# The Market Value and Reputational Effects from Lost Confidential Information

**Joseph K. Tanimura*, Eric W. Wehrly****

**Abstract**

According to many business publications, firms that experience information security breaches suffer substantial reputational penalties. This paper examines incidents in which confidential information, for a firm's customers or employees, is stolen from or lost by publicly traded companies. Firms that experience such breaches suffer statistically significant losses in the market value of their equity. On the whole, the data indicate that these losses are of similar magnitudes to the direct costs. Thus, direct costs, and not reputational penalties, are the primary deterrents to information security breaches. Contrary to many published assertions, on average, firms that lose customer information do not suffer reputational penalties. However, when firms lose employee information, we find significant reputational penalties.

**Keywords:** Confidential, Information Security, Data Security, Breaches, Reputational Penalties

## Introduction

A breach in information or data security occurs when confidential personal data is stolen from or lost by a firm. In one of the first widely-publicized incidents, on February 15, 2005, Choice Point announced that 145,000 personal records had been accessed by suspected criminals passing themselves off as legitimate customers. More recently, Western Union announced that hackers had stolen the names, addresses, phone numbers, and credit card numbers of more than 20,000 customers. In this paper, we estimate the costs of security lapses, and examine whether public firms incur any reputational penalties when they suffer data breaches.

A firm will incur a reputational penalty if the total costs of the breach—as measured by the market value loss in the company's shares—exceed the direct costs of the breach. The direct costs include unbudgeted, out-of-pocket spending for things such as notification letters and emails, legal and accounting fees, public and investor relations, and call center expenses. Direct costs also include the opportunity costs of spending company resources such as employee time in order to deal with the consequences of the data breach, and fines levied by government agencies. A reputational penalty exists when, for example, news of Western Union's lost information causes the firm's market value to decrease by an amount greater than the expected direct costs associated with the breach.

The existence and magnitude of a reputational penalty is important for public policy. For example, ChoicePoint was fined $10 million by the Federal Trade Commission in 2006. Whether this penalty is sufficient to deter future data breaches depends in large part on the reputational penalty that firms incur when they suffer breaches. If reputational penalties are large, then advocates for higher regulatory sanctions and lower legal hurdles for plaintiffs are misguided. If, however, reputational penalties are negligible, these advocates have greater standing.

The existence of reputational penalties also informs firms' investment policies. If reputational penalties are large, then investment in information security will yield greater returns. On the other hand, if—contrary to most media reports—reputational penalties are small or non-existent, firms have reduced incentive to invest resources in safeguarding information.

According to most business publications, firms suffer substantial reputational penalties as a result of information security breaches. For example, the chief technology officer of a company that suffered a breach states, "When something like this happens, we don't want to put a price

* Unaffiliated, Los Angeles, United States. E-mail: jtanimura@hotmail.com
** Visiting Assistant Professor, Seattle University, United States. E-mail: wehrlye@seattleu.edu

on reputation, but it's significant."[1] Commentators in a *Harvard Business Review* case study on compromised customer data echo a similar sentiment. One of them, a senior executive of ChoicePoint, states, "Mitigating the effects on [the fictional company's] brand and reputation will take, I estimate, three to five years."[2] Customer survey results also support the existence of reputational penalties: 78 percent of customers said they would be unlikely to continue shopping at a store once they had learned of a data breach there.[3]

Moreover, information breaches and reputational effects have received attention on a global stage, as this excerpt from *The Economist* indicates: "American firms and institutions seem particularly lax at safeguarding private information. The European Union's data-protection directive has encouraged firms in Europe to take the issue more seriously. In America firms have little incentive to do so. Carelessness brings few penalties other than a blow to a corporate reputation that may soon pass."[4] While *The Economist* takes a more moderate position regarding the duration of the reputational effect, all of the above suggest that there are reputational penalties.

On the contrary, there are some who doubt the existence of reputational penalties.[5] There are several reasons why a reputational effect may not exist. First, there is often no direct relation between the individual whose data are compromised and the responsible firms. Second, in the case of financial institutions, a consumer may face switching costs when changing his bank and credit relationships; moreover, there is no guarantee that the new institution will have better data security. Third, as data breaches become more commonplace, the public might gradually come to perceive data breaches as normal, and will be less likely to punish businesses by avoiding them. These arguments are especially persuasive given the lack of large-sample empirical results supporting the existence of reputational penalties.

Our study provides large-sample estimates of the share valuation impact, and is the first to estimate the market-value costs and reputational effects for firms that suffer confidential data breaches. We examine 152 incidents from 2000 to 2007, and find that news of a data breach corresponds to economically meaningful and statistically significant losses in the share values of the firms suffering the breaches. Initial press announcements are associated with an average abnormal stock return of -0.23 percent, which equates to an average decrease in market value of $136 million.

The individual firm market value losses, however, are of similar magnitudes to the direct costs of the breaches. Using an average of publicized estimates of costs, an information breach results in an estimated average direct cost of 0.93 percent of market value. Intriguingly, this study also suggests that instances involving employee information—but not customer information—induce a reputational effect. For 39 events involving breaches of employee data (26% of the full sample), the mean abnormal return is a highly significant -0.55 percent. For these observations, we find a highly significant -0.46 percent reputational effect; for these instances only, the market value losses exceed direct costs. In Section 5 we interpret these results.

This paper is organized as follows. Section 2 reviews the relevant literature, and formulates our research question. Section 3 describes our sample and Section 4 reports on the share value effects for firms that suffer data breaches. Section 5 reports on the reputational penalties for firms that experience breaches in data security. In Section 6, we investigate possible explanations for our failure to find a reputational penalty and the determinants of cross-sectional differences in stock price effects. Section 7 concludes the paper.

## Information Breaches and Quality Assurance through Reputation

Consumers, employees, and other stakeholders entrust companies with confidential information. In varying degrees, the safeguarding of this information is part of the product or service quality offered by a firm to its customers. For example, Peter Burns, vice president and director of the Payment Cards Center at the Federal Reserve Bank of Philadelphia, states, "Security can be a competitive differentiator." Similarly, consumer survey results suggest that consumers rank superior security

1 Information Week. 2006. "The High Cost of Data Loss." March 20.

2 Eric McNulty, Boss, I Think Someone Stole Our Customer Data, Harvard Business Review, September 2007.

3 McNulty, *supra* note 2.

4 The Economist. 2007. "Lax Maxx." March 30.

5 See, e.g., Paul M. Schwartz & Edward J. Janger, Notification of Data Security Breaches, 105 Michigan Law Rev. 913 (2007).

against identity fraud as the second most important factor they look for in a new credit card issuer, behind only low interest rates.[6]

A firm's reputation for protecting personal information can also affect its employees' salary demands or, possibly, labor turnover. Assessing the quality of a firm's information security is difficult and costly. Countless publications and Internet sites publish information about the health, safety, and performance of various consumer products, while investment banks and other research houses issue copious analyses of the strategic and financial positions of public companies. Information concerning a firm's exposure to information loss, however, is not readily available. Stakeholders must essentially rely on a company's reputation or brand identity as a quality-assuring device.

The seminal work of Klein and Leffler (1981) establishes the idea of reputations or brand names as quality-assuring devices. They develop a model in which firm-specific capital investments, such as those incurred in establishing a brand name, provide a mechanism for assuring contractual performance.[7] Similarly, firms invest in information security to reduce information loss, and therefore enhance their reputation for safeguarding confidential information. In this framework, the value of future, repeat transactions impels an investment to preserve the firm's brand name and reputation. When a firm leaks sensitive information, it manifests a product defect; thus, product quality reputation is harmed by incidents of information loss.

Consider a simple case in which a single firm is selling a product to consumers, and collects credit card information during the sales process. Consumers value a reduction in the probability of lost or otherwise compromised personal information, but the reduction is costly. Consumers can reduce the probability of compromised information by making firms face civil penalties and/or reputational losses. Civil actions are costly: direct costs include administrative, legal, and enforcement costs. Additionally, civil fines cause indirect costs to firms and consumers; as detailed in the next paragraph, the threat of civil actions induces optimally higher investment in information security, and thus higher prices to end users. Reputational penalties are also costly; their origins lie in the lost rents derived from high prices charged to consumers for high quality assurance, including information security.

Because the threat of fines or other penalties motivate additional investment in information security, consumers partially bear the costs of higher information security. At some point, the cost to consumers of extra security exceeds the incremental expected cost of compromised information. If the costs associated with information breaches are low, or if consumers can insure themselves against lost information for little cost, then firms will invest less in security and provide less quality assurance. If information breaches are costly, then firms will be induced to invest more and provide greater quality assurance. At some point, the costs of reducing the probability of an information breach exceed the expected benefits. As a result, the optimal number of information breaches is not zero. Firms will continue to increase investments in information security until the marginal cost equals the marginal benefit.

As a guarantor of quality, reputation encompasses many attributes, including security of confidential information. Reputation can result in supra-competitive prices and associated rents. As Klein and Leffler (1981) point out, firms will compete to obtain these rents by providing additional goods and services, including information safekeeping. Different firms can meet the demand of different consumer clienteles by investing in differing amounts of security. When an information breach occurs, consumers update their perception of the firm's investment in security, and a reputational loss can occur. A reputational loss is said to have occurred when the market value loss reflected by the stock price decrease is greater than the direct costs associated with the event.

Previous research has found reputational losses in a variety of industries, for diverse products, and for different behaviors. In the case of drug and auto recalls, Jarrell and Peltzman (1985) provide evidence of reputational effects--wealth losses in excess of out-of-pocket costs--associated with reduction in product quality.[8] Mitchell and Maloney (1989) examine plane crashes, and find reputational losses for crashes caused by pilot error, but no

6 Digital Transactions News. 2007. "Data Breaches Don't Spur as Much Fraud as Stolen Cards, Other Causes." February 8.

7 Benjamin Klein & Keith B. Leffler, The Role of Market Forces in Assuring Contractual Performance, 89 J. Pol. Econ. 615 (1981).

8 Gregg Jarrell & Sam Peltzman, The Impact of Product Recalls on the Wealth of Sellers, 93 J. Pol. Econ. 512 (1985).

such losses where the pilot or airline was not at fault.[9] In an examination of the 1982 Tylenol poisonings, Mitchell (1989) shows that market losses to Johnson & Johnson far exceed direct costs and losses shared with other pain-reliever producers, and concludes that the company suffered a substantial loss in the value of its brand-name (reputational) capital. For this same incident, Dowdell, Govindaraj, and Jain (1992) show that while Johnson & Johnson's stock value declined by 29 percent, competing drug firms' stocks showed no reaction until subsequent packaging regulations imposed costs on the industry.[10]

The above research shows that demonstrated changes in product quality cause reputational effects. Other behaviors also cause perceived changes in product quality, and can be penalized by reputation effects. Karpoff and Lott (1993) find that the reputational harm from criminal fraud is significant.[11] Announcements of alleged or actual fraudulent activity by firms result in a significantly negative 1.58 percent abnormal return for a (-1,0) window. The firm's expected legal fees and penalties constitute only a small fraction of the firm's stock market value loss; thus, at least part of the remaining loss represents reputational harm. The authors also find large reputational penalties associated with frauds of stakeholders, governmental agencies, and investors, but the reputation loss is negligible for frauds involving regulatory violations.

The research in this area establishes the following stylized facts: the market penalizes firms that violate the trust of those parties with whom the firm does business, but does not appear to impose losses in instances where there is no implicit or explicit contract with a stakeholder. As examples of the former, Clifford Smith (1992) also finds reputational costs stemming from deceptive bidding practices;[12] Karpoff and Lott (1999) find reputational penalties associated with punitive damages lawsuits.[13] Karpoff, Lee, and Vendrzyk (1999) find significant reputational effects for defense procurement fraud;[14] and Karpoff, Lee, and Martin (2008) show reputational effects for firms committing financial misrepresentation.

On the other hand, Karpoff, Lott, and Wehrly (2005) find that environmental violations are not disciplined through reputational penalties.[15] Unlike corporate frauds, which tend to harm stakeholders and business counterparties, environmental violations impose costs on parties other than those with whom the polluting firm does business. And while the abnormal returns are significantly negative around the announcement of an environmental violation, the expected legal penalties and clean-up costs explain the entire loss in market value; hence, no reputation effect exists.

To date, research regarding information security breaches has been generally hampered by small sample sizes, particularly for events involving compromised confidential information. Several studies related to the present paper examine a variety of "information security breaches," including such events as denial of service (DOS) attacks, Web site defacements, and virus attacks. In these events, no confidential personal information is actually compromised; firms suffer from interrupted commerce or virtual graffiti. Table 1 summarizes the key points from these studies.

Campbell, Gordon, Loeb and Zhou (2003) investigate 43 publicly announced security breaches, including the events mentioned above; of these, only 11 breaches involved compromised confidential data.[16] For these eleven events, the authors find a significantly negative three-day cumulative abnormal return, but do not examine reputational effects. Garg, Curtis, and Halper (2003) note

9 Mark L. Mitchell & Michael T. Maloney, Crisis in the Cockpit? The Role of Market Forces in Promoting Air Travel Safety, 32 J. Law & Econ.329 (1989).

10 Thomas D.Dowdell, Suresh Govindaraj, & Prem C. Jain, The Tylenol Incident, Ensuing Regulation, and Stock Prices, 27J. Fin. & Quantitative Analysis 283 (1992).

11 Jonathan M. Karpoff & John R. Lott, Jr., The Reputational Penalty Firms Bear from Committing Criminal Fraud,36 J. Law& Econ. 757 (1993).

12 Clifford Smith, Jr., Economics and Ethics: The Case of Salomon Brothers, 5 J. Applied Corp.Fin. 23 (1992).

13 Jonathan M. Karpoff & John R. Lott, Jr., On the Determinants and Importance of Punitive Damages Awards.62 J. Law & Econ.527 (1999).

14 Jonathan M. Karpoff, D. Scott Lee, & Valaria Vendrzyk, Defense Procurement Fraud, Penalties, and Contractor Influence.107J. Pol.Econ.809 (1999).

15 Jonathan M. Karpoff, John R. Lott, Jr., & Eric W. Wehrly. The Reputational Penalty for Environmental Violations: Empirical Evidence, 48 J. Law & Econ. 653 (2005).

16 Katherine Campbell, Lawrence R. Gordon, Martin P. Loeb, & Lei Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, 11 J. Computer Security 431 (2003).

that virus attacks often affect an entire market, and therefore isolating the impact on a single company is problematic.[17] For this reason, their study excludes virus attacks. For their study of 22 security breaches during the 1999-2002 period, the authors include Web site defacements and DOS attacks; less than 10 events involve the loss of confidential information. For their sub-sample of four high-profile events involving the theft of credit-card information, they find a negative 9.0 percent cumulative abnormal return for a (0,1) window. Cavusoglu, Mishra, and Raghunathan (2004) study 66 security breach announcements during the 1996-2001period.[18] These breaches include 34 Web site defacements and DOS attacks, which are grouped together as "availability attacks." The 32 other security breaches are coded as "other attacks." Importantly, the data used in the Cavusoglu, et. al. (2004) study do not distinguish between events which involve compromised personal information and other security-related events. For the entire sample, the authors find a significantly negative 2.1 percent two-day cumulative abnormal return for a (0,1) window. Kannan, Ress, and Sridhar (2007) study 102 security breaches involving 60 companies between 1997 and 2003.[19] These events include breaches of source code, viruses, worms, DOS attacks, power outages, and hardware failures. For the 72 events with sufficient data to estimate cumulative abnormal stock returns, the authors do not find any statistically significant results.

Our work categorically differs from those outlined above. Data on lost confidential information is used to evaluate whether firms suffer reputational penalties. When an information breach occurs, consumers update their perception of the firm's investment in security, and a reputational loss can occur. The resulting reputational loss, if any, will depend on a number of factors, including the nature of the information, the manner in which it was compromised, and the number of customers or employees affected. This paper will address those differences, and seeks to determine whether information breaches are perceived as significant deterrents to continued commercial relationships; finding a reputational loss for these events would suggest as much.

## Data

### Sample Selection

We examine 152 cases in which confidential data was stolen from or lost by publicly traded companies or their subsidiaries. The incidents involve 117 separate firms, and span the period from September 11, 2000 to June 23, 2007. The sample is obtained from two sources, Attrition and the Privacy Rights Clearinghouse (PRC). Attrition is a website focusing on information security. The Attrition database of security breaches runs from 2000 to the present, and contains a web link to a news article about each incident. The news articles were reviewed by the authors in order to confirm the gathered information and code the descriptive variables. These variables will be described in more detail below. The Attrition data was supplemented with a chronology of data breaches from the PRC. The PRC is a project of the Utility Consumers' Action Network, a non-profit consumer advocacy organization. The PRC chronology begins February 15, 2005, and contains basic descriptive information about each incident.

We verified the information obtained from Attrition and the PRC by searching the LexisNexis database for public announcements of the breaches. Each announcement was read in order to check whether (1) a data breach actually occurred, (2) the company identified in the announcement was actually responsible for the data breach, (3) the coding of the descriptive variables was accurate and consistent, and (4) additional companies needed to be added to the sample.[20] In cases where an announcement could not be found in LexisNexis, the incident was dropped if its only source was the PRC chronology; similar incidents from

17 Asish Garg, Jeffrey Curtis,& Hilary Halper, Quantifying the Financial Impact of IT Security Breaches,11 Info. Mgmt. & Computer Security 74 (2003).

18 Huseyin Cavusoglu, Birendra Mishra, & Srinivasan Raghunathan. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, 9 Int. J. Elec. Commerce 69 (2004).

19 Karthik Kannan, Jackie Rees, & Sanjay Srikhar, Market Reactions to Information Security Breach Announcements: An Empirical Analysis, 12 Int. J. of Elec. Commerce 69 (2007).

20 Companies were added to the sample if they were not listed in the Attrition database or PRC chronology, and the article indicated that they were partially responsible for the data breach. In all of these cases, the additional company was providing services to the company when the data breach occurred. As an example, Time Warner announced on May 2, 2005 that its outside storage company, Iron Mountain, had lost computer backup tapes.

Attrition were not dropped since the database contains a Web link to a news article about the incident. We focused on the first announcement to the general public, and not the date that affected individuals were directly notified that their personal data had been compromised. We searched LexisNexis for fourteen days prior to the Attrition and/or PRC dates for earlier announcements. If the search yielded an earlier announcement date, it was substituted for the Attrition and/or PRC dates. The Lexis Nexis date was also used as the event date if the PRC and LexisNexis dates differed, and the incident's only source was the PRC chronology.

An incident is excluded from the sample if the implicated company's stock or ADRs were not listed on a major U.S. stock exchange at the time of the announcement. In addition, an incident is excluded if there was a contemporaneous announcement of bad news unrelated to the data breach. This is necessary because any negative announcement-period stock price reaction could have been caused by the unrelated bad news.[21] Contemporaneous announcements are defined as ones that occurred within a 3-day window starting one day before and ending one day after the incident. The announcements were identified by searching the LexisNexis database. Finally, a few incidents were excluded because the historical return series was not long enough to properly estimate the market model.

## Descriptive Statistics

Table 2 contains summary information about the sample. The table classifies events according to the type of data, type of breach, relation of affected persons to the responsible company, and involvement of outside or third parties.

### Type of Data

The variable is coded according to the most important type of data contained in the personal information.[22] Thus if the information contains Social Security numbers, the variable is always coded as such. As an example, Wells Fargo reported on November 20, 2003 that customer names, addresses, account numbers, and Social Security numbers were stolen from a California office. The data-type variable in this instance is coded as "Social Security number" even though the information also contains customer names, addresses, and account numbers. Similarly, if the information contains credit or debit card numbers, the variable is coded as such unless the lost information also contains Social Security numbers. Finally, if the information contains other financial information such as account numbers that are not related to credit/debit cards, the variable is coded as such unless it also contains Social Security or credit/debit card numbers. Incidents coded as "Social Security number" comprise 59 percent of the sample. "Credit card number" and "Other financial information" account for 17 percent and 12 percent, respectively. All other data types are relatively infrequent, and are grouped under "Misc. personal information." This category includes names and street addresses, email addresses, and medical information.

### Breach Type

The breakdown of the sample by breach type shows that computer hardware such as laptop computers was stolen in 38 percent of the incidents. The second most common type of breach involves information that was lost, placed in the trash, or mistakenly disclosed via mail, fax, or email. The third most common type involves the Internet. In these incidents, a computer system was hacked via the Internet or personal information was mistakenly made available without proper security on the World Wide Web. Fraud is the least prevalent, accounting for only 15 percent of the breaches.

### Relation of Affected Persons to the Responsible Company

The categorization in Table 2 shows that in 97 of the 152 events, the information concerns direct-past or present-customers of the responsible companies. A further 16 events involve confidential information lost by companies providing services for businesses and government agencies. These are coded as "Indirect customer" because the affected individuals are not direct customers

21 Results do not materially change when good news events are also excluded.

22 Social Security numbers are widely regarded as posing the highest risk for identity theft. Credit card losses for individuals are limited to $50, and this amount is often reduced to zero by credit card issuers. Fair Credit Billing Act: http://www.ftc.gov/bcp/conline/pubs/credit/fcb.shtm , and http://www.ftc.gov/os/statutes/fcb/fcb.pdf

of the company. As an example, ChoicePoint reported on February 15, 2005 that thieves had penetrated the firm's computer network by impersonating as legitimate business entities. This incident is categorized as "Indirect customer" because ChoicePoint collects and sells personal data to businesses and government agencies.[23] The remaining 39 incidents are coded as "Employee" because the data contains personal information about the company's past or present employees. If the data contains both customer and employee information, the categorization depends on which group has the most affected persons.

### Inside or Outside Party Responsible

Table 2 shows that 59 of the 152 events were caused by an inside party. In these incidents, a company employee or a third party that was providing services to the company was responsible for the data loss. The 59 inside incidents are further broken down into accidental ones (n = 47) and malicious ones (n = 12). As an example of an "Accidental inside" event caused by a third party, McAfee announced on February 23, 2006 that its auditor, Deloitte & Touche, had lost a CD with data on its employees. The March 14, 2006 General Motors incidents an example of a "Malicious inside" event. In that case, a former General Motors security guard was charged with taking employee Social Security numbers. All other incidents are classified as "Outside" incidents. Accidental inside incidents usually involve lost data (74 percent) or the Internet (23 percent), while outside incidents usually involve stolen computer hardware (63 percent) or the Internet (21 percent).

### Third Party Involvement

Events are coded as involving a third party if another company was partially responsible for the data loss. In most of them, the information was lost by a third party while it was legitimately providing services to its client. As an example, consider the McAfee incident mentioned above in which Deloitte & Touche lost a data CD while it was providing auditing services to McAfee. In most cases (74 percent), a third party was not involved.

23 Examples of other services and the companies providing them include: administrative (Bisys Group), database management (IBM), records management (IronMountain), and payroll (Automatic Data Processing).

### Additional Summary Statistics

Table 3 classifies events according to the year of the first public announcement. Prior to 2005, there were only 15 publicized incidents of information breaches. The number of incidents dramatically increased from 4 in 2004 to 42 in 2005. This is likely the result of state security breach laws, which were passed with increasing frequency starting in 2005. Prior to 2005, California was the only state with a breach disclosure law. Twenty-eight state laws became effective during 2005 (n = 9) and 2006 (n = 19); as of June 2007, seven state laws have become effective.

Table 3 also provides a breakdown of the incidents by industry and the number of affected individuals. Two industries account for 62 percent of the incidents. The finance, insurance, and real estate industry comprises 39 percent of the sample, while the service industry comprises 22 percent of the sample. Data on the number of individual records is available for 102 of the 152 events in the final sample. We only collect data on the number of records if the figure was released contemporaneously with the initial announcement of the data breach. For announcements that update a previous figure, we calculate the increase in the number of records.

## Market Value Effects of Information Breaches:

In this section, we use event study methodology to investigate the effects on firm value when news about an information breach is first announced. Consistent with other event studies, the abnormal return for the common stock of firm *j* on day *t* is defined as

$$AR_{jt} = R_{jt} - \left(\alpha_j + \beta_j R_{mt}\right),$$

Where:

$R_{jt}$= return of common stock *j* on day *t*, and

$R_{mt}$= return of the CRSP value-weighted market index on day *t*.

The coefficients are ordinary least squares estimates of firm *j*'s market model parameters. Daily stock and market index returns were obtained from the Center for Research in Security Prices at the University of Chicago. The estimation period for the market model is 180 days,

beginning 200 days before the announcement. Z-statistics are calculated using the procedure outlined in Salinger (1992).[24]

The abnormal returns are calculated over the 2-day event window starting the day of the announcement. There are several reasons in favor of the (0,1) window. The (0,1) window is appropriate for an announcement made after the close of trading because any effect is captured by the stock price on the day after the announcement. The window is also proper if the initial announcement was not widely disseminated. According to our LexisNexis (accessed 2007 and 2008) database search results, many of the announcements in our sample were made after the close of trading (i.e., 1:00 PM Eastern). In addition, several of the announcements may not have been widely disseminated because they were made by local news sources or Internet sites (for example, pcworld.com, securitypronews.com, silicon.com, taxcut.com, techcrunch.com). Finally, the (0,1) window is consistent with past studies of information security breaches.[25] To the extent there was leakage or the actual announcement day preceded the day used in this study, our tests are biased toward accepting the null hypothesis of no abnormal returns in the event window.

In order to account for outliers, we set the minimum and maximum 2-day abnormal stock returns equal to the 5$^{th}$ and 95$^{th}$ percentiles, respectively. The average abnormal return for the entire sample is -0.23 percent with a Z-statistic of -1.967, which is significant at the 5% level.[26] This stock price reaction is substantially smaller than the average -2.1 percent found byCavusoglu, Mishra and Raghunathan (2004)) and -5.5 percent found by Campbell, Gordon, Loeb and Zhou (2003)). One possible explanation for the difference with Cavusoglu, Mishra and Raghunathan (2004) is that the samples contain different types of events. Their sample contains two types of breaches, availability (n = 34) and non-availability (n = 32), and our sample is a subset of the latter type. In addition, their sample does not contain any accidental data breaches, whereas accidents comprise 31 percent of our sample. If we exclude the 47 accidental data breaches in our sample, the average abnormal return is -0.27 percent with a Z-statistic of -2.034. Although the stock price reaction increases, it is still 87 percent smaller than the Cavusoglu, Mishra and Raghunathan (2004) result.

Table 4 reports the abnormal returns and Z-statistics broken down by various descriptive variables. The mean abnormal return accompanying announcements of data breaches involving Social Security numbers is -0.20 percent with a Z-statistic of -0.853. The result is surprising since Social Security numbers are the one of the most important pieces of individual identification. The average for incidents involving credit card numbers is also statistically insignificant. The mean abnormal stock return for incidents involving other financial information is -0.71 percent, and is statistically significant at the 10% level. Finally, the average return for events involving miscellaneous personal information is -0.17 percent with a Z-statistic of -1.867; non-parametric test results discussed below suggest that this test statistic is strongly influenced by extreme values.

The mean abnormal return accompanying announcements of data breaches involving stolen computer hardware is -0.37 percent, and is statistically significant at the 5% level. The averages for incidents involving the other three categories are statistically insignificant. The results are difficult to interpret because it is impossible to know ex ante which type of breach is worse. For example, a data breach in which a laptop computer was stolen from the front seat of an employee's unlocked car would be classified as involving stolen hardware. However, one can argue that it was the negligence of the employee that caused the data breach in the first place. In this case, the incident becomes similar to one involving lost data.

The average abnormal return for data breaches involving direct customer data is -0.09 percent, and is statistically insignificant—a surprising result, since customers can easily punish a firm with a poor reputation for protecting data. Interestingly, the results also suggest that the market penalizes firms that lose employee information. The mean abnormal return accompanying announcements of data breaches involving employee data is a highly significant -0.55 percent (Z-statistic of -2.287). This result complements the results found in studies examining the stock market effects associated with missteps in the

24 Michael Salinger, Standard Errors in Event Studies, 27 J. Fin. & Quantitative Analysis 39 (1992).

25 Garg, Curtis, & Halper, *supra* note 19; Cavusoglu, Mishra, & Raghunathan, *supra* note 20.

26 The average abnormal return is -0.38 percent if the outliers are not truncated, and is statistically significant at the 5% level.

labor market (see Hersch, 1991, and Davidson, Worrell, and Cheng, 1994).[27]

The mean abnormal return for announcements of data breaches involving outsiders is -0.29 percent, and is statistically significant at the 10% level. The averages for inside breaches, accidental and malicious, are statistically insignificant. The results suggest that the market only punishes a company if the breach was caused by outsiders. However, it is difficult to know ex ante what precautions the firm had in place. A lax security system that allows a theft would be classified as an outside incident even though the company could have easily prevented it. In this case, the incident becomes similar to ones classified as accidental inside.

The mean abnormal return for data breaches that do not involve a third party is -0.27 percent, and is statistically significant at the 5% level. Those breaches that do involve a third party entail an insignificant average abnormal return. These results are not surprising. For breaches occurring at a third party service provider, one would expect ex ante that the firm was not to blame for the breach unless it was negligent in hiring the third party service provider.

The only industry with a statistically significant stock price reaction is finance, insurance, and real estate (2-digit SIC code 60-62). The average 2-day abnormal stock return is -0.27 percent with a Z-statistic of -1.978.

The only year with a statistically significant stock price reaction is 2006. The mean abnormal return is -0.40 percent, and is statistically significant at the 5% level.

Nonparametric test statistics (not reported in Table 4) yield inferences that are similar to those reported above. The Wilcoxon signed-rank test statistic for all 152 observations is -2.090, which confirms the statistical significance of the result s above. The one exception is for incidents involving miscellaneous personal information such as names and email addresses. The Z-statistic for these 13 observations falls from -1.867 in the OLS regression to -0.454 for the Wilcoxon signed-rank test, which suggests that the former Z-statistic is being unduly influenced by outliers.

## Direct Costs and Reputational Penalties for Confidential Information Breaches

In this section, we compare the dollar size of the estimated loss in market value with estimates of the direct costs incurred by firms that suffered data breaches. The difference between the total loss in market value and the loss attributable to direct costs is an estimate of the reputational cost.

Two recent reports by Forrester Research and the Ponemon Institute contain estimates of the direct costs of data breaches on a per-record basis.[28] The first direct cost category is unbudgeted, out-of-pocket spending and includes costs related to (1) discounted product or service offers,(2) notification letters, phone calls, and emails, (3) legal, audit, and accounting fees, (4) call center expenses, and (5) public and investor relations. The 2007 Forrester study contains three cost estimates ($50, $55, $115; low, medium and high, respectively) with an average of approximately $73. The Ponemon estimates from the 2005 and 2006 studies are $50 and $54, respectively.

The second category is lost employee time and productivity. The average of three estimates ($20, $25, and $30) from the Forrester study is $25. The 2005 and 2006 Ponemon estimates are $15 and $30, respectively.

The third category is fines levied by government agencies (e.g., Federal Trade Commission). The Forrester study contains three estimates ($0, $25, $60) with an approximate average of $28. The Ponemon study does not include a fines figure.

In sum, the three estimates of total direct costs from the Forester study are $70, $105, and $205, with an average of $127. The average from the 2006 Ponemon study is

27 For example, Hersch examines the stock price reactions to announcements of violations of equal opportunity employment laws. Joni Hersch, Equal Employment Opportunity Law and Firm Valuation, J. Human Resources 26 (1991). Davidson, Worrell, and Cheng examine the stock price reactions to announcements of OSHA violations. Wallace N. Davidson III, Dan Worrell, & Louis T. W. Cheng, The Effectiveness of OSHA Penalties: A Stock-Market-Based Approach, Industrial Relations 33 (1994).

28 The Forrester figures are based on a survey sent to 28 companies that experienced a data breach. Forrester Research, Teleconference, The Cost Of A Security Breach, April 25, 2007. The Ponemon figures are based on a survey sent to 31 companies that experienced a data breach between 2005 and 2006. Ponemon Institute, LLC, 2006 Annual Study: Cost of a Data Breach.

$84 if fines are not included, and $112 if the $28 figure from the Forrester study is used to measure fines.

The two studies also contain estimates of the "opportunity costs" of the data breach. These costs are caused by turnover of existing customers and increased difficulty in acquiring new customers. The Forrester study contains three cost estimates ($20, $50, $100) with an average of approximately $57. The Ponemon estimates from the 2005 and 2006 studies are $75 and $98, respectively. These costs are not included because they are a component of the harm that is being measured, namely, reputational harm.

Considering the Forrester and Ponemon estimates above, excluding "opportunity costs", we first conduct analysis using a direct cost range of $50 to $200 per record, focusing on an average cost per record of $100. This amount is slightly less than the average of the studies above, and translates to an average cost per incident of $19.2 million, and a median cost of $3.2 million. Our choice of $100 per record is also influenced by the following studies, which find significantly lower costs on a per-incident basis. In the 12th Annual CSI Computer Crime and Security Survey, Richardson (2007) reports an average cost of $3.9 million per organization for theft of confidential information.[29] An August 2006 study of Department of Justice prosecutions of network attacks, conducted by Trusted Strategies Inc., found that the "average financial loss was more than $3 million per case."[30]

Table 5 presents direct cost and reputational effect estimates for the 103 observations for which data on the total number of records is available. If we use an average of $100 per record to calculate direct costs, the average implied change in market value as a result of the data breach is equal to -0.93 percent. This figure compares to an average abnormal stock return of -0.23 percent. The difference is a positive 0.69 percent; thus, no reputational effect exists. In order for a reputational loss to occur, the market value loss must exceed the direct costs expressed as a percentage of market value. Results for the $50 and $200 per-record cost levels are similar, indicating no reputational loss. For the entire range of per-record cost estimates considered, the estimated direct costs exceed the market value loss. A reputational effect does not appear; in fact, although not statistically significant, these estimates suggest that the market reaction falls short of the expected costs that a firm will incur as a result of the information security breach.

Table 5 also presents results when applying the CSI Survey figure of $3.9 million in costs per incident. For the 152 observations in the full sample, the mean abnormal stock return of -0.23 percent compares closely to the direct cost estimate of -0.27 percent. The resulting reputational effect of 0.04 percent approaches zero, and is not statistically significant. These results cast doubt on claims by various pundits and studies that market participants penalize firms' reputations for instances of information loss. At even the lowest published cost estimates, the market reaction does not indicate any damage to reputation; rather, the market value loss nearly matches the direct cost estimates expressed as a percentage of market value.

In un-tabulated results, we apply a $100 per-record cost estimate, and investigate reputational effects for data breaches broken down by: the type of data lost; the type of breach; whether customer or employee data was lost; whether the breach was effected from within the firm or from without; and whether a third party was involved. We find no statistically significant reputational effects, with one intriguing exception. For the 27 events involving employee information, the mean reputational effect is -0.77 percent, and is statistically significant at the 1% level. This result is confirmed using the $3.9 million per-incident cost estimate. For the 39 observations involving employee data, the reputational effect is -0.46 percent and highly significant. For these events, the market value loss exceeds the estimated direct costs, suggesting that the loss of employee information is more strongly penalized. Such an effect does not exist for the loss of customer information. One possible interpretation is that a firm's loss of internal (employee-related) confidential information signals an egregious lack of care, and creates the perception that all future transactions with this firm will entail a security risk. As a result, potential customers will be less likely to do business with the firm, or require

29 Computer Security Institute, 12th Annual CSI Computer Crime and Security Survey (2007). (Prior to 2007, this study was entitled the "CSI-FBI Computer Crime and Security Survey", reflecting the FBI's contribution to the report.) The average includes an estimate of $2.20 million for the average loss for confidential data originating from mobile device theft, and $5.69 million in losses for other (non-device) thefts of confidential data.

30 Trusted Strategies, Inc., Network Attacks: Analysis of Department of Justice Prosecutions 1999-2006 (2006).

a discount due to the perception of increased risk, and future revenues will decrease.

A complementary interpretation is that there are additional costs associated with breaches involving employee data. These costs will arise if the breach causes a reduction in employee job satisfaction. An employee cannot simply terminate his relationship with his employer because of the high switching costs involved. However, he can lower his effort due to the reduction in job satisfaction. Because an employer cannot enter into an explicit contract regarding the effort, above the minimum, that the employee will put in, there will be a lower level of effort due to reduced job satisfaction after employee-data breaches. In these cases, an employee can penalize his employer much more easily than a customer can penalize her producer. Therefore, when a firm suffers a blow to its reputation as a "good" employer, it will either incur (1) increased direct costs (for example, wages) in order to maintain the pre-breach level of output, or (2) reduced output given the pre-breach level of production costs.

Overall, our results indicate that investors penalize companies for information breaches, but the penalties are generally commensurate with some of the lowest published estimates of associated costs. That is, stock market value losses closely approximate the expected direct costs that the firm will incur in addressing a data breach. Reputational effects are statistically insignificant, and cannot be relied upon to motivate firms to aggressively safeguard confidential customer information.

From a public policy perspective, these findings indicate that advocates for increased legislation and/or fines concerning the protection of confidential information are not entirely misguided.[31] To the extent that the total social costs of breaches exceed the direct costs that are borne by the responsible firms, the lack of reputational penalties can induce an underinvestment in the safeguarding of confidential information. This could be a major issue with respect to the protection of consumer information. On the contrary, the loss of employee information may entail additional penalties. Thus advocates for increased legislation or fines might benefit from focusing their efforts on the protection of consumer data.

From the perspective of the firm's investment policy, for breaches involving customers, the lack of reputational penalties suggests a reduced incentive to invest in information security. However, the results suggest that firm reputation suffers when employee information is compromised. A complementary explanation is that costs are higher for employee-related breaches. The highly significant reputational penalties for these events indicate that these findings are relevant to all employers, both public and private, that are at risk of information security breaches.[32]

## Extensions

### Further Analysis into the Lack of a Reputational Penalty

In the introduction, we mentioned three possible explanations for the lack of a reputational penalty. First, there is often no direct relation between the individual whose data are compromised and the responsible firms. We test this explanation by examining only incidents in which the compromised information concerns direct—past or present—customers of the responsible companies; incidents involving employee data are excluded. We calculate the reputational effect using both the $100 per-record and $3.9 million per-incident cost estimates, and find no reputational effect. Second, in the case of financial institutions, a consumer may face switching costs when changing his bank and credit relationships. In order to test this explanation, we exclude companies from the financial services industries. We find no reputational effect for the remaining firms using both the $100 per-record and $3.9 million per-incident cost estimates. Third, as data breaches become more commonplace, the

31 Note that the lack of reputational penalties is necessary for advocacy of regulatory sanctions, but not sufficient. Social costs—which are difficult to measure—must also be large relative to the direct costs in order for increased sanctions to make sense.

32 Although this study focuses on information security breaches at publicly traded companies, they are also widespread in the public sector. As an example, in February 2007, the state of Connecticut announced that personal information for over 1,700 state employees, including their names and Social Security numbers, was inadvertently posted on the Internet. In another incident involving a public entity, the University of Idaho announced in March 2007 that a data file posted to the school's web site may have put at risk the personal information, including Social Security numbers, of approximately 2,700 university employees.

public might gradually come to perceive data breaches as normal, and will be less likely to punish businesses by avoiding them. Consumers may also believe that they are not told about all of the breaches that do occur.

As of June 2007, fourteen states did not have consumer notification laws. In addition, there are breaches that occur but go unreported because there is no evidence that data was actually lost, or the breach simply goes undetected. If this explanation is correct, the reputational losses will be significant in early years, and then decrease over time. The evidence, however, does not support this explanation.

Another possible reason for our failure to find a reputational penalty is that we overestimate direct costs. Certain companies may incur lower direct costs when there are multiple companies involved in the breach. Take, for example, the 2006 breach involving Williams and Sonoma. In this incident, a laptop computer was stolen from a Deloitte & Touche employee who was conducting an audit of Williams and Sonoma's financial statements. We may be overestimating costs if we impose all of the direct costs on the retailer. In order to test this explanation, we lower the direct costs for incidents involving third parties from $100 to $50 per record. The results are qualitatively unchanged.

Finally, it is possible that there are fixed costs associated with information breaches. In this case, if a firm suffers multiple breaches, the only costs incurred will be the variable costs associated with the breach. We test this by looking at only primary breaches for a given firm.

The average 2-day abnormal stock return for the 116 initial breaches in this sub-sample is -0.25 percent, and is statistically significant at the 10% level. For the remaining 36 events, the average 2-day abnormal stock return is -0.17 percent with a Z-statistic of -1.025. Although the point estimate is 32 percent smaller, given the small sample size, it is not possible to rule out that either the remaining events have the same impact on stock returns as the initial events or that they have no impact. The 90% confidence interval for the 36 remaining events includes both -0.25 percent and zero. (The actual 90% confidence interval runs from -0.47 percent to 0.13 percent.) We do not find a reputational effect for primary breaches using both the $100 per-record and $3.9 million per-incident cost estimates.

## Cross-Sectional Results

In this section, we investigate whether differences in abnormal stock returns are related to the number of individual records compromised in the information breach. Undoubtedly, the direct costs of a data security breach are positively related to the quantity of affected individuals. Indirect costs will have a similar relationship if a larger quantity serves as a stronger condemnation of a firm's reputation for protecting personal data. The magnitude of the abnormal return should therefore be positively related to the number of affected individuals.

The dependent variable in our tests is the 2-day abnormal stock return. The independent variable is the number of individual records compromised in the data breach. We also control for the responsible firm's market value because data breaches do not affect all companies equally. An incident involving, say, 10,000 customers is likely to have a larger stock price effect on a company with a smaller market value, ceteris paribus. This assumption is consistent with the finding in Cavusoglu, Mishra, and Raghunathan (2004) that smaller firms have larger stock price reactions to breach announcements. The coefficients on number affected and market value, both measured in logs, are not statistically significant.

One problem with the previous model is that it treats all data breaches equally after controlling for the number of affected individuals and market value. This creates an inaccuracy because breaches differ in terms of, say, the type of data stolen or the involvement of a third party. In order to address this shortcoming, we estimate five additional models in which we add categorical variables for the various descriptive variables. The (unreported) coefficients on number affected and market value are statistically insignificant in all five models.

We made some simple adjustments to check the robustness of our results. First, in order to account for possible outliers, we estimated a model in which the number of individual records was capped at 1 million. Second, we accounted for events that involved more than one company by equally allocating the total among the responsible companies. Third, we constructed a categorical variable with separate values for incidents involving (a) 10,000 or less individuals, (b) 10,001 to 100,000 individuals, and (c) more than 100,000 individuals. None of the adjustments sharpened our results.

## Conclusion

Debate over the security of confidential personal information frequently relies upon anecdotes or small-sample empirical studies. Relatively little is known about the size of the costs imposed on firms that suffer information security breaches, and whether such costs are direct or imposed by market forces. If significant penalties are imposed by market forces, higher penalties or lower legal hurdles for plaintiffs can lead to over-deterrence and/or overinvestment in information security.

In this paper we address these issues by providing empirical evidence on the costs to firms that suffer breaches in information security. We examine 152 incidents from 2000 to 2007, and find that news of a data breach corresponds to economically meaningful and statistically significant losses in the share values of the firms suffering breaches. The average abnormal stock return is -0.23 percent, and is statistically significant at the 5% level. This is the first large-sample evidence of a drop in stock price following data breaches.

The drop in market value, however, is of the same magnitude as the direct costs. This shows that the drop in market value is primarily caused by the expected direct costs of the breach. Thus, unlike other types of corporate missteps such as those involving the air transportation, pharmaceutical, and restaurant industries, reputational penalties are not incurred by firms suffering data breaches. This finding is noteworthy given the widespread belief in the business press that reputational penalties are a large concern to companies that suffer breaches. At the same time, with respect to customer information, this paper provides empirical support for legal commentators who doubt the existence of reputational penalties. As it concerns the loss of confidential employee information, however, our results suggest the market does penalize firms' reputations. A complementary interpretation is that there are additional costs associated with breaches involving employee data. The existence of reputational penalties, or the complementary interpretation of high costs related to these events, makes these findings meaningful to all public and private employers that are at risk of information security breaches.

## References


Campbell, K., Gordon, L. R., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security,* 11, 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce,* 9, 69-104.

Computer Security Institute (2007). *12th Annual CSI Computer Crime and Security Survey*.

Davidson, W. N., Worrell, D., & Cheng, L. T. W. (1994). The effectiveness of OSHA penalties: A stock-market-based approach. *Industrial Relations,* 33, 283-296.

Digital Transactions News (2007, February 8). Data breaches don't spur as much fraud as stolen cards, other causes.

Dowdell, T. D., Govindaraj, S., & Jain, P. C. (1992). The Tylenol incident, ensuing regulation, and stock prices. *Journal of Financial and Quantitative Analysis,* 27, 283-301.

Fair Credit Billing Act 15 USC 1601 (1986, July 9). Retrieved from http://www.ftc.gov/os/statutes/fcb/fcb.pdf

Forrester Research. (2007, April 25). *Teleconference, the cost of a security breach,*.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security,* 11, 74-83.

Hersch, J. (1991). Equal employment opportunity law and firm valuation. *Journal of Human Resources,* 26, 139-153.

*Information Week.* (2006, March 20). *The high cost of data loss.*

Jarrell, G., & Peltzman, S. (1985). The impact of product recalls on the wealth of sellers. *Journal of Political Economy,* 93, 512-536.

Kannan, K., Rees, J., & Srikhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce* 12, 69-91.

Karpoff, J. M., Lee, D. S., & Martin, G. S. (2008). The cost to firms of cooking the books. *Journal of Financial and Quantitative Analysis*, 43, 581-612. Retrieved from http://ssrn.com/abstract=652121.

Karpoff, J. M., Lee, D. S., & Vendrzyk, V. (1999). Defense procurement fraud, penalties, and contractor influence. *Journal of Political Economy,* 107, 809-842.

Karpoff, J. M., & Lott, J. R., Jr. (1993). The reputational penalty firms bear from committing criminal fraud. *Journal of Law and Economics,* 36, 757-802.

Karpoff, J. M.,& Lott, J. R., Jr. (1999). On the determinants and importance of punitive damages awards. *Journal of Law and Economics,* 62, 527-573.

Karpoff, J. M., Lott, J. R., Jr., & Wehrly, E. W. (2005). The reputational penalty for environmental violations: Empirical evidence. *Journal of Law and Economics,* 48, 653-675.

Klein, B., & Leffler, K. B. (1981). The role of market forces in assuring contractual performance. *Journal of Political Economy,* 89, 615-641.

McNulty, E. (2007). Boss, I think someone stole our customer data. *Harvard Business Review*.

Mitchell, M. L., & Maloney, M. T. (1989). Crisis in the cockpit? The role of market forces in promoting air travel safety. *Journal of Law and Economics,* 32, 329-55.

Mitchell, M. L. (1989). The impact of external parties on brand-name capital: The 1982 Tylenol poisonings and subsequent cases. *Economic Inquiry,* 27, 601-618.

Ponemon Institute, LLC. (2006). *2006 Annual Study: Cost of a Data Breach*.

Richardson, R. (2007). 12th Annual CSI computer crime and security survey. Computer Security Institute. Available at http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

Salinger, M. (1992). Standard errors in event studies. *Journal of Financial and Quantitative Analysis,* 27, 39-53.

Schwartz, P. M., & Janger, E. J. (2005). Notification of data security breaches. *Michigan Law Review,* 105, 913-984.

Smith, C. Jr. (1992). Economics and ethics: The case of salomon brothers. *Journal of Applied Corporate Finance,* 5, 23-28.

Maxx, L. (2007, March 30). Stealing customers' data still seems all too easy. *The Economist*.

Trusted Strategies, Inc. (2006). *Network attacks: Analysis of department of justice prosecutions 1999-2006.*

**Table 1. Summary of Studies Examining the Market Value Effects of Information Security Breaches**

| *Source* | *Time Period* | *Sample Size* | *Results* | *Announcement Sources* |
|---|---|---|---|---|
| Campbell, Gordon, Loeb, and Zhou (2003) | 1995-2000 | Total: 43 | T: -1.88% abnormal return for (-1,1) window; statistically insignificant | Financial Times, New York Times, USA Today, Wall Street Journal, Washington Post |
| | | Confidential: 11 | C: -5.46% abnormal return for (-1,1) window; Z-statistic of -2.783 | |
| | | | | |
| Garg, Curtis, and Halper (2003) | 1999-2002 | Total: 22 | T: -3.8% abnormal return for (0,1) window; statistically significant using Wilcoxan non-parametric test | Not mentioned |
| | | Credit Card: 4 | CC: -9.0% abnormal return for (0,1) window | |
| | | Other Confidential: 2 | OC: -0.8% abnormal return for (0,1) window | |
| | | | | |
| Cavusoglu, Mishra, and Raghunathan (2004) | 1996-2001 | Total: 66 | T: -2.09% abnormal return for (0,1) window; Z-statistic of -2.999 | CNet, LexisNexis, ZDNet |
| | | Other Attacks (incl. compromised confidential info.): 32 | OA: No difference from total | |
| | | | | |
| Kannan, Ress, and Sridhar (2007) | 1997-2003 | Total: 72 | T: -0.65% abnormal return relative to control group for (-1,2) window; statistically insignificant | CNet, New York Times, Wall Street Journal, ZDNet |
| | | Confidential: 22 | C: 1.40% abnormal return relative to control group for (-1,2) window; statistically insignificant | |

**Table 2. Data Theft Sample**

| | *Number* |
|---|---|
| *Type of data:* | |
| Social Security number | 89 |
| Credit card number | 26 |
| Other financial information | 18 |
| Misc. personal information | 13 |
| Unknown | 6 |
| Total | 152 |
| | |
| Type of breach: | |
| Stolen hardware | 57 |
| Lost | 37 |
| Internet | 32 |
| Fraud | 23 |

| *Type of data:* | *Number* |
|---|---|
| Unknown | 3 |
| Total | 152 |
| | |
| Customer or employee data stolen: | |
| Direct customer | 97 |
| Employee | 39 |
| Indirect customer | 16 |
| Total | 152 |
| | |
| Inside or outside breach: | |
| Outside | 90 |
| Accidental inside | 47 |
| Malicious inside | 12 |
| Unknown | 3 |
| Total | 152 |
| | |
| Third party involvement | |
| No | 113 |
| Yes | 38 |
| Unknown | 1 |
| Total | 152 |

Note: Distribution of 152 incidents in which personal data was stolen from or lost by publicly traded firms. The incidents cover the period from September 2000 to June 2007, and were identified using the Attrition database and the Privacy Rights Clearinghouse chronology of data breaches.

**Table 3. Additional Summary Statistics**

| *Year:* | *Number* |
|---|---|
| 2000 | 3 |
| 2001 | 3 |
| 2002 | 1 |
| 2003 | 4 |
| 2004 | 4 |
| 2005 | 42 |
| 2006 | 70 |
| 2007 (thru June 30) | 25 |
| Total | 152 |
| Industry (Two digit SIC code): | |
| Construction (15-17) | 1 |
| Manufacturing (20-39) | 24 |
| Transportation, Communication and Utilities (41-49) | 14 |
| Wholesale Trade (50-51) | 4 |

| | Number |
|---|---|
| Year: | |
| Retail Trade (52-59) | 15 |
| Finance, Insurance and Real Estate (60-62) | 60 |
| Service (70-89) | 34 |
| Total | 152 |
| | |
| Number affected: | |
| Less than or equal to 10,000 | 37 |
| 10,001 to 100,000 | 35 |
| 100,001 to 1,000,000 | 23 |
| More than 1,000,000 | 7 |
| Unknown | 50 |
| Total | 152 |

Note: Distribution of 152 incidents in which personal data was stolen from or lost by publicly traded firms. The incidents cover the period from September 2000 to June 2007, and were identified using the Attrition database and the Privacy Rights Clearinghouse chronology of data breaches.

**Table 4. Abnormal Stock Returns Associated with the Initial Public Announcement of Information Security Breaches**

| | Type of Data | Type of Breach | Customer or Employee | Inside or Outside | Third Party Involvement |
|---|---|---|---|---|---|
| | Social Security number | Stolen hardware | Direct customer | Outside | No |
| Mean | -0.20% | -0.37% | -0.09% | -0.29% | -0.27% |
| Median | -0.26% | -0.42% | -0.17% | -0.32% | -0.27% |
| Z-statistic | -0.853 | -2.021* | -0.765 | -1.929+ | -2.169* |
| Observations | 89 | 57 | 97 | 90 | 113 |
| | Credit card number | Lost | Employee | Accidental inside | Yes |
| Mean | -0.12% | -0.20% | -0.55% | -0.23% | -0.16% |
| Median | 0.01% | -0.09% | -0.76% | -0.27% | -0.29% |
| Z-statistic | -0.359 | -0.575 | -2.287* | -0.967 | -0.293 |
| Observations | 26 | 37 | 39 | 47 | 38 |
| | Other financial information | Internet | Indirect customer | Malicious inside | |
| Mean | -0.71% | 0.01% | -0.37% | -0.17% | |
| Median | -0.62% | 0.01% | -0.02% | -0.27% | |
| Z-statistic | -1.876+ | 0.150 | -0.606 | -0.649 | |
| Observations | 18 | 32 | 16 | 12 | |
| | Misc. personal information | Fraud | | | |
| Mean | -0.17% | -0.38% | | | |
| Median | -0.27% | -0.31% | | | |
| Z-statistic | -1.867+ | -1.542 | | | |
| Observations | 13 | 23 | | | |

Note: Average 2-day (0,1) cumulative abnormal return for incidents in which personal data was stolen from or lost by publicly traded firms. The incidents cover the period from September 2000 to June 2007, and were identified using the Attrition database and the Privacy Rights Clearinghouse chronology of data breaches.

+ Indicates statistical significance using a two-tailed test at the .10 level.

* Indicates statistical significance using a two-tailed test at the .05 level.

**Table 5. Reputational Costs for Information Security Breaches**

| | | *Per-record direct cost estimate* | | | *Per-incident direct cost estimate* |
|---|---|---|---|---|---|
| | | *$50* | *$100* | *$200* | *$3,900,000* |
| 1 | Mean % change in market value | -0.235 | -0.235 | -0.235 | -0.234 |
| | | | | | |
| 2 | Mean implied % change from cost estimates | -0.464 | -0.927 | -1.854 | -0.270 |
| | | | | | |
| 3 | Mean reputational effect (as % of market value) (row 1 - row2) | 0.229 | 0.692 | 1.619 | 0.036 |
| | | | | | |
| 4 | Reputational effect t-statistic | 0.802 | 1.354 | 1.642 | 0.287 |
| 5 | Number of observations | 103 | 103 | 103 | 152 |

Note: This table compares firms' market value losses to estimates of direct costs associated with data security breaches. Comparisons are presented using a range of cost estimates based on published studies. The mean percentage change in market value (mean abnormal return) is winsorized as discussed in Section 4. In each panel, row 1 reports the mean abnormal stock return and row 2 reports the estimated direct costs as a percentage of the firm's market value of equity. The implied reputational effect in row 3 is equal to the difference between rows 1 and 2. The t-statistics test the null of no reputational effect against the alternative that the effect is negative (that is, that there exists a reputational loss).