NetDiligence® 2013

Cyber Liability & Data Breach Insurance Claims

A Study of Actual Claim Payouts

Authored by:

Mark Greisiger

Sponsored by:

AllClear ID

Faruki Ireland & Cox PLL

Kivu Consulting

NetDiligence®
Cyber Risk Assessment & Data Breach Services

Introduction

The third annual NetDiligence® *Cyber Liability & Data Breach Insurance Claims* study uses actual cyber liability insurance reported claims to illuminate the real costs of incidents from an insurer's perspective. It is our hope that actuaries, risk managers and others working in the field of data security will use this information to properly price policies, perform more accurate risk assessments and implement better safeguards and action plans to protect organizations from data breaches.

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 and the business sector in which the incident occurred. For the first time, this year we also looked at the size of the affected organization. We then looked at the costs associated with Crisis Services (forensics, notification, credit monitoring, and legal counsel), Legal (defense and settlement), and Fines (PCI & regulatory).

This report summarizes our findings for a sampling of 145 data breach insurance claims, 140 of which involved the exposure of sensitive data in a variety of sectors, including government, healthcare, hospitality, financial services, professional services, retail and many more.

> ***Note**: We will be publishing additional Detailed Findings in November 2013 exclusively in the eRisk Hub® for the benefit 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 (28.7% of breaches), followed closely by PHI (27.2% of breaches).
- Lost/Stolen Laptop/Devices were the most frequent cause of loss (20.7%), followed by Hackers (18.6%).
- Healthcare was the sector most frequently breached (29.3%), followed by Financial Services (15.0%).
- Small-Cap ($300M-$2B) and Nano-cap (< $50M) companies experienced the most incidents (22.9% and 22.1% respectively). Mega-Cap (> $100B) companies lost the most records (45.6%).

- The median number of records lost was 1,000. The average number of records lost was 2.3 million.
- Claims submitted for this study ranged from $2,500 to $20 million. Typical claims, however, ranged from $25,000 to $400,000.
- The median claim payout was $242,500. The average claim payout was $954,253. However, many claims in our dataset have not yet been paid. *If we assume that, at a minimum, the SIR will be met, the median claim payout would be $250,000 while average claim payout would be $3.5 million.*
- The median per-record cost was $107.14. The average per-record cost was $6,790. *However, if we exclude outliers (incidents with a low number of records exposed but extremely high payouts), the median per-record cost was $97 and the average per-record cost was $307.*
- The median cost for Crisis Services (forensics, notification, credit monitoring and legal guidance) was $209,625. The average cost for Crisis Services was $737,473.
- The median cost for legal defense was $7,500. The average cost for legal defense was $574,984.
- The median cost for legal settlement was $22,500. The average cost for legal settlement was $258,099.

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 2010 and 2012
- The victimized organization had some form of cyber or privacy liability coverage
- A legitimate claim was filed

We received claims information for 140 events that fit our selection criteria. Of those, 93 claims specified the number of records exposed and 88 claims included a detailed breakout of what was paid out. Many of the events submitted for this year's study were recent, which means the claims are still being processed and actual costs have not yet been determined.

Readers should keep in mind the following:

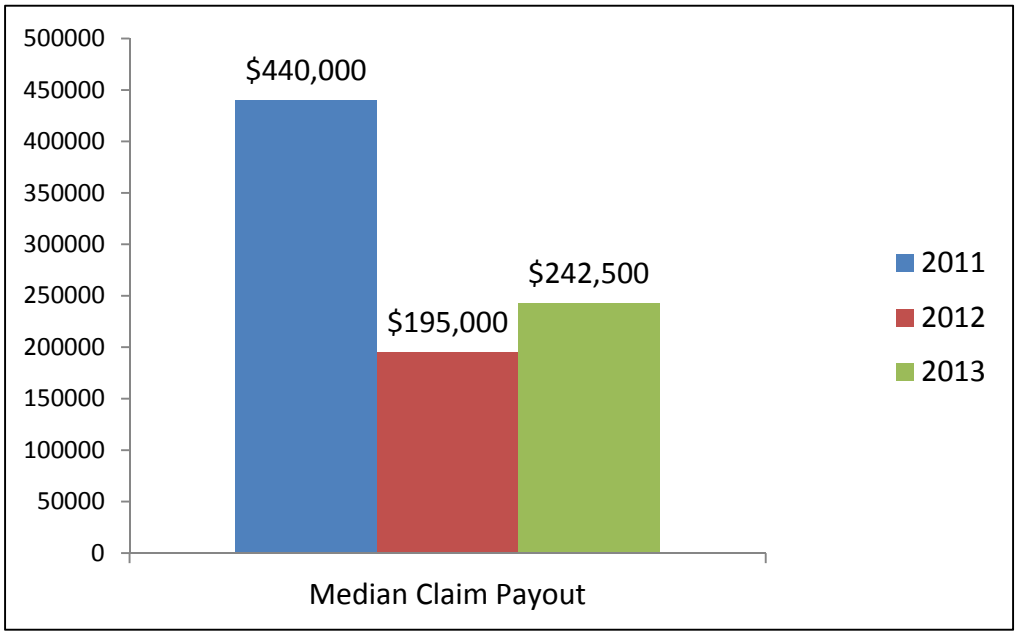
- Our sampling is a small subset of all breaches
- Our numbers are lower than other studies because we focus on claim payouts for specific breach-related expenses and do not factor in other financial impacts of a breach, including investigation and administration expenses, customer defections, opportunity 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 $100 million.

A Look at the Overall Dataset

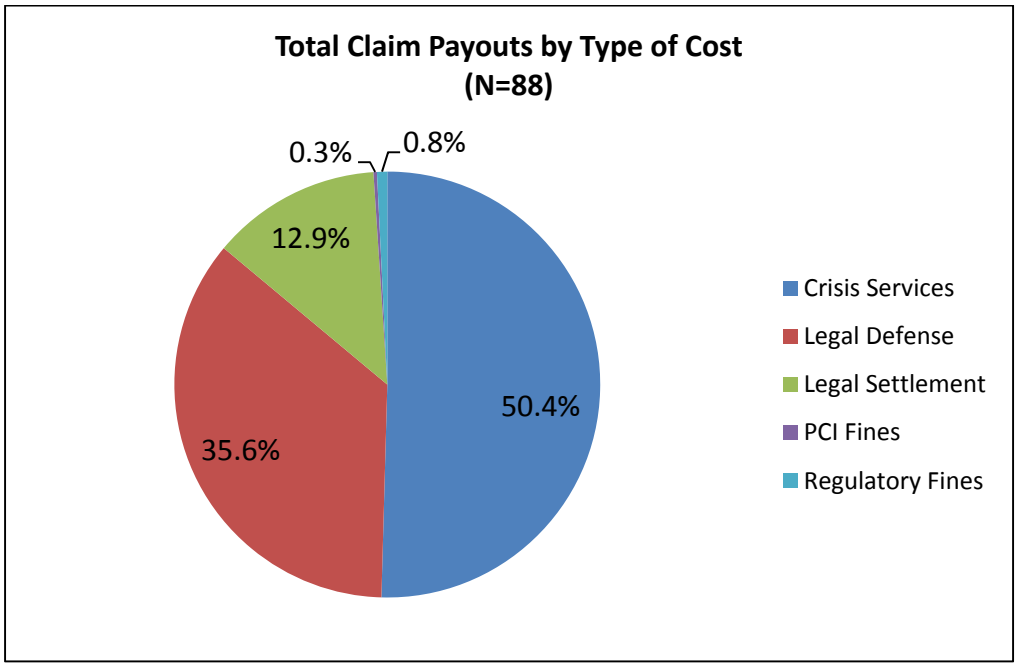
There were 145 cyber claims submitted for this year's study. Of that number, 140 claims involved the loss, exposure or misuse of some type of sensitive data. The remaining 5 incidents involved business interruption losses. In this document, we are first going to explore the 140 claims that represent the exposure of sensitive data, after which we will briefly address the 5 business interruption claims.

Costs

Of the 140 claims submitted, 88 reported claims payouts. Total payout for all 88 claims was $84 million. The smallest claim payout was $2,560 while the largest claim payout was $20 million. The mean payout was close to $1 million ($954,253), while the median payout was just under a quarter of a million dollars ($242,500). That represents a *25% increase* over the median cost per claim in last year's study.

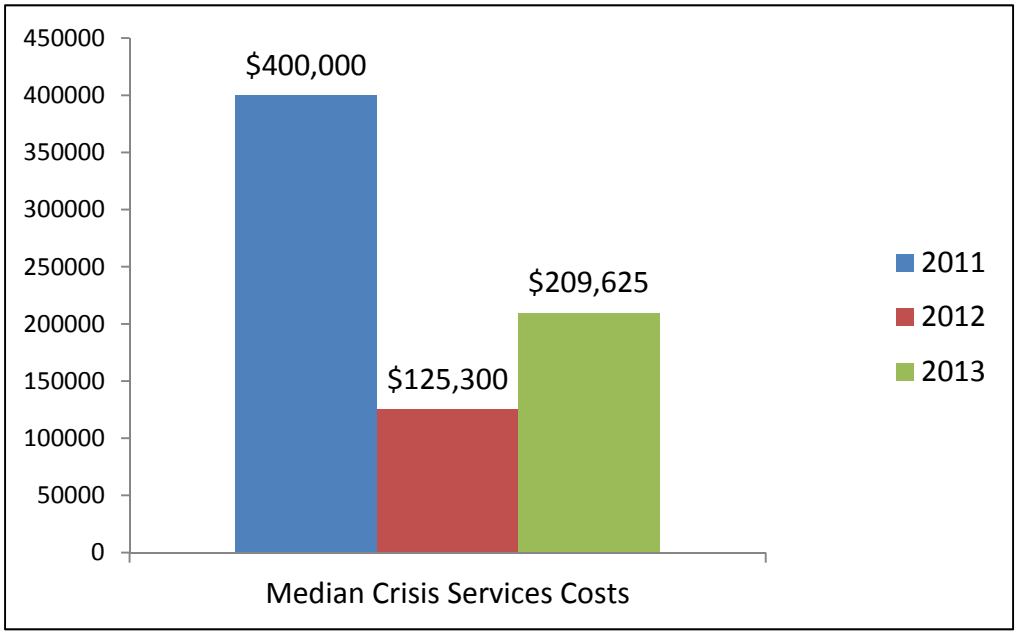


Of the $84 million in total payouts, approximately half (50.4%) was spent on Crisis Services, 35.6% on Legal Defense, 12.9% on Legal Settlements and less than 1% each for PCI and Regulatory Fines.

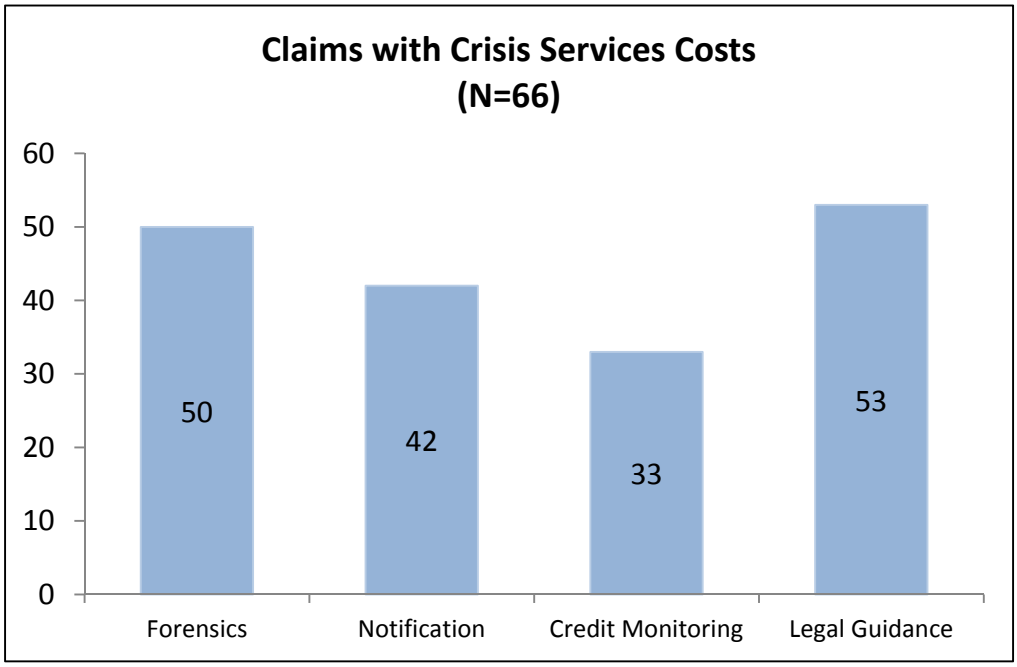


Crisis Services Costs

Of the 140 claims submitted this year, 66 included costs for one or more components of Crisis Services. The smallest payout for Crisis Services was $2,560, while the largest payout was $11.5 million. The average payout was $737,473. The median payout was $209,625.



Of course, not all claims included payouts for all four of the services that comprise Crisis Services. Of the 66 claims that reported payouts for individual components of Crisis Services (as opposed to reporting only the total paid for Crisis Services), 50 (75.8%) included forensics, 42 (63.6%) included notification, 33 (50.0%) included credit monitoring and/or identity theft remediation, and 53 (80.3%) 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.



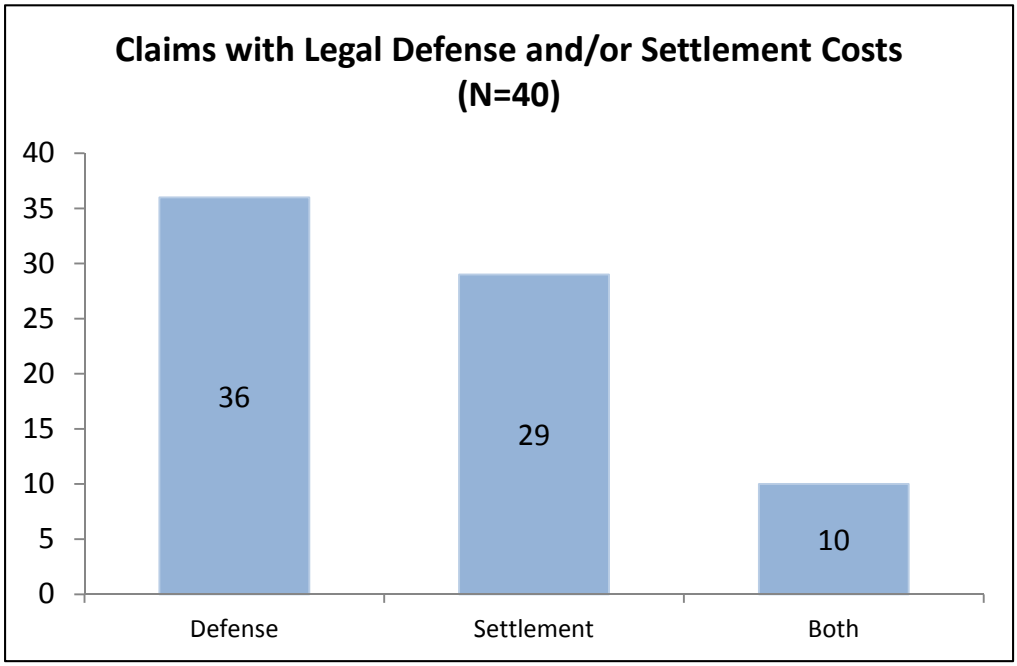
There was a wide range of costs for these services (see chart below). Forensics costs ranged from $0 to $1 million. Notification costs ranged from $0 to $3 million. Credit monitoring and identity theft remediation costs ranged from $0 to $935,000. Legal guidance (on complying with privacy and notification regulations) costs ranged from $0 to $150,000.

Crisis Services Costs

Service	Claims with Costs	Min	Median	Mean	Max
Forensics	50	0	10,000	104,740	1,000,000
Notification	42	0	14,636	126,703	3,000,000
Credit/ID Theft Monitoring	33	0	2,060	55,865	935,000
Legal Guidance	53	0	12,000	29,225	150,000

Legal Defense and Settlement Costs

Of the 140 claims submitted this year, 40 (28.6%) included costs for legal defense, legal settlement or both. 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 $0 to $10 million. Payouts for legal settlements ranged from $0 to $4 million.

Legal Defense Costs

Legal	Claims with Costs	Min	Median	Mean	Max
Defense	20	0	7,500	574,984	10,000,000
Settlement	16	0	22,500	258,099	4,000,000

Regulatory and PCI Fines

Of the 88 claims that reported payouts, 7 (3.4%) included PCI fines. These fines ranged from $11,000 to $120,000. The median PCI fine was $20,000 and the mean was $50,000. Two of these incidents occurred in the hospitality industry (restaurants) and were caused by hackers—one at a mid-cap company and the other at a micro-cap. The third incident occurred at a small-cap organization in the education sector and involved the hacking of a point-of-sale (POS) device.

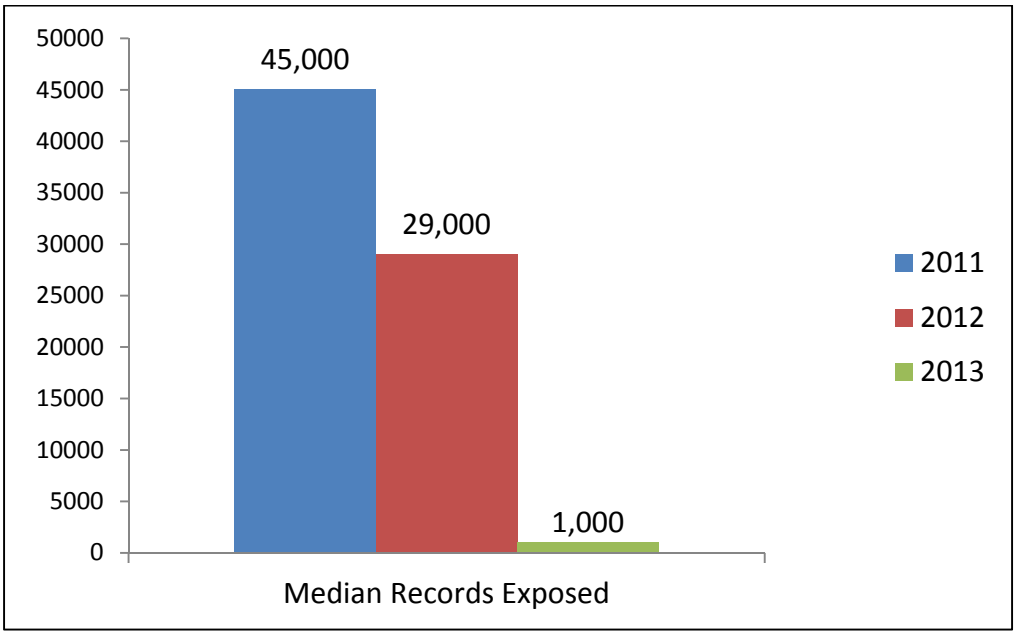
Payouts for regulatory fines were reported for 4 (4.5%) claims. All 4 incidents involved the loss of PHI and all 4 fines were the same, $150,000. One incident occurred in a nano-cap company in the healthcare sector—the loss caused by improper handling of paper records. The other three incidents occurred at non-profits, two caused by malware/virus and one by the improper handling of paper records.

All of these incidents were small (200 records or less). So it appears that the potential for fines should be included when evaluating any organization's risk exposure, regardless of the size of the organization or the size of the breach.

Records Exposed

Of the 140 claims submitted, 93 reported the number of records exposed. The number of records exposed ranged from 1 to 109,000,000. The mean number of records exposed was 2,360,642, while the median was much smaller, coming in at 1,000.

The median number of records exposed in this year's study (1,000) is dramatically smaller than prior years. That continues a trend we saw in last year's study, that more claims are being submitted for breaches with a relatively small number of records exposed.



Cost per Record

Of the 140 claims submitted, 63 reported both the number of records lost and the claim payout. The minimum cost per record was $.01 and the *maximum cost per record was more than a quarter of a million dollars* ($251,430). The mean cost per record was almost seven thousand dollars ($6,790), while the median cost was just over a hundred dollars per record ($107.14).

The median cost per record in this year's study ($107.14) is much higher than prior years. This is primarily due to incidents in which few records were disclosed but there were large payouts for forensics and/or legal expenses.

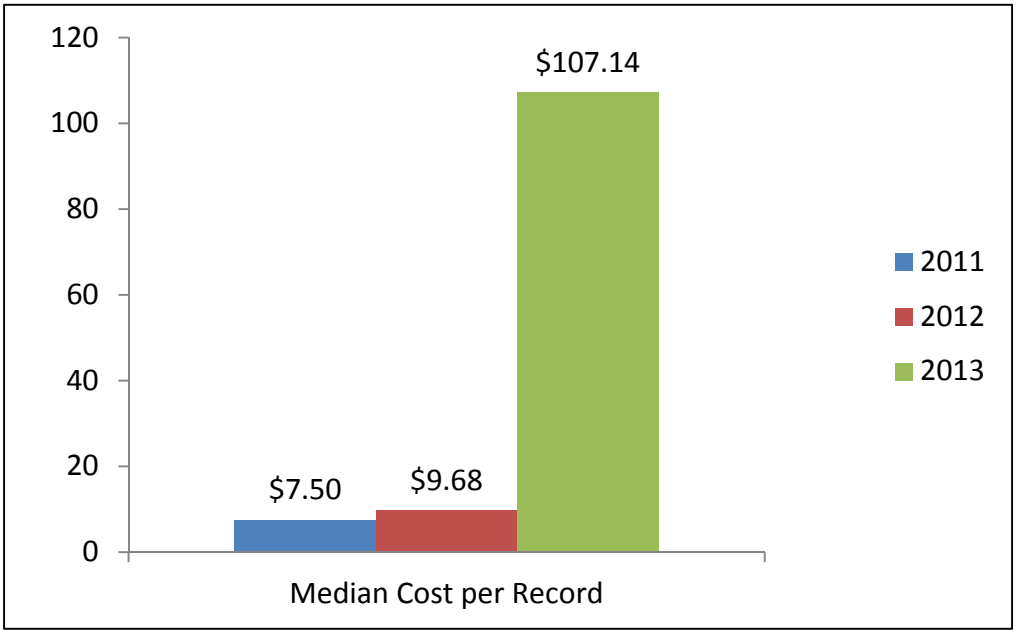
For example, one case involved the staff of a healthcare provider commenting on a patient's diagnosis on a social media website. The resulting legal expenses caused the per-record cost for that incident to exceed a quarter of a million dollars. In another example, the theft of one donor's credit card information from a non-profit resulted in a forensics investigation, a lawsuit and a PCI fine. The per-record cost for that incident was $50,000.

These examples illustrate that stunningly high per-record costs *are possible*, so both insurers and the organizations they cover should be aware of that.

However, these per-record costs are *not typical*. If we classify incidents in our dataset that show per-record costs in excess of $5000 as "outliers" and eliminate them from our calculations, our numbers are much more in line with other industry studies. The median per-record cost was $97, while the average per-record cost was $307.

That said, we found no correlation between the number of records lost and the total cost of the breach. Even when we excluded outliers by using only 90% of the data (from the 5th to the 95th percentiles), we still found a complete lack of correlation between the number of records lost and the total cost of the breach. Based on this relatively small dataset, we conclude that the cost per record is a meaningless number for budgetary and actuarial purposes.

That conclusion was consistent across all data types, so it does not appear that the type of data lost suggests a higher or lower cost per record. It is possible that other criteria influence the cost per record, such as the state in which the breach occurred, but that information was not collected for this particular study.

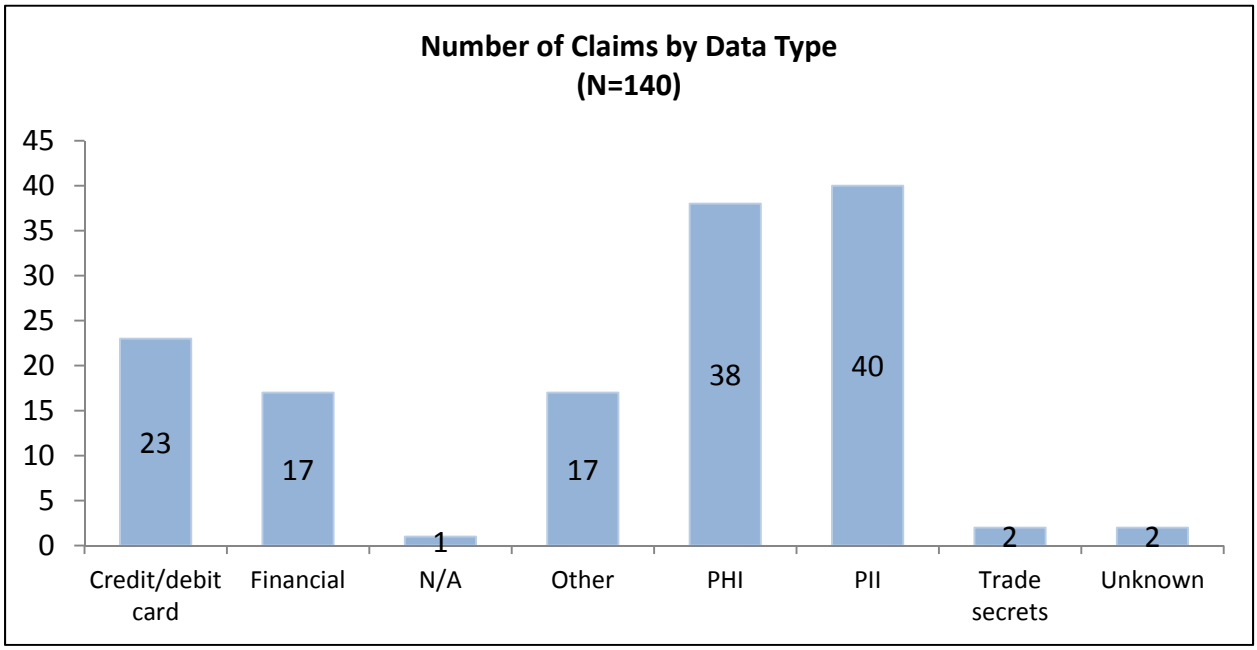


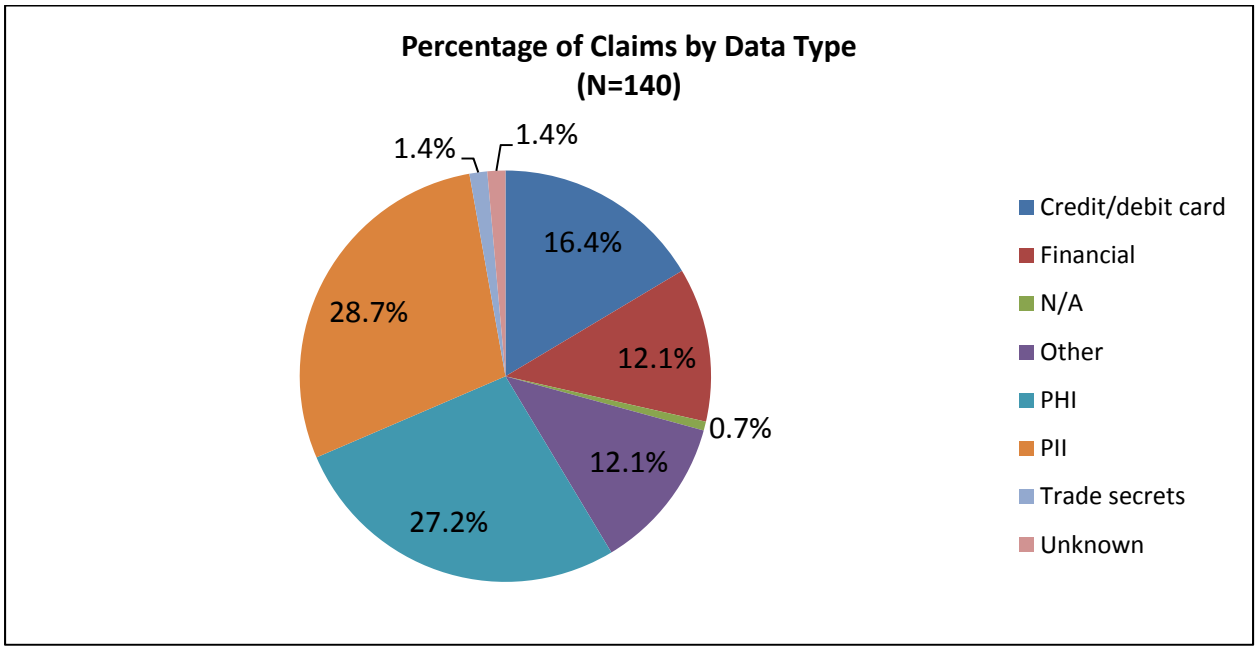
Viewing the Data through Different Lenses

Type of Data Exposed

As expected, PII (personally identifiable information) and PHI (private health information) were the most commonly exposed data. In this year's study, the number of claims submitted for these two data types was almost identical, 40 for PII (28.7% of claims) and 38 for PHI (27.1%).

Credit/Debit Card information was exposed in 23 of the claims submitted (16.4%) and Other Financial data was exposed in 17 of the claims (12.1%). Other data (primarily proprietary business information, such as billing records) were exposed in 17 claims (12.1%). There were 2 claims (1.4%) that involved the exposure of trade secrets, 1 claim (0.7%) involving copyright infringement and 2 claims (1.4%) for which the type of data was not provided.





In this year's study, there were 2 large claims for incidents in which more than 100 million records (PII) were exposed. For this reason, PII accounted for more than 95% of the records exposed. PHI accounted for only 2.48% of records exposed, while credit/debit cards accounted for only 1.79% of records exposed.

Records					
Data Type	Claims with Records	Min	Median	Mean	Max
Credit/debit card	15	1	76,000	261,992	2,000,000
Financial	9	1	250	1,863	10,000
Other	5	75	6,000	92,744	450,000
PHI	32	1	192	170,185	5,000,000
PII	32	1	6,750	6,552,607	109,000,000
Total	**93**				

Across all data types, the range of claim payouts was enormous, from a low of $2,560 up to $20 million. Surprisingly however, the median payout—regardless of data type—fell within a relatively narrow range, between $207,000 and $317,000.

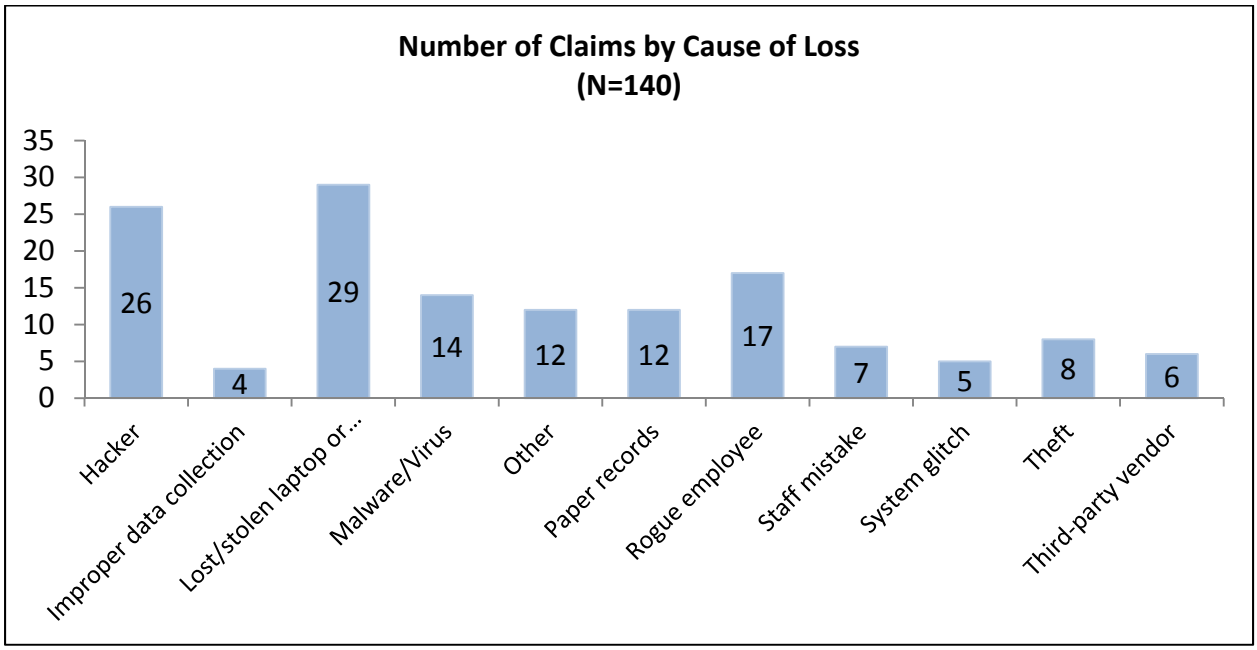
Total Costs (including SIR)					
Data Type	Claims with Costs	Min	Median	Mean	Max
Credit/debit card	12	50,000	252,500	701,029	4,750,000
Financial	7	50,000	209,500	558,133	1,553,365
Other	10	12,500	317,000	410,150	1,135,000
PHI	26	15,915	251,615	1,376,227	20,000,000
PII	31	2,560	207,000	1,007,324	11,550,000
Trade secrets	2	34,500	272,250	272,250	510,000
Total	**88**				

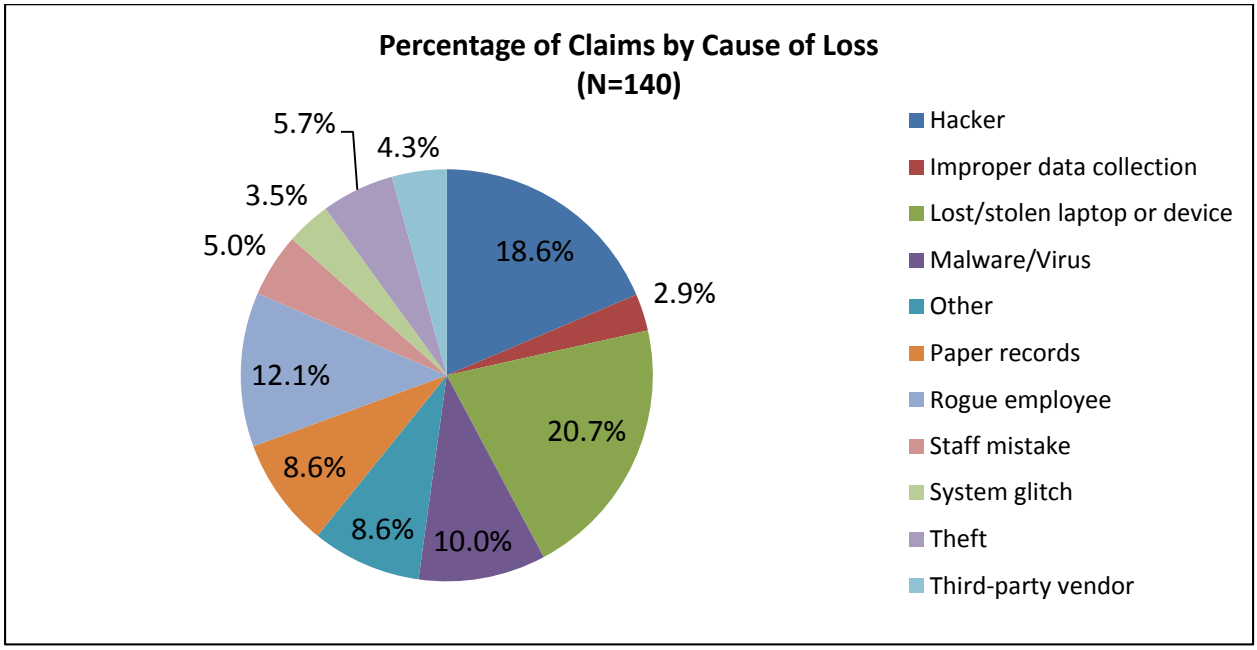
Cause of Loss

As in our previous studies, lost or stolen laptops/devices and hackers were the leading causes of loss. This year, however, lost or stolen laptops/devices moved into first place with 29 claims (20.7%). Hackers were close behind, responsible for 26 claims (18.6%).

Rogue employees moved into third place, responsible for 17 claims (12.1%). Malware/virus dropped to fourth with 14 claims (10.0%), followed by paper records with 12 claims (8.6%).

New this year—following passage of California's Song-Beverly Act in 2011 which changed the definition of PII—there were 4 claims (2.9%) involving the improper collection of sensitive data (e.g., zip codes). The "other" category included 12 claims (8.6%) for losses caused by FACTA lawsuits, online copyright infringement and poor data security practices (weak passwords and unencrypted email).





While lost/stolen laptops and devices accounted for 20.7% of claim events, those incidents resulted in less than 1% of records exposed. Conversely, hackers accounted for fewer incidents (18.6%), but were responsible for a stunning 97.6% of records exposed. This is primarily due to two large hacking attacks that exposed 100 million records each.

Records					
Cause of Loss	Claims with Records	Min	Median	Mean	Max
Hacker	12	200	93,000	17,647,708	109,000,000
Improper data collection	1	23,000	23,000	23,000	23,000
Lost/stolen laptop or device	20	7	1,100	29,875	300,000
Malware/Virus	10	3	1,587	114,426	1,000,000
Other/Unknown	4	10	94	19,050	76,000
Paper records	10	1	157	10,369	77,000
Rogue employee	14	1	138	6,975	50,000
Staff mistake	6	1	143	1,103	6,000
System glitch	5	8	11,374	28,776	95,000
Theft	6	1	43,500	923,000	5,000,000
Third-party vendor	5	60	2,000	7,281	22,000
Total	**93**				

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 tend to result in slightly higher costs than incidents caused by simple errors, such as staff mistakes, or actions by a third-party provider.

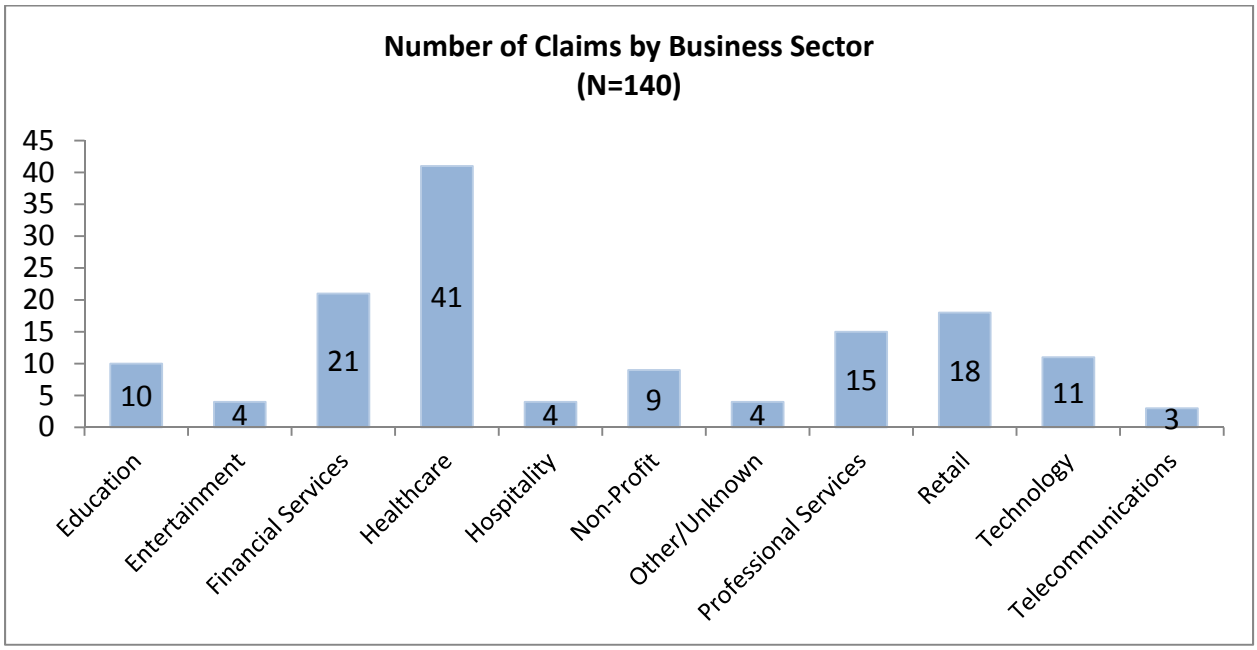
The exception is hacking incidents which, while not directly caused by the affected organization, were extremely expensive. This is probably attributable to the fact that hacking incidents tend to expose a much larger number of records than do other types of incidents.

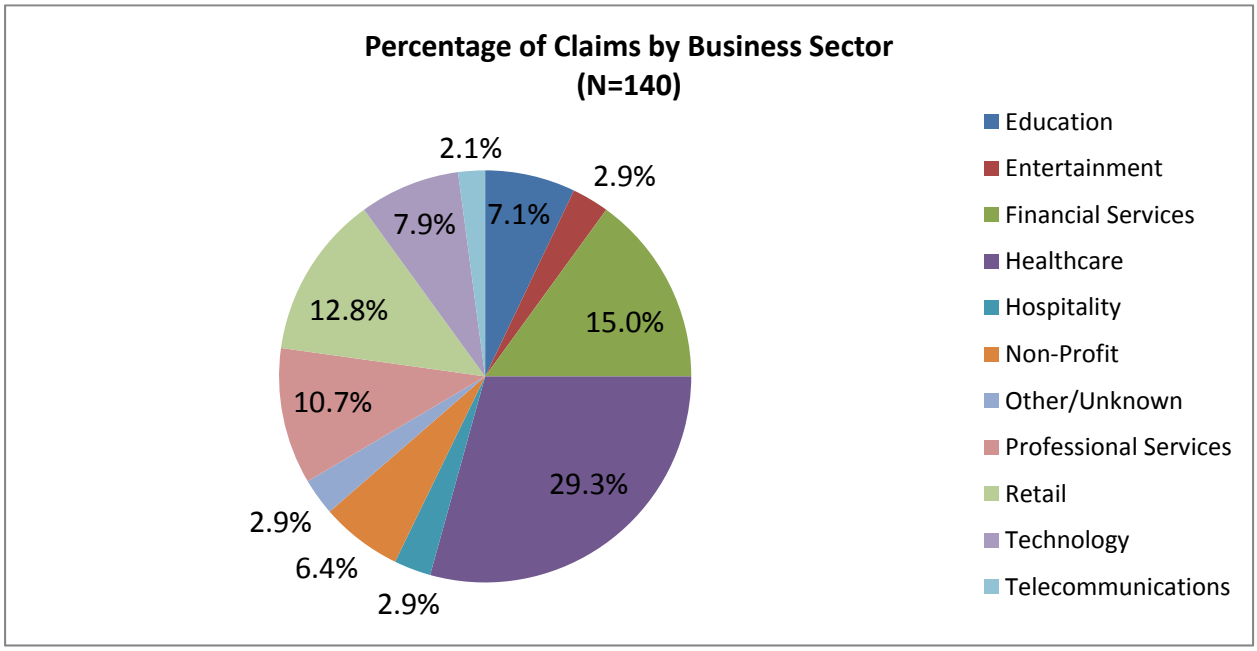
Total Costs (including SIR)					
Cause of Loss	Claims with Costs	Min	Median	Mean	Max
Hacker	18	5,390	327,500	1,013,371	10,500,000
Improper data collection	4	55,000	460,000	3,131,250	11,550,000
Lost/stolen laptop or device	16	13,000	166,000	1,754,986	20,000,000
Malware/Virus	7	30,000	275,000	851,329	4,750,000
Other/Unknown	6	12,500	222,375	376,042	1,300,000
Paper records	7	122,000	254,000	282,229	565,000
Rogue employee	11	15,915	251,430	423,663	1,045,400
Staff mistake	3	20,100	150,000	435,033	1,135,000
System glitch	2	225,000	327,500	327,500	430,000
Theft	8	45,000	182,000	672,130	3,000,000
Third-party vendor	6	2,560	80,222	490,034	2,500,000
Total	**88**				

Business Sector

In our first two studies, Healthcare and Financial Services suffered similar numbers of claim events—and those two sectors were far and away the most affected sectors. That changed in this year's study. Healthcare is now the clear leader with 41 claims (29.3%), almost twice the 21 claims (15.0%) that occurred in Financial Services.

Retail held onto third place with 18 claims (12.8%), followed by Professional Services with 15 claims (10.7%), Technology with 11 claims (7.9%), Education with 10 claims (7.1%) and Non-Profits with 9 claims (6.4%). The remaining sectors included Entertainment (4 claims, 2.9%), Hospitality (4 claims, 2.9%), Other/Unknown (4 claims, 2.9%) and Telecommunications (3 claims, 2.1%).





The two massive breaches of 100 million records each that we previously referenced both occurred in the Entertainment sector, which caused that sector to be responsible for 95.2% of all records exposed. The "Other" category accounted for 2.3% of records exposed, due almost entirely to the theft of backup tapes in the manufacturing sector. Retail accounted for 1.5% of records exposed. All other sectors combined accounted for the remaining 1% of records exposed.

Records					
Business Sector	Claims with Records	Min	Median	Mean	Max
Education	6	100	8,861	29,682	130,000
Entertainment	4	1	50,050,000	52,275,000	109,000,000
Financial Services	11	8	1,200	13,638	84,000
Healthcare	34	1	352	19,256	300,000
Hospitality	4	10	600	267	600
Non-Profit	6	1	78	18,571	111,000
Other/Unknown	2	86,000	2,543,000	2,543,000	5,000,000
Professional Services	8	75	850	60,438	450,000
Retail	12	3	4,813	266,086	2,000,000
Technology	6	45	5,500	97,008	450,000
Telecommunications	0	0	0	0	0
Total	**93**				

The two massive data breaches also caused the costs in the Entertainment sector to skyrocket. The Technology sector also experienced a large hacking attack and the costs in that sector reflect that fact. Surprisingly however, the single largest payout occurred in the Healthcare sector.

When we look at the median cost of these claim events—discounting the Entertainment and Technology sectors as outliers—we find that breaches in Healthcare, Retail and Professional Services were incrementally more costly than breach events in other sectors.

Total Costs (including SIR)					
Business Sector	Claims with Costs	Min	Median	Mean	Max
Education	8	2,560	132,650	204,858	680,000
Entertainment	2	1,125,000	5,812,500	5,812,500	10,500,000
Financial Services	8	20,100	166,000	1,060,138	4,750,000
Healthcare	29	5,390	254,000	1,612,343	20,000,000
Hospitality	4	55,000	113,282	129,141	235,000
Non-Profit	6	12,500	47,500	131,750	500,000
Other/Unknown	5	34,500	86,000	721,250	3,000,000
Professional Services	9	33,000	209,500	189,389	354,000
Retail	11	50,000	270,000	247,741	520,000
Technology	6	510,000	1,100,000	1,021,394	1,553,365
Telecommunications	0	0	0	0	0
Total	**88**				

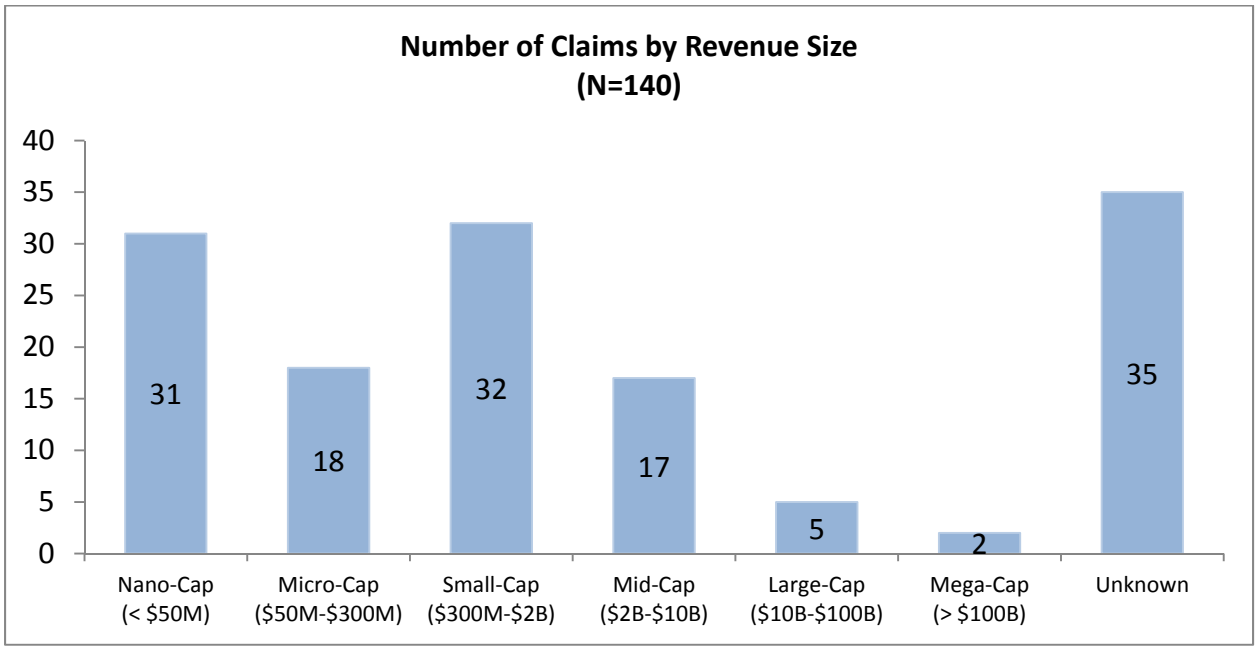
Size of Affected Organization (based on revenue)

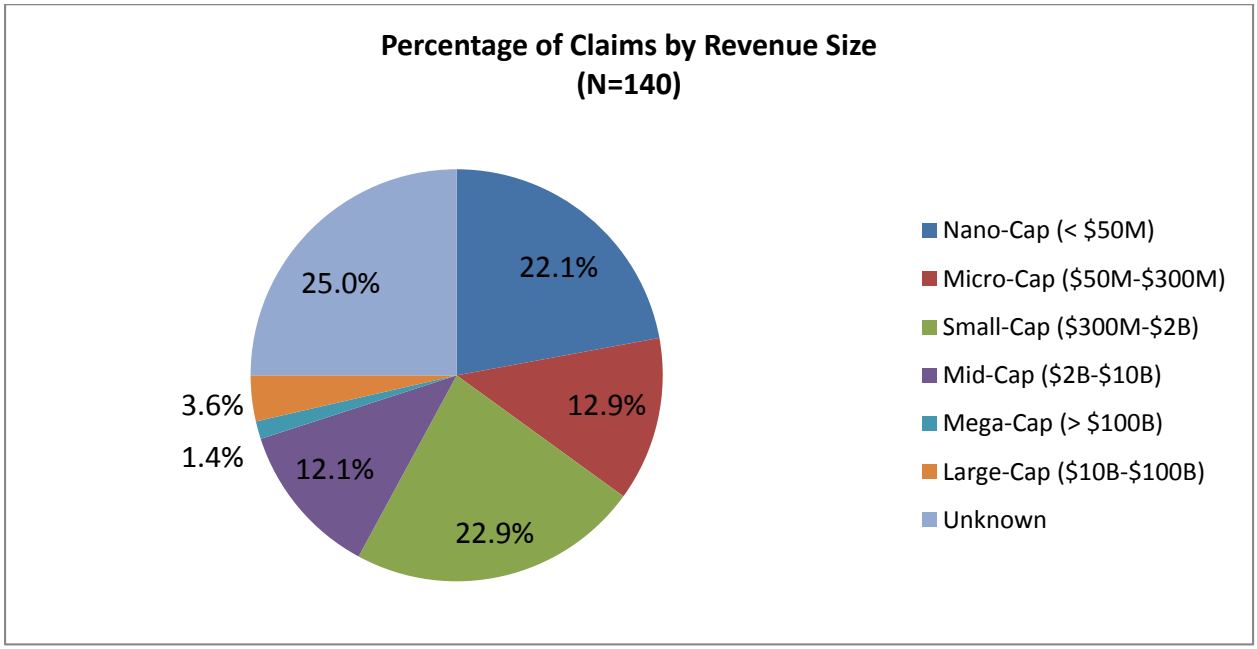
For the first time, we also asked insurers to tell us the size of the organization affected by each incident.

Revenue size was not reported for 35 claims (25%) in our dataset. Small-Cap accounted for 32 claims (22.9%), followed by Nano-Cap which accounted for 31 claims (22.1%). Micro-Cap organizations accounted for 18 claims (12.9%) and Mid-Cap accounted for 17 claims (12.1%). The largest organizations, Large-Cap and Mega-Cap, combined accounted for only 7 claims (5%).

Our findings indicate that smaller organizations experienced most of the incidents. This may be because smaller organizations are less aware of their exposure or they disregard the risk thinking they are not targets. Or it may be that they have fewer resources to provide appropriate data protection and/or security awareness training for employees.

However, since fully one quarter of the claims submitted did not include the revenue size of the affected organization, it is difficult to draw any meaningful conclusions from these numbers.





While Mega-Cap companies accounted for only 1.4% of claim events (that we know of), they were responsible for 45.6% of records exposed. Organizations of "unknown" size accounted for 50% of records exposed. It is clear that one of the outlier breaches (100 million records exposed) in this dataset was incurred by a Mega-Cap company and the other by a company of unknown size. Based on the sheer number of records exposed, we might suspect the second company is also Mega-Cap, but we do not know that for certain.

Large-Cap companies, which experienced 3.6% of the claim events, were responsible for 2.3% of records exposed, while Small-Cap companies (22.9% of claim events) were responsible for only 1.1% of records exposed. All other size categories combined accounted for the remaining 1% of records exposed.

Records					
Revenue Size	Claims with Records	Min	Median	Mean	Max
Nano-cap (< $50M)	18	1	250	69,761	1,000,000
Micro-cap ($50M-$300M)	13	2	700	22,268	100,000
Small-Cap ($300M-$2B)	24	1	1,100	102,101	2,000,000
Mid-Cap ($2B-$10B)	9	45	7,500	92,654	450,000
Large-Cap ($10B-$100B)	2	29,000	2,514,500	2,514,500	5,000,000
Mega-Cap (> $100B)	1	100,000,000	100,000,000	100,000,000	100,000,000
Unknown	26	1	724	4,218,508	109,000,000
Total	**93**				

In terms of costs, Mega-Cap and Large-Cap companies incurred the most expensive claim events. The *minimum* payouts in these two size categories were $10.5 and $3 million, respectively.

For the other size categories, the median cost of a claim event appears to reflect the organization size. In other words, the median cost for a claim in a Nano-Cap company is less than for a Micro-Cap company, which in turn is less than for a Small-Cap company. This could be indicative of smaller breaches, less insurance coverage, or both.

Total Costs (including SIR)					
Revenue Size	Claims with Costs	Min	Median	Mean	Max
Nano-cap (< $50M)	17	2,560	50,000	106,794	390,600
Micro-cap ($50M-$300M)	13	15,915	88,037	277,724	1,553,365
Small-Cap ($300M-$2B)	24	32,000	229,875	447,736	1,300,000
Mid-Cap ($2B-$10B)	11	121,000	656,650	2,707,229	20,000,000
Large-Cap ($10B-$100B)	2	3,000,000	3,000,000	3,875,000	4,750,000
Mega-Cap (> $100B)	1	10,500,000	10,500,000	10,500,000	10,500,000
Unknown	20	20,100	255,100	988,657	11,550,000
Total	**88**				

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 five such incidents—all involving business interruption. The incidents occurred in Retail (2), Financial Services, Manufacturing and Telecommunications. Four were caused by distributed denial of service attacks (DDoS) and one by malware. The costs for these incidents are still pending.

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.

Our 2011 study saw ten first-party loss incidents caused by DDoS attacks, malware and cyber extortion. That year, claims reported approximately $1.22 billion in lost business income and $23 million in expenses. One incident resulted in fines of approximately $4 million.

Conclusion

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.

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.

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. We're making progress in that direction. 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.

So we are seeing growing support within the insurance industry for this study and we hope that trend continues in 2014 to the benefit of all parties.

--- ### ---

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
Digital Risk Managers
Hiscox
Hylant
Kiln
Liberty International Underwriters
Marsh
OneBeacon Professional Insurance
Philadelphia Insurance Companies
SH Smith
Travelers
United States Liability Insurance
Wells Fargo Insurance Services
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 ALERT NETWORK

AllClear ID is the price, service, and product leader in the data breach response industry. We partner with cyber insurers to provide unique solutions that save money and effectively cover data breach events. Our innovative, proactive approach to breach response offers significant cost savings compared to a standard response, while providing better protection to victims, resulting in fewer customer complaints and less brand tarnish. Year-after-year, AllClear ID is recognized for unsurpassed customer service, patented technology and innovative identity protection services. AllClear ID has received 10 international awards for outstanding customer service and maintains an industry-leading 97% customer satisfaction rating. For more information, visit **AllClearID.com/business**.

FIC FARUKI IRELAND & COX P.L.L. www.ficlaw.com

At Faruki Ireland and Cox, we not only excel at representing you in litigation and resolving the conflicts that threaten your business's future, but also are working to keep you out of the fight in the first place. We have taken our broad experience in the litigation trenches to help clients strategize, plan and account for information privacy and security requirements as part of their business development and risk compliance functions before an event occurs. Most look at data privacy and security as onerous, expensive compliance burdens. Not us. We develop seamlessly integrated responsible information management practices. Be it HIPAA, GLBA, FCRA, or data breach response planning, accounting for privacy can keep you out of the press, courtroom or regulators' cross-hairs. Whether before or after an event, let Faruki Ireland and Cox lead you to success. For more information, visit **ficlaw.com**.

KIVU

Since 2009, Kivu has been providing incident response, forensic analysis and technical remediation in data breaches nationwide. Our findings have allowed organizations to avoid unnecessary notification and reduce their exposure to subsequent litigation. Using in-house experts and proprietary remote analysis tools, we swiftly and cost-effectively determine if a breach has occurred, determine its size and scope, and provide valuable evidence for responding to regulators, customers and litigants. Kivu is a pre-approved vendor with most cyber-insurance carriers. We have an established record working with the leading breach coaches and law firms handling cyber events. For more information, visit **kivuconsulting.com**.

About the Author

Mark Greisiger is president of Network Standard Corp., which does business as NetDiligence®, a Philadelphia-based firm that provides cyber risk assessment services for chief financial officers and risk managers to help assess whether their organizations deploy reasonable and prudent safeguards to mitigate data breach losses and liability risk. Since 2001, NetDiligence services have been used by insurers in the United States and the United Kingdom that offer data and privacy risk insurance products, providing loss control services to their insured business clients. Prior to starting NetDiligence, Mr. Greisiger worked for more than a decade directly in the insurance industry where he developed and underwrote a 'hacker insurance' product.

NetDiligence®
Cyber Risk Assessment & Data Breach Services

eRiskHub®

NetDiligence's eRisk Hub® web portal helps companies respond to data breaches quickly, efficiently and cost-effectively. For more information, visit www.eRiskHub.com.

NetDiligence®
A Company of Network Standard Corporation
P.O. Box 204
Gladwyne, PA 19035
www.NetDiligence.com