



Complete. On Demand. Affordable.

A Comprehensive Study of Financial Data Security Breaches in the United States - 2008

Kevin Prince
Chief Technology Officer
Perimeter eSecurity

TABLE OF CONTENTS

Abstract.....	3
What is a Data Security Breach?.....	3
Regulations.....	4
Data Breach Disclosure Laws.....	6
What is Personal Information?.....	6
Notification Procedures.....	7
Notification Timelines.....	7
Exceptions.....	7
The Security Breach Disclosure Bandwagon.....	8
National Data Breach Notification Law.....	9
Data Security Breach Trending.....	11
Types of Data.....	13
Data Breaches by Business Type.....	14
Data Compromise Categories.....	15
Data Breach Sources.....	16
Data Location at the Time of Breach.....	18
Security Breach Impact on Public Companies.....	19
Security Breach Impact on Small Companies.....	21
Cost of a Security Breach.....	21
Record Format at the Time of Breach.....	23
Heartland Payment Systems Case Summary.....	23
Conclusion.....	24
Appendix A - Chronological list of known U.S. financial service companies data security breaches between 2000-2008.....	25

New laws and regulations regarding data security breaches and disclosure laws affect the way in which financial institutions do business. This study provides a review of the scope and impact of data security breaches in the financial industry in an effort to encourage proactive modification to risk mitigation technologies, policies, and procedures that reduce exposure to a data breach incident.

The data breaches mentioned in this report exposed personal information that is useful to identity thieves for unlawful purposes. This information could include Social Security numbers, account numbers, and driver's license numbers. Some breaches that did not expose sensitive information have been included to underscore the variety and frequency of data breaches. The breaches include only those reported in the United States.

WHAT IS A DATA SECURITY BREACH?

Nearly all organizations maintain records of their customers and employees. A data breach occurs when that information falls into the wrong hands, is extracted, viewed, exposed to, or captured by an unauthorized individual. The following are some examples of data breaches that have happened in just the past few years:

- Hacker compromises a firewall and downloads patient information from a database server
- Employee information not properly disposed (thrown into a dumpster or not shredded)
- Sensitive data transmitted via e-mail to unauthorized users
- Malicious employee copies data to a thumb drive and takes it home
- Laptop with unencrypted customer or employee data is stolen
- Untrained employee inadvertently posts sensitive information to a public forum or Web site.

According to laws in over 45 states, when a data security breach occurs, notification must be made to the affected individuals. Depending upon the size and scope of the breach, notification can be handled in a variety of ways, including by mail, telephone, e-mail, or through the news media.¹ According to a survey taken at a recent RSA conference, only 11% of companies disclosed security breaches that occurred in 2008.² Therefore, the number of breaches we know about and can be analyzed in this study are a small percentage of all data breaches.

Key Finding: Only 11% of companies reported security data breaches in 2008

When a data security breach is discovered and subsequent notifications are made, some organizations maintain records of those breaches,³ whereas others take the data and correlate it, add to it, and present findings.⁴ The data captured varies based on the organization that collects it. Some only capture data

¹ Additional Information on Page 7

² http://www.darkreading.com/document.asp?doc_id=160591&f_src=drdaily

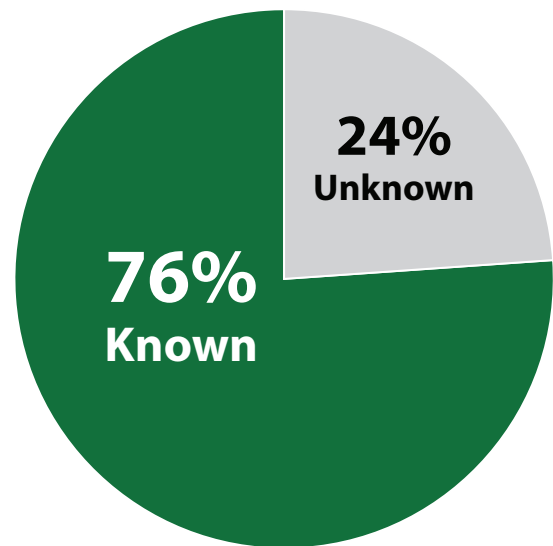
³ <http://www.datalossdb.org/>; <http://www.privacyrights.org/>; <http://www.idtheftcenter.org/>;

⁴ <http://www.atthebreach.com>

Figure 1: Number of Records Known vs. Unknown

for U.S.-based security breaches; others cover the globe. Most capture the name of the organization and number of records compromised. Some capture vertical, breach type, data type, and other interesting data.

Often, the exact number of compromised records or number of affected individuals is unknown, making it difficult to quantify security breaches. The following chart illustrates all 1,258 publicly disclosed data breaches in the U.S. between 2000 and 2008, where nearly one-quarter of respondents reporting incidents did not or could not disclose the number of records that were part of their data breach.



Statistics, charts and graphs displayed in this study are based on the 76% of incidents where the number of records compromised was disclosed.

Key Finding: 24% of disclosed data breaches in the U.S. either do not know, or do not specify the number of records compromised.

An attempt was made in this study to look up the number of compromised records in cases where that information had not been disclosed. There were a few cases where additional data was available. We discovered a total of 14 records compromised in one case, while 1.1 million records were part of another incident. This illustrates the diversity of these types of incidents. The 24% that is unknown could account for little in the number of total records lost, or it could be the equivalent of many multiples of the 76% we know about.

REGULATIONS

Gramm-Leach-Bliley Act (GLBA)

The 1999 Gramm-Leach-Bliley Act (GLBA) requires financial institutions to develop, implement, and maintain a comprehensive written information security program that protects the privacy and integrity of customer records. The Federal Financial Institution Examination Council (FFIEC) recently updated the GLBA information security standards. These new mandates emphasize the need for each bank, thrift, and credit union agency to adopt a proactive information security and technology risk management capability. By doing so, your institution can protect information, applications, databases, and the network as part of a comprehensive information security program.

Gramm-Leach-Bliley Bill Section 501(b) reads:

FINANCIAL INSTITUTIONS SAFEGUARDS. In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards

1. to insure the security and confidentiality of customer records and information
2. to protect against any anticipated threats or hazards to the security or integrity of such records
3. to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

Examination procedures have been written to help a financial services company achieve compliance. According to one examination handbook,⁵ there are several key questions and considerations an organization should make including:

- Determine the involvement of the Board of Directors
- Evaluate the risk assessment process
- Evaluate the adequacy of the program to manage and control risk
- Assess the measures taken to oversee service providers
- Determine whether an effective process exists to adjust the program
- Summarize and communicate your findings

Each section has a series of additional specific questions to help guide a financial services company towards a comprehensive security program that can protect their customer information.

Other Regulations

There are other regulations that impact financial services companies as well, although at this time several are not enforced the way GLBA rules and regulations are.

- The Federal Rules of Civil Procedure (FRCP) outline regulations for e-Discovery during litigation.
- The Payment Card Industry Data Security Standard (PCI-DSS) must be adhered to by any organization who accepts credit cards.
- The Sarbanes-Oxley Act (SOX) came into force in July 2002 and introduced major changes to the regulation of corporate governance and financial practice.
- The Red Flags Rules require financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. It must provide for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft.

⁵ http://www.ffiec.gov/exam/InfoBase/documents/o2_joi_exam_proc_eval_afeguard_customer_info_010700%20.pdf

DATA BREACH DISCLOSURE LAWS

California Bill SB 1386 was signed into law by Gov. Gray Davis on September 25, 2002, and filed with the California Secretary of State the next day. The law became operative on July 1, 2003.⁶

This personal information privacy law requires any organization (state agency, person, or business) conducting business in California and processing personal information for California residents to disclose any information security breach to those California residents whose unencrypted personal information was obtained by an unauthorized person.

Notifications can be delayed if law enforcement determines it could hinder a criminal investigation. SB 1386 will preempt all local regulation of this issue. The primary requirements, as listed within the regulatory text, will require:

1. Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
2. Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
3. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

What is *Personal Information*?

In terms of the way California defines “Personal information,” it is a person’s first name or first initial and last name in combination with any one of the following when at least one of the pieces of information is not encrypted:

- Social Security number
- Driver’s license number or California Identification Card number

⁶http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

- Account number, credit or debit card number, in combination with any required security code, access code, or password that allows access to a financial account

Personal information does not include information that is publicly and lawfully available from federal, state, or local government sources.

Notification Procedures

Individuals affected by data breaches that meet the personal information definition and notification requirements must be notified by using one of three methods: written notice, electronic notice with customer's consent, or substitute notice (developed to handle large/costly breaches).

Potential issue: Several states do not require organizations to notify consumers of a breach if there is no "reasonable likelihood of harm" to the individual. The definition of reasonable likelihood is open for interpretation by the breached organization.

Notification Timelines

Notification requirements are vaguely defined in most legislation, except Florida and Ohio (45 days after the security breach). Many use the California definition of "the most expedient time possible and without unreasonable delay" and include provisions for the needs of law enforcement.

Potential issue: The term unreasonable delay is subjective. It may take months for an organization to fully assess the impact of a large breach.⁷

Exceptions

Among the states, encryption of customer data generally provides an exemption to disclosure requirements. Security professionals and computer engineers know that encryption is not the end-all to protecting data; it's designed to prevent unauthorized persons from accessing that data. If a hacker can fool a system into recognizing him or her as an authorized user, the hacker will gain access to the data.

Security of encryption keys is also very important; if the keys are stolen along with the data, then the hacker can gain access to the information. These gaps were apparently being considered in Pennsylvania when Senate Bill 712 was passed. That bill states, "An entity must PROVIDE NOTICE OF the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the

⁷ http://www.vigilantminds.com/files/vigilantminds_state_security_breach_legislation_summary.pdf

encryption keys.”

Kansas, Colorado, and Delaware are among 18 states that have provisions exempting companies from disclosure if, upon investigation, it is believed that the stolen data will likely not be misused. Companies should be cautioned against relying too heavily on such a provision. For one thing, how can the hacker’s intent be proved? In addition, there is a clear conflict of interest for a company to conduct its own investigation to determine whether or not the stolen data will likely be misused. The risk, then, is creating a negative public perception of the company.

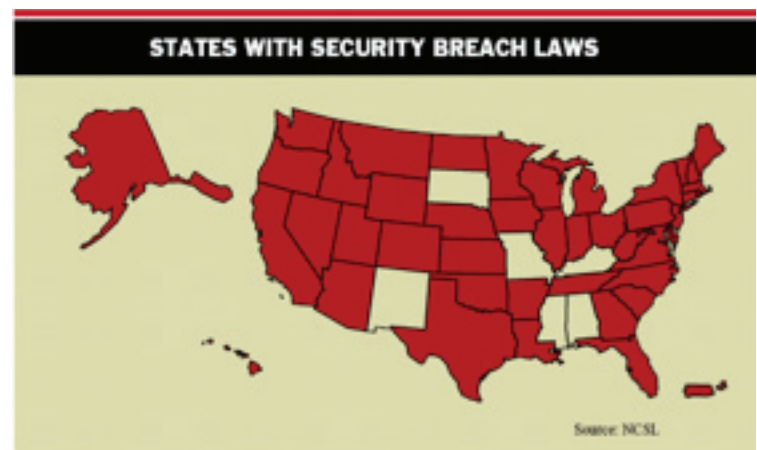
Half of the states with data breach laws specifically mention data redaction as offering an exemption to disclosure requirements (as is the case in Arizona’s Senate Bill 1338). An example would be to edit (redact) a credit card account number so that it would no longer be a true account number. The lesson here is to use only nonpublic personal information (NPI) when it is critical to do so. For example, many companies use internally developed customer identification numbers rather than Social Security numbers to track customers. This meets the needs of businesses while at the same time reduces data security risks.

As noted earlier, information breach notification laws are not limited to electronic data. A handful of states, including California, New York, Utah, Vermont, and Virginia, have laws specific to the secure disposal of NPI on paper. Many companies nationwide provide secure document disposal services.⁸

Most states that have information-breach-notification laws hold businesses liable for the security of NPI, yet only 22 apply the same requirements to their own government agencies. That means 11 states—Alabama, Colorado, Georgia, Maine, Minnesota, Montana, North Carolina, Oklahoma, Texas, Utah, and Vermont—gave themselves a pass on their own laws. A caution for the would-be hacker: Several states have made it a criminal offense to steal somebody’s identity. Arizona House Bill 2484, for example, makes identity theft a felony.⁹

The Security Breach Disclosure Bandwagon

Following high-profile data security breaches in 2005 at ChoicePoint (where 163,000 records were compromised) and CardSystems (where 40,000,000 records were compromised), many states began using California SB 1386 as a model for developing their own data security breach disclosure laws. Today, 45 states in the country (including Washington D.C.) have



⁸ <http://www.intelligententerprise.com/showArticle.jhtml?articleID=198800638>

⁹ <http://www.intelligententerprise.com/showArticle.jhtml?articleID=198800638>

passed data security breach disclosure laws, each with its own distinct notification requirements. Additionally, the full text of the laws is available online. An interactive map with a summary of state-by-state disclosure laws is available online.¹⁰

The following table shows the status of disclosure laws for each state in the United States.¹¹ Additionally, the full text of the laws is available online.¹²

Table 1: Dates Laws Went Into Effect for Each State in the United States

STATE	DISCLOSURE LAW	EFFECTIVE DATE	EXCEPTION FOR ENCRYPTED DATA
ALASKA	2008 H.B. 65	7/1/09	YES
ALABAMA	SB 114	PENDING	YES
ARIZONA	SB 1338	1/1/07	YES
ARKANSAS	SB 1167	4/4/05	YES
CALIFORNIA	SB 1386	7/1/03	YES
COLORADO	SB 06-1119	9/1/06	YES
CONNECTICUT	SB 650	1/1/06	YES
DELAWARE	HB 116	7/12/06	YES
FLORIDA	BILL 481	6/14/05	YES
GEORGIA	SB 230	5/5/05	YES
HAWAII	SB 2290	1/1/07	YES
IDAHO	SB 1374	7/1/06	YES
ILLINOIS	HB 1633	1/1/06	YES
INDIANA	SB 503	7/1/06	YES
IOWA	S.F. 2308	7/1/08	No
KANSAS	SB 196	7/1/06	YES
KENTUCKY	NONE	N/A	N/A
LOUISIANA	SB 205	1/1/06	YES
MAINE	LD 1671	1/31/06	YES
MARYLAND	HB 208	1/1/08	YES
MASSACHUSETTS	S 2058	2/3/08	N/A
MICHIGAN	HB 4658	7/2/07	YES
MINNESOTA	HF 2121	1/1/06	YES
MISSISSIPPI	NONE	N/A	N/A
MISSOURI	NONE	N/A	N/A
MONTANA	HB 732	4/25/05	YES

¹⁰ http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State/1

¹¹ <http://www.guardianedge.com/resources/breach-disclosure.php>; <http://privacylaw.proskauer.com/2008/07/articles/security-breach-notification-l-northern-disclosure-alaska-enacts-44th-state-breach-notification-law/>;

http://www.scottandcottllp.com/resources/state_data_breach_notification_law.pdf

¹² <http://books.google.com/books?id=-2VB77a7KJUC&pg=PA38&lpg=PA38&dq=louisiana+data+breach+disclosure+law+%2211+06%22&source=web&ots=EJEvxhWnsl&sig=jpY2gAQIhBPWrwf7cazyZNBWFKQ&hl=en#PPA38,M1>

Table 2 (cont): Dates Laws Went Into Effect for Each State in the United States

STATE	DISCLOSURE LAW	EFFECTIVE DATE	EXCEPTION FOR ENCRYPTED DATA
NEBRASKA	LB 876	7/14/06	YES
NEVADA	SB 347	1/1/06	YES
NEW HAMPSHIRE	HB 1660	1/1/07	YES
NEW JERSEY	A-4001	1/1/06	YES
NEW MEXICO	NONE	N/A	N/A
NEW YORK	A-4254	12/7/05	YES
NORTH CAROLINA	SB 1048	12/1/05	YES
NORTH DAKOTA	FRBS-0500	4/22/05	YES
OHIO	HB 0104	11/17/05	YES
OKLAHOMA	HB 2357	6/8/06	YES
OREGON	SB 583	10/1/07	YES
PENNSYLVANIA	SBG 712	6/20/06	YES
RHODE ISLAND	HB 6191	3/1/06	YES
SOUTH CAROLINA	SB 453	4/4/08	YES
SOUTH DAKOTA	NONE	N/A	N/A
TENNESSEE	HB 2170	7/1/05	YES
TEXAS	SB 122	9/1/05	YES
UTAH	SB 0069	1/1/07	No
VERMONT	S 284	1/1/07	YES
VIRGINIA	SB 307	3/11/08	YES
WASHINGTON	SB 6043	7/24/05	YES
WEST VIRGINIA	SB 340	3/8/08	YES
WISCONSIN	SB 164	3/30/06	No
WYOMING	W.S. 40-12-501 THROUGH 40-12-509	7/1/06	No

National Data Breach Notification Law

At this time there is no national data breach notification law. However, the Cyber Security Industry Alliance (CSIA), a trade group made up of US-based security vendors, is in full gear to pressure members of Congress to enact data security and breach legislation. CSIA was launched in February 2004 as a public policy association and has been working with the U.S. Congress on data security and other policy issues since its founding. The CSIA criticized Congress for failing to pass a comprehensive data security law in 2006 requiring companies with data breaches to notify victims. The group is calling for a

law that emphasizes encryption. The group said the law would apply equally to all government agencies and businesses that collect and maintain personal information of consumers.¹³

DATA SECURITY BREACH TRENDING

The data used to extrapolate the charts, graphs, and representations for this study is by its very nature misleading. For example, see the chart below, which represents data breach incidents by year in the U.S. (across all industries).

Figure #2 shows a clear growth pattern from the year 2000 through 2006 with a slight dip for 2007 and again in 2008.¹⁴ The red line indicates when California SB 1386 went into effect, the first state to adopt such legislation. Figure #3 represents the years when state data breach notification laws went into effect. It is unlikely that there were fewer data security breaches in years prior to 2006, but rather companies weren't required to make them public.

IDTheftCenter.org is another research firm that collects data on breaches. They report a different number of breaches from those of several other organizations. However, the total number of records compromised in 2008 was very similar. The IDTheftCenter.org reports 656 incidents (see Figure #4) in 2008 compared to 381 for the other research organizations (see privacyrights.org, datalossdb.org).

Figure 2: Data Breach Incidents by Year in the U.S.

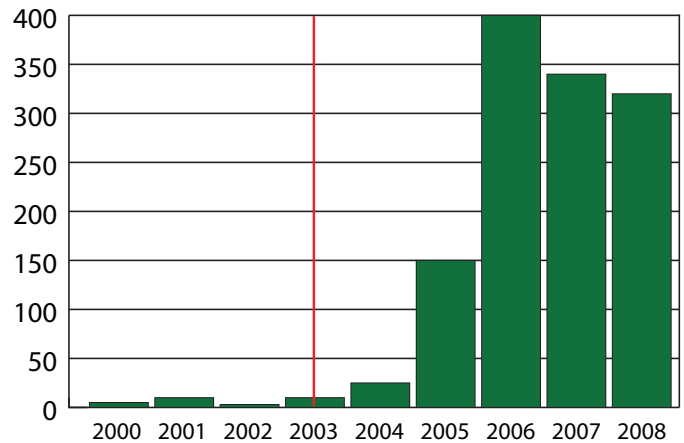
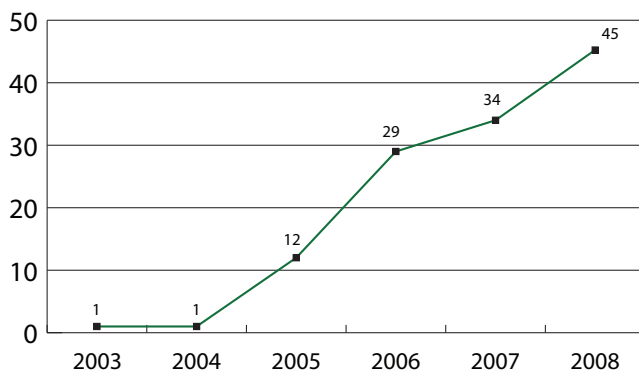


Figure 3: States Adopting Data Breach Disclosure Laws by Year



As stated above. There could be several reasons for the discrepancy between research firms. Different qualification for what constitutes a data breach, the inclusion or exclusion of international breaches, different methods of gathering breach info, the snapshot in time when the data was gathered (post mortem data is more accurate than initial estimates), etc.

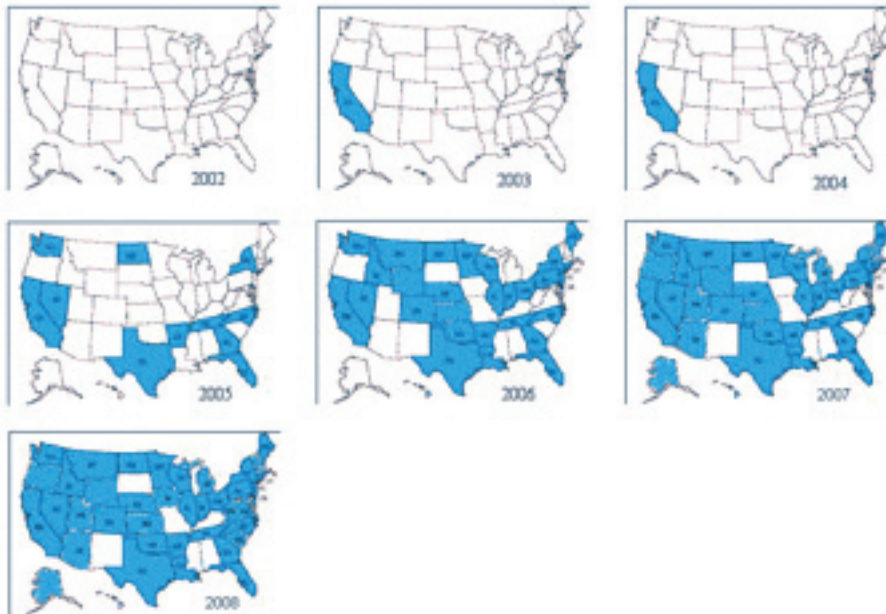
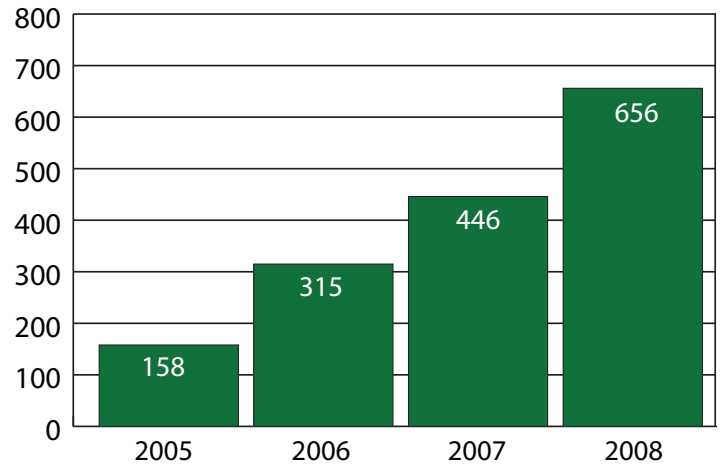
Data breach incidents haven't just begun to occur in the past few years, rather the requirement to disclose those events give a first view into the nature and

severity of the problem. Publicly known data breaches prior to these laws going into effect are nearly all known as a result of fraud committed using the data, or by media leaks.

¹⁴ www.atthebreach.com

Although there are different reports of the total number of incidents, the number of records compromised across all known data breaches in the United States hit an all time high in 2007 and then saw a significant decrease in 2008. The average number of records compromised in a single incident is 296,000 (which encompass nearly three hundred million records across 971 data security breach incidents in the U.S. between 2000 and 2008 where the number of records breached was known). 33 incidents include more than 1 million records compromised, with several being in the tens of millions. Over 230 of these same events had fewer than 1,000 records compromised, with more than 50 being in the double digits.

Figure 4: Data Breach Incidents by Year in the U.S.
Source: Identity Theft Resource Center



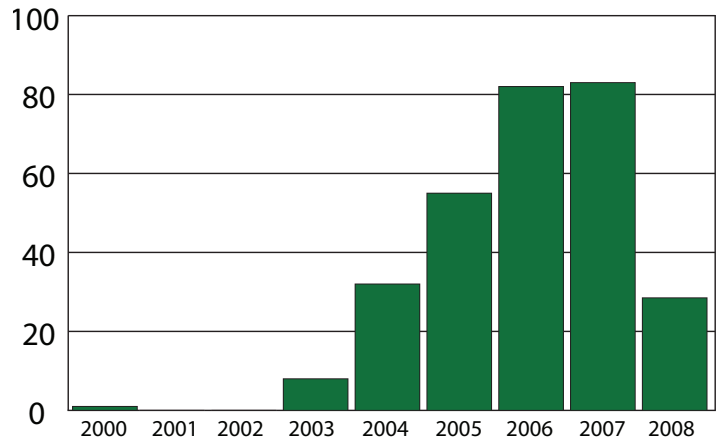
Over the years, there were some significant contributors to the number being as large as it is. The following list includes some incidents that have become household names:

- U.S. Department of Veterans Affairs – 5/22/06 – 26,500,000 records
- America Online – 6/24/04 – 30,000,000 records
- CardSystems (Visa, Mastercard, American Express) – 6/19/05 – 40,000,000 records
- TJX Companies – 1/17/07 – 45,700,000 records

2008 did not have any data security breaches in an order of magnitude similar to the above list. While not likely the sole cause of such a sharp reduction of records compromised, it may be an indication that data breach laws are beginning to be effective in reducing breaches.

The purpose of data breach notification laws is to reduce the amount of fraud and identity theft that has swept the nation over the past several years. While corporate and business data breaches account for 30% of identity theft, in a Dartmouth College study entitled “Do Data Breach Disclosure Laws Reduce Identity Theft?”¹⁵, they find that these laws have made little impact in the reduction of identity theft. The study does not take into consideration 2007 or 2008 data. They also note that with many of these laws being recently enacted, it may be too early to see any positive impact. 2007 had a jump in records compromised largely due to TJX Companies with nearly 45 million records. 2008 had data compromise below 2004 levels, which may indicate that the data breach notification laws are helping reduce crime levels, but it is still not certain how much fraud and identity theft is being reduced.

Figure 5: Records Compromised by Year in the U.S. (In Millions)



TYPES OF DATA

Organizations store a lot of information, both electronically and on paper. The value of this data can vary. For example, a Social Security number or credit card number by itself has little value. When combined with the full name, or even the partial name, of the owner, the data becomes valuable. Other types of data alone, or in combination, have varying degrees of value to a criminal. The following chart is based on the percentage of records compromised between 2000 and 2008 from financial organizations in the U.S. Social Security number (82 incidents) is by far the highest for its inherent flexibility. Fraudsters can use that number to assume a victim’s complete identity, open accounts, and obtain loans. Only 3% of records (where the data type was known) had multiple types of data compromised within the same incident.

Figure 6: Incidents by Data Type

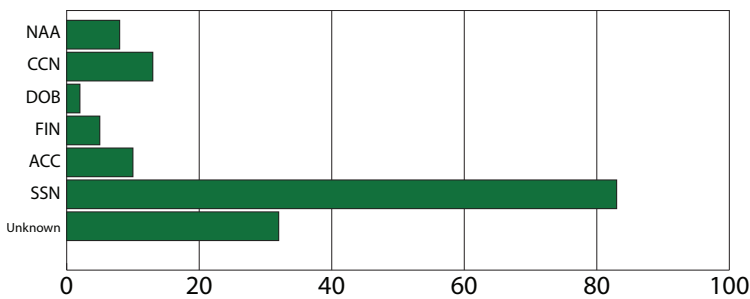
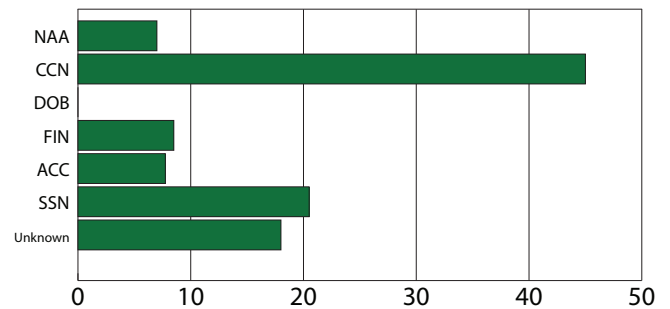


Figure 7: Records by Data Type (in millions)



NAA - Name & Address DOB - Date of Birth ACC - Account Number
 CCN - Credit Card Number FIN - Financial Information SSN - Social Security Number

¹⁵ <http://weis2008.econinfosec.org/papers/Romanosky.pdf>

Compromised records from financial organizations between 2000 and 2008 totaled 104,679,781 (roughly 1/3 of the U.S. population). As indicated by the charts on the previous page¹⁶, financial information such as credit card numbers as well as social security numbers are the most targeted.

DATA BREACHES BY BUSINESS TYPE

Figure 8: Incidents by Business Type

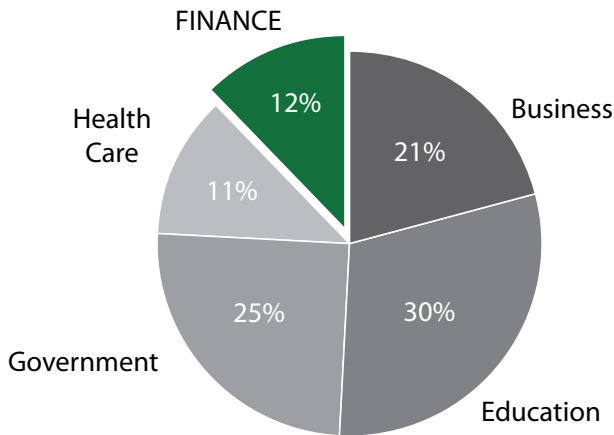
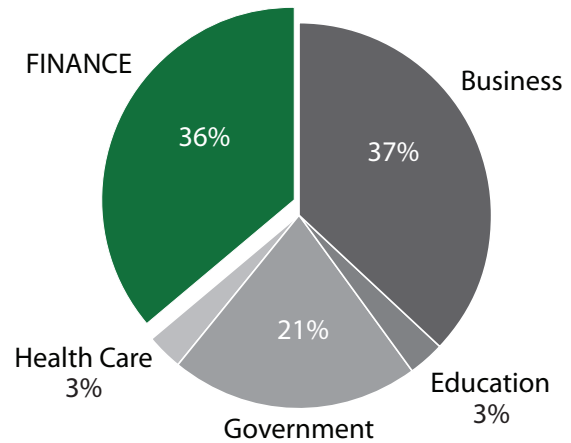


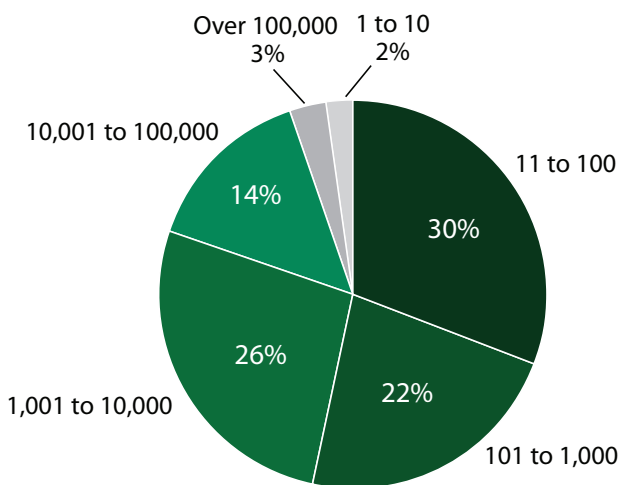
Figure 9: Records Compromised by Business Type



Financial Services companies are responsible for 12% of all data breach incidents in the U.S. between 2000 and 2008 but 36% of all records lost during that same period. Education is responsible for 30% of breaches but only accounts for 3% of all records compromised.

When an organization reports a data security breach, they should include the total number of records compromised. Financial institutions report this information for 2 out of every 3 incidents. On average every other business type reports these 6 out of every 7 incidents.

Figure 10: Data Breach Employee Level



Many assume that the larger the company (in terms of number of employees) the more likely they are to be compromised. According to the 2008 Cybertrust Data Breach Report¹⁷, 78% of breaches had between 11 and 10,000 employees (see Figure #10). The Cybertrust Data Breach Report is an in depth analysis of 500 specific data breach incidents over a four year period of time between 2005 and 2008. Some might construe that very large companies have data forensic security engineers on staff and very small companies may not pay to have professional outside forensic help which could skew these results compared to all known data breaches.

¹⁶ <http://www.atthebreach.com>

¹⁷ www.verizonbusiness.com/resources/security/databreachreport.pdf

DATA COMPROMISE CATEGORIES

Data breaches can be classified into the following categories:

1. Data Breach

- A hacker breaking in and downloading sensitive data.
- System(s) being infected with malicious software that captures, sends, or otherwise puts sensitive data into criminal hands.
- Social engineering techniques whereby employees or other insiders are tricked into exposing sensitive information.
- Theft of computer systems, devices, or storage media that has sensitive data stored.

2. Data Exposure

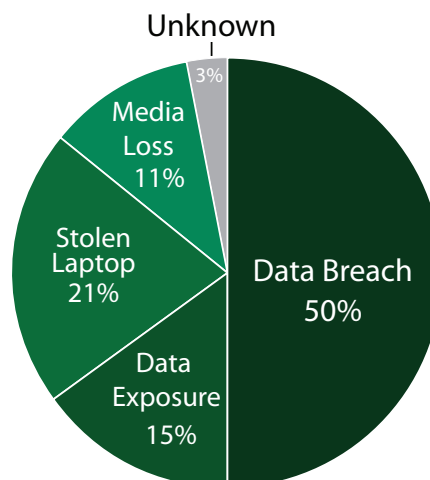
- Sending sensitive information in email.
- Posting sensitive information to a public forum such as a web site.
- A computer glitch that causes the exposure of sensitive data.
- Sending sensitive information through the mail system in a way that is not secure. Often where you can view sensitive information without opening the envelope.
- Paper or other physical files that are placed in a public area that can be viewed or taken by unauthorized individuals.
- Not disposing of documents properly. Often found in dumpsters.

3. Incidents concerning portable laptop computers, usually theft, often while away from the office (users home, car, or while traveling).

4. Loss of Media

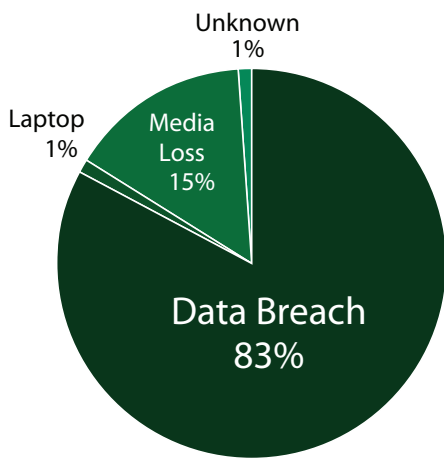
- Backup tapes, CDs, DVDs, or other storage medium lost.
- Computers or computer components that are donated or sold while sensitive information remains stored on the device.

Figure 11: Incidents by Breach Category



Between 2000 and 2008, 50% of publicly known security incidents at financial organizations are classified as data breaches. Data breaches are always malicious in nature, whereas data breaches from laptops being stolen (21%) aren't as clearly defined. Perhaps the perpetrator was after the sensitive information on the laptop (which can be the case when a laptop is missing from an office), but often theft of portable electronics is for the value of the asset itself (as in many cases of stolen laptops from cars, hotels, etc.). With theft, because the data was exposed to an unauthorized person, it is classified as a data security breach incident. Those incidents that cause data exposure (15% of incidents), however, were rarely done with malicious intent. This type of data breach incident is often caused by untrained or careless employees, or sometimes the computer or another system has a glitch and inadvertently exposes sensitive data.

Figure 12: Records Compromised by Breach Category



Data breaches (hackers, malicious employees, social engineering, etc.) constitute 50% of incidents and account for 83% of all records compromised, nearly five times the next closest category. The number of records compromised due to data exposure and stolen laptop is very low. Media loss at 15% is the only other significant contributor to compromised records.

Even the loss of a handful of records can result in negative media exposure, eroding your company brand, customer trust and loyalty, and eventually your bottom line. Data breach disclosure laws require notification regardless of how many records are compromised.

Key Finding: The greatest exposure and loss of sensitive data is in the form of data breaches, most often caused by hackers, theft and malicious employees

DATA BREACH SOURCES

Breaches caused by hackers are both the leading cause of incidents as well as most records compromised. Financial services companies appear to have strong, enforced policies and procedures in that both the number of incidents as well as records lost as a result of a careless or untrained employee are very low. Careless and untrained insiders are a much larger problem in other business types.

Figure 13: Financial Vertical Incidents by Breach Source

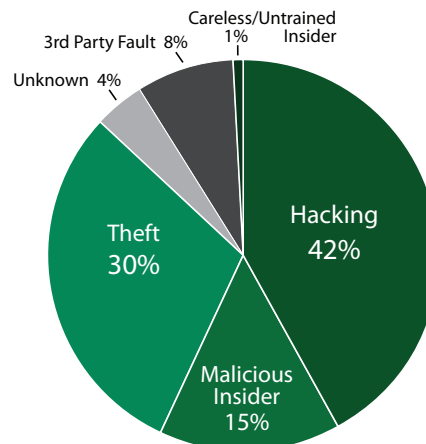
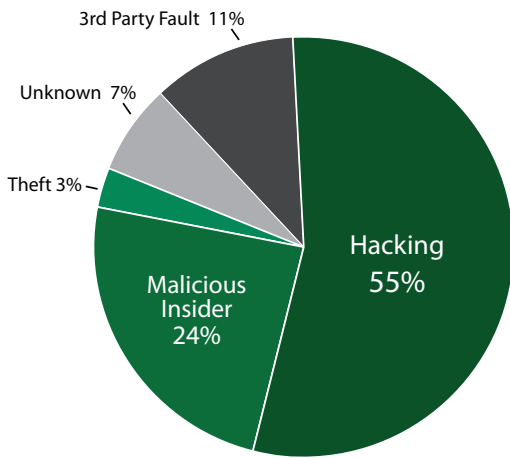


Figure 14: Financial Vertical Records Compromised by Breach Source



Relatively few records are compromised as a result of theft although it accounts for 30% of incidents. Theft can have different intentions and lead to a variety of uses, many of which won't be known. For example, a person who steals a laptop from an automobile may want it for personal use or to sell to a pawn shop. He may have had no intention of looking at the hard drive for data that could be used to perpetrate identity theft. That may also be the very reason he stole the laptop. Perhaps when it ends up at the pawn shop, the owner discovers this data and uses it for fraudulent purposes. Perhaps the person who buys it from the pawn shop uses the data to commit crime. The point is that when theft occurs, it must be assumed the sensitive data will be used for a malicious purpose, therefore it is classified as a data breach.

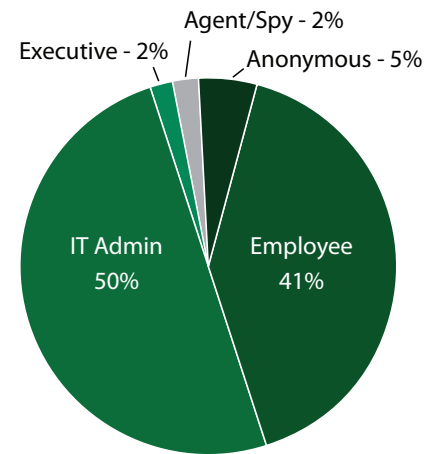
While financial services companies focus much of their effort on the mitigation of the risks associated with hackers, malicious insiders and 3rd parties are a significant cause of records lost through a data security compromise (24% and 11% respectively).

Figure 15: Notable Financial Industry Data Breaches

COMPANY	DATE	RECORDS	DESCRIPTION
IBILL	08-MAR-06	17,781,462	Dishonest insider or possibly malicious software linked to iBill used to post names, phone numbers, addresses, e-mail addresses, Internet IP addresses, logins and passwords, credit card types, numbers, and purchase amount online.
MORTGAGE LENDERS NETWORK USA	23-MAY-06	231,000	A former employee was arrested for extortion for attempting to blackmail his former employer for \$6.9 million. He threatened to expose company files containing sensitive customer information - including customers' names, addresses, and Social Security numbers
BANK OF AMERICA	14-DEC-06	UNKNOWN	A former contractor for Bank of America accessed restricted personal information (name, address, phone number, Social Security number) of an undisclosed number of customers, for the purpose of committing fraud.
COMMERCE BANCORP	13-NOV-07	UNKNOWN	A Commerce Bancorp Inc. employee gave out personal information on an unspecified number of the Cherry Hill bank's customers.
COUNTRYWIDE FINANCIAL CORP.	02-AUG-08	2,000,000	The FBI arrested a former Countrywide Financial Corp. employee and another man in an alleged scheme to steal and sell sensitive personal information, including Social Security numbers. The breach occurred over a two-year period.

The Cybertrust 2008 Data Breach Study¹⁸ digs deeper into data breach sources. Your IT administrator may not want you to know that they account for 1/2 of data breaches sourced from insiders (see Figure #16). Other employees account for 41%, which illustrates the point that data breaches are not necessarily caused by those that have higher levels of network access. While this is not financial vertical specific it does illustrate a broad view of breaches attributed to insiders.

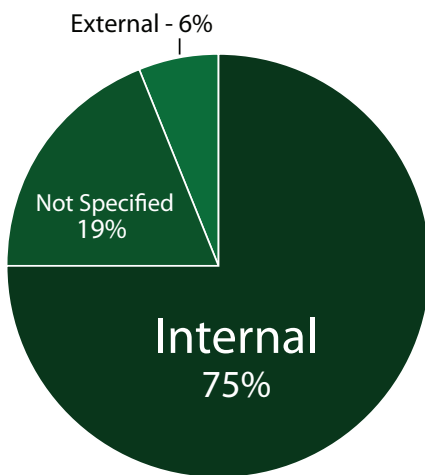
Figure 16: Data Breach Insider Sources



DATA LOCATION AT TIME OF BREACH

The location of the data at the time of the compromise is a statistic worth reviewing. For 19% of records it is unknown if the

Figure 17: Location of Records When Compromised



data was inside the secured facility or outside. Although this is lower than many other industries, if organizations did not allow sensitive data to leave their facility without being encrypted (for electronic data) or disposed of properly (for physical data), it could eliminate nearly one-fifth of records compromised.

3rd parties, careless employees, and theft account for most of the data compromised while away from the office. Most of these incidents involving a careless or untrained employee involved throwing away sensitive data into the dumpster. Theft that occurred usually involved a laptop or media tapes being stolen from an employees car.

Very few incidents where data was compromised from the inside of the network involved 3rd parties, although one incident compromised 2.3 million records. Nearly half of the incidents caused by careless employees involved peer to peer (P2P) software. P2P software is normally used to share music and movies over the Internet. These software programs can be modified to scan and post sensitive data rather than music for download.

Hacking, malicious insiders, and theft make up the balance of internal records that are compromised. In one case, nearly 18 million records were compromised as a result of a malicious insider, another 40 million records were compromised through a hacking attack, all the while theft never accounted for more than 1 million records in any single incident.

Strong, enforced policies and procedures aren't enough to stop all incidents. This is where technology solutions can be implemented to mitigate the risks. Financial services companies must focus most of

¹⁸ www.verizonbusiness.com/resources/security/databreachreport.pdf

their data security budget on protecting information while it is at rest on the inside of the network and keeping their systems from becoming infected or compromised by malware.

SECURITY BREACH IMPACT ON PUBLIC COMPANIES

Approximately one third of financial services companies that experienced data security breaches between 2000 and 2008 were public companies. Public companies accounted for 10 times the number of records compromised than private companies. Compromised records from public companies totaled just over 61.4 million while private companies during that same period totaled 6.3 million. It would appear that public companies fall under greater scrutiny to provide specifics around data breach incidents. Public companies disclose the number of records lost twice as often as private companies. The following table lists those public financial services companies where more than one million records were compromised.

COMPANY	DATE	TICKER	RECORDS	DESCRIPTION
CITIGROUP	06-JUN-05	C	3,900,000	Lost backup tapes
VISA MASTERCARD AMERICAN EXPRESS	19-JUN-05	MA AXP	40,000,000	Hacking
LA SALLE BANK	21-DEC-05	ABN	2,000,000	Backup tape with residential mortgage customers lost in shipment by DHL, containing SSNs and account information.
CHASE CARD SERVICES	07-SEP-06	JPM	2,500,000	Chase Card Services mistakenly discarded 5 computer data tapes in July containing Circuit City cardholders' personal information.
FIDELITY NATIONAL INFORMATION SERVICES	03-JUL-07	FIS.N	8,500,000	A worker at one of the company's subsidiaries (Certegy Check Services, Inc.) stole customer records containing credit card, bank account and other personal information.
TD AMERITRADE	14-SEP-07	AMTD	6,300,000	One of Ameritrades databases was hacked and contact information for more than 6.3 million of its customers was stolen.

Plotting data security breach dates against a stock trending chart is interesting to correlate. In many cases a dip in the overall stock price occurs, which could be associated with the news of the security breach. The recent problems with the U.S. economy, many of which are directly tied to financial services companies, make it difficult to plot. When looking at a stock chart, perhaps a 5% to 15% drop from a data security breach is significant, but not when 50% to 90% stock value is lost and represented on the same chart.

The impact on high-profile data security breaches seems more quantifiable. There was a 20% drop in the TJX Companies stock (symbol: TJX) within weeks of the data security breach that included the compromise of 45 million records. This was a temporary drop in that the stock since it recovered 75% of its losses within three months and was fully recovered within about seven months.

Figure 18: TJX Companies, Inc



TJX has reported that it has now spent or put aside approximately \$250 million in connection with the incident.¹⁹

In times past it does appear that the size, scope, media exposure, and how the incident is handled by the organization can significantly impact the stock price of public companies. The public also seems to have a fairly short memory in that the stock price will quickly return to its former highs within a short period of time.

Sometimes, insider trading is the cause of a sudden drop in stock price, when executives and employees believe there will be large fallout from a security breach that has not yet been made public. For example, –from a CNN report, “The chairman and the president of ChoicePoint—under fire for allowing phony businesses to buy access last fall to their database of personal information on consumers—have between them sold almost 500,000 shares of company stock for a profit of \$17.6 million since November, according to Securities and Exchange Commission filings.”²⁰

¹⁹ <http://www.high-tower.com:80/blogs/gschultz/ninth-prediction-for-2008/>

²⁰ http://money.cnn.com/2005/02/25/news/midcaps/ChoicePoint_stock/index.htm

SECURITY BREACH IMPACT ON SMALL COMPANIES

It usually isn't the fear or reality of public backlash, but rather the hard and soft costs associated with recovering from a security breach that impacts small companies the most. In an Information Week article entitled "Companies Say Security Breach Could Destroy Their Business"²¹ it states:

- One-third of companies said in a recent poll that a major security breach could put their company out of business
- A data breach that exposed personal information would cost companies an average of \$268,000 to inform their customers -- even if the lost data is never used
- 61% of respondents said data leakage is the doing of insiders, and 23% said those leaks are malicious
- 46% said they don't debrief or monitor employees after they give notice that they are leaving the company
- 23% said they were able to estimate the total annual cost of data leakage, putting the figure at \$1.82 million

COST OF A SECURITY BREACH

The costs of recovering from a security breach vary depending on the type of company or industry, the circumstances surrounding the security breach, type of data compromised, liability, and so forth. Many organizations are required by federal law to perform risk assessments to determine their exposure to a variety of threats and risks. To perform a comprehensive risk analysis, an organization needs to know what it would cost to recover from a given compromise.

According to a Ponemon data breach report²² recently updated, the average cost of a data security breach is \$6.6 million and more than \$200 per compromised record. The report, sponsored by PGP Corp., examined the costs incurred by 43 organizations that experienced a data breach. Breaches ranged as high as 113,000 records and the average total cost per company ranged from more than \$613,000 per breach to nearly \$32 million. The report found that most of the cost is due to lost business, which averaged nearly \$4.6 million. Forty-four percent of the organizations surveyed reported a breach by a third party, such as a contractor or outsourcer, and more than 88 percent of all cases this year involved incidents resulting from insider negligence, according to the study.

Here are a few items from the news that relate to the cost of recovering from a data security breach.

- The Veterans Administration has agreed to pay a \$20 million settlement to a class-action suit filed on behalf of 26.5 million people. In this case, a laptop and media were stolen and later found. It was determined that the data had not ever been used for fraud and had not even been accessed. The result of the data being found and not used did not impact the success of the class-action lawsuit.

²¹ http://www.informationweek.com/news/security/showArticle.jhtml;jsessionid=WoA23QSERJNEYQSNDRSKHoCJUNN2JVN?articleID=199201085&_requestid=58557

²² http://www.pgp.com/insight/newsroom/press_releases/2008_annual_study_cost_of_data_breach.html

²³ <http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/>

- Visa and TJX agree to provide U.S. issuers up to \$40.9 million for data breach claims.²⁴
- ChoicePoint settles data security breach charges; to pay \$10 million in civil penalties, \$5 million for consumer redress. At least 800 cases of identity theft arose from company's data breach.²⁵
- Hannaford Bros. Co. already has been hit with two class-action lawsuits filed on behalf of consumers whose credit and debit card numbers were compromised as a result of a major security breach.
- Data breach incidents cost companies \$197 per compromised customer record in 2007, compared with \$182 in 2006.²⁶
- A breach that exposes 46,000 identities will cost an organization \$7.6 million on average.²⁷
- Forrester recently surveyed 28 companies that had data breaches and estimated that such a breach will cost an organization between \$90 and \$305 per exposed record, depending on the public profile of the breach and the regulations that apply to the organization.²⁸
- The average total cost per reporting company was \$4.8 million per breach and ranged from \$226,000 to \$22 million.²⁹
- Direct incremental costs averaged \$54 per lost record, which included free or discounted services offered, notification letters, phone calls, and e-mails, legal, audit, and accounting fees, call center expenses, public and investor relations, etc.³⁰
- Lost productivity costs averaged \$30 per lost record.³¹
- Customer opportunity costs averaged \$98 per lost record.³²
- Customer turnover averaged 2 percent and ranged as high as 7 percent.³³
- The cost of new preventative measures averaged 4 percent of the total breach cost, or \$180,000 on average.³⁴
- Many companies had to subscribe customers or employees to free credit monitoring services that ranged from \$10 to \$25 per month/customer or employee.

To use an online calculator to arrive at an estimated cost of a breach based on the number of records exposed, visit this Web site: www.tech-404.com/calculator.html.

²⁴ http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20071130005355&newsLang=en

²⁵ http://www.boston.com/news/local/maine/articles/2008/03/19/hannaford_hit_with_class_action_suit_in_data_breach_1205971643/

²⁶ www.pgp.com/newsroom/mediareleases/ponemon-us.html

²⁷ http://www.news.com/8301-10784_3-6176074-7.html

²⁸ http://www.news.com/8301-10784_3-6176074-7.html

²⁹ www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

³⁰ www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

³¹ www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

³² www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

³³ www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

³⁴ www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

RECORD FORMAT AT TIME OF BREACH

It is interesting to review the percentage of records that were in electronic versus paper format at the time they were compromised. Very few records were compromised while in paper format. Nearly all data compromised was while in electronic format. This can be data that is extracted from a server or database, magnetic media such as backup tapes, CDs, DVDs, or portable devices such as laptops, USB Thumb drives, stolen PCs, etc.

According to the PGP Research Study – Summary October 2006 nearly 90% of all data breaches were in electronic form.³⁵

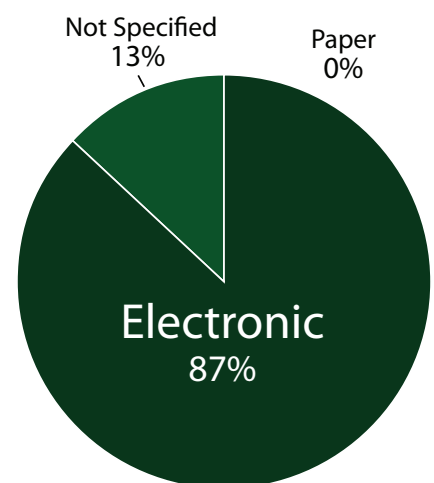
HEARTLAND PAYMENT SYSTEMS CASE SUMMARY

Until recently TJX Companies held the top spot in total number of records compromised in a data security breach at 45.6 million records. Heartland Payment System of Princeton New Jersey announced that they experienced a data security breach that is believed to be the largest in U.S. history. The number of records compromised starting at the 100 million mark but could reach much higher. Lawsuits have already been filed against Heartland. The lawsuits seek damages and relief for the “inexplicable delay, questionable timing, and inaccuracies concerning the disclosures” with regard to the data breach.

The attack was much more sophisticated than TJX and is similar to Hannaford (the New England based grocery store chain that had a 4.2 million record security breach) where malware was loaded on servers where payment transactions were routed. Hannaford was notified by the FBI that 1800 fraud cases were linked to cards used by Hannaford customers that lead investigators to find the malicious software. Heartland was notified by Visa and MasterCard of suspicious activity surrounding processed card transactions. The company found evidence of malicious software that compromised card data that crosses Heartland’s network. Initial investigation suggests this may be the result of a global cyberfraud operation.

The 100 million records being breached is being assumed because that is how many transactions they process each month, which the malware had access to. Currently it is unknown how many months of information were captured. It is also unknown at this time the various data types of information captured.

Figure 19: Record Format at Time of Breach



³⁵ www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

CONCLUSION

Financial services companies clearly are a key target for criminals of all types. Financial services companies have been required through GLBA to be compliant with rules and regulation for longer than any other industry. Although the number of incidents and records compromised is still quite high, the implementation of risk mitigation strategies has clearly reduced the total number of data security compromises. Criminals are redoubling their efforts and continue to target financial services companies for the valuable data they maintain. Companies offering financial services need to continue to identify security gaps and implement technologies that offset these sophisticated attacks. With policies, procedures, security solutions, training, and auditing, financial institutions can achieve and maintain the level of security the American people have come to expect.

KEVIN PRINCE
Chief Technology Officer
Perimeter eSecurity
KPrince@perimeterusa.com

ABOUT THE AUTHOR

Named Chief Technology Officer of Perimeter in 2009, Kevin Prince spearheads the company's technology strategy and leads the technical team in working closely with its customers to manage all of the complexity and compliance requirements of securing information across the enterprise.

With more than 19 years of expertise in Information Technology and 11 years focused on Internet security, Mr. Prince is an evangelist on Internet security topics, including network security threats, fraud, identity theft, cyber terrorism and data breaches. Through regular speaking engagements, webinars, whitepapers and blog postings, Mr. Prince is dedicated to educating organizations on how to manage information complexity, meet increasingly stringent compliance and security requirements, and mitigate risk. Mr. Prince has trained federal examiners for several years.

ABOUT PERIMETER eSECURITY

Perimeter is the trusted market leader of information security services that delivers enterprise-class protection and compliance for businesses of any size. Through its cost-effective security-as-a-software platform, Perimeter offers the most comprehensive compliance, security and messaging services that include but aren't limited to: hosted email, encrypted email, firewall management and monitoring, vulnerability scanning, host intrusion and prevention, email antivirus and spam, remote data backup and email archiving.

As companies struggle with the increasing cost, complexity and stringent compliance requirements associated with their information intensive businesses, Perimeter is the only provider that can simultaneously reduce the cost, manage all of the complexity and meet all of the compliance requirements from a single platform.

Headquartered in Milford, CT, with seven geographically distributed technical operations centers and three redundant datacenters, Perimeter's on demand services, which are offered both on a Network (in-the-cloud) and CPE (customer-provided equipment) basis, are validated by TruSecure and guaranteed for current and future regulatory compliance. If you would like to speak with us or view a product demo, please don't hesitate to call at 800.234.2175 Option #2 or visit our web site at www.PerimeterUSA.com.

APPENDIX A- Chronological list of known U.S. financial service companies data security breaches between 2000-2008³²

DATE	NAME	STATE	RECORDS
11/14/2000	Western Union		15,700
5/7/2003	Virginia Credit Union		800
11/22/2003	Wells Fargo		
12/19/2003	Bank Rhode Island		43,000
3/29/2004	GMAC Financial Services		200,000
4/16/2004	Fleet Credit Card Services		
11/25/2004	Brazos Higher Education Service Corporation		550,000
2/26/2005	Bank of America	NC	1,000,000
3/1/2005	Paymaxx	FL	100,000
4/20/2005	Ameritrade	NE	200,000
5/12/2005	Westborough Bank	MA	750
5/23/2005	Bank of America / Wachovia	USA	676,000
6/6/2005	Citigroup	TX	3,900,000
6/19/2005	Visa MasterCard American Express	USA	40,000,000
6/30/2005	Bank of America	USA	18,000
7/8/2005	City National Bank	CA	
8/30/2005	JPMorgan Chase	TX	
9/2/2005	Iowa Student Loan		165,000
9/16/2005	ChoicePoint	GA	
9/17/2005	North Fork Bank	NY	9,000
9/28/2005	RBC Dain Rauscher	USA	300,000
10/7/2005	Bank of America		
11/8/2005	ChoicePoint	GA	
11/26/2005	Scottrade	USA	140,000
12/3/2005	First Trust Bank	PA	
12/9/2005	Oregon Community Credit Union		200
12/21/2005	LaSalle Bank	IL	2,000,000
1/2/2006	H&R Block	USA	
1/11/2006	People's Bank	MA	90,000
1/25/2006	Ameriprise Financial	MN	226,000
2/6/2006	Regions Bank		100,000

³⁶ Privacyrights.org; <http://datalossdb.org/>

DATE	NAME	STATE	RECORDS
2/9/2006	Bank of America / OfficeMax	USA	200,000
3/2/2006	Olympic Funding Chicago	IL	
3/8/2006	iBill	FL	17,781,462
3/23/2006	Fidelity Investments	MA	196,000
4/13/2006	Fifth Third Bank		1,000
4/26/2006	Clydesdale Bank - Morgan Stanley		2,000
5/5/2006	Wells Fargo	CA	39,442
5/11/2006	Columbus Bank and Trust		2,000
5/12/2006	Mercantile Potomac Bank	MD	48,000
5/17/2006	M & T Bank	NY	2,524
5/19/2006	Frost Bank		100
5/23/2006	Mortgage Lenders Network USA	CT	231,000
5/25/2006	Security Savings Bank		13
5/31/2006	Texas Guaranteed Student Loan Corp.	TX	1,300,000
5/31/2006	VyStar Credit Union	FL	34,000
6/10/2006	Nationwide Retirement Systems		
6/14/2006	American International Group	NY	969,000
6/16/2006	ING	FL	8,500
6/18/2006	ING U.S. Financial Services	DC	13,000
6/20/2006	Equifax Inc.	GA	2,500
6/29/2006	Allstate	AL	27,000
7/5/2006	Bisys Group Inc.	NJ	61,000
7/7/2006	National Association of Securities Dealers	FL	73
7/24/2006	Wolters Kluwer		8,500
7/25/2006	Old Mutual Capital Inc	USA	6,500
7/29/2006	Sentry Insurance	WI	112,198
8/1/2006	CoreLogic for ComUnity Lending	CA	
8/1/2006	U.S. Bank	KT	
8/4/2006	Matrix Bancorp Inc.	CO	
8/22/2006	Aflac	SC	612
8/25/2006	Sovereign Bank	MA	
9/1/2006	Wells Fargo	CA	
9/7/2006	Chase Card Services	DE	2,500,000
9/13/2006	American Family Insurance	WI	2,000
9/16/2006	Howard Rice	CA	500

DATE	NAME	STATE	RECORDS
9/17/2006	Direct Loan	USA	21,000
9/22/2006	Bank of America	USA	
9/23/2006	An illegal dumping site northwest of Quinlan, TX	TX	
10/16/2006	VISA/FirstBank	USA	
10/26/2006	Empire Equity Group	NC	
10/28/2006	Hancock Askew & Co. LLP	GA	
11/1/2006	Home Finance Mortgage, Inc.	NC	
11/3/2006	West Shore Bank	MI	1,000
11/17/2006	Automatic Data Processing (ADP)	NJ	
11/30/2006	TransUnion Credit Bureau	AZ	1,700
12/1/2006	TD Ameritrade	NE	300
12/5/2006	H&R Block	USA	
12/6/2006	Premier Bank	MO	1,800
12/22/2006	Bank of America	NC	
12/29/2006	KeyCorp	OH	9,300
1/2/2007	News accounts are not clear as to source, but thought to be a realty office	NV	
1/12/2007	MoneyGram	MN	79,000
1/26/2007	Chase Bank / Bank One	LA	4,100
2/3/2007	CTS	MI	800
2/6/2007	Metro Credit Services	TX	
2/8/2007	Piper Jaffray	MN	1,000
3/20/2007	Tax Service Plus	CA	4,000
4/5/2007	Security Title Agency	AZ	
4/9/2007	Turbo Tax	USA	
4/11/2007	New Horizons Community Credit Union	CO	9,000
4/12/2007	Bank of America	NC	
4/26/2007	Ceridian Corp.	MN	150
5/1/2007	J. P. Morgan	NY	
5/1/2007	JPMorgan Chase	IL	47,000
5/21/2007	Columbia Bank (NJ)	NJ	
5/23/2007	Check into Cash	IL	
5/31/2007	Priority One Credit Union	CA	
6/1/2007	JAX Federal Credit Union	FL	7,500
6/6/2007	HarborOne Credit Union	MA	9,000

DATE	NAME	STATE	RECORDS
6/22/2007	Texas First Bank	TX	4,000
7/3/2007	Fidelity National Information Services	FL	8,500,000
7/7/2007	Securitas Security Services USA Inc.		100,000
7/16/2007	Prudential Financial Inc.	NJ	1,000
7/17/2007	Western Union	CO	20,000
8/2/2007	E.On	KY	
8/4/2007	Kellogg Community Federal Credit Union	MI	
8/7/2007	Merrill Lynch	NJ	33,000
8/16/2007	Utica Title and Escrow	OK	
9/14/2007	TD Ameritrade	NE	6,300,000
9/21/2007	ABN Amro Mortgage Group	IL	5,208
10/10/2007	Commerce Bank	KS	3,000
10/30/2007	Hartford Financial Services Group	CT	237,000
11/6/2007	Butte Community Bank	CA	
11/13/2007	Commerce Bancorp	PA	
11/16/2007	A.J. Falciani Realty Company	NJ	500
12/1/2007	Community Blood Center/Battelle & Battelle LLC	OH	600
1/2/2008	Workers Compensation Fund	UT	2,800
1/17/2008	GE Money	MA	650,000
1/25/2008	OmniAmerican Bank	TX	100
1/28/2008	T. Rowe Price Retirement Plan Services	MD	35,000
1/30/2008	Davidson Companies	MT	226,000
2/10/2008	Administrative Systems, Inc	WA	
2/15/2008	First Magnus Financial	FL	
3/19/2008	Affordable Realty	MI	
3/21/2008	Compass Bank		1,000,000
3/26/2008	BNY Mellon Shareowner Services	PA	3,500
4/15/2008	First Federal Bank of California	CA	
4/19/2008	Central Collection Bureau	IN	700,000
4/22/2008	CollegelInvest	CO	200,000
4/22/2008	Fishback Financial Corp	SD	
4/22/2008	LendingTree	NC	
5/1/2008	Cove Creek Mortgage/Front Range Mortgage	CO	
5/7/2008	Bank of New York Mellon		4,500,000
5/29/2008	State Street Corp	MA	45,500

DATE	NAME	STATE	RECORDS
6/10/2008	1st Source Bank	IN	
6/19/2008	Citibank	NY	
6/23/2008	Bank Atlantic	FL	
7/8/2008	LPL Financial	MA	10,219
7/9/2008	Wagner Resource Group	VA	2,000
8/2/2008	Countrywide Financial Corp	CA	2,000,000
8/18/2008	Dominion Enterprises / InterActive Financial Marketing Group	VA	92,095
8/19/2008	Kingston Tax Service	WA	
9/10/2008	Franklin Savings and Loan	OH	25,000
11/5/2008	Wells Real Estate Funds		0
11/26/2008	TD Bank, N.A.		3,235
12/8/2008	CheckFree Corporation (FiServ)		5,000,000
12/16/2008	Merrill Lynch		0
12/23/2008	RBS Worldpay		1,500,000
12/29/2008	Merrill Lynch	NY	0