



ANATOMY of a DATA BREACH **DISASTER**

Avoiding a Cyber Catastrophe

June, 2011

Sponsored by:



ANATOMY of a DATA BREACH DISASTER

Avoiding a Cyber Catastrophe

An Advisen Special Report Sponsored by Chartis

Security incidents in which information is released to or accessed by unauthorized individuals, known as “data breaches,” are occurring with alarming frequency. A data protection research firm estimates that nearly 90 percent of U.S. organizations have experienced at least one data breach over the twelve month period spanning 2009 through 2010.¹ Even if a breach does not result in serious damage to an organization or its customers, data breach



notification laws in 46 states may nonetheless require disclosure. This requirement may then set into motion an elaborate chain of potentially expensive activities including notifying affected individuals, providing credit monitoring services, and undertaking damage control measures to protect the organization’s reputation.

Catastrophic and potentially ruinous breaches are becoming more common. What may begin as an investigation into a seemingly manageable security problem sometimes mushrooms into a disaster, with skyrocketing notification, monitoring, remediation and reputational damage costs, as well as fines, and penalties. Such a breach has the potential for tens, or even hundreds, of millions of dollars in litigation and related costs. Additionally, a data breach may lead to lost business, especially for companies where the bond of trust with clients is a key component to doing business.

The three most expensive data breaches known to date are:

- A credit card processing company had more than 130 million digital records stolen from its database. Cyber criminals employed software that compromised credit card data which crossed the company’s network. The company incurred expenses of nearly \$150 million, of which approximately three quarters was related to settlement of claims, with the remainder attributable to investigating and defending various claims

Companies can take practical steps to limit their exposure to potentially catastrophic data breaches.

and actions, remedial actions, and crisis management services. The company continues to face numerous consumer and financial institution putative class action suits.

- A major clothing and home goods retailer experienced an intrusion into its computer systems that process and store customer transactions including credit card, debit card, check, and merchandise return transactions. Information pertaining to more than 45 million credit and debit cards was stolen. Through fiscal year 2010, the company had incurred expenses of more than \$170 million for claims and costs related to the intrusion.
- In 2005, criminals pretending to be legitimate customers of a data broker acquired personal information of more than 160,000 individuals listed in the company's database. As of 2008, the company had recorded more than \$33 million in expenses related to the incident.

Companies can take practical steps to limit their exposure to data breaches. Increasingly, data security is recognized as not exclusively an IT Department concern, but a risk management function that extends throughout the organization. However, despite the most effective controls, data breaches may occur and companies need to be prepared to deal with them quickly and effectively. Rapid action following a breach will not only help reduce financial losses, it may also prevent damage to a company's reputation. Additionally, to mitigate the risk posed by a data breach, companies need to realistically assess their exposure and purchase appropriate limits of insurance coverage.

The Costs of Large Data Breaches

Research has shown that data breach costs tend to be linear: the more records compromised, the greater the costs. Expenses associated with a large data breach include:

- Detection, escalation, notification, and response;
- Lost business;
- Fines and penalties;
- Restitution;
- Lost productivity;
- Additional security and audit requirements; and
- Miscellaneous additional costs.

Detection, escalation, notification, and response. A sophisticated attack by a hacker may take months to uncover, after which, the full extent of the damage may not be known for several additional months. Once a breach is discovered, affected parties must be notified

Certain types of organizations are more vulnerable to reputational risk – and consequently lost business – as a result of a data breach

and steps must be taken to mitigate the damage. Repairing a breach can be expensive and may involve hiring a forensic expert to discover the source of an intrusion. Discovery, notification, and response costs following a breach have been estimated by Forrester Research to average about \$50 per record.²

Lost business. Business can be lost both as a result of customer attrition as well as difficulty in attracting new customers. Lost business is the largest component of the average data breach loss, comprising 63 percent of the total loss, according to the Ponemon Institute, LLC, a data security research firm.³ Certain types of organizations are more vulnerable to reputational risk – and consequently lost business – as a result of a data breach. Companies in the financial service and healthcare sectors, where trust and security are cornerstones of the business relationship, are especially vulnerable to damaged reputations as a result of a data breach.

Fines and penalties. Fines and penalties can come from a number of sources. Various federal and state privacy laws impose significant fines for violations. The Health Insurance Portability and Accountability Act (HIPAA), for example, calls for penalties of up to \$50,000 per violation of its privacy provisions.

The enforcement of many federal data security and privacy laws falls to the Federal Trade Commission (FTC). For example, the data broker described above paid \$10 million to the FTC to settle charges that its security and record-handling procedures violated consumers' privacy rights and various federal laws, including the Fair Credit Reporting Act.

The major credit card brands also levy potentially significant fines for violations of their security standards. These companies are members of the Payment Card Industry Security Standard Council, which has created a security standard known as the Payment Card Industry Data Security Standard (PCI DSS). Compliance with this standard forms part of the agreement signed by merchants who accept members' credit or debit cards.

Restitution. Individuals and businesses that claim to have been damaged as a result of a data breach often seek restitution. However, the claimants' success in litigating these types of cases is far from certain. For instance, a Massachusetts Supreme Court decision, rejected most of the standard legal theories used by banks to attempt to recover card reissuance costs. However, legislation has been passed in three states, Washington, Nevada, and Minnesota, which now explicitly holds organizations responsible to financial institutions for certain costs arising from payment card information breaches. Under the Washington legislation, businesses that process more than 6 million credit or debit card transactions annually, and which fail to reasonably safeguard card information, may be required to reimburse financial

institutions for costs related to the reissuance of cards as well as attorneys' fees in the event of a payment card security breach.

Individuals whose personal information is stolen sometimes sue the company subject to the breach, typically via class action lawsuits. Settlement amounts in such cases can be very high. As a result of the incident described above involving the credit card processing company, the company agreed to a settlement whereby consumers were able to make claims for out-of-pocket expenses related to card cancellations or replacements, as well as up to \$10,000 if their identity had been stolen as a result of the breach. This breach involved more than 130 million records.

In many instances, however, legal experts note that courts commonly reject data breach claims brought by persons who did not suffer any meaningful injury. Merely having one's personal information lost or stolen typically is not sufficient – the plaintiff must have actually suffered a loss in order to be awarded damages.

Companies experiencing a data breach may deem it necessary to implement enhanced monitoring and auditing protocols

Companies experiencing data breaches that result in a material impact on share price may also be targeted for securities class action lawsuits. As a result of the breach, the data broker was sued by shareholders who alleged that the company violated federal securities laws by issuing false or misleading information in connection with the fraudulent data access. Without admitting liability, the company agreed to a \$10 million settlement.

Lost productivity. While difficult to quantify, lost productivity can be a very real cost of a data breach. Depending on the nature of the breach, IT personnel may be pulled off of other projects to identify the source of a breach and fix it. Employees will be tasked with identifying affected businesses and individuals, notifying them, and responding to questions. Lawyers will often spend a significant amount of time working with regulators and law enforcement agencies. Senior management's time is perhaps the most significant area of loss productivity following a large breach: an event that threatens the reputation of a company can become nearly all-consuming for a significant period of time.

Additional audit and security requirements. Companies experiencing a data breach may deem it necessary to implement enhanced monitoring and auditing protocols. The FTC and other regulatory agencies may require heightened security measures and audits as conditions of a settlement. A shoe retailer, for example, agreed as part of a settlement with the FTC concerning a 2005 breach to maintain a comprehensive information security program, and to undergo a bi-annual assessment of that program by an independent auditor. If credit card information is lost a forensic audit at the company's expense most likely will be required by PCI DSS, and subsequent additional audits may be necessary.

Miscellaneous additional costs. Additional costs arising from a data breach can include attorney fees, consultant fees, and various settlement costs. As a result of a 2007 data breach, a check authorization company, for example, agreed to donate \$125,000 to the Florida attorney general's Seniors vs. Crime Program for educational, investigative, and crime prevention programs and to also pay \$850,000 for the state's investigative costs in settlement of the lawsuit brought by the attorney general's office.

The makings of a data breach disaster

Sometimes a data breach spirals out of control, and ultimately can cost a company tens of millions – even hundreds of millions – of dollars

Consulting firm Forrester Research estimates that the average cost of a U.S. data breach involving sensitive data is \$14 million.⁴ According to Forrester, the costs of a data breach vary widely, ranging from \$90 to \$305 per customer record. The differences in cost depend on whether the breach is “low-profile” or “high-profile” and whether the company is in a non-regulated or regulated area, such as banking.

Sometimes a data breach spirals out of control, and ultimately can cost a company tens of millions – even hundreds of millions – of dollars. The most expensive breaches have common factors:

- Credit Information;
- A large number of records;
- Criminal intent;
- Delayed discovery; and
- Lack of compliance.

Credit information. A breach compromising medical records, for example, may violate HIPAA privacy requirements and cause distress to those affected, but the actual monetary damages are usually comparatively small. The loss of banking or credit-related information, on the other hand, can be disastrous.

Most of the largest breaches involve credit card records. Companies handling credit card information, both vendors and credit card processing companies, are enticing targets for criminals because they often handle a large number of transactions and, despite rigid credit card security standards, sometimes employ security and control measures that can be compromised.

Credit card brand managers have been aggressive in pursuing restitution following large breaches. For example, the clothing and home goods retailer previously described, paid about \$65 million in settlements with two of the largest credit card brands to help credit card

In most large data security incidents, the victim was not in compliance with PCI DSS, or with various privacy and security laws

issuers such as banks recover costs related to the breach. Breaches involving credit cards also may be subject to large penalties for non-compliance with security standards.

A large number of records. Within a given category of record – credit card records versus medical records, for example – the size of the loss tends to be more-or-less linear: the more records involved, the greater the ultimate loss. Historically, the largest losses have typically involved millions of records. There are, however, notable exceptions. The incident concerning the data broker involved 163,000 records, but ranks among the most costly of all times. Nearly one-third of the reported losses were the result of penalties levied by the Federal Trade Commission.

Criminal intent. While a significant number of data breach incidents result from accidents, such as lost laptops and internal errors, the most costly data security incidents have resulted from criminals specifically targeting companies. One hacker, Albert Gonzalez, and two associates were implicated in three of the largest data breach incidents. Gonzalez and his associates also allegedly compromised cards at a number of major retailers. According to The 2010 Verizon Data Breach Investigations Report, produced by Verizon in collaboration with the U.S. Secret Service, organized crime was responsible for 85 percent of all stolen data in the incidents they investigated in 2009.⁵

Delayed discovery. According to the Verizon study “organizations remain sluggish in detecting and responding to incidents. Most breaches are discovered by external parties and only then after a considerable amount of time.”⁶

The breach at the credit card processing company occurred over a period of 14 months. Intruders spent nearly six months attempting to access the company’s processing network, bypassing different anti-virus packages it used. The company took notice only after being notified by credit card companies of suspicious transactions. A large breach at a grocery chain occurred over roughly a four month period, and the breach at the clothing and home goods retailer took place over approximately five months.

When discovery is not immediate, criminals continue to accumulate records and to make use of the stolen credit card information – typically selling it to others.

Lack of compliance. In most large data security incidents, the victim was not in compliance with PCI DSS, or with various privacy and security laws. The data broker, for example, paid \$10 million to the FTC to settle charges that its security and record-handling procedures violated consumers’ privacy rights and federal laws such as the Fair Credit Reporting Act. Documents filed by banks suing in regard to the matter concerning the clothing and home goods retailer allege that the company was not in compliance with most of the security controls mandated by PCI DSS when the breach occurred.

Avoiding a data breach disaster

There is no way to guarantee that a company will not fall victim to clever and determined hackers. Criminals tend to look for weaker victims, however, and they are likely to look elsewhere if they encounter a well-fortified system. The Verizon study notes that “most breaches could have been avoided without difficult or expensive controls.” Verizon recommends seven basic steps for improved security:

- Eliminate unnecessary data; keep tabs on what’s left;
- Ensure essential controls are met;
- Check the above again;
- Test and review web applications;
- Audit user accounts and monitor privileged activity;
- Filter outbound traffic; and
- Monitor and mine event logs.⁷

Companies increasingly recognize that risk management practices alone are not sufficient protection. Despite best efforts at data security, things can go wrong, and sometimes, horribly wrong.

Being prepared to move quickly and effectively following the discovery of a breach is often essential to keeping a problem from escalating. Companies almost always fare better when following a well-conceived plan rather than scrambling to respond after a data breach has occurred.

Some post-breach activities are prescribed by law. Notification laws require businesses, non-profit organizations, and state institutions to notify consumers when personal information may have been compromised, lost or stolen. Forty-six states, D.C., Puerto Rico, and the U.S. Virgin Islands have enacted such consumer notification laws.

For any loss of sensitive records, once a breach has been discovered and the appropriate people within the organization have been notified, an effective response typically includes the following steps:

- Identify and fix the cause of the breach. The timing and method of the fix will depend upon the nature of the breach (e.g., a system is hacked versus implementing more robust laptop security protocols);
- Notify law enforcement officials;
- Notify critical vendors and business partners;

- Notify the cyber liability insurer and activate coverages for remediation or damage control activities, including hiring a damage control specialist or a public relations firm;
- Notify regulatory agencies (e.g., Department of Health and Humans Services for a health information breach), if required;
- Notify data loss subjects;
- Notify other stakeholders such as investors; and
- Implement activities such as credit report monitoring services to mitigate potential future harm.

Quickly and effectively communicating with customers and other stakeholders is an important step to mitigating damage. Working within the requirements of the applicable laws, senior management should make informed strategic decisions about when and how notification takes place. According to the Ponemon Institute, notifying customers too quickly, that is, before all of the facts are known, may result in larger losses.

Data breach insurance coverage

While robust data security can help avoid breaches, and emergency preparedness can lead to an effective response should one happen, insurance coverage remains essential.

Coverage of data breaches under traditional Commercial General Liability and various types of Errors & Omissions policies is available, but most likely for limited circumstances. The insurance industry has responded in recent years to the exposures presented by data breaches by introducing cyber liability policies tailored especially to computer-related risks. In addition to coverage related to data security, most cyber liability policies cover other risks associated with conducting business digitally.

Data breach coverage typically is provided in three parts: first-party; third-party; and coverage for related issues. First-party coverage is for direct losses incurred by the insured as a result of a data breach, such as recovering lost and destroyed data, forensic investigation expenses, business interruption losses, and extortion demands. First-party coverage may also include notification costs, credit monitoring services, call center services, and expenses for emergency public relations services. For these first party coverages, many carriers apply sublimits that can substantially decrease the available coverage.

Third-party coverage insures policyholders against liability to entities such as customers, credit card companies, and banks. Coverage extends to both defense costs and damages

in civil lawsuits. Policy forms are typically divided into two sections as respects third-party coverage: privacy and network security.

Because technology changes rapidly, insurance buyers should routinely check their policy forms to ensure that their coverage and limits are appropriate for their exposure. In the not-too-distant past, coverage varied widely from insurer to insurer, and most insurers offered only modest policy limits. More recently, as coverages have become more standardized and the exposures better understood, primary limits have increased and an excess cyber liability market has emerged, permitting companies to readily access tens of millions of dollars of capacity. Coverage is generally broader today than it was a few years ago, but insurance buyers and their brokers nonetheless need to carefully review policy terms to understand the full extent of coverage. ■

1. *2010 Annual Study: U.S. Enterprise Encryption Trends*, Poneman Institute, LLC, sponsored by Symantec, November 2010, p. 5.
2. Larry Dignan, "What that data breach will really cost you," ZDNet, May 8, 2007 <http://www.zdnet.com/blog/btl/what-that-data-breach-will-really-cost-you/5007>.
3. *2010 Annual Study: U.S. Cost of a Data Breach*, Ponemon Institute, LLC, sponsored by Symantec, March 2011, p. 5.
4. Forrester Research, "Calculating the Cost of a Security Breach," cited in Sharon Gaudin, "Security Breaches Cost \$90 To \$305 Per Lost Record," InformationWeek, April 11, 2007, <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199000222>.
5. *The 2010 Verizon Data Breach Investigations Report*, Verizon Risk Team in collaboration with the U.S. Secret Service, p. 15.
6. *The 2010 Verizon Data Breach Investigations Report*, Verizon Risk Team in collaboration with the U.S. Secret Service, p. 3.
7. Verizon, p. 3.

ABOUT CHARTIS

Chartis is a world leading property-casualty and general insurance organization serving more than 70 million clients around the world. With one of the industry's most extensive ranges of products and services, deep claims expertise and excellent financial strength, Chartis enables its commercial and personal insurance clients alike to manage virtually any risk with confidence.

Chartis is the marketing name for the worldwide property-casualty and general insurance operations of Chartis Inc. For additional information, **please visit our website at <http://www.chartisinsurance.com>**. All products are written by insurance company subsidiaries or affiliates of Chartis Inc. Coverage may not be available in all jurisdictions and is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain coverage may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.

ABOUT ADVISEN

Advisen's data, analytics and news offerings are game-changers for 100,000 commercial P&C professionals. For Underwriters, Reinsurers, Brokers and Risk Managers, the resources of Advisen provide productivity and insight into underwriting, marketing, broking and purchasing commercial insurance. Configurable applications allow Advisen to customize each solution and/or craft special offline delivery, too. Our result is a measurable increase in your book of business and more favorable insurance transactions. **Visit us at www.advisen.com or contact support@advisen.com** to learn more.

