

Cyber Liability & Data Breach Insurance Claims

A Study of Actual Payouts for
Covered Data Breaches

Mark Greisiger
President
NetDiligence®
June 2011



Cyber Liability & Data Breach Insurance Claims

A Study of Actual Payouts for Covered Data Breaches

Executive Summary

In 2010, some 16 million confidential records were exposed through more than 662 reported security breaches, according to the national nonprofit Identity Theft Resource Center (ITRC). Most recently, in a blog post that appeared on April 26, 2011, Sony Computer Entertainment America reported a security breach of its PlayStation Network in which hackers obtained personal information on some 100+ million subscribers, resulting in a security investigation so broad it suspended business operations, and resulted in multiple class action lawsuits.

“Last year, privacy breaches ran about 1-2 per week. This year, it is more like 6-8 per week.”

In cases like Sony’s, insurers will help foot the bill for the data breach—an amount that has been estimated at up to \$2 billion—and insurers are fielding increasing numbers of data breach-related claims. “Last year, privacy breaches ran about 1-2 per week. This year, it is more like 6-8 per week,” says Beth Diamond, Insurance Claims Focus Group Leader for Technology, Media and Business Services at Beazley Group. Diamond says the rising numbers are the result of increased legislation and companies’ heightened awareness about their legal obligations to report breach incidents.

That cyber security breaches are now a painful reality for organizations of all kinds, at all levels, is well established. What insurers and corporate risk managers are looking for are more effective ways to predict and prevent these incidents while developing a greater understanding of their financial implications.

This NetDiligence® cyber liability claims study, the first of its kind, examines where the bulk of these breaches are occurring and what kind of impact they have had on affected organizations. Major underwriters of cyber liability provided information about 117 events that occurred between 2005 and 2010, which we analyzed for emerging patterns. Among our findings: PII (personal identification information) is the most typically exposed data type, followed by PHI (personal health information). Topping the list of the most frequently breached sectors are healthcare and financial services. The average cost per breach was \$2.4 million, with the majority devoted to legal services.

“... this study is both timely and important because it ... demonstrates the real dollars that are being spent both dealing with the event as well as ultimate damages ...”

While previous studies have shed light on data breach events through anecdotal information, this study uses actual cyber liability insurance policy reported claims to illuminate the real costs of such incidents. 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 establish better safeguards and action plans to protect themselves from data breaches. “Given the recent well-publicized events, this study is both timely and important because it sheds light on what is driving these incidents, demonstrates the real dollars that are being spent both dealing with the event as



well as ultimate damages, and dispels the myth that data breach events don't carry significant damages to organizations that are affected," commented Norm Rafsol, Executive Vice President of ACE Professional Risk.

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), **business interruption costs**, 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 between 2005 and 2010 in a variety of industries, including airlines, consulting, education, financial services, retail, manufacturing, information technology and healthcare.

Study Methodology

This study, although limited, is the first of its kind, focusing 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 2005 and 2010
- The victimized organization had some form of cyber or privacy liability coverage
- A legitimate claim was filed

We received claims information for 117 events that fit our selection criteria. Of those, 77 events included a detailed breakout of what was paid on the claim.

We used our entire sampling of 117 events to analyze the type of data breached, the cause of data loss and the business sectors affected. We used the smaller sampling (77 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



Findings Highlights

The Big Picture

Based on the claims payout data submitted for this study, the average cost for a data breach was \$2.4 million. We calculated that average using 116 of the 117 events in our sampling. The one incident we excluded from our calculation was an outlier incident: a billion dollar business interruption event.

The average cost per record was \$1.36 when we considered all events in our sampling. However, when we excluded outlier events (those which exposed millions of records), the average cost per record was \$5.00. The number of records exposed ranged from 100 to 12 million. While the average number of records exposed was 1.7 million, the typical number of records exposed was 100,000.

“From our perspective, the retail sector is a large target since retailers store PII data that is not always protected...”

Legal damages represented the single largest component of costs. The average cost for legal defense was \$500,000. The average legal settlement was \$1 million.

Crisis services represented the second largest component of costs. The average cost for crisis services, including forensics, notification, call center and legal counsel, was \$800,000.

Type of Data Exposed

More than half of the events involved the unauthorized disclosure of **PII** (personally identifiable information). Approximately 75 percent of the records exposed contained credit card information. “From our perspective, the retail sector is a large target since retailers store PII data that is not always protected through firewalls or encryption,” says Jason Krause, Assistant Vice President, Arch Insurance. “With breach events such as TJ Maxx, however, which increased awareness, this has started to change.”

“We are starting to see an uptick in emotional distress cases as a result of increased public awareness of healthcare privacy issues since the passage of HITECH.”

PHI (personal health information) accounted for the second largest type of data, comprising 21 percent of breach incidents. According to Elizabeth Kim, Head of Claims for Technology, Media and Telecommunications at Hiscox USA, increased regulations such as **HITECH** (Health Information Technology for Economic and Clinical Health) are driving the next wave of third-party liability lawsuits. “We are starting to see an uptick in emotional distress cases as a result of increased public awareness of healthcare privacy issues since the passage of HITECH,” said Kim.

Although crisis services associated with **PII**, **PHI** and **credit card** data breaches were significant, much of the costs were due to legal damages awarded.



Cause of Data Loss

The cause of loss varied in our sampling, but ninety-five percent of the breaches were caused by one of three things: hackers, rogue employees, and loss/theft of equipment.

Hackers caused 32 percent of breach events and were responsible for 75 percent of all exposed records. Industry experts concur that these incidents can be directly attributed to increased use of malware.

According to Diamond, 36 percent of the attacks her claims department sees are from hackers. “With a hacking event you need forensics to determine the cause. In addition, you cannot underestimate the importance of a qualified attorney to advise you on compliance, crisis management and contingency planning. Although these expenses are increasing, they are necessary,” Diamond says.

Malicious breaches by **rogue employees**—due to firings, downsizing, generally poor economic conditions or the relative ease of selling stolen information—are another growing area. Our findings show rogue employees to be the second largest cause of breaches, comprising 19 percent of breach events.

“33% of our reported data breach incidents arose from lost or stolen items like laptops, backup tapes, USB drives and smart-phones – with another 7% arising from lost paper documents. ...”

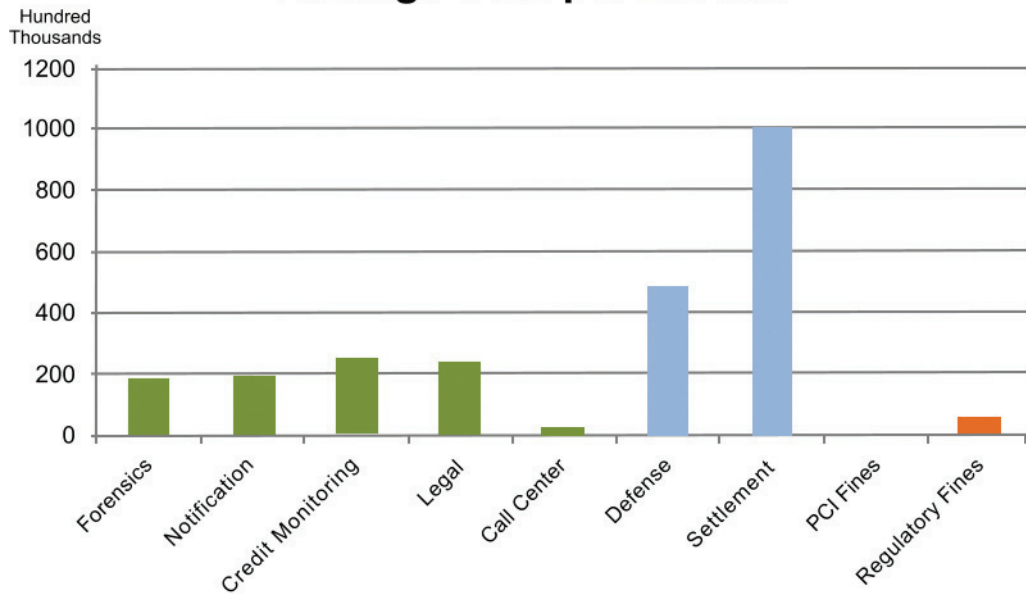
Lastly, **loss or theft** is right at the top of the list. According to Meredith Schnur, Vice President, Professional Risk Group, Wells Fargo Insurance Services, “In the last six months, we’ve had six to ten data breach claims reported from lost thumb drives, missing laptops and missing hard copy reports.” Lost or stolen equipment made up 15 percent of data breach incidents in our sampling and accounted for 10 percent of all personal records exposed. Noting slightly more frequency in this category was Richard Sheridan, a Vice President of Professional Liability Claims for ACE, who noted, “33% of our reported data breach incidents arose from lost or stolen items like laptops, backup tapes, USB drives and smartphones – with another 7% arising from lost paper documents. This demonstrates that many of these incidents are not protected by firewalls and require additional physical controls as well.”



Business Sectors Affected

More than 60 percent of breaches in our sampling occurred in **financial services, healthcare** and **retail**. A full 88 percent (122 million) of records exposed occurred in financial services alone. Costs across business sectors were fairly spread between crisis services, legal damages and first-party losses. However, the average cost for legal damages in these incidents was significantly higher than the average cost for crisis services. Average expenses per breach for crisis services were about \$200,000 per service (forensics, notification, credit monitoring, and legal counsel), while legal damages ranged between \$450,000 and \$1,000,000.

Average Cost per Breach





Conclusion

Despite increasing awareness around cyber security and the increasing frequency of data breach events, it has been difficult to assess the cost to companies when such incidents occur, due to the lack of hard data on the subject. This study lays the groundwork for risk management professionals and insurance underwriters to understand the true impact of data insecurity.

An empirical look at actual data breach events that occurred between 2005 and 2010 in organizations that had cyber or privacy liability coverage reveals that companies spent on average \$2.4 million per event. The healthcare, financial and retail sectors and records containing PII, PHI and credit card information were most at risk, with hackers and rogue employees and contractors responsible for the majority of data loss.

While this small sample covers only 77 data breach incidents in that five-year span, it demonstrates the areas where companies can better focus their cyber risk management practices and use these findings to guide the development of their data breach policies and action plans to guard against these events in the future.



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 'backer insurance' product.



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