Cyber Liability & Data Breach Insurance Claims

A Study of Actual Payouts for Covered Data Breaches

Mark Greisiger
President
NetDiligence®
October 2012
Executive Summary

In 2011, some 23 million confidential records were exposed through more than 414 reported security breaches, according to the national nonprofit Identity Theft Resource Center (ITRC). These figures represent a 44 percent increase in the number of records exposed, yet a 37 percent decrease in the number of reported incidents, over what was reported for 2010. Clearly while 2011 brought us fewer incidents, many of the incidents that did occur were large in scale.

In fact, 2011 saw some of the biggest data breaches ever reported: Sony, Sutter Health, Science Applications International Corporation (a third-party provider for Tricare), Epsilon and the Texas Comptroller’s Office.

While this paper focuses on incidents that occurred from 2009 through 2011, we should note that 2012 has already seen a significant number of really large breaches, including Global Payments (1.5 million records), Yahoo! (400 thousand passwords), Wyndham Hotels (600 thousand credit cards), eHarmony (1.5 million passwords), LinkedIn (6.5 million passwords), Zappos (24 million records), Gamigo (3 million records), and the Texas Attorney General’s Office (6.6 million records).

2011 also revealed some significant new trends in cyber risk and liability.

The Definition of Personally Identifiable Information (PII) is Getting Broader

In 2011, we saw a massive expansion in the types of information that regulators, litigators and the courts consider PII. After two monster breaches at large email marketing firms (Epsilon and Silverpop), email addresses are now arguably considered PII. Also, in February of 2011 the California Supreme Court found that zip codes qualify as PII for the purposes of California’s Song-Beverly Credit Card Act. As a result of this holding, many class action suits have been filed against retailers in California, potentially costing them and their insurers many millions of dollars.

Delaying Notification Can Cost You Dearly

In March 2011, insurer Health Net disclosed a data breach that exposed the personal data of 2 million people. Unfortunately, this was a second incident for the company. In 2009, Health Net had another security breach in which a portable disk drive holding the personal data of 1.5 million people disappeared. Health Net was fined by several states as a result of the 2009 breach ($375 thousand in Arizona, $55 thousand in Vermont, etc.). For this reason, penalties for the 2011 breach could be significant.
another cautionary tale about delaying notification, in May 2011, lawyers for Honda customers filed a class action lawsuit accusing Honda of putting 283,000 customers at risk, in part by waiting two months to inform them of a data exposure. The lawsuit seeks 200 million Canadian dollars ($206 million) on behalf of the plaintiffs.

Privacy Violation Lawsuits Are Increasing

2011 and early 2012 saw an explosion in the number of lawsuits filed alleging violations of customer privacy. Privacy violation lawsuits, many of them class-actions, have been filed against Apple, Samsung, HTC, Google, Facebook, Amazon, CVS Caremark Corporation, Aaron’s Inc., Michaels Stores, UCLA Health System, Comscore, and Royal Bank of Canada (RBC), to name just a few (see a summary of class action lawsuit cases in eRisk Hub®). It is clear that consumers and trial lawyers are testing the courts to determine whether a monetary value can (and will) be assessed when companies collect, share or retain customer information inappropriately.

Hackers Escalate Attacks on Infrastructure

In 2011, we learned that hackers were targeting (perhaps testing) critical infrastructure systems. In January 2011 we learned that hackers had attacked computers at an unidentified railway company in the Pacific Northwest, disrupting railway signals for two days in December 2010. In February 2011, we learned that perpetrators had repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Exchange. The Nasdaq situation reportedly set off alarms in the U.S. Department of Homeland Security because of the exchange’s critical role in the nation’s infrastructure. In December 2011, an FBI official confirmed that Supervisory Control and Data Acquisition (SCADA) systems in three cities had been compromised but claimed the attackers had not done any damage. Since then, of course, we’ve been introduced to Stuxnet and Flame as next-generation tactics for attacking SCADA systems. Note: See more on this topic at Junto (http://juntoblog.net/), the NetDiligence® blog.

Financial Services Remain a Favored Target

A significant number of financial institutions were victimized in 2011. Among those publicly acknowledging breaches were Bank of America, Citigroup, Sovereign Bank and Royal Bank of Scotland (RBS). Numerous smaller institutions were also targeted by hackers and phishers.

From an insurer’s perspective, 2011 also revealed one worrisome and one welcome trend on the part of insured companies.
Worrisome

Despite the continuing threat of cyber incidents like those discussed above, and the cost of these incidents to company bottom lines, 2011 also saw data security moved out of the C-suite and relegated to front-line managers.

“As an underwriter, it concerns me when IT security is no longer considered an executive issue, but pushed back to operations to manage,” commented Tracey Vispoli, Senior Vice President of Chubb Specialty Insurance. “And trends are pointing in that direction. A recent PricewaterhouseCoopers (PwC) survey indicated that in 2011 only 39% of executives evaluated their security policies annually, compared to 52% in 2009. At a time of unprecedented data security events, this is hard to imagine. A June 2011 Ponemon Institute survey presents a frightening paradox … that while fewer executives are evaluating their security policies, 90% of companies surveyed experienced at least one breach in the prior 12 months.”

These figures are even more difficult to interpret and understand in light of the SEC’s newly released Disclosure Guidance on Cybersecurity (CF Disclosure Guidance: Topic No. 2 Cybersecurity), which requires not only reporting the material risks associated with a specific data breach or other cyber incident, but the disclosure of the financial and legal impact along with the controls and processes in place to prevent such losses.

Clearly, it is incumbent on insurers and other industry experts to understand why companies are not more actively engaged in ongoing cyber risk assessment.

Welcome

“Our ongoing efforts in client awareness and education are paying dividends for our clients,” says Meredith Schnur, Senior Vice President of Wells Fargo Insurance Services. “It used to be that clients who were victimized by a cyber incident responded to the event on their own. They didn’t contact us until much later. That isn’t happening any more. Clients are more aware of their responsibilities and the potential cost if they fail to meet those responsibilities. Their first call now is to us or their Breach Coach®. We’re involved earlier, which means we’re in a position to help our clients avoid mistakes and minimize the negative impact of an incident.”

Tracie Grella, Global Head of Professional Liability at Chartis Insurance, agreed that increased client awareness is helping to minimize damage and contain costs. “People know more about how cyber insurance works,” said Grella. “They know when to call about a data breach and they’re much more cooperative in working with us to respond to the event. The market’s maturing. People with repeat breaches are more open to communicating with their insurer. They’re appreciating the value of their insurance and trusting our recommendations regarding the vendors to use when responding to an incident.”
Claims, Claims, Claims

The second annual NetDiligence® Cyber Liability & Data Breach Insurance Claims study examines whether actual cyber and privacy liability claims mirror the anecdotal breach information that we see reported in the media and industry reports. Our study uses actual cyber liability insurance policy 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 assessment and implement better safeguards and action plans to protect organizations from data breaches.

Major underwriters of cyber liability provided information about 137 events that occurred between 2009 and 2011, which we analyzed for emerging patterns. Among our findings: PII (personal identification information) is the most typically exposed data type, followed by PHI (private health information). Topping the list of the most frequently breached sectors are healthcare and financial services. The average cost per breach was $3.7 million, with the majority devoted to legal damages.
When compared with the Ponemon Institute’s *Seventh Annual U.S. Cost of a Data Breach Study*, our figures appear to be extremely low. The institute reported an average cost of $5.5 million per breach and $194 per record. However, Ponemon differs from our study in two distinct ways: the data they gather is from a consumer perspective and as such they consider a broader range of cost factors such as detection, investigation and administration expenses, customer defections, opportunity loss, etc. Our study concentrates strictly on costs from the insurer’s perspective and therefore provides a more focused view of breach costs.

The NetDiligence study also focuses primarily on insured per-breach costs, rather than per-record costs. As explained by Thomas Kang, Senior Claims Specialist at ACE USA, “You have to be careful in correlating too closely the cost of a breach response to the number of records. Certainly, it will cost more to notify and offer credit monitoring to more people, and there is greater risk of potential third-party claims for incidents involving a higher number of records. However, the legal and forensic costs can vary significantly depending on the complexity of the incident and the specific requirements in the policyholders industry, independent of the number of records. There appears to be an expectation in the marketplace for a breach to cost a certain amount simply based on the number of records, but our policyholders have been surprised to find that the actual response costs generally will be unique to the specifics of the breach. For example, we have breach incidents involving less than 5 thousand records, with remediation costs in six figures because of the policyholders’ industry and the complexity of the breach.”

“Sometimes, people expect their breach to cost a certain amount simply based on the number of records, but are surprised to find that the actual costs can be unique to the specifics of the breach.”

*Thomas Kang, Senior Claims Specialist at ACE USA*


About this Study

For this study, we asked insurance underwriters about data breaches and the claim losses they sustained. We looked at the type of data exposed, what caused the loss, and which business sector suffered the incident. We also looked at the number of records exposed and the associated Crisis Services (forensics, notification, credit monitoring, and legal counsel), Legal Damages (defense and settlement), and Fines (PCI & regulatory). Lastly, we asked leaders in the industry representing insurance carriers, law firms, general counsel and cyber breach consultants to offer their insights into recent developments and trends in breach events.

This report summarizes our findings for a sampling of data breach insurance claims occurring in a variety of sectors, including government, healthcare, hospitality, financial services, transportation, telecommunications, online services, professional services, retail and many more.

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 2009 and 2011
- The victimized organization had some form of cyber or privacy liability coverage
- A legitimate claim was filed

We received claims information for 137 events that fit our selection criteria. Of those, 58 events included a detailed breakout of what was paid on the claim. 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.

We used our entire sampling of 137 events to analyze the type of data breached, the cause of data loss and the business sectors affected. We used the smaller sampling (58 events) to evaluate the payouts associated with the events—again based on type of data breached, the cause of data loss and the business sectors affected.

As a result, 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 focused on claims payouts rather than expenses incurred by the victimized organizations
- Our numbers are empirical as they were supplied directly by the underwriters who paid the claims
- Most claims were reported for total losses. Of those that mentioned retentions, these ran anywhere from $50 thousand to $1 million.
Findings Highlights

The Big Picture

Important: Please bear in mind that this year’s study (2012) analyzes claims that were submitted in 2011 based on incidents that occurred from 2009 through 2011.

Based on the claims submitted for this year’s study, the average number of records exposed per incident was 1.4 million, a decrease of 18 percent from last year’s study (1.7 million). The average cost per incident was $3.7 million, up steeply from last year ($2.4 million). The average cost per record was $3.94, also up sharply compared to last year ($1.36).

Please note that we calculated cost averages using only 58 of the 137 events in our sampling. The remaining 79 incidents that were submitted for our study did not include details of claim payouts so were included in our analysis of the events, but omitted from our analysis of costs.

In our study, average costs are greatly affected by the number of records exposed versus actual claims payouts for things like legal settlements. For example:

• Our $3.94 average cost per record does not take into account the per-record cost for extraordinarily large settlements. The recent Minnesota AG settlement ($2.5 million) against Accretive Health, resulted in an average per-record cost of $108 mainly because a relatively small number of records (approximately 20 thousand) were exposed. However, breaches that expose massive numbers of records often result in per-record costs of just pennies.

• Our $3.7 million average cost per breach is not representative of the typical breach, which ranges from $25 - $200 thousand.
As in last year’s study, Legal Damages represented the single largest component of costs. The average cost for legal defense was $582 thousand (compared to $500 thousand last year), while the average legal settlement was $2.1 million (compared to $1 million last year). Crisis Services represented the second largest component of costs. The average cost for Crisis Services, including forensics, notification, call center, credit monitoring and legal guidance, was $983 thousand (compared to $800 thousand last year).

A closer look at the individual components of Crisis Services costs reveals sharp increases across the board with the exception of Notification and Legal Counsel, both of which dropped this year.
As the above chart indicates, the average cost for Forensics was $341 thousand (up sharply from $170 thousand in last year’s study). Overall, forensics costs ranged from as little as $350 to more than $1 million. However, the typical cost for forensics ranged from $10 thousand and $225 thousand.

The average cost for Notification was $180 thousand (down from $201 thousand last year). Overall, notification costs ranged from as little as $300 to $2.5 million. The typical cost for notification ranged from $20 thousand to $100 thousand.

The average cost for Call Center was $50 thousand (up from $15 thousand last year). Overall, call center costs ranged from $0 to more than $1 million. The typical cost for call center ranged from $5 thousand to $40 thousand.

The average cost for Credit Monitoring was $354 thousand (up from $253 thousand last year). Overall, credit monitoring costs ranged from $0 to $15 million. The typical cost for credit monitoring ranged from $6 thousand to $300 thousand.

Finally, the average cost for Legal Counsel was $66 thousand (down sharply from $242 thousand last year). Overall, legal counsel costs ranged from $0 to $1 million. The typical cost for legal counsel ranged from $5 thousand to $100 thousand. Recall that legal counsel, as a component of Crisis Services, does not include costs for legal defense or settlement.

Despite anecdotal evidence that regulatory agencies and State Attorneys General are beginning to proactively investigate breaches and levy fines for non-compliance with security and privacy regulations, fines were almost non-existent as a cost factor in our study. This may be because the insurers participating in our study do not cover fines or they elected not to submit incidents that resulted in fines. On the other hand, the explanation may simply be that the claims occurred in states that do not allow coverage of fines or that the fines (typically assessed later in the claims cycle) have not yet been levied.
Type of Data Exposed

Similar to last year’s results, nearly half of the events (42 percent) involved the unauthorized disclosure of PII (personally identifiable information). This represents a 27 percent increase in PII-related claims compared to last year.

PHI (private health information) was again the second-most frequently exposed data, comprising 15 percent of claims incidents submitted for this year's study. This represents a 16 percent decrease in the number of PHI-related claims, compared to last year.

Credit Card and Other Financial data accounted for the remaining 40 percent of reported cyber claims incidents. For Credit Cards, this represents an 11 percent decrease in reported claims and for Other Financial it is a 180 percent increase in reported claims, compared to last year.

In terms of records exposed, PII led the way with 210 million records (60 percent). Credit Cards came in second with 107 million records (31 percent) and PHI came in a distant third with 4 million records (1 percent).

Finally, in terms of costs, Crisis Services costs were incurred for virtually all claim events, regardless of the type of data exposed. For Other Financial claims, Crises Services accounted for 100 percent of costs. For Credit Card-based incidents, Legal Damages accounted for 95 percent of costs. Fines were minimal and reported only for PHI- and Credit Card-related incidents.

Cause of Data Loss

Again for this year’s study, the cause of loss varied in our sampling, with 70 percent of the reported breaches being caused by one of three things: Hackers, Lost Laptops/Devices and Other (e.g. unwanted text messages or data collection from mobile phones/tablets).

Hackers caused 23 percent of breach events and were responsible for 62 percent (217 million) of all exposed records. This seems to be a decrease from last year (where it made up 76 percent of reported claims). However, in the 2011 study, Malware/Virus was reported as part of the Hacker category which may have affected this figure. As a new category this year, Malware/Virus accounted for only 5 percent of all reported claims but 29 percent (100 million) of records exposed.

Lost Laptops/Devices was the second leading cause of loss. Lost Laptops/Devices made up 19 percent of all claims submitted this year, but accounted for only 2 percent (7.2 million) of records exposed. Last year this category was reported as part of Loss/Theft which was 15 percent of all reported claims.
Other (e.g. web and personal device data loss) was the third largest cause of loss. Other made up 18 percent of claims submitted this year, but accounted for a tiny number of records exposed (150 thousand). This represents a 71 percent increase in number of incidents but a 90 percent decrease in records exposed, compared to last year's results.

In the 2011 study, Rogue Employees was one of the top three causes of loss. This year, Rogue Employee-caused incidents dropped to only 10 percent (from 19 percent) of reported breach events. This may be due to increased emphasis on security and privacy awareness training by businesses. However, while the number of incidents attributable to Rogue Employees declined, the number of records exposed by these bad actors increased by 71 percent, from 15 million records last year to 25 million records this year.

As far as costs were concerned, Crisis Services represented 100 percent of costs in three cause-of-loss categories: Paper Records, Staff Mistake and Theft. Legal Damages were very significant for Malware/Virus (98 percent of costs), Other (79 percent of costs) and Rogue Employees (74 percent of costs). Again, fines were marginal and accounted for 36 percent of costs for Third-Party incidents and a modest 1 percent for Malware/Virus incidents.

**Business Sectors Affected**

Findings by business sector were similar to last year with 56 percent of the claims submitted for this study occurring in Financial Services, Healthcare and Retail. Last year, these three sectors accounted for 60 percent of claims submitted for the study.

Financial Services accounted for 26 percent of claims (as opposed to 21 percent in last year's study) and 37 percent (131 million) of records exposed, a 511 percent increase over last year (21.4 million records exposed).

Healthcare accounted for 20 percent of claims (as opposed to 24 percent last year) and 2 percent (6.4 million) of records exposed, but that is a 1218 percent increase over last year (500 thousand records exposed).

Retail accounted for 10 percent of claims (as opposed to 15 percent last year) and 7 percent (24.5 million) of records exposed, a 140 percent increase compared to last year (10.2 million records exposed).

Finally, Crisis Services accounted for 100 percent of costs for four sectors: Education, Non-Profit, Online Services and Retail. Legal Damages accounted for 84 percent of costs for Financial Services, 81 percent for Technology and 64 percent for Other. Healthcare was the only sector to report Fines, but accounted for only 1 percent of the costs incurred in that sector.
About First-Party Claims

There were a limited number (5) of first-party claims submitted for this year’s study. The incidents occurred in the Telecommunications, Professional Services and Manufacturing sectors. The causes of loss were DDoS Attacks and Theft of IP/Trademarks. Most of the costs for these incidents are still pending; however, one of the claims has already paid out more than $495 thousand for forensics.

In our 2011 study, we saw 10 first-party loss incidents. Last year’s incidents occurred in Financial Services, IT/Technology, Manufacturing, Healthcare, Retail and Non-Profit. Causes of loss included DDoS Attack, Rogue Employee, Malware/Virus and Cyber Extortion. Last year’s claims reported approximately $1.22 billion in lost business income and $23 million in expenses.

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.

“Accurate information regarding losses and claims attributable to information and technology risks remains sparse—or at least non public,” observed Robert Parisi, Managing Director, Marsh Inc. “Risk managers, and underwriters, continue to struggle in evaluating these risks given the comparative lack of statistically significant actuarial data. And often the data that is available is either conflicting and/or encumbered with assumptions that vary dramatically from one survey to the next. Unfortunately, this ‘information vacuum’ can be a distraction from properly addressing what are key operational risks—risks that go to the very core of how a company operates.”

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 hope that each year more and more insurers and brokers will participate in this study 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 and this year (2012), our sampling included 137 claims. So we are seeing growing support within the insurance industry for this study and we hope that trend continues in 2013 to the benefit of all parties.
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.