The Costs of Data Security Breaches and Identity Theft

February 2006
Summary

California’s Security Breach Information Act and similar state and federal laws mandate disclosure of security breaches involving personal identity data. The disclosures have provided visibility, not previously available, into the costs of breaches and identity theft to consumers and companies. This paper provides an overview of the effect of data breach notifications and the associated costs through a survey and examination of key findings from research studies, government reports and news stories. The paper concludes that companies should assess online fraud and identity data theft solutions, specifically, as part of an information risk management program and implement solutions that provide the best return on investment.

Note: selected text in this paper is italicized by the author to emphasize key points.
A Duty to Disclose

Disclosure of high-profile, personal information thefts in 2005 attracted the attention of the public, the media, the government and other groups concerned with an increase in the incidence of identity theft and Internet fraud. However, it is unclear whether there was an actual increase in the number of incidents, or just the number of disclosures.

It is clear that prior to recent state and federal legislation incidents were not fully reported. The Computer Security Institute 2003 Computer Crime and Security Survey surveyed 530 information security professionals: thirty-six percent of the 490 respondents experienced a system breach in the prior year, while twenty-one percent had dealt with theft of proprietary information. Only thirty percent of respondents reported incidents to law enforcement and twenty-one percent to legal counsel, while fifty percent did not report the incident at all.

One specific breach during 2002 is generally credited as the triggering event that permanently altered the practice of non-reporting.

On April 5, 2002, computer intruders successfully gained unauthorized access to state employees’ sensitive financial and personal information stored at the Stephen P. Teale Data Center in Sacramento, California. The intrusion affected approximately 265,000 California state employees. Although the incident was reportedly discovered as of May 7, 2002, the affected state employees were not notified until May 21, 2002. Between the time the database was breached and the disclosure, attempts were made to access one worker’s bank account and to change the address for another worker’s credit card account.

This testimony during hearings associated with Senate Bill 1386 prompted amendments that would have far-reaching implications.

On July 1, 2003, California Civil Code 1798 titled California’s Security Breach Information Act and commonly known as California Senate Bill 1386, took effect. It mandates that organizations must disclose security incidents that involve private information about California residents. Specifically section 1798.29(a) states, “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.”

In addition, when database operators store computerized data they do not own, they also have a duty to disclose unauthorized access of data (containing personal information) to the data’s owner or licensee.
“immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

ChoicePoint, a nationwide data broker, disclosed a security breach in early 2005 that affected nearly 150,000 people from all fifty states. The company limited its initial notification to California residents only, in accordance with California Civil Code 1798. After discussions with state attorneys general, the company conducted a voluntary nationwide notification, and since then, the “best practice” has been to disclose breaches to individuals nationwide.

The Effect of Data Breach Notifications

A research study, conducted by Ponemom Institute LLC and released in November 2005, entitled National Survey on Data Security Breach Notification examined how organizations met their legal obligations to notify individuals after the loss or theft of personal information. The study also examined how individuals reacted to the organization’s communication and handling of this critical event. Following are some of the key survey findings:

• 11.6% (1,109 of 9,154) respondents reported that they have received notification of a data security breach within the last year, suggesting that more than 23 million U.S. adult-aged residents may have received a breach notification.

• About 86% of security breaches involved the loss or theft of customer or consumer information, and about 14% involved employee, student, medical and taxpayer data.

• The most likely organizations to report a breach are banks, credit card companies, governmental organizations (including state universities) and healthcare providers.

• 19% of respondents have already discontinued their relationship with the company as a result of the data breach.

• More than 40% said that they might discontinue their relationship with the company as a result of the notification.

The Costs to Individuals


• The total U.S. annual identity fraud cost in 2004 was $52.6 billion, essentially unchanged from the 2003 inflation adjusted level of $51.4 billion.
The Costs of Data Security Breaches and Identity Theft

- The 9.3 million new victims of identity fraud corresponded to a 7.9% decrease from the 2003 survey level of 10.1 million.
- The mean total cost of identity fraud per victim in 2004 was $5,686, a 12% increase over the 2003 mean total of $5,072, due to a small number of high value cases.
- Most victims (67%) continue to pay no out-of-pocket costs.
- The mean out-of-pocket cost for those victims who did pay was $652 in 2004, a 21.6% increase over the 2003 total of $536.
- In 2004, victims on average spent 28 hours resolving credit, financial and other problems caused by fraud, five hours less than the 2003 average of 33 hours.
- 11.6% of stolen identity information was obtained online.9

The Costs to Companies

Another research study, conducted by Ponemom Institute LLC, also released in November 2005, entitled Lost Customer Information: What Does a Data Breach Cost Companies?, examines the costs incurred by 14 companies, in 11 different industries, that experienced a data breach. Breaches included in the survey ranged from 1,500 records to 900,000 records, with estimated total costs ranging from a low of $477,950 to a high of $52,500,800.

The average number of records affected in the breaches studied was 99,667, and the total costs for a company to recover from a data breach averaged $14 million per company or $140 per lost customer record. Total costs consist of three components:

- Direct costs for incremental, out-of-pocket, unbudgeted spending averaged $5 million per company or $50 per lost customer record for outside legal counsel, mail notification letters, calls to individual customers, increased call center costs, and discounted product offers.
- Indirect costs for lost employee productivity averaged $1.5 million per company or $15 per customer record.
- Opportunity costs covering loss of existing customers and increased difficulty in recruiting new customers averaged $7.5 million per company or $75 per lost customer record.10

Regulations and the Costs of Non-Compliance

Federal regulators have become more active in protecting customer data. This has become evident through a series of enforcement actions and consent decrees by the FTC and state attorneys general. In January 2006, ChoicePoint agreed to pay $15 million to settle charges it violated consumer privacy rights — a $10 million penalty.
to the government, and $5 million to compensate approximately 800 individuals who the FTC says became identity-theft victims as a result of the lapse. The $10 million fine is the highest ever levied by the FTC. ChoicePoint also must revamp the way it screens customers, implement new information-handling procedures and obtain independent security audits every other year until 2026.¹¹

In June 2005, BJ’s Wholesale Club agreed to implement a comprehensive data-security system and undergo biannual third-party security audits for the next 20 years in order to settle FTC charges that its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated federal law.¹²

Other companies have reached agreement with the FTC regarding their alleged failure to provide adequate security for their data, including Sunbelt Lending Services, Petco Animal Supplies, Tower Records, Microsoft and Eli Lilly. Barnes and Noble and Ziff Davis Media have reached similar agreements with the Attorney General of New York.

The Cost of Adverse Publicity

In the aforementioned ChoicePoint settlement with the FTC, the company’s share price dropped $3.35, or 7.2%, the day of the announcement.¹³ This is not unusual. A Congressional Research Service Report for Congress published in April 2004 and titled, “The Economic Impact of Cyber-Attacks,” shows that companies identified as victims of cyber-attacks in media reports suffered stock price drops of 1% to 5% in the days immediately following the reports. For the average New York Stock Exchange Corporation, price drops of these magnitudes translate into shareholder losses of between $50-million and $200-million.¹⁴

The Costs of Retaining Customers

Financial institutions are extremely sensitive to the potential loss of customers as a result of a data security breach. PNC offers coverage to customers with multiple accounts, covering expenses associated with restoring a credit history. Washington Mutual offers its coverage to its checking account customers, which includes up to $5,000 for recovery expenses.¹⁵

E*Trade Financial Corporation, reacting to the increasing importance of online security to many customers, offers to cover client losses from fraud on the Web. E*Trade COO R. Jarrett Lilien said, “The cost of doing nothing is that customers lose faith and confidence in transacting online,” and projected E*Trade’s exposure in offering the protection to be as much as $5 million in 2006 and $10 million in 2007.¹⁶

ChoicePoint agreed to pay $15 million to settle charges it violated consumer privacy rights – a $10 million penalty to the government, and $5 million to compensate approximately 800 individuals who the FTC says became identity-theft victims as a result of the lapse.

Companies identified as victims of cyber-attacks in media reports suffered stock price drops of 1% to 5%, which translates into shareholder losses of between $50 million and $200 million.

The cost of doing nothing is that customers lose faith and confidence in transacting online.
The Cost of Lawsuits

A July 21, 2005 article by David Banks in the Wall Street Journal titled, Security Breaches of Customers’ Data Trigger Lawsuits, describes class-action suits filed in connection with several breaches including Bank of America, ChoicePoint, LexisNexis and CardSystems Solutions and states that BJ’s Wholesale Club has a $16-million reserve to cover all costs related to their breach. According to Tom Holt Jr., a lawyer with Kirkpatrick & Lockhart, Nicholson Graham LLP in Boston, which defends companies against data-loss claims, “The class-action suits will in a somewhat perverse way allow the forces of the marketplace to act as the enforcement mechanism. The companies that have behaved most diligently will be in the best position to defend themselves.”

The Cost of Handling a Breach Well

Early on the morning of July 28, 2003, Acxiom Corporation, a leading provider of customer data integration technology headquartered in Little Rock, AK, was contacted by the Hamilton County, OH, Sheriff’s Office. Evidence uncovered during the investigation of a known hacker in the area eventually revealed that Daniel Baas, an employee of an Acxiom client, had used his legitimate online access to execute an unauthorized download of a password table. He subsequently used passwords to access multiple customer accounts. Acxiom officials immediately took actions to mitigate the damage, including:

- Identifying the scope of the compromise and taking corrective actions
- Working with potentially impacted clients
- Assisting law enforcement
- Communicating with regulators and the media
- Initiating internal and third-party security audits

By most standards, Acxiom handled the data security breach very well. Law enforcement officers continually confirmed that there was no evidence of any attempt to use the stolen data for identity theft or other consumer harm, and there were no fines or lawsuits. At an American Conference Institute presentation on Data Security Breaches and ID Theft in September 2005, Tim Spainhour, Legal Compliance Leader for Acxiom Corporation, stated that a recent financial audit showed that Acxiom’s breach related costs totaled $7 million.
Conclusion

The annual cost of identity fraud is over $50 billion. About 10% is in the form of out-of-pocket costs paid by the victims, and 90% is initially absorbed by the affected institutions (although, much, if not all, of that cost is eventually paid by consumers in the form of higher prices and by shareholders in the form of lower earnings and reduced stock value).

The rapid deployment of Web access by businesses, especially financial institutions and data brokers, has magnified vulnerabilities that are not adequately addressed by traditional network security techniques, and increased the risk of online data theft. According to the Federal Trade Commission, “Attacks on Web applications often pass undetected through firewalls and other network defense systems, putting at risk the sensitive information that these applications access. Application vulnerabilities are often neglected, but they are as important to deal with as network issues.”

The annual cost of data theft due to online fraud and application hacking is about $6 billion, with the costs to the financial institutions and data brokers referenced in this paper ranging from a low of $7 million to over $52 million, and E*Trade projecting annual losses up to $5 million or $10 million to cover customer losses from online fraud. TowerGroup estimates that every $1 financial institutions spend on fraud management technology yields a reduction in fraud loss of up to $8. Therefore, companies should assess online fraud and identity data theft solutions as part of an information risk management program and implement solutions that provide the best return on investment.

— END —
About the Author and the Company

Bruce Pharr is Director of Marketing for Covelight Systems. He has written articles on technical and business topics which have appeared in American, Asian and European publications. He has over two decades of experience in strategic analysis and planning, product and brand management, and marketing communications with companies involved in information technology and the evolution and convergence of voice, data and multimedia communications.

Covelight Systems is a leader in the emerging technology of passive, real-time user monitoring and profiling for online fraud and information risk mitigation. Covelight provides a single source solution to detect external and internal threats without degrading Web application availability or performance.

Annotations

1 Elizabeth Robinson, Stemming Identity Theft: The Regulators Step In, TowerGroup, p 1 (April 2005).
3 California Senate Assembly Committee on Business and Professions, Hearing on SB 1386, 2001-2002 Legislative Second Session (August 5, 2002).
5 California Civil Code § 1798.82(b) (2003).
8 Id. at p 4.
16 Gaston F. Ceron, E*Trade to Offer Brokerage Clients Loss Protection for Online Fraud, Wall Street Journal, p D2 (January 18, 2006).
20 Virginia Garcia, Taming the Hydra: The Emergence of Enterprise Fraud Management in Financial Services, TowerGroup, p 6 (June 2005).