Data Breach Cost

Part one: risks, costs and mitigation strategies for data breaches
Data Breaches: Greater frequency, greater costs for all companies

Part one of a two-part series on the risks, costs and mitigation strategies for data breaches

Cyber attacks make the news almost weekly these days, especially when they hit global credit card companies and banks, major retailers, high-tech leaders, and even federal government agencies. Increasingly, the data of small and middle-sized businesses is also being hacked. “In 2010, the U.S. Secret Service and Verizon Communication Inc.’s forensic analysis unit, which investigates cyber attacks, reported 761 data breach cases, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer. Visa also estimates that about 95% of the credit-card data breaches it discovers are on its smallest business customers.”1

At this year’s World Economic Forum in Davos, Switzerland, cyber security was included as one of the top five global risks for companies in 2011.2 The Forum’s report cited a plethora of new hacker opportunities including corporate espionage, the increase in the use of cloud computing, and mobile device use, all of which can make corporate data more vulnerable to attack. The panel of leading cyber specialists at the Forum also noted that despite the looming cyber threats, many senior managers remain in denial.3

Privacy regulations have been enacted at the Federal and State level in an effort to protect customers from these cyber threats. Regulators are now giving extra scrutiny to a company’s response to a breach, as well as the risk management measures in place prior to the breach. In addition, consumers’ expectations of their personal privacy rights have increased as they become more educated about privacy laws and acceptable practices. Given these factors, data breaches that result in the wrongful disclosure of personally identifiable information of customers or employees can have a particularly significant impact on a company’s bottom line. Companies should prepare themselves for the direct costs, as well as the indirect costs, of a data breach scenario.

Financial exposures to a breach

The costs and expenses of a data breach can be wide ranging. According to the 2010 Annual Study: US Cost of a Data Breach conducted by the Ponemon Institute, the average cost of a data breach in 2010 was $7.2 million.4 Although each breach has its own set of unique factors, the financial impact is fairly consistent across each of them.

The following are expenses a company may incur when a data breach results in the loss or theft of third party information:

1) Forensic Examination

This examination determines the severity and scope of a breach involving compromised computer systems or networks. It is considered a crucial step in the process, as companies that act too quickly to publicly disclose details of a data breach may actually worsen the situation and suffer additional long-term costs. According to the 2010 Ponemon report on data breach costs, companies that responded with quick notification ended up paying an average of $268 per record compared to the average of $174 per record by companies that took the appropriate time to analyze the event. In addition, there have also been cases

---

Case study: Consumer information theft

A company specializing in consumer information aggregation suffered a data breach that resulted in the theft of almost 100,000 Social Security numbers. The Federal Trade Commission (FTC) launched an investigation against the company alleging unfair and deceptive trade practices. The FTC found that the company did not have basic security measures in place at the time of the breach, despite the advertisements on its website and contents of its privacy policy that described robust and sophisticated information security management practices. The company was fined $500,000 and required to implement a Comprehensive Written Information Security Program that was subject to audit for 10 years.
Data breach costs: part one of two

1) Forensic Exams

A forensics exam can be performed either by a company’s internal staff or an outsourced third party. However, internal investigations can inadvertently lead to destroyed evidence or questionable authentication, so third parties are typically engaged to ensure quality and maintain objectivity. The costs of a forensics exam may vary greatly, but generally, firms charge on a fee basis with average fees ranging from $200 to $2000 per hour. The cost of engaging a third party forensics firm is typically covered under most network risk policies.

2) Notification of Third Parties

Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted data breach notification laws. The state laws require companies or individuals that maintain unique personally identifiable information of individuals to notify those individuals if such information is lost, stolen or otherwise compromised. Beyond the legal requirement, many companies believe it is good business practice to notify affected individuals in the event of a breach.

While the basic purpose of each state notification law is similar, differences arise in the specific process required such as the use of U.S. Postal Service, certified mail, or other special delivery. A breached company will need to review each state’s specific requirements, which is a time consuming and costly process on its own. Many companies hire third party law firms or consultants to assist in determining applicability of state notification laws after a breach has occurred.

Additionally, Massachusetts and other states have adopted “compliance” models that allow for less stringent reporting requirements when specific security measures such as encryption are in place at the time of the breach. One of the goals behind this approach is to encourage companies to take proactive steps to protect personal information.

Notification costs can vary depending on the number of records or individuals affected. A scaled approach is common with the charge per notice gradually decreasing as the number of records or individuals increases. Charges can range from $.50 to $5 per notice.

The direct costs associated with determining applicability of state notification laws and actual notification of affected third parties is typically covered under most network risk insurance policies. The costs associated with implementing proactive risk management procedures to mitigate the impact of a breach before it occurs, however, are not.

3) Call Centers

Companies consider it a customer service best practice to include a phone number in the notification letters for affected individuals wanting more information about the extent of the breach, the company’s response, or next steps. Depending on the severity and scope of a breach, a company’s internal call center may not have the capacity to handle a significant increase in the volume of calls. Companies often hire third party vendors that specialize in comprehensive breach response to provide call center services. Costs are typically calculated by call volume, number of weeks or months the center will be dedicated to fielding questions, as well as hours available (24/7 versus normal business hours).

4) Credit or Identity Monitoring

While credit or identity monitoring is not required by most state notification laws, many companies believe that providing this service maintains good customer relationships. Consequently, credit and identity monitoring has become a
Data breach costs: part one of two

standard element of a comprehensive beach response. While credit monitoring services are focused primarily on financial elements like credit history and account activity, identity monitoring goes further by tracking activities relative to medical, employment, and other types of fraud. One service may be more appropriate than the other depending on the type of information compromised during a breach.

Identity restoration is an additional service that can be requested by affected parties if they do suffer actual identity theft. Combined costs for credit monitoring, identity monitoring, and restoration can range from $10 to $30 per individual per year. The costs can add up very quickly when you consider that one breach can compromise thousands or even millions of records.

5) Public Relations

A company may engage an external PR firm that specializes in damage control to help mitigate harm to its reputation caused by a data breach. The direct cost of obtaining a PR firm is covered under most network risk policies, but the indirect adverse impact on the company is largely uninsurable. According to the 2010 Ponemon Study, the average cost of a data breach is $214 per record with $141 of that amount attributed to decreased stock price and customer churn. The remaining $73 was a result of direct costs such as notification, credit monitoring, defense, forensics, call center services, and PR consultation fees. The more concerning issue associated with the Public Relations aspect of a data breach is the potential long-term loss of confidence among customers and business partners, which in turn can impact sales and revenue.

6) Legal Defense

Claims from a data breach can come from a number of parties, but most frequently from consumers and banks. Defending these claims results in legal defense expenses in addition to the actual cost of settlements. According to the NetDiligence Cyber Liability and Data Breach Insurance Claims Study, legal damages represented the single largest component of costs paid by insurance carriers who participated in the survey. The average cost for legal defense was $500,000 while the average legal settlement was $1 million.

Consumers whose personally identifiable information has been compromised as a result of a breach may file suits alleging a number of violations including:

- Negligence
- Breach of warranty
- Failure to protect data
- Failure to disclose defects in products or services regarding capabilities of protecting data
- Unreasonable delay in remedying suspension of service or loss of data
- Violations of various applicable state/federal laws
- False advertising
- Unfair or deceptive trade practices

Consumer claims are typically filed as class action lawsuits, but tend to have limited success given the difficulty in proving injury in the absence of actual identity theft. However, new legal theories continue to evolve and so may the outcome of such claims. While it is uncertain whether consumers may successfully prove damages, it is certain that the breached company will face significant costs in hiring legal counsel to defend itself.

Case study: Pilfered health information

A hospital employee left a physical file on public transportation while traveling home from work. The file contained highly sensitive protected health information including names, birthdates, and medical record numbers, and medical conditions of patients. The hospital incurred costs of notifying the patients along with legal defense costs from patient claims. The U.S. Department of Health and Human Services also levied a fine of $500,000 for violation of the Privacy Rule under the Health Insurance Portability and Accountability Act (HIPPA). As part of the settlement, the hospital was also required to implement a more robust risk management program to prevent future breaches.
Banks that issue payment cards have also sought damages from the breached company for the costs of reissuing cards that were compromised during the breach. It is estimated that a bank may pay between $12 and $22 to reissue a single payment card.\(^5\) The costs of this card reissuance is one of the reasons banks have been successful in recouping this expense from retailers or other breached organizations. Certain states, like Washington and Minnesota, have even passed legislation that makes a payment card processor or business liable if reasonable steps were not taken to protect against unauthorized access to the account information that leads to the loss of such information.

Issues can also occur relative to a company’s service offering. An organization with business customers may experience errors and omissions (E&O) claims that allege negligence in professional services after a data breach. For example, consider an IT service provider that needs to disable key security functionality for several hours during a network upgrade to a third party. During that installation, a malicious third party could gain entry to the network and download a cache of personally identifiable information from company’s customer database. The customer company may pursue legal action against the service provider alleging negligence in technology services that lead to the breach, and seek damages for costs incurred including notification, credit monitoring of third parties, forensics, and other expenses.

### 7) Regulatory Proceedings, Fines and Penalties

Increased scrutiny by the federal and state government is affecting all companies, but particularly health care and financial services firms due to the sensitive and personal nature of the information they handle. Depending on the nature of the data breach, a company may have to defend itself against investigations launched by applicable federal or state authorities, such as the Federal Trade Commission or state attorneys general. A company that experiences a breach may also be subject to fines and penalties if found to be non-compliant with basic requirements which, in many cases, are self imposed.

One example of a Federal law is the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPPA), which outlines basic requirements for healthcare organizations regarding the handling of Protected Health Information. As part of the American Recovery and Reinvestment Act of 2009 (ARRA), the Health Information Technology for Economic and Clinical Health Act (HITECH) established a tiered civil penalty structure for HIPAA violations. Fines can range from $100 per violation to a maximum of $1.5 million. The Department of Health and Human Services has already fined several entities as a result of violations of the Privacy Rule.

After a breach, transparency will typically foster good will between the company and the regulator. However, the costs of an investigation remain significant given the need for specialized counsel and the cost of potential fines or penalties. Fines and penalties may or may not be insurable depending on jurisdiction and the actions of the company.

In addition to government regulatory bodies, there are also non-government entities that set best practice standards and have the ability to levy fines and penalties. One such entity is the Payment Card Industry Security Standards Council that was established by the major payment card brands in 2006. The Council established the Payment Card Industry Data Security Standard as a uniform best practice requirement for any company that processes, stores or transmits credit card information. The Council engages third party vendors to assess compliance levels of organizations subject to the standard and has the ability to levy fines against organizations that do not comply. Fines can range from $5,000 to $100,000 per month for PCI compliance violations.
8) Comprehensive Written Information Security Program
An ongoing trend around regulatory settlements has been the requirement that the breached company implement a Comprehensive Written Information Security Program. These programs usually accompany a fine or penalty and are subject to periodic audits conducted by the enforcing body. Audits can continue over the course of several years, and the costs include both the fine itself as well as the cost to implement the program through reallocation of existing human capital or in direct costs incurred in retaining an outside firm if internal resources are not available.

While the potential costs associated with a data breach can add up rapidly, there are a number of steps a company can take to lessen the financial blow should one occur. The harsh reality is that a company cannot ever completely avoid the potential for a breach, so risk assessment and response preparation should be a priority for every risk manager. In Part 2 of this data breach series, we will look at the elements of an effective information security risk management program, including how to help protect your digital assets and bottom line using available insurance solutions.

<table>
<thead>
<tr>
<th>Breach Response</th>
<th>Cost Implications</th>
<th>Coverage Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic Examination</td>
<td>Average fees can range from $200 to $1500 per hour for reputable firms.</td>
<td>The cost of obtaining a third party forensics firm is covered under most network risk policies.</td>
</tr>
<tr>
<td>Notification of Affected Third-parties</td>
<td>Cost of mailings; hiring of attorneys, etc.</td>
<td>Covered by most network risk insurance policies.</td>
</tr>
<tr>
<td>Call Centers</td>
<td>Costs are usually calculated by call volume and length of time the center will be dedicated to fielding questions and providing information.</td>
<td>Typically covered under a network risk policy.</td>
</tr>
<tr>
<td>Credit/Identity Monitoring</td>
<td>Typical credit monitoring costs can range from $10-$30 per individual per year.</td>
<td>Identity Monitoring and Identity Restoration are covered by a limited number of policies in the market.</td>
</tr>
<tr>
<td>Public Relations</td>
<td>Loss of corporate reputation, which is incalculable</td>
<td>The direct cost of obtaining a PR firm is covered under most network risk policies</td>
</tr>
<tr>
<td>Legal Defense</td>
<td>Defense costs</td>
<td>Coverage for Legal Defense costs and Indemnity payments to third parties is available under Cyber Risk policies</td>
</tr>
<tr>
<td>Fines and Penalties from Regulatory Proceedings and PCI DSS violations</td>
<td>Fines vary from $100 to $1 million+</td>
<td>Coverage for general Fines and Penalties is available from some markets, however, insurability varies depending on jurisdiction and circumstances. Defense of a regulatory investigation/proceeding is typically covered under most policies.</td>
</tr>
<tr>
<td>Comprehensive Written Information Security Program</td>
<td>Audits may be required over a period of several years</td>
<td>Typically not covered by cyber policies</td>
</tr>
</tbody>
</table>
**Case study: Small bank data heist**

A community bank's backup data tapes were stolen from a vendor's truck while in transit to a storage location. The data tapes contained customer names, social security numbers, account numbers, and other sensitive information. The bank ended up paying the costs of notifying and providing identity theft monitoring to 90,000 potentially affected customers.

References

1. “Hackers Shift Attacks to Small Firms”, *Wall Street Journal*  
   online.wsj.com/article/SB10001424052702304567604576454173706460768.html

2. “Cybersecurity named one of top five global threats”  
   www.homelandsecuritynewswire.com/cybersecurity-named-one-top-five-global-threats

3. “Industries under Cybersiege: Time for Action” World Economic Forum Report,  
   January 29, 2011

4. “2010 Annual Study: US Cost of a Data Breach”, Ponemon Institute,  
   www.ponemon.org


6. Digital Transactions “Mass Reissuance May be Overkill in Merchant Breach Cases”  