NetDiligence®

CYBER CLAIMS STUDY 2014

INTRODUCTION

Introduction

The fourth annual NetDiligence® Cyber Claims Study uses actual cyber liability insurance reported claims to illuminate the real costs of incidents from an insurer's perspective.

For this study, we asked insurance underwriters about data breaches and the claim losses they sustained. We looked at the type of data exposed, the cause of loss, the business sector in which the incident occurred and the size of the affected organization. For the first time, this year we also looked at the two additional data points: was there insider involvement and was a third-party vendor responsible for the incident.

We then looked at the costs associated with Crisis Services (forensics, notification, legal counsel and miscellaneous other), Legal Damages (defense and settlement), Regulatory Action (defense and settlement) and PCI Fines.

This report summarizes our findings for a sampling of 117 data breach insurance claims, 111 of which involved the exposure of sensitive personal data in a variety of business sectors. The remaining six claims, which involved either business interruption or the theft of trade secrets, are discussed at the close of this report.

NOTE:
In 2015, we will be adding a new research database with anonymized data from all our claims studies to the eRisk Hub® for the exclusive use of eRisk Hub licensors and their clients. For more information about the eRisk Hub, contact Mark Greisiger at mark.greisiger@netdiligence.com.

KEY FINDINGS

PII was the most frequently exposed data (41% of breaches), followed by PHI (21%) and PCI (19%).

Hackers were the most frequent cause of loss (30%), followed by Staff Mistakes (14%).

Healthcare was the sector most frequently breached (23%), followed closely by Financial Services (22%).

Small-Revenue ($300M-$2B), Micro-Revenue ($50M-$300M) and Nano-Revenue (< $50M) companies experienced the most incidents (25%, 24% and 23% respectively).

Third parties accounted for 20% of the claims submitted.

There was insider involvement in 32% of the claims submitted.

The median number of records lost was 3,500. The average number of records lost was 2.4 million.

Non-zero claim payouts in this year's study ranged from $600 to almost $6.5 million. Typical claims, however, ranged from $30,000 to $400,000.

The median claim payout was $144,000. The average claim payout was $733,109. The average claim payout for a large company was $2.9 million, while the average payout in the Healthcare sector was $1.3 million.

The median per-record cost was $19.84. The average per-record cost was $956.21.

The median cost for Crisis Services (forensics, notification, legal guidance and miscellaneous other) was $110,594. The average cost for Crisis Services was $366,484.

The median cost for legal defense was $283,300. The average cost for legal defense was $698,797.

The median cost for legal settlement was $150,000. The average cost for legal settlement was $558,520.

The average claim payout was
$733,109.
The average claim payout for a large company was
$2.9 million,
while the average payout in the Healthcare sector was
$1.3 million.

The average cost per-record was
$956.21.

The average cost for Crisis Services was
$366,484.

The average cost for legal defense was
$698,797.

STUDY METHODOLOGY

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

- The incident occurred between 2011 and 2013
- The victimized organization had some form of cyber or privacy liability coverage
- A legitimate claim was filed in 2013

We received claims information for 117 events that fit our selection criteria. Of those, 91 claims (82%) specified the number of records exposed and 106 claims (95%) included a detailed breakout of what was paid out. Many of the events submitted for this year's study were recent, which means many claims are still being processed and actual costs have not yet been finalized.

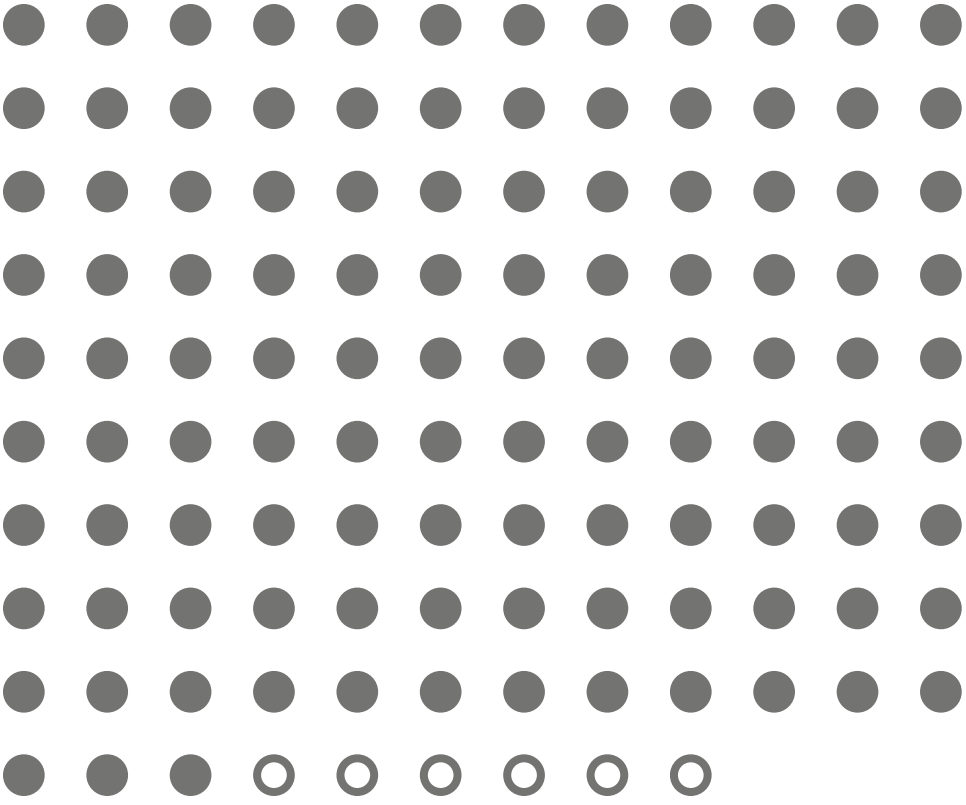
Readers should keep in mind the following:

- Our sampling is a small subset of all breaches. We estimate that our dataset represents 5-10% of the total number of cyber claims handled by all markets in 2013.
- 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 $1.5 million.

A LOOK AT THE OVERALL DATASET

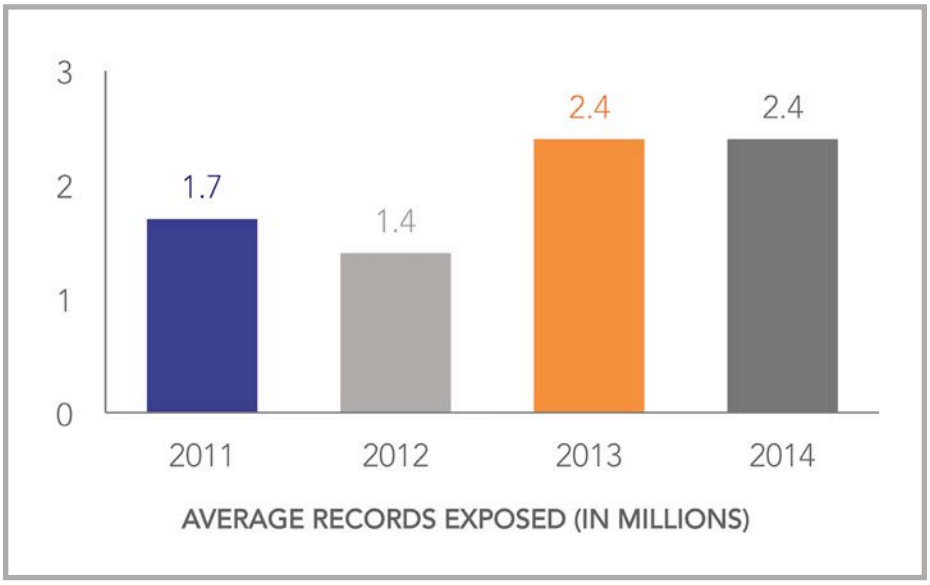
A Look at the Overall Dataset

There were 117 cyber claims submitted for this year's study. Of that number, 111 claims involved the loss, exposure or misuse of some type of personal sensitive data. The remaining 6 incidents involved business interruption losses or the theft of trade secrets. In this document, we are first going to explore the 111 claims that represent the exposure of sensitive data, after which we will briefly address the six business interruption and trade secret theft claims.



RECORDS EXPOSED

Of the 111 claims in the dataset, 91 (82%) reported the number of records exposed. The number of records exposed in a data breach claim ranged from 0 to 109,000,000. The average number of records exposed was 2,411,730.



The median number of records exposed was much smaller, coming in at 3,500. This continues a trend we saw in the past two years' studies. The median number of records exposed was 45,000 in our inaugural 2011 study, 29,000 in 2012 and a mere 1,000 in 2013. It is clear that more claims are being submitted for breaches with a relatively small number of records exposed.

COST PER RECORD

Of the 111 claims in the dataset, 70 (63%) reported both the number of records lost and the claim payout. The minimum cost per record was $0 and the maximum cost per record was $33,000.00. The average cost per record was $956.21, while the median cost was $19.84.

The average cost per-record was
$956.21.

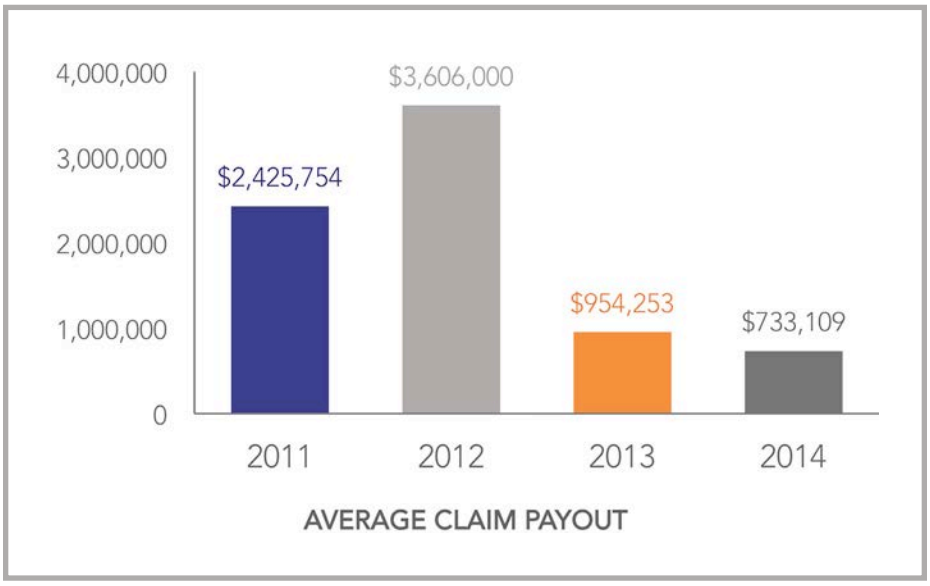
But we would like to emphasize that insurers should not feel comfortable estimating potential losses using any standard cost-per-record figure. There continues to be no meaningful correlation between the number of records exposed and the total payout for the claim. For example, in one incident in this year's dataset, only 80 were lost. However, the legal defense and settlement costs were quite high, resulting in a cost-per-record of more than $11,000.00. We think this is especially true in the Healthcare sector, where enforcement by State Attorneys General has been aggressive. Relatively small breaches can incur significant first-party costs for legal (Breach Coach®) guidance, forensic investigations, victim notification, credit monitoring, etc. For this reason, high per-record costs **are possible**, and both insurers and the organizations they cover should be aware of that.

Insurers should not feel comfortable estimating potential losses using any standard cost-per-record figure. There continues to be no meaningful correlation between the number of records exposed and the total payout for the claim.

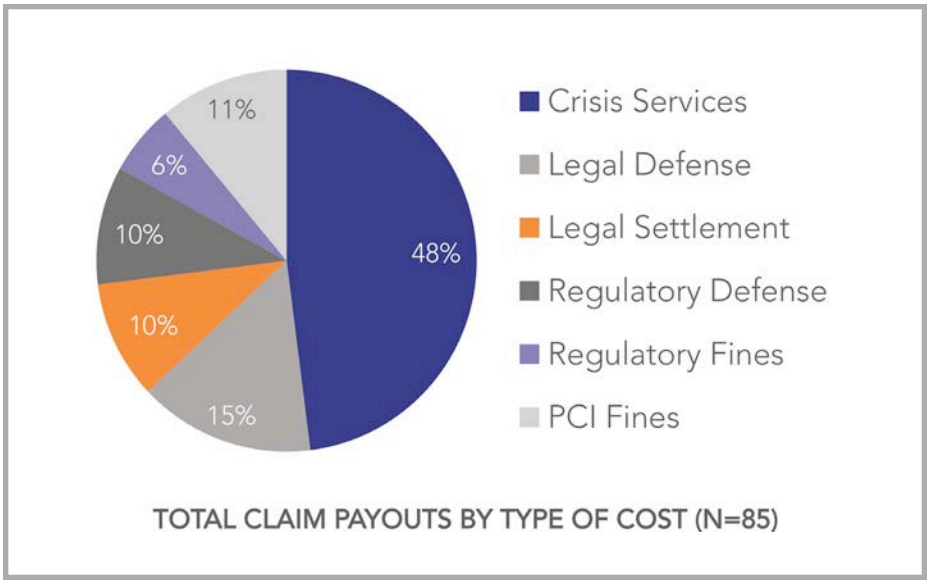
COSTS

Of the 111 claims submitted, 85 reported claims payouts. Total payout for all 85 claims was $62.3 million. The smallest claim payout was $1,000 while the largest claim payout was $13.7 million. The median payout was $144,000, while the average payout was $733,109. Note that the average payout decreased by 23% compared to last year's study.

Average payout was
$733,109.



Of the $62.3 million in total payouts, almost half (48%) was spent on Crisis Services, 15% on Legal Defense, 10% on Legal Settlements, 10% on Regulatory Defense, 6% on Regulatory Fines and 11% for PCI Fines.

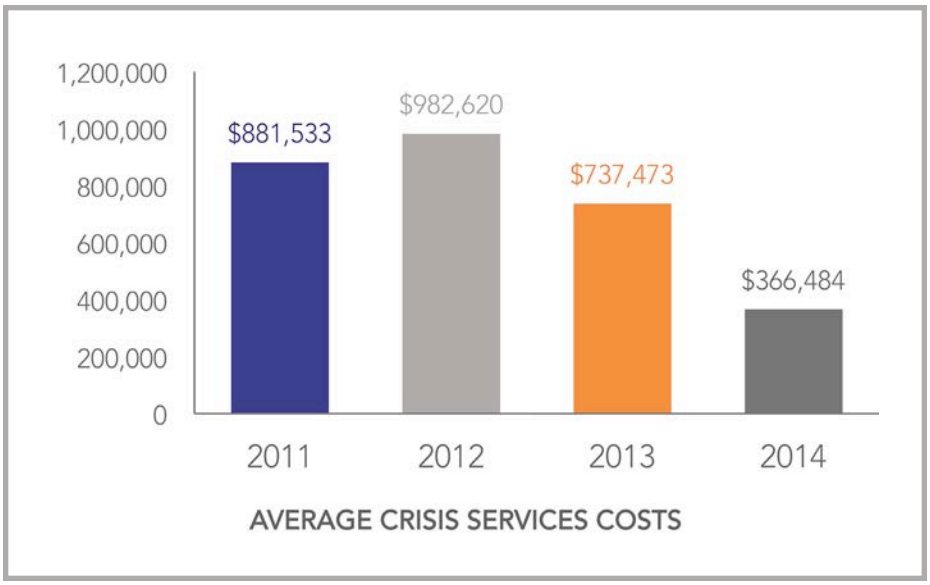


TOTAL CLAIM PAYOUTS BY TYPE OF COST (N=85)

CRISIS SERVICES COSTS

Of the 111 claims submitted this year, 80 included costs for one or more components of Crisis Services. The smallest (non-zero) payout for Crisis Services was $600, while the largest payout was $13.7 million. The average payout for Crisis Services was $366,484. The median payout was $95,000. Note that the average payout for crisis services decreased by 50% compared to last year's study.

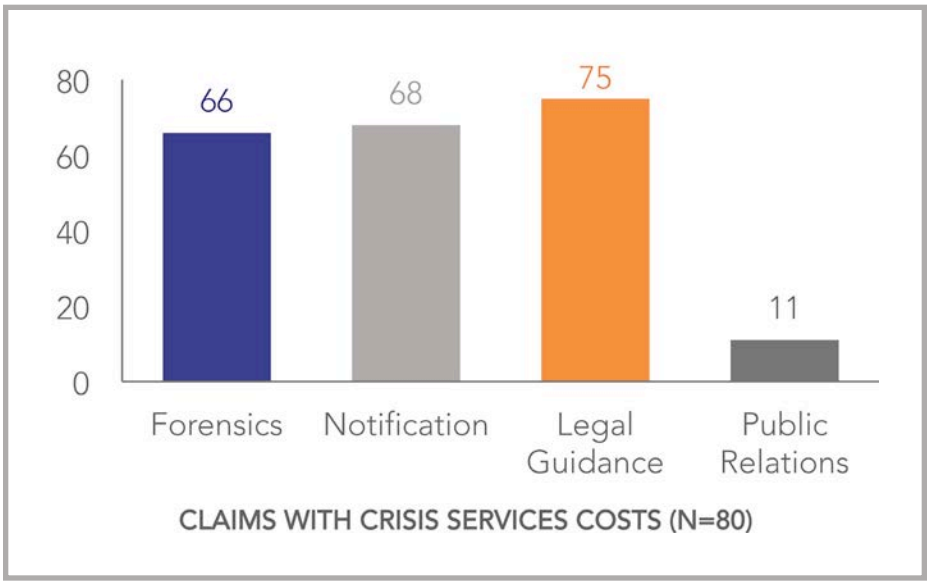
The average payout for Crisis Services was
$366,484.



AVERAGE CRISIS SERVICES COSTS

Once again, not all claims included payouts for all of the services that comprise Crisis Services. Of the 80 claims that reported payouts for individual components of Crisis Services (as opposed to reporting only the total payout for all Crisis Services combined), 66 (83%) included forensics, 68 (85%) included notification*, and 75 (94%) included legal guidance. These numbers reflect all claims that reported a dollar figure for a particular service, even if the dollar figure reported was zero. For the first time, a material number of claims in the dataset (11) included public relations costs.

A significant number of the claims submitted for the 2014 study reported a single amount for bundled services that included notification, call center, credit monitoring and ID restoration, rather than individual amounts for each service. For this reason, beginning this year we will also report the aggregate total for these services under a single category called "Notification."



CLAIMS WITH CRISIS SERVICES COSTS (N=80)

There was a wide range of costs for these services (see chart below). Forensics costs ranged from $0 to $1.5 million. Notification costs ranged from $0 to $6.15 million. Legal guidance (on complying with privacy and notification regulations) costs ranged from $0 to $2.5 million. Public Relations costs ranged from $0 to $135,000.

CRISIS SERVICES COSTS					
Service	Claims with Costs	Min	Median	Mean	Max
Forensics	66	0	38,500	119,278	1,500,000
Notification	68	0	10,839	175,147	6,150,000
Legal Guidance	75	0	38,000	117,613	2,500,000
Public Relations	11	0	0	4,513	135,000

LEGAL DAMAGES

Of the 111 claims submitted this year, only 13 (12%) included costs for legal damages. This number reflects all claims that reported a dollar figure for legal defense and/or settlement, even if the dollar figure reported was zero.

Like Crisis Services, the range of legal costs was extremely broad. Payouts for legal defense ranged from $7,805 to $4 million. Payouts for legal settlements ranged from $0 to $2.5 million.

LEGAL DAMAGES					
Expense	Claims with Costs	Min	Median	Mean	Max
Legal Defense	13	7,805	283,300	698,797	4,000,000
Legal Settlement	11	0	150,000	558,520	2,500,000

REGULATORY ACTION

Of the 111 claims submitted this year, only 6 (5%) included costs for regulatory actions, half of which were HIPAA related. This number reflects all claims that reported a dollar figure for regulatory defense and/or settlement, even if the dollar figure reported was zero.

As we've discovered in other cost categories, there was a wide range of regulatory costs. Payouts for regulatory defense ranged from $0 to $5 million. Payouts for regulatory settlements ranged from $0 to $2.5 million.

REGULATORY ACTION					
Expense	Claims with Costs	Min	Median	Mean	Max
Regulatory Defense	6	0	100,000	1,041,906	5,000,000
Regulatory Settlement	4	0	625,000	937,500	2,500,000

Whatever factors generate regulatory scrutiny for a given claim event, it appears that the number of records exposed is not necessarily a primary consideration. The claims that included regulatory costs in this year's study ranged from 80 records exposed to 35 million records exposed. For that reason, the potential for regulatory action and its associated costs should be considered when evaluating any organization's risk exposure, regardless of the size of the organization or the size of the breach.

PCI FINES

Of the 111 claims submitted this year, only 3 (3%) included costs for PCI fines. This sampling is too small to derive any meaningful insight into what is currently occurring with respect to PCI.

PCI FINES					
Expense	Claims with Costs	Min	Median	Mean	Max
Fines	3	11,000	75,000	2,328,667	6,900,000

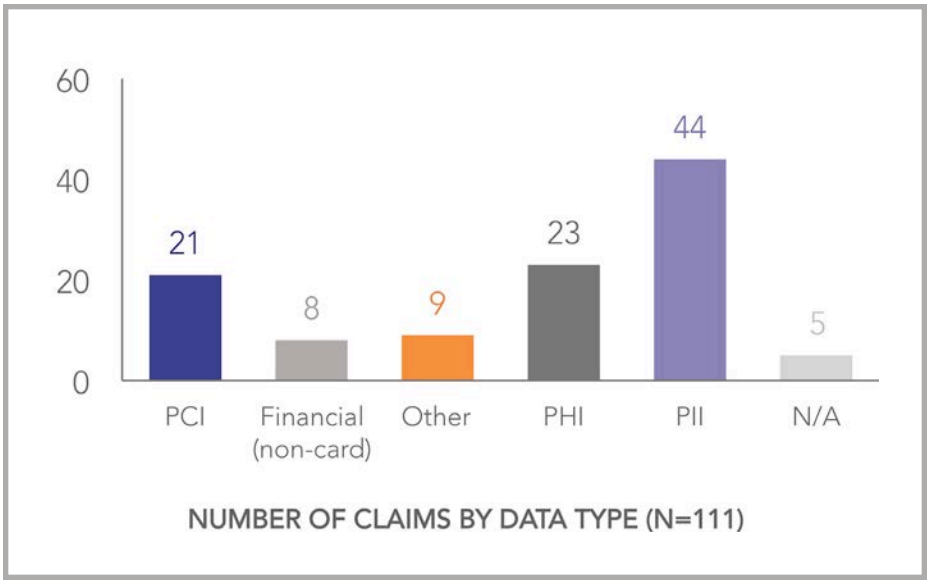
VIEWING THE DATA THROUGH DIFFERENT LENSES

Viewing the Data Through Different Lenses

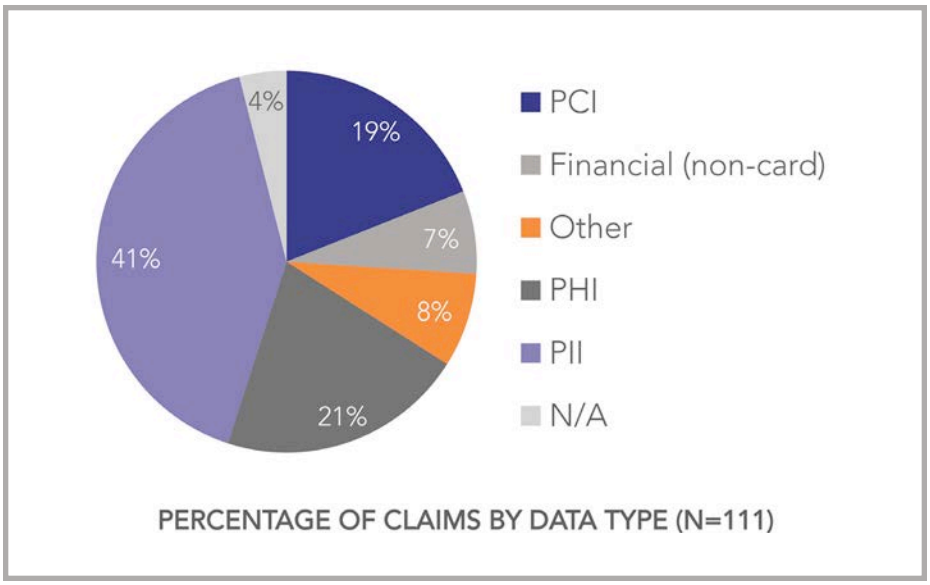
TYPE OF DATA EXPOSED

In this year's study, PII (personally identifiable information) was the runaway leader in type of data exposed, occurring in 44 claims submitted (41% of the dataset). PHI (private health information) was a distant second occurring in 23 claims (21%), followed closely by PCI (payment card information) in 21 claims (19%).

Non-card financial information was exposed in 8 of the claims (7%). Other data were exposed in 9 claims (8%). No sensitive data was exposed in 5 claims (4%).



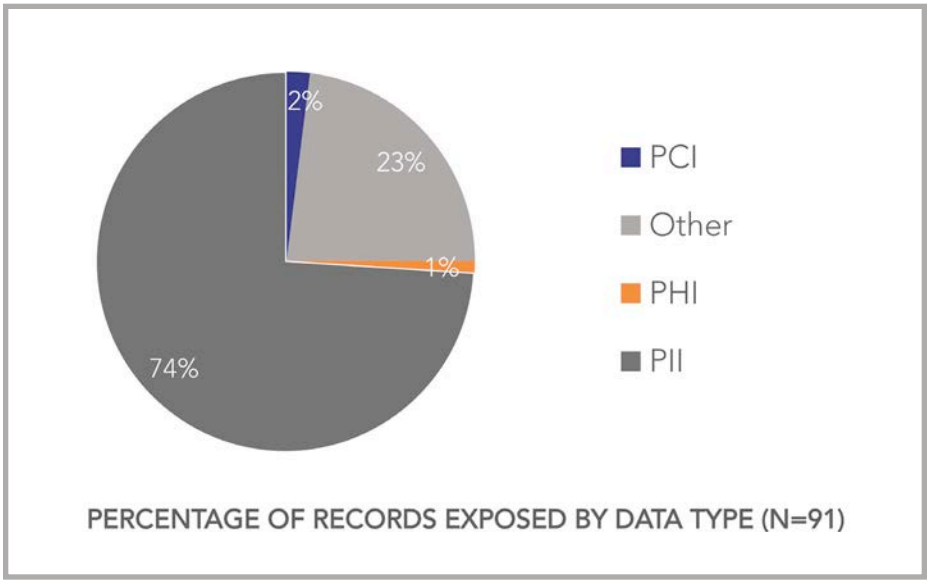
NUMBER OF CLAIMS BY DATA TYPE (N=111)



PERCENTAGE OF CLAIMS BY DATA TYPE (N=111)

RECORDS EXPOSED

Of the 111 claims in this year's dataset, 91 reported the number of records exposed. Of those 91 claims, PII was the most frequently exposed type of data.



PERCENTAGE OF RECORDS EXPOSED BY DATA TYPE (N=91)

It's important at this point to mention that the definition of PII is expanding. The "other data" exposed in this year's study were email addresses and passwords, which would be considered PII today. That means based on today's definition of PII, PII would account for fully 97% of data exposed.

Based on today's definition of PII, PII would account for fully 97% of data exposed.

RECORDS EXPOSED

Data Type	Claims with Records	Min	Median	Mean	Max
PCI	17	3	8,700	280,625	2,400,000
Financial (non-card)	7	3	4,000	13,739	40,000
Other	3	1	3,500	16,667,834	50,000,000
PHI	19	1	2,500	109,849	763,000
PII	44	1	4,109	3,693,409	109,000,000
N/A (no data exposed)	1	0	0	0	0
TOTAL	**91**				

COSTS

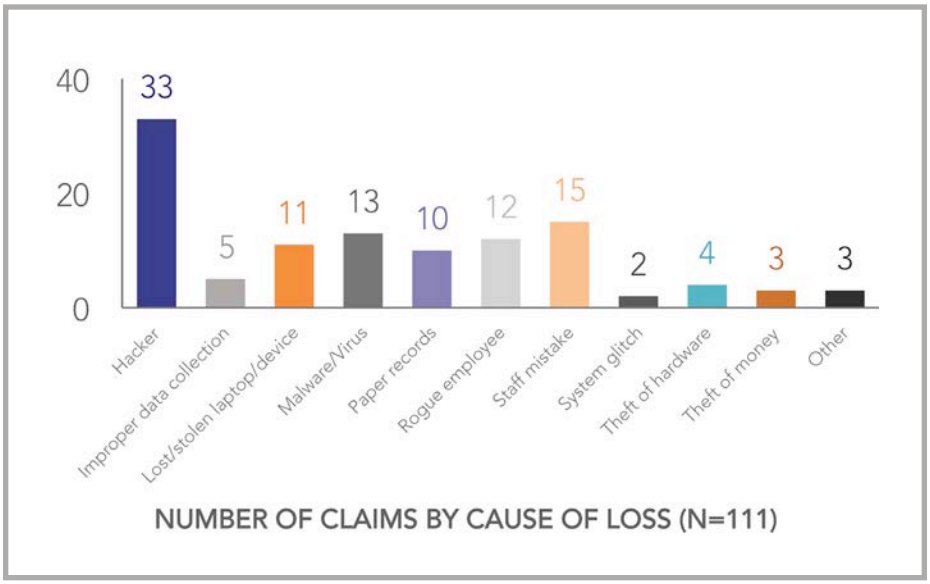
There were 81 claims in this year's dataset that included both the data type and the total payout amount. As we have seen in prior studies, there was a wide range of claim payouts for every data type, from a minimum of $1,000 up to $13.7 million. It should be noted that the median payout for PHI-related breaches was substantially higher than other data types; 41% higher than PCI and a whopping 66% higher than PII.

TOTAL COSTS (INCLUDING SIR)					
Data Type	Claims with Costs	Min	Median	Mean	Max
PCI	17	5,000	243,574	957,821	11,750,000
Financial (non-card)	6	1,000	118,234	115,165	248,000
Other*	7	7,500	53,100	154,181	775,669
PHI	14	2,500	414,000	1,461,795	13,700,000
PII	37	8,000	140,000	627,222	6,529,000
N/A	4	95,000	115,000	147,174	263,695
TOTAL	81				

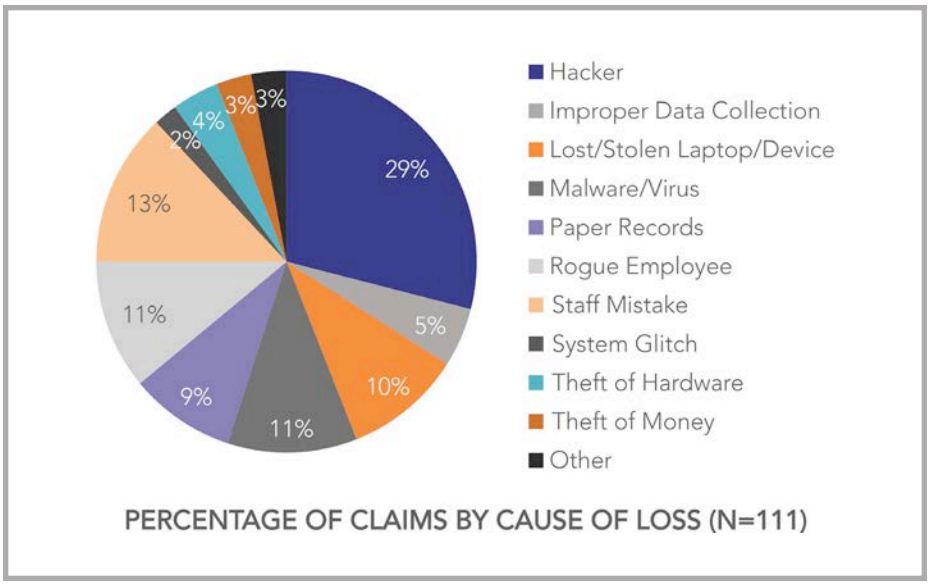
REMINDER:
The "other data" in this chart were email addresses and passwords, which would be considered PII today.

CAUSE OF LOSS

In this year's study, Hackers were the most frequent cause of loss, accounting for 33 claims (29% of the dataset). Staff Mistakes were a distant second, responsible for 15 claims (13%), followed closely by Malware/Virus with 13 claims (11%) and Rogue Employees with 12 claims (11%). Note that insiders (staff mistakes and rogue employees) accounted for a combined 27 claims, almost a quarter of the dataset (24%).



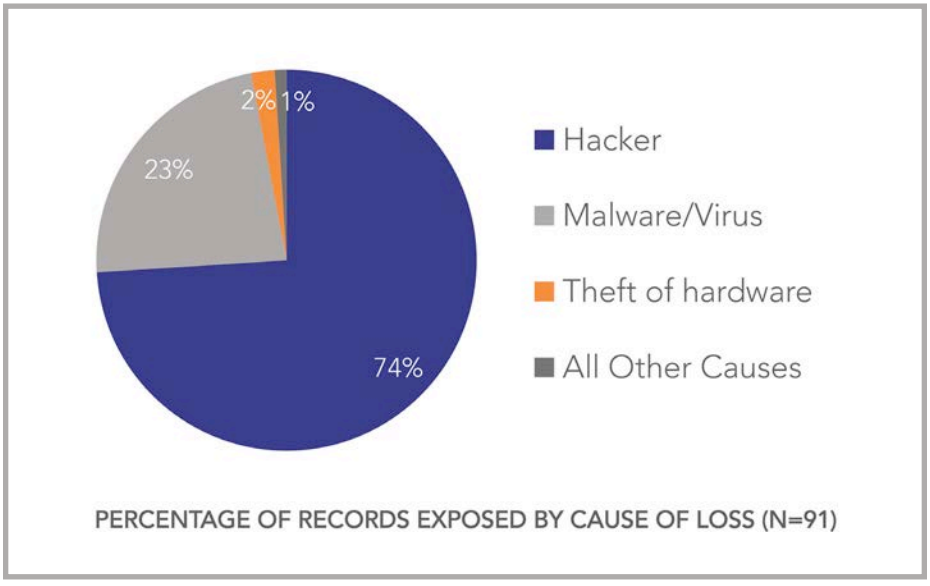
NUMBER OF CLAIMS BY CAUSE OF LOSS (N=111)



PERCENTAGE OF CLAIMS BY CAUSE OF LOSS (N=111)

RECORDS EXPOSED

Of the 111 claims in this year's dataset, 91 reported the number of records exposed. For those 91 claims, Hackers accounted for the vast majority of exposed data.



PERCENTAGE OF RECORDS EXPOSED BY CAUSE OF LOSS (N=91)

While Hackers accounted for only 29% of claim events, those incidents resulted 74% of records exposed. Malware/Virus accounted for only 11% of claim events, but 23% of records exposed. Since Hacker attacks often begin with the introduction of malware into the organization's network, it's instructive to look at the combined impact of these two causes of loss. Together, Hackers and Malware accounted for 40% of the claims in our dataset, and an eye-opening 97% of the records exposed.

Conversely, Theft of Hardware accounted for 4% of claim events, but only 2% of records exposed. All other causes combined accounted for the remaining 1% of data exposed.

Together, Hackers and Malware accounted for 40% of the claims in our dataset, and an eye-opening 97% of the records exposed.

RECORDS

Cause of Loss	Claims with Records	Min	Median	Mean	Max
Hacker	30	1	13,500	5,419,679	109,000,000
Improper Data Collection	3	1	50	33,805	101,363
Lost/Stolen Laptop/Device	8	100	2,033	14,703	80,000
Malware/Virus	11	0	16,000	4,624,231	50,000,000
Other	2	1,000	1,000	1,000	1,000
Paper Records	9	28	570	2,633	14,829
Rogue Employee	10	3	800	84,878	763,000
Staff Mistake	13	1	150	7,247	40,000
System Glitch	1	6,700	6,700	6,700	6,700
Theft of Hardware	4	100	408,000	1,204,025	4,000,000
TOTAL	**91**				

COSTS

There were 85 claims in this year's dataset that included both the cause of loss and the total payout amount.

TOTAL COSTS (INCLUDING SIR)

Cause of Loss	Claims with Costs	Min	Median	Mean	Max
Hacker	28	1,000	242,762	929,804	11,750,000
Improper Data Collection	5	7,500	55,000	285,008	1,294,538
Lost/Stolen Laptop/Device	8	2,500	158,916	1,850,483	13,700,000
Malware/Virus	12	40,854	164,125	338,394	1,845,000
Other	3	15,000	82,000	396,333	1,092,000
Paper Records	7	1,600	34,230	159,319	926,200
Rogue Employee	9	7,805	152,137	466,089	1,363,895
Staff Mistake	7	5,000	40,000	95,199	203,925
Theft of Hardware	4	125,000	891,000	2,109,000	6,529,000
Theft of Money	2	125,000	194,348	194,348	263,695
TOTAL	**85**				

When viewing the costs based on the cause of loss, we see some subtle distinctions.

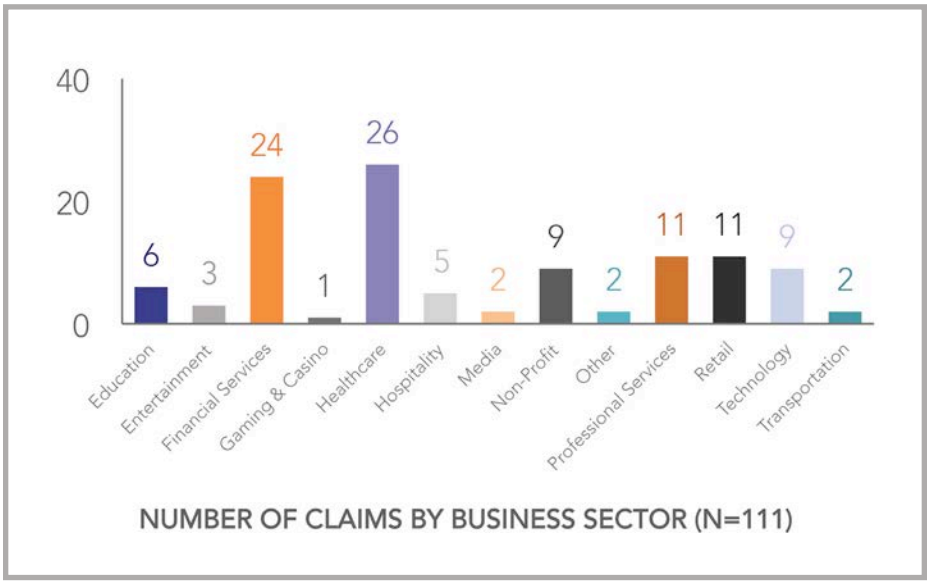
Incidents that were caused by improper actions or negligence on the part of the affected organization tended to result in slightly higher costs than incidents caused by simple errors, such as staff mistakes, or actions by a third-party provider.

The exception is theft of hardware and hacking incidents which, while not directly caused by the affected organization, were extremely expensive. This is probably attributable to the fact that theft of hardware and hacking incidents tend to expose a much larger number of records than do other types of incidents.

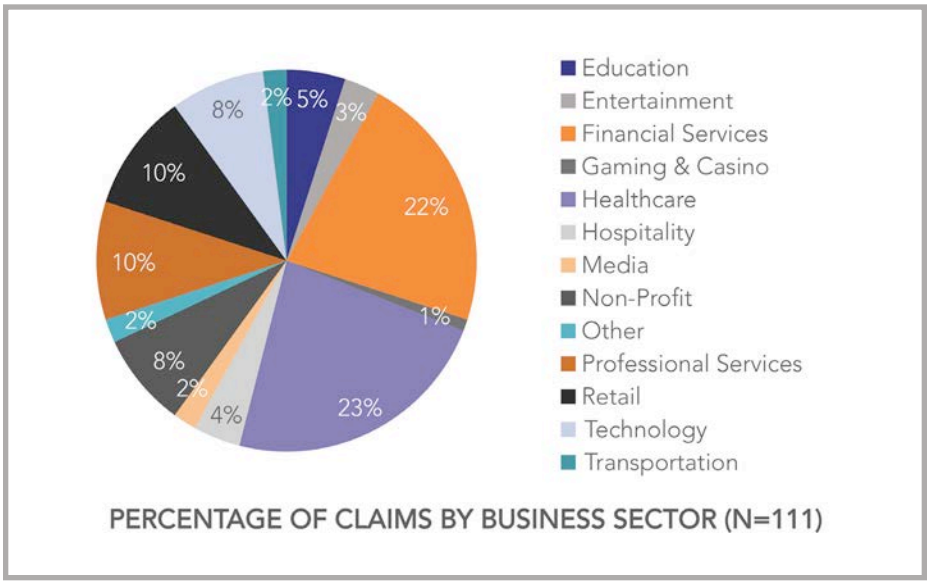
BUSINESS SECTOR

Again this year, Healthcare and Financial Services reported similar numbers of claim events—and those two sectors were far and away the most affected sectors. Healthcare led the way with 26 claims (22% of the dataset). Financial Services followed closely with 24 claims (22% of the dataset).

Retail and Professional Services tied for third, each with 11 claims (10%). Tied for fourth were Non-Profit and Technology, with 9 claims each (8%).



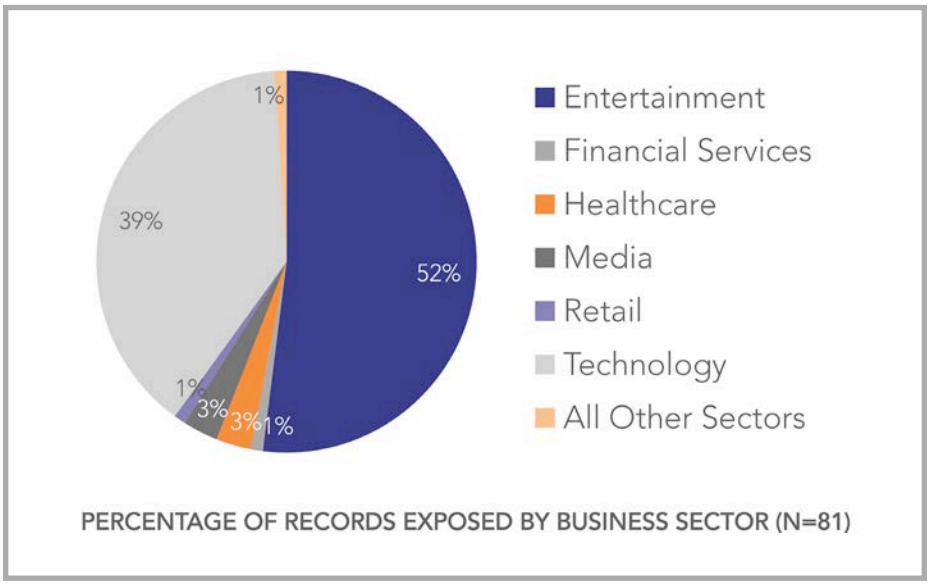
NUMBER OF CLAIMS BY BUSINESS SECTOR (N=111)



PERCENTAGE OF CLAIMS BY BUSINESS SECTOR (N=111)

RECORDS EXPOSED

There were 81 claims in this year's dataset that included both the business sector and the total payout amount.



PERCENTAGE OF RECORDS EXPOSED BY BUSINESS SECTOR (N=81)

Once again this year, the Entertainment sector accounted for the majority of records exposed (52%), although that sector was responsible for only 5% of the claims in our dataset. Technology came in second, accounting for 39% of records exposed. Despite the fact that Healthcare and Financial Services accounted for almost half the claims in our dataset, the number of records exposed was relatively minor, only 4% combined. Media accounted for another 3%, while all other sectors combined accounted for the remaining 1% of records exposed.

RECORDS					
Business Sector	Claims with Records	Min	Median	Mean	Max
Education	6	570	8,250	12,145	40,000
Entertainment	3	101,363	6,000,000	38,367,121	109,000,000
Financial Services	21	1	10,580	134,424	1,600,000
Healthcare	25	1	1,000	244,257	4,000,000
Hospitality	5	0	5	2,632	13,000
Media	1	7,000,000	7,000,000	7,000,000	7,000,000
Non-Profit	4	169	3,700	10,392	34,000
Other	2	3,000	41,500	41,500	80,000
Professional Services	8	9	2,270	88,706	450,000
Retail	8	28	9,350	310,547	2,400,000
Technology	6	1	12,675	14,170,895	50,000,000
Transportation	2	50	3,375	3,375	6,700
TOTAL	**91**				

COSTS

There were 85 claims in this year's dataset that included both the business sector affected and the total payout amount.

TOTAL COSTS (INCLUDING SIR)					
Business Sector	Claims with Costs	Min	Median	Mean	Max
Education	6	12,900	53,000	98,591	241,950
Entertainment	3	140,000	1,294,538	1,453,179	2,925,000
Financial Services	16	1,000	231,787	287,957	1,363,895
Gaming & Casino	1	144,000	144,000	144,000	144,000
Healthcare	19	2,500	152,137	1,381,421	13,700,000
Hospitality	5	5,000	14,212	99,203	364,000
Media	1	1,152,317	1,152,317	1,152,317	1,152,317
Non-Profit	6	15,000	110,000	141,339	398,000
Other	2	203,000	331,500	331,500	460,000
Professional Services	7	40,000	230,000	388,453	995,000
Retail	10	15,000	183,750	1,413,039	11,750,000
Technology	8	7,500	94,050	787,617	5,000,000
Transportation	1	55,000	55,000	55,000	55,000
TOTAL	**85**				

This year, large Hacker events in Entertainment, Media, Retail and Technology resulted in higher payouts for those sectors.

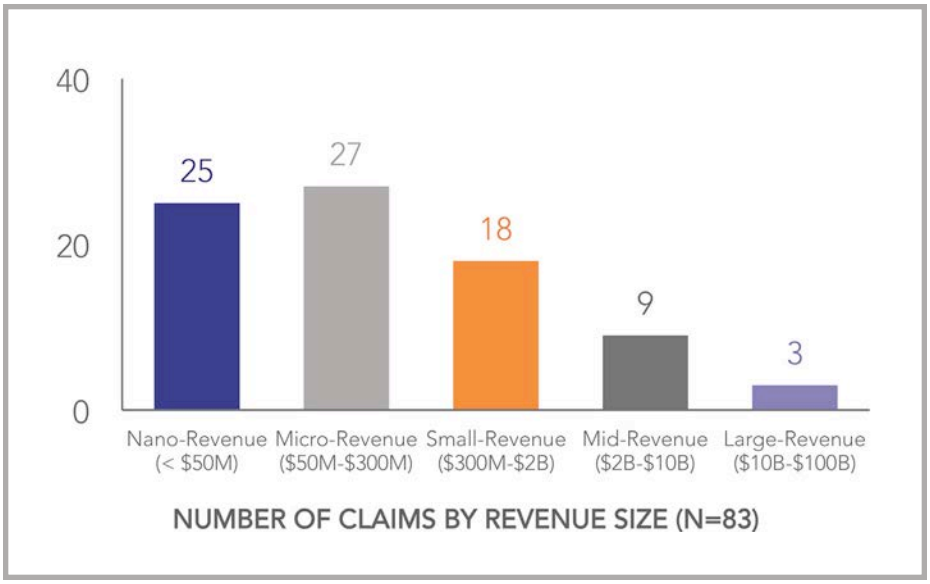
It is interesting to note that across all sectors, Crisis Services costs remained relatively consistent, which indicates that Crisis Services costs are driven more by size of breach and type of data than the business sector in which the event occurred. The same cannot be said of Legal and Regulatory costs, which were concentrated in the Entertainment, Healthcare and Retail sectors, and significantly impacted the costs in those sectors.

Across all sectors, Crisis Services costs remained relatively consistent. The same cannot be said of Legal and Regulatory costs.

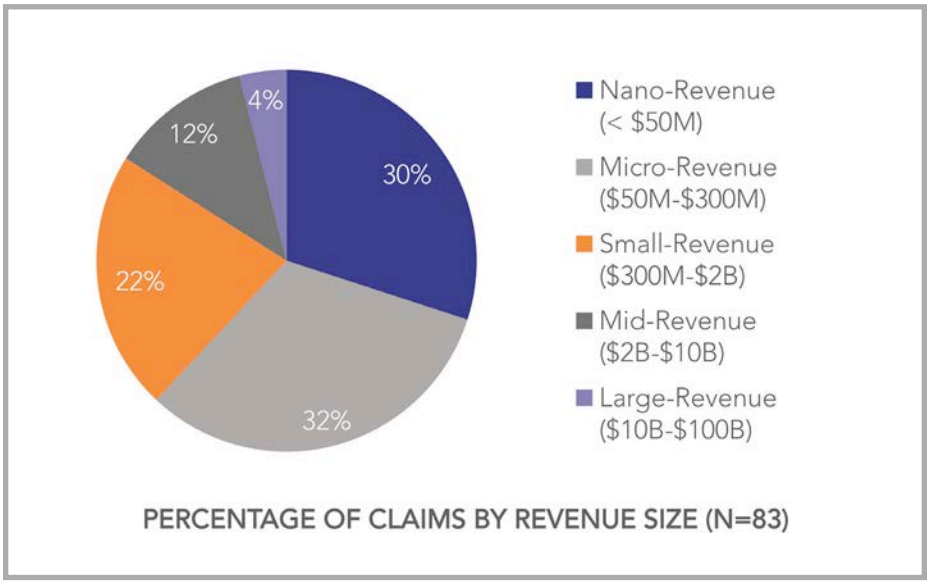
SIZE OF AFFECTED ORGANIZATION
(BASED ON REVENUE)

Again this year, revenue size was not reported for 25% of the claims submitted for the study. Of the 83 claims that reported the revenue size of the affected organization, Micro-Revenue organizations were the most impacted, accounting for 27 claims (33%). They were followed by Nano-Revenue, which accounted for 25 claims (30%), and Small-Revenue, which accounted for 18 claims (22%). Mid-Revenue organizations accounted for 9 claims (12%), while Large-Revenue organizations accounted for only 3 claims (4%). There were no claims for Mega-Revenue organizations.

This mirrors our findings from last year's study: smaller organizations experienced most of the incidents. We presume this is due to a variety of factors, including 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=83)



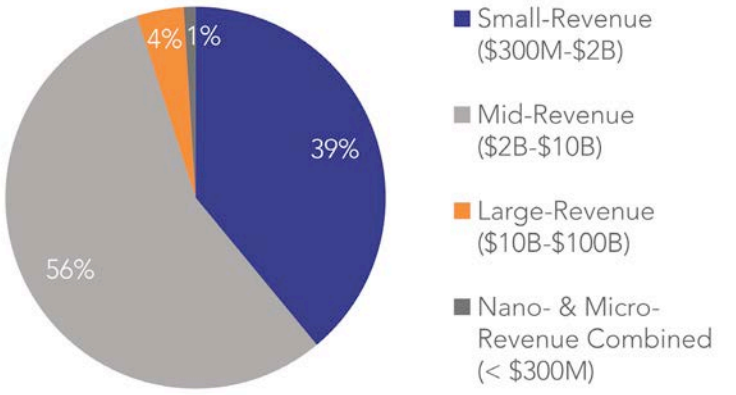
PERCENTAGE OF CLAIMS BY REVENUE SIZE (N=83)

RECORDS EXPOSED

While Nano- and Micro-Revenue organizations accounted for a combined 62% of the claims in our dataset, they were responsible for only 1% of records exposed. That falls in line with our expectations that smaller organizations are likely to have weaker security controls, but also that they typically store less data.

The converse is equally true. Mid- and Large-Revenue organizations accounted for only 16% of claims, but they were responsible for 60% of records exposed.

Falling between those extremes, Small-Revenue organizations accounted for 22% of claims, but 39% of records exposed.



PERCENTAGE OF RECORDS EXPOSED BY REVENUE SIZE (N=64)

RECORDS

Revenue Size	Claims with Records	Min	Median	Mean	Max
Nano-Revenue (< $50M)	19	1	100	9,170	101,363
Micro-Revenue ($50M-$300M)	19	3	2,400	21,488	250,000
Small-Revenue ($300M-$2B)	15	1	25,000	2,583,224	35,000,000
Mid-Revenue ($2B-$10B)	9	0	14,829	6,238,694	50,000,000
Large-Revenue ($10B-$100B)	2	116,000	2,058,000	2,058,000	4,000,000
TOTAL	**64**				

COSTS

As might be expected, overall payouts for breaches occurring in Large-Revenue organizations were higher than payouts for smaller organizations. The minimum payout for a Large-Revenue claim was more than $1 million, while the average payout was more than $6 million.

With this in mind, it was surprising that the two largest payouts ($13.7 and $11.7 million) in this year's dataset were to Small-Revenue organizations. What drove the costs up on both of these claims were legal and regulatory actions. Interestingly, these two events had virtually nothing in common. In one, a healthcare provider lost a device with a relatively modest number of PHI records (approximately 25,000). In the other, a hacker stole almost 2.5 million PCI records from a retailer. Nevertheless, in both cases, legal/regulatory defense and settlements were in the millions of dollars.

The two largest claim events had virtually nothing in common—one involved a small number of PHI records and the other a large number of PCI records—yet legal/regulatory costs for both were in the millions of dollars.

TOTAL COSTS (INCLUDING SIR)

Revenue Size	Claims with Costs	Min	Median	Mean	Max
Nano-Revenue (< $50M)	18	7,500	7,500	224,758	1,294,538
Micro-Revenue ($50M-$300M)	21	1,000	196,467	200,638	465,000
Small-Revenue ($300M-$2B)	16	2,500	237,000	2,086,469	13,700,000
Mid-Revenue ($2B-$10B)	9	30,962	203,000	688,355	2,925,000
Large-Revenue ($10B-$100B)	3	1,042,000	1,092,000	2,887,667	6,529,000
TOTAL	**67**				

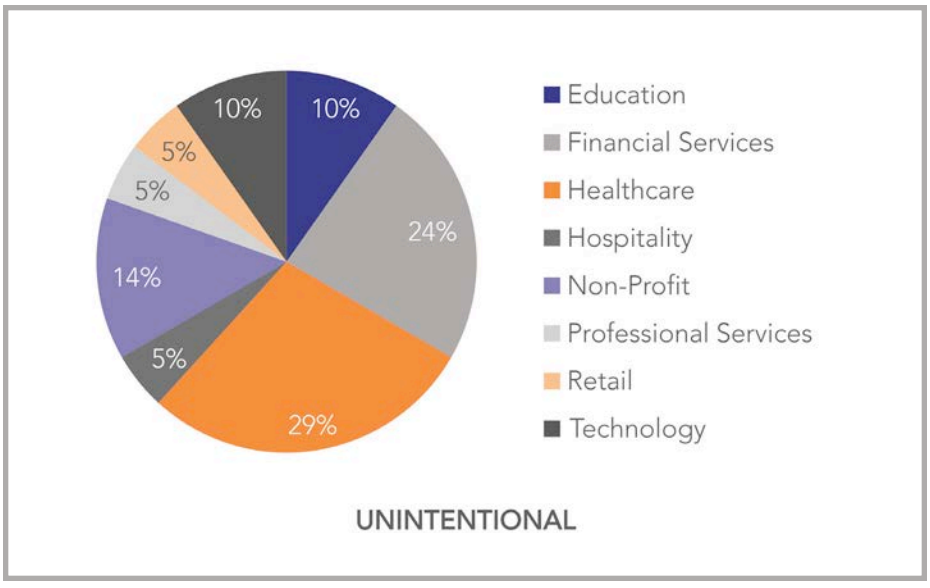
INSIDER INVOLVEMENT

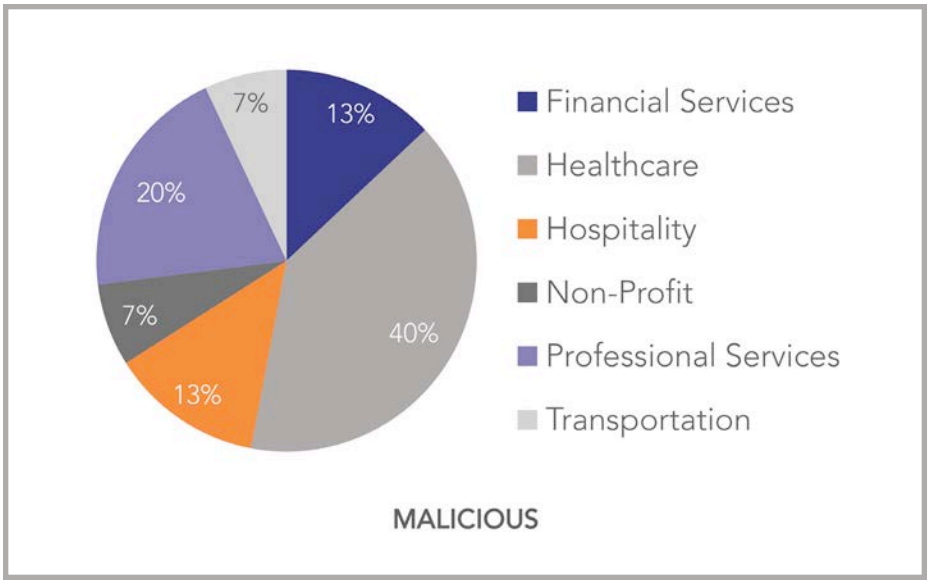
Insider Involvement

New this year, we asked insurers to tell us whether there was insider involvement in the claim events they submitted. Of the 111 events in our dataset, almost one third (32%) were attributable to insiders. More than half of those events (58%) were unintentional, caused primarily by staff mistakes. The rest were malicious in nature, 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. Of note, however, is that a disproportionate number of malicious insider incidents occurred in the Healthcare sector. While only 23% of the claims in our dataset occurred in Healthcare, that sector was responsible for 40% of malicious insider incidents.

A disproportionate number of malicious insider incidents occurred in the Healthcare sector.





Not surprisingly, malicious incidents tended to expose a larger number of sensitive records than did unintentional ones. Records exposed in malicious incidents were approximately double that of unintentional incidents.

RECORDS

Insider Involvement	Number of Claims	Min	Median	Mean	Max
Unintentional	18	1	375	30,020	405,000
Malicious	13	3	800	65,433	763,000
TOTAL	**31**				

The same holds true for costs. Despite the fact that the single largest payout for an insider claim event was caused by a staff mistake, overall, malicious incidents tended to result in much higher costs.

TOTAL COSTS (INCLUDING SIR)

Insider Involvement	Number of Claims	Min	Median	Mean	Max
Unintentional	21	0	1,600	137,778	1,745,000
Malicious	15	0	20,784	224,653	1,113,895
TOTAL	**36**				

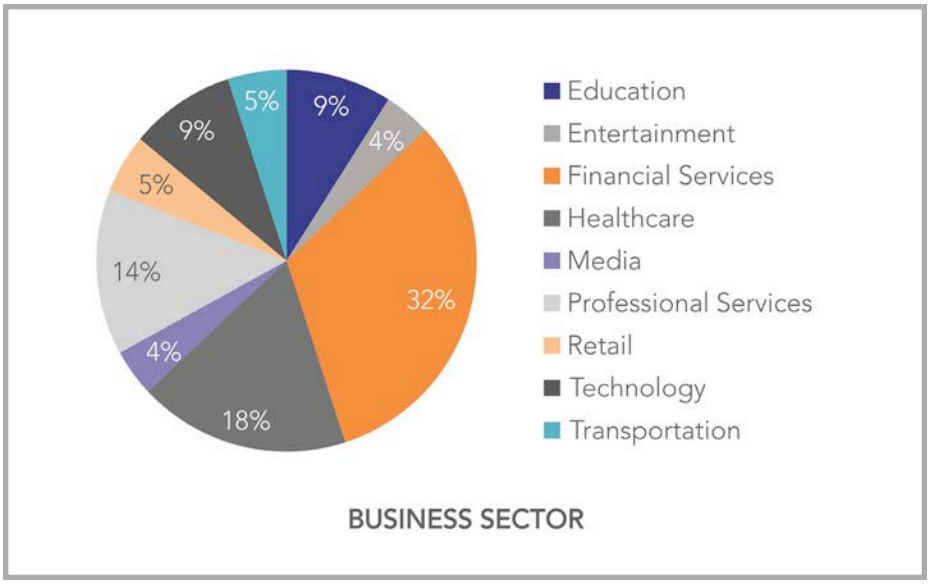
THIRD-PARTY BREACHES

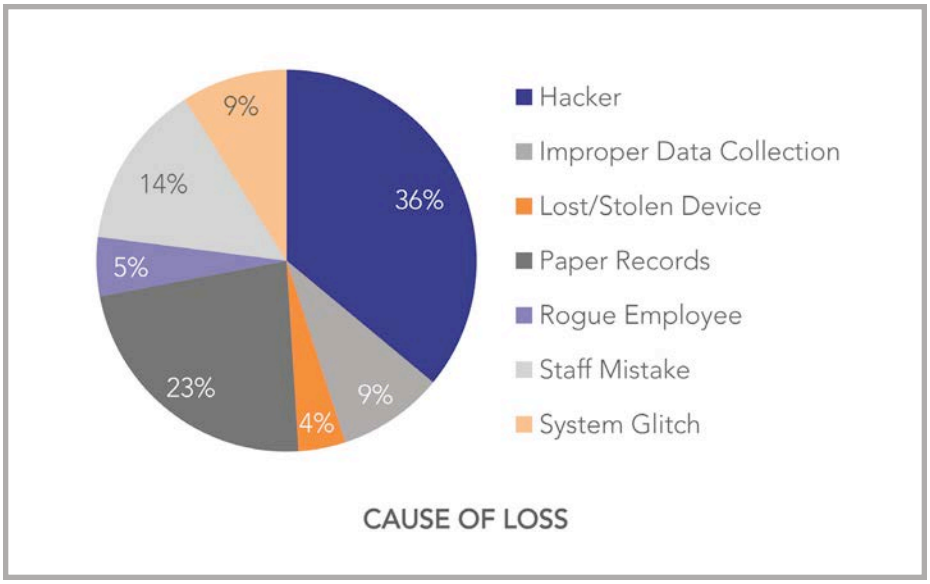
Third-Party Breaches

Also new this year, we asked insurers to indicate whether their claim events were caused by a third-party vendor. Of the 111 events in our dataset, 20% were attributable to third-parties.

Most organizations use third-party vendors, so third-party breaches occurred in virtually every business sector. However, we found that almost a third (32%) of third-party breaches occurred in Financial Services. We also found that the most common causes of loss in third-party breaches were Hackers (36%) and Paper Records (23%).

Of the 111 events in our dataset, 20% were caused by third-party vendors.





CAUSE OF LOSS

It is interesting that the third-party breach events in our dataset exposed significantly fewer records than breach events that occurred at the policyholder organization.

RECORDS

Third-Party Involvement	Number of Claims	Min	Median	Mean	Max
Yes	18	1	1,400	124,577	1,600,000
No	73	0	4,000	2,975,685	109,000,000
TOTAL	**91**				

Perhaps because the third-party breach events were smaller, payouts for third-party events were also smaller. Overall, payouts for third-party breaches were just a fraction (17% to 26%) of the payouts for in-house breaches.

TOTAL COSTS (INCLUDING SIR)

Third-Party Involvement	Number of Claims	Min	Median	Mean	Max
Yes	19	0	12,900	154,582	1,279,538
No	87	0	75,000	585,403	13,700,000
TOTAL	**106**				

ABOUT FIRST-PARTY LOSSES

About First-Party Losses

Many (if not 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 six such incidents—three involving business interruption and three involving theft of trade secrets.

All three business interruption incidents were caused by distributed denial of service (DDoS) attacks. One incident occurred in the Financial Services sector, one in Technology and one in Media. The DDoS attack in Financial Services was stopped before data was exposed or money stolen, so there was no reported payout for that claim. However, the other two claims resulted in sizable payouts (ranging from $1.5 to $5 million) for lost business income, recovery expenses and legal defense.

Not surprisingly, all three incidents that involved the theft of trade secrets occurred in the Technology sector and were caused by hackers. Payouts ranged from $150,000 to $900,000, primarily for forensics.

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

- 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 appoximately $4 million.

CONCLUSION

Conclusion

Our objective for this study is to help risk management professionals and insurance underwriters 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 first time since we began this study, however, we received fewer claims from fewer insurers than we did the preceding year. In our inaugural study (conducted in 2011), our sampling included 117 claims, our 2012 study included 137 claims and our 2013 study included 145 claims. This year, we took a step backward, with only 117 claims in our dataset.

Despite this year's smaller dataset, we continue to see growing interest in these types of studies within the insurance industry. 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 significant 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:

ACE
AIG
Ascent Underwriting
Beazley
Chubb Group of Insurance Companies
CUNA Mutual Group
Freedom Specialty Insurance
Lockton
Hylant
Liberty International Underwriters
Marsh
OneBeacon Professional Insurance
Philadelphia Insurance Companies
Travelers
XL Group
Zurich NA

CONTRIBUTOR

Risk Centric Security, Inc.
Risk Analysis for the 21st Century®

A special thank you also goes to 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. Risk Centric Security offers state-of-the-art SaaS tools and training for quantitative risk and decision analysis. For more information, visit riskcentricsecurity.com.

SPONSORS

AllClear ID is the technology, cost savings, and customer service leader in the data breach response market. We have notified over 160 million consumers on behalf of Fortune 1000 companies, top healthcare organizations, government agencies, and universities. The AllClear Breach Response provides a better experience for affected individuals, significantly reduces response costs, and helps retain customers after a breach. We were named "Best in Resolution" by Javelin Strategy & Research, have won 15 international awards for outstanding customer service, and our customer support team maintains a 97% customer satisfaction rating.

For more information, visit us at:
ALLCLEARID.COM

ICSA Labs, an independent division of Verizon, has been providing credible, independent, third-party product assurance for end-users and enterprises since 1989. ICSA Labs provides accredited testing and certification of security and health IT products, as well as network-connected devices, to measure product compliance, reliability and performance for the world's top technology and Health IT vendors.

For more information, visit us at:
ICSALABS.COM

McGladrey is a leading provider of professional services focused on the middle market, with more than 7,000 people across 75 U.S. cities and 32,000 people in over 110 countries. McGladrey's experienced global cybersecurity advisors provide a wide range of solutions to help clients identify and mitigate risks including: IT risk assessments, incident response plan development and exercises, network vulnerability testing and PCI compliance. Our experienced Security and Privacy Consulting team specializes in a number of areas including incident response for data breach/data privacy incidents and digital forensic investigations.

For more information, visit us at:
MCGLADREY.COM

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.

NetDiligence is also an acknowledged leader in data and privacy breach prevention and recovery. Our eRisk Hub® 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.

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.

NetDiligence's QuietAudit Cyber Risk Assessments give organizations a 360 degree view of their people, processes and technology, so they can:

- Reaffirm that reasonable practices are in place
- Harden and improve their data security
- Qualify for network liability and privacy insurance
- Bolster their defense posture in the event of class action lawsuits

NetDiligence 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 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.

Cyber Health Check for Healthcare Providers

NetDiligence conducts its Cyber Health Check assessment of the healthcare provider's data security strengths and weaknesses with a special focus on the data security standards mandated by HIPAA/HITECH.

Cyber Health Check for Retailers

NetDiligence conducts its Cyber Health Check assessment of the retailer's data security strengths and weaknesses with a special focus on PCI gaps and Point-of-Sale (POS) security.

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.

eRiskHub®

The eRisk Hub® is a licensed service that positions insurers and brokers to effectively assist clients with loss control. The eRisk Hub 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 eRisk Hub 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.

Key Features of the eRisk Hub Portal

- Incident Roadmap – includes suggested steps to take following a network or data breach incident, free consultation with a Breach Coach® and access to the insurer's preferred breach response team
- News Center – cyber risk stories, security and compliance blogs, security news, risk management events and helpful industry links
- Learning Center – best-practices articles, white papers and webinars from leading technical and legal practitioners
- Risk Manager Tools – tools to help organizations manage their cyber risk including free online self-assessment tools (excerpted from NetDiligence's QuietAudit system), recap of state breach notification laws, vendor management tools, downloadable policy templates and much more
- eRisk Resources – a directory of third-party vendors with expertise in pre- and post-breach disciplines

When a breach event occurs, time is of the essence. With a good response plan in place and access to highly skilled third-party resources, a victimized organization can more efficiently and cost-effectively respond to and recover from a data breach.

The eRisk Hub portal is an effective way for insurers and brokers to help their clients combat cyber losses with minimal, controlled and predictable costs.

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.