Rogue employee	67K	9K	6K	76K	15K	112K	4
Social engineering[9]	48K	14K	20K	23K	93K	75K	10
Staff mistake	39K	48K	21K	22K	4K	51K	14
System glitch	84K	55K	2K	51K	100K	107K	5
Theft of money	28K	2K	3K	48K	1K	63K	13
Trademark/Copyright infringement				91K		91K	6
Wire transfer fraud	35K	9K	9K	28K	113K	68K	11
Wrongful data collection				80K		80K	8

* Includes public relations, data restoration, and sometimes ransom payment and fraudulent wire transfer
**Ranking is based on average Total Crisis Services

Table 12

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

Large Companies

For the five-year period, hackers, malware/virus, third-party legal actions, and social engineering generated the greatest number of claims by large companies.

Table 13 presents summary statistics and ranking for each cause of loss based on Breach Costs. The highest total Breach Costs were caused by hackers, malware/viruses, system glitches, and rogue employees. Excluding a very large breach caused by a system glitch ($80M), the highest average Breach Costs were caused by malware/virus, hackers, rogue employees, and ransomware.

Table 14 provides a breakdown of Crisis Services Costs for each cause of loss. Hacker, malware/virus, and rogue employees caused the highest Crisis Services Costs, which tracks closely with the types of events that caused the highest Breach Costs.

Percentage of Claims by Cause of Loss
Large Companies - 2014-2018
(N=78)

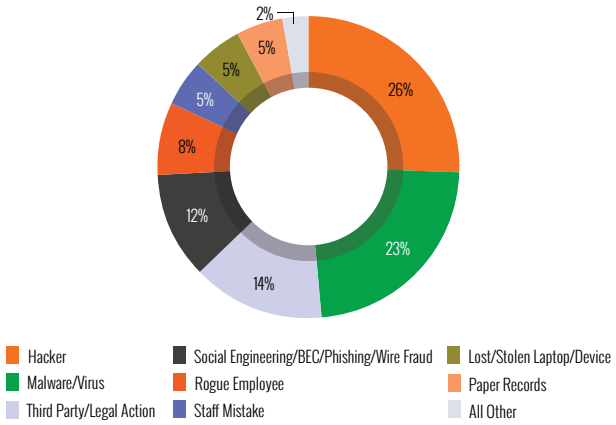


Figure 25

Breach Costs by Cause of Loss
Large Companies - 2014-2018

Cause	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Business email compromise (BEC)	3	72K	341K	77K	875K	1.0M	12
Hacker	20	60K	7.9M	2.6M	64.0M	158.6M	3
Legal action/Third party	11	13K	1.9M	1.6M	5.0M	21.2M	6
Lost/stolen laptop/device	4	10K	699K	142K	2.5M	2.8M	9
Malware/Virus	18	20K	6.9M	4.6M	33.0M	124.2M	4
Paper records	4	3K	35K	18K	100K	139K	16
Phishing	1	165K	165K	165K	165K	165K	14
Programming error	1	678K	678K	678K	678K	678K	10
Ransomware	1	15.0M	15.0M	15.0M	15.0M	15.0M	2
Rogue employee	6	111K	4.3M	4.6M	11.5M	25.9M	5
Social engineering[10]	9	72K	409K	165K	1.5M	3.7M	11
Staff mistake	4	100K	813K	325K	2.5M	3.3M	8
System glitch	1	80.0M	80.0M	80.0M	80.0M	80.0M	1
Theft of money	1	103K	103K	103K	103K	103K	15
Wire transfer fraud	2	505K	990K	505K	1.5M	2.0M	7
Wrongful data collection	1	249K	249K	249K	249K	249K	13

*Ranking is based on average Breach Cost

Table 13

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

Average Crisis Services Costs by Cause of Loss
Large Companies - 2014-2018

Cause	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Business email compromise (BEC)	348K	66K	55K	56K		331K	5
Hacker	1.2M	6.9M	4.9M	2.5M	431K	6.7M	1
Legal action	50K			10K		35K	11
Lost/stolen laptop/device	6K	6K	18K	8K		22K	12
Malware/Virus	4.9M	613K	96K	611K	131K	4.9M	2
Paper records		4K	2K	4K		7K	13
Phishing		13K	104K	20K	8K	145K	9
Programming Error	106K	100K	375K	77K	20K	678K	4
Ransomware						0K	N/A
Rogue employee	1.1M	508K	859K	297K	4K	1.8M	3
Social engineering[11]	205K	48K	80K	45K	8K	226K	6
Staff mistake	18K	200K				218K	7
System glitch							N/A
Wire transfer fraud	44K			63K		107K	10
Wrongful data collection				199K		199K	8

* Includes public relations, data restoration, and sometimes ransom payment and fraudulent wire transfer
**Ranking is based on average Total Crisis Services

Table 14

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

Criminal vs Non-Criminal Activities

One of the clearest trends in the data is the increasing percentage of claims caused by criminal activity. This percentage has increased from 72% in 2014 to 86% in 2017 and 2018.

"The increase in data breaches resulting from criminal conduct shows the importance of retaining counsel and notifying law enforcement as soon as a breach is discovered. Counsel must work with law enforcement to determine whether breach notification can be delayed pending any investigation. And having law enforcement involved early in the process will help the company control the narrative once the breach is publicly disclosed."

Brian Kint, CIPP/US
Member, Cozen O'Connor

Criminal events included hacking, ransomware, malware/virus, social engineering, business email compromise (BEC), phishing, distributed denial of service (DDoS) attacks, stolen devices, theft of money via wire transfer, and banking/ACH fraud.

Non-criminal events included staff mistakes, mishandling of paper records, lost laptops, programming errors, system glitches, and legal actions.

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

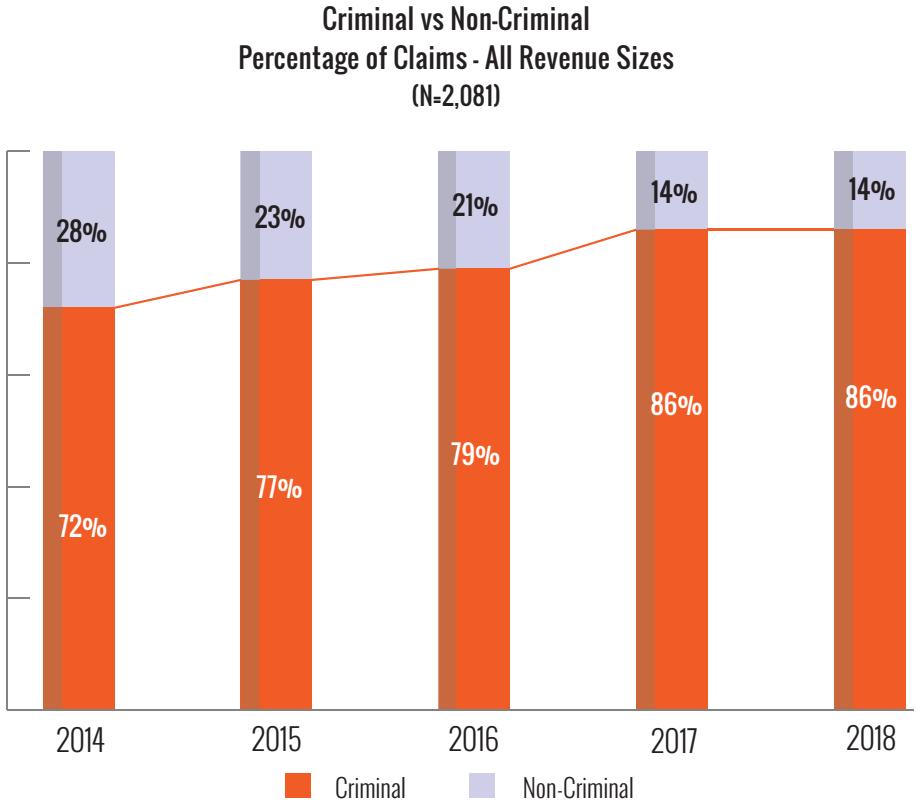


Figure 26

Criminal vs Non-Criminal Financial Impact

Revenue Size	Time Period	Nature of Cost	Type of Activity	Claims	Minimum	Average	Median	Maximum	Total
SMEs	2018	Crisis Services	Criminal	242	1K	68K	31K	1.3M	16.4M
			Non-Criminal	14	1K	26K	11K	90K	362K
		Total Breach	Criminal	550	1K	107K	44K	7.4M	58.9M
			Non-Criminal	90	2K	35K	18K	501K	3.1M
	2014-2018	Crisis Services	Criminal	1,167	1K	121K	36K	8.2M	140.9M
			Non-Criminal	167	1K	51K	14K	679K	8.6M
		Total Breach	Criminal	1,646	1K	188K	51K	20.0M	309.3M
			Non-Criminal	357	1K	133K	25K	17.5M	47.5M
Large Companies	2018	Crisis Services	Criminal	3	58K	3.4M	77K	10M	10.1M
			Non-Criminal	1	199K	199K	199K	199K	199K
		Total Breach	Criminal	7	58K	1.6M	150K	10.0M	11.1M
			Non-Criminal	3	5K	168K	249K	250K	504K
	2014-2018	Crisis Services	Criminal	40	10K	4.4M	688K	64.0M	175.6M
			Non-Criminal	6	3K	187K	105K	678K	1.1M
		Total Breach	Criminal	66	10K	5.3M	2.0M	64.0M	347.3M
			Non-Criminal	12	3K	7.2M	250K	80.0M	85.8M

Table 15

Social Engineering, Business Email Compromise (BEC), Phishing, and Banking Fraud

Social engineering may be generally defined[12] as malicious action that causes a deviation from standard operating procedures or policies and subsequent losses by the organization. Very often, this is accomplished through highly-skilled persuasion by bad actors against organizational employees who fail 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, phishing, and banking fraud as separate categories.

Social engineering as a cause of loss distinct from the other three causes mentioned above 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.

BEC involves well-crafted, highly personalized attacks. Criminals invest considerable time and research into the wording and tone of fraudulent emails to obtain their desired outcomes. The danger of this type of attack is that it exploits gaps in the insured's processes resulting in banking fraud, wire transfer, ACH, or theft of money. Software exploits in Office 365 and other productivity software are also soft targets for criminals.

Phishing attacks are indiscriminate and impersonal. When thinking about phishing, the word "campaign" comes to mind – 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.

SMEs

Figure 27 depicts the individual causes of loss that can be categorized as social engineering. In addition to the three primary causes, which account for almost 90% of claims, there are a small number of other causes.

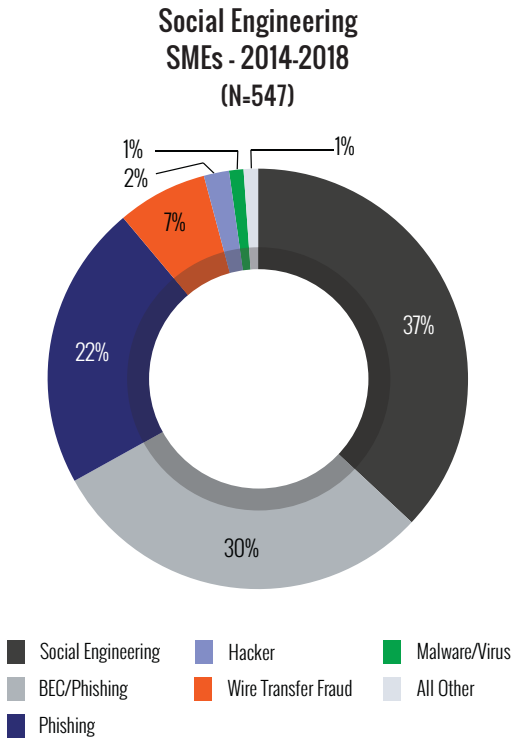


Figure 27

[12] Based upon discussions with insurers and lawyers at the NetDiligence® Cyber Risk Summit Philadelphia, June 2019

Social Engineering

Revenue Size	Cause of Loss	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	Combined* Social Engineering	2018	Crisis Services	75	2K-1.3M	92K	45K
			Total Breach	314	2K-3.4M	100K	57K
		2014-2018	Crisis Services	272	1K-1.3M	75K	35K
			Total Breach	547	1K-3.4M	107K	54K
	BEC	2018	Crisis Services	50	4K-1.3M	118K	58K
			Total Breach	62	13K-3.4M	202K	80K
		2014-2018	Crisis Services	140	1K-1.3M	83K	44K
			Total Breach	164	4K-3.4M	156K	67K
	Phishing	2018	Crisis Services	12	2K-136K	28K	13K
			Total Breach	29	3K-250K	44K	21K
		2014-2018	Crisis Services	104	1K-834K	68K	25K
			Total Breach	133	1K-1.1M	80K	37K
	Banking Fraud	2018	Crisis Services	14	4K-128K	42K	31K
			Total Breach	41	7K-938K	132K	105K
		2014-2018	Crisis Services	58	1K-479K	68K	25K
			Total Breach	106	4K-1.4M	180K	105K
Large Companies	Combined* Social Engineering	2018	Crisis Services	1	77K	77K	77K
			Total Breach	4	77K-505K	247K	203K
		2014-2018	Crisis Services	6	72K-845K	226K	108K
			Total Breach	9	72K-1.5M	409K	165K
	BEC	2018	Crisis Services	1	77K	77K	77K
			Total Breach	1	77K	77K	77K
		2014-2018	Crisis Services	3	72K-845K	331K	77K
			Total Breach	3	72K-875K	341K	77K
	Phishing	2018	Crisis Services	0			
			Total Breach	0			
		2014-2018	Crisis Services	1	145K	145K	145K
			Total Breach	1	165K	165K	165K
	Banking Fraud	2018	Crisis Services	0			
			Total Breach	1	505K	505K	505K
		2014-2018	Crisis Services	1	107K	107K	107K
			Total Breach	2	505K-1.5M	990K	990K

*Includes social engineering, BEC, phishing, and banking fraud

Table 16

Ransomware

The increased frequency of ransomware events is no secret. In this study, the increase in the number of ransomware claims from 2014 through 2018 has been dramatic: 7 in 2014, 19 in 2015, 92 in 2016, 211 in 2017, and 151 so far in 2018.[13]

"For several years in a row the focus of attackers has shifted to SMEs, and this year's data does nothing to change the trend. Attackers are focusing on small and mid-sized business almost to the exclusion of all others. Data breaches within large companies carry the headlines while ransomware and email compromise within SMEs carries the majority of the cost."

Daimon Geopfert
National Leader, Security and Privacy Services
RSM US

The ransoms demanded have also increased significantly. Ransoms in 2018 were double the five-year average ($72K vs $36K). The highest ransoms demanded that year were in excess of $1M.

The majority of ransomware-related claims in our dataset (362) occurred in 2017 and 2018. NotPetya, WannaCry and Locky were the top variants noted in the detailed descriptions of the events. BitPaymer and DoppelPaymer banking malware have been important tools for malicious actors, enabling them to demand much higher ransoms than before.

As seen by the table below, ransomware appears to be a much greater risk factor for SMEs than for large companies. This stands to reason, given that large companies tend to have greater resources and targeted management directives to invest in both technology solutions and employee training. That having been said, exceptions can and do occur. The dataset contains one ransomware claim by a large company for a loss of $15M.

Ransomware

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Ransom	49	1K-1.1M	72K	10K
		Crisis Services	121	1K-355K	46K	24K
		Total Breach	151	1K-2.6M	91K	33K
	2014-2018	Ransom	149	1K-1.1M	36K	9K
		Crisis Services	392	1K-460K	46K	28K
		Total Breach	478	1K-20M	150K	40K
Large Companies	2018	Ransom	0			
		Crisis Services	0			
		Total Breach	0			
	2014-2018	Ransom	0			
		Crisis Services	0			
		Total Breach	1	15M	15M	15M

Table 17

[13] Data for 2018 will continue to be collected in 2020 and 2021.

Hacking and Malware/Virus

Hacker and Malware/Virus (Malware) are categories that often overlap. It was sometimes difficult to determine which one to assign as the cause of loss. For this reason, results have been presented for each cause of loss separately as well as combined.

Hacker and Malware/Virus

Revenue Size	Cause of Loss	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	Hacker and Malware/Virus Combined	2018	Crisis Services	42	1K-406K	79K	42K
			Total Breach	61	3K-7.4M	201K	39K
		2014-2018	Crisis Services	369	1K-8.2M	257K	57K
			Total Breach	427	1K-9M	327K	72K
	Hacker	2018	Crisis Services	30	1K-406K	69K	34K
			Total Breach	44	3K-7.4M	247K	38K
		2014-2018	Crisis Services	249	1K-7.1M	247K	58K
			Total Breach	285	1K-7.4M	337K	74K
	Malware/Virus	2018	Crisis Services	12	18K-356K	105K	63K
			Total Breach	17	5K-360K	81K	43K
		2014-2018	Crisis Services	120	1K -8.2M	249K	57K
			Total Breach	142	2K-9M	308K	70K
Large Companies	Hacker and Malware/Virus Combined	2018	Crisis Services	2	58K-10M	5M	5M
			Total Breach	2	58K-10M	5M	5M
		2014-2018	Crisis Services	28	10K-64M	6M	2.1M
			Total Breach	38	20K-64M	7.4M	2.7M
	Hacker	2018	Crisis Services	1	10M	10M	10M
			Total Breach	1	10M	10M	10M
		2014-2018	Crisis Services	17	10K-64M	6.7M	2.2M
			Total Breach	20	60K-64M	7.9M	2.6M
	Malware/Virus	2018	Crisis Services	1	58K	58K	58K
			Total Breach	1	58K	58K	58K
		2014-2018	Crisis Services	11	58K-33M	4.9M	2M
			Total Breach	18	20K-33M	6.9M	4.6M

Table 18

Rogue Employees and Malicious Insiders

In order to obtain a more accurate analysis of the impact of malicious insiders, claims that identified a rogue employee as the cause of loss were combined with claims indicating that a malicious insider was involved. The Financial Services sector lost more than $19M due to rogue employees, including more than $11M due to the theft of client data. Employees who accessed personal patient files cost the Healthcare sector $6M.

Rogue Employees and Malicious Insiders

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	5	1K -191K	46K	8K
		Total Breach	11	3K-216K	34K	18K
	2014-2018	Crisis Services	53	1K-1.5M	112K	40K
		Total Breach	80	1K-2.5M	151K	60K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	4	91K-5.7M	1.8M	691K
		Total Breach	6	111K-11.5M	4.3M	4.6M

Table 19

Lost and Stolen Devices

This study distinguishes claims for devices that were stolen from claims for devices that were lost. It also provides insight into the financial impact of device encryption and location of device theft.

During the earlier years of this decade, lost/stolen laptop events involving professional employees in healthcare and financial services made big headlines (and generated sizable cyber insurance claims). These incidents constituted data privacy violations. Device encryption is an effective loss mitigation solution to help prevent these types of data privacy breaches.

This year's dataset contained 15 claims associated with lost/stolen laptops, with six of those being encrypted. While the lower claims volume represents a positive trend overall, there is a more important point to be made. Among this particular claims population, the average cost for cases involving encrypted devices was a modest $35K, while for the ***average cost for unencrypted devices was six times that amount at $232K***.

Average Breach Costs for devices stolen from cars or homes were $46K, significantly lower than the $209K average for devices stolen from offices or facilities.

Lost and Stolen Devices

Revenue Size	Cause of Loss	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	Lost and Stolen Devices Combined	2018	Crisis Services	5	5K-90K	31K	20K
			Total Breach	20	3K-115K	32K	21K
		2014-2018	Crisis Services	70	1K-1.5M	78K	25K
			Total Breach	95	2K-1.5M	76K	27K
	Stolen Devices	2018	Crisis Services	4	5K-29K	16K	16K
			Total Breach	19	3K-100K	28K	16K
		2014-2018	Crisis Services	54	1K-1.5M	80K	25K
			Total Breach	76	2K-1.5M	77K	27K
	Lost Devices	2018	Crisis Services	1	90K	90K	90K
			Total Breach	1	90K	90K	90K
		2014-2018	Crisis Services	16	2K-355K	73K	11K
			Total Breach	19	3K-355K	73K	21K
Large Companies	Lost and Stolen Devices Combined	2018	Crisis Services	0			
			Total Breach	0			
		2014-2018	Crisis Services	2	10K-34K	22K	22K
			Total Breach	4	10K-2.5M	699K	142K
	Stolen Devices	2018	Crisis Services	0			
			Total Breach	0			
		2014-2018	Crisis Services	2	10K-34K	22K	22K
			Total Breach	3	10K-250K	98K	34K
	Lost Devices	2018	Crisis Services	0			
			Total Breach	0			
		2014-2018	Crisis Services	0			
			Total Breach	1	2.5M	2.5M	2.5M

Table 20

W-2 Fraud

W-2 fraud represents a specific type of data privacy breach in which copies of employee W-2 forms (which contain Social Security Numbers and sensitive pay data) find their way into the hands of people who are not authorized for that access.

The number of W-2 fraud claims has increased steadily each year from 2014 (8) to 2017 (48). In 2018, however, the number of W-2 fraud claims dropped to 11, ten for SMEs and one for large companies. Since claims for events in 2018 will continue to be collected in 2020 and 2021, that number will likely increase in future studies.

W-2 Fraud

SMEs

Time Period	Nature of Cost	Claims	Range	Average	Median
2018	Crisis Services	8	4K-94K	35K	31K
	Total Breach	10	10K-122K	49K	36K
2014-2018	Crisis Services	110	1K-413K	56K	28K
	Total Breach	112	1K-413K	66K	38K
Large Companies					
Time Period	Nature of Cost	Claims	Range	Average	Median
2018	Crisis Services	0			
	Total Breach	1	5K	5K	5K
2014-2018	Crisis Services	1	145K	145K	145K
	Total Breach	2	5K-165K	85K	85K

Table 21

W-2 fraud occurred via a surprising number of causes and in a variety of business sectors, with Professional Services, Financial Services, Education, Nonprofit, and Healthcare accounting for 70% of claims for SMEs. Not surprisingly, among Professional Services firms, those providing tax and payroll services experienced the greatest number of incidents.

Social engineering-related tactics were the most common causes of W-2 fraud. Well-meaning employees fulfilled requests for W-2 records that appeared to be legitimate, but were not. BEC and phishing accounted for 54% of SME W-2 fraud claims.

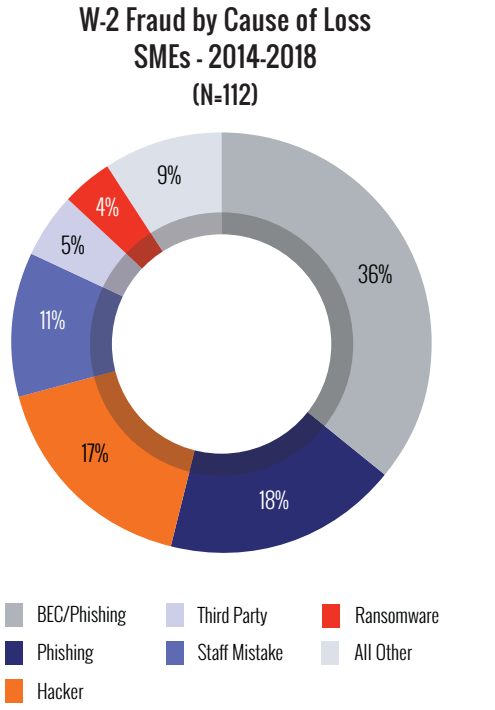


Figure 28

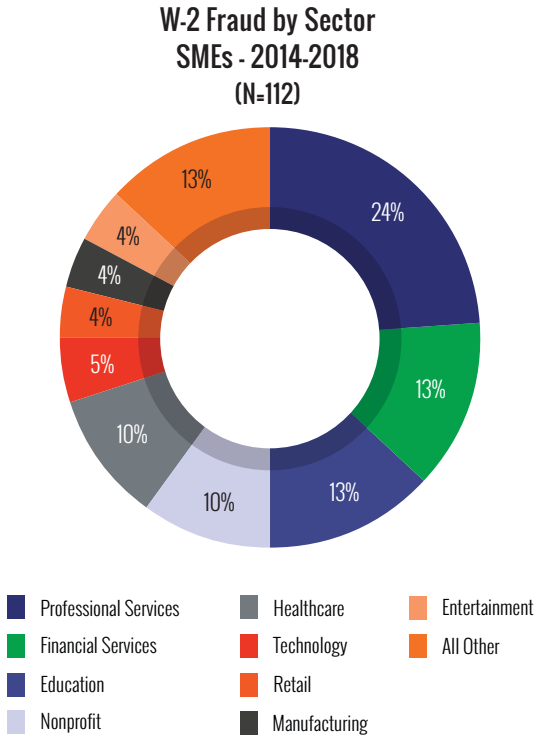


Figure 29

Banking Fraud

The investigation and prosecution of cyber-related banking fraud are extensions of existing banking criminal law. As a federal crime, cyber banking fraud may draw the attention of the Treasury Department, FBI, and local authorities.

The top four sectors impacted by banking fraud, which includes wire transfer and ACH fraud, were Professional Services, Manufacturing, Financial Services, and Retail. Due to the nature of their work, accounting and law firms often have access to client banking accounts. It is not surprising, therefore that they accounted for almost 40% of the banking fraud claims in the Professional Services sector.

Banking fraud losses were typically attributed to phishing, BEC, and social engineering. The yearly number of these incidents has been increasing: five in 2014, six in 2015, 14 in 2016, to 42 in both 2017 and 2018.

Banking Fraud

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Fraud Amount	34	2K-928K	134K	100K
		Crisis Services	14	4K-128K	42K	31K
		Total Breach	41	7K-938K	132K	105K
	2014-2018	Fraud Amount	78	2K-1M	166K	103K
		Crisis Services	58	1K-479K	68K	25K
		Total Breach	106	4K-1.4M	180K	105K
Large Companies	2018	Fraud Amount	0			
		Crisis Services	0			
		Total Breach	2	505K	505K	505K
	2014-2018	Fraud Amount	1	1.3M	1.3M	1.3M
		Crisis Services	1	107K	107K	107K
		Total Breach	2	505K-1.5M	990K	990K

Table 22

Distributed Denial of Service (DDoS) Attacks

For the 2019 dataset, the top three causes of loss for distributed denial of service (DDoS) events were hackers (69%), malware/virus (23%), and rogue employees (8%). None of these incidents included a third party, the cloud, or IoT, and none exposed data. Three involved a Bitcoin extortion; only one paid. One claimed a loss of ten thousand subscribers due to the web servers being down. Several others reported being offline but did not provide the number of hours. Three of the claims reported that the perpetrator had been apprehended and charged. All three were identified as rogue employees.

DDoS attacks have been around for many years and are among the easiest types of attacks to conduct. Although there are effective technologies for detecting and deflecting these attacks, they have been relatively expensive and many companies have yet to deploy them.

That may change over the next several years. Many vendors have developed more cost-effective solutions for defeating and mitigating DDoS attacked. How enthusiastically they will be embraced by the marketplace remains to be seen.

Denial of Service Attacks

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	10	4K-1.6M	221K	46K
		Total Breach	12	4K-7.5M	929K	154K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	1	10K	10K	10K
		Total Breach	1	60K	60K	60K

Table 23

Office Productivity Software Exploits

As cloud-based business applications have become more widely adopted, criminals have increasingly targeted them, including office productivity software like Microsoft Office 365 and SharePoint, as well as products from Peoplesoft and Workday. The attraction of these environments is that stolen user credentials can provide an entry point into an entire computing environment. Victims of these kinds of exploits included companies in almost every sector. Professional Services, Financial Services, Healthcare, and Manufacturing companies occupied the top four spots.

Office Productivity Software Exploits

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	23	12K-1.3M	182K	72K
		Total Breach	23	13K-3.4M	296K	85K
	2014-2018	Crisis Services	41	11K-1.3M	143K	70K
		Total Breach	42	13K-3.4M	247K	89K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	1	72K	72K	72K
		Total Breach	1	72K	72K	72K

Table 24

Losses Due to Non-Criminal Factors

In many cyber loss events, "blame" is not really a factor. Accidents and honest mistakes happen all the time, and sometimes they can be quite costly. Although it is probably impossible to eliminate the causes of loss listed below, they are ones that organizations can work to manage with reasonable investments and attention to policies/procedures.

- Staff mistakes
- Programming errors
- System glitches
- Negligence
- Mishandling of paper records
- Lost devices
- Legal actions – card brand, regulatory, civil

These categories of manageable risks are individually discussed in the following sections.

Staff Mistakes

Staff mistakes occurred for a variety of reasons. Many of the items listed above could be considered staff mistakes. On average, there have been 24 staff mistakes per year (21-28) for the five-year period 2014-2018. As a percentage of all claims in a year, staff mistakes have fallen from 13% in 2014 to 3-4% in 2017 and 2018.

Staff Mistakes

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	7	2K-90K	22K	10K
		Total Breach	25	2K-250K	30K	12K
	2014-2018	Crisis Services	87	1K-679K	51K	10K
		Total Breach	120	1K-2.5M	78K	25K
Large Companies	2018	Crisis Services	0			
		Total Breach	1	250K	250K	250K
	2014-2018	Crisis Services	1	218K	218K	218K
		Total Breach	4	100K-2.5M	813K	325K

Table 25

Programming Errors

Some claims categorized as staff mistakes or system glitches can also be identified as programming errors. Such errors are especially troublesome insofar as they often remain latent in effect, and the incidents arising from them might occur months or even years after the original error took place. Examples include misconfiguration of network hardware, firewalls and routers, as well as poor application-level coding technique that left networks, servers, and individual applications open to exploit.

While 2018 has been a quiet period thus far for programming errors, given the latency involved in detection or exploitation of these errors, future years might well reveal 2018 events that have not as yet been discovered.

In addition, it should be noted that the increasing reliance by programmers on third-party software libraries—that could contain and thus proliferate security flaws—may represent an aggregation risk for insurers.

Programming Errors

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	22	2K-679K	140K	40K
		Total Breach	24	2K-3.6M	305K	63K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	1	678K	678K	678K
		Total Breach	1	678K	678K	678K

Table 26

System Glitches and Hardware Failures

A review of claims categorized as system glitches and hardware failures showed that almost every claim categorized in this way was really a programming error. Claims for system/ hardware glitches are rare – only 10 since 2014 and 3 of those in 2018.

Nevertheless, this category is another that may represent aggregation risk for insurers. A handful of companies dominate the computer processing industry. A single flaw in one chip could affect hundreds of millions of computing devices.

System Glitches and Hardware Failures

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	3	28K-524K	209K	75K
		Total Breach	3	38K-933K	491K	501K
	2014-2018	Crisis Services	8	2K-524K	107K	33K
		Total Breach	10	2K-17.5M	1.9M	79K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	0			
		Total Breach	1	80M	80M	80M

Table 27

Mishandling of Paper Records

Although the mishandling of paper records continues to be a maddening and costly event, there were no new claims in 2018 for this cause of loss. Historically, these events have been caused by a failure to follow policy, although, on occasion, the fault lay with a third-party service.

Mishandling of Paper Records

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	21	1K-197K	35K	17K
		Total Breach	23	3K-600K	69K	25K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	2	3K-11K	7K	7K
		Total Breach	4	3K-100K	35K	18K

Table 28

Legal and Third-Party Actions

Legal actions took the form of card brand-initiated common point of purchase (CPP) investigations, regulatory actions, and civil actions. During the 5-year period, there were 29 claims for CPP investigations initiated by card brands. Many of these claims used the words "possible" or "suspected." Some of the claims involved an investigation by a card brand-mandated PCI Forensic Investigator (PFI) who, in many cases, determined that no compromise had occurred. Unfortunately, such investigation costs are not refundable by PCI upon determination of non-liability. The average cost of these claims was $52K.

Claims regulatory action costs included:

- Canadian Data Protection Laws for hosting customer information on servers in the United States (privacy)
- Confidentiality of Medical Information Act under HIPAA
- FTC enforcement actions due to PII and PHI exposure
- Threat Protection Act
- Unfair Deceptive Trade Practices Act

Claims for legal action costs included:

- Trademark and copyright infringement
- Trade secrets
- Theft of intellectual property (IP)
- Card brand/CPP investigations/PCI actions
- Negligence

Legal and Third-Party Actions

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	0			
		Total Breach	1	104K	104K	104K
	2014-2018	Crisis Services	58	1K-171K	33K	21K
		Total Breach	112	3K-10M	241K	51K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	2	11K-60K	35K	35K
		Total Breach	11	13K-5M	1.9M	1.6M

Table 29

Type of Data

Events that exposed Personally Identifiable Information (PII, including W-2 data), HIPAA-governed Protected Health Information (PHI), and Payment Card Industry (PCI) data constituted only 16% of claims for 2018. That resulted in a dramatic decrease in the five-year percentages of these types of events – 39% for the current five-year period 2014-2018, down from 55% for the prior five-year period 2013-2017.

The decrease is happening for two reasons: the increasing frequency of social engineering and ransomware events that do not expose records, and the dramatic drop in value of PII and PCI data on the dark web.

Last year's report introduced three new data classifications, the most important of which were Files–Critical and Files–Not Critical. These categories were created to more accurately characterize events that did not involve the exposure of personal data, such as ransomware events and network outages. Most ransomware events lock down computing resources, which could involve a single desktop PC or an entire network. In many cases, the victim of ransomware is critically impacted and unable to operate, even though no personal data may have been exposed. These are the kinds of events that fall into the category of Files–Critical.

Other kinds of events, also typically ransomware, have a lesser impact. In these cases, a victim might elect to wipe an infected machine clean, or even throw the machine away. These types of events are characterized as Files–Not Critical.

W-2 data as well as payroll data have further been defined as a sub-category of PII. W-2 data has been analyzed separately as well as combined with PII.

SMEs

As previously mentioned, social engineering and ransomware have become the dominant causes of loss since 2017. For this reason, it is no surprise that the Files–Critical category has the highest percentage of claims.

The following two figures illustrate the percentage of SME claims for each type of data.

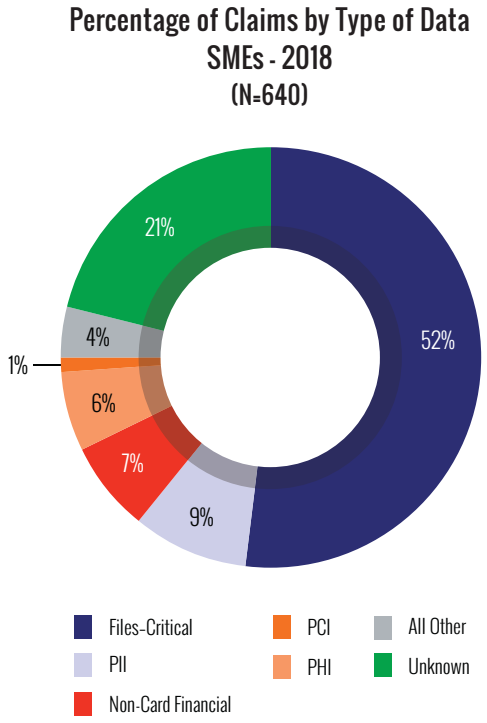


Figure 30

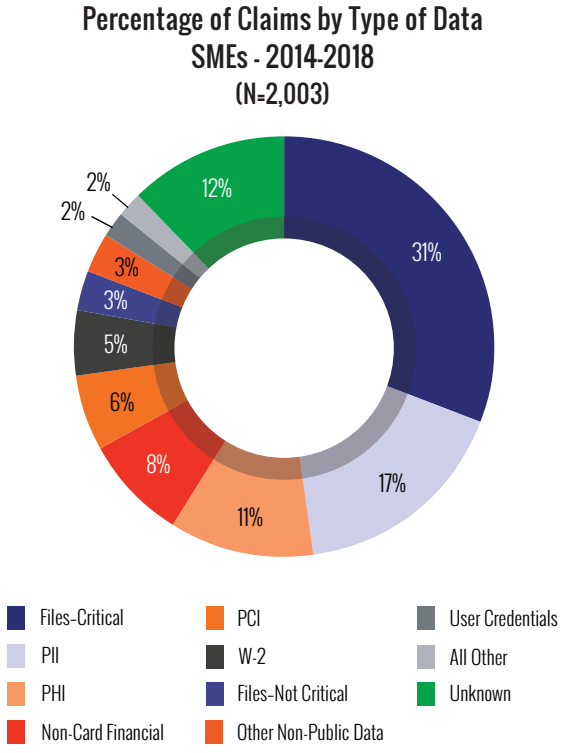


Figure 31

Table 30 below illustrates the financial impact to SMEs based on type of data exposed. Events that exposed PCI, PHI and PII data were quite costly, with PCI and PHI claims having two of the three highest average Breach Costs. With regard to total Breach Costs, the aggregate total for Files–Critical & DDoS events was more than double the aggregate total for the second most common type of data exposed, PII & W-2 combined.

Breach Costs by Type of Data
SMEs - 2014-2018

Type of Data	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Files-Critical & DDoS	627	1K	202K	49K	20.0M	127.0M	4
Files-Not Critical	66	1K	41K	24K	250K	2.7M	12
Intellectual Property & Trade Secrets	23	3K	388K	60K	5.0M	8.9M	2
Non-Card Financial	156	2K	141K	74K	1.4M	22.0M	7
Other Non-Public Data	55	3K	82K	36K	665K	4.5M	9
PCI	126	2K	392K	77K	6.9M	49.4M	1
PHI	222	2K	259K	54K	10.0M	57.6M	3
PII	342	1K	163K	54K	9.0M	55.8M	6
PII & W-2 Combined	449	1K	140K	50K	9.0M	62.8M	8
User Credentials	38	4K	167K	90K	933K	6.4M	5
User Online Tracking	1	25K	25K	25K	25K	25K	13
W-2 Data	107	1K	66K	37K	413K	7.1M	10
Unknown	240	1K	66K	25K	2.8M	15.8M	11

*Ranking is based on average Breach Cost

Table 30

Table 31 below provides average Crisis Services Costs, both by category and in total, when analyzed by type of data. Events that exposed PII, PHI and PCI data represent three of the four most costly kinds of events. Claims that involved the exposure of User Credentials & Logins/Passwords had the second highest average Total Crisis Services Costs.

Please note that not all claims include costs for every category of Crisis Services. This is why the averages of some individual categories could be greater than the average of the Total Crisis Services.

Average Crisis Services Costs by Type of Data
SMEs - 2014-2018

Type of Data	Forensics	Notification	Credit/ID Monitoring	Breach Coach	Other*	Total Crisis Services	Rank**
Files-Critical & DDoS	50K	21K	11K	14K	40K	59K	8
Files-Not Critical	30K	68K	26K	10K	6K	33K	12
Intellectual Property & Trade Secrets	62K			52K		66K	6
Non-Card Financial	28K	15K	7K	21K	90K	54K	10
Other Non-Public Data	35K		1K	39K	13K	64K	7
PCI	252K	69K	62K	50K	118K	288K	1
PHI	72K	153K	84K	35K	125K	195K	2
PII	69K	74K	35K	39K	49K	130K	4
PII & W-2 Combined	66K	59K	34K	34K	39K	111K	5
User Credentials	84K	24K	15K	33K	33K	131K	3
User Online Tracking	15K				10K	25K	13
W-2 Data	49K	10K	30K	19K	9K	56K	9
Unknown	22K	25K	7K	11K		37K	11

* Includes public relations, data restoration, and sometimes ransom payment and fraudulent wire transfer
**Ranking is based on average Total Crisis Services

Table 31

Large Companies

In large companies during the five-year period, events that exposed PII, PHI, and PCI data accounted for 69% of claims and over half of total Breach Costs ($262M of $433M).

Ransomware and social engineering events (Files–Critical & DDoS) accounted for another significant part of total Breach Costs.

Events that involved this type of data had the highest average Breach Costs by far ($14.4M). The next highest average Breach Costs were for events that exposed PII ($6.5M).

Data breaches at large companies exposed very large numbers of PII, PHI, and PCI records. PII breaches exposed almost 31M records on average. PHI breaches exposed 7.6M records on average. Breaches of PCI data exposed an average of 23M records. These numbers drove per-record costs down dramatically when compared to the overall averages reported above (Table 2). Excluding a small number of outliers in each category, the average costs per record for PII, PHI, and PCI events were $24, $40, and $36, respectively.

Percentage of Claims by Type of Data
Large Companies - 2014-2018
(N=78)

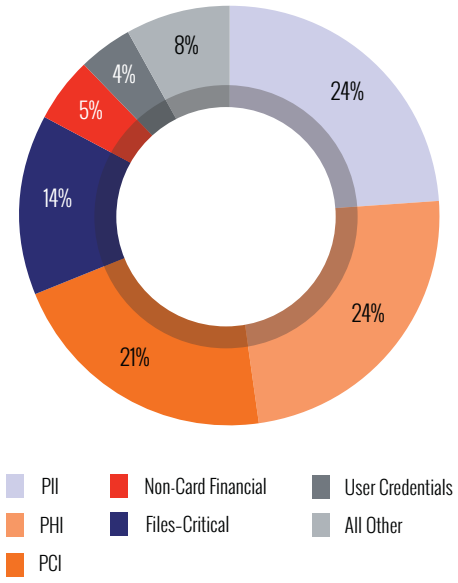


Figure 32

Breach Costs by Type of Data
Large Companies - 2014-2018

Type of Data	Claims	Minimum	Average	Median	Maximum	Total	Rank*
Files-Critical & DDoS	12	58K	14.4M	2.7M	80.0M	158.6M	1
Files-Not Critical	2	3K	359K	359K	716K	719K	9
Non-Card Financial	4	103K	1.4M	308K	5.0M	5.7M	7
Other Non-Public Data	1	4.1M	4.1M	4.1M	4.1M	4.1M	5
PCI	16	20K	4.9M	2.5M	16.8M	78.3M	4
PHI	19	10K	3.2M	2.0M	15.0M	60.6M	6
PII	19	13K	6.5M	678K	64.0M	123.0M	2
PII & W-2 Data	21	5K	5.9M	400K	64.0M	123.2M	3
User Credentials	3	77K	575K	172K	1,475K	1.7M	8
W-2 Data	2	5K	85K	85K	165K	170K	10

*Ranking is based on average Breach Cost

Table 32

Personally Identifiable Information (PII)

For purposes of this report, PII and W-2 data were analyzed together. As is the case in many categories, there is a dramatic difference between SMEs and large companies in average Breach Costs, both in 2018 (and $139K vs $5M) and for the five-year period. ($140K vs $5.9M).

Personally Identifiable Information (PII)

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	67	5K-1.3M	94K	53K
		Total Breach	69	5K-3.4M	139K	57K
	2014-2018	Crisis Services	425	1K-8.2M	113K	39K
		Total Breach	449	1K-9M	140K	50K
Large Companies	2018	Crisis Services	1	10M	10M	10M
		Total Breach	2	5K-10M	5M	5M
	2014-2018	Crisis Services	16	11K-64M	6.4M	327K
		Total Breach	21	5K-64M	5.9M	400K

Table 33

Protected Health Information (PHI)

Six percent of SME claims in 2018 and 11% for the five-year period involved the exposure of PHI data. For large companies, 24% of claims for the five-year period involved PHI exposure. The average Crisis Services and Breach Costs were down quite a bit in 2018 compared to the five-year averages.

Protected Health Information (PHI)

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	26	2K-1M	100K	35K
		Total Breach	41	2K-1.3M	90K	41K
	2014-2018	Crisis Services	170	1K-7.1M	195K	37K
		Total Breach	222	2K-10M	259K	54K
Large Companies	2018	Crisis Services	1	199K	199K	199K
		Total Breach	2	249K-250K	249.5K	249.5K
	2014-2018	Crisis Services	7	10K-5.7M	1.5M	199K
		Total Breach	19	10K-15M	3.2M	2M

Table 34

Payment Card Information (PCI)

As mentioned previously, there is a sizable discrepancy between the number of claims involving PCI-related data and the number of claims that included PCI fines. For the five-year period, there were 142 claims for exposure of PCI data, but only 21 claims for PCI fines.[14] Breach Costs were as high as $6.9M for SMEs and $4.9M for large companies.

Payment Card Information (PCI)

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	4	21K-64K	52K	62K
		Total Breach	4	21K-69K	54K	63K
	2014-2018	Crisis Services	114	600-5.9M	288K	62K
		Total Breach	126	2K-6.9M	392K	77K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	9	60K-4.9M	2.1M	2.0M
		Total Breach	16	20K-16.8M	4.9M	2.5M

Table 35

Files–Critical & DDoS

Files–Critical was introduced as a specific type of data in the 2018 report, assigned when ransomware, DDoS attacks, or other types of incidents disrupt an organization's ability to operate but does not expose any personal data. Events that locked out critical files were sometimes quite costly and included two of the most expensive claims in the dataset.

Files-Critical & DDoS

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	109	600-406K	48K	23K
		Total Breach	332	1K-7.4M	109K	44K
	2014-2018	Crisis Services	330	1K-1.6M	59K	29K
		Total Breach	627	1K-20M	202K	49K
Large Companies	2018	Crisis Services	1	58K	58K	58K
		Total Breach	3	58K-255K	154K	150K
	2014-2018	Crisis Services	7	10K-33M	6.1M	680K
		Total Breach	12	58K-80M	13.2M	1.7M

Table 36

[14] Data for 2018 will continue to be collected in 2020 and 2021.

Files–Not Critical

Files–Not Critical was another new classification in 2018. This data type was assigned to the same kinds of ransomware and disruption events as the Files–Critical category, but only when the event appeared to have a low impact on the organization's ability to conduct normal operations. Although these kinds of events were sometimes costly, for the most part, they were not.

Files-Not Critical

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	56	1K-194K	33	13K
		Total Breach	66	1K-250K	41K	24K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	2	2.6K-696K	349K	349K
		Total Breach	21	2.6K-716K	359K	359K

Table 37

Non-Card Financial

Non-card financial data includes the personal details, account numbers, and balances of a bank or brokerage account. It does not include PCI-related credit card data. Approximately 10% of the claims in the dataset involved the exposure or theft of non-card financial data.

Non-Card Financial

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	15	4K-128K	40K	27K
		Total Breach	44	7K-938K	128K	104K
	2014-2018	Crisis Services	101	1K-479K	54K	27K
		Total Breach	156	2K-1.3M	141K	74K
Large Companies	2018	Crisis Services	0			
		Total Breach	2	103K-505K	304K	304K
	2014-2018	Crisis Services	1	110K	110K	110K
		Total Breach	4	103K-5M	1.4M	308K

Table 38

Other Non-Public Data

Information that is not publicly available, and does not fit in one of the other categories, is classified as Other Non-Public Data. Examples include information about customers, business partners, and donors, as well as employee records and confidential financial information. These kinds of events accounted for less than 3% of the claims and approximately 1% of Breach Costs ($8.6M/$790M).

Other Non-Public Data

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	4	23K-240K	85K	38K
		Total Breach	4	33K-665K	206K	63K
	2014-2018	Crisis Services	1K-600K	64K	33K	27K
		Total Breach	3K-665K	82K	36K	74K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	1	1.2M	1.2M	1.2M
		Total Breach	1	4.1M	4.1M	4.1M

Table 39

Insider Involvement

For the five-year period, only 14% of SME claims involved the actions of insiders. Two-thirds of these (10% overall) were the result of unintentional insider actions and one-third (4%) involved the actions of malicious insiders. The aggregate total Breach Costs for malicious insider activity was small ($12M) and half that of unintentional insider activity ($25M).

This proportion of insider-related events is approximately half of what was reported in last year's report. Although the reasons for the decline are unknown, it is possible that increased cybersecurity investments have mitigated this kind of event.

Percentage of Claims - Insiders
SMEs - 2014-2018
(N=2,003)

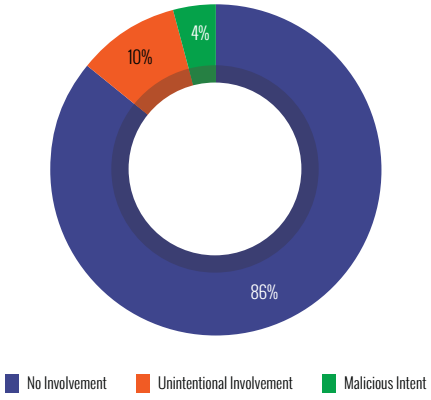


Figure 33

Total Breach Costs - Insiders
SMEs - 2014-2018
(N=2,003)

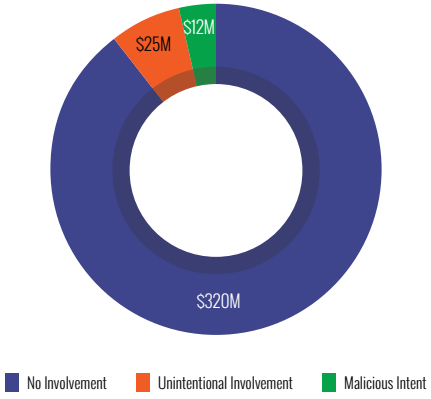


Figure 34

For large companies, 22% of claims in the dataset involved the actions of insiders. Two-thirds of these were the result of unintentional insider actions and one-third involved the actions of malicious insiders. The aggregate total Breach Costs for malicious insider activity was small and less than one-third that of unintentional insider activity.

Percentage of Claims - Insiders
Large Companies - 2014-2018
(N=78)

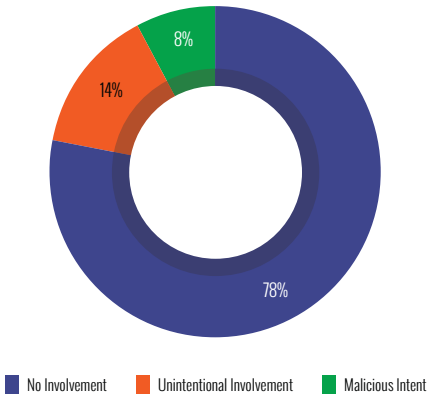


Figure 35

Total Breach Costs - Insiders
Large Companies - 2014-2018
(N=78)

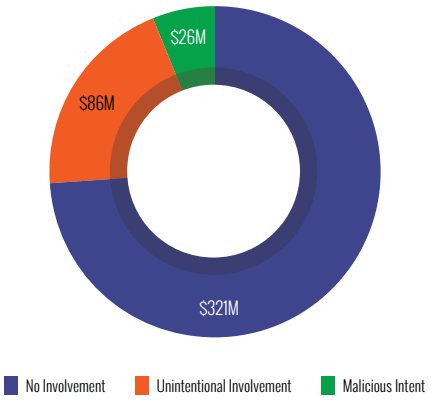


Figure 36

Third Parties

The involvement of third parties in cyber events has been well documented. Despite aggressive efforts in recent years to evaluate the security and privacy practices of supporting vendors and heightened scrutiny by regulators (e.g., EU GDPR), these types of events continue to occur.

Cyber events are typically caused by one of two types of third parties:

- **Vendors**: Vendors in a supply chain, web-hosting and cloud providers, personnel and payroll service providers, etc., cause cyber events either by their own errors or by being hijacked by criminals as an attack vector. The HVAC vendor to Target is a textbook example of how obscure this kind of relationship can be and still result in sizable cyber losses.
- **Service Providers**: Organizations that are third parties by the nature of the services provided include law firms, accounting firms, real estate firms, consulting firms, etc. When a cyber breach occurs in organizations like these, it will very likely impact one or more clients of the organization. The most significant example of this kind of relationship involves Anthem (79M records exposed), the health insurance giant. The dataset contains several claims involving a large breach in 2015 of U.S. health insurer.

The financial impact of cyber events caused by malicious third parties was much higher than the impact of events caused by the unintentional actions of third parties. That having been said, and as reflected in the Figures 37 through 40, financial losses attributable to third-party events constitute a very small percentage of overall losses in the dataset.

SMEs

For SMEs, 6% of the claims in the five-year period involved the unintentional (2%) or criminal (4%) actions of third parties. Third parties were not involved in the majority (94%) of events.

For SMEs, criminal actions accounted for $25M (7%) of Breach Costs.

Percentage of Claims - Third Parties
SMEs - 2014-2018
(N=2,003)

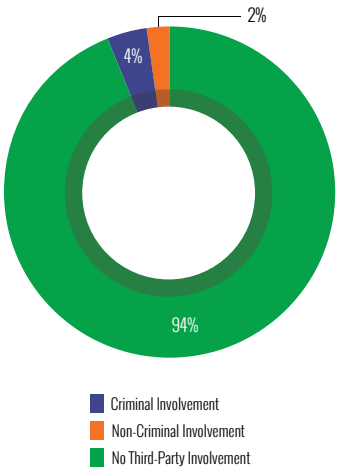


Figure 37

Total Breach Costs - Third Parties
SMEs - 2014-2018
(N=2,003)

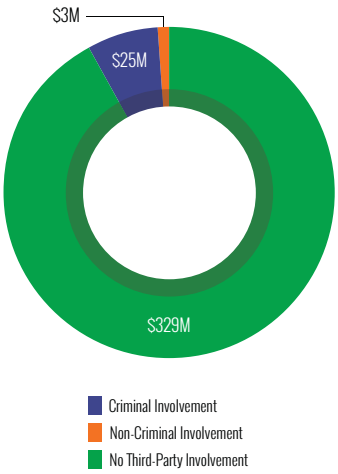


Figure 38

Third Parties - SMEs

Time Period	Type of Activity	Nature of Cost	Claims	Range	Average	Median
2018	Criminal	Crisis Services	4	1K-98K	49K	49K
		Total Breach	9	5K-119K	70K	87K
	Non-Criminal	Crisis Services	4	1K-75K	27K	15K
		Total Breach	5	2K-501K	111K	8K
2014-2018	Criminal	Crisis Services	69	1K-918K	72K	31K
		Total Breach	85	1.8K-10M	298K	60K
	Non-Criminal	Crisis Services	36	1K-355K	46K	29K
		Total Breach	41	1.8K-501K	76K	30K

Table 40

Large Companies

For large companies, 18% of the claims involved either unintentional (3%) or criminal actions (15%).

Percentage of Claims - Third Parties Large Companies - 2014-2018 (N=78)

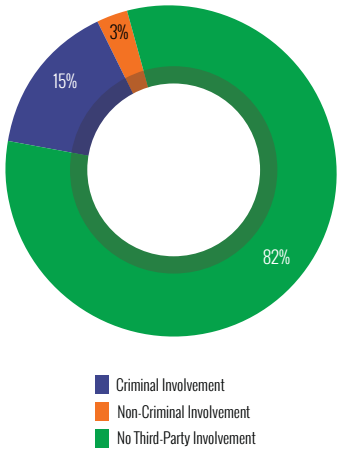


Figure 39

For large companies, criminal actions accounted for $23M (5%) of Breach Costs.

Total Breach Costs - Third Parties Large Companies - 2014-2018 (N=78)

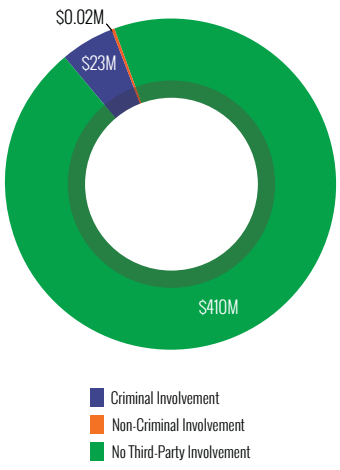


Figure 40

Cloud

Starting in 2017, study participants were asked to note and describe any cloud-related factors involved in a claim. To date, 44 such events have been identified: 43 for SMEs and one for a large company.

Cloud-related claims came from several business sectors, including Professional Services, Healthcare, Financial Services, and Manufacturing. The majority (75%) of these claims were due to a criminal act (hacking, malware/virus, ransomware, or rogue employee), while the remainder of claims (25%) were due to staff mistakes and programming errors.

Cloud-Related Events

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	14	11K-1M	150K	73K
		Total Breach	16	5K-1.25M	192K	84K
	2014-2018	Crisis Services	39	1K-1M	115K	56K
		Total Breach	43	5K-6.6M	294K	78K
Large Companies	2018	Crisis Services	0			
		Total Breach	0			
	2014-2018	Crisis Services	1	2.7M	2.7M	2.7M
		Total Breach	1	2.7M	2.7M	2.7M

Table 41

Internet of Things (IoT)

For the first time in 2018, study participants were asked to note if a claim involved IoT[15] devices. So far, 16 claims have been submitted for IoT-related events. Of these, one involved a hacking event that utilized a photocopy machine to compromise a network and execute W-2 fraud. Another involved the malicious use of data copied from a cell phone by a retail cell phone store employee. Both events resulted in moderately small settlements.

IoT-Related Events

Revenue Size	Time Period	Nature of Cost	Claims	Range	Average	Median
SMEs	2018	Crisis Services	8	11K-125K	45K	34K
		Total Breach	8	16K-130K	47K	36K
	2014-2018	Crisis Services	15	9K-125K	42K	35K
		Total Breach	16	9K-130K	48K	41K

Table 42

To date, no IoT-related claims for large companies have been submitted for this study.

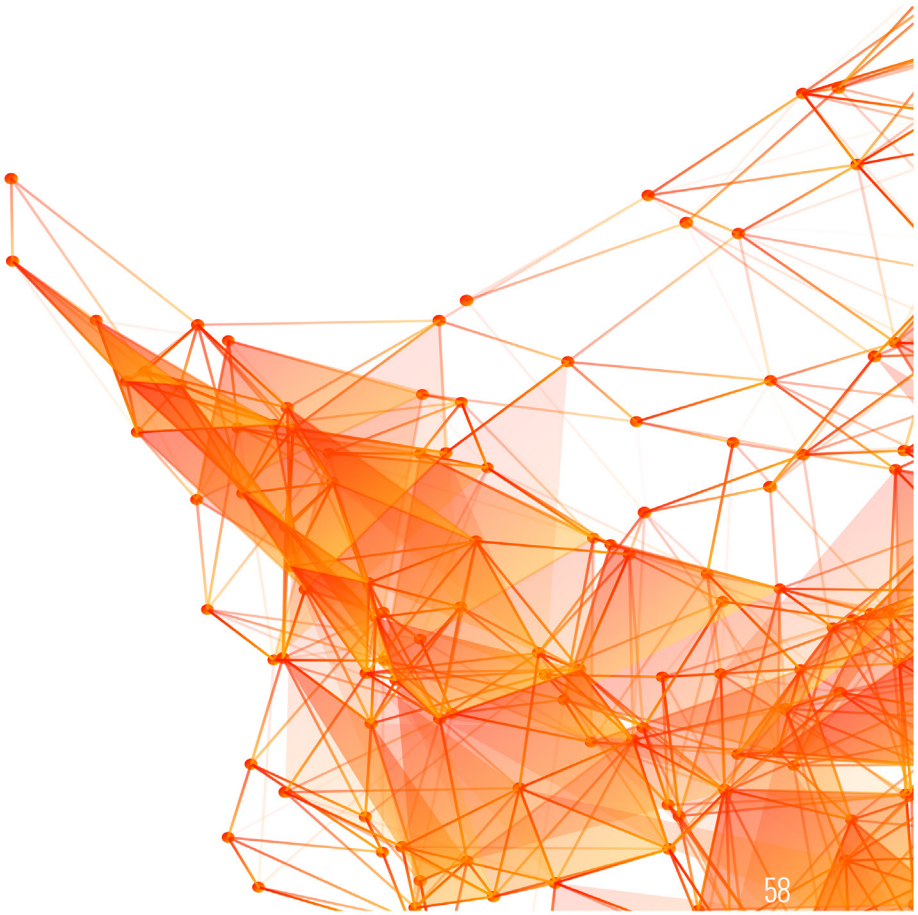
[15] It was left to study participants to define what constitutes an IoT device.

Conclusion

The cyber claims studies published by NetDiligence® represent 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. Almost 1,100 new claims were submitted this year—a 100% increase over last year—and were added to an existing dataset of over 1,000 claims. The result is one of the most comprehensive, representative, and objective datasets of cyber claims events, including their causes and monetary impacts, in existence.

As more and more insurers and brokers participate in this study and share even more claims and more information about each claim, the value of the study will increase. For the benefit of the industry overall, underwriters are encouraged to participate in next year's study. 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 2019 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:

- Dave Chatfield, Business Impact Analyst – Vice President & Chief Operating Officer, NetDiligence
- Heather Osborne, Sponsorships – Director of Global Events & Programming, NetDiligence
- Sharon Lyon, Publisher – President, Lion's Share Marketing Group, Inc.

Sponsor – RSM US

Growing Confidence Conflicts with Rising Cyber Concerns

Cybercrime has become a reality for the middle market. In fact, 15% of executives surveyed for RSM's 2019 Cybersecurity Special Report indicated that their organization has experienced a data breach in the last year, a significant jump from 5% just four years ago. In addition, 55% of middle market executives stated that an attempt to illegally access their companies' data or systems is either "very likely" or "somewhat likely" this year.

Despite more middle market companies experiencing a data breach or other cyber incident in the last year, and rising levels of concern over future attacks, almost all of the executives polled in RSM's research are confident in their current security measures. RSM's survey found that 93 percent of middle market executives are confident in their organization's measures to safeguard sensitive customer data or their own environments for the second consecutive year. While the number of reported breaches has tripled over the last five years, the level of confidence expressed by executives has actually grown by 18 points. This creates a potentially dangerous situation where executives have a false sense of security, seeing their peers falling victim to attacks but fully believing that "it can't happen to us."

Increased spending on information security is one potential reason for a high level of confidence. We have found that middle market companies are indeed making larger cybersecurity investments, but many need to implement more defined plans to ensure the right products and services are chosen and appropriate changes are made to their environment and business processes.

In addition, many middle market companies have aligned their processes to an established information technology security framework, whether due to regulatory compliance obligations or in an effort to improve their security posture. However, while mapping controls and functions to one of these frameworks is an effective first step, it does not mean that an organization is fully secure. These standards are meant to provide a strong foundation for information security, but companies must also consider several additional elements based on their specific industry and business objectives. Adopting a security framework can provide a sense of security, but not further adjusting it to the business can create security gaps.

Finally, communication breakdowns can occur among executives, the board and the people on the ground who are implementing security processes and controls. Sometimes what is communicated to the board is a vastly different view than the perception of security inside the data center. Organizations must ensure their stakeholders are on the same page from top to bottom to properly understand and address potential security issues.

Our research shows that the threat to the middle market is growing, but the organizations have only become more confident in current protections. Generally, companies have taken steps to improve cybersecurity, but criminals are becoming more sophisticated and determined. Cyberthreats are going to continue to evolve and attackers will continue to get smarter. Middle market businesses must ensure that security investments, controls and communications align with rising threats, and that current actions do not create a false sense of security.

About RSM US

RSM US LLP is the leading provider of audit, tax and consulting services focused on the middle market, with nearly 11,000 people in 87 cities and four locations in 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 41,000 people in 116 countries. RSM uses its deep understanding of the needs and aspirations of clients to help them succeed. For more information visit https://rsmus.com/

Sponsor – Cozen O'Connor

Cybersecurity Risk in the World of the Internet of Things

Now in its ninth year, the NetDiligence *Cyber Claims Study* shows that cyber risk management is more important than ever. With the explosion of the Internet of Things ("IoT"), the world is interconnected like never before. There are more internet-connected devices than there are people. Emerging 5G networks, with their faster speeds and increased bandwidth, have the potential to further fuel the spread of IoT devices. They will also allow many more IoT devices to connect to the Internet through the cellular network, rather than having to connect through a WiFi network or a separate cellular enabled device.

Every IoT device presents a potential access point for a malicious actor to attack a system to shut it down or to steal sensitive data. To make matters worse, IoT devices rarely contain antivirus software and they are notoriously difficult to update or patch should a security vulnerability be discovered. IoT devices present a security risk that cannot be overlooked.

Moreover, IoT devices often collect biometric information, some of the most sensitive personally identifiable information out there. Fitness trackers collect health statistics, doorbells and phones contain facial recognition software, and smart speakers can identify users by their voiceprints. This information is fundamentally different from traditional PII, such as social security numbers or bank account numbers. Social security numbers and bank account numbers can be changed if compromised. Biometric information, on the other hand, is not easily changed, if it can be changed at all.

To be sure, states and nations are increasingly moving to regulate the collection and use of biometric data. Within the next several years, it is likely that companies will face a patchwork of laws setting out procedures they must follow before they collect biometric data, limiting what they can do with it, and controlling who they must notify in case of a breach. Given the uniqueness of biometric data, these laws will be substantially more restrictive than laws currently in force regulating the collection and use of personal data more broadly.

Given this state of affairs, companies must be proactive with their cyber risk management program. Cybersecurity must be a board-level priority with buy in across all levels of management. Companies should be encouraged to utilize seal programs and certifications to ensure that their cyber risk management programs comply with or exceed industry standards. And companies must regularly review and assess their cyber risk management programs to keep them ahead of emerging technologies and risks.

The proliferation of IoT devices certainly has the potential to change our daily lives for the better. But it also presents substantial privacy and data security risks. A company's success will depend largely on its ability to anticipate, recognize, and mitigate those risks before they come to fruition.

About Cozen O'Connor

Cozen O'Connor has a multidisciplinary team of highly skilled and nationally regarded attorneys who focus on all aspects of privacy and data security counseling and litigation. We help companies protect data, comply with regulations, and respond to investigations and litigation. Ranked among the top 100 law firms in the country, Cozen O'Connor has more than 750 attorneys in 27 cities across two continents. A full-service firm with nationally recognized practices in litigation, business law, and government relations, our attorneys have experience operating in all sectors of the economy. Our diverse client list includes global Fortune 500 companies, middle-market firms poised for growth, ambitious startups, and high-profile individuals. cozen.com

About NetDiligence®

NetDiligence® is a leading provider of Cyber Risk Readiness & Response services. We have been providing cyber risk management services and software solutions to the cyber insurance industry, both insurers and policyholders, since 2001.

Our Cyber Risk Summit conferences and our cyber advisory groups serve as platforms for insurers, legal counsel, and technology specialists to exchange knowledge. 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.

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, including:

Vendor Risk Management (VRM) — SaaS

Companies that use third-party vendors to manage systems or sensitive customer/patient data need to conduct due-diligence on the cybersecurity practices of the vendors they use. QuietAudit VRM eliminates the time-consuming and insecure practice of using spreadsheets to collect detailed information about vendor security practices. QuietAudit VRM makes monitoring your vendors more manageable, more efficient, and more secure. Reporting includes an online dashboard and a "scorecard" for each vendor.

Underwriting Loss Control (ULC) — SaaS

Our QuietAudit Underwriting Loss Control (ULC) module makes due-diligence and control verification more efficient. QuietAudit ULC helps insurers gather, assess and "score" a client's data security and privacy safeguards. The module comes pre-loaded with a survey that gauges a client's practices against ISO and NIST. Licensors can customize the survey, if desired.

eRiskHub® — SaaS

The eRiskHub® portal, powered by NetDiligence, is an effective way to help both insurers and their clients combat cyber losses with minimal, controlled and predictable costs. 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 minimize the effects of breaches on their organizations. 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.

Breach Plan Connect® — SaaS

Breach Plan Connect® provides step-by-step guidance to help companies develop a comprehensive, yet actionable, data breach response plan. The software comes loaded with a plan that companies can easily customize for their organizations. NetDiligence also hosts the plan, so employees can access it at any time, from anywhere, on any device. Breach Plan Connect includes a comprehensive default data breach response plan, plus an online "Build Your Plan" tool that guides an organization step by step in customizing the default plan. This SaaS offering also includes an Incident Tracking Report and an Incident Response Checklist.

Contact Us

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

NetDiligence®

Study Methodology

In 2019, we asked the major underwriters and carriers of cyber insurance to submit claims information based on the following criteria:

- The event occurred in 2016, 2017, or 2018.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to 80 individuals at 53 organizations in the United States, Canada and the United Kingdom. From this group, 17 individuals representing 17 organizations provided 1,098 analyzable new claims, using the proprietary NetDiligence® claims data collection worksheet.

The 2019 report also included data from NetDiligence® studies published in 2015-2018, representing 1,008 events that occurred in 2014, 2015, 2016 and 2017. After the elimination claims that were less than $1,000, the combined dataset included 2,081 events, each one, a data breach insurance claim. This number represents an almost 100% increase in the number of claims analyzed compared to last year.

There were 2,016 claims in the dataset from American organizations, 11 claims from Canadian organizations, and 24 claims from organizations in the United Kingdom. There were 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 20 claims in the dataset.

When factoring in SIRs, we were able to calculate total data Breach Costs to date for all 2,081 (100%) of the claims in the dataset. In addition, 787 claims (38%) specified the number of records exposed and 1,379 claims (66%) included an accounting of Crisis Services Costs.

We calculated Per Record costs for all claims where the number of records exposed was provided (N=787). 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).

1,637 (79%) of the claims in the dataset were flagged as closed, 425 (20%) as open and 19 (1%) as unknown claim status. 1,487 (71%) of the claims were for primary coverage, 42 (2%) for excess coverage and 552 (27%) had an unknown, but most likely primary coverage level.

There were 262 claims in the dataset for which the revenue size of the organization was unknown. After comparing the distribution of breach 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 much larger than ever before, is a small subset of all breaches. Some of the data points are lower than other studies because we focus on claims payouts and Breach Costs for specific breach-related expenses and do not factor in other financial impacts of a breach, including in-house investigation and administration expenses, customer defections, opportunity loss, etc.
- 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 breach has costs at least $X, but we 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 breach, including amounts that were excluded due to policy provisions. While a few participants in 2017 provided these estimates, a greater number of participants did so in 2018 and 2019, thereby increasing our ability to understand the true costs of a breach.
- The numbers are empirical as they were supplied directly by the underwriters who paid the claims.
- 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."
- There is no attempt here to consider whether records associated with the same person/entity appear multiple times in the dataset. Given the anonymized state in which we receive these records, there is no possible way for us to do so.

It is important to note that 20% of the claims submitted for this study remain 'open'. Therefore, aggregate costs as presented in this study include "payouts to-date" and "Breach 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.

NetDiligence®

P.O. Box 204, Gladwyne, PA 19035 • 610.525.6383 • management@netdiligence.com