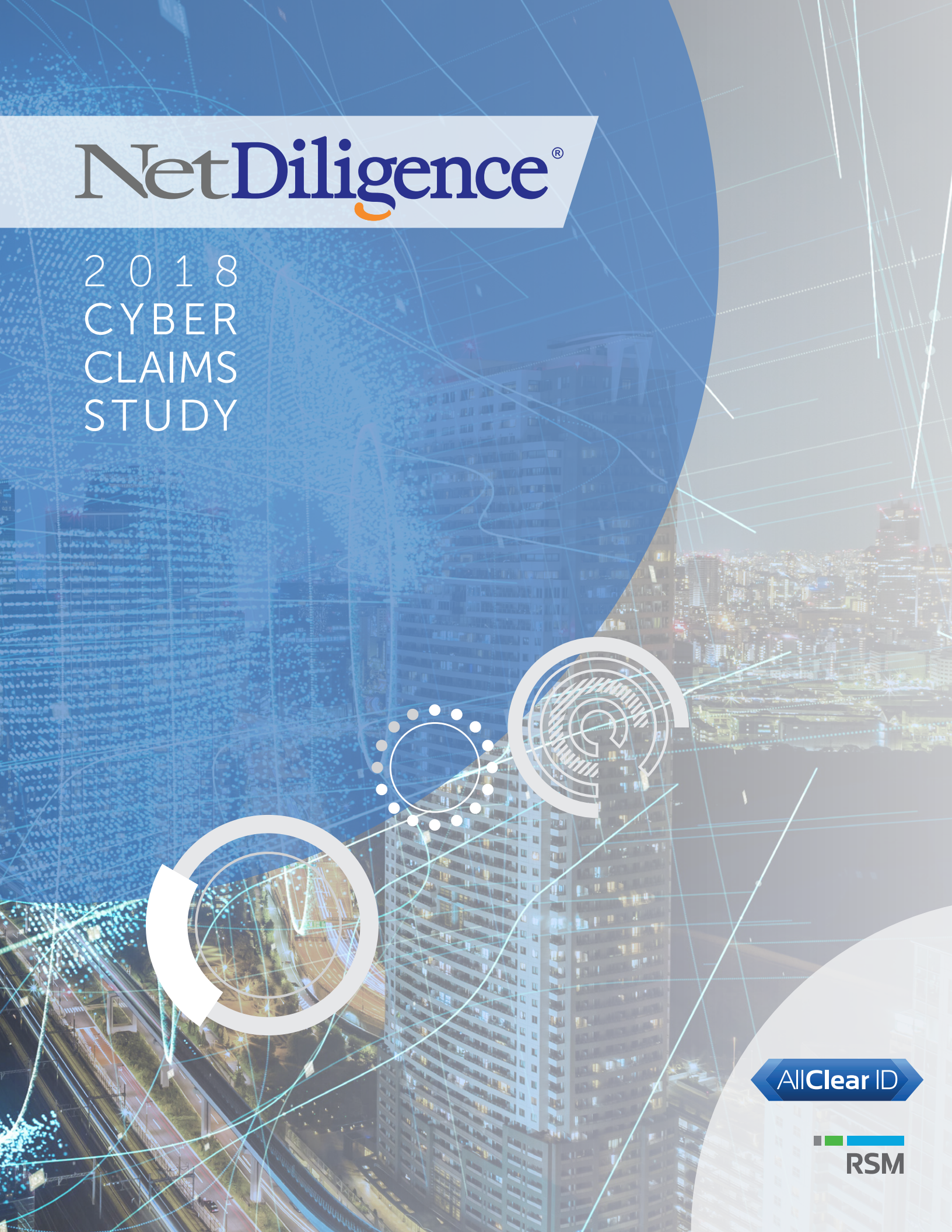
NetDiligence®

2018 CYBER CLAIMS STUDY



AllClear ID

RSM

Contents

Introduction

The eighth edition of the *NetDiligence® Cyber Claims Study* offers insights for business innovation. In the same way that a business gains operational perspective by going through an audit, both the insurer and the insured can use the findings of this research to inform decision making and risk management.

By the Numbers

- 1,201 claims analyzed, arising from incidents occurring from 2013–2017
- 298 claims analyzed arising from incidents occurring in 2017
- Over 500 new claims collected in 2018, from incidents occurring from 2015–2017
- 85% of the claims were from smaller organizations (< $2 billion in revenues)

The data from these claims have been aggregated and analyzed from many angles, including number of records exposed, crisis services cost, total breach cost and per-record cost. In addition, the study includes more than twenty categorizations of the data, including analyses by type of data, sector, revenue size, and cause of loss; losses caused by business interruption; losses for incidents that exposed no records; losses caused by criminal and non-criminal activity; and losses caused by a third party.

"Organizational stakeholders need to understand the potential financial impact of a breach when deciding how much they want to invest in security. With claims impacting organizational revenue sizes of less than $50M and more than $100B, the NetDiligence® study shows that no company is immune to cyber criminals. It is time that organizations accept how valuable their data is to attackers and why it is so important that they spend the time and effort necessary to protect that data."

Daimon Geopfert
National Leader of Security, Privacy, and Risk Services
RSM US LLP

Key Findings

Records

- **Records Exposed:** average = 1.2M, median = 1K
- **Per-Record Cost[1]:** average = $308, median = $42.58

Organization (Company) Size

- **Predominantly SMEs:** 85% less than $2B in Revenue

Overall Cost

- **Total Breach Cost:** average = $603.9K, median = $61.2K
- **Crisis Services Cost:** average = $307K, median = $40K
- **Large Company Breach:** average = $8.8M, median = $5M

Legal Cost

- **Defense:** average = $106K, median = $17K
- **Settlement:** average = $224K, median = $58K
- **Regulatory Defense:** average = $514K, median = $84K
- **Regulatory Fines:** average = $18K, median = $11K

Business Interruption Cost

- **All Cost:** average = $2M, median = $50K
- **Recovery Expense:** average = $957K, median = $30K

Sectors Affected (top 4)

- **Professional Services:** average = $168K, median = $43K
- **Healthcare:** average = $555K, median = $68K
- **Financial Services:** average = $854K, median = $50K
- **Retail:** average = $1.2M, median = $94K

Cause of Loss (top 4)

- **Hackers:** average = $1.05M, median = $114K
- **Ransomware:** average = $229K, median = $53K
- **Malware/Virus:** average = $1.2M, median = $93K
- **Lost/Stolen Laptop/Device:** average = $195K, median = $41K

[1] 90% of events (eliminating bottom and top 5%)

An Overview of the Data

Distribution of Claims by Year of Incident

In this year's study, 1,201 cyber claims were analyzed for incidents dating from 2013–2017. The overall distribution of claims is depicted in Figure 1. The number of claims collected and analyzed per year increased from 175 in 2013 to approximately 300 in both 2016 and 2017.

Percentage of Claims by Date of Event: 2013–2017

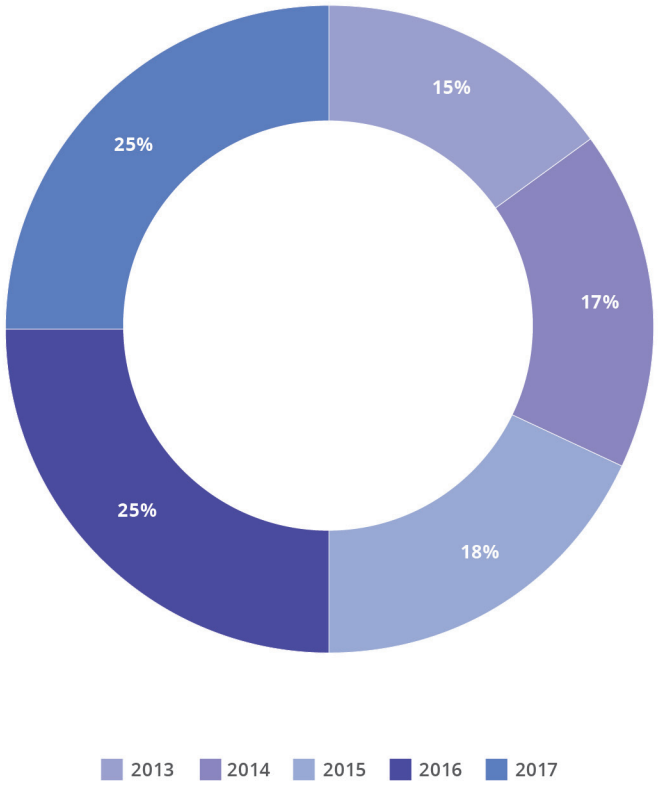


Figure 1

Exposed Records

Of the 1,201 claims in the dataset, 627 were events that exposed 762M records. The average number of records exposed varies substantially from year to year. The higher numbers in 2013, 2014 and 2015 were driven by a few breaches that exposed millions of records. The data for 2016 and 2017 contained fewer breaches that exposed large numbers of records, resulting in much lower averages.

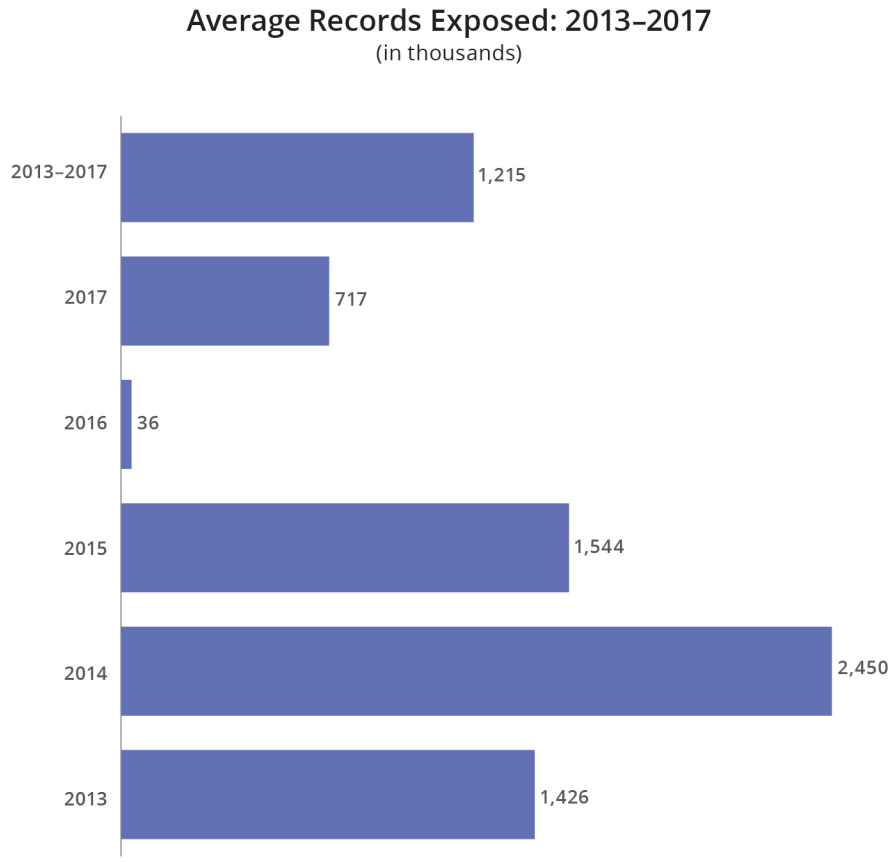


Figure 2

With the exception of breaches in 2016, the average number of records exposed per year was quite high. However, the medians were very low, ranging from 500 to 2,300 records, with a 5-year median of 1,000 records.

Breach Cost

Total Breach Costs, inclusive of Self-Insured Retention (SIR), ranged from a low of $110 to a high of $80M. Figure 3 depicts the total Breach Cost year by year and for the 5-year period 2013–2017. Figure 4 depicts the average and median Breach Cost for the same period.

Note that the averages were influenced by some very expensive claims. This was especially true for 2017, as there were 5 claims ranging from $6M to over $60M. The median Breach Cost ranged from $39K to $103K, with a 5-year median of $61K.

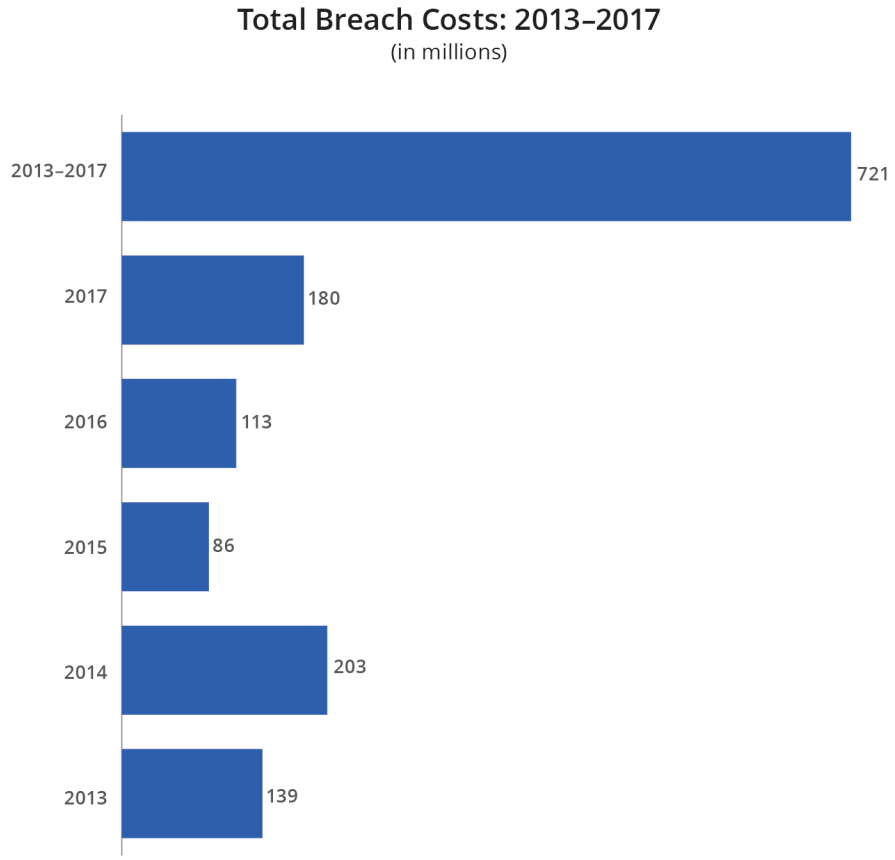


Figure 3

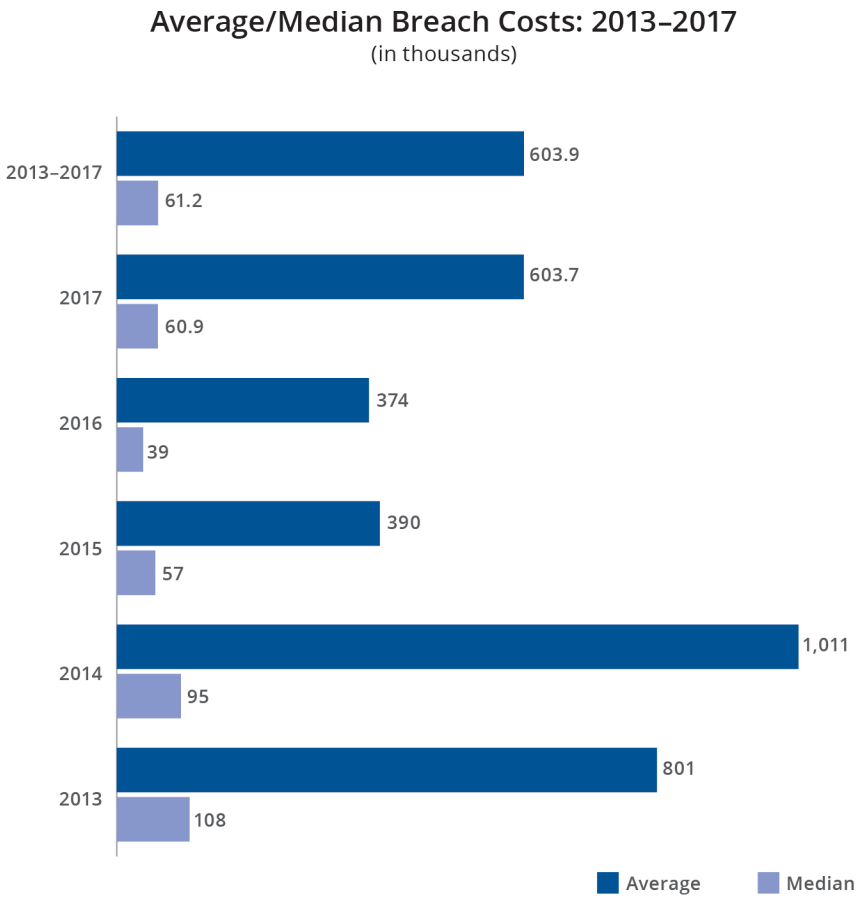

Average/Median Breach Costs: 2013–2017
(in thousands)
2013–2017
603.9
61.2
2017
603.7
60.9
2016
374
39
2015
390
57
2014
1,011
95
2013
801
108
Average
Median

Figure 4

Crisis Services Cost

Over the 5-year period 2013–2017 Crisis Services Cost ranged from a low of $14 to a high of $64M. In 2017, total Crisis Services Cost ranged from $130 to $64M. Figure 5 shows the average and median Crisis Services cost.

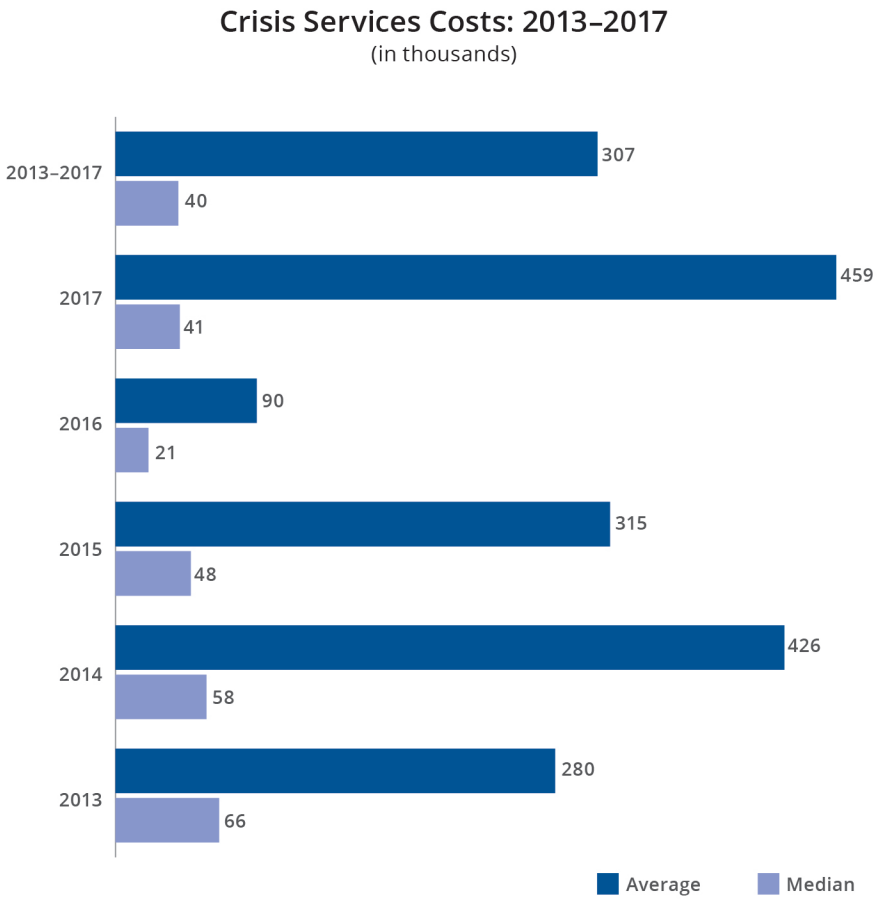


Figure 5

Legal Defense and Settlement

For the 5-year period 2013–2017, the dataset contains 134 claims with costs for Legal Defense and 74 claims with costs for Legal Settlement. For defense, the amounts ranged from $319 to $2.5M. For settlement, the amounts ranged from $1,500 to $4.8M. Figure 6 depicts the average and median cost for each category.

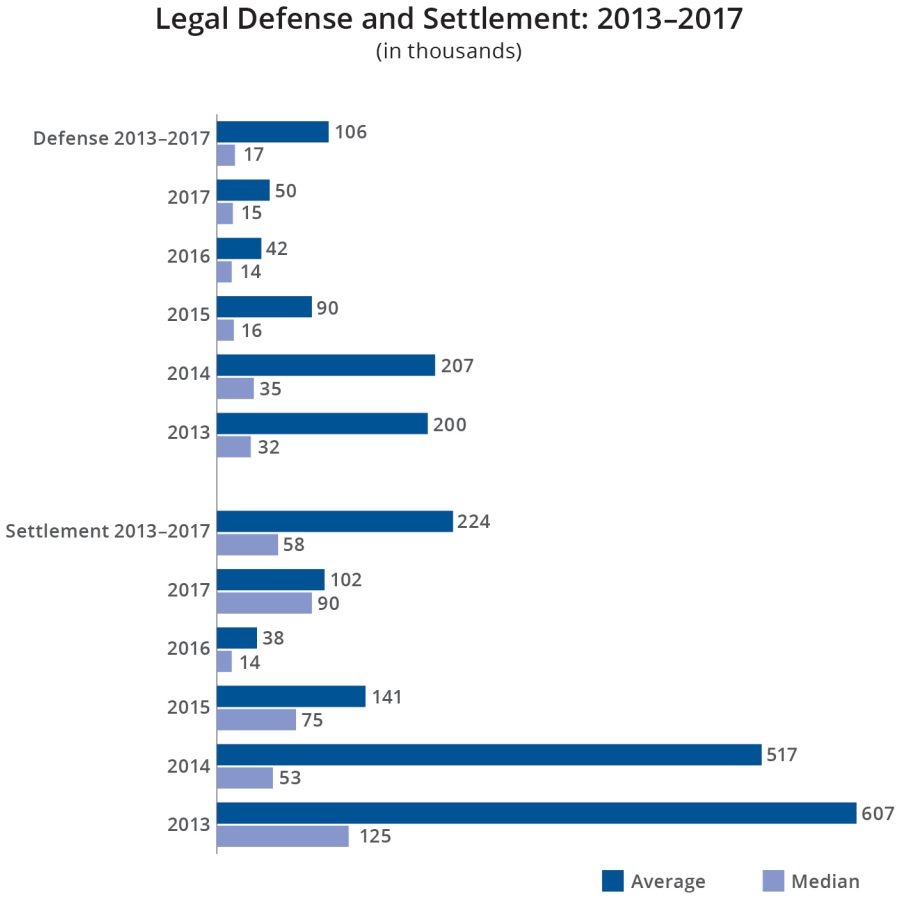


Figure 6

Regulatory Defense and Fines

For the 5-year period 2013–2017, the dataset contains 16 claims with amounts for Regulatory Defense and 8 claims for Regulatory Fines. For defense, the amounts ranged from $2K to $5.8M. For regulatory fines, the amounts ranged from $5K to $60K.

There have been few claims per year since 2013 for regulatory defense and only 2 claims before 2017 for regulatory fines—6 of 8 claims for regulatory fines occurred in 2017.

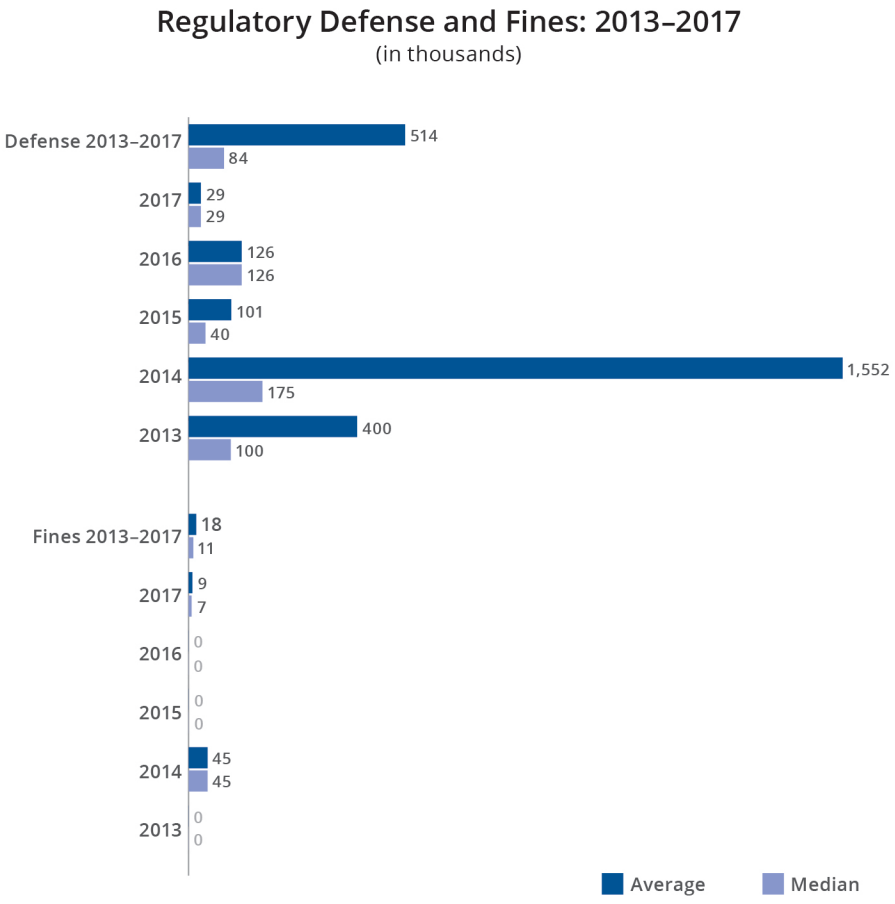


Figure 7

PCI Fines

Only 23 claims in the dataset included PCI fines. The fines ranged from $3K to $6.9M and totaled $14M. Aggregated Total Breach Costs for those claims was $24M. Two claims were especially costly: $5.7M and $11.8M. In addition to large PCI fines, both organizations incurred significant crisis services costs.

Nearly half of the claims involved legal action by a Card Brand or by CPP (Common Point of Purchase) investigations. The business sectors most affected were Retail and Hospitality.

Year by year average and median PCI fines varied widely, as illustrated in Figure 8.

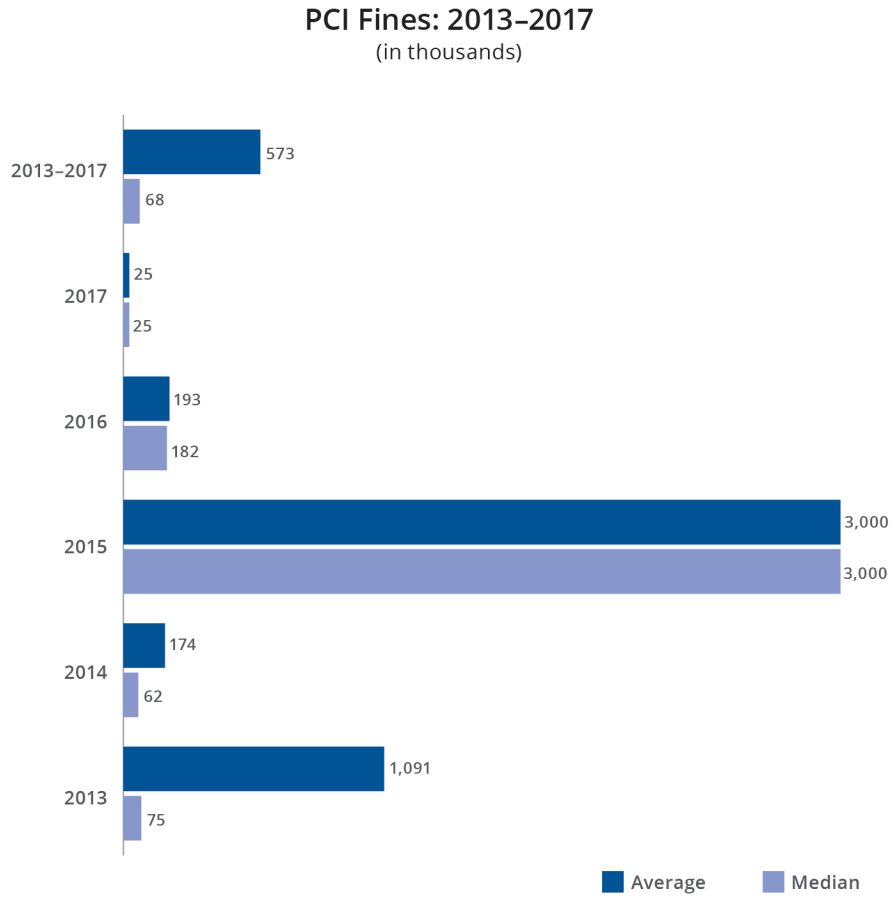


Figure 8

Lost Business Income and Recovery Expense

Of the 1,201 claims in the dataset, 68 included Lost Business Income (N=40) and/or Recovery Expense (N=28). The data collected showed increased service disruptions in 2016 and 2017 due to the increased frequency of ransomware and system glitches.

Lost Business Income claims ranged from $2,500 to $60M. Recovery Expense claims ranged from $3K to $20M. The average and median values for these categories are depicted in Figure 9.

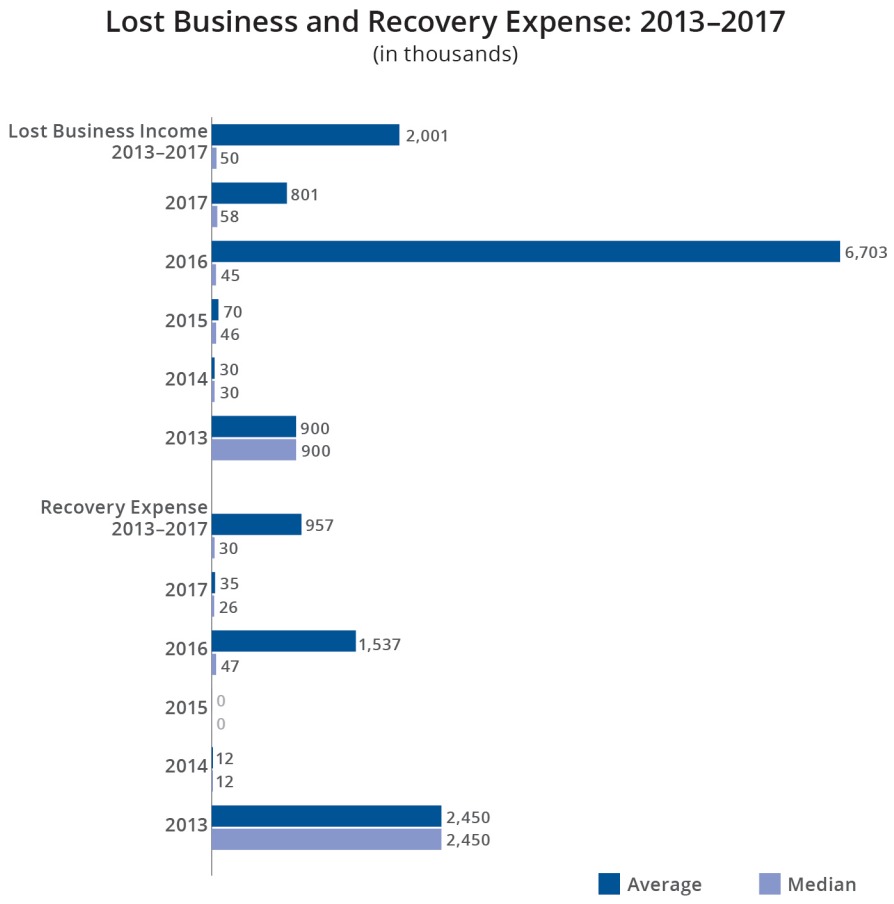


Figure 9

Per Record Cost

Average cost per record is heavily influenced by outliers at both ends of the spectrum. For example, the dataset contains per record costs ranging from $0.001 to $1.6M. The first of these involved a data breach with millions of records; the second involved a settlement for exposing the protected health information of one person.

To understand the outsized influence these outliers can have, Table 1 displays costs per record based upon 100%, 95%, 90% and 80% of the data. The results highlight the variances in the averages and the consistency in the median value.

Per Record Costs—5 Year Average 2013–2017

Percent of Data	Claims	Minimum	Average	Median	Maximum
100%	620	0.001	5,233	42.58	1,603,800
95% (2.5–97.5 percentiles)	588	0.30	627	42.58	30,000
90% (5^{th}–95^{th} percentiles)	558	0.82	308	42.58	6,169
80% (10^{th}–90^{th} percentiles)	496	1.87	163	42.58	1,433

Per Record Costs—2017 only

Percent of Data	Claims	Minimum	Average	Median	Maximum
100%	115	0.001	776	47.52	40,000
95% (2.5–97.5 percentiles)	109	0.82	263	47.52	6,250
90% (5^{th}–95^{th} percentiles)	103	1.29	169	47.52	1,450
80% (10^{th}–90^{th} percentiles)	91	2.71	108	47.52	750

Table 1

Note: Soft costs, brand and reputation damage, and stock price devaluation are not specifically collected as part of this study, and therefore are not factored in to the costs per record presented here.

Recordless Events

A critical finding of the study was the prevalence of "recordless" events, representing 39% of the claims in the dataset. Examples included most ransomware, denial of service (DDoS) and theft of money-related claims. The largest claim in the dataset ($80M) was caused by a network outage involving no exposure of records.

The average Breach Cost associated with recordless events was somewhat lower than for events that exposed records, however the average Crisis Services Cost for events that exposed records was higher.

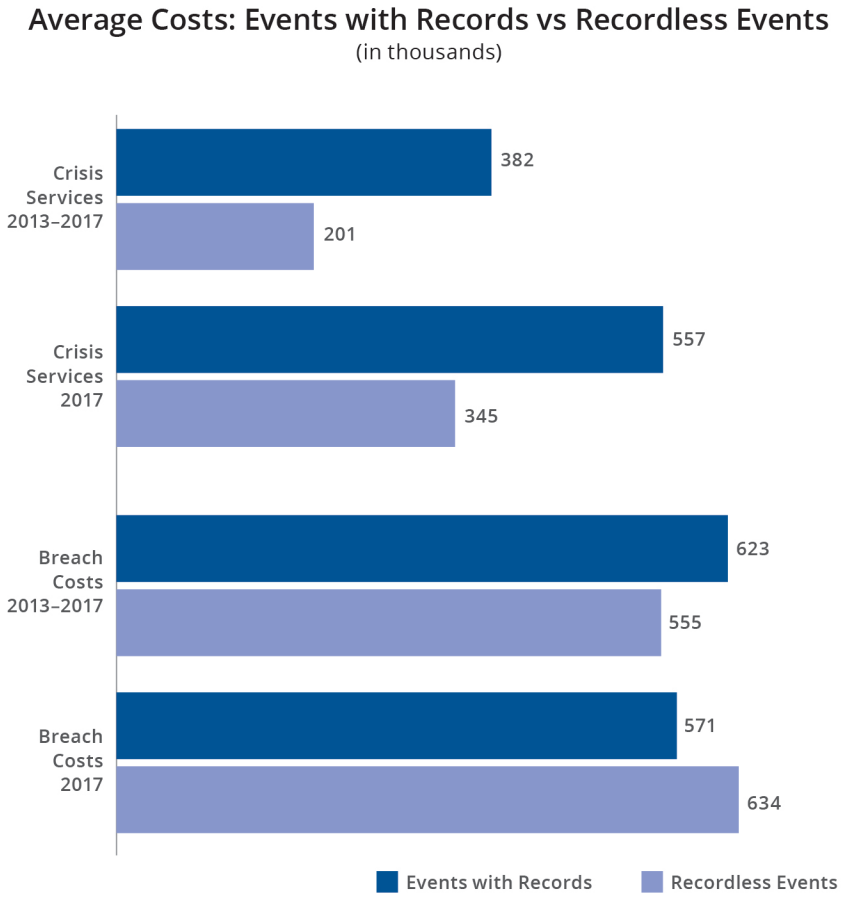


Figure 10

A Word about Self-Insured Retentions (SIR)

The dataset contains 1,049 claims that reported a value for SIR. Over 5 years, the value of SIR has ranged from $0 to $20M. In 2017, SIR ranged from $0 to $10M. As indicated in Table 2, the averages were $291K for 2013–2017 and $148K in 2017 alone. Median values were $20K and $10K, respectively.

Self-Insured Retention (SIR)	2017	2013–2017
Cases	270	1,049
Min	0	0
Average	148,181	290,868
Median	10,000	20,000
Max	10,000,000	20,000,000

Table 2

Taking a Closer Look at the Data

Crisis Services Cost by Category

In addition to Total Crisis Services, the dataset contains costs for five categories of crisis services: Forensics, Credit/ID Monitoring, Notification, Legal Guidance/Breach Coach®, and Other. Sometimes, only a total was provided, and not every claim reported an amount in each category, so the Total Crisis Cervices cost was usually higher than the sum of the categories. The graph below plots the yearly average of these categories as columns, with the average Total Crisis Services cost as a line.

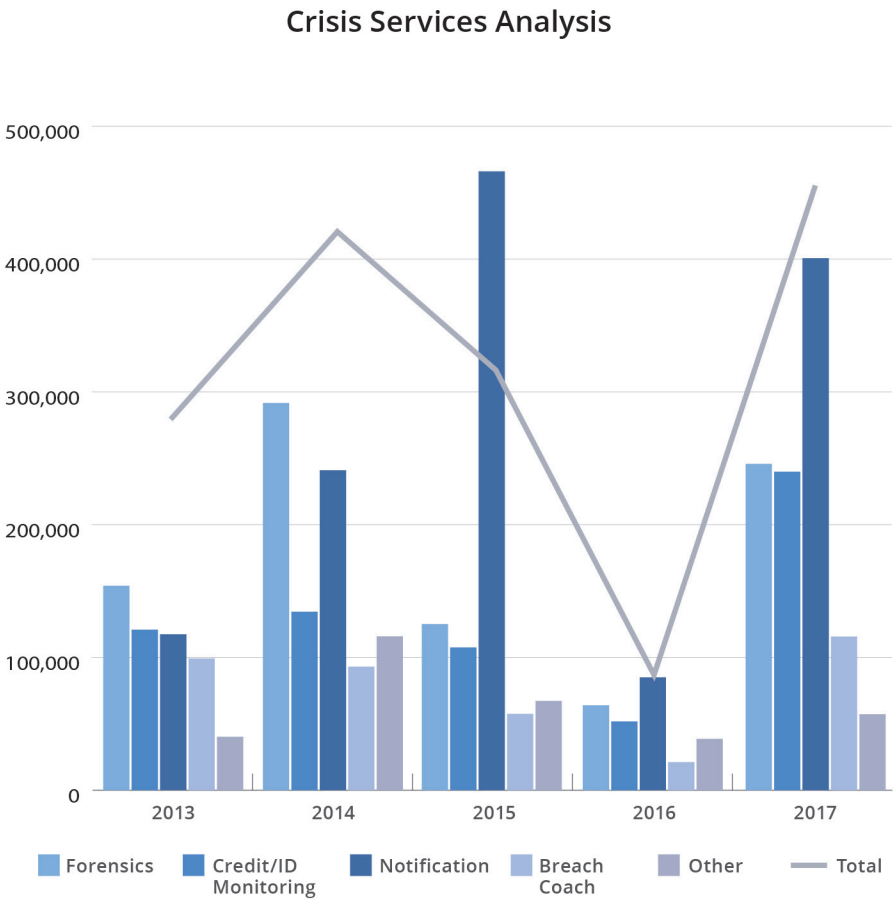


Figure 11

"To protect customers and your brand after a data breach, businesses need more than a written response plan—it must be pressure tested and the availability of the resources required to execute it must be guaranteed. Working with crisis services vendors should be a critical component of every business' breach readiness efforts."

Bo Holland
President,
AllClear ID

Forensics

Of the claims that included Forensics cost from 2013–2017, 32% occurred in 2017. The largest claim for forensics also occurred in 2017. The average forensics claim in 2017 is almost 40% higher than the average for 2013–2017, while the median claim is somewhat lower ($246K/$28K).

Credit/ID Monitoring

Over the 5-year period, 21% of all claims reported amounts for Credit/ID Monitoring. Coincidently, it was the same percentage of claims in 2017. Credit/ID Monitoring accounted for 5% of overall Breach Cost for the 5-year period, and 8% in 2017. Average Credit/ID Monitoring in 2017 was 74% higher than the 5-year average. The median cost in 2017 was higher by about 50%, but the practical difference ($7,500 vs $5,800) is not significant.

Notification

Approximately 20% of the claims with Notification cost and 30% of total Notification cost were incurred in 2017. The average Notification cost in 2017 was 55% higher than the average for 2013–2017, while the median claim was less than half of that from 2013–2017.

Legal Guidance/Breach Coach®

Legal Guidance/Breach Coach® cost was present in 65% of all claims in the 5-year period and 79% of claims in 2017. The percentage of claimants utilizing the services of a Breach Coach® (typically a specialized lawyer) increased from 58% in 2015 to 69% in 2016 to 79% in 2017.

Other Crisis Services

Other Crisis Services includes the cost of public relations, the cost of data restoration, and even the cost of a ransom or fraudulent wire transfer. The average in 2017 decreased by approximately 8% while the median increased by 20%.

Business Sector

The dataset contains claims from 17 business sectors. Overall, the Professional Services, Healthcare, Financial Services and Retail sectors accounted for 60% of the claims. In 2017, 23% of claims occurred in Professional Services.

Percentage of Claims by Sector: 2013–2017
(N=1,201)

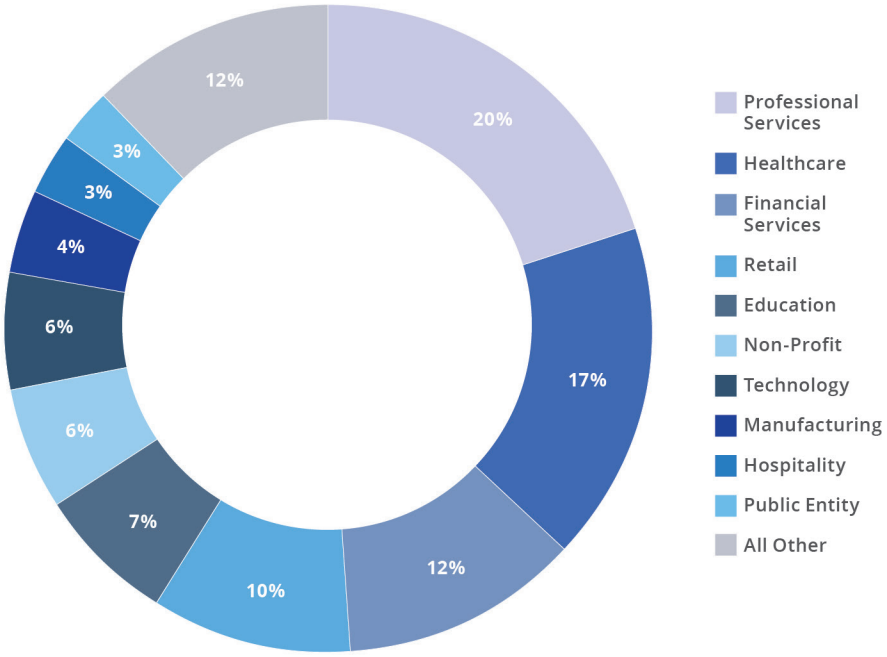


Figure 12

Percentage of Claims by Sector: 2017

(N= 298)

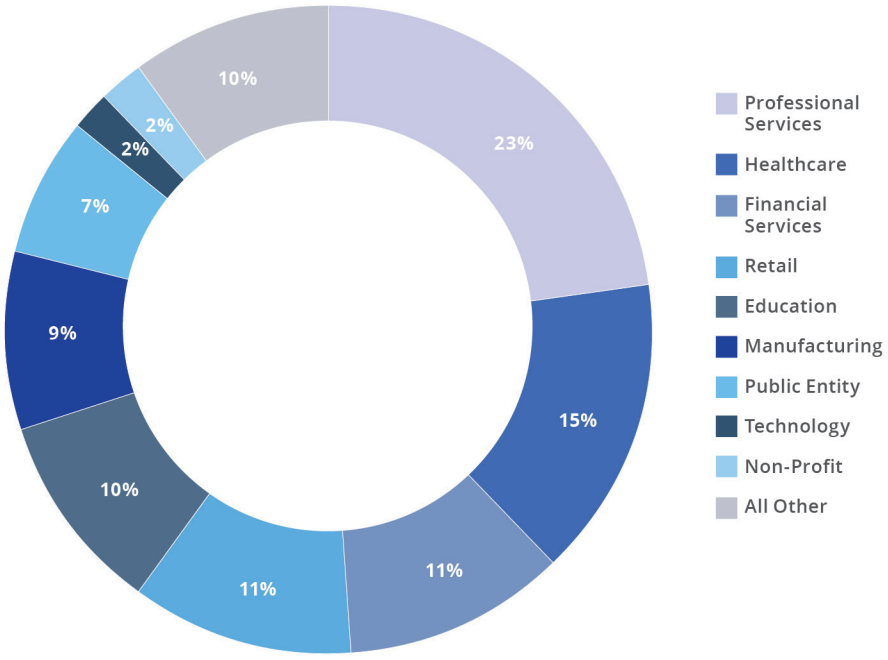


Figure 13

The tables below present the total Breach Cost (Table 3) and the average Crisis Services Cost by category (Table 4) for each sector.

Total Breach Cost by Sector 2013–2017 (thousands)

	Cases	Minimum	Average	Median	Maximum	Total
Education	79	1.5	154	61	1,533	12,155
Energy	10	11	1,790	142	5,000	17.901
Entertainment	12	7	143	87	764	1,717
Financial Services	145	0.1	854	50	64,000	123,895
Gaming & Casino	7	76	299	144	1,126	2,092
Healthcare	199	0.9	555	68	15,000	110,448
Hospitality	39	5	411	103	5,650	16,032
Manufacturing	47	0.8	1,196	39	33,000	56,235
Media	16	5	502	139	2,469	8,034
Non-Profit	74	1.2	84	16	1,607	6,189
Other	36	0.7	81	44	779	2,924
Professional Services	263	0.3	168	43	9,093	44,139
Public Entity	38	5	78	57	328	2,968
Restaurant	11	4	79	75	250	869
Retail	123	7	1,186	94	16,849	145,852
Technology	67	8	648	115	10,000	43,422
Telecommunications	11	4	2,308	239	20,000	25,390
Transportation	17	14	5,928	119	80,000	100,781

Table 3

Average Crisis Services Cost by Sector 2013–2017 (thousands)

Sector	Forensics	Notification	Credit/ID Monitoring	Legal Guidance	Other	Total Crisis
Education	79	59	36	27	72	116
Energy	65	0	0	5	65	73
Entertainment	120	2	83	27	37	133
Financial Services	204	589	397	298	24	740
Gaming & Casino	220	47	12	18	25	275
Healthcare	107	581	203	46	100	442
Hospitality	156	29	21	97	49	233
Manufacturing	1,346	9	6	13	10	976
Media	101	73	0	114	15	175
Non-Profit	97	7	4	18	26	82
Other	53	40	27	19	12	68
Professional	95	35	29	32	46	115
Public Entity	39	21	19	21	8	63
Restaurant	43	38	0	32	82	71
Retail	291	72	78	107	178	373
Technology	153	47	179	129	26	280
Telecommunications	115	900	0	584	11	475
Transportation	117	7	8	15	0	93

Table 4

Professional Services

The dataset contains 263 claims (20% of claims) for Professional Services, ranging from $290 to $9M. Claims in 2017 made up 31% of claims for 2013–2017 but only 3% of the total Breach Cost for the same period. The average and median cost for Professional Services claims tends to be lower than those of other Sectors.

Healthcare

Healthcare claims accounted for 17% of claims in the 5-year period and 15% of the total Breach Cost. In 2017, they accounted for 15% of claims and 7% of total Breach Cost. When ranked by average Breach Cost, Healthcare occupied eighth place.

Financial Services

Claims in the Financial Services sector accounted for 12% of claims in the 5-year period and 17% of the total Breach Cost. In 2017, they accounted for only 11% of claims but 38% of total Breach Cost. When ranked by average Breach Cost, Financial Services occupied sixth place.

Retail

Claims in the Retail sector represented 10% of claims in the 5-year period and 20% of the total Breach Cost. In 2017, they constituted 11% of claims but only 3% of total Breach Cost. When ranked by average Breach Cost, Retail occupied fifth place.

Education and Higher Education

Claims in Education accounted for 7% of claims in the 5-year period but less than 2% of the total Breach Cost. In 2017, they accounted for 10% of claims and 3% of total Breach Cost. When ranked by average Breach Cost, Education occupied thirteenth place.

Higher Education Only

Higher Education accounted for 57% of claims in the Education sector. For the 5-year period, the average Crisis Services Cost was 31% higher in this sub-sector and the average Breach Cost was 34% higher than costs for the Education sector overall. For 2017, average Crisis Services Cost was 20% higher while average Breach Cost was 27% higher.

Revenue Size

The distribution of claims by the revenue size of the claimant was consistent over the 5-year period with 85% of claims coming from organizations with less than $2B in annual revenues, 7% of claims coming from organizations with more than $2B in revenues and 8% of claims with no revenue size reported.

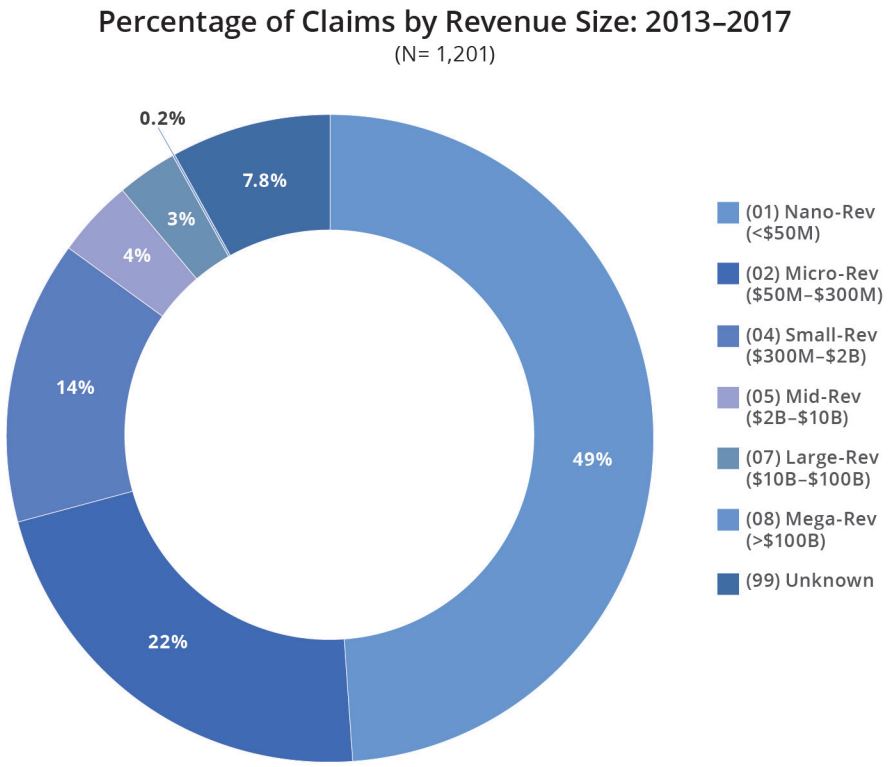


Figure 14

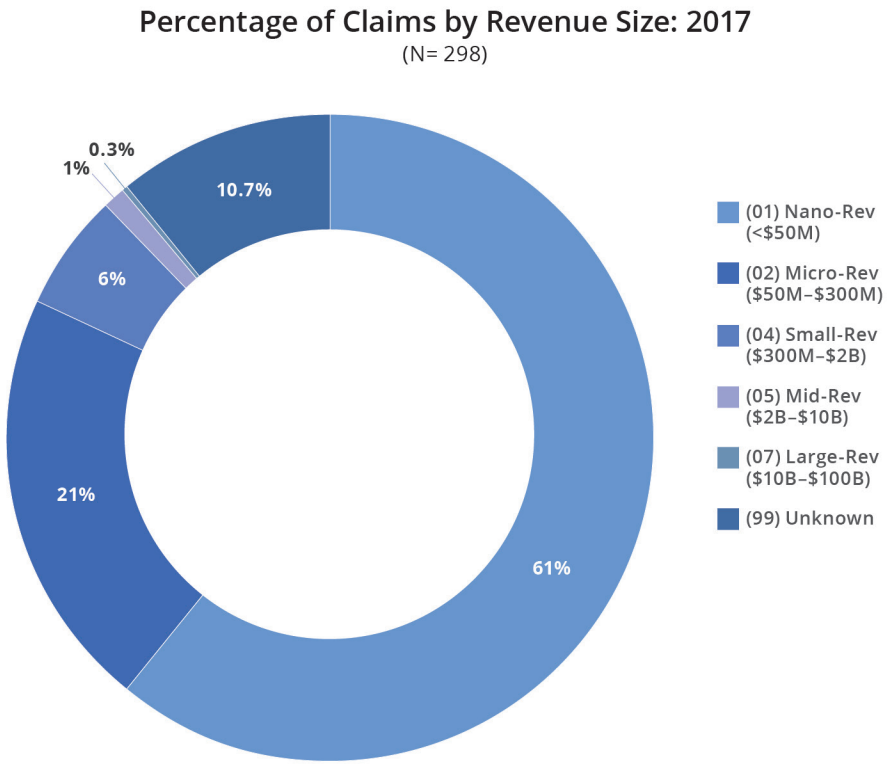


Figure 15

There was a 20-fold difference in the average and median breach cost between organizations with less than $2B in annual revenues and those with more than $2B in revenues. For smaller organizations, the average Breach Cost was $226K vs $5.2M for larger organizations. For median Breach Cost, the numbers were $55K vs $1M.

The tables below present the total Breach Cost (Table 5) and average Crisis Services cost by category (Table 6) for organizations above and below $2B in annual revenues.

Breach Cost by Rev Size: 2013–2017 (thousands)

	Cases	Minimum	Average	Median	Maximum	Total
Revenues <$2B	1,011	0.1	226	55	11,750	219,349
Revenues >$2B	82	3	5,159	1,000	80,000	423,027
Nano-Rev (<$50M)	587	0.3	134	39	7,500	69,450
Micro-Rev ($50M–$300M)	261	0.2	239	75	6,600	62,491
Small Rev ($300M–$2B)	163	0.1	536	125	11,750	87,408
Mid-Rev ($2B–$10B)	48	2.7	2,598	294	64,000	124,712
Large-Rev ($10–$100B)	32	32	8,885	5,000	80,000	284,324
Mega-Rev (>$100B)	2	2,500	6,996	6,996	11,491	13,991
Unknown Revenue Size	0.1	3	671	99	20,000	69,832,125

Table 5

Average Crisis Services Costs by Rev Size: 2013–2017 (thousands)

	Forensics	Notification	Credit/ID Monitoring	Legal Guidance	Other	Total Crisis
Revenues <$2B	1,729	1,646	1,098	828	186	3,183
Revenues >$2B	87	80	56	35	39	128
Nano-Rev (<$50M)	109	211	88	62	112	267
Micro-Rev ($50M–$300M)	2,456	1,000	1,712	532	2,000	4,100
Small Rev ($300M–$2B)	4,860	2,804	994	1,065	242	5,786
Mid-Rev ($2B–$10B)	737	1,221	1,083	792	34	2,268
Large-Rev ($10–$100B)	222	104	77	64	33	269
Mega-Rev (>$100B)	92	72	80	43	34	141
Unknown Revenue Size	48	72	37	23	45	83

Table 6

Causes of Loss

Hackers, Ransomware and Malware/Viruses were the leading causes of loss in this year's report, with Ransomware occupying the second spot overall and the top spot in 2017. The increasing prevalence of Ransomware was quite obvious: 15% of the five-year total versus 31% in 2017. The overall distribution of claims by cause of loss is presented in Figures 16 and 17.

Percentage of Claims by Cause of Loss: 2013–2017
(N=1,201)

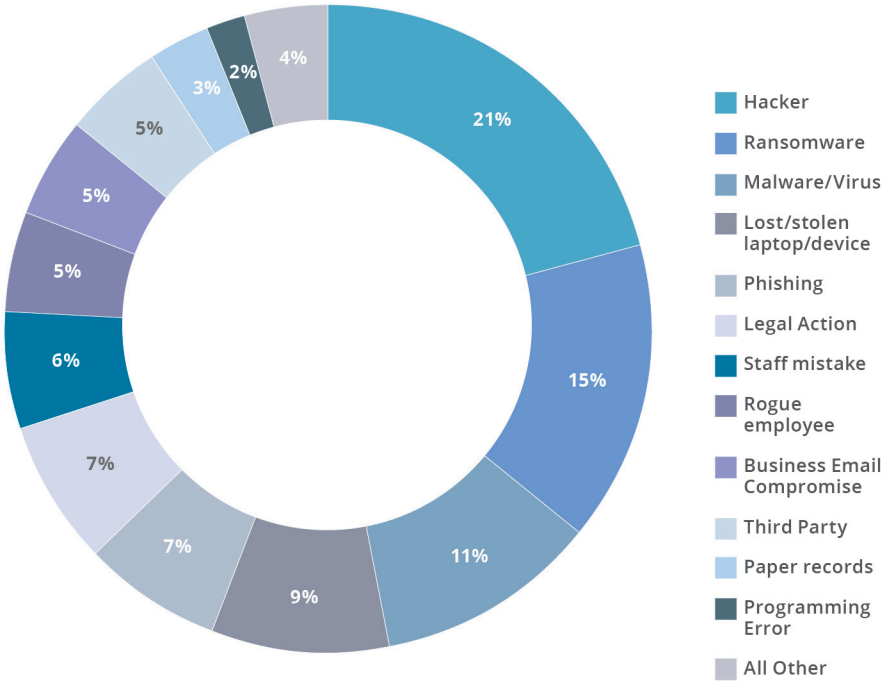


Figure 16

Percentage of Claims by Cause of Loss: 2017

(N=298)

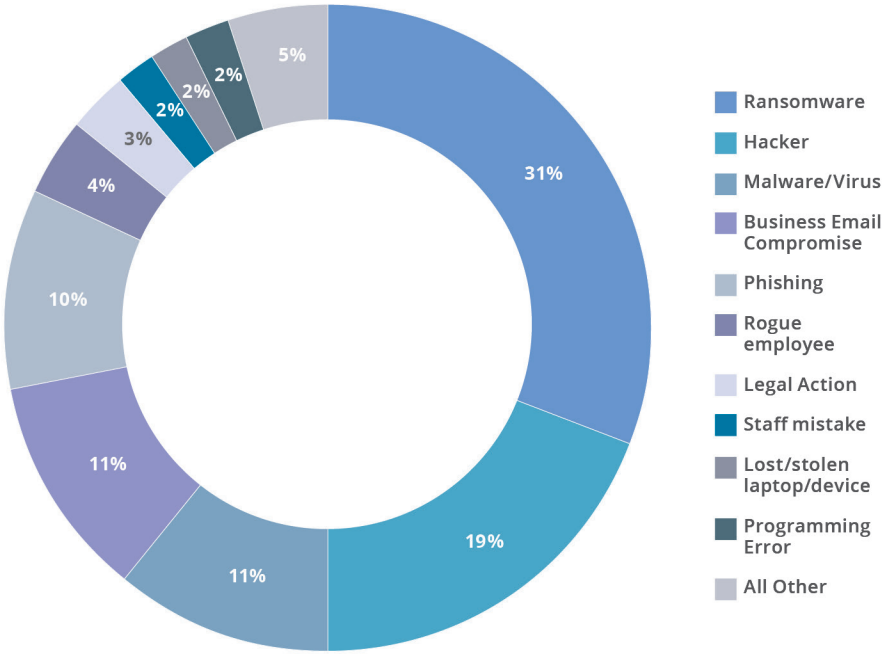


Figure 17

Table 7 below provides cost data for each cause of loss. The top four causes of loss by number of claims were Hacker, Ransomware, Malware/Virus, and Legal Action. Excluding a very large breach caused by a system glitch ($19M), the four causes of loss with the highest average Breach Costs were Malware/Virus, Hackers, Rogue Employees and Ransomware.

Total Breach Cost by Cause of Loss 2013–2017 (thousands)

Cause of Loss	Cases	Minimum	Average	Median	Maximum	Total
Business Email Compromise	62	4	115	46	1,123	7,134
Hacker	251	1	1,054	114	64,000	264,483
Improper Data Collection	2	8	33	33	58	66
Legal Action	79	3	136	43	1,604	10,714
Lost/Stolen Laptop/Device (Combined)	109	0	195	41	6,529	20,867
Malware/Virus	129	2	1,213	93	33,000	155,327
Negligence	7	5	58	27	135	409
Paper Records	33	1	69	22	926	2,281
Phishing	83	1	87	51	585	7,250
Programming Error	30	2	184	63	1,000	5,515
Ransomware	186	1	229	53	20,000	42,544
Rogue Employee	64	3	858	90	20,000	54,085
Social Engineering	8	16	34	35	58	273
Staff Mistake	73	0	53	12	600	3,820
System Glitch	5	2	19,523	107	80,000	97,614
Theft of Money	7	35	174	69	470	1,217
Third-Party	61	1	744	69	10,000	43,880
Trademark/Copyright Infringement	4	15	249	257	468	997
Wire Transfer Fraud	7	9	359	144	1,475	2,514
Wrongful Data Collection	1	55	55	55	55	55

Table 7

Table 8 below provides a breakdown of Crisis Services Costs for each cause of loss. The three causes with the highest Crisis Services Costs were Hacker, Malware/Virus and Rogue Employees, which tracks closely with the causes of loss with the highest total Breach Costs.

Average Crisis Services Cost by Cause of Loss 2013–2017 (thousands)

Sector	Forensics	Notification	Credit/ID Monitoring	Legal Guidance/ Breach Coach®	Other	Total Crisis
Business Email Compromise	31	18	21	23	11	47
Hacker	249	630	283	206	92	757
Improper Data Collection	0	0	0	3	0	3
Legal Action	23	12	2	16	26	30
Lost/Stolen Laptop/Device	41	133	140	31	58	162
Malware/Virus	594	229	152	93	97	690
Negligence	6	24	1	24	0	37
Paper Records	10	14	18	20	15	30
Phishing	54	16	39	18	38	68
Programming Error	50	73	130	31	29	133
Ransomware	38	21	66	13	22	56
Rogue employee	182	109	120	97	8	281
Social Engineering	6	0	1	9	0	13
Staff mistake	27	24	10	26	7	37
System Glitch	0	3	0	2	0	3
Theft of Money	25	0	4	47	168	78
Third-Party	25	22	22	14	8	34
Trademark/Copyright Infringement	0	0	0	91	0	91
Wire Transfer Fraud	44	0	0	47	244	156
Wrongful Data Collection	5	0	0	0	0	5

Table 8

Criminal vs Non-Criminal Activities

This year, in addition to providing data about individual causes of loss, we aggregated the data into Criminal and Non-Criminal categories. One of the clearest trends in the dataset was the increase in the percentage of criminal claims. In each year since 2013, this percentage has increased, from 69% in 2013 to 92% in 2017. Criminal events included hacking, ransomware, malware/virus, phishing/BEC/social engineering, DDoS attacks, stolen devices, and 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.

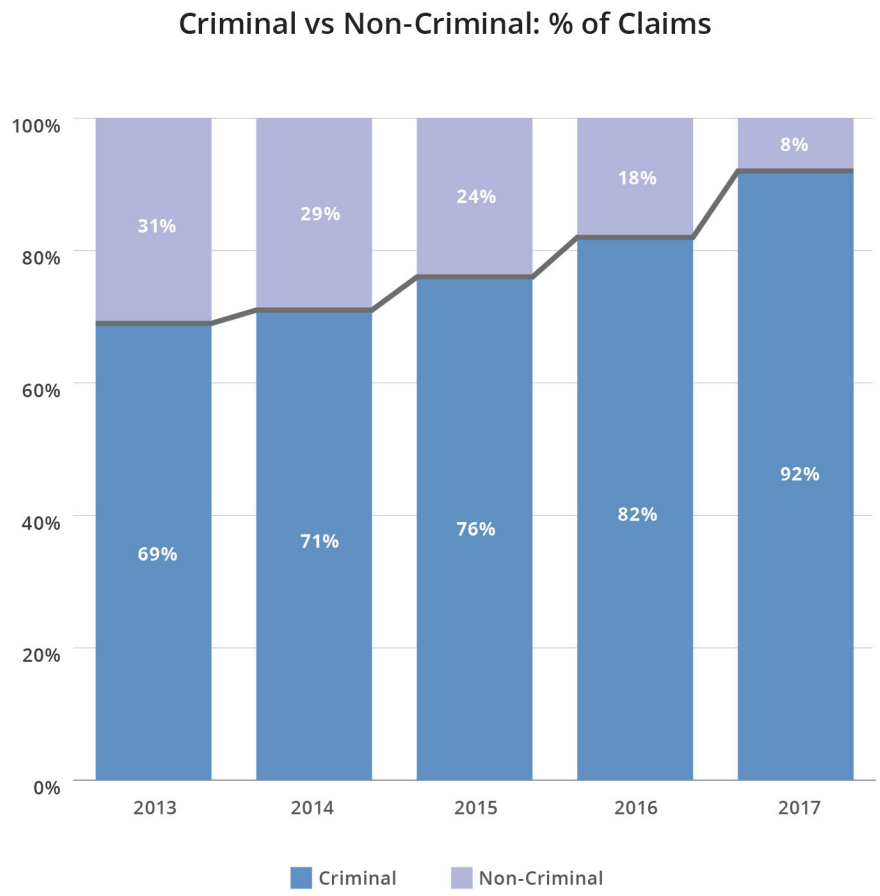


Figure 18

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

Criminal

Crisis Services	2013–2017	2017
Claims	801	242
Min	110	130
Average	364,615	488,353
Median	45,644	41,821
Max	64,000,000	64,000,000
Total	292,056,674	118,181,408
Breach Costs		
Claims	954	274
Min	110	1,542
Average	620,242	584,406
Median	69,821	64,780
Max	64,000,000	64,000,000
Total	591,711,192	160,127,114

Table 9

By the Numbers

- 80% of claims
  - Average records exposed: 1.6M
    - Median records exposed: 1.5K

Non-Criminal

Crisis Services	2013–2017	2017
Claims	181	18
Min	14	299
Average	53,896	68,042
Median	11,640	23,974
Max	679,293	540,000
Total	9,755,210	1,224,755
Breach Costs		
Claims	240	24
Min	225	3,418
Average	538,889	823,817
Median	33,375	48,605
Max	80,000,000	17,500,000
Total	129,333,391	19,771,603

Table 10

By the Numbers

- 20% of claims
  - Average records exposed: 28K
    - Median records exposed: 0.5K

Ransomware

The increased frequency of Ransomware is no secret to anyone. In the dataset, the increase in the number of Ransomware claims from 2013 through 2017 was dramatic: 1 claim in 2013, 7 in 2014, 19 in 2015, 68 in 2016 and 91 in 2017.

The vast majority of Ransomware-related Breach Costs in our dataset occurred in 2017, followed by 2016 (82% and 14%, respectively). NotPetya, WannaCry and Locky are the top variants when given a detailed description of the incident.

2013–2017

- Ransom Amounts: $300 to $101K; average = $23K; median = $13K
- Crisis Services Cost: $750 to $460K; average = $57K; median = $33K
- Total Breach Cost: $600 to $20M; average = $229K; median = $53K

Hacking and Malware/Virus

Hacking and Malware/Virus (Malware) are categories that often overlap. It is sometimes difficult to determine which one to assign as the cause of loss. Only 65% of Hacking events could be categorized by a single cause of loss. The remaining 35% could be characterized by more than one cause of loss, like a DDoS attack, theft of money, or a W-2 exploit perpetrated by a hacker.

The situation was similar with Malware/Virus. 57% of Malware/Virus incidents were clearly that. But the remaining 43% of incidents could have been assigned to causes of loss like Ransomware or Phishing.

Hacking 2013–2017:

- Crisis Services Cost: $300 to $64M; average = $757K; median = $85K
- Total Breach Cost: $1K to $64M; average = $1.05M; median = $114K

Malware/Virus 2013–2017:

- Crisis Services Cost: $600 to $33M; average = $690K; median = $70K
- Total Breach Cost: $2.4K to $33M; average = $1.2M; median = $93.5K

Phishing/Business Email Compromise (BEC)/Social Engineering Combined

Phishing, Business Email Compromise and Social Engineering are categories with considerable potential overlap. For this reason, we have provided data on the three categories together, as well as each category separately.

Phishing attacks are indiscriminate and impersonal. When thinking about phishing, the word "campaign" comes to mind—mass emails sent in the hope of snaring a small percentage of victims.

Business Email Compromises involve well-crafted, highly personalized attacks. Criminals often invest considerable time and research into the wording and tone of the messages to make them seem legitimate. From what we have seen in the claims data, this approach was quite effective. Wire transfer and ACH/banking fraud, theft of money, W-2 fraud, and Office 365/productivity software exploits were, in many cases, caused by BEC.

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

Combined Phishing/BEC/Social Engineering 2013–2017:

- Crisis Services Cost: $500 to $834K; average = $61K; median = $25K
- Total Breach Cost: $1K to $1.12M; average = $99K; median = $48K

Phishing 2013–2017:

- Crisis Services Cost: $500 to $834K; average = $73K; median = $26K
- Total Breach Cost: $3.5K to $1.11M; average = $93K; median = $50K

BEC 2013–2017:

- Crisis Services Cost: $1K to $351K; average = $47K; median = $27K
- Total Breach Cost: $1K to $1.12M; average = $115K; median = $46K

Social Engineering 2013–2017:

- Crisis Services Cost: $2.5K to $77K; average = $19K; median = $10K
- Total Breach Cost: $16K to $1.12M; average = $140K; median = $35K

Rogue Employee and Malicious Insiders

To obtain a more accurate analysis of the impact of malicious insiders, we combined claims that indicated a malicious insider was involved with claims that identified Rogue Employee as the cause of loss. In the Telecommunications sector, 85% of the aggregate Breach Cost from 2013—2017 involved incidents in which Rogue Employees accessed sensitive data. Two of these incidents occurred in 2017. Financial Services suffered a loss of more than $19M due to a Rogue Employee, including more than $11M due to the theft of client data. Employees who accessed personal patient files cost the Healthcare sector $6M.

2013–2017:

- Crisis Services Cost: $100 to $5.7M; average = $261K; median = $52K
- Total Breach Cost: $2.5K to $20M; average = $801K; median = $80K

Stolen Devices

Careful review of event descriptions allowed us to differentiate between devices that were stolen and devices that were lost. In some cases, we could also determine whether the devices were encrypted, as well as whether the devices were stolen from cars or facilities.

2013–2017:

- Crisis Services Cost: $100 to $6.5M; average = $194K; median = $35K
- Total Breach Cost: $100 to $6.5M; average = $191K; median = $57K

While the average Breach Cost for stolen, unencrypted devices was $218K, the average Breach Cost for encrypted devices was only $22K. The average Breach Cost for devices stolen from cars ($90K) was also significantly lower than for devices stolen from facilities ($2M).

By the Numbers

Average Breach Cost for devices that were:

- Encrypted = $22K
- Unencrypted = $218K

W-2 Fraud

The number of W-2 fraud claims in the dataset has increased steadily since 2013, when only 4 claims were reported. There were 30 such claims in 2016 and 28 in 2017.

2013–2017:

- Crisis Services Cost: $1K to $413K; average = $57K; median = $20K
- Total Breach Cost: $1K to $413K; average = $72K; median = $33K

W-2 Fraud occurred via a surprising number of causes and in a variety of business sectors.

The most common causes of W-2 fraud were Business Email Compromise and Phishing.

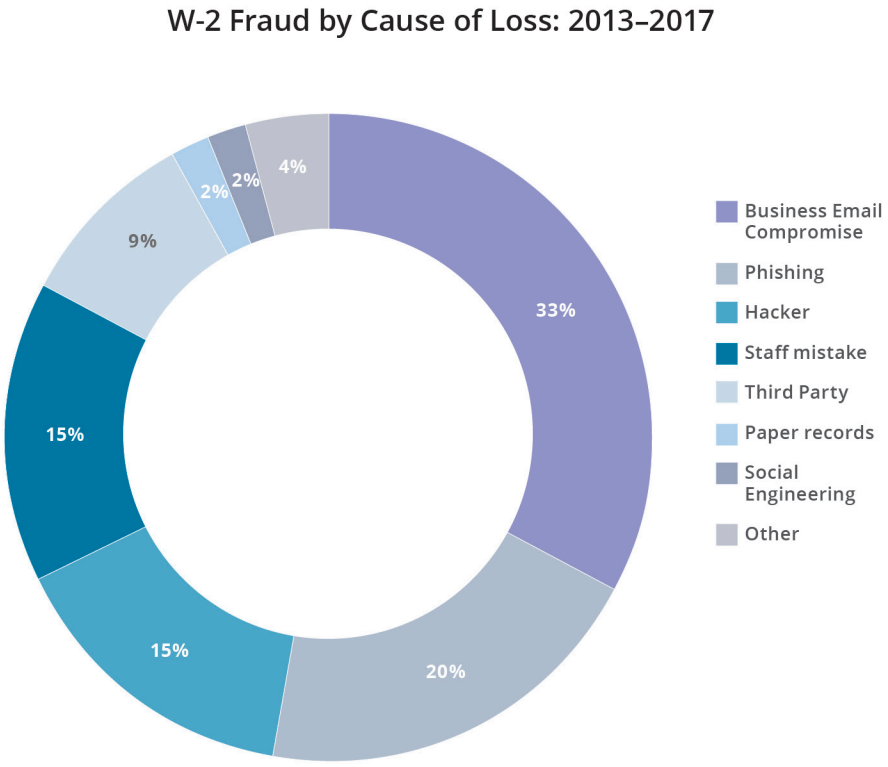


Figure 19

The sectors most affected were Professional Services, Non-Profit, Healthcare, Financial Services and Education. Not surprisingly, among Professional Services firms, those providing tax and payroll services experienced the greatest number of events.

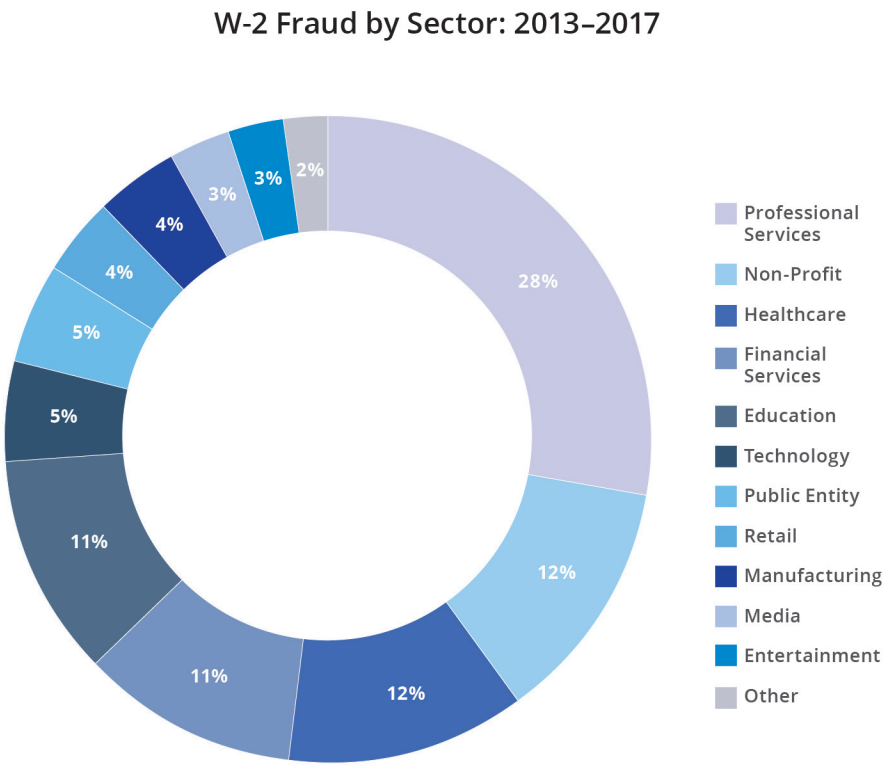


Figure 20

Banking and ACH Fraud

The top three sectors impacted by wire transfer and banking fraud were Professional Services firms, Financial Services and Retail. Overall, law firms accounted for almost 20% of the total claims. These events were typically caused by phishing, business email compromise and social engineering. The number of these events has been increasing during the past 5 years, from 4 in 2013, 5 in 2014, 6 in 2015, 12 in 2016, to 27 in 2017.

2013–2017:

- Fraud Amount: $3.5K to $9M; average = $422K; median = $90K
- Crisis Services Cost: $1K to $479K; average = $81K; median = $26K
- Total Breach Cost: $3.5K to $9.1M; average = $386K; median = $117K[2]

[2] The average fraud amount was higher than the average Breach Cost due to a single large event in 2013.

Denial of Service Attacks

Denial of Service attacks have been with us for many years. Although there are effective technologies for detecting and deflecting these attacks, many companies have yet to deploy them. The three causes of loss for DDoS events were Hackers (71%), Malware/Virus (18%), and Rogue Employees (11%).

2013–2017:

- Crisis Services Cost: $3.5K to $1.6M; average = $167K; median = $41K
- Total Breach Cost: $3.5K to $7.5M; average = $747K; median = $76K

Office Productivity Software Exploits

Criminals have been increasingly targeting office productivity software suites like Microsoft Office 365 and SharePoint, as well as products from Peoplesoft and Workday. The attraction of these environments is that stolen user credentials usually provide an entry point to an entire computing environment. Victims of these kinds of exploits included organizations in Financial Services, Professional Services (especially law firms), Manufacturing and Transportation.

2013–2017:

- Crisis Services Cost: $27K to $465K; average = $136K; median = $72K
- Total Breach Cost: $16K to $955K; average = $236K; median = $82K

Losses Due to Non-Criminal Factors

Although it is probably impossible to eliminate the risks listed below, they are ones that organizations can work to manage.

- Staff Mistakes
- Programming Errors
- System Glitches
- Negligence
- Mishandling of Paper Records
- Lost/Stolen Devices
- Legal Actions—Card Brand, Regulatory, Civil

In the following sections, we present commentary and tables for these categories of manageable risks.

Staff Mistakes

Staff mistakes occurred for all sorts of reasons. Many of the items listed above could be considered staff mistakes.

There were between 20–33 staff mistake claims each year for the 4-year period 2013–2016, then the number dropped to 7 in 2017. Because we will continue to collect claims for events occurring in 2017 for the 2019 and 2020 studies, it is too early to say whether the reduced number of claims is a trend.

2013–2017:

- Crisis Services Cost: $14 to $679K; average = $41K; median = $8K
- Total Breach Cost: $110 to $2.5M; average = $90K; median = $26K

Programming Errors

Review of the data revealed that a certain number of claims categorized as staff mistakes or system glitches could also be analyzed as programming errors. Examples include misconfiguration of network hardware, firewalls and routers, as well as poor coding technique that left networks and data open to exploit.

2013–2017:

- Crisis Services Cost: $1.8K to $679K; average = $133K; median = $37K
- Total Breach Cost: $1.8K to $1M; average = $184K; median = $63K

System Glitches and Hardware Failures

The 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 5 since 2013 and 2 in 2017.

2013–2017:

- Crisis Services Cost: $1.9K to $5K; average = $3.4K; median = $3.4K (same as average)
- Total Breach Cost: $1.8K to $80M; average = $19.5M; median = $107K

Mishandling of Paper Records

The mishandling of paper records continues to be an annoying and expensive event. For the most part, these events were caused by a failure to follow policy for the proper disposal of records, although, on occasion, the fault lay with a third-party service.

2013–2017:

- Crisis Services Cost: $14 to $197K; average = $30K; median = $15K
- Total Breach Cost: $600 to $926K; average = $69K; median = $22K

Lost Devices

As mentioned above in the section for Stolen Devices, we were able to differentiate between claims for Stolen Devices and claims for Lost Devices. The average and median Crisis Services Costs for Lost Devices ($58K / $11K) were quite a bit lower than for Stolen Devices ($194K / $35K). The average Breach Cost for Lost Devices was slightly higher than for Stolen Devices ($207K / $21K), while the median cost was much lower ($191K / $57K).

2013–2017:

- Crisis Services Cost: $300 to $1.2M; average = $58K; median = $11K
- Total Breach Cost: $300 to $2.5M; average = $207K; median = $21K

Legal Actions

Legal actions took the form of Card Brand-initiated Common Point of Purchase (CPP) investigations, Regulatory Actions and Civil Actions.

The dataset contains 32 claims for events that were initiated by Card Brands, 29 of which were CPP investigations. 24 (83%) of these claims used the words “possible” or “suspected.” Some of these claims involved an investigation by a Card Brand-mandated PFI (PCI Forensic Investigator) who, in many cases, determined that no compromise had occurred. The average cost of these claims was $34K.

Regulatory Actions included:

- Canadian Data Protection Laws by hosting customers information on servers in the US (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

Other legal action claims included:

- Trademark and Copyright Infringement
- Trade Secrets
- Theft of Intellectual Property
- Card Brand/CPP Investigations/PCI Actions
- Negligence

2013–2017:

- Crisis Services Cost: $2K to $100K; average = $30K; median = $20K
- Total Breach Cost: $2.5K to $1.6M; average = $136K; median = $43K

Type of Data

Overall

Events involving the exposure of Personally Identifiable Information (PII), Protected Health Information (PHI) and Payment Card Industry (PCI) data accounted for 54% of the claims that exposed records. Other categories included Non-Card Financial data and Other Non-Public data.

We have introduced three new data classifications in this year's report, the most important of which are "Files-Critical" and "Files-Not Critical." We created these categories to more accurately characterize events that do 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 has been exposed. These are the kinds of events we have labelled "Files-Critical."

Other kinds of events, typically ransomware also, have a lesser impact. In these cases, a victim might elect to wipe an infected machine clean, or even throw the machine away. We have characterized events like these at "Files-Not Critical."

We have also identified a sub-category of PII that we call W-2. This is data involved in payroll and W-2 fraud, but not involved in the creation of fraudulent financial and credit card accounts.

Percentage of Claims by Type of Data: 2013–2017
(N=1,201)

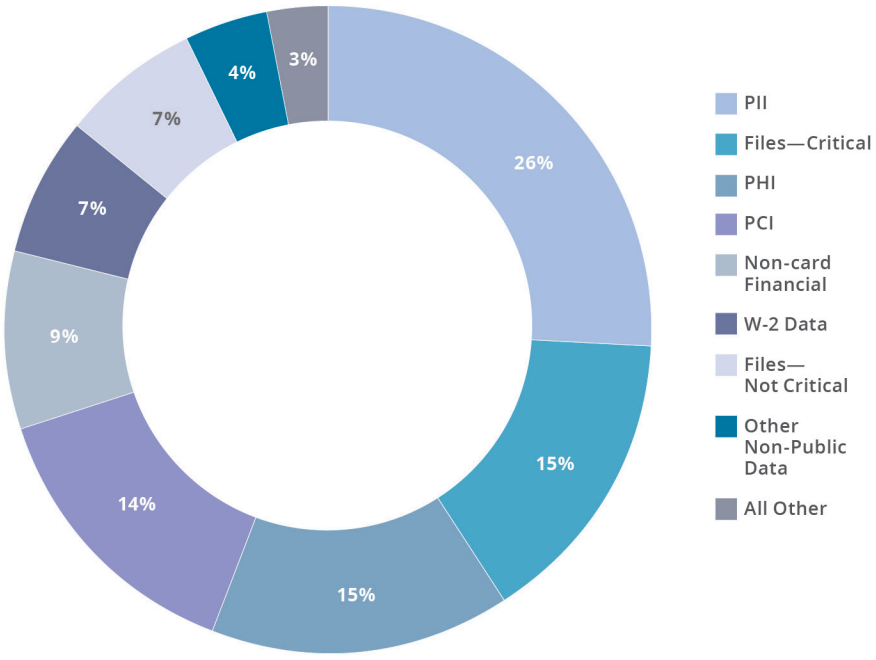


Figure 21

Percentage of Claims by Type of Data: 2017
(N=298)

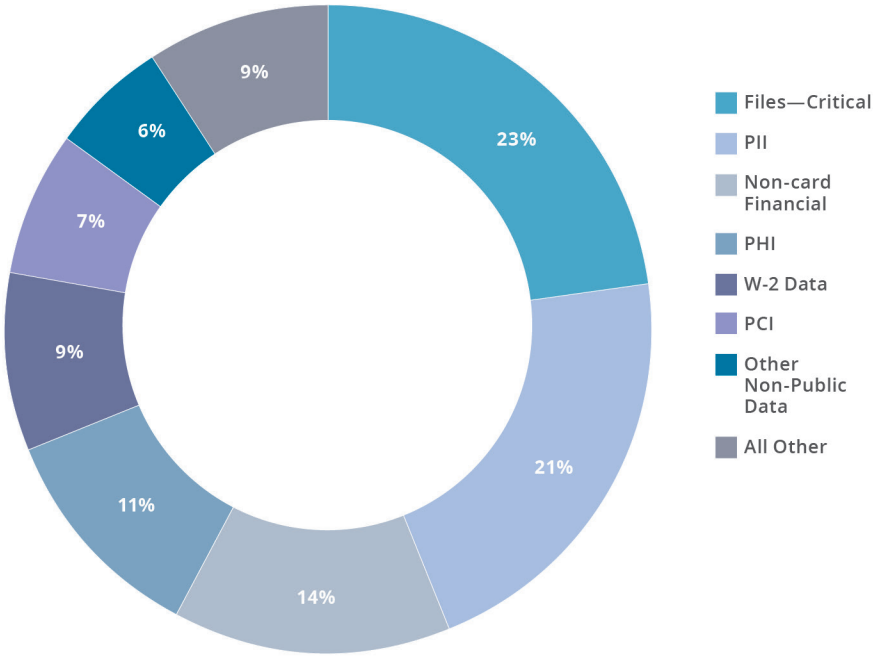


Figure 22

Table 11 below provides a numeric view of the dataset when analyzed by "Type of Data." While events that expose PCI, PHI and PII data were quite costly, the costliest category was "Files-Critical," with an average Breach Cost of $1.3M and a maximum cost of $80M. The table also shows the very large spread between the average and median cost of events labeled "Files-Critical" and "Files-Not Critical."

Total Breach Cost by Type of Data 2013–2017 (thousands)

	Cases	Minimum	Average	Median	Maximum	Total
Files-Critical	183	2	1,260	75	80,000	230,528
Files-Not Critical	78	0.2	48	20	716	3,736
Intellectual Property	15	3	570	182	4,961	8,546
Non-card Financial	107	1	255	58	9,093	27,055
Other Non-Public Data	54	3	69	38	600	3,708
PCI	163	1	959	94	16,849	154,439
PHI	171	0.3	617	92	15,000	104,823
PII	313	0.1	533	56	64,000	165,111
Trade Secrets	2	4	8	8	12	15
User Credentials (Login & Passwords)	21	4	234	115	1,475	4,917
User Online Tracking	2	25	41	41	58	83

Table 11

Table 12 below provides a view of the average Crisis Services Cost, both by category and in total, when analyzed by Type of Data. Events that expose PII, PHI and PCI data represent 3 of the 4 most costly kinds of events. The Files-Critical category rounds out the top 4, in second place.

Please note that not all claims report each category of Crisis Services in addition to the total. This is why the averages of some individual categories are greater than the average of Total Crisis Services.

Average Crisis Services Cost by Type of Data 2013–2017 (thousands)

	Forensics	Notification	Credit/ID Monitoring	Legal Guidance/	Other	Total Crisis
Files-Critical	394	103	295	27	46	389
Files-Not Critical	48	68	17	10	6	43
Intellectual Property	118	0	0	76	0	127
Non-card Financial	27	16	2	21	72	51
Other Non-Public Data	35	7	16	39	13	62
PCI	231	92	76	120	142	353
PHI	108	304	136	48	98	313
PII	161	422	222	149	35	502
Trade secrets	12	0	0	4	0	8
User Credentials (Login & Passwords)	91	9	10	36	6	140
User Online Tracking	15	0	0	0	10	25

Table 12

Personally Identifiable Information (PII)

Here is a detailed look at costs for exposure of PII, for the 5-year period as well as 2017. The averages were driven up by a single large claim involving a financial institution and hackers ($60M).

2013–2017:

- Crisis Services Cost: $14 to $64M; average = $502K; median = $42K
- Total Breach Cost: $110 to $64M; average = $533K; median = $56K

Protected Health Information (PHI)

Events involving the exposure of PHI represented approximately 10% of claims overall and in 2017. The average Crisis Services and Breach Costs were down quite a bit in 2017 versus the 5-year averages.

2017 only:

- Crisis Services Cost: $130 to $1.46M; average = $147K; median = $42K
- Total Breach Cost: $1.8K to $1.53M; average = $187K; median = $51K

2013–2017:

- Crisis Services Cost: $130 to $7.1M; average = $313K; median = $41K
- Total Breach Cost: $170 to $15M; average = $617K; median = $92K

Payment Card Industry (PCI)

As mentioned previously, we found it odd that we had a large number of claims involving PCI-related data but only a small number of claims with PCI fines. For the 5-year period, we analyzed Breach Cost for 161 claims with PCI data, but only 23 claims with PCI fines.

2013–2017:

- Crisis Services Cost: $400 to $4.9M; average = $353K; median = $69K
- Total Breach Cost: $600 to $16.8M; average = $959K; median = $94K

Files-Critical

As discussed above, Files-Critical is a new type of data, designated when ransomware, DDoS attacks, or any other type of event disrupts 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.

2013–2017:

- Crisis Services Cost: $500 to $33M; average = $389K; median = $42K
- Total Breach Cost: $1.5K to $80M; average = $1.26M; median = $75K

Files-Not Critical

Files-Not Critical is another new classification, also discussed previously. We assigned this data type to the same kinds of ransomware and disruption events as the Files-Critical category, but only when the incident seemed 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.

2013–2017:

- Crisis Services Cost: $225 to $696K; average = $43K; median = $12.5K
- Total Breach Cost: $225 to $716K; average = $48K; median = $20K

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 8% of the claims in the dataset involved the exposure or theft of Non-Card Financial data.

2013–2017:

- Crisis Services Cost: $1K to $479K; average = $51K; median = $29K
- Total Breach Cost: $1K to $9.1M; average = $255K; median = $58K

Other Non-Public Data

Other Non-Public Data includes anything not available to the public that does not fall into one of the other categories. These kinds of events accounted for less than 5% of the claims and less than 1% of the Total Breach Cost ($3.7M/$721M) in the dataset.

2013–2017:

- Crisis Services Cost: $900 to $600K; average = $62K; median = $31K
- Total Breach Cost: $2.5K to $600K; average = $69K; median = $38K

Insider Involvement

Only 25% of claims in the dataset involved the actions of insiders: 19% were the result of unintentional insider actions and 6% involved the actions of malicious insiders. The aggregate total Breach Cost for malicious insider activity, $55M out of $721M (7.5%), was small and about half that of unintentional insider activity.

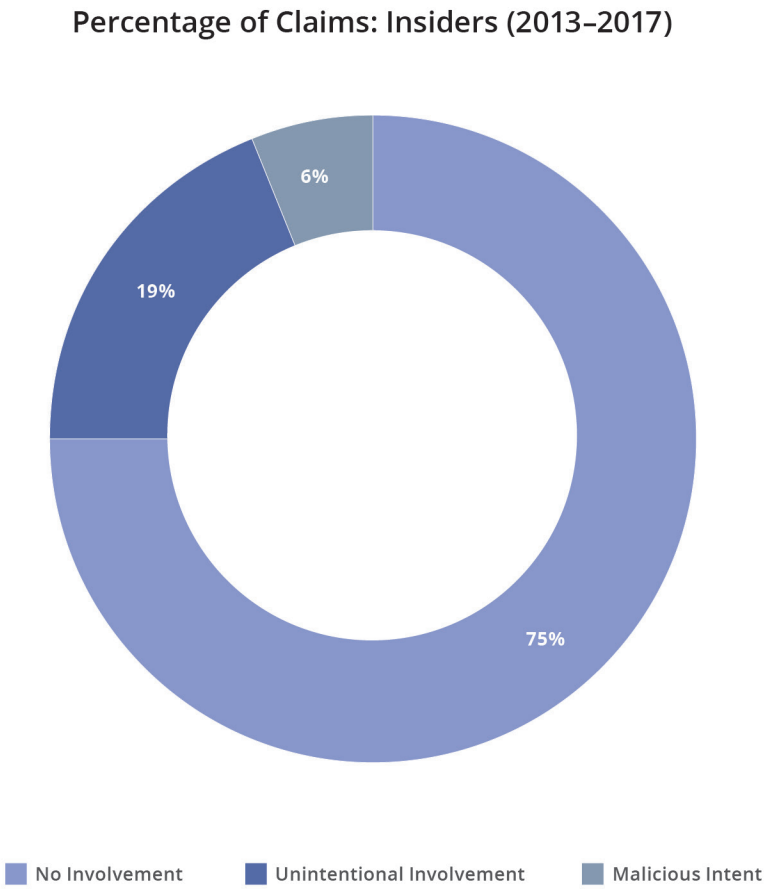


Figure 23

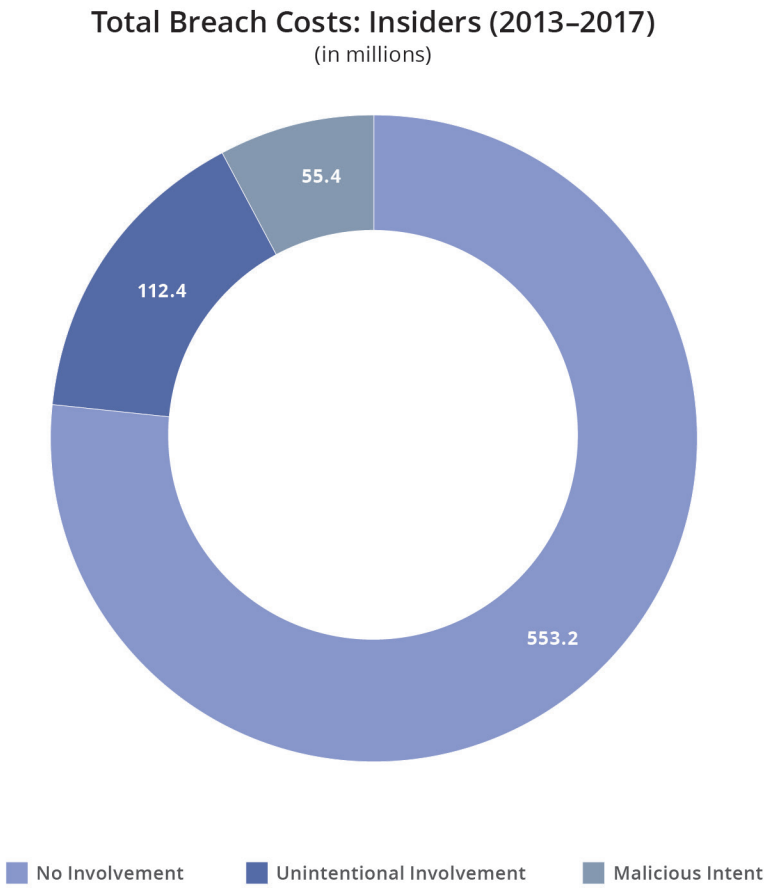

Total Breach Costs: Insiders (2013–2017)
(in millions)
55.4
112.4
553.2
No Involvement
Unintentional Involvement
Malicious Intent

Figure 24

Third Parties

The involvement of third parties in cyber events has been well documented. 11% of the claims in the 5-year period involved the unintentional (4%) or criminal (7%) actions of third parties. Third parties were not involved in the majority (89%) of events.

There are two different ways to look at third-party events:

- Third-party 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 involved in the Target breach comes to mind when thinking about this kind of relationship.
- Third-party Service Providers: Organizations that are third parties by the nature of the services provided include law firms, accounting 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, the health insurance giant. The dataset contains several claims involving the Anthem breach in 2015.

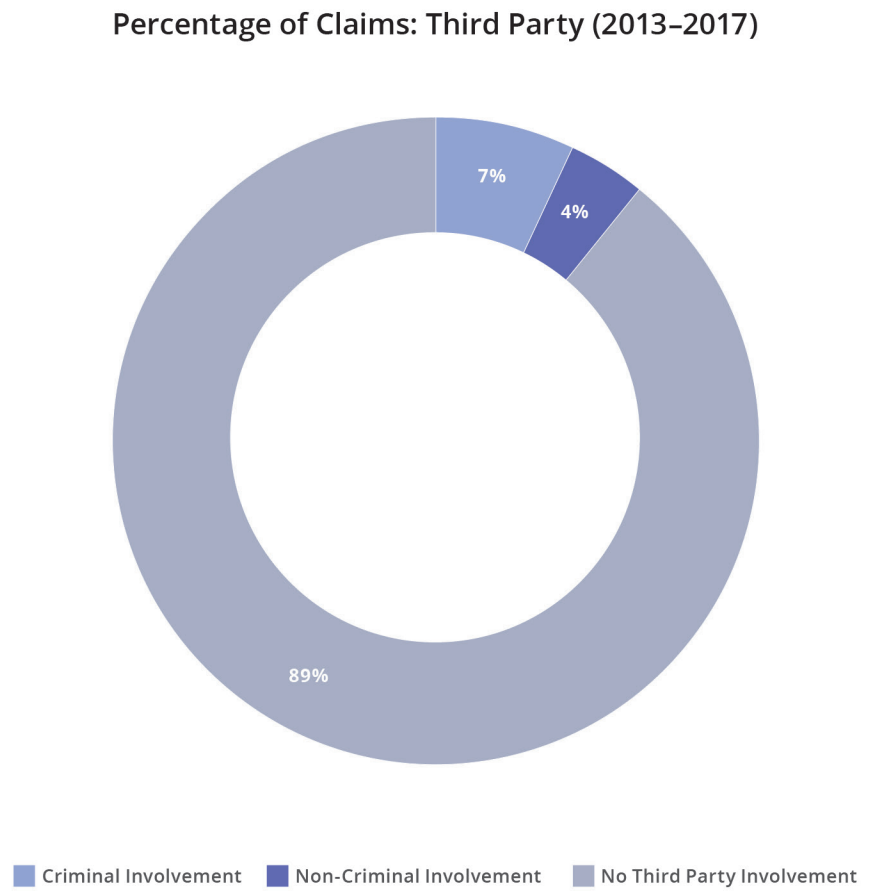


Figure 25

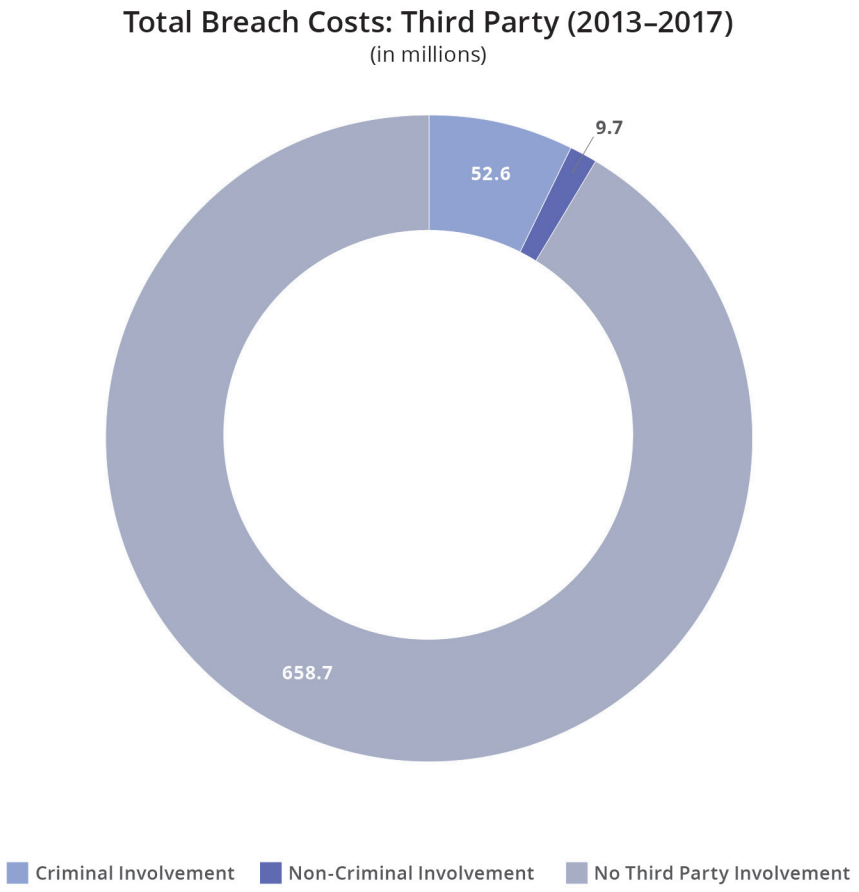


Figure 26

As the numbers below show, 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.

Third-Party Criminal Activity 2013–2017:

- Crisis Services Cost: $1K to $918K; average = $81K; median = $31K
- Total Breach Cost: $1.8K to $10M; average = $626K; median = $83.5K

Third-Party Non-Criminal Activity 2013–2017:

- Crisis Services Cost: $300 to $355K; average = $45K; median = $25K
- Total Breach Cost: $700 to $5M; average = $216K; median = $31K

Cloud

Last year, we began asking study participants to note and describe any cloud-related factors in a claim. So far, we have received 17 events to analyze. We expect this total to rise in the coming years.

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

2013–2017:

- Crisis Services Cost: $300 to $2.74M; average = $226K; median = $21K
- Total Breach Cost: $5.3K to $6.6M; average = $616K; median = $34K

Internet of Things (IoT)

For the first time in 2018, study participants were asked to note if a claim involved IoT devices. So far, we received data on 8 events, only 2 of which appeared to be IoT-related. One involved a hacking incident that utilized a photocopy machine to compromise a network and perform W-2 fraud. The other involved the malicious use of data copied from a cell phone by a retail cell phone store employee. Both incidents resulted in moderately small settlements. Crisis Services Cost was $50K and Breach Cost was $60K.

Conclusion

The cyber claims studies published by NetDiligence® represent the gold standard, certainly in the cyber insurance space and, arguably, in the entire cyber security space. No other studies provide more or better evidence-based information.

In this year's study, we have provided more data and analysis than ever before—5 years of claims data and more granular analysis, delving into more categorizations and details of the data. We collected over 500 new claims this year, a greater than 40% increase over last year and added them to an existing dataset of almost 700 claims. The result is the most comprehensive, representative and objective dataset of cyber claims financial impact in existence.

Having said that, it is our sincerest hope that each year more and more insurers and brokers will participate in this study and share even more claims and more information about each claim. It is important that measurable progress be assessed and discussed along the way while providing a good dose of reality.

For the benefit of the industry overall, we encourage all underwriters to participate in next year's NetDiligence study. We also hope that each participating insurer shares a larger percentage of their cyber claims. If we can expand participation in these two ways, our findings will be richer and more representative of changing market conditions.

Insurance Industry Participants

We want to thank the following companies whose participation made this study possible:

AIG	Ascent Underwriting	Aspen Insurance	AXA XL	Beazley	CFC Underwriting
Chubb Group of Insurance Companies	CUNA Mutual Group	Great American Insurance Group	Hiscox	Hylant	Kiln
Liberty International Underwriters	Lockton	NAS	Nationwide	OneBeacon Insurance Group	Philadelphia Insurance Companies
Safehold Special Risk	Sompo International	Travelers	United States Liability Insurance	USI	Zurich NA

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 and a Distinguished Fellow of the Ponemon Institute, who analyzed the data submitted for this study and wrote 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 riskcentricsecurity.com.

Other

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

Heather Osborne, Sponsorships
Director of Global Events & Programming, NetDiligence

Sharon Lyon, Publisher
President, Lion's Share Marketing Group, Inc.

Platinum Sponsor

The 2018 Cyber Claims Study highlights the complex breach response landscape businesses are facing today. The uptick in unpredictable and unique threats such as ransomware and cyber extortion adds a new layer of complexity to the already complex response landscape. While businesses cannot block every type of attack against their sensitive information, they can and should take steps to ensure they are ready to respond to their customers with quality, speed, and care after a data breach.

New regulations across the globe (such as the GDPR, NYDFS and the California Consumer Privacy Act) demand as-fast-as 72-hour reaction times to data breach events. This means that businesses must take a proactive approach to breach readiness, and be certain their plans and teams will hold up to a live breach incident. To that end, there are two key components a business must have to be ready to execute a customer response:

Documented Customer Response Plan

The biggest gap we see in even the most robust incident response plans are the details of how to execute a customer-facing response, despite this being the most visible part of a response. To be ready to respond to customers in a way that helps restore trust and brand loyalty, businesses should take a few keys steps:

- Build and document the details of your customer-facing response, including notification and communication plans, identity theft protection offerings, and how you your business will handle the influx of customer questions
- Identify a response partner with the resources to execute that plan
- Secure response guarantees if they are appropriate for your business

Pressure Tested Customer Response Plan

Having a documented customer response plan is the first step toward success, however, it does not tell a company whether or not they are able to execute during a live response. To know this, every business must run their response team and plan through a breach response war game to simulate the real pressures of a data breach. Not taking this critical

step is what can lead to a poor response, creating a chaotic situation for businesses. Here are some components a war game should include:

- Mock "discovery" of the data breach, either by an internal or external party (like the media)
- Activation of your incident response team to assess the situation, review their plans, and launch the appropriate response steps
- Simulated customer notification
- Activation of call center services and identity protection offerings

A data breach is one of the most trying events a business will face. Through continued opportunities for collaboration and information sharing among industry leaders, like this study, we will develop a more comprehensive picture of actionable ways to make breach response more effective and efficient, driving better outcomes for industry partners, businesses, and their customers.

About AllClear ID

AllClear ID provides comprehensive breach response services to help businesses protect their greatest asset: their customers. With over 10 years of experience helping thousands of businesses prepare, respond, and recover from the most destructive, complex breaches in history, AllClear ID is recognized for our expertise, partnership, and innovative solutions. Learn more: **www.allclearid.com/business** or email **ResponseTeam@allclearid.com**

Sponsor

Understanding the cybersecurity threat: The importance of a risk assessment

Data carries a high value to cybercriminals who seek sensitive customer and employee data or intellectual property. Unfortunately, it is also valuable to cybercriminals who seek sensitive customer and employee data or intellectual property. In fact, a **recent survey** issued by RSM US LLP found that the number of middle market companies reporting breaches has nearly tripled in the last three years.

One item that organizations should consider when evaluating their security posture is whether they have conducted a risk assessment. Risk assessments help you prioritize remediation areas, and can provide insights into the how your security program is performing overall. Additionally, by correlating it back to your cyber insurance policy you can discover whether you are adequately covered should your organization experience a breach.

It is also important that key stakeholders are aware of how their cybersecurity budgets are allocated. The cybersecurity special report revealed that 97 percent of executives are moderately to very confident in their organization's ability to safeguard data and yet there has been a 160 percent increase in breaches in midsize businesses since 2015. A potential explanation is that rising cybersecurity budgets are giving executives false confidence that they are equipped to handle any problems that arise. By conducting regular risk assessments, stakeholders can be sure that their dollars are put towards the most impactful threats.

Cyber threats are going to continue to evolve and attackers will continue to get smarter. By fully understanding where your organization's security program stands you will be better equipped to withstand the threats.

About RSM US

RSM US LLP is the leading provider of audit, tax and consulting services focused on the middle market, with 9,000 people in 90 offices nationwide. 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 over 120 countries. RSM uses its deep understanding of the needs and aspirations of clients to help them succeed. For more information, visit **rsmus.com**.

About

NetDiligence®

NetDiligence® (https://netdiligence.com) 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.

NetDiligence has conducted thousands of enterprise-level **QuietAudit®** Cyber Risk Assessments for a broad variety of corporate and public entity clients. The QuietAudit platform that our engineers use to conduct assessments can also be licensed for Vendor Risk Management and/or Underwriting Loss Control.

The **eRiskHub®** portal (https://eriskhub.com) is licensed by more than 50 cyber liability insurers to provide cyber risk management and breach recovery services to their clients.

Breach Plan Connect® (https://breachplanconnect.com) is an affordable, easy-to-use service that assists organizations with data breach response planning.

NetDiligence's **Cyber Risk Summits** (https:// netdiligence.com/conferences/cyber-conferences) are premier educational and networking events attended by cyber insurers, client risk managers, privacy attorneys, cybersecurity experts and regulators from all over the globe. NetDiligence hosts Cyber Risk Summits annually in Philadelphia, Santa Monica, Toronto, London and Bermuda.

QuietAudit®

Cyber Risk Assessments—Consultant Led

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
- Bolster their defense posture in the event of class action lawsuits

NetDiligence offers a variety of consultant-led assessments that are tailored to meet the unique needs of small, medium and large organizations, including:

Cyber Health Check

NetDiligence assesses the organization's data security strengths and weaknesses, including data security "scores" for each key practice area. NetDiligence's Executive Summary report of its findings includes actionable recommendations to improve the organization's overall cyber risk posture.

CFO Cyber Risk Assessment—Consultant Led

In addition to conducting a thorough and comprehensive Cyber Health Check assessment, NetDiligence performs a network vulnerability scan to test the effectiveness of firewalls and web servers. Our scan can identify 6,000+ vulnerabilities that hackers can exploit, including unpatched, non-hardened or misconfigured externally-facing network servers and devices.

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®

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, as well as a free QuietAudit Cyber Risk Assessment online survey. Breach Plan Connect can optionally include one-click hotlinks to the insurer's eRiskHub portal.

Contact Us

For more information about NetDiligence or any of our service offerings, please email us at **management@netdiligence.com** or call us at 610.525.6383.

Study Methodology

In 2018, we asked the major underwriters of cyber liability to submit claims information based on the following criteria:

- The incident occurred between 2015 and 2017
- The victimized organization had some form of cyber or privacy liability coverage

We sent requests for data to 52 individuals at 37 organizations in the United States, Canada and the United Kingdom. From this group, 19 individuals representing 17 organizations provided 538 analyzable new claims, using our proprietary claims data collection worksheet.

The 2018 report also includes data from NetDiligence® studies published in 2014–2017, representing 663 incidents that occurred in 2013, 2014, 2015, 2016 and 2017. The combined dataset comprises 1,201 incidents, *each one, a data breach insurance claim*. This number represents a 100% increase in the number of claims analyzed compared to last year.

1,133 of the cases in the dataset represent claims from American organizations, 10 cases from Canadian organizations, 9 cases from organizations in the United Kingdom and 3 cases from organizations in Australia. There are also 4 claims (1 each) for organizations in China, Germany, Ireland and South Africa. The country was not specified in 42 claims in the dataset.

627 claims (52%) specified the number of records exposed and 982 claims (82%) included an accounting of Crisis Services Cost. When factoring in SIRs, we were able to calculate total data Breach Cost to date for 1,194 (99%) of the claims in the dataset.

768 (64%) of the claims in the dataset are flagged as closed, 392 (33%) as open and 41 (3%) as unknown claim status. 1,008 (84%) of the claims are for primary coverage, 38 (3%) for excess coverage and 155 (13%) have an unknown, but most likely primary, coverage level.

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 Cost 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 cost reported as a lower bound—i.e., we know that a given breach has cost at least the amount specified, but we cannot say how much more than that amount it may have cost.
- Having said that, beginning in 2017, we asked respondents to provide us with an estimate of the total cost of the breach, including amounts that were excluded due to policy provisions. While a few participants in 2017 provided these estimates, an increased number of participants did so in 2018, thereby increasing our ability to understand the true cost 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 including self-insured retentions (SIRs), which ranged from $0 to $15 million.
- In statistical terms, our sample is a "convenience" sample, which means that we have taken the data we have been given and have described it. We cannot make any statements about "significance" or "non-significance."

It is important to note that approximately one-third of the claims submitted for this study remain 'open,' therefore aggregate cost as presented in this study represent "payouts to date" and "Breach Cost to date." It is virtually certain that additional payouts will be made on a number of the claims in the dataset and therefore the costs in this study are almost certainly understated.