NetDiligence®

2016 CYBER CLAIMS STUDY

SPONSORED BY:

AllClear ID

RSM

CIPRIANI & WERNER

Symantec

TABLE OF CONTENTS

Introduction . . . 1

Key Findings . . . 2

A Look at the Overall Dataset . . . 4

- Records Exposed . . . 4
- Cost per Record . . . 5
- Costs Overall . . . 6
- Crisis Services Costs . . . 8
- Legal Damages . . . 10
- Regulatory Action . . . 10
- PCI Fines . . . 10

Viewing the Data through Different Lenses . . . 11

- Type of Data Exposed . . . 11
  - Records Exposed . . . 13
  - Costs . . . 14
- Cause of Loss . . . 15
  - Records Exposed . . . 17
  - Costs . . . 18

Business Sector . . . 19
Records Exposed . . . 21
Costs . . . 23
Size of Affected Organization (based on revenue) . . . 24
Records Exposed . . . 26
Costs . . . 28
Insider Involvement . . . 29
Third-Party Breaches . . . 32
Cloud involvement . . . 34
Cyber Extortion/Ransomware . . . 34
Phishing . . . 35
Phishing and Wire Transfer Fraud . . . 35
POS-Related/Common Point of Purchase (CPP) investigations . . . 35
About First-Party Losses . . . 36
Conclusion . . . 38
Insurance Industry Participants . . . 39
Contributor—Risk Centric Security, Inc. . . . 39

Platinum Sponsor—AllClear ID 40

Sponsor—RSM US LLP 42

Sponsor: Cipriani & Werner 44

Sponsor: Symantec 46

About NetDiligence® 48

Study Methodology 51

P02

INTRODUCTION

NetDiligence® is proud to present our sixth annual Cyber Claims Study. Our study provides the most comprehensive analysis to date of claims data reported from Insurers on losses sustained from data breaches and other kinds of cyber events.

Our reports, unique in the marketplace, are valued by Insurers, Underwriters, Risk Managers, CEO's, CFO's, and CISO's. The report includes informative numerical and graphical descriptions of the types of data exposed, causes of loss, business sectors involved, sizes of affected organizations, insider involvement, and third party involvement. We have also included several new analyses:

- Cloud involvement
- Cyber Extortion/Ransomware
- Phishing
- Phishing and Wire Transfer fraud
- POS-Related / Common Point of Purchase/CPP investigations

Additionally, you will see costs associated with Crisis Services, (forensics, notification, credit/ID monitoring, legal counsel and miscellaneous other), Legal Damages (defense and settlement), Regulatory Action (defense and settlement) and PCI Fines.

"As breach activity continues to evolve, so does the industry's understanding of its associated damages, ranging from data and system loss to business interruption and reputational harm. This study is a great resource to validate the latest threats and help organizations evaluate their security vulnerabilities and measures."

ANDY OBUCHOWSKI, DIRECTOR

RSM US LLP

KEY FINDINGS

Breaches are not just for the Fortune 500 companies anymore.

The majority (87%) of claims submitted for this study are for organizations with revenues less than $2B.

The numbers of records lost can be large, no matter how large or small an organization may be.

Our dataset contains breaches of 1M or more records occurring in organizations of all sizes, except Mega Revenue (>$100B).

Breaches can be very costly, no matter how large or small an organization may be.

In our dataset, breaches with total costs greater than $5M occurred in organizations of all sizes except Mid Rev ($2–10B).

Breaches with few records can be very costly. One event in our dataset involved 1 record (PHI) with a cost of between $1.5–2.0M.

The average number of records lost was 2.04 million. The median number of records lost was 1,339.

The greatest numbers of exposed records occurred in the Financial Services (78M records) sector, followed by Retail (56M records).

The average claim payout was $495K. The median claim payout was $49K.

The highest average payout was in the Financial Services sector ($1.3M), while the average payout in the Healthcare sector was $726K, down from $1.3M last year.

The average breach cost was $665K. The median total breach cost was $60K.

The breach costs in this year's study ranged from $290 to $15 million. Typical breach costs, however, ranged from $5,822 to $1.6M (80%, from the 10th–90th percentile).

The most expensive breaches occurred in Financial Services (~$15M) and Retail ($10M).

The average breach cost for a large company was $5.97M million. The highest average breach cost was in the Financial Services sector ($1.8M). The Retail sector experienced the second highest average breach cost ($1.7M)

The average payout for a large company was $3.04 million, while the average payout in the Financial Services Sector was $1.3M and in the Healthcare sector was $726K.

The average per-record cost was $17K. The median per-record cost was $39.82. This extraordinarily high per record average has been driven by three large outliers: fewer than 10 records each, with per record costs between $35K and $1.6M.

PII was the most frequently exposed data (40% of claims), followed by PCI (27%) and PHI (15%).

Hackers were the most frequent cause of loss (23%), followed by Malware/Virus (21%). Following at third and fourth were Staff mistakes (9%) and Rogue employees (7%).

Healthcare was the sector most frequently breached (19%), followed by Professional Services (13%).[1]

The average cost for Crisis Services (forensics, notification, credit monitoring, legal guidance/Breach Coach® and miscellaneous other response costs) was $357K. The median cost for Crisis Services was $43K.

The average cost for legal defense was $130K. The median cost for legal defense was $16K.

The average cost for legal settlement was $815K. The median cost for legal settlement was $250K.

The dataset contains only two cases with regulatory legal data, one less than $30K and one greater than $5M. These data are for defense only—no regulatory settlement/fine data were provided.

The dataset contains 8 cases that report PCI fines. The average PCI fine was $462K. The median PCI fine in these cases was $58K.

The dataset included one claim for the loss of trade secrets. The payout for this claim was almost $5M, more than fifty times the median cost of a PCI-related claim.

Third parties accounted for 13% of the claims submitted.

There was insider involvement in 30% of the claims submitted.

Note: We've added a new research database with anonymized data from all our claims studies to the eRiskHub® for the exclusive use of eRiskHub licensors and their clients. For more information about the eRiskHub, contact Mark Greisiger at mark.greisiger@netdiligence.com.

[1]18% of breaches were not classified into our 13 sector categories

A LOOK AT THE OVERALL DATASET

There were 176 cyber claims submitted for this year's study. Of that number, 163 claims involved the loss, exposure or misuse of some type of sensitive personal data. The remaining 13 incidents involved business interruption, lost hardware, and DDoS attacks.

RECORDS EXPOSED

68% of the claims reported the number of records exposed. The number of records exposed in a data breach claim ranged from 1 to 78M. The average number of records exposed was 2.04M.

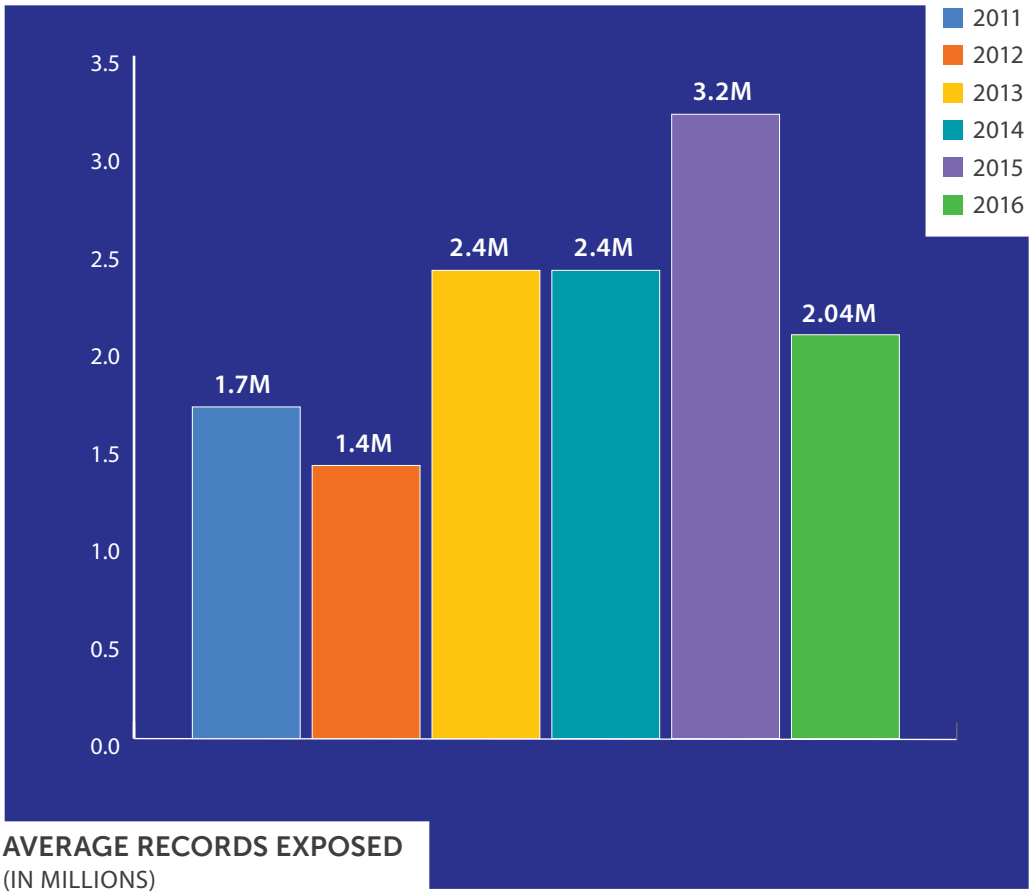


FIGURE 1

The median number of records exposed was much smaller, coming in at 1,339. This continues a trend we have seen in previous studies. The median number of records exposed was 45,000 in our inaugural 2011 study, 29,000 in 2012, 1,000 in 2013, 3,500 in 2014, and 2,300 in 2015. It is clear that more claims are being submitted for breaches with a relatively small number of records exposed.

COST PER RECORD

Data breaches involve many types of data and many types of costs. The costs can range from a few hundred dollars to hundreds of millions of dollars.[2] As was mentioned in the Key Findings above, **high per-record costs are possible regardless of breach size (1 record / $1.5–2M).**

66% of the claims in the dataset reported both the number of records lost and the total breach cost. The minimum cost per record was $0.03 and the maximum cost per record was $1.6M. The **average cost per record was $17K,** while the median cost was $39.82.

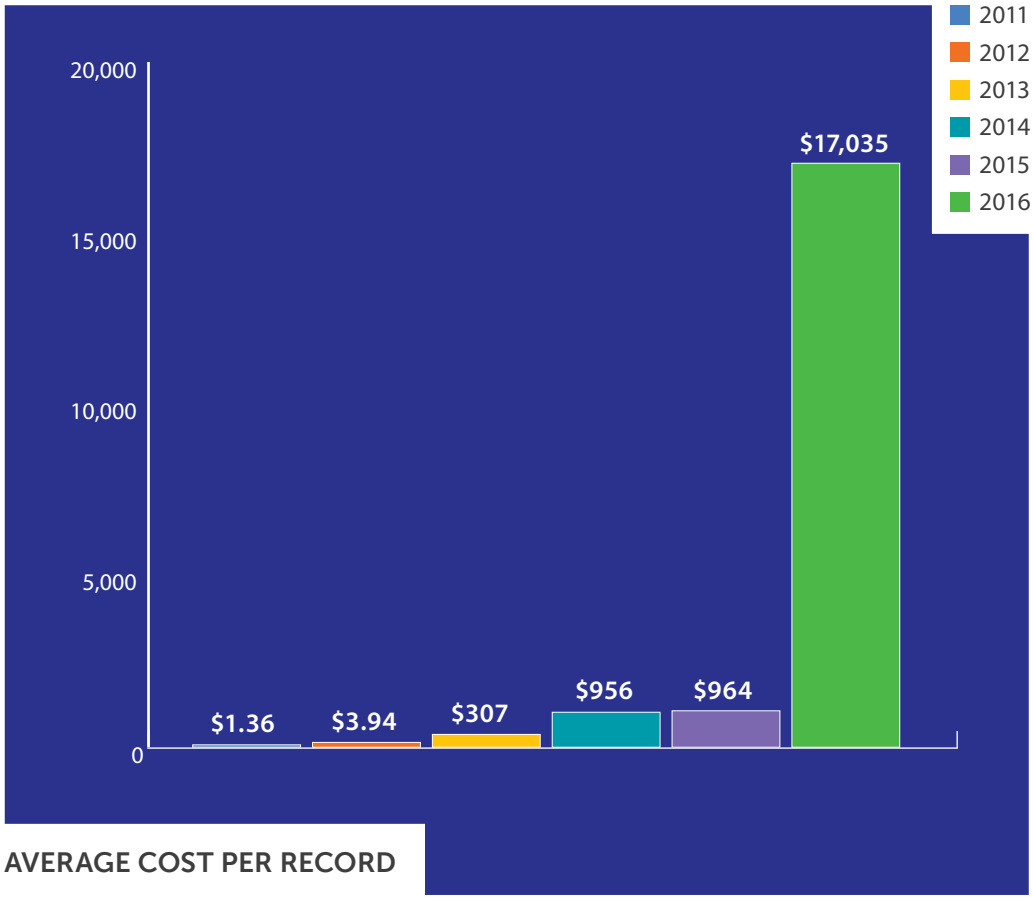


FIGURE 2

The extraordinarily high per record average this year has been driven by three large outliers: fewer than 10 records each, with per record costs between $35K and $1.6M.

[2]At the time of this writing, the breach at Target has incurred costs in excess of $250M.

COSTS OVERALL

Of the claims submitted, 98% reported total breach costs. The smallest breach cost was $290 while the largest was $15 million (note that some claims are still open). The **average breach cost was $665K, down slightly compared to last year's study.** The median breach cost was $60K.

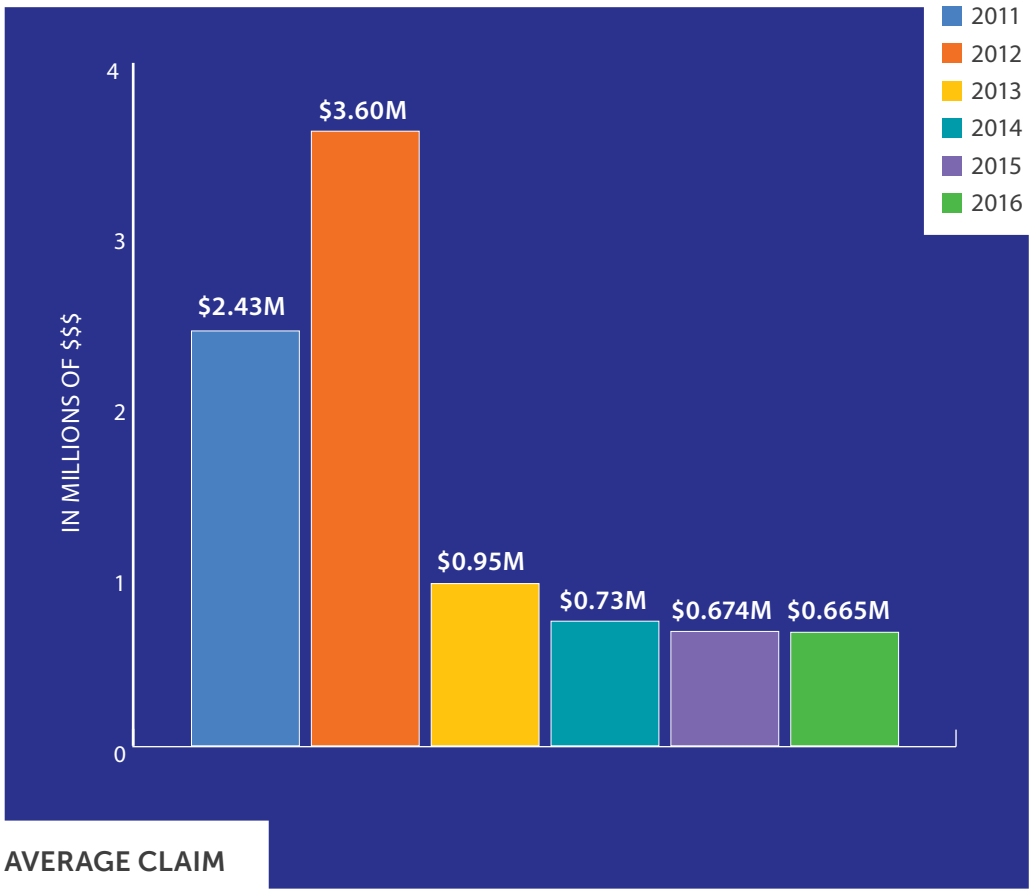


FIGURE 3

"The increase in the number of claims in the Nano-Rev and Micro-Rev offers strong indication that businesses of these sizes are becoming more attractive targets. It may also suggest that the number of law suits may increase and the need for both legal defense as well as cyber services will drive more companies of this size to obtain appropriate levels of cyber insurance."

CIPRIANI & WERNER

Of the $114M million in total claims, only $76M of the claims reported individual categories of expenses. Using $76M as a base, 75% was spent on Crisis Services, 3% on Legal Defense, 10% on Legal Settlements, 8% on Regulatory Defense, and 5% for PCI Fines.

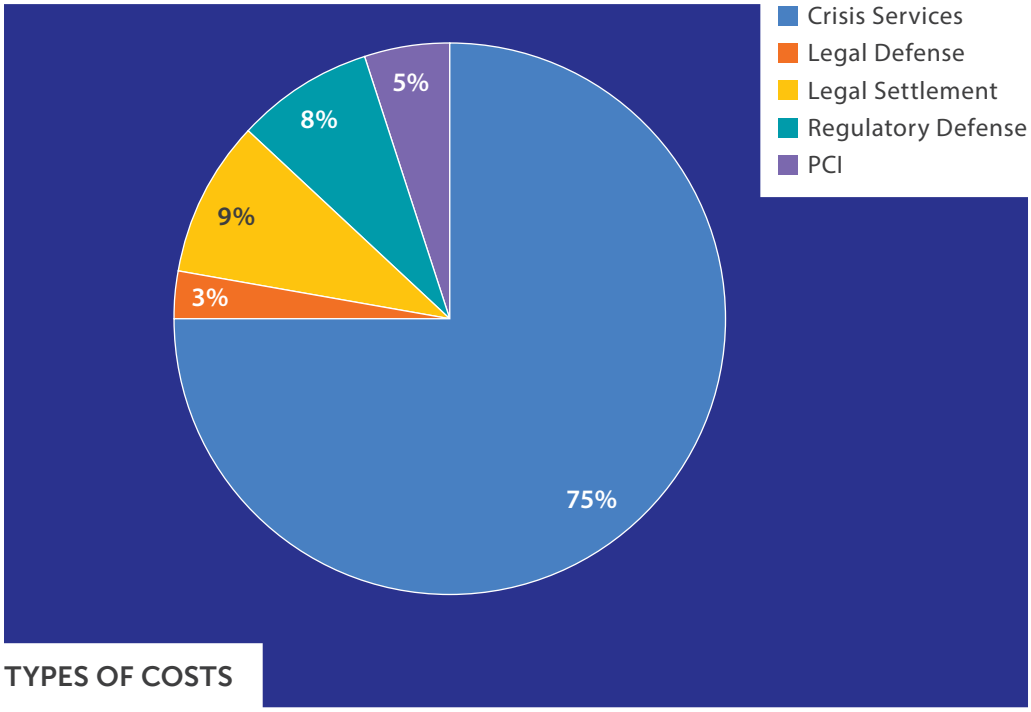


FIGURE 4

CRISIS SERVICES COSTS

91% of claims included costs for one or more components of Crisis Services. The smallest claim for Crisis Services was $290, while the largest claim was $7.1M. The **average for Crisis Services was $357K.** The median was $43K.

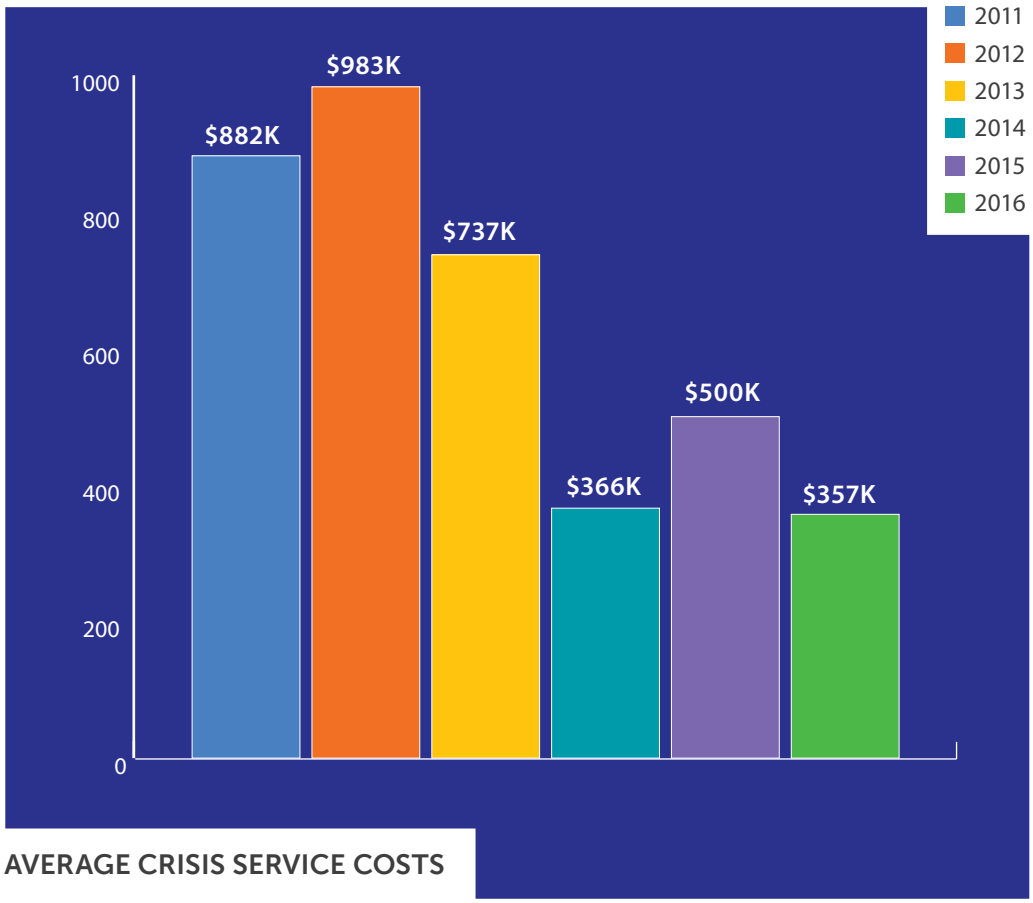


FIGURE 5

Not all claims included all of the services that comprise Crisis Services. Of the claims that reported the Total Crisis Services costs, 66% included forensics, 36% included notification, 33% included credit/ID monitoring and 68% included legal guidance/Breach Coach®. These numbers reflect all claims that reported a dollar figure for a particular service. This year, 21% included other costs, including public relations and post-breach cleanup.

"Over the last year, we've worked with Fortune 500 companies and government organizations before a data breach occurs to help them be ready to respond with the expert resources and reserved manpower should they ever need it. Through continued efforts like this, we hope to drastically reduce not only the hard costs associated with data breaches, like the ones in this study, but also soft costs like reputational harm and customer churn that often result from botched responses."

ALLCLEAR ID

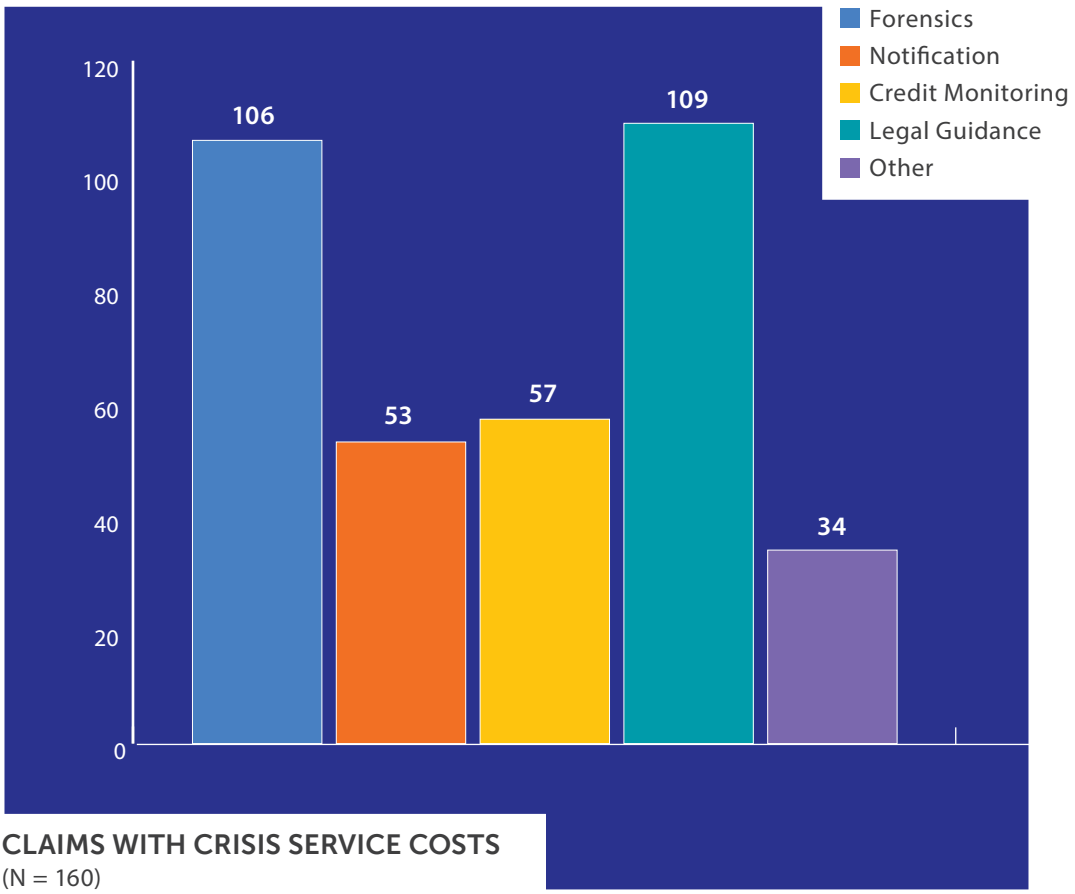


FIGURE 6

There was a wide range of costs for these services (see table 1 below). Forensics costs ranged from $1,234 to $2.46 million. Notification costs ranged from $58 to $2 million. Credit/ID monitoring costs ranged from $298 to $2.9M million. Legal guidance/Breach Coach® costs ranged from $290 to $2.5 million. Public Relations costs ranged from $15 to $1.07M.

CRISIS SERVICE COSTS

Service	Claims with Costs	Total	Min	Median	Mean	Max
Forensics	106	18,983,603	1,234	35,450	179,091	2,456,000
Notification	53	8,942,659	58	5,000	168,729	2,000,000
Credit/ID Monitoring	57	15,990,149	298	12,198	280,529	2,900,000
Legal Guidance/Breach Coach®	109	11,012,155	290	28,394	101,029	2,500,000
Public Relations/Other	34	1,843,399	15	6,839	54,218	1,065,000

TABLE 1

LEGAL DAMAGES

10% of claims included costs for legal defense and damages. The range of legal costs was extremely broad. Legal defense payouts ranged from $594 to $750K. Payouts for legal settlements ranged from $19K to $4.8M.

LEGAL DEFENSE AND SETTLEMENTS						
	Claims with Costs	Total	Min	Median	Mean	Max
Legal Defense	17	2,201,760	594	16,000	129,515	750,000
Legal Settlement	9	7,332,301	18,755	250,000	814,700	4,800,000

TABLE 2

REGULATORY ACTION

Only 1% of claims submitted this year included costs for regulatory actions. These claims reported data for legal defense only. The two data points for Regulatory Defense were $25K and $5.79M. Claims that included regulatory costs in this year's study ranged from 788 records exposed to 700K records exposed.

REGULATORY DEFENSE AND SETTLEMENTS						
	Claims with Costs	Total	Min	Median	Mean	Max
Regulatory Action Defense	2	5,816,163	25,163	2,908,082	2,908,082	5,791,000
Regulatory Action Fines	0					

TABLE 3

PCI FINES

5% of claims included costs for PCI fines. Payouts for PCI fines ranged from $3,000 to $3M.

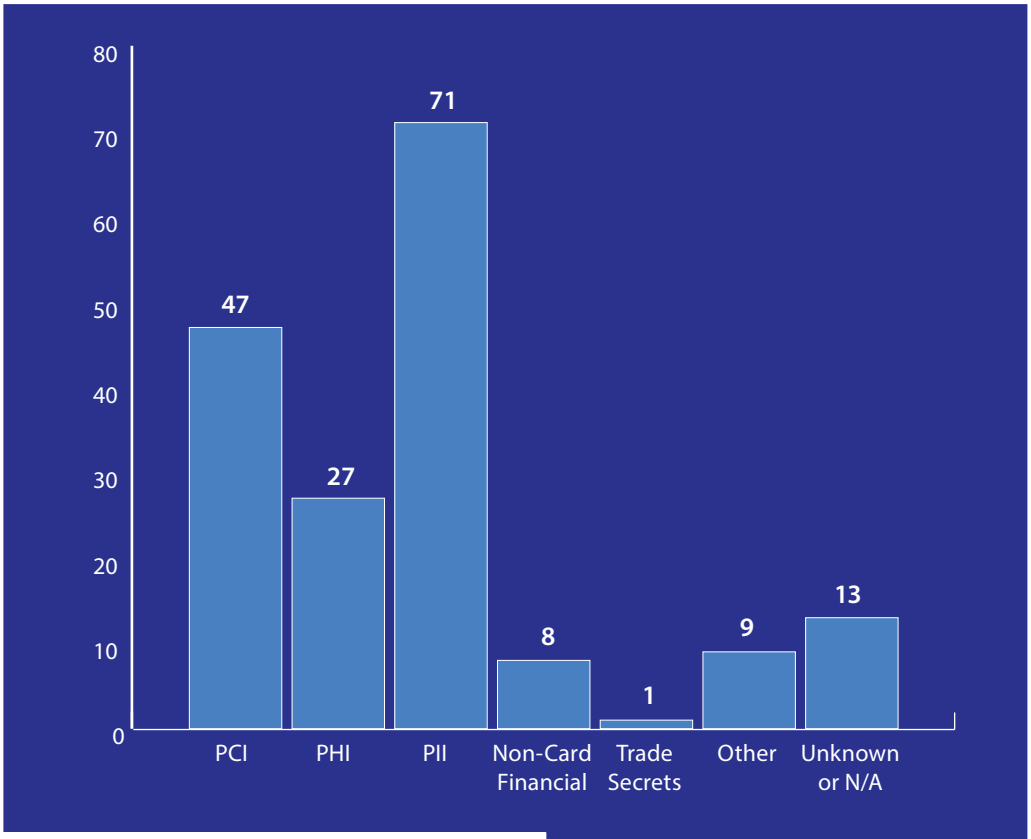
PCI Fines						
	Claims with Costs	Total	Min	Median	Mean	Max
PCI	8	3,963,285	3,000	58,006	461,661	3,000,000

TABLE 4

VIEWING THE DATA THROUGH DIFFERENT LENSES

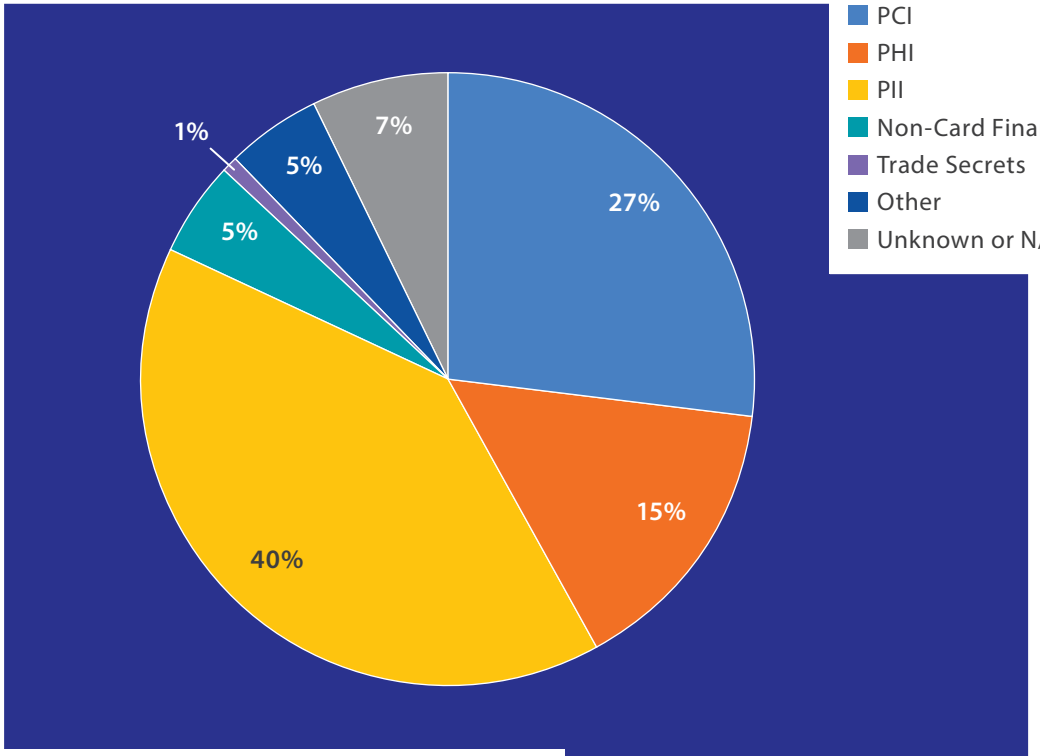
TYPE OF DATA EXPOSED

Data breaches exposing PII represented 40% of the claims in the dataset; PCI, 27%; and PHI, 15%. Non-card financial information was exposed in 5% of the claims. One case reported theft of trade secrets. In 13 cases, the type of data was either not specified or not applicable.



NUMBER OF CLAIMS BY TYPE OF DATA
(N = 176)

FIGURE 7

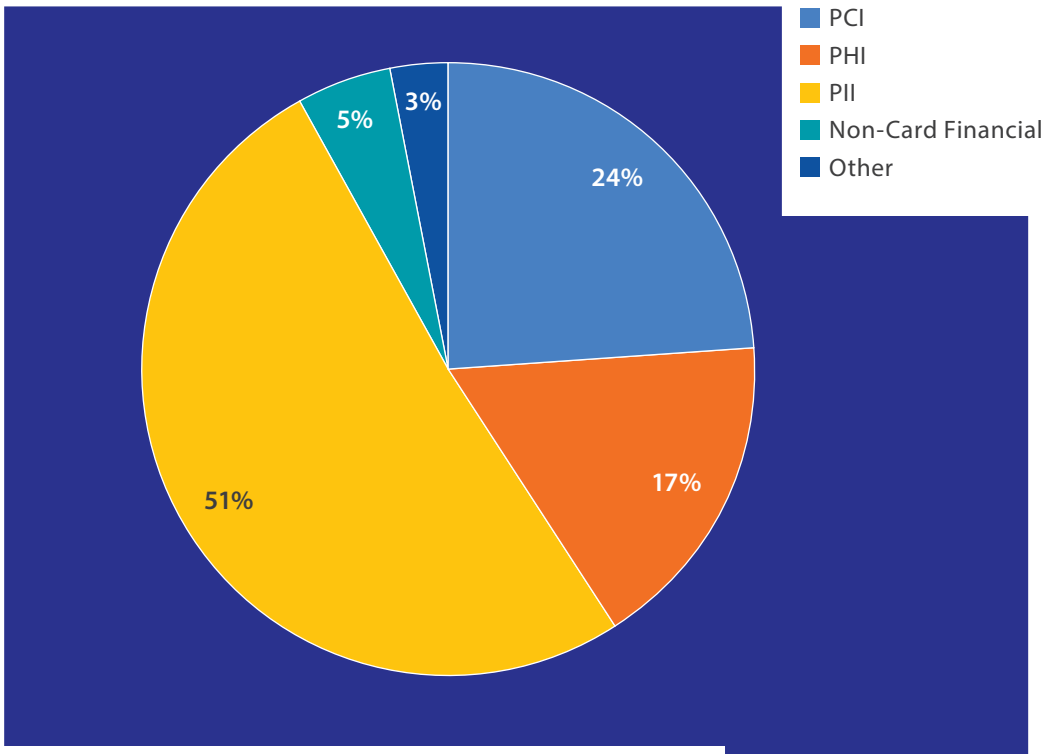


PERCENTAGE OF CLAIMS BY DATA TYPE
(N = 176)

FIGURE 8

Records Exposed

68% of claims reported the number of records exposed. Of those 120 claims, PII was the most frequently exposed type of data (N=61 / 51%).



PERCENTAGE OF RECORDS EXPOSED BY DATA TYPE
(N = 120)

FIGURE 9

RECORDS EXPOSED

	Cases with Records	Min	Median	Mean	Max
Non-Card Financial	6	8	200	116,865	700,000
Other	4	2	52,589	301,295	1,100,000
PCI	29	71	16,000	4,809,705	56,000,000
PHI	20	1	2,637	5,073,428	78,000,000
PII	61	1	216	36,517	1,274,700
Total	**120**				

TABLE 5

Costs

98% of claims included both the data type and the total cost amount, including SIR. As we have seen in prior studies, there was a wide range of claim costs for every data type, from a minimum of $290 up to $15 million. This year, the median claim for PCI-related breaches was higher than other data types—with one notable exception. This year's dataset included one claim for the loss of trade secrets. The payout for this claim was almost $5M, more than fifty times the median cost of a PCI-related claim.

TOTAL COSTS (including SIR)

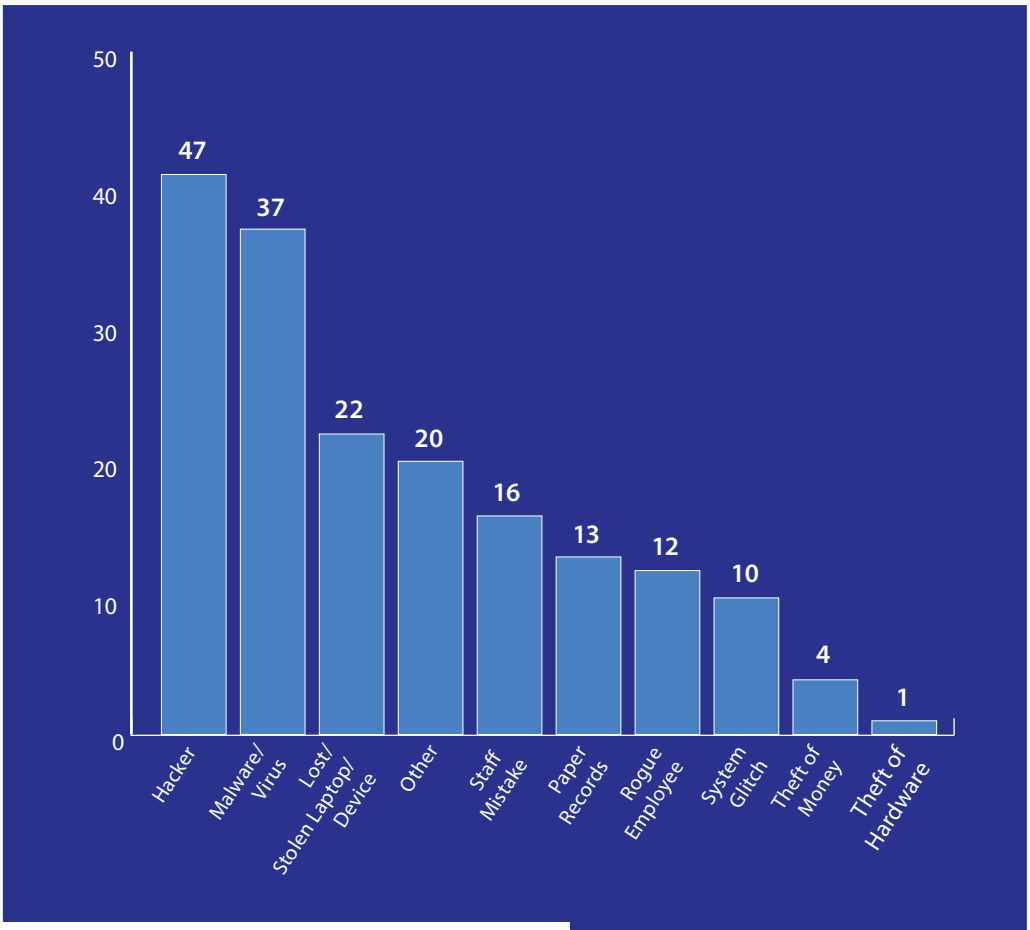
	Cases	Min	Median	Mean	Max
N/A	9	14,949	52,545	183,687	1,049,643
Non-Card Financial	8	11,280	58,633	1,545,744	11,491,000
Other	9	1,190	73,480	405,991	1,606,550
PCI	47	594	93,199	894,650	10,000,000
PHI	27	290	58,851	1,515,149	15,000,000
PII	67	661	50,186	125,263	917,827
Trade Secrets	1	4,961,000	4,961,000	4,961,000	4,961,000
Unknown	4	26,181	67,990	89,773	196,931
Total	**172**				

TABLE 6

The payout for loss of trade secrets was more than fifty times the median cost of a PCI-related claim.

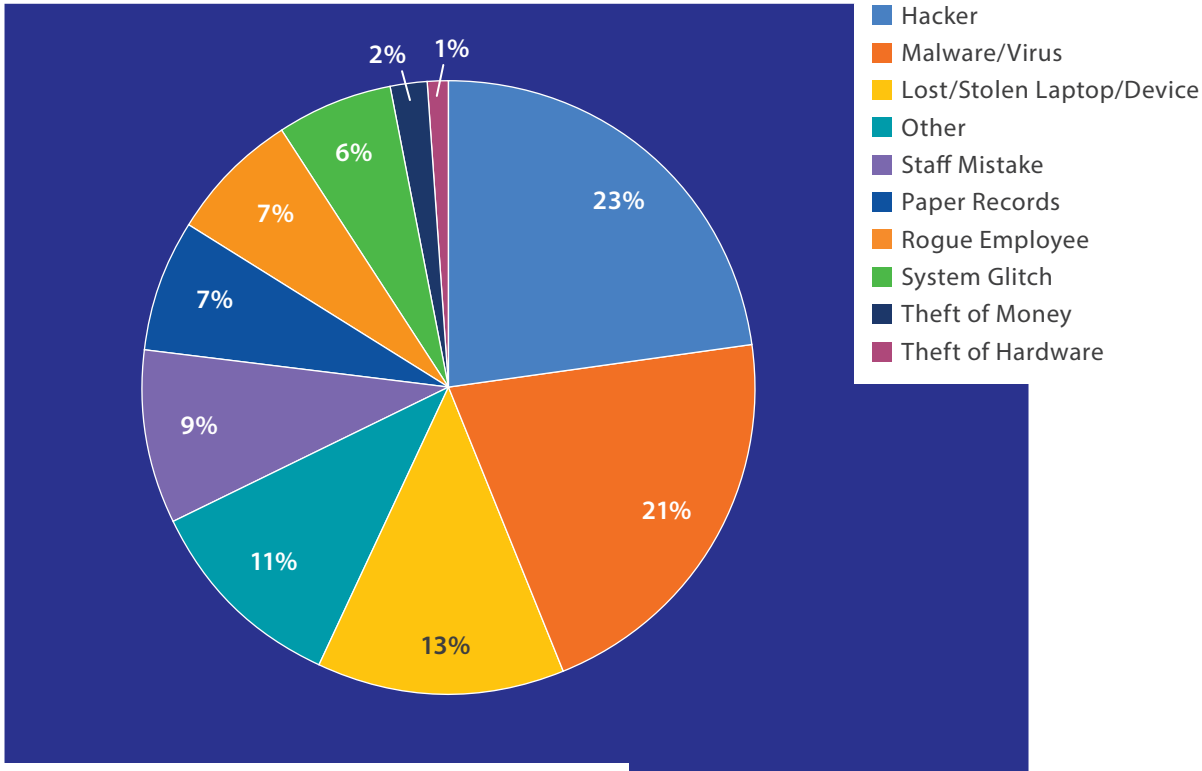
CAUSE OF LOSS

Hackers were the most frequent cause of loss, accounting for 41 claims (23% of the dataset). Malware/Virus were second, responsible for 37 claims (21%), followed by Lost/stolen laptop/ device with 22 claims (13%), Other with 20 claims (11%), Staff Mistakes with 16 claims (9%), Paper Records with 13 claims (7%), and Rogue Employees with 12 claims (7%). Note that insiders (Staff mistakes, Rogue employees, and System glitches) accounted for a combined 38 claims, or 22% of this year's dataset.



NUMBER OF CLAIMS BY CAUSE OF LOSS
(N = 176)

FIGURE 11

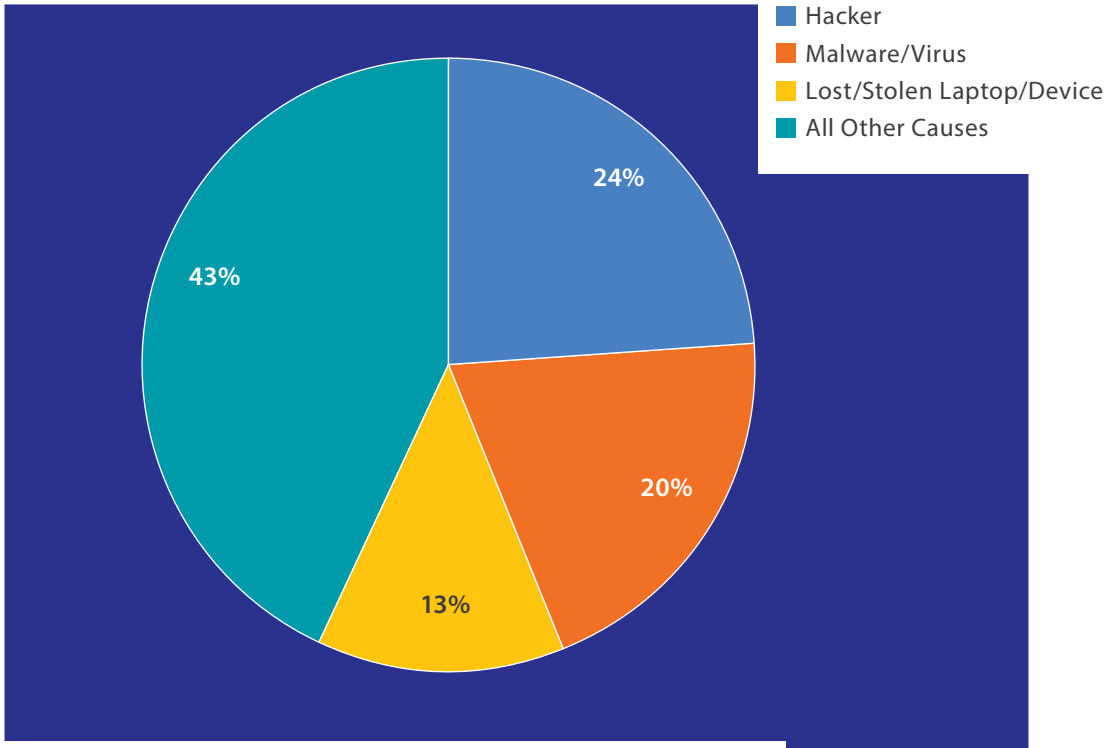


PERCENTAGE OF CLAIMS BY CAUSE OF LOSS
(N = 176)

FIGURE 12

Records Exposed

68% of the claims reported the number of records and cause of loss. Hackers, Malware/Virus, and Lost/stolen laptop/device accounted for 58% of exposed data.



PERCENTAGE OF RECORDS EXPOSED BY CAUSE OF LOSS
(N = 120)

FIGURE 13

RECORDS					
	Cases	**Min**	**Median**	**Mean**	**Max**
Hacker	29	1	16,500	6,332,064	78,000,000
Lost/Stolen Laptop/Device	16	1	688	33,292	300,000
Malware/Virus	24	2	11,547	2,446,812	56,000,000
Other	5	25	64	59	72
Paper Records	12	1	86	218	983
Rogue Employee	9	270	3,050	79,918	700,000
Staff Mistake	14	1	49	78,833	1,100,000
System Glitch	10	9	686	36,908	248,900
Theft of Money	1	3,000	3,000	3,000	3,000
Total	**120**				

TABLE 7

Costs

98% of the claims in the dataset included both the cause of loss and the total claim cost. Incidents caused by malicious activity (Hackers, Malware/Virus and Rogue Employees) resulted in higher average costs than incidents caused by simple errors, such as staff mistakes or actions by a third-party provider. This is probably attributable to the fact that malicious activity, by its nature, exposed larger numbers of records than other types of incidents.

TOTAL COSTS (including SIR)

	Cases	Min	Median	Mean	Max
Hacker	41	2,500	210,856	1,863,419	15,000,000
Lost/Stolen Laptop/Device	21	290	55,000	140,784	1,650,000
Malware/Virus	36	1,190	99,380	468,788	3,952,626
Other	20	1,789	14,940	44,447	287,000
Paper Records	11	1,000	12,634	22,987	60,000
Rogue Employee	12	8,914	80,338	1 ,023,595	11,491,000
Staff Mistake	16	1,234	9,871	133,609	1,603,800
System Glitch	10	1,825	25,878	207,867	779,293
Theft of Hardware	1	110,000	110,000	110,000	110,000
Theft of Money	4	23,755	49,250	94,314	255,000
Total	**172**				

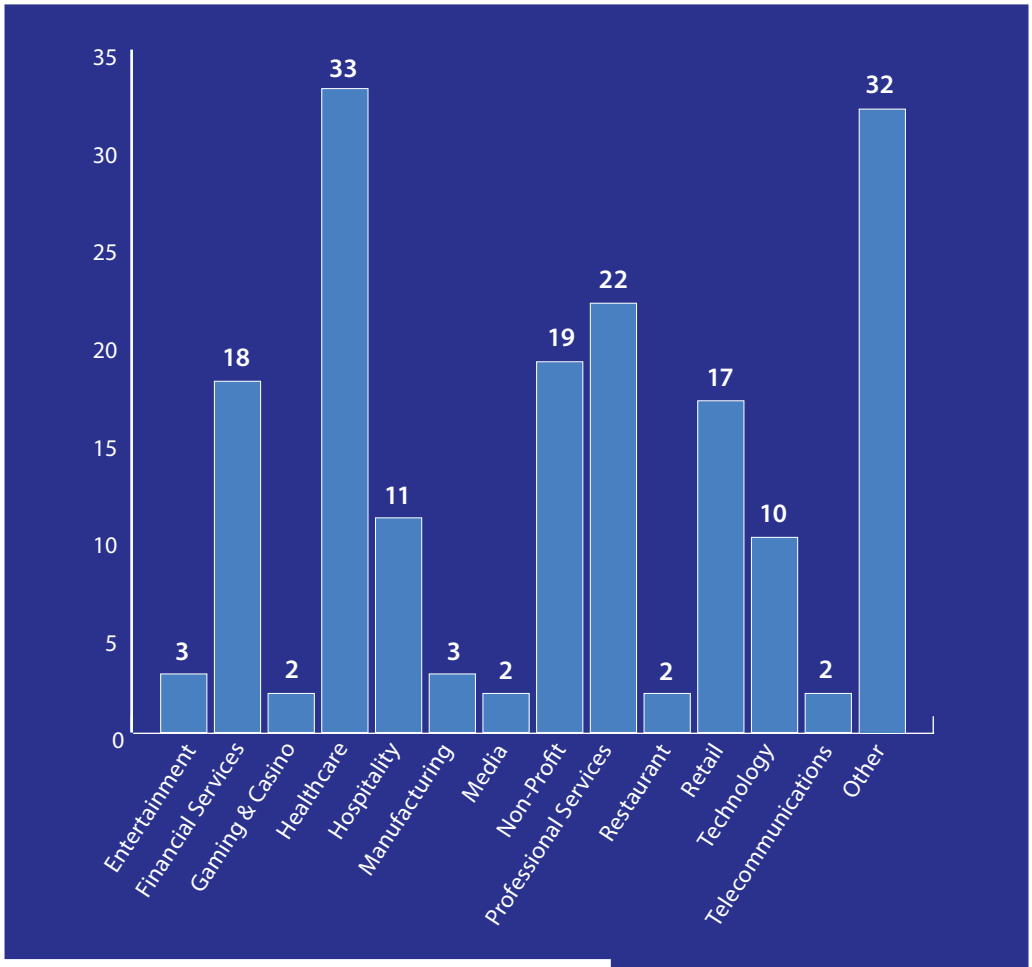
TABLE 8

"Symantec discovered more than 430 million new unique pieces of malware in 2015, up 36% from the year before. Understanding the cost of cyber crime with this year's NetDiligence claims study is more important than ever."

SYMANTEC

BUSINESS SECTOR

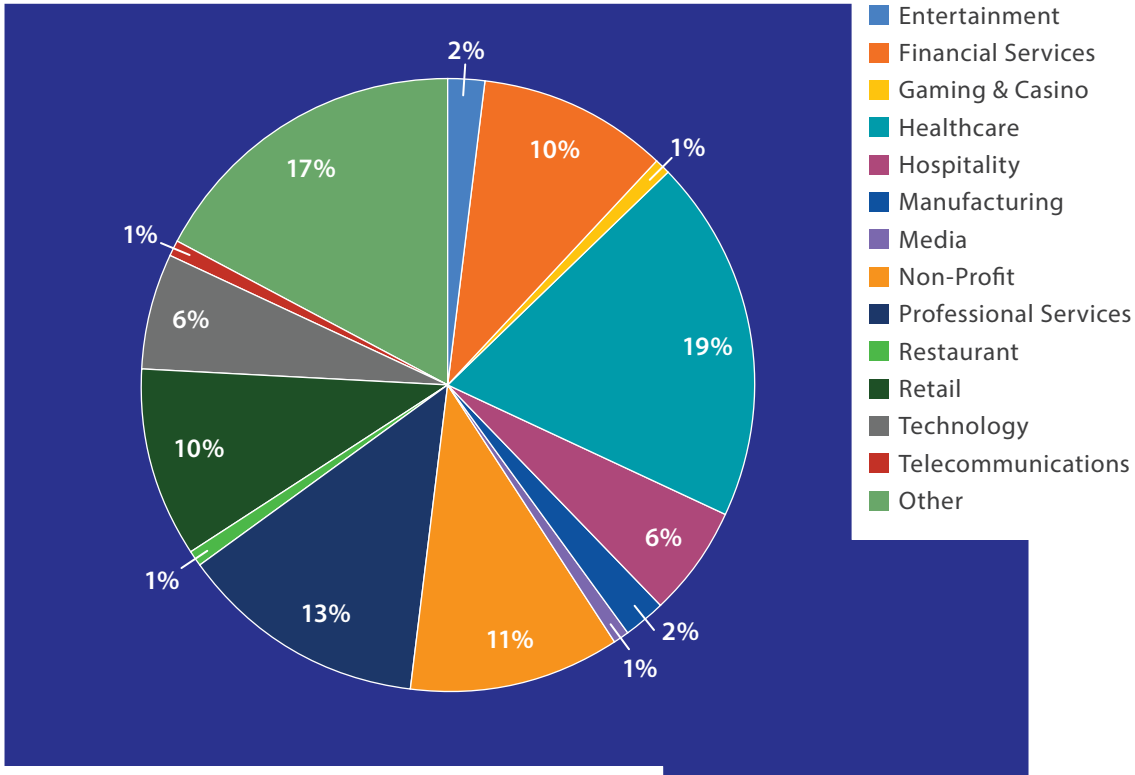
Again this year, Healthcare was the most affected sector with 33 claims. The "Other" category (claims from companies that did not fit into our categories) came in second this year with 32 claims.[3] Professional Services came in third with 22 claims, followed by Non-Profit (19 claims), and Financial Services 18 claims, and Retail with 17 claims.



NUMBER OF CLAIMS BY BUSINESS SECTOR
(N = 176)

FIGURE 15

[3]The data collection form uses 13 pre-defined business sectors, not including the "Other" category. If an organization does not fit into one of the 13 categories, it will be classified as "Other". We will consider expanding the number of business sectors in next year's report.

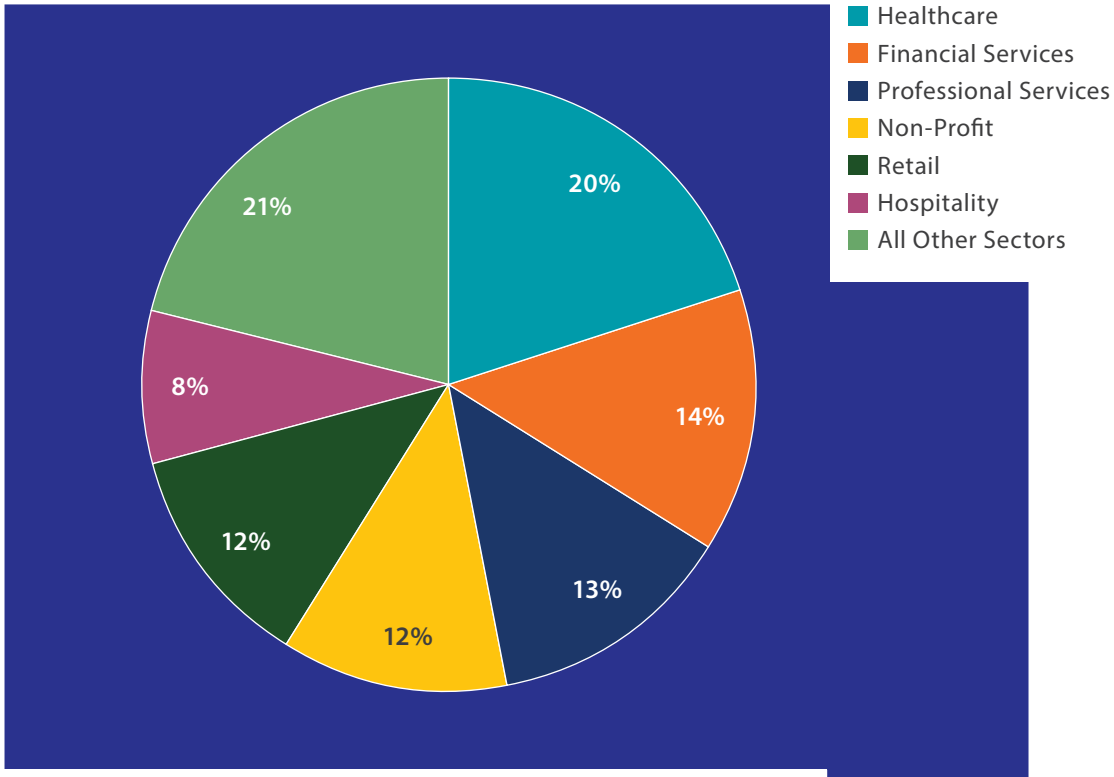


PERCENTAGE OF CLAIMS BY BUSINESS SECTOR
(N = 176)

FIGURE 16

Records Exposed

120 claims (68%) reported number of records exposed. The largest number of incidents occurred in Healthcare, Other, and Financial Services.



PERCENTAGE OF RECORDS EXPOSED BY BUSINESS SECTOR
(N = 120)

FIGURE 17

RECORDS					
	Cases	**Min**	**Median**	**Mean**	**Max**
Entertainment	1	332	332	332	332
Financial Services	17	2	983	5,167,548	78,000,000
Gaming & Casino	1	100,000	100,000	100,000	100,000
Healthcare	24	1	712	647,559	3,900,000
Hospitality	9	2,000	17,000	22,783	100,000
Manufacturing	2	250	2,225	2,225	4,200
Non-Profit	14	1	331	12,659	163,625
Professional Services	15	1	100	87,474	1,100,000
Retail	14	1,630	19,750	9,831,667	56,000,000
Technology	4	875	151,000	295,719	880,000
Telecommunications	1	1,000,000	1,000,000	1,000,000	1,000,000
Other	18	1	111	3,823	56,000
Total	**120**				

TABLE 9

Costs

98% of the claims in this year's dataset included both the business sector affected and the total claim amount, including SIR. Financial Services and Retail sectors had the highest average costs. This is primarily due to a few extremely large incidents (caused by Hackers and Malware/Virus) within those two sectors.

TOTAL COSTS (including SIR)					
	Cases	**Min**	**Median**	**Mean**	**Max**
Entertainment	3	6,950	21,890	17,532	23,755
Financial Services	17	1,000	118,671	1,806,172	15,000,000
Gaming & Casino	2	287,000	706,500	706.500	1,126,000
Healthcare	32	4,000	640,815	717,160	7,130,000
Hospitality	11	2,500	184,385	868,203	5,650,000
Manufacturing	3	11,625	34,343	27,919	37,790
Media	2	73,480	74,240	74,240	75,000
Non-Profit	19	1,234	32,806	208,015	1,606,550
Other	30	1,789	28,519	76,958	779,293
Professional Services	22	290	20,409	80,378	446,946
Restaurant	2	17,047	19,059	19,059	21,070
Retail	17	17,408	210,856	1,704,774	10,000,000
Technology	10	26,121	323,655	1,039,792	4 ,961,000
Telecommunications	2	12,994	997,345	997,345	1,981,695
Total	**172**				

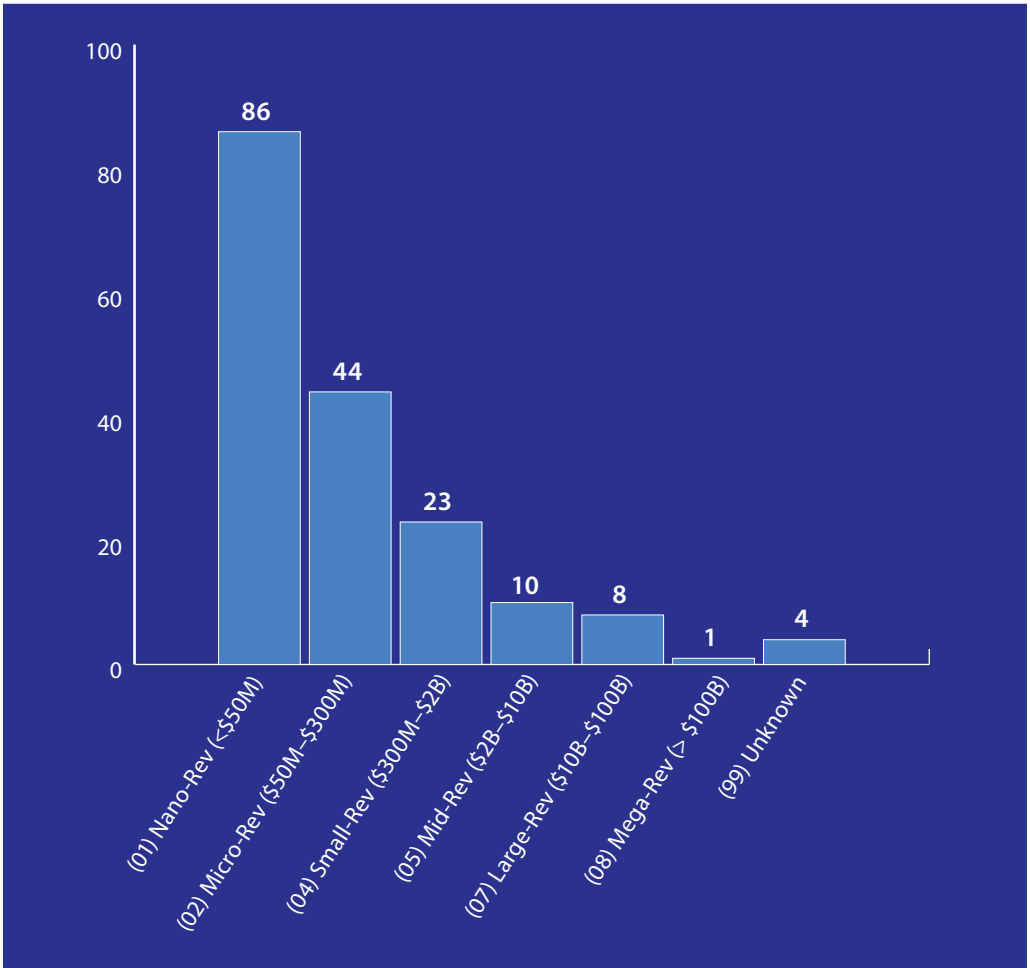
TABLE 10

Individually, Financial Services and Retail had the highest average costs of all sectors.

SIZE OF AFFECTED ORGANIZATION (BASED ON REVENUE)

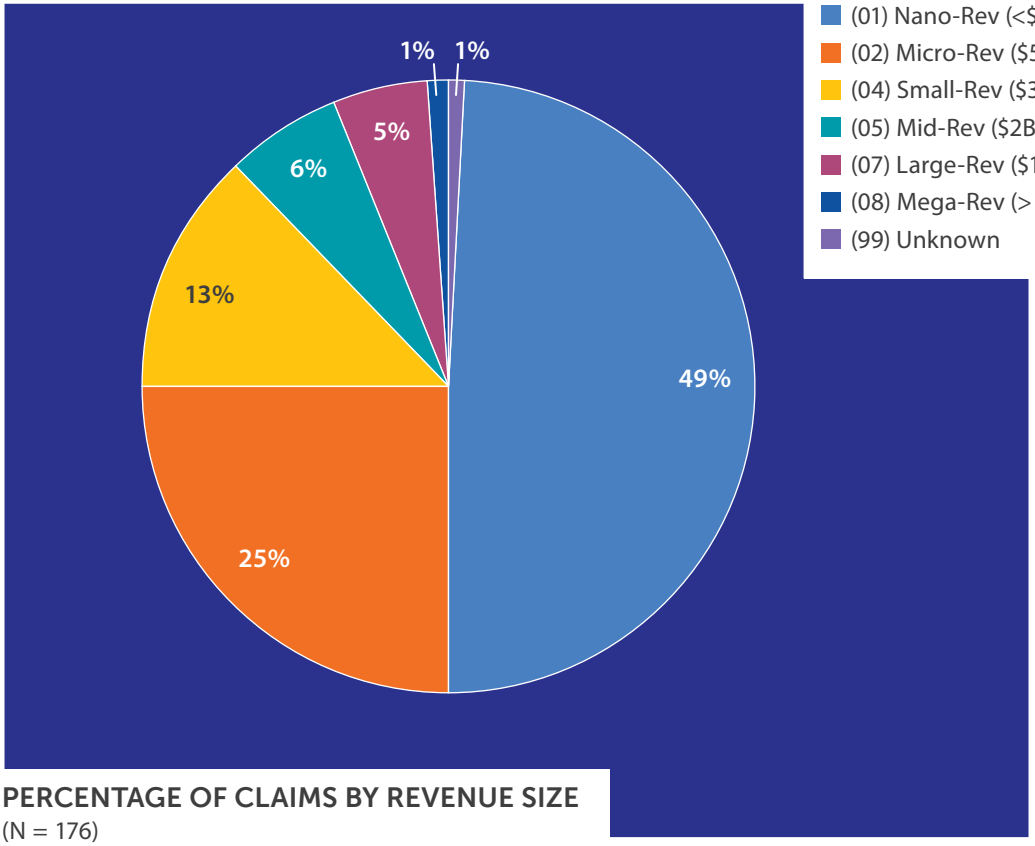
Revenue size was reported for almost all (98%) of the claims in the dataset. Nano-Revenue (<$50M) organizations were the most impacted, accounting for 86 claims (49%). They were followed by Micro-Revenue ($50–300M), which accounted for 44 claims (25%), and Small-Revenue ($300M–$2B), which accounted for 23 claims (13%). Mid-Revenue ($2–10B) organizations accounted for 10 claims (6%), while Large-Revenue ($10–100B) organizations accounted for 8 claims (5%). There was one claim for a Mega-Revenue (>$100B) organization and four claims that did not report the size of the organization.

This mirrors our previous findings: smaller organizations experience most of the incidents. Our continuing hypothesis—which nothing in this year's study disproves—is that this is due to the fact that there are simply more small organizations than there are large ones. Other contributing factors may be that smaller organizations are less aware of their exposure or they have fewer resources to provide appropriate data protection and/or security awareness training for employees.



NUMBER OF CLAIMS BY REVENUE SIZE
(N = 176)

FIGURE 19



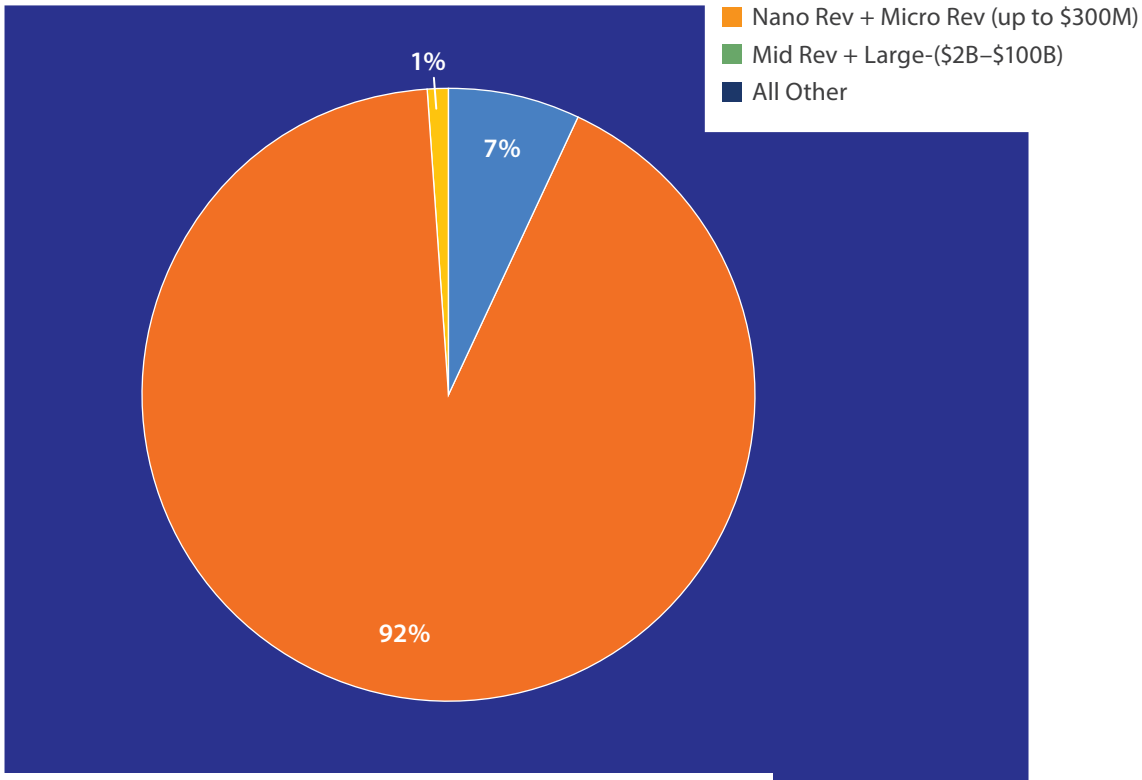
PERCENTAGE OF CLAIMS BY REVENUE SIZE
(N = 176)

FIGURE 20

Records Exposed

While Nano-, Micro- and Small-Revenue organizations accounted for a combined 87% of the claims in our dataset, they were responsible for only 7% of records exposed. That falls in line with our expectations that smaller organizations are likely to have weaker security controls, but also that they would typically store less data.

The converse is equally true. Mid- and Large-Revenue organizations accounted for only 10% of claims, but they were responsible for 92% of records exposed.



PERCENTAGE OF RECORDS EXPOSED BY REVENUE SIZE
(N = 120)

FIGURE 21

RECORDS					
	Cases	**Min**	**Median**	**Mean**	**Max**
(01) Nano-Rev (<$50M)	52	1	838	234,711	3,900,000
(02) Micro-Rev ($50M–$300M)	31	1	788	131,793	3,200,000
(04) Small-Rev ($300M–$2B)	15	4	5,178	142,670	1,000,000
(05) Mid-Rev ($2B–$10B)	9	1	674	170,145	1,274,700
(07) Large-Rev ($10B–$100B)	8	1	24,500,000	28,033,750	78,000,000
(08) Mega-Rev (>$100B)	1	700,000	700,000	700,000	700,000
(99) Unknown	4	47	152	38,003	151,662
Total	**120**				

TABLE 11

Costs

As might be expected, claims for breaches occurring in larger organizations were substantially higher than claims for smaller organizations. The average claim for a Large-Revenue organization was **ten times** the average claim for a Small-Revenue organization.

With that in mind, it was surprising that once again this year some of the largest claims came from Nano-, Micro-, and Small-Revenue organizations. This year's dataset included 21 claims in excess of $1 million (12%). 86% these cases involved Hackers or Malware/Virus (18 out of 21). And, 81% of these cases (17 out of 21) involved Nano-, Micro-, and Small-Revenue organizations that were the victims either of hackers or malware.

The largest legal costs (defense and settlements) in this year's study were from two Micro-Revenue organizations ($50–300M), one of which lost valuable trade secrets to a hacker and the other of which exposed PHI due to a lost laptop. The combined legal costs for these two organizations ranged from $1.5 million to more than $4.5 million. The largest regulatory claim occurred in a Mega-Revenue organization, and totaled almost $6 million.

TOTAL COSTS (including SIR)

	Cases	Min	Median	Mean	Max
(01) Nano-Rev (<$50M)	85	290	49,000	215,297	7,130,000
(02) Micro-Rev ($50M–$300M)	44	1,000	88,154	487,411	6,570,000
(04) Small-Rev ($300M–$2B)	23	4,278	118,671	599,907	5,650,000
(05) Mid-Rev ($2B–$10B)	9	2,662	91,457	173,851	678,000
(07) Large-Rev ($10B–$100B)	8	1,603,800	3,326,313	5,965,571	15,000,000
(08) Mega-Rev (>$100B)	1	11,491,000	11,491,000	11,491,000	11,491,000
(99) Unknown	2	7,338	9,482	9,482	11,625
Total	**172**				

TABLE 12

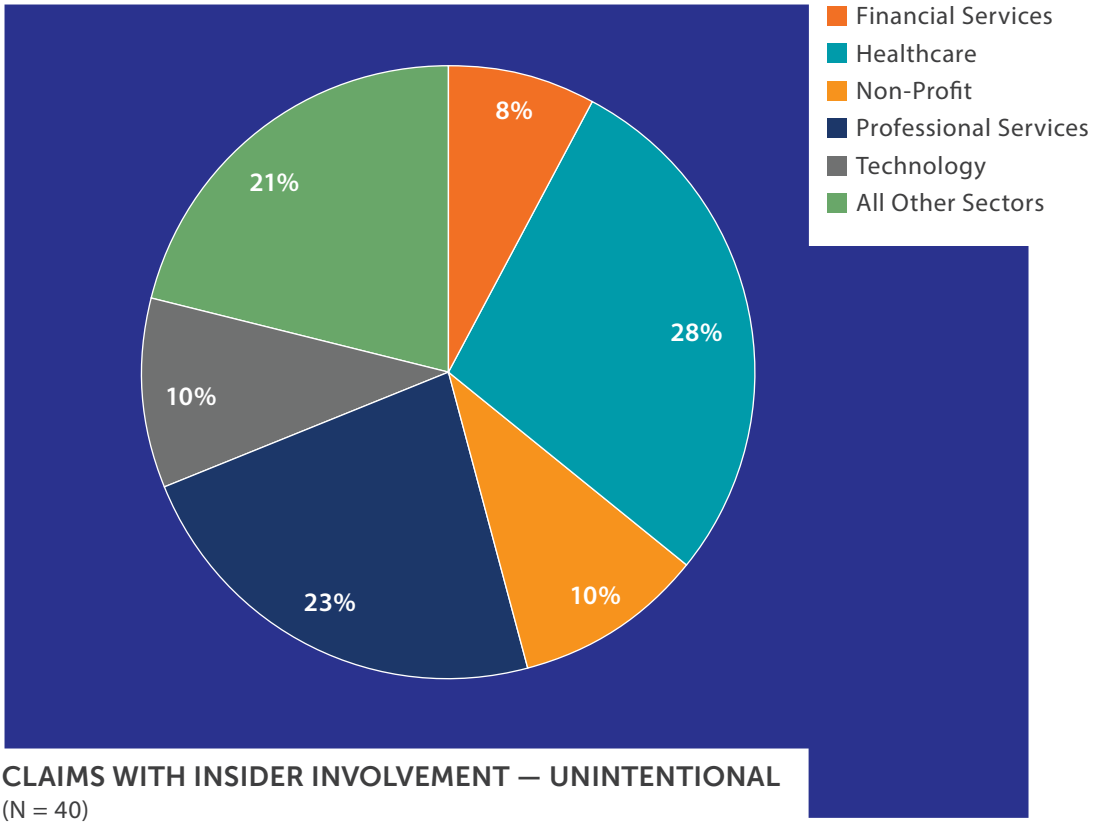
The largest legal costs were from Micro-Revenue organizations. The largest regulatory costs were from the actions of a rogue employee at a Mega-Revenue organization.

INSIDER INVOLVEMENT

We asked insurers to tell us whether there was insider involvement in the claim events they submitted. 30% (52 out of 176) were attributable to Insiders. This percentage is slightly lower than what we found in last year's study (32%).

Of the claims attributable to Insiders, 77% (40 out of 52) were unintentional, caused primarily by staff mistakes and errors in paper handling. The remaining 23% (12 out of 52) were malicious in nature, all caused or abetted by rogue employees.

Insider-related incidents resulted in the exposure of every type of data and occurred in almost every business sector. Half of the insider-related incidents occurred in Healthcare and Professional Services (20 out of 40). Also of note: even though Financial Services accounted for about 6% of incidents (4 out of 52)[4], the single malicious financial services related insider event in our database created a claim in excess of $10 million.

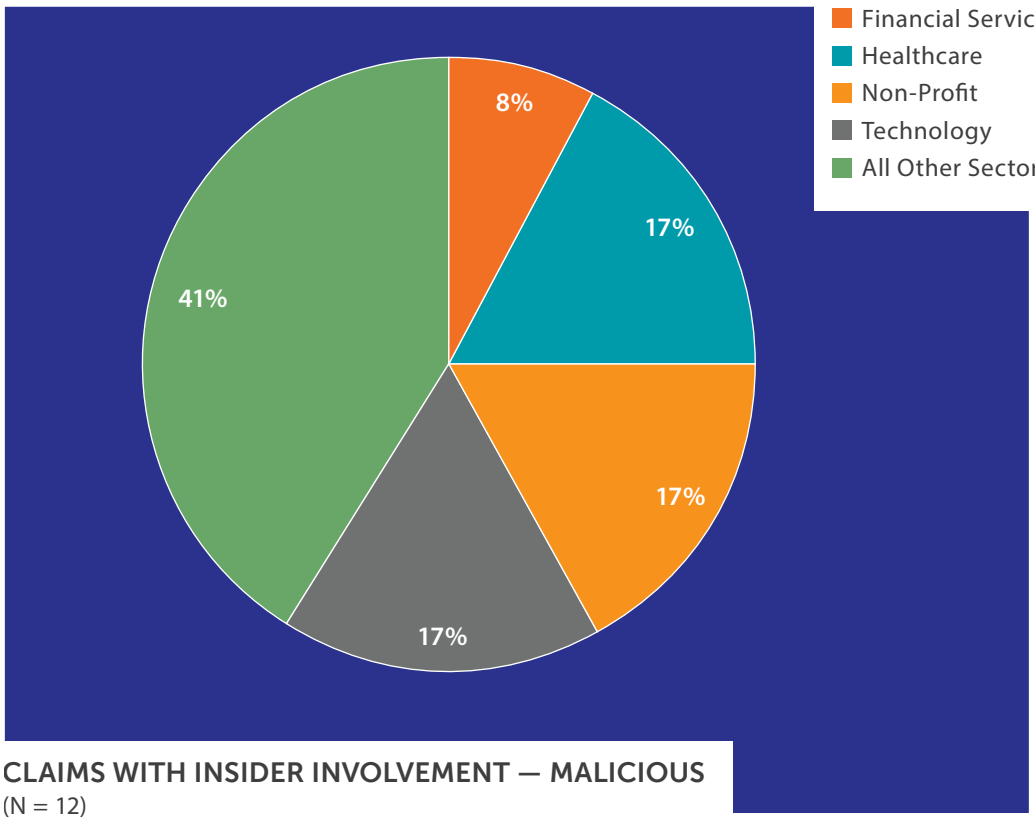


CLAIMS WITH INSIDER INVOLVEMENT — UNINTENTIONAL
(N = 40)

FIGURE 23

Insider events were few in the Financial Services sector. However, the single malicious event in our database generated a claim in excess of $10 million.

[4]There were 4 Financial Services Insider events: 8% (3/40) non-malicious and 6% (4/52) overall.



CLAIMS WITH INSIDER INVOLVEMENT — MALICIOUS
(N = 12)

FIGURE 24

Of the 52 claims attributable to insider actions, 35 (67%) reported the number of records exposed. Three claims—one due to Malware/Virus, one due to an unintentional disclosure (Staff mistakes), and one due to a malicious rogue employee—accounted for the overwhelming majority of records exposed.

RECORDS

Insider Involvement	Number of Claims	Total Records	Min	Median	Mean	Max
Unintentional	26	2,033,069	1	68	78,195	1,100,000
Malicious	9	719,260	270	3,050	79,918	700,000
Total	**35**	**2,752,329**				

TABLE 13

For the first time, total costs were reported for almost all of the insider-related claims. As was the case last year, maliciously motivated insider events result in more expensive average claims, by a factor of nearly five in this year's study.

TOTAL COSTS (including SIR)

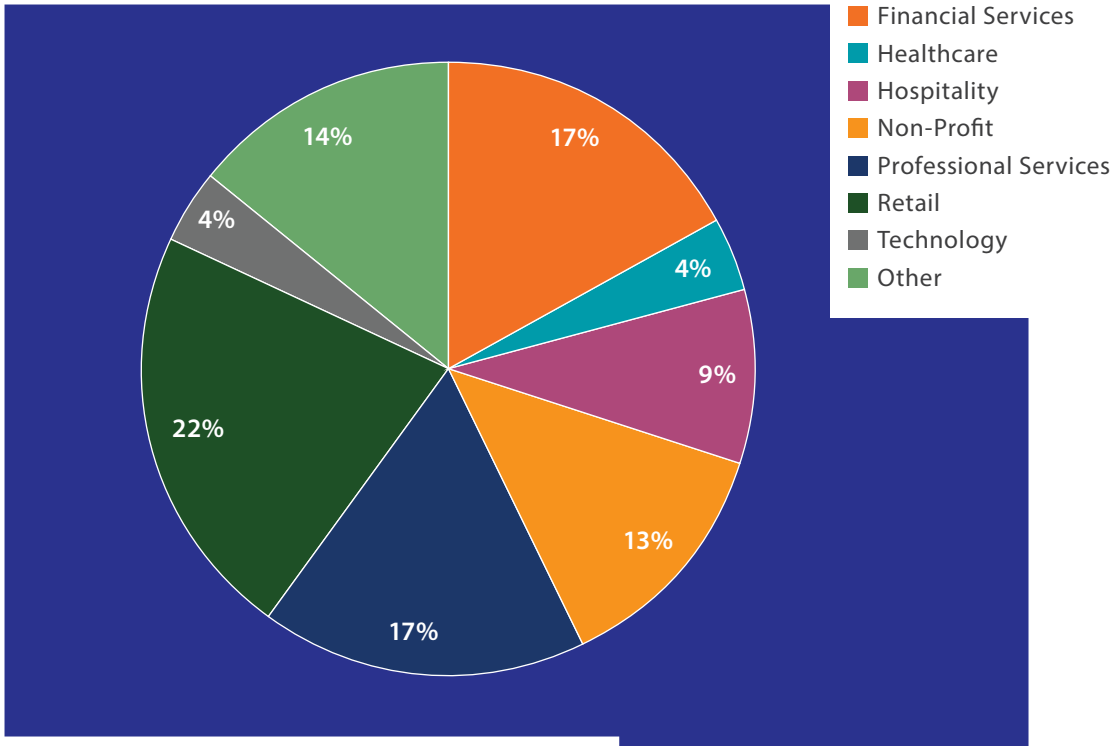
Insider Involvement	Number of Claims	Total Cost	Min	Median	Mean	Max
Unintentional	39	8,984,135	594	31,645	230,362	4,961,000
Malicious	12	12,283,139	8,914	80,338	1,023,595	11,491,000
Total	**51**	**21,267,274**				

TABLE 14

THIRD-PARTY BREACHES

Again this year we asked insurers to indicate whether their claim events were caused by a third-party vendor: 13% were attributable to third parties.

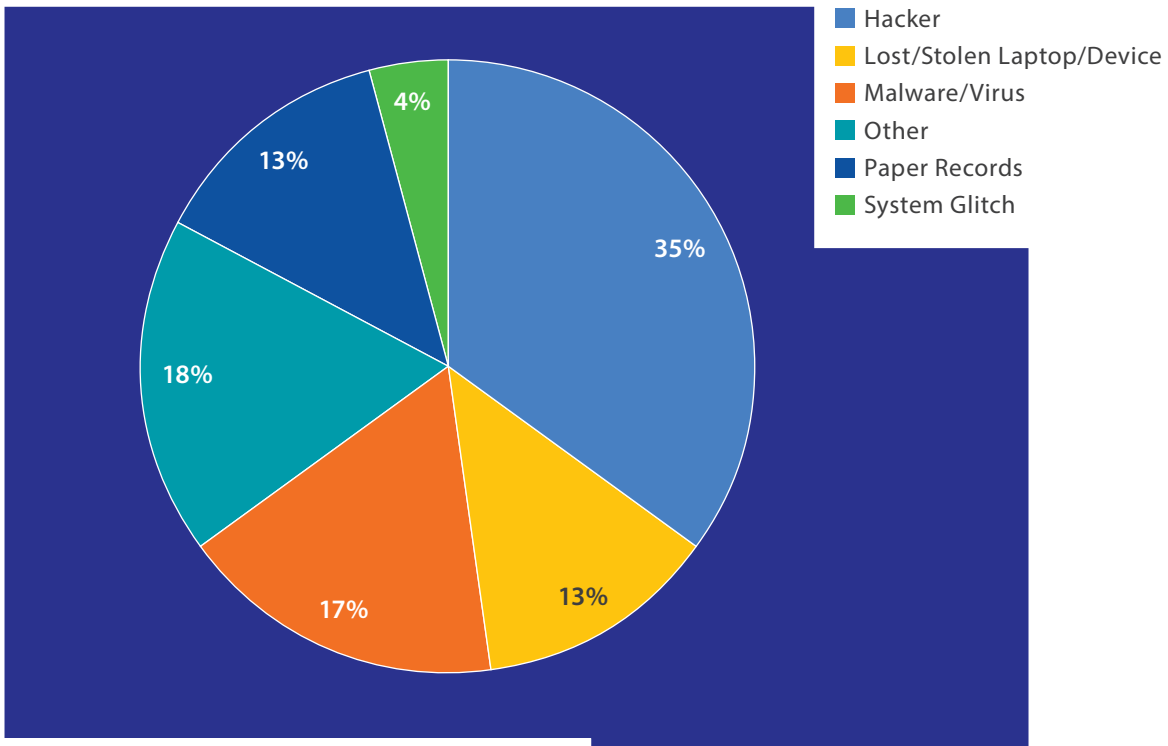
Since most organizations use third-party vendors, it should be no surprise third-party breaches occurred in almost every business sector. Again this year, the greatest percentage (22%) of third-party breaches occurred in the Retail sector. Financial Services and Professional Services tied for second place at 17%. Hackers accounted for twice as many (35%) third party incidents as the second most frequent causes of loss (Malware/Virus and Other at 17% each). Other causes that contributed to third party claim events included Lost/stolen laptop/device, Paper Records, and System Glitches. Each of these causes were cited in 4–13% of the claims in this year's dataset.



THIRD PARTY CLAIMS BY BUSINESS SECTOR
(N = 23)

FIGURE 25

13% of events in the dataset were caused by third-party vendors.



THIRD PARTY CLAIMS BY CAUSE OF LOSS
(N = 23)

FIGURE 26

On average, third-party breach events exposed significantly fewer records than breach events that occurred at policyholder organizations. This can easily be explained by several large outliers in the dataset where there was no third party involvement.

RECORDS						
Third-Party Involvement	**Number of Claims**	**Total Records**	**Min**	**Median**	**Mean**	**Max**
Yes	17	587,396	8	983	34,553	300,000
No	103	244,496,520	1	1,500	2,373,753	78,000,000
Total	**120**	**245,083,916**				

TABLE 15

Perhaps because the third-party breach events were smaller, breach costs for these events were also smaller. Average breach costs for third-party breaches were not quite one-quarter of the of those for in-house breaches whereas median breach costs were about half.

TOTAL COSTS (including SIR)						
Third-Party Involvement	**Number of Claims**	**Total Cost**	**Min**	**Median**	**Mean**	**Max**
Yes	22	3,533,940	611	27,549	160,634	1,650,000
No	150	110,809,395	290	67,113	738,729	15,000,000
Total	**172**	**114,343,335**				

TABLE 16

CLOUD INVOLVEMENT

This year, the data collection form included two new data elements related to cloud: a "Yes/No" for cloud involvement and a description for the type of involvement, if any.

Although we suspect a much higher degree of cloud involvement, only two respondents indicated a cloud component in a claim. One claim involved a malicious employee and DropBox and one involved a staff mistake. Both claims were small: less than $50K each.

CYBER EXTORTION/RANSOMWARE

We were able to identify six cases of ransomware: 5 in Nano-Rev companies and 1 in a Micro-Rev Company. Malware/Virus was the cause of loss in 5 of 6 events, with 1 event caused by a Hacker. Claims costs ranged from $12.5K to 75K, with an average cost of $32K and a median cost of approximately $26K. All costs reported were for Crisis Services, split between forensics costs and legal guidance. As one would expect, there were no Notification or Credit/ID Monitoring costs.

PHISHING

We were able to identify 8 claims that involved Phishing and Social Engineering. These incidents had total costs ranging from $24K to nearly $450K, with an average cost of $123K and a median cost of $62K. Most cases had Crisis Services costs only (5 of 8), ranging from a low of $2.5K to a high of nearly $400K. Notably, however, were three cases with Legal Damages Settlements ranging from $19K to $250K. The companies involved were all Small-Rev or smaller, and the sectors were varied: Professional Services, Healthcare, Technology, and Entertainment. Data types were also varied: PCI, PII, and non-card Financial. Causes of loss included Theft of Money, Malware/Virus, and Hackers.

Phishing and Wire Transfer Fraud

Of the 8 claims discussed above, 3 involved phishing and social engineering that led to the fraudulent transfer of money from the victim company to the criminal perpetrators. The costs of these incidents ranged from $26K to nearly $400K, all in Crisis Services. We do not believe that these numbers include the amounts of money fraudulently transferred.

POS-RELATED/COMMON POINT OF PURCHASE (CPP) INVESTIGATIONS

Given the attention paid by the news to POS-related breaches in 2014 and 2015, we thought that it might be informative to examine all of the POS-related events in the database. There were two ways we were able to find these events: 1) by looking at the event description for clues that a POS System was involved; and 2), by identifying all of the Common Point of Purchase (CPP) Investigation claims.

Using this approach, we were able to identify 14 claims. Not surprisingly, all of these events involved PCI-related data. Nano-Rev (11) and Micro-Rev (2) companies comprised the large majority of organizations. The remaining organization was a Large-revenue one. The organizations operated in the sectors one would expect: Restaurant, Retail, Hospitality, Entertainment, and Gaming/Casino.

Total costs ranged from $2.5K to nearly $4 million, with an average cost of $387K and a median cost of $17K. The largest claim ($4 million) occurred at a Large-Revenue organization. It should be noted that this claim has a powerful skewing effect on this subset of the data which can be seen in the wide variance between the median and average values—a factor of over 20.

ABOUT FIRST-PARTY LOSSES

Most claim events include both first-party and third-party losses. But there are some incidents that are exclusively first party.

This year, there were thirteen such incidents—three involving business interruption, one theft of trade secrets, six instances involving ransomware, and three instances involving phishing that resulted in fraudulent wire transfers.

Two of the business interruption incidents were caused by Malware/Virus and the third by Hacking. All of the business interruption incidents involved Distributed Denial of Service (DDoS) attacks. One of the incidents occurred in the Technology sector and two in Retail. The payouts for actual business interruption were all <$35K, suggesting that the disruptions were of limited duration, but one of the incidents included a $750K damages settlement, and the overall total claims amounts for these three events, including Crisis Services, Legal Settlements, and other costs ranged from $17.4K to over $1 million.

The trade secrets theft occurred at a Small-Rev ($300M–$2B) technology company and involved the theft of digital film by hackers. The total breach costs were nearly $5M, almost all of which were due to a legal damages settlement.

The ransomware and other phishing claims were described in the previous section.

For comparison purposes, below are the exclusively first-party claims payouts included in prior years:

- In our 2015 study, there were six first-party claims—two involving business interruption, one theft of trade secrets, and three instances of wrongful data collection. Both business interruption incidents were caused by Malware/Virus. One incident occurred in the Healthcare sector and one in Retail. The Healthcare incident was resulted in a 330+ hour systems outage, but no loss of data. The Retail incident was much larger, exposing more than 50 million records and causing a business outage that lasted five months.

  The incident that involved the theft of trade secrets occurred in the Healthcare sector and was caused a Rogue Employee.

  The three instances of Wrongful Data Collection all resulted in class action lawsuits.

- In the 2014 study, there were also six first-party claims—three involving business interruption and three involving theft of trade secrets. The business interruption claims ranged from $1.5 to $5 million for lost business income, recovery expenses and legal defense. The claims for theft of trade secrets ranged from $150,000 to $900,000, primarily for forensics
- In our 2013 study, there were five first-party claims submitted: four distributed denial of service (DDoS) attacks and one malware incident. The costs for these incidents were pending at the time we conducted our study.
- In our 2012 study, there were five first-party claims submitted: two business interruption incidents, two incidents involving theft of trade secrets and one incident involving online copyright infringement. Most of the costs for these incidents were pending at the time we conducted our study; however, one claim had paid out almost $500,000 for forensics.
- Our 2011 study saw ten first-party claims submitted for DDoS attacks, malware and cyber extortion. The incidents accounted for approximately $1.22 billion in lost business income and $23 million in expenses. One incident resulted in fines of approximately $4 million.

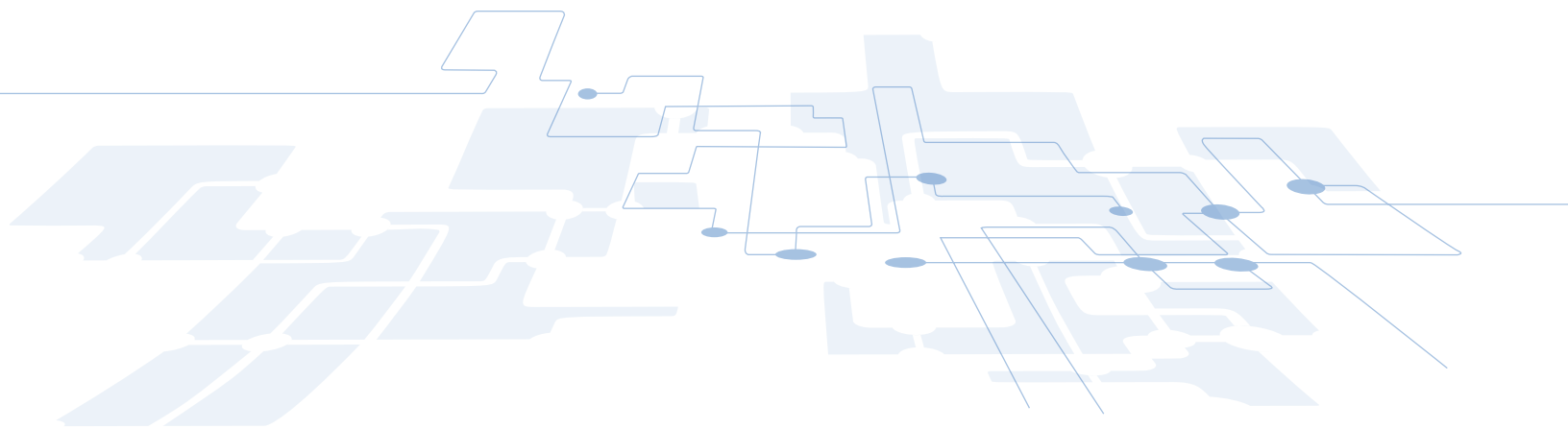
CONCLUSION

Our objective for this study is to help Insurers, Underwriters, Risk Managers, CEO's, CFO's, and CISO's understand the true impact of data insecurity by consolidating claims data from multiple insurers so that the combined pool of claims is sizable enough that it allows us to ascertain real costs and project future trends.

Despite increasing awareness around cyber security and the increasing frequency of data breach events, it has been difficult to fully assess the insurance cost (severity) of these incidents.

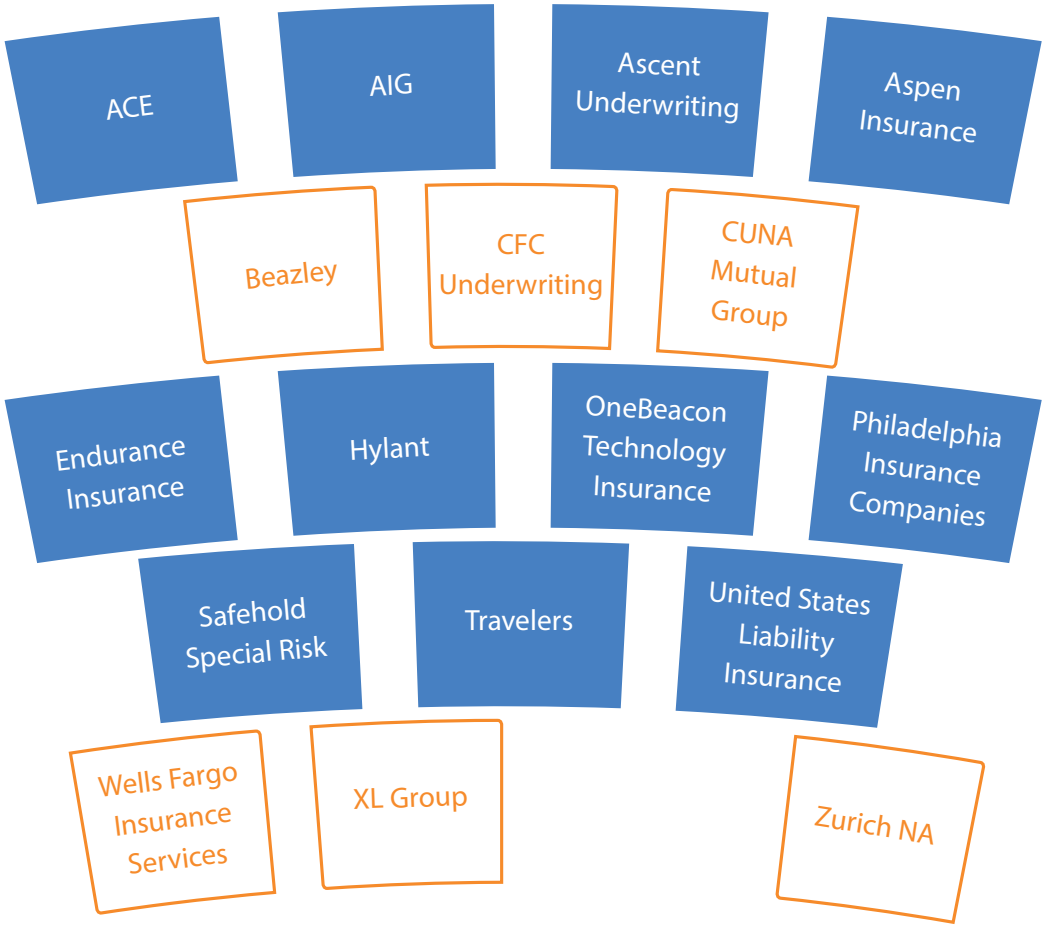
While many leading cyber liability insurers are participating in this study, there are many insurers that have not yet processed enough cyber claims to be able to participate. So our analysis is a work in progress, but still producing some interesting results.

It is our sincerest hope that each year more and more insurers and brokers will participate in this study—that they share more claims and more information about each claim—until it truly represents the cyber liability insurance industry overall. 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 total cyber claims. If we can expand participation in these two ways, our findings will become much more meaningful to everyone involved in the cyber insurance market.



INSURANCE INDUSTRY PARTICIPANTS

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



CONTRIBUTOR

Risk Centric Security, Inc.

A special thank you goes to Heather 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 helped analyze the data submitted for this study and write 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, Event & Sponsorships Manager, NetDiligence
- Dane Greisiger, Analytics Intern, NetDiligence
- Sharon Lyon, President, Lion's Share Marketing Group, Inc.

PLATINUM SPONSOR

The 2016 Cyber Claims Study again highlights the complex and unpredictable data breach response landscape that businesses face. While the data in the study points to widely variable and relatively high claims costs for services like notification, identity theft protection, and even resulting legal settlements, we have seen that reserving resources before an incident greatly reduces response costs.

Today, almost every business has an incident response plan in place. What many businesses don't realize, however, is that simply having an incident response plan no longer guarantees a successful breach response. with over ten years of experience helping leading businesses successfully prepare for and respond to the largest and most complex breaches in history, we have seen 3 key components that supplement an incident response plan and make a business truly ready to respond to data breach events with quality and speed.

1. Specialized Breach Response Manpower

A data breach drives an immense and immediate demand on your business, so having an army of experts who are guaranteed to mobilize immediately with high quality in the event of a breach is critical to success. These experts need to be trained in identity theft protection best practices and incident specifics to ensure they can effectively answer customer questions. To do this, partner with a data breach response partner who will offer a contractual guarantee that resources will be available when you need them. This type of a promise requires an upfront investment on the part of your business and the response provider.

2. Scalable Breach Response Infrastructure

Normal business operations do not stop when a breach occurs, and your employees need to be able to focus on continuing to run your business. Partnering with specialists who have the proven tools, processes, and systems to stand up a response quickly without draining your internal resources is another critical component of true breach readiness. One common mistake we see businesses make is thinking they can handle the influx of customer calls with their internal call centers. This fails to account for the "run the business" work that the existing call centers will need to handle, as well as the training and specialization required to successfully reassure customers after a data breach. It's important to choose a partner with the response expertise and infrastructure to enable a successful response.

3. Robust Customer Response Readiness

The biggest gap we see in even the most robust incident response plans are the details of how to execute a customer-facing response. To move beyond mere preparation and become truly breach-ready, planning your customer-facing response is key. Here are some aspects to consider:

- 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
- Test your response plan through mock breach simulations and drills to expose any gaps in your plan and prepare your response team for critical decision-making and communication
- Regularly train your response team on the plan to build muscle memory

A data breach is one of the most trying events your business will face. Through continued collaboration and information sharing among industry leaders, 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

5 key considerations for effective business interruption coverage

Most key business processes are now automated and built on technology. Consequently, disruptions from a cyberattack can lead to significant lost sales and productivity, recovery costs and reputational harm. Accounting for business interruption costs is almost as important as mitigating the breach itself, especially as exposure is only expected to increase in the future.

The true cost of business interruption often requires complex calculations to accurately quantify the loss. Business owners must be prepared to objectively track and document losses from business interruption following a breach in order to work effectively with their insurer. Reimbursement of losses from the insurance company can help a business recover, but it is important to understand what insurers require following a breach, thus increasing the likelihood of an efficient claim process. These include:

- **Properly scope insurance coverage:** In many cases, companies' policies are incorrectly set up at policy inception and consequently, do not adequately transfer the risk under the policy. This often leads to a circumstance where the business is not properly indemnified for its full loss when an event occurs. For example, a common error at policy inception is a focus on worst case scenario events while a significant amount of money is left on the table for much more common, lesser-loss events.
- **Show proximity to the cause:** The purpose of most business interruption insurance is to get the business back to the same position as if the breach did not occur. For this reason, a business owner must show the loss estimates are directly related to the breach event. In other words, additional costs or lost sales would not have occurred "but for" the cyberattack. As an example, the mere fact a customer is lost may not be enough to include lost sales in a business interruption claim. One would likely need to show that the customer would not have been lost if the cyberattack had not occurred.
- **Have the facts in order:** If a cyberattack occurs, documented evidence of the breach and its economic impact must be provided. Affected entities are encouraged to immediately begin tracking unproductive time, lost sales, lost product, additional work hours or other costs associated with a breach. Comparison of trends in costs or sales before and after the breach can also be used to support a business interruption claim. Losses must be documented, and losses calculated or estimated with "reasonable certainty."
- **Duty to mitigate the loss:** Most insurers expect a claimant to mitigate the loss following a cyberattack. For example, if employees are unable to perform their work responsibilities following an attack and a business is obligated to pay them, it would likely be considered a business interruption cost. However, it would also be expected that management would mitigate the cost by reassigning the employees to other functions or sending hourly employees home when it became clear they would be unable to perform their duties.
- **Actual loss sustained:** The business interruption loss suffered should be quantified in a manner that illustrates the actual economic impact. This may mean that the loss claimed

under an insurance policy is reduced by successful mitigation measures, or by resources that are distracted by the claim circumstances but do not result in additional costs. For example, upper management is generally salary remunerated and therefore, a company does not actually incur additional costs despite the inevitable extra hours devoted to the company subsequent to a breach.

Organizations typically, and understandably, focus on getting systems running following an incident, but also must be prepared to document costs and losses related to business interruptions. Business interruption claims can be complex; therefore, notifying the insurance company, reviewing the insurance coverage and seeking advice regarding identifying and tracking losses related to business interruption following a breach are all critical elements of recovering from a cyberattack.

It is often difficult to go back and recreate the timeline and support for business interruptions after the fact. Inadequate planning and playing catch-up can leave you vulnerable to insufficient insurance coverage and difficulties supporting a business interruption claim.

Authors:

Sue Evelsizer, Senior Director, RSM US LLP
sue.evelsizer@rsmus.com, +1 309 497 1403

Brett Eaton, Senior Manager, RSM International LLP
brett.eaton@rsmza.co.za, +27 11 329 6000

SPONSOR:

CIPRIANI & WERNER
ATTORNEYS AT LAW

The NetDiligence 2016 Cyber Claims Study ("Study") continues its tradition of offering those involved in the cyber claims industry vital data as they prepare for, respond to and recover from, cyber breach events. The greater the volume of reported data, and the more frequent the interaction among those professionals in this industry, the greater the awareness and understanding of breach events. This information suggests certain "best practices" for insureds to follow as they consider what is needed to obtain appropriate coverage and minimize the risk exposure in the event of a breach. These two categories, preparation through thorough assessment and rapid response to maximize loss mitigation, are two essential topics companies need to address as they navigate through the cyber-related business and legal risks that confront them.

Many organizations are now addressing the decision of whether to obtain cyber insurance coverage. Recently reported legal decisions from different jurisdictions suggest that the number of cyber breach damage claims, and, more than likely, lawsuits will increase as: 1) additional courts follow the 7th Circuit Court decision and allow Plaintiffs to establish "standing" where there is an "objectively reasonable likelihood" that injury will occur to customers who have had their PII stolen; and 2) insurance carriers have begun to scrutinize the conduct of their insured's actions both pre- and post-breach, while placing Cyber coverage.

Cyber insurance coverage is best obtained after the applicant has taken appropriate steps to assess its vulnerabilities and evaluate its other cyber related risks. This assessment is not simply related to its information technology or network security. It includes internal processes and procedures to educate and train personnel and to evaluate third-party risks such as vendor contracts. The assessment should also include a review and understanding of state and federal regulations that address a company's responsibility to preserve and protect information as well as regulations specific to an industry, e.g. HIPAA.

Once the assessment has been completed and thoroughly evaluated by corporate officers, recommendations should be presented to the Board of Directors. This will ensure the involvement of management as well as directors, each of whom will have their own risk tied to compliance standards for E&O/D&O Policies. From these recommendations should flow decisions, reduced to an action plan for the implementation of actions to correct deficiencies in advance of seeking coverage, and if thorough, an incident response plan that addresses breach response that includes actions to be taken by employees as well as outside professionals who will be needed immediately to respond to the emergency.

With cyber insurance in place the insured must remain vigilant in order to meet the terms and conditions of many cyber policies and to maintain awareness and compliance with the evolving "industry standards" and government regulations for maintaining privacy and protecting against cyber breaches. This means that all businesses, not simply those in the high breach sectors identified by the Study such as health care, financial services or retail, must deploy and maintain appropriate data protection measures.

Such vigilance will place the insured in the best position in the event a breach results in regulatory claims or litigation. Traditional elements of tort liability will require failure on the part of the insured to satisfy standards, i.e. the legal breach of duty. Absent a strict liability standard, the vigilant insured provides not only protection to the officers and directors but also the foundation its attorneys will need to mount an aggressive defense.

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 is a proud sponsor of the NetDiligence® Cyber Claims Study. The 2016 report shares a wealth of insights on the state of cyber insurance claim severity and is a natural compliment to the event frequency data we see in our product telemetry and global intelligence network. Cyber insurance makes companies more resilient to a wide range of cyber risks and the costs associated with data breaches and business interruption.

Symantec Cyber Insurance (**www.symantec.com/solutions/insurance**) is committed to empowering actuaries, underwriters, brokers, portfolio managers and risk analysts with security analytics tailored to the cyber insurance industry, incorporating data from the insurance and cyber security communities.

Key Challenges in Cyber Underwriting

Underwriters lack access to the same data, and evaluation criteria as other insurance lines. Underwriters need to understand the risks associated with a potential client, including the company's industry, geography, scale, services and security posture in a dynamically changing environment.

Symantec Cyber Insurance Analytics for Underwriters

Gain Speed and Efficiency: Symantec's tools help underwriters to ask the right questions and pre-populate information about the client. This leads to faster response times, more informed underwriting decisions and a competitive advantage.

Refine Risk Selection Process: Underwriters can assess the sources and drivers of risk using publicly available information, and aggregated data for comparable peers, using Symantec's analytics. This can improve underwriting margins and lead to more informed risk selection.

Yield Profitable Returns: Insurers should ascertain a customer's ability to not just prevent cyber attacks, but also proactively detect. Symantec leverages its internal data and outside-in insights to spot clients that could have lower average claims.

Key Challenges in Cyber Catastrophe Modeling

Insurers are concerned about commercial cyber insurance because they don't have a well-defined framework to manage these newer types of risks. Insurers are unsure about whether the individual loss events can be managed across a portfolio of insurance policies and the nature of aggregation risk.

Symantec Cyber Catastrophe Modeling for Portfolio Managers

Model Cyber Catastrophe Scenarios: To understand the key elements related to a cyber catastrophe and its impact, insurers need to model a variety of extreme but conceivable scenarios that could lead to worldwide impact. Symantec has developed cyber catastrophe scenarios and analytics for insurers.

Track Portfolio Risk with Loss Projections: Symantec enables insurers to stress test their portfolio corresponding to potential cyber catastrophe scenarios. Insurers are able to better quantify the probability of unexpected losses using a robust cyber model informed by historical cyber security data.

Grow your Book of Business Systematically: Cyber catastrophe is an accumulation risk, so it's vital for insurers to model and appropriately diversify risk to increase capacity. When combined with Symantec's analytics for Underwriters, insurers are better placed to meet demands from their clients and manage their risk capital.

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments, and individuals secure their most important data wherever it lives.

NetDiligence®

ABOUT NETDILIGENCE®

NetDiligence® (**www.netdiligence.com**) is a Cyber Risk Assessment and Data Breach Services company.

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. Starting in 2016, the QuietAudit® platform that our engineers use to conduct their in-depth cyber risk assessments can be licensed!

NetDiligence® is also an acknowledged leader in data and privacy breach prevention and recovery. Our eRiskHub® portal (www.eriskhub.com) is licensed by more than 50 cyber liability insurers to provide ongoing education and breach recovery services to their clients. NetDiligence technical experts assist many of these insurers with cyber liability claims investigations.

Last, but not least, NetDiligence is a champion of cyber education and awareness. In addition to this annual study, NetDiligence hosts Cyber Conferences annually in Philadelphia, Santa Monica and Toronto. We also publish a monthly newsletter that aggregates the media stories about cyber risk, privacy liability and related concerns, including regulatory enforcement, legal developments, international issues, data breach notifications, emerging attack vectors and industry research.

Cyber Risk Assessments

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.

NetDiligence offers a variety of 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.

QuietAudit®

Vendor Risk Management

NetDiligence's **QuietAudit Vendor Risk Management (VRM)** can help organizations "vet" the third-party vendors that manage their systems or handle their sensitive customer/patient data.

QuietAudit VRM is mobile-friendly and flexible. Organizations can choose from one of NetDiligence's standard security questionnaires or use their own customized questionnaire. The system automatically tallies responses, creating a scorecard for each vendor that can be benchmarked against industry standards. Responses are also retained, facilitating annual reviews that compare year-over-year responses to ensure that security safeguards are still in place.

Whether an organization has an existing VRM program that needs to be automated for greater ease, or is just starting a vendor review program, QuietAudit VRM streamlines the process of overseeing third-party vendors to ensure they are properly guarded against cyber incidents.

QuietAudit®

Underwriting Loss Control

Our QuietAudit® Underwriting Loss Control (ULC) module makes underwriting due-diligence and control verification more efficient. QuietAudit ULC helps insurers gather, assess and "score" a client's data security and privacy safeguards. Insurers can choose from one of NetDiligence's standard security questionnaires or use their own customized questionnaire. Standard surveys include: Cyber Risk (spirit of ISO); HIPAA Security Rule; NIST; California 20 Mandatory Controls; and Top 10 CVEs (Common Vulnerability Exposures).

The system automatically tallies responses, creating a scorecard for each client that can be benchmarked against industry standards. Responses are also retained, facilitating annual reviews prior to renewal.

QuietAudit ULC mobile-friendly and flexible, and can be branded for the licensing insurer.

eRiskHub®

The eRiskHub® is a licensed service that positions insurers and brokers to effectively assist clients with loss control. The eRiskHub cyber risk management web portal provides general information about sound security practices **before** a breach occurs, and facilitates appropriate reporting and recovery efforts **after** a breach. It provides tools and resources to help clients understand their exposures, establish response plans and minimize the effects of a breach on their organizations.

More than 50 insurers in global cyber liability insurance market license the eRiskHub portal to provide their clients with information and a suite of technical resources that can assist them in the prevention of IT and cyber losses and support them in the timely reporting and recovery of losses once an incident occurs.

BreachCoach®

NetDiligence's Breach Coach® Cyber Portal is a marketing and services platform for law firms. The portal is designed to help firms expand their Privacy & Data Security practices and provide risk management and breach recovery services to the firm's clients.

This Software-as-a-Service (SaaS) platform not only positions the firm to receive that critical first call following a breach event, it also provides a platform like no other to truly showcase all the areas of expertise the firm has to offer.

The portal can be fully branded for the firm, showcase their attorneys, and feature their proprietary intellectual property.

BreachPlan Connect™

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 an online "Build Your Plan" tool, plus Incident Logs and Incident Response Checklists that guide the organization in responding to a breach and ensuring their response follows the organization's approved plan. Breach Plan Connect can optionally include hotlinks to the insurer's eRiskHub® so the insured organization can easily access the insurer's preferred Breach Response Vendors, Risk Manager Tools, News Center, Learning Center, etc.

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 2013 and 2015
- The victimized organization had some form of cyber or privacy liability coverage

We sent requests for data to 88 individuals at 58 organizations, 12 of which organizations were in Canada. None of the Canadian organizations was able to provide data this year. 174 cases in the dataset represent claims from American organizations, and 1 case each represent claims from Canada and the UK. These data were provided by 20 individuals representing 19 organizations. This number of contributors is comparable to last year, when 20 organizations provided data.

Our 2016 Report summarizes findings from a sampling of 183 submissions: each one, a data breach insurance claim. After removing 1 duplicate case and 6 cases that were not truly cyber related (VISA Code 70 Chargebacks), we analyzed claims information for 176 events that fit our selection criteria. This number represents a 10% increase in the number of cases compared to last year.

One hundred sixty-three of these submissions involved the exposure of sensitive personal data in a variety of business sectors. Three business interruption claims did not involve the loss of sensitive information.

120 claims (68%) specified the number of records exposed and 161 claims (91%) 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 172 (98%) 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 is a small subset of all breaches. Some of our data points are lower than other studies because we focus on claim payouts 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.
- 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 $10 million.
- In statistical terms, our sample is a "convenience" sample, which means that we have taken the data we have been given and have described it. We cannot make any statements about "significance" or "non-significance".

It is important to note that many of the claims submitted for this study remain 'open', therefore aggregate costs as presented in this study represent "payouts 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.