

NetDiligence[®]

2017 CYBER CLAIMS STUDY



Contents

Introduction	1
Key Findings	2
A Look at the Overall Dataset	4
Records Exposed.....	4
Costs Overall	5
Cost Per Record	5
Crisis Services Costs	6
Legal Defense and Settlement	9
Regulatory Defense and Fines.....	9
Viewing the Data through Different Lens	10
Type of Data Exposed	10
Records Exposed	11
Costs.....	12
Cause of Loss	13
Records Exposed	13
Costs.....	15
Business Sector.....	16
Records Exposed	17
Costs.....	18
Size of Affected Organization (based on revenue)	20
Records Exposed	21
Costs.....	22
Insider Involvement	23
Third-Party Breaches	26
Cloud Involvement.....	28
Ransomware/Cyber Extortion	29
W-2 Fraud	30



Phishing/Business Email Compromise (BEC)/Wire Transfer Fraud.....	31
Wire Transfer Fraud.....	33
Point of Sale (POS) Related/Common Point of Purchase (CPP) Investigations.....	34
Intellectual Property/Trademark Infringement.....	35
Business Operating Losses.....	36
A Word about First- and Third-Party Claims.....	37
Conclusion.....	38
Insurance Industry Participants.....	39
Contributors.....	39
Risk Centric Security, Inc.....	39
Other.....	39
Platinum Sponsor—AllClear ID.....	40
Sponsor—RSM US.....	42
Sponsor—Cipriani & Werner.....	43
Sponsor—Symantec.....	44
About NetDiligence®.....	46
Study Methodology.....	49

Note: Figures 8, 11, 14, 17 are omitted by design. They appear only in the eRiskHub® Exclusive Expanded Edition of the report.



Introduction

NetDiligence® is pleased to present its seventh annual *Cyber Claims Study*. Our objective is to provide reliable, insightful, rigorous and informed analysis. By consolidating claims data from multiple insurers, we strive to subdivide the information into meaningful and manageable chunks. Our goal is to create an information repository that technologists and executives can call upon to solve problems and find answers to specific issues.

The 2017 *Cyber Claims Study* is pivotal with extensive data-driven analysis distilled and modeled in three distinct measures: numbers of records, costs of breaches, and per record costs. Notable in this year's study, we have contrasted and compared datasets aggregated over the last four years.

The data graphics provided distinguish the rich and complex statistical material, successfully organizing a large collection of numbers and making comparisons between different parts of the data narrative.

In coming years, we will closely follow costs associated with exposures for companies that have a presence in the EU. The General Data Protection Regulation (GDPR) goes into effect in May 2018. This regulation applies to all EU member countries and companies based in those countries and any non-EU companies that process the data of EU citizens. The maximum fines for lack of compliance could be enormous — up to 4% of overall turnover/revenues or €20M, whichever is greater.

“Many security studies focus on the technical aspects of an incident, which is useful in helping organizations understand the ways in which a security incident can occur. However, these studies fail to include the robust business data necessary for organizations to actually make strategic decisions that address the motivations, targets and damages associated with a breach. This study cuts through the ‘sound and fury’ of the usual cybersecurity alarms by providing the information necessary for organizations to effectively manage their cyber risks.”

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

Key Findings

Retail exposed 67% (420M) of the number of records in the total dataset.

Companies with less than \$50M in revenue were the most impacted, accounting for 47% of the claims.

The average total breach cost was \$394K, the median \$56K.

Companies with revenues greater than \$2B suffered an average breach cost of \$3.2M.

The largest Regulatory claim was upwards of \$6M.

Cyber Event Recovery expense was reported as high as \$475K.

The Gaming & Casino Sector incurred the highest Forensics costs averaging \$345K, as well as the highest median breach cost of \$190K.

Healthcare claims for Notification were the highest at \$695K.

The median cost of Third-Party breaches was comparable to in-house events, but exposed twice as many records.

Wire Transfer Fraud & Theft of Money averaged \$179K in breach cost.

Ransomware / Cyber Extortion affected every sector with maximum breach costs in excess of \$500K.

Trademark Infringement and / or the Loss of Trade Secrets averaged \$865K, with a median of \$182K and a maximum of \$4.9M.

Healthcare and Professional Services suffered 44% of the fraudulent W-2 claims.

Breach costs were 20% higher when there was Cloud involvement.

The average per-record cost was \$8K, the median \$46.50.

PCI data was exposed in 16% of claims but accounted for 67% of records. PHI data represented 15% of claims and 17% of exposed records, while PII data accounted for 36% of claims but only 16% of exposed records. PCI, PHI and PII data accounted for 99% of all records exposed.

Maliciously motivated Insider events resulted in more expensive claims by a factor of four.

The median payout (\$64,324) for PCI Fines was similar to last year. The average of these fines was \$389K. The maximum PCI fine paid was \$3M.

Lost or Stolen Devices more than doubled in claims this year, and Paper Records claims almost tripled.

Hackers were identified as the most common Cause of Loss, followed by Malware / Virus, Ransomware / Cyber Extortion and Staff Mistake.

Maximum Notification cost, when compared to last year, increased 176% to \$5.52M; average Notification cost was 39% higher.

Note: The eRiskHub® portal contains a database of anonymized data from all our claims studies for the exclusive use of eRiskHub licensors and their clients. For more information about the eRiskHub, contact Mark Greisiger at mark.greisiger@netdiligence.com.

A Look at the Overall Dataset

Records Exposed

In claims that reported records, the number of records exposed ranged from 1 to 110M. The average number was 1.8M, the median was 1,091. The average for the period 2014–2017 is the lowest since 2011.

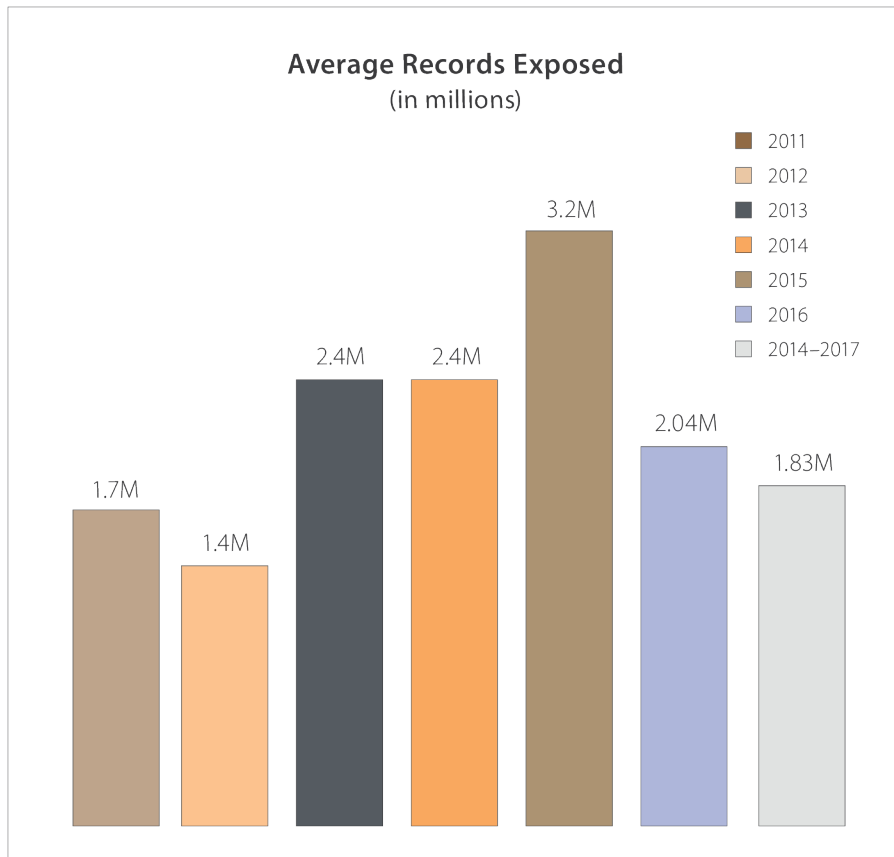


Figure 1

Costs Overall

Total breach costs for the claims submitted in years 2014–2017 were \$202M. The smallest breach cost reported was \$110 while the largest was \$16.8M. The average cost for the period 2014–2017 was \$394K; the median cost was \$56K.

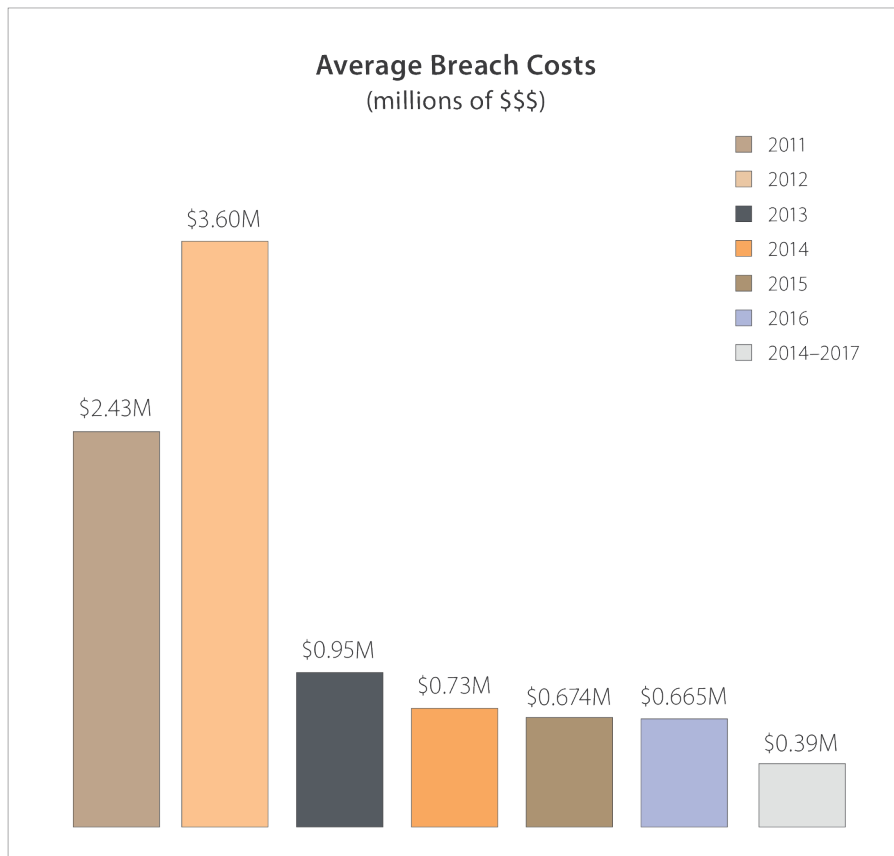


Figure 2

Cost Per Record

Cost Per Record can be a controversial metric because it is difficult to find a useful relationship between the number of records exposed and the total cost of a breach. Examining the 2014–2017 dataset, it is interesting to note that the costs per record range from a few pennies to over \$1.5M

Fifty percent of the claims in the dataset reported both the number of records lost and the total breach cost. As mentioned in the key findings, the average cost per record was \$8,100, while the median cost was \$46.50.

The Per Record numbers are heavily skewed by outliers — data points that are either much bigger or much smaller than the other data elements. Excluding the top and bottom five and ten percent of the dataset, the average cost per record changed substantially, coming in at \$787 (95% of the data) and \$303 (90% of the data). The median cost per record of \$46.50 did not change¹.

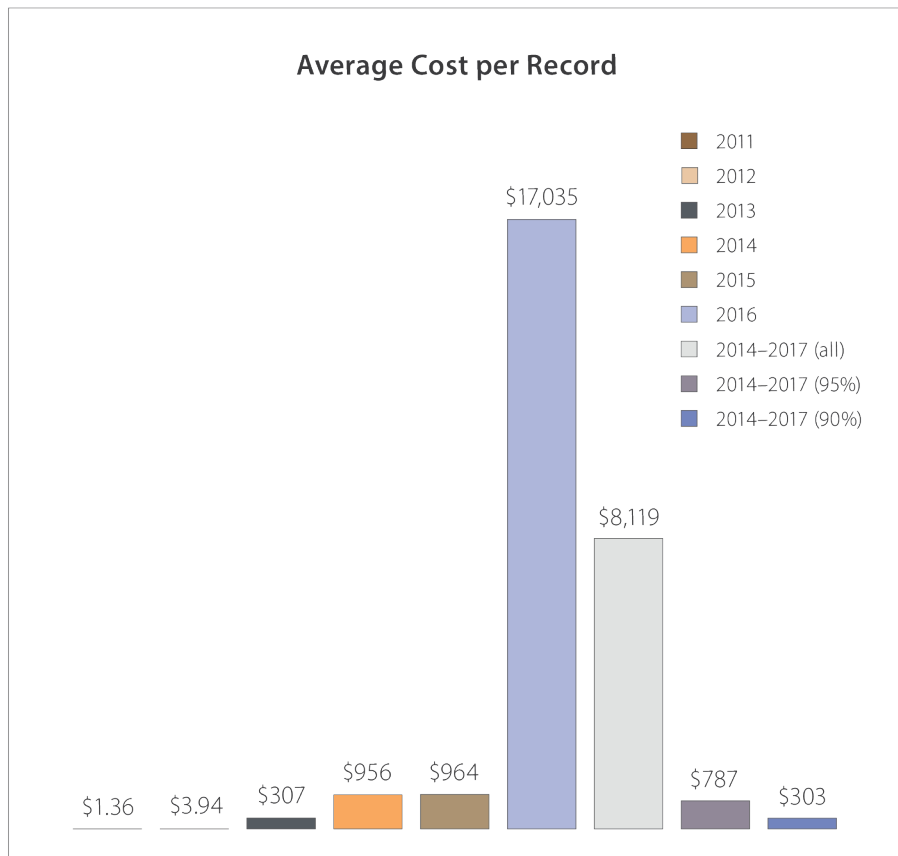


Figure 3

Crisis Services Costs

Eighty-seven percent of claims (2014–2017) included costs for one or more components of Crisis Services. The smallest claim for Crisis Services was \$14, while the largest claim was \$8.2M. The average for Crisis Services was \$249K, the median \$36K.

“Over the last year, we’ve seen regulators take action ensure customers will be protected in the event of a data breach. To meet the new regulatory mandate and protect customers after a data breach, businesses must move past simply having a documented response plan to operationalizing that plan prior to a breach occurring. Working with crisis services vendors should be a critical component of every business’ breach readiness efforts.”

Bo Holland
President,
AllClear ID

¹eRiskHub® license holders and their clients will find the full percentile analyses in the long form of the report available exclusively in the eRiskHub®.

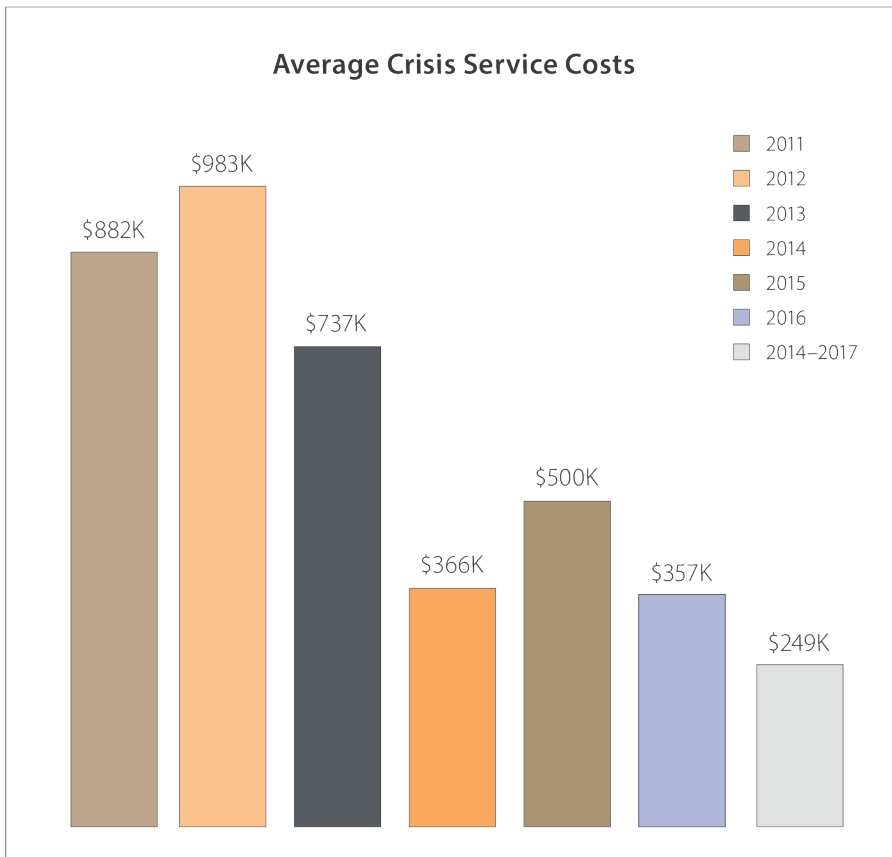


Figure 4

Not all claims detailed the services that comprise Crisis Services. Of the claims that detailed these costs, 62% included Forensics, 31% included Notification, 26% included Credit/ID Monitoring and 76% included Legal Guidance/Breach Coach®. These numbers reflect all claims that reported a dollar figure for one or more specific services. This year, 16% included costs associated with Public Relations and Post-Breach Cleanup.

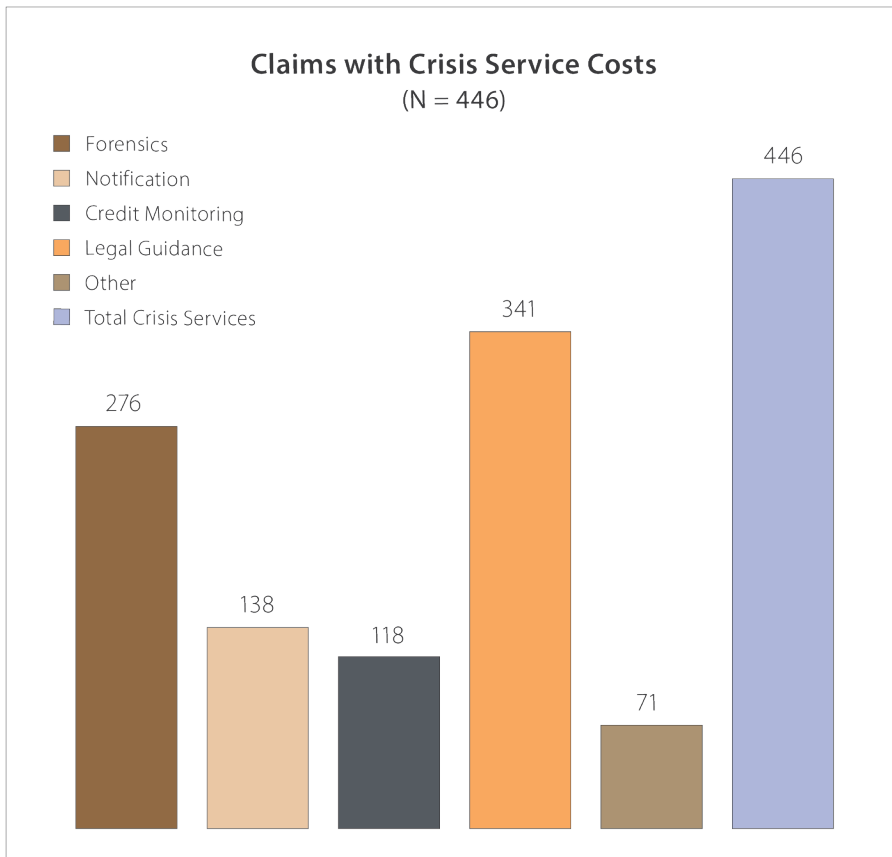


Figure 5

Table 1 below presents a breakout of Crisis Services Costs aggregated for the reporting years 2014–2017. Forensics costs ranged from \$265 to \$3.86M—this maximum represents a 57% increase from last year’s report. Notification costs, when compared to last year, were lower on one side of the scale, paying out \$14 as a minimum, however increasing by 176% to \$5.52M as a maximum and a 39% higher average. Public Relations and Other costs were up dramatically with a range of \$149 to \$2.0M, and an average of \$81K compared to \$54K last year.

Crisis Services Costs 2014–2017

	Cases	Min	Average	Median	Max
Forensics	276	265	141,479	35,175	3,860,000
Credit/ID Monitoring	118	10	112,886	5,511	2,000,000
Notification	138	14	234,011	13,323	5,520,000
Legal Guidance / Breach Coach®	341	112	53,133	14,922	2,500,000
Other	71	149	80,643	10,295	2,000,000
Total Crisis	446	14	248,980	35,577	8,209,000

Table 1

Legal Defense and Settlement

By including the data from the past three studies, we have been able to make a meaningful analysis of Legal Defense and Settlement claims. The gap between the lowest and highest defense payouts ranged from \$319 to \$2.5M. Legal Settlements were as low as \$1,500 but as high as \$4.8M. The average for Legal Defense was about the same as in 2016, but the Legal Settlement average was three times lower.

**Legal Costs—Damages Defense
& Settlement 2014–2017**

	Cases	Min	Average	Median	Max
Legal Damages Defense	64	319	120,606	15,500	2,500,000
Legal Damages Settlement	37	1,502	254,851	50,000	4,800,000

Table 2

Regulatory Defense and Fines

Combing data from the past three studies also enabled us to make a more meaningful analysis of the legal costs associated with regulatory matters. Regulatory Defense costs averaged \$697K, ranging from \$25K to \$5.8M.

**Legal Costs—Regulatory Defense
& Fines 2014–2017**

	Cases	Min	Average	Median	Max
Regulatory Action Defense	10	25,163	696,524	83,750	5,791,000
Regulatory Action Fines	2	28,943	44,634	44,634	60,324

Table 3



Viewing the Data through Different Lenses

Type of Data Exposed

Data breaches exposing PII represented 36% of the claims in the dataset; PCI, 16%; and PHI, 15%. Non-card Financial information was exposed in 5% of the claims. Compared to last year's study, there was a higher number of cases reported relating to the theft of Trade Secrets or Intellectual Property/Trademark Infringement.

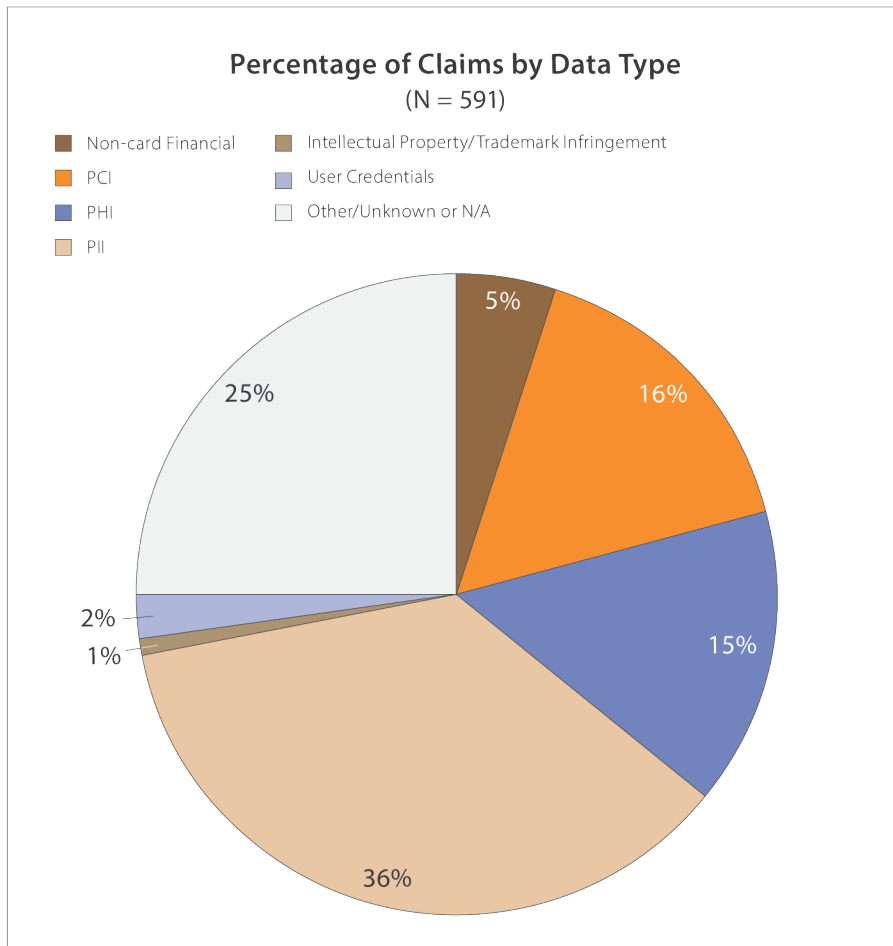


Figure 6

Records Exposed

There were 343 claims in the dataset that provided the number of records exposed and the data type. Per the chart below, PCI, PHI and PII comprised over 99% of the total records exposed. Of this 99%, two-thirds involved the exposure of PCI data.

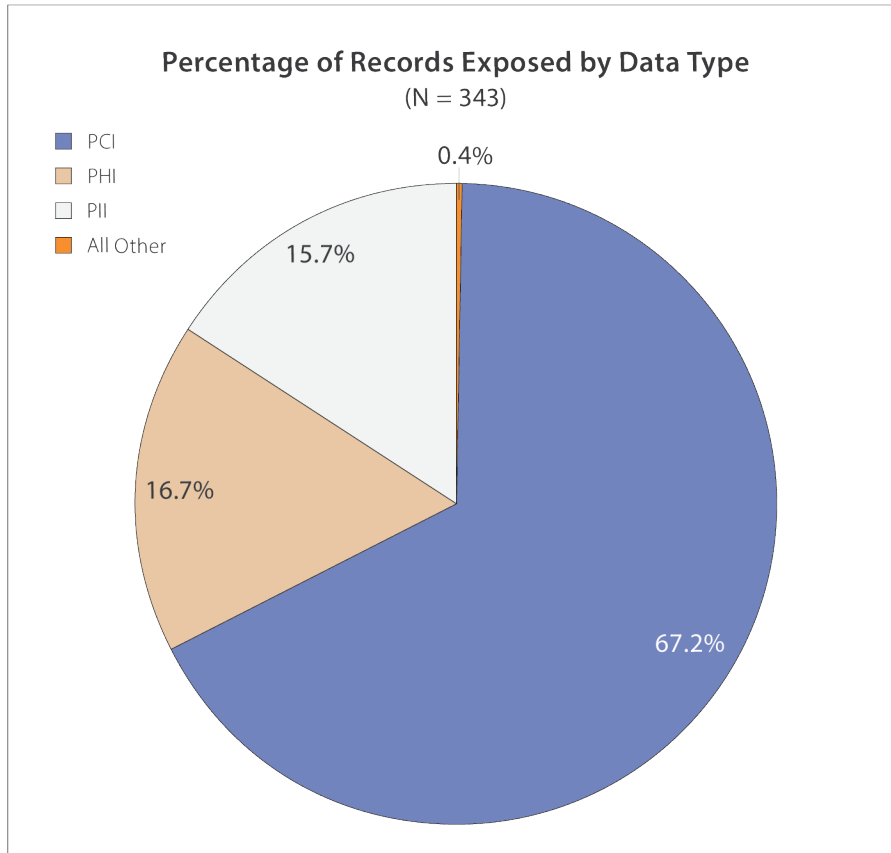


Figure 7

Records Exposed by Data Type 2014–2017

	Cases	Min	Average	Median	Max	Total
Business Email Compromise (BEC)	2	1	26	26	50	51
Non-Card Financial	14	2	59,332	525	700,000	830,652
PCI	65	12	6,506,044	12,300	110,000,000	422,892,838
PHI	61	1	1,718,327	1,091	78,000,000	104,817,959
PII	164	1	601,331	602	80,000,000	98,618,306
User Credentials (Login & Passwords)	6	1	21,303	897	120,000	127,820
Other, Unknown or N/A	31	1	55,273	463	1,100,000	1,713,450

Table 4

Costs

There was a wide range of breach costs for every data type, from a minimum of \$110 up to \$16.8M. Intellectual Property/Trademark Infringement had the highest average breach cost reaching \$865K, with PCI-related breaches closely following at \$844K. Following the top four categories, the average breach costs drop off significantly.

Total Breach Costs (Including SIR) by Type of Data 2014–2017					
	Cases	Min	Average	Median	Max
Business Email Compromise (BEC)	6	74,459	279,185	199,839	866,817
Intellectual Property/Trademark Infringement	7	11,821	864,964	182,484	4,961,000
Non-Card Financial	21	11,280	684,646	69,302	11,491,000
Other Non-Public Data	6	7,000	47,727	29,932	114,645
PCI	81	6,670	843,993	94,351	16,849,411
PHI	82	290	612,367	50,881	15,000,000
PII	172	110	229,590	46,974	8,959,000
User Credentials (Login & Passwords)	10	4,300	144,560	42,989	926,452
N/A	35	561	128,082	52,545	1,049,643
Other	32	1,190	240,086	76,196	1,606,550
Unknown	62	2,062	146,226	51,465	2,740,020

Table 5

Cause of Loss

Cause of Loss is an important metric. Hackers again top the chart with the most claims, followed by Malware/Virus, Ransomware/Cyber Extortion and Staff Mistake. Business Email Compromise and Wire Transfer Fraud appear as categories for the first time this year. The Lost or Stolen Device category more than doubled this year and the Paper Records category almost tripled.

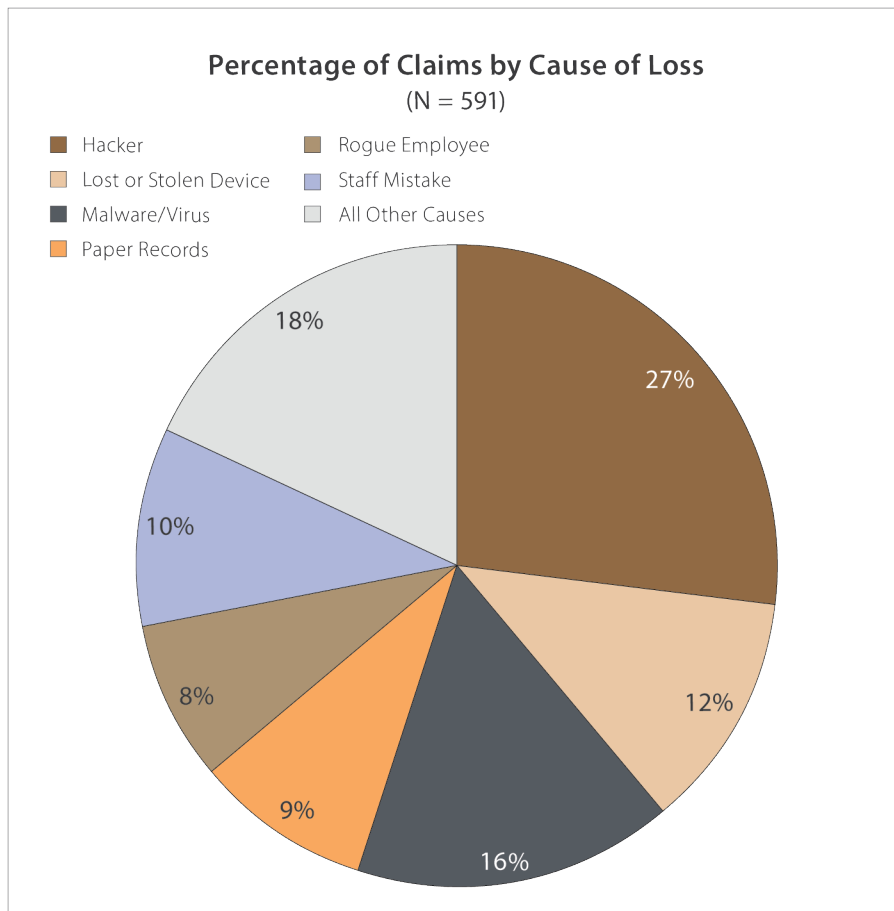


Figure 9

Records Exposed

When looking at the number of records exposed by Cause of Loss, Hackers and Malware/Virus are the categories responsible for exposing 99% of all records, with the remaining twelve categories adding up to only 1% of the dataset analyzed.

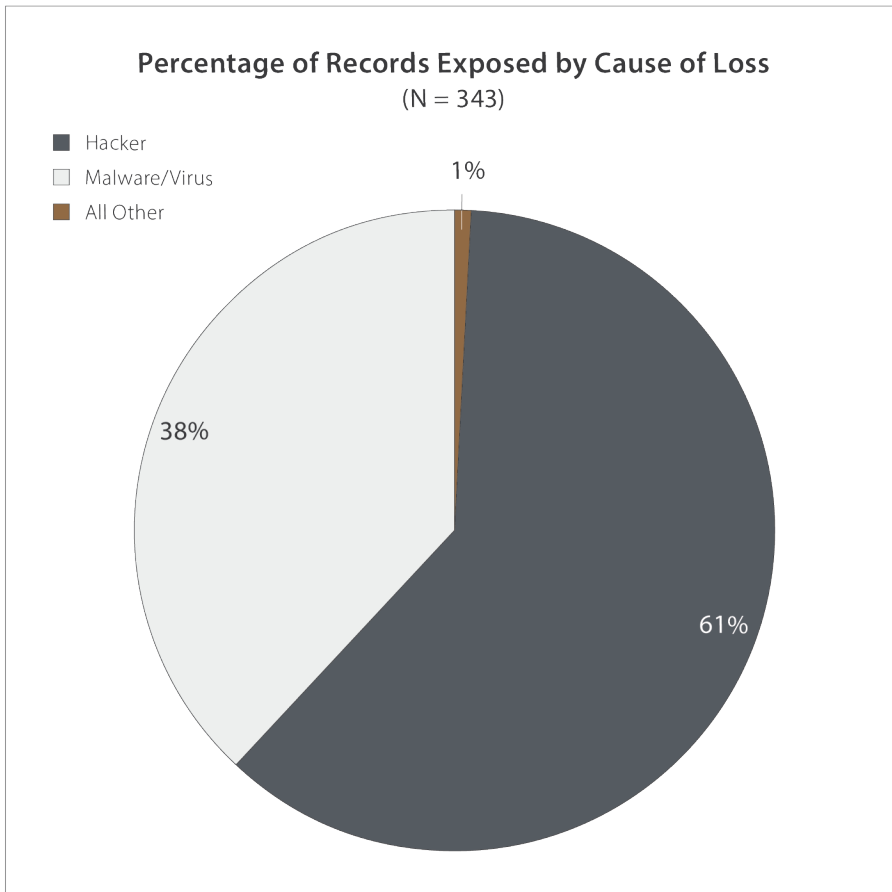


Figure 10

Records Exposed by Cause of Loss 2014–2017

	Cases	Min	Average	Median	Max	Total
Business Email Compromise (BEC)	13	6	2,076	337	11,335	26,984
Hacker	91	1	4,224,996	9,000	80,000,000	384,474,620
Lost or Stolen Device	42	1	11,374	998	174,000	477,700
Malware/Virus	54	1	4,440,138	2,612	110,000,000	239,767,456
Paper Records	30	1	2,245	168	36,398	67,348
Phishing	5	213	3,193	1,500	8,161	15,965
Ransomware/Cyber Extortion	7	22	134,181	178	900,000	939,269
Rogue Employee	26	1	36,919	832	700,000	959,888
Staff Mistake	33	1	48,200	80	1,100,000	1,590,587
System Glitch	15	2	28,052	1,481	248,900	420,783
Theft of Money	3	99	1,100	200	3,000	3,299
Wire Transfer Fraud	1	94	94	94	94	94

Records Exposed by Cause of Loss 2014–2017

	Cases	Min	Average	Median	Max	Total
Wrongful Data Collection	2	13	90	90	167	180
Other	21	25	12,233	357	100,000	256,903

Table 6

Costs

Analyzing the total breach costs by the Cause of Loss provides insight into which incidents resulted in the highest breach costs. Incidents initiated by the malicious activity of Hackers, Malware/Virus and Rogue Employees resulted in higher average costs than incidents produced by simple errors, such as Staff Mistakes. Compared to claims submitted in 2016, there was a significant increase in the number of claims due to Lost or Stolen Devices and Paper Records. However, the median cost for Lost or Stolen Device claims was almost the same as last year's median cost. And this year's median cost for incidents involving Paper Records was half of last year's median. Also of note are the costs reported for the new categories of Business Email Compromise and Wire Transfer Fraud.

Total Breach Costs (including SIR) by Cause of Loss 2014–2017

	Cases	Min	Average	Median	Max
Business Email Compromise (BEC)	17	2,619	67,723	37,209	340,671
Hacker	116	4,440	1,060,213	93,275	16,849,411
Lost or Stolen Device	44	290	89,942	56,926	397,900
Malware/Virus	83	1,190	457,817	80,700	8,959,000
Paper Records	26	110	41,452	26,819	224,949
Phishing	4	10,876	92,245	77,909	202,286
Ransomware/Cyber Extortion	55	561	64,967	28,053	519,184
Rogue Employee	27	1,785	481,596	50,862	11,491,000
Staff Mistake	35	225	105,471	10,533	1,603,800
System Glitch	17	1,825	157,802	70,500	779,293
Theft of Money	5	43,336	132,693	52,500	266,631
Wire Transfer Fraud	5	8,615	167,806	45,366	478,771
Wrongful Data Collection	3	11,640	86,242	26,186	220,899
Other	77	1,685	131,576	55,970	2,740,020

Table 7

Business Sector

Professional Services was the sector that experienced the largest number of claims, closely followed by Healthcare. Financial Services and Retail occupied the third and fourth positions. Each of these sectors ranked in the top four in last year's report, although Healthcare and Financial Services held the top two spots in that report.

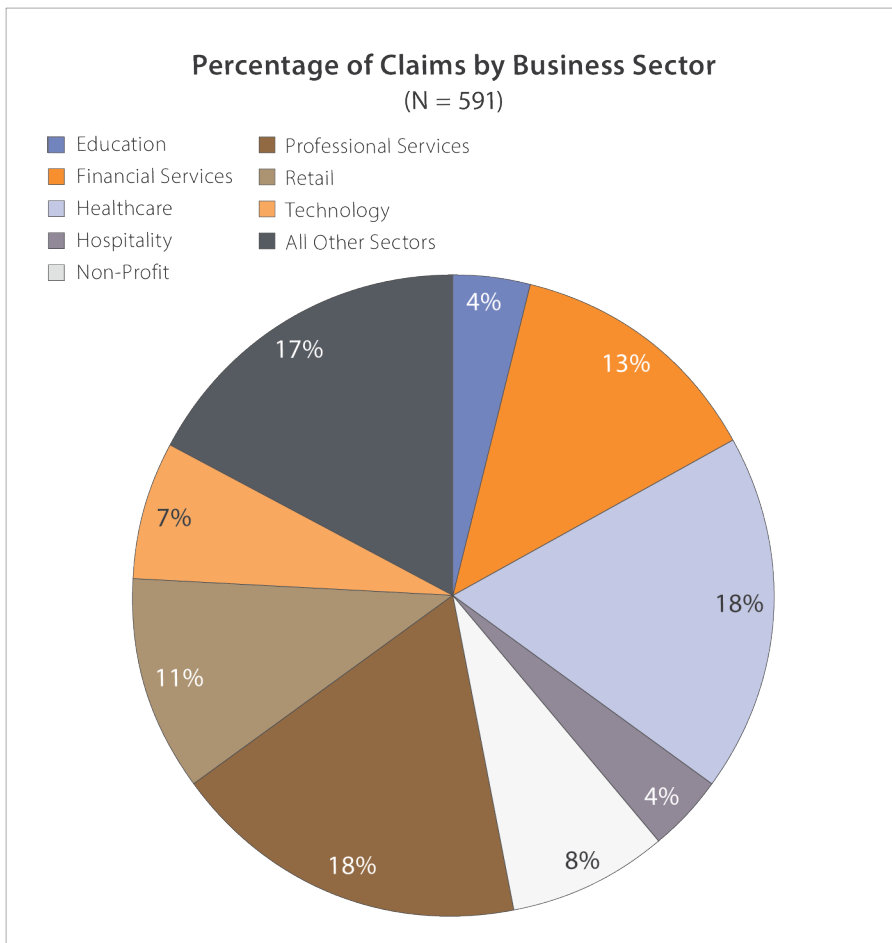


Figure 12

Records Exposed

Retail overwhelmingly exposed the most records, followed by Healthcare and Financial Services. Combined, these sectors accounted for 99% of all records exposed. The other 15 sectors accounted for only 1% of the records exposed.

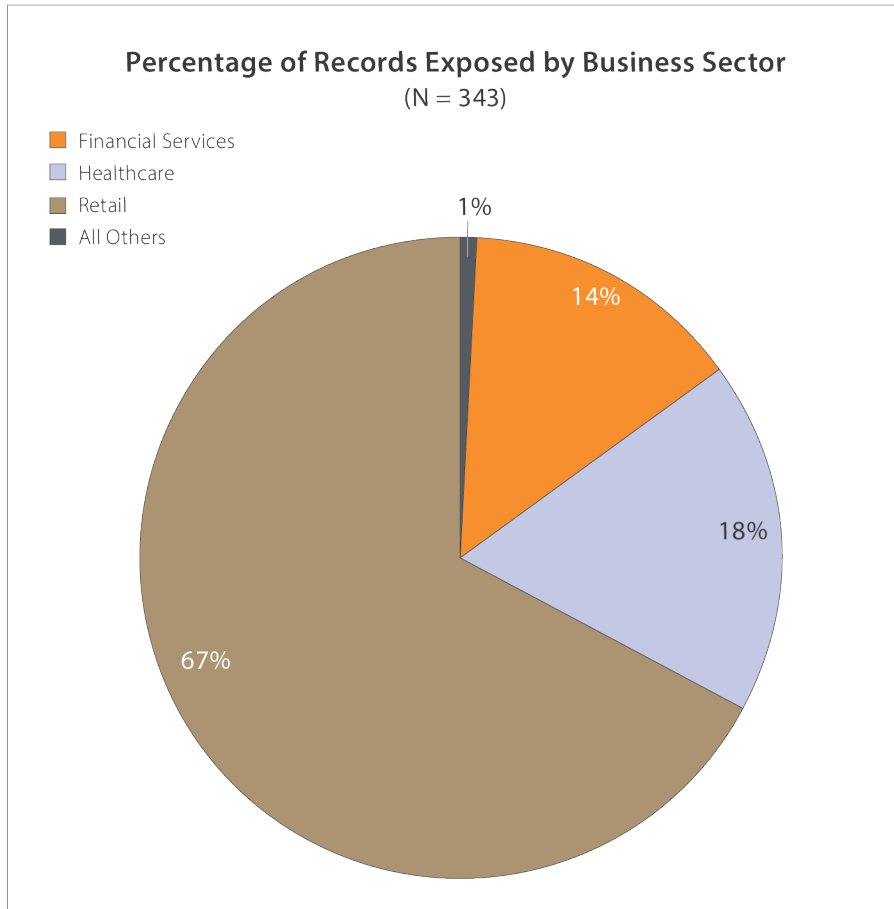


Figure 13

Records Exposed by Business Sector 2014–2017

	Cases	Min	Average	Median	Max	Total
Education	14	12	30,350	1,563	163,299	424,898
Energy	1	6,500	6,500	6,500	6,500	6,500
Entertainment	3	50	666,794	332	2,000,000	2,000,382
Financial Services	49	2	1,807,984	915	78,000,000	88,591,223
Gaming & Casino	2	3,800	51,900	51,900	100,000	103,800
Healthcare	69	1	1,620,000	1,091	80,000,000	111,779,978
Hospitality	19	12	14,807	2,723	100,000	281,325
Manufacturing	4	26	1,264	415	4,200	5,056
Media	2	44	572	572	1,100	1,144
Non-Profit	28	1	6,970	445	163,625	195,161
Professional Services	56	1	31,040	295	1,100,000	1,738,224
Public Entity	4	13	1,902	297	7,000	7,607
Restaurant	3	59	3,953	800	11,000	11,859
Retail	41	1	10,265,272	16,500	110,000,000	420,876,167
Technology	16	13	83,186	938	880,000	1,330,975
Telecommunications	3	9,000	436,333	300,000	1,000,000	1,309,000
Transportation	2	31	4,616	4,616	9,200	9,231
Other	27	1	12,168	854	163,299	328,546

Table 8

Costs

The Retail and Telecommunications sectors had the highest average costs of \$1M and \$666K respectively. Gaming & Casino and Hospitality had the highest median, both just under \$200K.

**Total Breach Costs (including SIR)
by Business Sector 2014–2017**

	Cases	Min	Average	Median	Max
Education	20	3,241	121,735	54,604	800,000
Energy	2	27,793	31,120	31,120	34,446
Entertainment	7	6,950	170,403	73,968	763,743
Financial Services	60	110	588,263	28,763	15,000,000
Gaming & Casino	4	80,000	396,888	190,775	1,126,000
Healthcare	92	765	537,045	57,335	8,959,000
Hospitality	22	15,909	580,734	176,715	5,650,000
Manufacturing	10	5,152	20,297	18,504	37,790
Media	7	6,000	96,557	73,480	207,574
Non-Profit	41	1,234	132,903	35,095	1,606,550
Professional Services	100	290	140,353	36,285	6,160,000
Public Entity	8	5,675	76,984	45,585	328,000
Restaurant	5	21,070	61,504	70,649	76,000
Retail	52	7,000	1,044,968	95,456	16,849,411
Technology	36	11,000	447,697	109,015	4,961,000
Telecommunications	3	3,500	666,063	12,994	1,981,695
Transportation	7	90,244	167,885	137,500	330,107
Other	38	708	123,929	65,904	800,000

Table 9



Size of Affected Organization (based on revenue)

Revenue size was reported for almost 96% of the claims in the dataset. Companies with less than \$50M in revenue were the most impacted, accounting for almost half of the claims. Companies with \$50–300M in revenue accounted for 24%, followed by companies with \$50–2B in revenues at 16%. Companies with revenues of \$2B–10B accounted for 5%, while companies with revenues of \$10B–100B accounted for 4%. Very few claims (0.3%) were from companies with >\$100B. Revenue size was unknown in 4.4% of claims.

In all, organizations with <\$2B in revenues accounted for 88% of the claims in the dataset. This mirrors our previous findings.

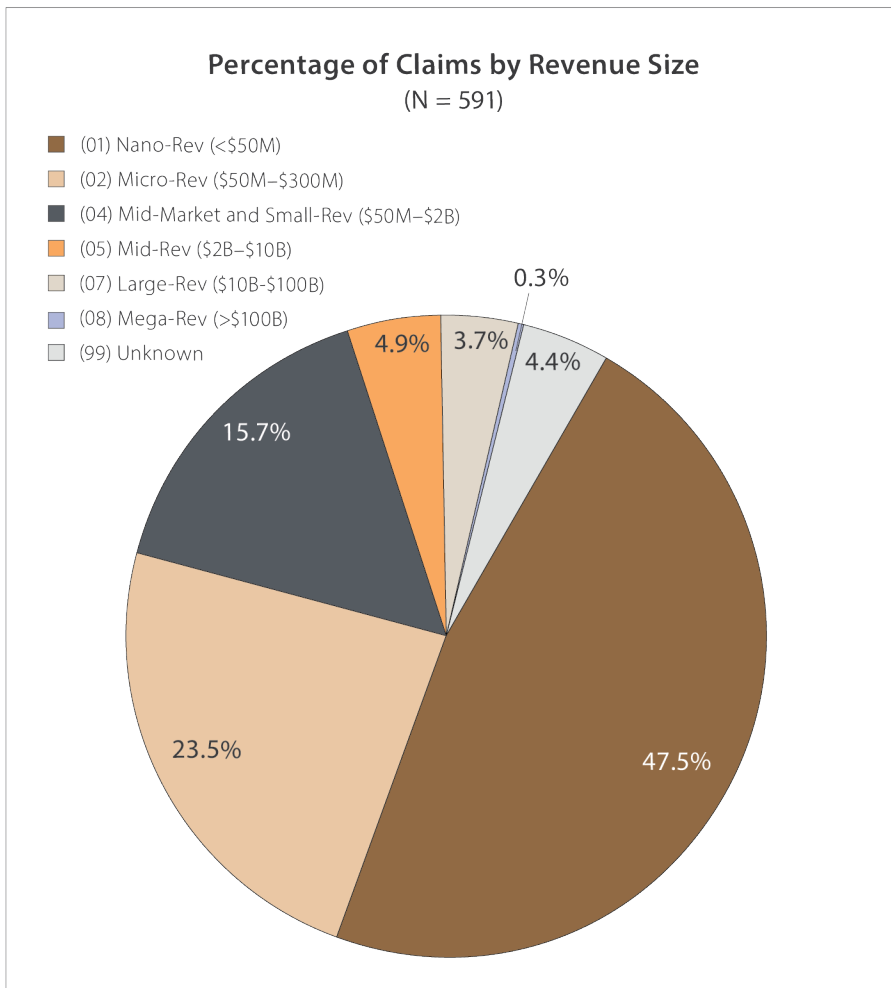


Figure 15

“No company is immune to a breach. This NetDiligence study makes clear that middle market companies are becoming an increased target for cyber attacks. Companies must prioritize data privacy and cyber security to protect consumer trust and confidence, prevent damage to brands and reputations. Failing to do so endangers a company’s ability to remain competitive in today’s market.”

Carolyn Purwin Ryan, Esquire
Partner
Cipriani & Werner PC

Records Exposed

Smaller organizations accounted for 88% of the claims in our dataset, but exposed only 23% of records. Conversely, larger organizations accounted for 12% of the claims, but exposed 76% of records.

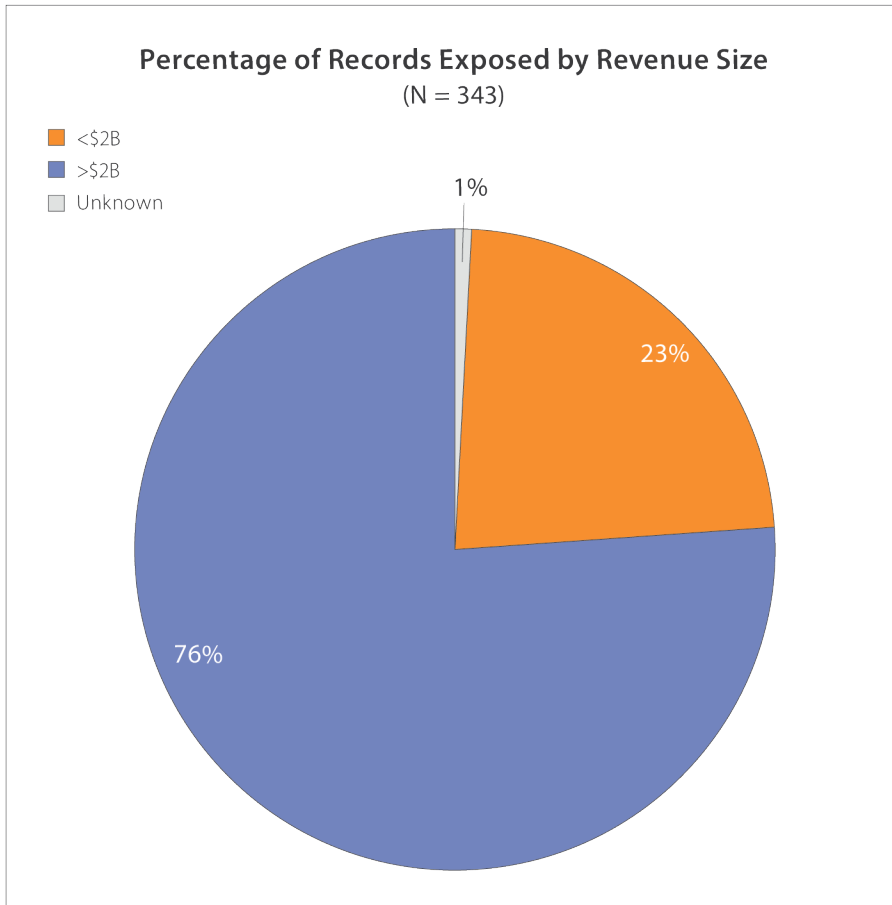


Figure 16

Records Exposed by Revenue Size 2014–2017

	Cases	Min	Average	Median	Max	Total
<\$2B	288	1	499,058	865	60,000,000	143,728,625
>\$2B	41	1	11,669,698	36,026	110,000,000	478,457,635
Nano-Rev (<\$50M)	150	1	507,184	513	60,000,000	76,077,622
Micro-Rev (\$50M–\$300M)	77	1	62,651	915	3,200,000	4,824,163
Mid-Market and Small-Rev (\$50M–\$2B)	61	1	1,029,948	3,800	53,000,000	62,826,840
Mid-Rev (\$2B–\$10B)	20	1	394,754	8,100	3,000,000	5,895,084
Large-Rev (\$10B–\$100B)	19	1	22,203,292	1,200,000	110,000,000	421,862,551
Mega-Rev (>\$100B)	2	700,000	25,350,000	25,350,000	50,000,000	50,700,000
Unknown	14	29	486,773	229	6,500,000	6,814,816

Table 10

Costs

As might be expected, costs for breaches occurring in organizations with revenues >\$2B were substantially higher than costs for smaller organizations. The average cost for a larger organization was more than fifteen times greater than the average cost for a smaller organization.

Total Breach Costs (including SIR) by Revenue Size 2014–2017

	Cases	Min	Average	Median	Max
<\$2B	463	110	194,853	54,533	7,130,000
>\$2B	32	2,662	3,196,698	708,000	16,849,411
Nano-Rev (<\$50M)	259	290	125,195	39,315	7,130,000
Micro-Rev (\$50M–\$300M)	127	225	265,152	81,994	6,570,000
Mid-Market and Small-Rev (\$50M–\$2B)	77	110	313,207	87,389	5,650,000
Mid-Rev (\$2B–\$10B)	21	2,662	1,691,971	171,513	16,894,411
Large-Rev (\$10B–\$100B)	9	1,603,800	5,863,549	2,700,000	15,000,000
Mega-Rev (>\$100B)	2	2,500,000	6,995,500	6,995,500	11,491,000
Unknown	19	765	519,518	34,230	8,959,000

Table 11

Insider Involvement

Of the claims that provided data about insider involvement, 75% indicated no insider involvement at all, 19% were unintentional, introduced primarily by staff mistakes and errors in paper handling, and 6% were malicious in nature.

Insider incidents resulted in the exposure of every type of data and occurred in almost every business sector. Healthcare, Financial Services and Professional Services were the most vulnerable. One Financial Services claim exceeded \$10M.

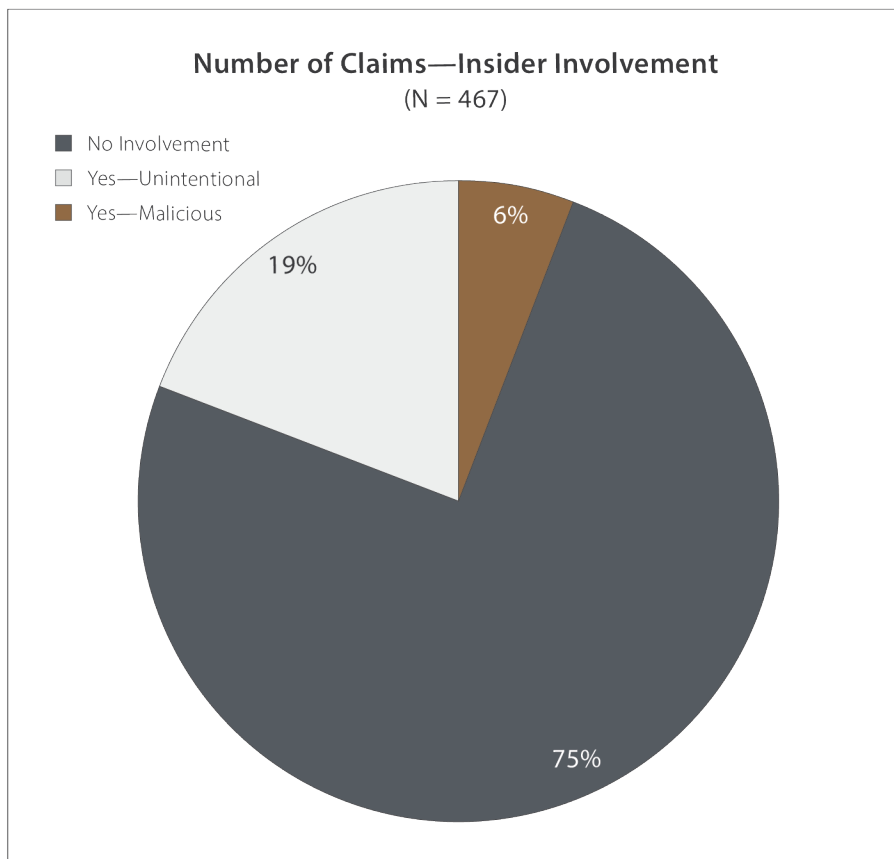


Figure 18

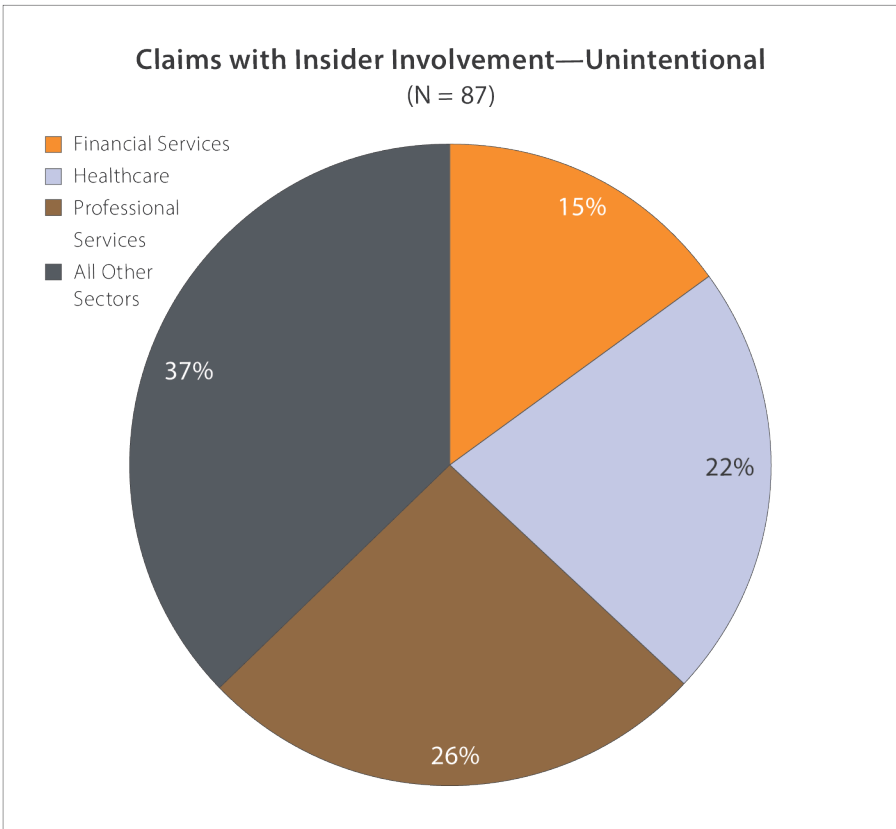


Figure 19

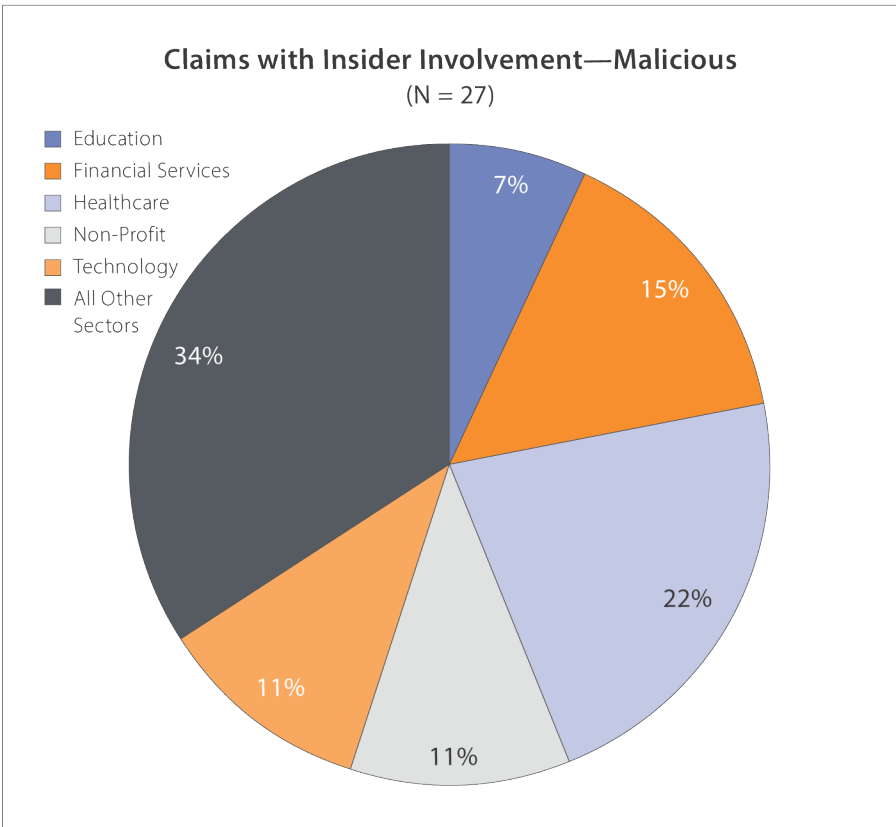


Figure 20

Events with no insider involvement or unintentional involvement had much higher numbers of records exposed, but lower average breach costs. For the first time, total costs were reported for almost all insider-related claims. Maliciously motivated insider events resulted in more expensive average breach costs, by a factor of four.

Insider Involvement 2014–2017

No	Cases	Min	Average	Median	Max
Records Exposed	255	1	2,245,056	1,800	110,000,000
Total Payout	405	110	298,283	43,208	10,000,000
Breach Costs	409	110	433,601	61,544	16,849,411
Cost Per Record	224	0.02	9,282	36.99	1,603,800
Yes—Unintentional	Cases	Min	Average	Median	Max
Records Exposed	65	1	854,716	200	53,000,000
Total Payout	78	14	129,249	13,742	4,936,000
Breach Costs	82	225	144,510	32,823	4,961,000
Cost Per Record	51	0.03	4,095	154	82,500
Yes—Malicious	Cases	Min	Average	Median	Max
Records Exposed	23	1	41,534	900	700,000
Total Payout	23	1,140	447,499	53,385	8,991,000
Breach Costs	23	6,140	573,447	82,230	11,491,000
Cost Per Record	18	0.39	5,050	36.17	89,537

Table 12



Third-Party Breaches

In 13% (77 of 591) of claims, a Third-Party vendor triggered an event—the same proportion as in last year’s study. The greatest percentage of Third-Party breaches occurred in the Retail sector, with Professional Services a close second.

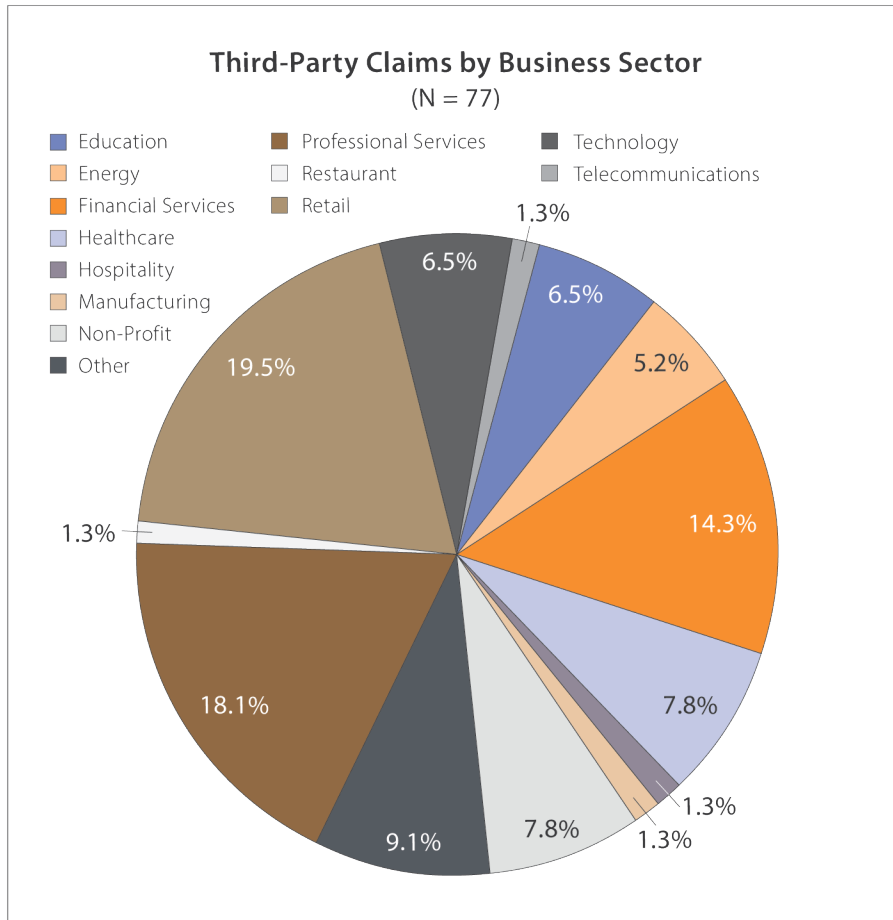


Figure 21

Hackers accounted for three times as many (44%) Third-Party incidents as the second most frequent causes of loss (Malware/Virus at 14%). Other elements that contributed to Third-Party claim events included Lost or Stolen Devices, Paper Records and System Glitches. Each of these causes of loss was cited in 4–12% of the claims in this year’s study.

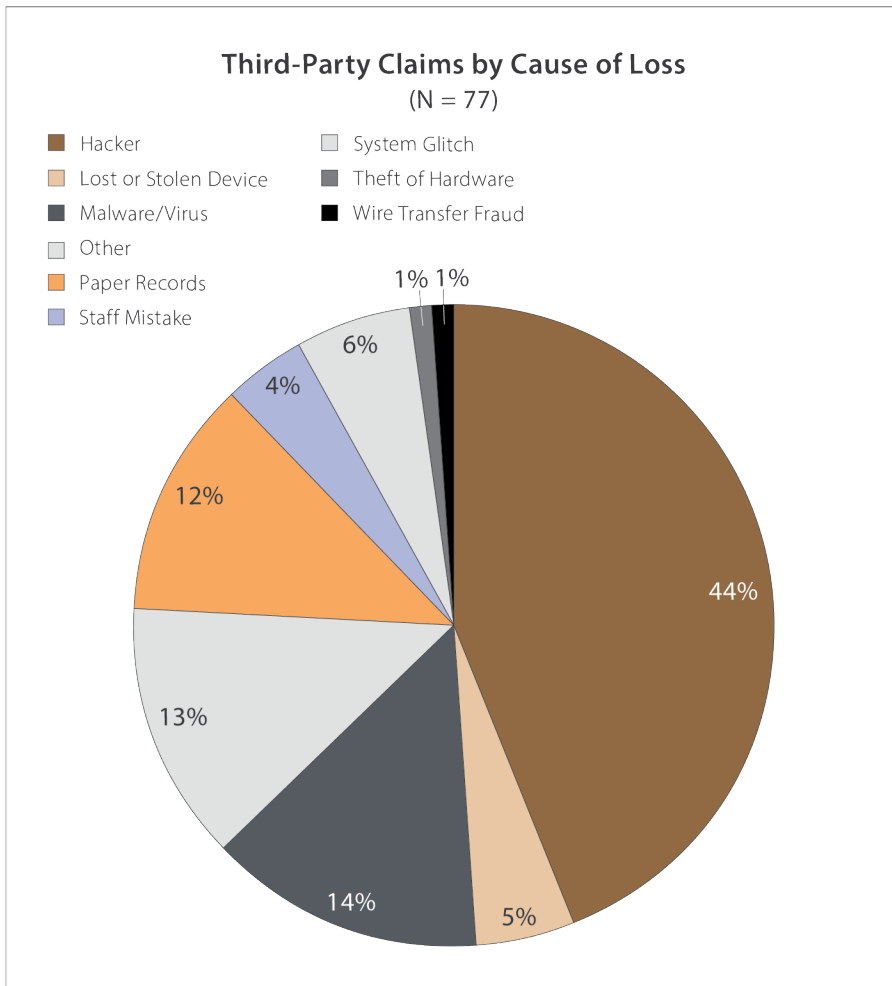


Figure 22

Breach events involving a Third Party exposed almost twice as many records as breaches that did not involve a Third Party. Average costs for Third-Party breaches were not quite a quarter of the payouts of in-house breaches and the maximum cost for an in-house event was over six times greater than a Third-Party event. Median breach costs for both categories were comparable.

Third-Party Involvement 2014–2017

Yes	Cases	Min	Average	Median	Max
Records Exposed	56	2	2,922,504	1,064	110,000,000
Total Payout	55	886	110,450	32,230	2,500,000
Breach Costs	57	661	122,632	43,115	2,500,000
Cost Per Record	40	0.02	1,088	49.66	36,947
No	Cases	Min	Average	Median	Max
Records Exposed	287	1	1,621,397	1,091	80,000,000
Total Payout	451	14	299,565	40,500	10,000,000
Breach Costs	457	110	427,554	58,851	16,849,411
Cost Per Record	253	0.03	9,231	43.51	1,603,800

Table 13

Cloud Involvement

In this year's study, we evaluated two new data points related to Cloud: was there Cloud Involvement and, if so, what type of involvement?

Six respondents indicated a Cloud component in a claim. When Cloud was involved, the average and median breach costs in this category were about 20% higher than breach costs overall.

Cloud Events 2014–2017

	Cases	Min	Average	Median	Max
Records Exposed	6	26	194,216	2,598	1,100,000
Total Payout	6	5,268	410,052	34,854	2,240,020
Breach Costs	6	23,964	505,886	50,044	2,740,020
Cost Per Record	5	0.03	92	8	311

Table 14

Ransomware/Cyber Extortion

Ransomware/Cyber Extortion affected every sector. Professional Services, Healthcare, Non-Profit and Financial Services occupied the top four spots. As indicated by a maximum breach cost of \$519K, Ransomware/Cyber Extortion can have a considerable financial impact.

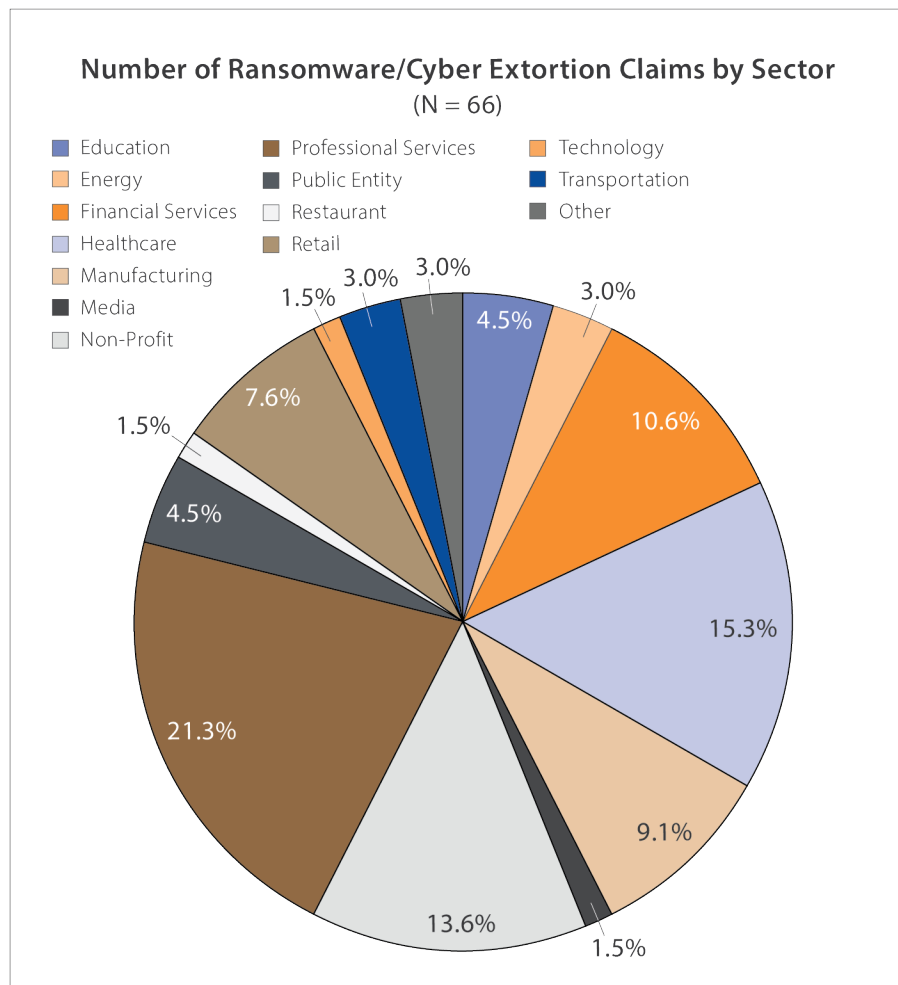


Figure 23

Ransomware/Cyber Extortion 2014–2017

	Cases	Min	Average	Median	Max
Records Exposed	7	22	134,181	178	900,000
Total Payout	47	152	51,111	18,053	448,599
Breach Costs	56	561	61,004	28,777	519,184
Cost Per Record	5	0.18	297	47	779

Table 15

W-2 Fraud

The greatest proportion of W-2 fraudulent claims occurred in Healthcare and Professional Services (22% each), but many other sectors suffered from this kind of cybercrime.

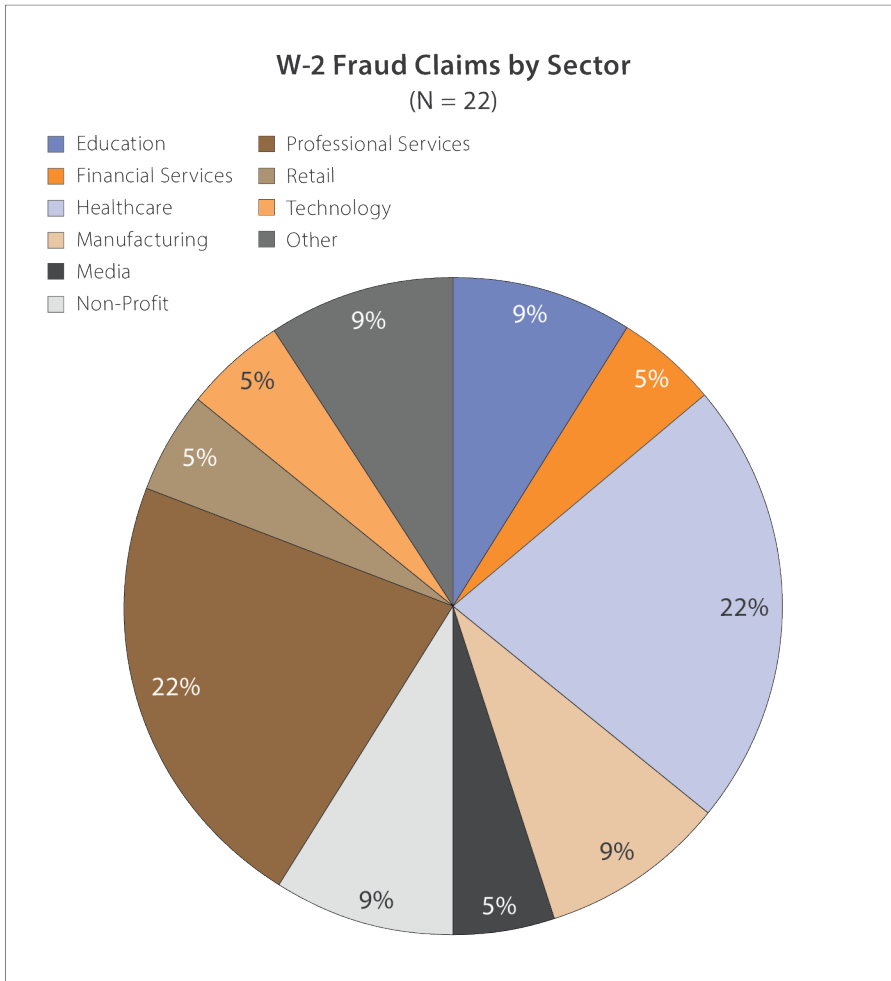


Figure 24

The costs of these incidents ranged from \$3,200 to \$413K with an average cost of \$95K and a median cost of \$50K. The numbers of records stolen ranged from few (26) to many (11K).

“Ransomware attacks such as Petya and WannaCry impacted businesses around the globe and heightened their concerns around robust cyber security, as well as the role insurers can play in holistically managing enterprise cyber risk. In addition to protecting their insureds, cyber insurers need claims data and comprehensive security analytics to understand the risk that they are taking on their balance sheets as they build a cyber insurance book in this important new market.”

Pascal Millaire
VP & GM, Cyber Insurance
Symantec

	Need Title				
	Cases	Min	Average	Median	Max
Records Exposed	22	26	1,439	319	11,000
Total Payout	20	3,241	70,816	37,777	363,000
Breach Costs	20	3,241	95,251	50,277	413,000
Cost Per Record	20	15	260	91	2,101

Table 16

Phishing/Business Email Compromise (BEC)/Wire Transfer Fraud

There are several ways that Phishing can trigger a cyber event. For this reason, we have chosen to aggregate Phishing, Business Email Compromise (BEC)², and Wire Transfer Fraud. Most sectors were impacted, but Financial Services and Professional Services were hardest hit with 26% of claims each. These incidents had total costs ranging from \$3,500 to over \$1.1M, with an average cost of \$181K and a median cost of \$80K.

²BEC or Business Email Compromise is an acronym introduced a few years ago by the FBI. The FBI has been tracking BEC incidents for a couple of years. Additional information is available from the FBI and from InfraGard.

Number of Phishing/Business Email Compromise/ Wire Transfer Fraud Claims by Sector

(N = 46)

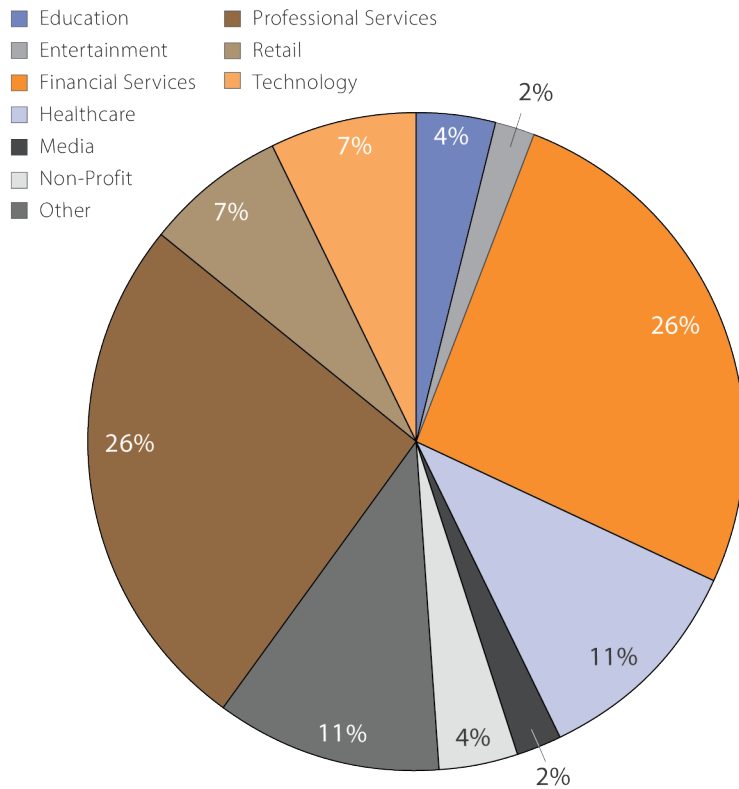


Figure 25

Phishing/Wire Transfer Fraud/BEC Combined 2014–2017

	Cases	Min	Average	Median	Max
Records Exposed	26	1	2,837	796	20,115
Total Payout	43	876	107,443	57,500	841,817
Breach Costs	46	3,550	180,703	79,622	1,118,088
Cost Per Record	25	15	4,737	117	82,500

Table 17

Wire Transfer Fraud

Since Wire Transfer Fraud represents one of the most puzzling and preventable types of cyber exploits, we thought that it would be useful to examine this type of event separately from the combined category of Phishing, BEC, etc. (above). Professional Services (30%) and Financial Services (38%) were the sectors most harmed by this kind of exploit.

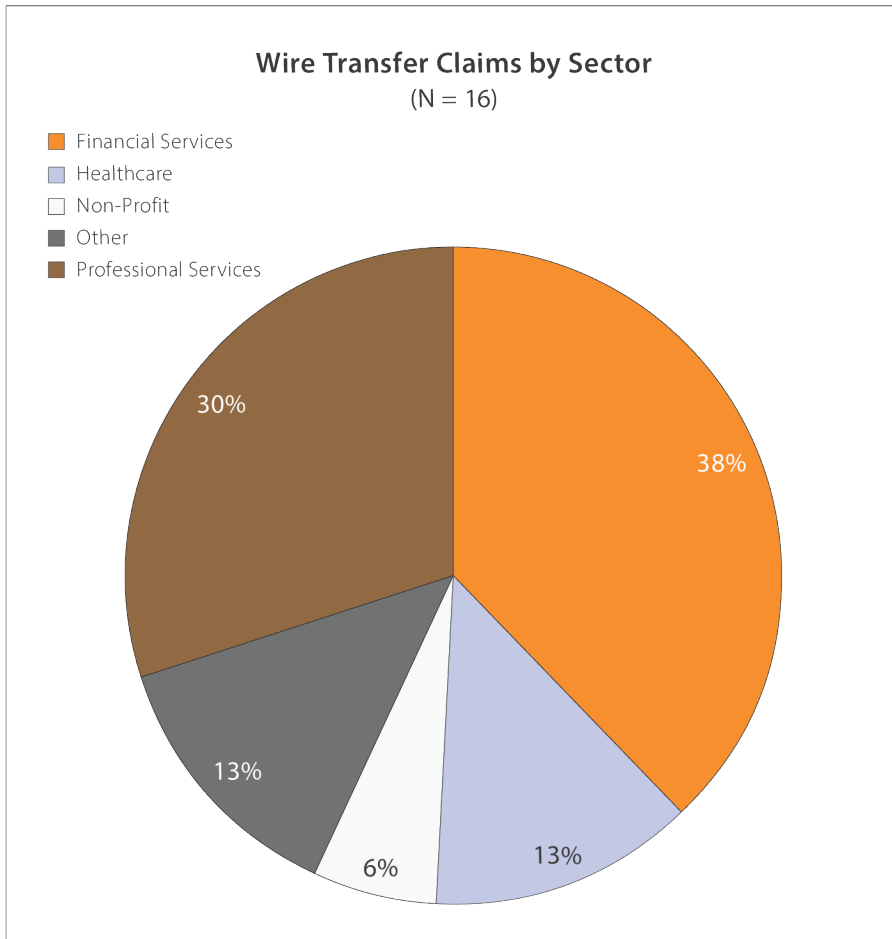


Figure 26

The costs of these incidents ranged from \$3.5K to \$867K. Some, but not all, study participants provided the amount of the fraudulent transfer, and a few indicated whether the amount of money transferred was covered by the victim's cyber policy. Four of these events reported both number of records and associated costs.

Wire Transfer Fraud 2014–2017

	Cases	Min	Average	Median	Max
Records Exposed	4	1	18	21	30
Total Payout	15	1,050	142,822	57,500	841,817
Breach Costs	16	3,550	179,713	77,200	866,817
Cost Per Record	4	347	26,950	12,478	82,500

Table 18

Point of Sale (POS) Related/Common Point of Purchase (CPP) Investigations

Our methodology for assessing POS-related events included looking at the event description for clues that a POS System was involved, as well as identifying all CPP Investigation claims.

Using this approach, we identified 27 claims. Almost all these events involved PCI-related data and occurred in sectors that one would expect: Restaurant, Retail, Hospitality and Entertainment.

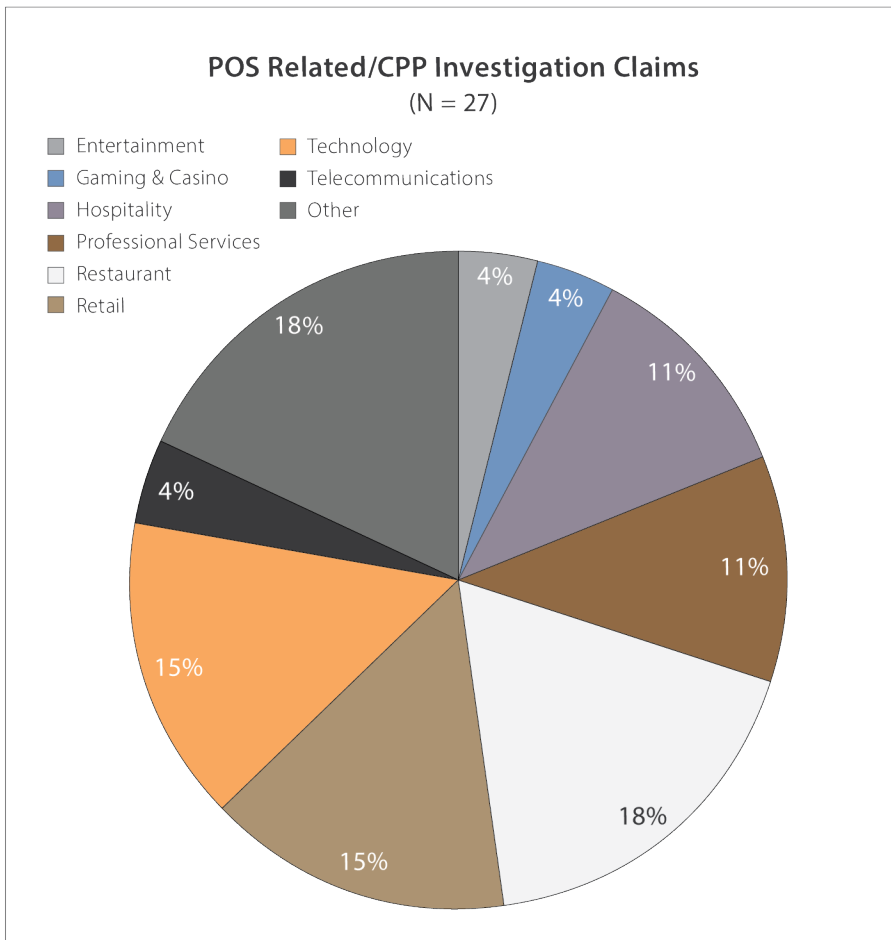


Figure 27

Total costs ranged from \$6,900 to nearly \$17M, with an average cost of \$735K and a median cost of \$53K. The largest cost (\$17M) occurred at a large (\$2B–\$10B) organization and had a powerful skewing affect, which resulted in a factor-of-fourteen variance between median and average values.

POS Related/CPP Investigation 2014–2017					
	Cases	Min	Average	Median	Max
Records Exposed	11	59	113,277	2,327	1,100,000
Total Payout	27	6,950	162,884	40,000	1,849,411
Breach Costs	27	6,950	734,829	53,294	16,849,411
Cost Per Record	11	2.91	264	41.82	1,197

Table 19

Intellectual Property/Trademark Infringement

There were seven Intellectual Property/Trademark Infringement claims in the dataset, six of which were included for the first time in 2017. These kinds of claims can be very costly, with a maximum in our dataset of nearly \$5M. Three of these claims occurred in the Professional Services sector and two occurred in the Retail Sector. Hackers were involved in two cases; the Cause of Loss was unspecified in the other five cases.

Intellectual Property/Trademark Infringement 2014–2017					
	Cases	Min	Average	Median	Max
	7	11,821	864,964	182,484	4,961,000

Table 20

Business Operating Losses

For the first time this year, we had a sufficient number of claims involving Lost Business Income and cyber event Recovery Expense. One significant claim paid nearly \$475K in Recovery Expense.

Business Operating Loss 2017

	Cases	Min	Average	Median	Max
Lost Income	8	7,408	32,938	28,037	105,375
Recovery Expense	9	3,000	120,102	25,158	473,935

Table 21



A Word about First- and Third-Party Claims

Given the interconnectedness of the modern digital world, it is often difficult, from an analytical point of view, to make a clear distinction about First- and Third-Party impacts. Many Distributed Denial of Service (DDoS) events affect only the victim organizations. However, this is not always the case. When information systems become unavailable, customers and business partners can also be impacted.

The same is true of Ransomware/Cyber Extortion. Although Ransomware/Cyber Extortion typically impacts individual machines, sometimes entire systems are shut down, with often severe consequences for third parties. Consider the case of a healthcare system whose files were encrypted, forcing it to operate with pencil and paper. Or a cloud provider that suffered a Ransomware/Cyber Extortion event at the level of its basic platform or infrastructure services. Dozens, and possibly hundreds or thousands, of customers and businesses could be affected.

W-2 fraud is perhaps more clearly identifiable as a first-party event, although we have cases in the dataset where the W-2's exposed were those from a professional services firm that provided accounting services for multiple companies.

Perhaps the clearest example of a first-party event can be found in the cases of wire transfer fraud, where the funds lost were the property of the organization that was defrauded.



Conclusion

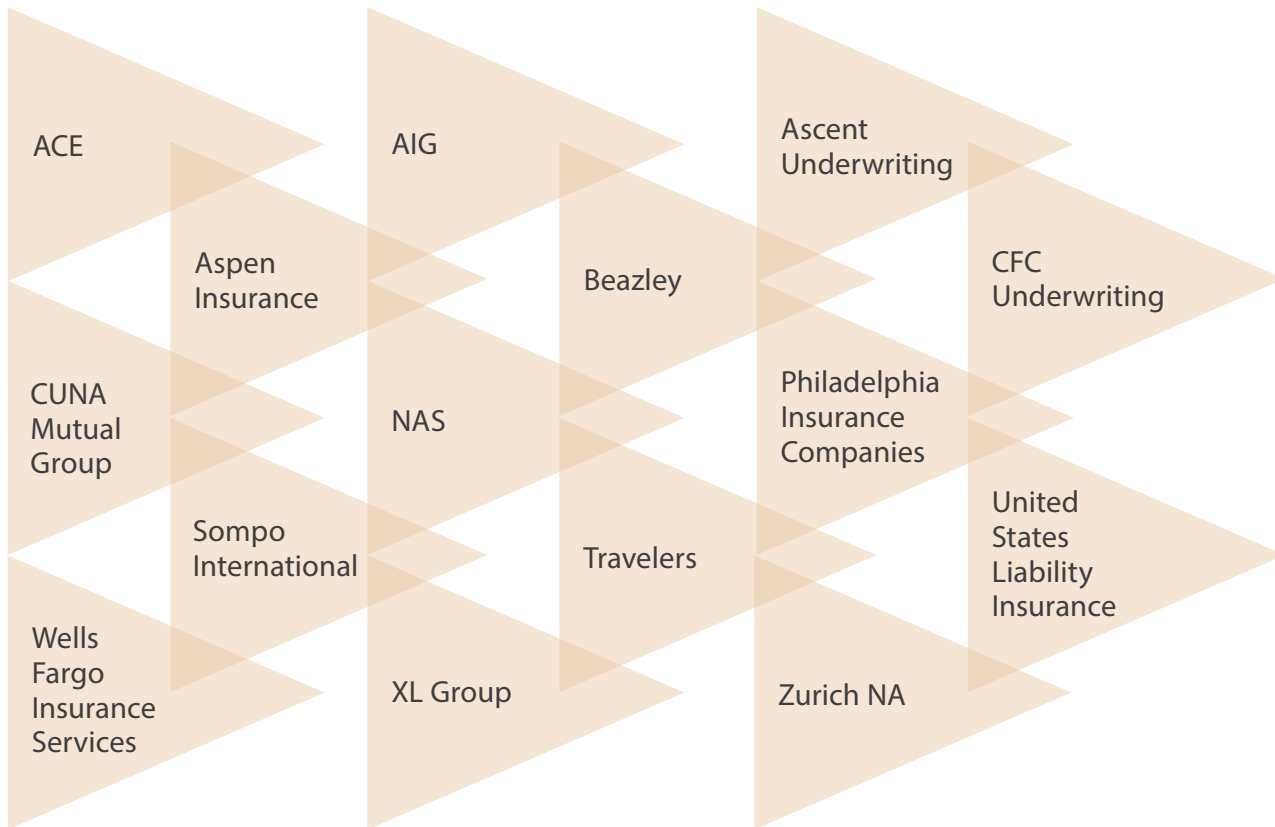
It is our sincerest hope that each year more and more insurers and brokers will participate in this study and share more claims and more information about each claim. It is important that measurable progress be assessed and discussed along the way while providing a good dose of reality.

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:



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 state-of-the-art SaaS tools and training for quantitative 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
- Dane Greisiger—Analytics Intern, NetDiligence
- Sharon Lyon, Publisher—President, Lion's Share Marketing Group, Inc.

Platinum Sponsor—AllClear ID



The 2017 *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 regulations) 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 key 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

Continuous Testing of Your Plan and Team via a War Game

Having a documented customer response plan is the first steps toward success, however, does not tell a company whether or not they are able to execute during a live response when it matters most. 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, expose any gaps, and see their plan unfold as it will during an active data breach. Not taking this critical step is what trips many businesses up during their response, and they end up discovering that their plans were not sufficient or their teams were not prepared in the midst of a breach, when customers, regulators, and the media are calling. 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—RSM US



A whole new world of privacy protection

The growth of digital and internet-based communication and commerce, along with the increase of cyber criminals looking to exploit information, has made the protection of personal information a global requirement. Countries and geopolitical unions around the world are rapidly introducing new and more stringent requirements for businesses and other organizations to follow.

The latest example is the European Union's General Data Protection Regulation (GDPR). GDPR requires all organizations that hold, transmit or process EU resident data to comply with the law—regardless of whether they actually operate in the EU. Many organizations underestimate the amount of EU data they hold and how broadly “private data” is categorized under this law. Compliance presents challenges, however failure to comply can result in significant financial penalties that would be particularly damaging to most organizations.

However, GDPR represents a broader trend, indicating organizations should prepare for privacy compliance on a global level. U.S. organizations will greatly benefit from assessing their customer data and aligning their privacy policies and procedures with this emerging global movement. By doing so, they will not only be able to comply with the requirements of GDPR, but will also be prepared to address additional new privacy laws that may arise from other regions and countries. Instead of looking at privacy compliance as another cost of doing business, organizations should consider it a leading practice that can help them differentiate themselves from competitors.

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.

Sponsor—Cipriani & Werner

CIPRIANI & WERNER ATTORNEYS AT LAW

The 2017 *Cyber Claims Study* demonstrates that all businesses, not simply those in the target breach sectors such as health care, financial services or retail, recognize that data and privacy protection must become part of an industry standard. Data breach and privacy issues are also not an issue only limited to large companies. Instead, small and medium size businesses have become increasingly targeted for breaches as cybercriminals perceive those organizations as less prepared and particularly vulnerable.

Ransomware and phishing attacks have markedly increased across all industries. Companies, as a response, have taken a more proactive role in the pre-breach process. Risk assessments and strategic development of incident response plans have been critical for company preparedness, reducing recovery time and loss. An effective incident response plan designates individuals within the company who are responsible for communications, human relations, coordination with forensic teams, insurance carriers, counsel and outside vendors. All vendor and service contracts should be assessed for determining where there is data access. Table-top exercises with representative simulated-breach scenarios are now a typical practice for organizations. Companies should consider the most effective organizational structure to meet cyber security objectives and define the responsibilities for their CISO/CSO and CCSO and realign the C-suite, if necessary. Boards and C-level executives must be involved in risk assessments and made aware of potential liabilities. Recently, regulators have enacted measures to enforce senior-level accountability and oversight, such as the cybersecurity regulation enacted by the New York State Department of Financial Services. We expect the trend of Board involvement and responsibility to continue to expand into other industries.

About Cipriani & Werner

Cipriani & Werner's Cyber security practice group is uniquely equipped to assist clients in the diverse and quickly-evolving field of cyber-security assessment, data privacy and information security liability. Our team works cooperatively with industry cyber-experts to develop a coordinated, interdisciplinary approach to each matter confronting our clients. Our attorneys also work closely with companies to assist them in adequately securing and protecting sensitive information by developing and implementing security practices, incident analysis protocols and response plans and programs. Our extensive knowledge of privacy laws and government regulations enables us to position our clients to effectively protect their corporate assets, by providing them with risk management advice that reduces the risk of costly breaches and data loss. From advising our clients on matters of compliance to leading them through the aftermath of a cyber-crisis, Cipriani & Werner attorneys are prepared to work with company management, Boards of Directors, outside vendors and government agencies to ensure that the interests of our clients are protected. For more information, visit www.c-wlaw.com.

Sponsor—Symantec



Symantec is a proud sponsor of the NetDiligence *Cyber Claims Study*. The 2017 report provides a wealth of insights on the state of cyber insurance claim severity and is a natural complement to the event frequency data we see in our product telemetry and intelligence network.

Symantec Cyber Insurance empowers cyber underwriters, portfolio managers and actuaries with underwriting and cyber risk analytics purpose built for the cyber insurers. Symantec Cyber Insurance platform consists of two analytics products:

Symantec CyberWriter

Streamline your cyber underwriting with comprehensive security insights and benchmarks.

Accelerate Underwriting Decisions:

- Review prepopulated business information including outside-in client-specific security data; prepopulated firmographics and historical breach data
- Focus on the most relevant questions during the underwriting process

Grow a Profitable Book of Business:

- Build a balanced portfolio by tying underwriting insights to claims
- Lower your operational costs with greater automation in risk selection

Improve Cyber Risk Selection:

- Establish a consistent enterprise-wide application scoring and rules
- Get a clearer picture of risk with analytics on 6 million companies and 130 million domains

Symantec CyberCube

Manage cyber aggregation risk within your portfolio by modeling systemic cyber events.

Manage the tail risk of insurance portfolios:

- Measure the probability and loss potential of systemic cyber attacks
- Determine the level of reinsurance to optimize the risk-adjusted return

Enhance your underwriting strategy:

- Simplify the data collection requirements needed for modeling
- Identify the segments and risk characteristics that result in long-term profitability

Develop your own view of cyber risk:

- Configure frequency and severity controls to create your own view of risk
- Leverage a multi-dimensional narrative of systemic attacks to customize your risk outlook

About Symantec

Symantec Corporation (NASDAQ:SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks.

About Symantec Cyber Insurance

Symantec Cyber Insurance empowers cyber underwriters, portfolio managers and actuaries with underwriting and cyber risk analytics purpose built for the cyber insurers, incorporating data from the insurance and cyber security communities. Symantec gathers and analyzes petabytes of cyber security data on global threat actors, cyber attacks, security incidents and data breaches to provide a deep understanding of the cyber threat landscape.

About

NetDiligence®

NetDiligence® (<https://netdiligence.com>) specializes in Cyber Risk Readiness & Response.

Since 2001, NetDiligence has conducted thousands of enterprise-level **QuietAudit® Cyber Risk Assessments** for a broad variety of corporate and public entity clients. Our time-tested risk management approach (eliminate, mitigate, accept and cede residual risk) enables us to effectively help organizations of all types and sizes manage their cyber risk. The QuietAudit platform that our engineers use to conduct their in-depth cyber risk assessments can also be licensed for **Vendor Risk Management and/or Underwriting Loss Control**.

NetDiligence is also an acknowledged leader in data and privacy breach prevention and recovery. Our **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®** is an affordable, easy-to-use service that assists organizations with data breach response planning.

QuietAudit®

With cyber risks growing daily, many organizations don't know where they're most vulnerable; who has access to their data; whether their network security measures meet legal standards for prudent and reasonable safeguards. NetDiligence can help answer these critical questions. Our QuietAudit Cyber Risk Assessments document the organization's Risk Profile, so they know where their exposures are and can take the appropriate actions to mitigate them.

Consultant-Led Assessments

NetDiligence's QuietAudit Cyber Risk Assessments—conducted by data security engineers—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 stores the assessment results online, so it's easy for organizations to re-evaluate their risk posture regularly and monitor changes over time.

NetDiligence offers a variety of consultant-led QuietAudit Cyber Risk Assessments that are tailored to meet the unique needs of small, medium and large organizations in a variety of business sectors, 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**

In addition to conducting a thorough and comprehensive Cyber Health Check assessment, NetDiligence performs a network vulnerability scanning service to test the effectiveness of firewalls and web servers and identify 6000+ vulnerabilities that hackers can exploit, including unpatched, non-hardened or misconfigured externally-facing network servers and devices.

Vendor Risk Management (VRM)—Software as a Service (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 Vendor Risk Management (VRM) enables a company to require their vendors complete a self-assessment of data security/privacy practices. Reporting includes an online dashboard and a "scorecard" for each vendor.

Underwriting Loss Control (ULC)—Software as a Service (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.



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.



With our Breach Plan Connect® service, NetDiligence builds and hosts an organization’s customized Incident Response Plan (IRP), enabling employees to access their IRP 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

This study is unique because it focuses on covered events and actual claims payouts and total breach costs. We asked the major underwriters of cyber liability to submit claims information based on the following criteria:

- The incident occurred between 2014 and 2016
- The victimized organization had some form of cyber or privacy liability coverage

We sent requests for data to 93 individuals at 75 organizations in the United States and Canada. Of the cases in the analysis data subset, 582 cases represent claims from American organizations, and two cases represent claims from Canada. There are also four cases from the United Kingdom and two cases from Australia. These data were provided by 17 individuals representing 16 organizations. This number of contributors is somewhat lower than last year, when 20 organizations provided data. However, the number of cases from the 2017 data collection effort was doubled: 354 compared to 176.

Our 2017 report includes data from studies published in 2014-2016, as well as 354 cases collected in 2017. It summarizes findings from a sampling of 2,411 submissions: each one, a data breach insurance claim. After removing many cases that did not meet our analysis criteria (missing two or more stratifiers) and/or were settled within SIR, we analyzed claims information for 591 events. This number represents a large increase in the number of cases compared to last year.

343 claims (58%) specified the number of records exposed and 506 claims (86%) included a detailed breakout of what had been paid out so far. When factoring in SIRs, we have been able to calculate total data breach costs to date for 514 (87%) of the cases in the dataset. Many of the events submitted for this year's study were recent, which means many claims are still open and actual costs have not yet been finalized.

Readers should keep in mind the following:

- Our sampling, although much larger than ever before, is a small subset of all breaches. Some of our data points are lower than other studies because we focus on claim payouts and breach costs for specific breach-related expenses and do not factor in other financial impacts of a breach, including investigation and administration expenses, customer defections, opportunity loss, etc.

- We are not privy to the terms of the cyber 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 cost at least \$X, but we cannot say how much more than this amount.
- Having said that, for the first time 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. A few participants provided these data, thereby increasing our ability to understand the true cost of a breach.
- A certain number of the claims in the dataset were settled within SIR. Because we were not usually told much of the SIR was exhausted, we included these cases in some of the counts, but have excluded them from the payout, breach cost, and cost per record analyses.
- Our 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”.

It is important to note that many of the claims submitted for this study remain ‘open’, therefore aggregate costs as presented in this study represent “payouts to-date” and “breach costs to-date”. It is virtually certain that additional payouts will be made on a significant portion of the claims in our dataset and therefore the costs in this study are almost certainly understated.