Journal of Service Research
14(1) 44-59

DOI: 10.1177/1094670510383409
http://jsr.sagepub.com

Evaluating Customer Information Breaches as Service Failures: An Event Study Approach

Arvind Malhotra[1] and Claudia Kubowicz Malhotra[1]

Abstract

Firms are collecting more information about their customers than ever before in an attempt to understand and better serve customer needs. At the same time, firms are becoming more vulnerable to the compromise of customer information through security breaches. This study attempts to associate breach reports with the decline in market value of firms using an event study. The results show that firms suffer significant market value depreciation over a short as well as a long time window. Further, the greatest devaluation occurs when larger amounts of customer information are compromised at large companies. Due to the greater potential of customer backlash, negative publicity and liability risk, managers must view customer information breaches as service failures rather than as information system failures. Employing established service failure recovery strategies may allow firms to quickly and proactively address customer privacy concerns and thereby mitigate negative market reaction to information breaches.

Keywords

customer information breach, information privacy, service failures, service recovery, event study

Introduction

Enabled by advanced information technologies and increased e-commerce activity, firms are collecting more customer information than ever before. Video cameras capture consumers' shopping behavior and store cards reveal purchasing information in the physical retail environment. In the online retail environment, everything from browsing to buying is also being captured. Collecting and using this extensive customer data often allow companies to better target their marketing message to individual customers, customize products and services, and even personalize the product or shopping experience (Blattberg and Deighton 1991; Glazer 1991), creating a competitive advantage for firms (Glazer 1991; Pine 1992). Additionally, customers reap benefits through better product offerings and service from sharing personal information with companies they trust. While the advantages resulting from the collection and analysis of customer data are numerous to companies and consumers alike, the increasing occurrence of customer information breach incidents exposes companies to the downside of collecting and holding such large databases of customer information. The focus of this study is to explore the financial market impact of these customer information breaches for firms in the United States.

Forrester Research has reported that more than 100 million personally identifiable customer records have been breached in the United States over the past 2 years and that most of these breaches occurred at well-known companies.[1] A *Wall Street & Technology* (2007) survey found that 85% of midsize to large companies suffered an information security breach in a 24-month period. Moreover, the customer information breach incidents have not been trivial in terms of magnitude. In 2007, T. J. Maxx, a U.S. retailer, made an announcement of the theft of millions of credit and debit card accounts resulting from a breach of computer systems.

As in the incident at T. J. Maxx, most customer information breaches occur through security failures of information technologies. Even though it may be the technology that fails and the technologists who are the first to respond to a breach within a company, the occurrence and handling of customer information breaches are serious and important marketing issues with critical service quality and service recovery implications. If a breach should occur, service marketers play a critical role in informing customers of the breach and the recovery actions undertaken by the firm. Once informed of the breach, customers are more than likely to contact the company's customer service department to inquire about the security of their information. From brand management to crisis management and public relations to customer service, it is clear that security

[1] Kenan-Flagler Business School, University of North Carolina at Chapel Hill, Chapel Hill, NC, USA

Corresponding Author:
Arvind Malhotra, Kenan-Flagler Business School, University of North Carolina at Chapel Hill, McColl Building, Campus Box 3490, Chapel Hill, North Carolina 27599, USA
Email: Arvind_Malhotra@kenan-flagler.unc.edu

breaches greatly impact the marketing organization within a firm. Although customer information breach incidents have not been explored in a service context to date, we believe there is great value in doing so.

In this article, we attempt to make a link between customer information breach incidents and the potential severe negative implications that will be reflected in the market value of the firm. For most companies, meeting the needs of the customers is a fundamental objective of the company. Customers are major stakeholders of a firm; their satisfaction impacts other stakeholders and the well-being of the firm as a whole. Thus, an efficient financial market takes into account how well the firm satisfies the needs of its customers and reflects customer satisfaction in evaluating the firm. Furthermore, in efficient markets, investors take into account short-run as well as more damaging long-run impacts on firms' cash flow of negative incidents (Kannan, Rees, and Sridhar 2007). Technically, the impact on share prices of a breached firm reflects the behavior of investors and not the impacted customers. However, investors in the markets are also customers (and some of them are customers of breached firms). Therefore, their investment decisions (in the case of breaches, devaluing the stocks of breached firms) are driven by their rational (as investors) and emotional (as customers) reactions. The research question this study attempts to answer is:

> Research Question: What impact do customer information breach reports have on the market value of firms suffering from such breaches?

Throughout the article, an underlying objective is to urge marketing managers and customer service managers to view security breaches as "customer service" failure incidents rather than "information systems" failure issues. Customer information breaches must be explored in a service failure context in order to fully understand the implications for customer satisfaction and the financial performance of the firm.

Theory Development

Customer Information Breach as a Service Failure

Prior research has found that collecting massive amounts of customer information has a downside (Bloom, Milne, and Adler 1994), and one such negative implication involves information privacy. Consumers have expressed concerns about how and when information about them is being collected, how will it be used, will someone other than the company collecting the information have legitimate or illegitimate access to their information, and what is the recourse available if the information is collected, accessed or used in a manner not appropriate (Smith, Bolton, and Wagner 1999). In other words, there are consumer concerns about the collection and use of the data (information control concerns) as well as how information will be protected (security concerns; Dutta and McCrohan 2002). By willingly exchanging information with a company, a customer views this act as a social contract (Culnan and Armstrong 1999) that is, customers receive enhanced services/products in exchange for their personal information (labeled the second exchange). Therefore, an information breach can be construed as a violation of trust—"buyer perceives that seller's failure violated a psychological contract between the seller and buyer (Wang and Huff 2007, p. 1035)." As a result, there is an inherent risk for consumers that the companies may not fulfill their end of the contract—by failing to render enhanced services, by gaining more from the information than perceived fair by the customers, or by being callous about the security of customers' information. If such a violation does occur, research has found that three distinct consumer reactions are common (Wang and Huff 2007): cognitive—reduction in future trust (Robinson and Rousseau 1994), emotional—anger, hurt, and frustration (Lewicki and Bunker 1996), and behavioral—spreading negative word of mouth reduced intent to repurchase (Brown and Beltramini 1989). In summary, any breach of a social contract can erode customer trust in the company (Hoffman, Novak, and Peralta 1999).

Customer information breach incidents compromise the privacy of customers and as such can be construed as violation of trust. The Ponemon Institute (2008) found that 57% of respondents in a survey, who were impacted by an information breach agreed or strongly agreed that the breach caused them to lose trust and confidence in the breached company, and 31% of the respondents discontinued their relationship with the company after the breach occurred. Given this violation of trust, any breach of customer information privacy can be considered a service failure potentially leading to an erosion of customer's perceptions of service quality. Therefore, the consequences of such data breaches can be viewed through a service failure lens in which trust/privacy issues have been identified as the key drivers of customer service quality perceptions (Berry 1995; Parasuraman, Zeithaml, and Malhotra 2005). Customer information privacy concerns have been empirically associated with attitudes toward the use of online financial services (Montoya-Weiss, Voss, and Grewal 2003). Negative word of mouth (Bitner, Brown, and Meuter 2000), customers switching service providers (McCollough, Berry, and Yadav 2000; Roos 1999), and the creation of a "grudge-holding" situation such that even if customers do not switch services, they continue a downward trend in their interaction with the company (Bunker and Ball 2008) are some of the many negative costs associated with service failure incidents. As a result, customer information breaches and related privacy concerns can negatively impact not only current purchasing behavior but also future purchase intentions (Culnan and Armstrong 1999; Parasuraman and Zinkhan 2002; Wirtz, Lwin, and Williams 2007). The combination of short- and long-term intangible costs makes it difficult to assess the true financial impact of customer information breaches on firms.

Customer Data Breaches: Impact on Market Value of Firms

Research studies found either no significant impact or moderate immediate (short-window) impact on the market value of firms that suffered from information security breaches (Acquisti, Friedman, and Telang 2006; Campbell et al. 2003; Cavusoglu, Mishra, and Raghunathan 2004; Hovav and D'Arcy 2003; Kannan, Rees, and Sridhar 2007). These findings are counter to the anecdotal evidence that suggests that reports of breached customer information systems should have a significantly large and longer term negative impact on the market value of firms suffering from such breaches. Previous studies have either focused on information technology failure incidents, such as worms and viruses (without isolating the specific effect of information privacy breach events) or grouped customer information and employee information breaches together (e.g., Acquisti, Friedman, and Telang 2006). Therefore, it may be beneficial to look at customer information security breaches specifically.

It can be argued that in the case of customer information breaches, the impact may unfold differently from other information systems security incidents. There may be a smaller market impact in an immediate time frame (short window), as in many cases only a few details about the breach are available immediately. The market impact of customer information may only unfold over a long window as the details pertaining to the full extent (in terms of what was the nature of the breach, how many customer records were exposed, and how the breach was handled/secured) of the customer information security breach only become available over a few week period after the breach. Consequently, the market continues to take into account the details and continues to respond over a longer period of time following the day of the report of a security breach incident. As opposed to previous research findings, we argue that firms that are reported to have suffered from customer information breaches will see a decrease in market value in the short as well as a relatively long time window. Therefore, we hypothesize:

Hypothesis 1: Reports of customer information breaches suffered by firms result in significant negative cumulative abnormal returns (CARs) for those firms over a short time window.

Hypothesis 2: Reports of customer information breaches by firms result in significant negative CARs for those firms over a long time window.

Firm Size Effect

Researchers have posited and found that the market penalizes larger firms less severely when compared to smaller firms in response to news of information security incidents. In other words, smaller firms that suffer negative information security incidents experience more negative CARs than larger firms.[2] The resource-based view of the firm is often invoked to explain the reason behind the differential market reaction related to firm size. It is argued that larger firms have more slack resources (such as skilled personnel, technological skills, and information systems competency) than smaller firms. Therefore, when information systems security breaches occur, larger firms can leverage these slack resources to recover (and recover faster) than smaller firms. Larger firms may have a large IT department (and consequently more IT skilled personnel) who can be mobilized to stop the bleeding.

The slack resources argument may hold true when the security incidents are related to virus attacks and other technological malfunction incidents that may be contained and rectified using slack resources by larger firms. Whereby, the labor and material costs to recover from security breach incidents may be lower for larger firms due to economies of scale. However, in the case of customer information breaches, the intangible costs and impacts may be different. Larger firms operate larger and more intricate information systems. Therefore, any isolated information security incident may cause the market and customers alike to wonder how vulnerable the company is on a larger scale due to the complexity of their information systems. The legal and liability costs may also be higher for larger firms (such as future insurance premiums). Larger firms may also have more critical dependencies than smaller firms, that is business partners that may need to be compensated for information systems security breaches recovery as well. More importantly, given the focus on customer information security breaches in this study, larger firms may have a sizable customer base. Consequently, due to network effects, larger firms may suffer a greater negative word-of-mouth impact than smaller firms. Along the same lines, smaller firms by virtue of having a smaller customer base can address customers' concerns in a more personal manner than larger firms (e.g. T.J. Maxx posting a letter of explanation on its websites to mass address more than a million customers) thereby suffering smaller consequences in terms of customer dissatisfaction. The "the bigger they are the harder they fall" argument adopted in this study leads to the following hypothesis:

Hypothesis 3: As a consequence of customer information breach reports, larger firms suffer larger market value loss than smaller firms.

Magnitude of Breach Effect

The reaction of investors in the market can be argued to be dependent on the number of customers impacted by the breach. The PGP Research Report (2006) estimates that it costs $182 per record lost/exposed due to customer information breaches. Of the overall cost of $182/record, $54 was attributable to direct incremental cost (free or discounted services offered; notification letters, phone calls, and e-mails; legal, audit and accounting fees; call center expenses; public and investor relations), $30 due to lost productivity, and $98 due to customer opportunity costs (turnover of existing customers and increased costs to acquire new customers). These numbers allude to the fact that the greater the number of customers affected by an

information breach,[3] the greater the direct costs incurred by the firm that experiences the information security breach. Further, the "snowballing" negative word of mouth will be more severe the greater the number of customers that are initially directly impacted by an information breach. Therefore, the larger the magnitude of the breach, the more the market is going to devalue the company, which leads to the following hypothesis:

Hypothesis 4: The larger the magnitude of customer information breach suffered by a firm the greater the loss of firm's market value.

Magnitude of Breach and Firm Size Interaction

In addition to the main effect hypotheses above, it may be the case that an interaction emerges between the magnitude of the breach and the size of the company. For small companies, any breach may be considered a large negative event. Therefore, there will be no significant differences in the market devaluation based on the differences in magnitude of breaches, that is small companies will be penalized heavily no matter what. On the other hand, for large companies, there may be a differential negative impact on market value based on the magnitude of the breach. Larger firms have a much larger potential of class action suits from angry customers especially when a large set of customers is affected. This unity in customer response can be construed as a severe instance of "grudge-holding" situation (Bunker and Ball 2008). Larger breaches at large firms may signal to the customer that a large firm was grossly negligent ("how could they have let such a big breach occur"), that is the feeling that the violation is repeatable rather than it being a one off incident that is out of control of the company. Research has shown that when customers perceive a violation as repeatable, there is more negative reaction than if the violation is seen as one time event (Wang and Huff 2007). Another reason why large companies could suffer a bigger market loss due to larger magnitude breaches (as compared to small ones) is that the market is taking into consideration the negative network effects at play. This negative network effect can result in slower growth (if not a decline) in the customer base for larger companies (which are expected to demonstrate better growth by the market). Correspondingly, we hypothesize:

Hypothesis 5a: For smaller firms, market value loss will not differ significantly based on the magnitude of the information breach.

Hypothesis 5b: For larger firms, the magnitude of the information breach will significantly impact the market value loss incurred, with larger magnitude breaches leading to greater market value losses.

Exploratory Questions

In addition to the hypotheses above, we seek to explore the effect on market evaluation of (a) the industry sector to which the breached firm belongs and (b) the type of information breached. With regard to the industry sector, anecdotal evidence suggests that firms in the financial sector suffer 17% higher data breach costs compared to other firms (Banking Technology 2008) and graver consequences due to loss of customer personal information (Wolfe 2007). Recent court decisions and emerging laws have also tended to penalize financial services firms severely for information breaches (Smith 2006). Similarly, retailers have also started to suffer extensive costs from customer information breaches. Shifts in legal policies requires retailers to share the liability costs related to customer information breaches and the illegal use of credit cards with banks who issue credit cards on behalf of the retailers (Kuykendall 2004). Moreover, the legal liability and tangible recovery costs may be negligible when compared to the intangible costs that result from customer freezes in conducting transactions with the affected retail firms as well as the overall negative publicity for the retail brand. Therefore, we ask the following:

Exploratory Question 1: Are different industry sectors (e.g., financial services, retail, etc.) impacted differently by customer information breaches?

The type of information compromised may also lead to a differential market value impact on the firm. Specifically, two different types of consumer information are susceptible to breaches. The first type is of financial nature (i.e., credit card numbers, bank accounts, etc.) and the second is consumers' personal information (i.e., social security numbers, addresses, etc). When a customer information breach involves a financial information breach, customers may incur direct financial loss. Even if they do not, the threat of such financial loss is very real. Therefore, it can be argued that consumers feel a large sense of the violation of trust when their financial information is compromised. That said, the effects of financial information loss can be mitigated by simple actions (e.g., cancellation of credit card), which result in less financial liability (if at all) for consumers immediately following the breach incident. On the other hand, customers may see a personal information breach (e.g. social security numbers) as more damaging because identity theft cannot be resolved quickly and easily, and may actually be more financially damaging in the long run. Therefore, we ask the following:

Exploratory Question 2: Does the type of information breached affect the firms differently in terms of market value loss?

Methodology Employed for the Study

Event Study Methodology

In this study, the event study methodology is used to explore the impact of customer information breach reports on the market value of firms suffering from the breach. Event study methodology is commonly used in the accounting and finance

literature (Conrad, Cornell, and Landsman 2002; Conrad and Kaul 1993; Hsu, Reed, and Rocholl 2010), marketing literature (Swaminathan, Mushed, and Hulland 2008; Ting-Heng, Che-Chun, and Prather 2005), and strategy literature (Capron and Shen 2007) to explore the impact of various events on firms' stock performance and market value.

The basic tenet of event study methodology is that markets are efficient (Fama 1970). Investors in efficient markets value firms based on their expectation of future positive abnormal returns (ARs) due to actions that are significantly beneficial to the firm. In a similar vein, investors in efficient markets devalue firms based on their expectation of future negative ARs when firms are affected by incidents that are significantly detrimental to the future of the firm. When there is a consensus among a large set of investors, the market creates a positive or negative abnormal stock market return for the firm's stock around the date of report of the underlying events. MacKinlay (1997) suggests that focusing on ARs—returns that are adjusted for risks—in a window of time can provide a clue as to whether an event (e.g., public announcement, news report, etc.) has an impact on a firm's expected future profitability.

In order to assess whether an event has an impact on the firm's stock price performance, it has to be ascertained what the performance would have been if the event had not been reported. In order to do so and also to control for the market effects, the return of the stock is regressed against the return of a market index. The following market model regression equation (Equation 1) is used to estimate coefficients that are then used to calculate the predicted return of a firm's stock adjusting for market effects (Dos Santos, Peffers, and Mauer 1993):

$$R_{it} = \alpha + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

where R_{it} = return of stock i on day t:

$$R_{it} = \frac{\mathrm{Pr}\,ice_{it} - \mathrm{Pr}\,ice_{it-1}}{\mathrm{Pr}\,ice_{it-1}}$$

R_{mt}= marketreturnonday t.

The market return on day t is the average of returns of all firms included in the market index. The Center for Research in Security Prices (CRSP) database used in this study includes monthly and daily price quotations for common stocks, traded on the New York and American stock exchanges and NASDAQ. Therefore, all the stocks in these markets are used as the baseline for calculation. Finally, ε_{it} is a random error for stock i on day t, and α_i and β_i are coefficients with firm i. The return of the stock rather than stock price is used in the regression model to control for autocorrelation (Subramani and Walden 2001).

CARs are calculated over two event windows: (a) Short window: 1 trading day prior to the event (news report about customer information breach) to 1 trading day after the event. (b) Long window: From 2 trading days after the event (report about customer information breach) to 30 days after the event. The coefficient estimates from the market model regression Equation 1 and the realized returns from the market index were used to predict normal returns for the two event periods [−1, +1] and [+2, +30]. The prediction errors during the two event periods, that is deviation of realized returns from normal returns, are the estimates of ARs. The AR for the common stock of firm i on event day t is computed using Equation 2 (Hovav and D'Arcy 2003).

$$\mathrm{AR}_{it} = \mathrm{R}_{it} - \left(\hat{\alpha}_i + \hat{\beta}_i R_{mt}\right) \quad (2)$$

where the coefficients $\hat{\alpha}_i$ and $\hat{\beta}_i$ are the ordinary least square parameter estimates obtained by regressing R_{it} over R_{mt} over the estimation period prior to the event, and AR_{it} is the AR of firm i on day t. The assumption of this methodology is that ARs are seen due to the event and not due to a random event occurring on the same day (Subramani and Walden 2001). For the event period [−n, +n], the CAR is calculated as:

$$\mathrm{CAR_i} = \sum_{t=-n} \mathrm{AR_{it}} \quad (3)$$

Thus, for a sample of N firms, the average event period announcement effect is:

$$\mathrm{ACAR}_i = \frac{1}{N}\sum_{i=1}^{N} \mathrm{CAR}_i \quad (4)$$

Test Statistics Used in the Event Study

In this study, three test statistics were used based on the work of Cowan and Sergeant (1996, pp. 5-9): (a) The Patell (1976) standardized residual test as used by Brown and Warner (1985) in their study, (b) Standardized cross-sectional test (Boehmer, Musumeci, and Poulsen 1991), and (c) Rank test (Corrado 1989). In each of the tests, the null hypothesis is that the mean AR is equal to zero. Since each of these tests has its distinct advantages and disadvantages, we use all three tests to demonstrate robustness of the results of this study. The details behind computation of each of the test statistic can be found in the web appendix.

The 4-Factor Model of ARs Estimation

In recent days, in the face of anomalous evidence, researchers have questioned the usefulness of the Capital Asset Pricing Model (CAPM) to explain ARs (Equations 1 and 2) using a "single factor." To incorporate additional risk factors a 3-factor model was proposed by Fama and French (1993). The 3-factor model argues that a single factor—β (market excess returns)—may not be adequate to explain variance in equity returns, and that two additional factors, that is, size premium (differences in returns between portfolios of small capitalizations firms and big capitalization firms) and book-to-market premium (historic excess returns of value stocks) need to be taken into account. The 3-factor model was later modified by Carhart (1997) to incorporate the momentum factor. The momentum factor takes into account the monthly return

differences between returns on high and low prior return portfolios to capture cross-sectional return patterns. The momentum factor is designed to take into account that short-run winners outperform losers and stock returns continue to drift after specific announcements. The 4-factor model is shown in Equation 5 below. In essence, the 4-factor model focuses on isolating the impact of event on security price performance taking into account factors that are a proxy for risk or indicators of market inefficiencies (Kothari and Warner 2006). In order to test the robustness of our findings related to ARs using the CAPM model, we also used the 4-factor model to see whether similar trends in ARs were observed taking into account additional risk factors.

$$R_{jt} = \alpha + \beta + s_j \mathrm{SMB}_t + h_j \mathrm{HML}_t + u_j \mathrm{UMD}_t + \varepsilon_{jt} \quad (5)$$

where

R_{jt} is firm j's return on day t;
R_{mt} is the rate of return of a market index on day t;
SMB_t is the average return on small market capitalization portfolios minus the average return on the three large market capitalization portfolios;
HML_t is the average return on two high book-to-market equity portfolios minus the average return on two low book-to-market equity portfolios;
UMD_t is the difference between the return on the portfolio of past 1-year "winners" and "losers";
ε_{jt} is the random variable that has an expected value of zero and is assumed to be uncorrelated with R_{mt}.

Based on Equation 5, the AR is then calculated using Equation 6:

$$A_{jt} = R_{jt} - \left(\alpha_j + \beta_j R_{mt} + s_j \mathrm{SMB}_t + h_j \mathrm{HML}_t + m_j \mathrm{UMD}_t + \varepsilon_{jt}\right) \quad (6)$$

where A_{jt} is firm j's AR on day t, and α_j, β_j, s_j, h_j, and m_j are firm-specific multiple regression parameter estimates from Equation 5.

Hypotheses and Exploratory Questions Testing

In order to test Hypotheses 1 and 2 pertaining to the significant negative CARs in the short and long windows due to a customer information breach, we use the ARs obtained from the CAPM (Equations 1 and 2) and the 4-factor model (Equation 5). We then use the CARs from the event study to calculate net present value loss (NPVLoss). NPV has been used as a dependent variable in previous event studies (Chan et al. 1997; Kalaignanam, Shankar, and Vardarajan 2007) and is computed as product of overall CAR over the entire window [−1, +30] and the market capitalization of the firm 20 days prior to the reported customer information breach incident. The reason for using the decrease in NPVLoss over the CAR is that researchers have pointed out that the CARs have the tendency to vary with firm size (Anand and Khanna 2000). Larger firms tend to exhibit smaller CARs as compared to smaller firms. Following the model of Kalaignanam Shankar, and Vardarajan (2007), we use the total financial loss associated with the breach event to overcome the size bias problem.

In order to test the hypotheses and exploratory questions, Equation 7 was used. The dependent variable in the equation (NPVLoss) is the decrease in NPV or shareholder wealth resulting from the customer information breach incident. The main and interaction dependent variables are associated with the hypotheses and exploratory questions.

If a similar event has occurred to same firm previously, then the market reaction next time the event occurs is more pronounced (Swaminathan and Moorman 2009). In this study, we have also included a variable (REPEAT) to control for the fact that some of the firms in our sample had suffered multiple breaches. The underlying assumption is that the market is more likely to have a more severe reaction to firms that have suffered earlier breaches. Repeat breaches are clear signs of severe vulnerability and/or lack of effort to improve information security by a firm.

$$\begin{aligned}\mathrm{NPVLoss}_i = {} & \beta_0 + \beta_1 \mathrm{REPEAT}_i + \beta_2 \mathrm{IMPACT}_i + \beta_3 \mathrm{SIZE}_i \\ & + \beta_4 \mathrm{FINANCE}_i + \beta_5 \mathrm{RETAIL}_i + \beta_6 \mathrm{INFOTYPE}_i \\ & + \beta_7 (\mathrm{SIZE}_i \times \mathrm{IMPACT}_i) \\ & + \beta_8 (\mathrm{FINANCE}_i \times \mathrm{INFOTYPE}_i) \beta_9 \\ & (\mathrm{RETAIL}_i \times \mathrm{INFOTYPE}_i) + \varepsilon_i \end{aligned} \quad (7)$$

where

REPEAT_i = Control variable for number of times company i has been breached previously;
IMPACT_i = Magnitude of impact of breach at firm i (total number of customer records breached/total revenue of the firm);
SIZE_i = Number of employees in breached firm i;
$\mathrm{FINANCE}_i$ = Dummy variable = 1 if breached firm i is in financial services industry; = 0 otherwise;
RETAIL_i = Dummy variable = 1 if breached firm i is retail services industry; = 0 otherwise;
$\mathrm{INFOTYPE}_i$ = Dummy variable = 1 if the breach involves customers financial information;
ε_i= error term.

Data Sources

The data to test the hypotheses proposed in this study was obtained from three different sources. First, the organization attrition.org[4] maintains an open source database (DLDOS) of information breaches and data theft incidents from 2000 to date. The database comprises public reports (mainly media reports) of breaches worldwide. The database contains data related to the date of information breach, the company that reported the breach, the type of information breaches, the number of records impacted, and third-party companies involved.

The database is exhaustive and contains 952 reported information breaches worldwide (from 2000 onward). In order to ascertain the comprehensiveness of the DLDOS, Lexis-Nexis and the Wall Street Journal Index were used to cross-check for information breach reports that may not have been captured by attrition.org's DLDOS database. The cross-check confirmed that DLDOS captured all incidents of information security breaches reported in the public domain. Of the 952 reported breaches, 282 were reports concerning businesses in the United States (the rest were international businesses or educational or government institutions). Only 144 of the 282 were publicly traded U.S. companies for whom stock market data was possibly available. Further, 46 out of the 144 breaches at publicly traded companies were concerning employees information. We only included those breaches that affected customers rather than employees.

The sample size used in this study was further dependent on the time windows used in the event study methodology. A word of caution about using long windows in event study research is the presence of confounding effects. The choice of length of the window has generated much debate among researchers who employ the event study methodology. Long windows make it hard to isolate the impact of a particular event (e.g., customer information breach, mergers, etc.) on security prices. The reason being that as the window is extended, several other major events (such as earnings announcement, change in executives at the company, etc.) occur and therefore confound the effects of the particular event under consideration. For this reason, previous studies have looked at 15 to 30 days after the event as the long-window in event studies (Cable, Henley, and Holland 2002; Graddy and Strickland 2007; Kwansa 1994). In this study, we chose the longest [+30] feasible window. Most event studies show that 30 days (or even shorter) adequately capture the permanent effect, if any, of the event under consideration. That said, we also understood that the longer the time window used, the higher the chances that other significant events may be the cause of CARs (Brown and Warner 1985). Therefore, an attempt was made to ensure that companies that made other announcements (e.g., earnings loss, negative advisory, etc.) that could result in negative CAR in the window of interest (i.e., −1 to +30) of this study were not included in the sample. The list of companies was refined by using the Wall Street Journal index to check whether any confounding announcements or reports (mergers, acquisitions, stock splits, etc.) were made in the [−1 to +30] window around the date of reported customer information breach. Even though some companies with other major announcements in the long window had to be dropped from our sample, we feel confident that this reduced sample allowed us to isolate the effect of customer information breach reports on the firm's market value. Our resulting sample consists of 93 publicly traded U.S. companies for which customer information breaches have been reported between 2000 and 2007. Appendix A presents some examples of these customer information breach reports.

The stock price and number of outstanding shares for firms was obtained using the CRSP database. CRSP is a financial research center at the Graduate School of Business at the University of Chicago, which maintains a comprehensive database that includes a historical performance record of common stocks listed on the NYSE (New York Stock Exchange), AMEX (American Stock Exchange), and NASDAQ Stock Markets (from December 1925 to the present). The database takes into account factors such as stock splits, and so on and has been extensively used by researchers conducting event studies. The CRSP database was leveraged for this analysis using the statistical software package EVENTUS™, which is specifically designed to perform event studies. EVENTUS™ can read raw returns, prices, bid and ask quotations, trading volume, and number of trades and shares outstanding from the CRSP database. EVENTUS™ converts calendar dates to CRSP trading day numbers, extracts event study cumulative or compounded ARs for cross-sectional analysis, conducts the event study specified and provides the test statistics associated with event study discussed earlier.

Results

In this section, we present the results of the event study and test our hypotheses examining the negative impact of customer information breaches on the market valuations of firms. Specifically, we seek to confirm whether customer information breaches will negatively impact market value when the time window is short (Hypothesis 1) as well as long (Hypothesis 2). Additionally, we tested whether the negative market impact will be greater based on the size of the breached firm (Hypothesis 3), magnitude of the breach (Hypothesis 4), and the interaction between the size of the firm and magnitude of the breach (Hypothesis 5). The greatest negative impact is expected when large magnitude breaches occur at large companies because of larger scale recovery measures required, possible regulatory involvement, increased media scrutiny and attention, and large-scale negative customer network effects (Hypothesis 5). In addition, we explored whether the loss of market value is dependent on the industry the breach firm belonged to (finance and retail sector), the type of customer information breached (financial versus personal), and any interaction between the type of industry sector and type of information breached.

Effect of Customer Information Breach News Reports/Announcements

The mean CARs for 93 firms reported to have suffered customer information breach incidents and the tests for significance of the CARs are shown in the Table 1. The breached companies came from diverse set of industries. Thirty-six ($\sim$40% of the sample) of the companies in our sample were from the financial services industry. The next two biggest industries represented in our sample were the retail sector (17 companies or $\sim$18% of the sample) and technology sector (10 companies or $\sim$11% of the sample). The remaining companies in our sample belonged to the data services, insurance

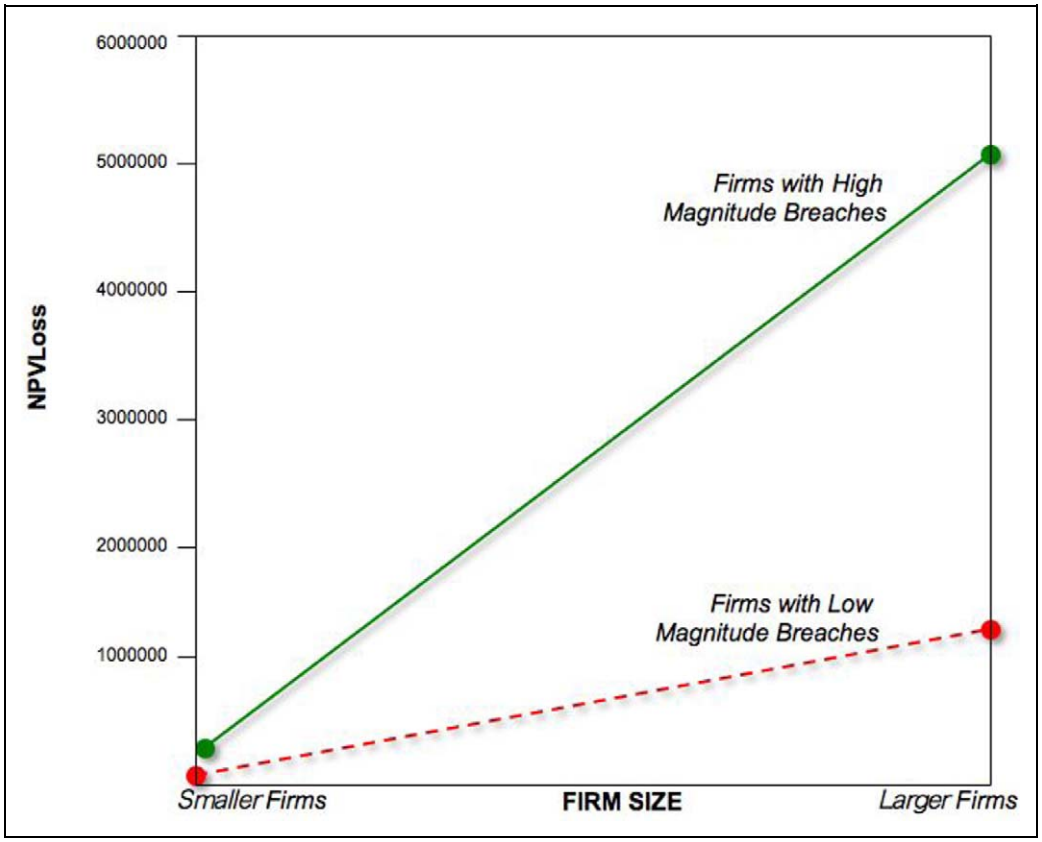

Figure 1. Results for the Interaction Hypotheses (5a and 5b). NPV = net present value.

sector, medical sector, hotels, technology services, real estate, and manufacturing.

As the results demonstrate in Table 1, the overall mean CAR for firms for whom a customer information breach is reported is negative in both time windows. The mean CAR for firms is negative (mean $CAR = -0.78\%$) and statistically significant in the short window (based on three statistical tests discussed earlier). Similarly, the mean CAR is negative (mean $CAR = -1.92\%$) and statistically significant in the long window as well (based on two of the three statistical tests). Therefore, the results provide strong support for Hypothesis 1 and support for Hypothesis 2.

In order to test for robustness of our results and to ensure that the results discussed above are not an artifact of the time window chosen for this study, we ran several alternate short and long windows. The alternate short windows were the ones that are typically used in event studies, i.e. $[-3, +3]$, $[-5, +5]$, and $[-10, +10]$. The alternative long windows were then based on the alternative short windows. The results are shown in Appendix B and are similar to the original time windows used in this study. Significant negative CARs are seen in the short windows and long windows.

As mentioned in the methodology section, we also ran a 4-factor model to isolate the impact of the event on security price performance, taking into account factors that are a proxy for risk or indicators of market inefficiencies (Kothari and Warner 2006). The results are shown in Table 2. The overall mean CAR for firms for whom customer information breach is reported is negative in both time windows. The mean CAR for firms is negative (mean CAR $= -0.82\%$) and statistically significant in the short window (based on three statistical tests). In addition, the mean CAR is negative (mean CAR $= -1.47\%$) and statistically significant in the long window (at $p < .05$ level based on Rank test and $p < .1$ level on two of other three statistical tests).

We checked for robustness of our results in two ways.[5] First, we also used S&P 500 as the proxy for market (instead of all stocks in NYSE, AMEX, and NASDAQ). An advantage of using the S&P 500 as the index of the market is that it is a capitalization-weighted index based on a broad cross-section of the market and has been employed by other researchers (Hovav and D'Arcy 2003; Subramani and Walden 2001). The results were similar to those shown in Tables 1 and 2. In addition, we wanted to ensure that the ARs were not subject to volatility (that can cause β estimates to change before and after event day) around the estimation period. To do so, we varied the estimation period to end 5, 10, 20, and 40 days prior to event day, and also 5, 10, and 20 days after the event day. The CARs were similar to those shown in Tables 1 and 2. This ensured that the volatility around the event day did not affect the results.

Next the main and interaction effect hypotheses (Hypothesis 3−Hypothesis 5) as well as the exploratory questions were tested using 3-stage Ordinary Least Squares (OLS) regression

Table 1. Announcement Effect in Short-Term and Long-Term Window

Event Windows	Mean CAR (All Firms)	Positive: Negative	Tests		
			Patell *Z*	Standard Cross-Sectional *Z*	Rank Test *Z*
Short-term window [−1 to +1]	−0.78%	32:61	−3.21***	−2.38***	−1.96*
Long-term window [+2 to +30]	−1.92%	41:52	−2.03*	−1.76*	−1.42

Note. CAR = cumulative abnormal return.
* $p < .05$ level.
** $p < .01$ level.
*** $p < .001$ level.

Table 2. Fama-French-Momentum Time-Series Model Using Value Weighted Index

Event Windows	Mean CAR (All Firms)	Positive: Negative	Tests		
			Portfolio Time Series (CDA) *t*	Cross Sectional Error *T*	Rank Test *Z*
Short-window [−1 to +1]	−0.82%	35:58	−2.55**	−2.33**	−1.87*
Long-window [+2 to +30]	−1.47%	40:53	−1.47$	−1.38$	−2.31*

Note. CAR = cumulative abnormal return; CDA = crude dependence adjustment.
$ $p < .1$ level.
* $p < .05$ level.
** $p < .01$ level.
*** $p < .001$ level.

as suggested by Aiken and West (1991) using Equation 7. The NPVLoss was the dependent variable in each of the stages. The results of the regression are shown in the Table 2. In the first stage (Model 1 in Table 3), we introduced the control variables (REPEAT). In the second stage, we introduced the main effects in addition to the control variables (Model 2 in Table 3). Subsequently, in Stage 3 (Model 3 in Table 3), we entered the interaction variable related to Hypothesis 5 (Size of the Breached Firm × Magnitude of the Breach) in addition to the control and main variables. Finally, in the Model 4, we entered the exploratory interaction term (Type of Industry Sector × Type of Information Breached). Following Aiken and West (1991), the interaction effect was inserted in the equation after inclusion of the simple main effects. Variance inflation factors for all variables were well within acceptable limits (ranged between 1.1 and 2.9).

From Model 2 in Table 3, it can also be observed that the coefficient associated with firm size, that is, number of employees in a firm, was statistically significant ($\beta = 0.32$, $t = 255$). This provides support for Hypothesis 3, that is, larger firms suffer a larger market value loss than smaller firms due to reports of a customer information breach. However, the coefficient associated with the magnitude of breach, that is, ratio of number of customer records breached to the total revenue of the firm ($\beta = 0.02$, $t = 0.22$) was not statistically significant. Therefore, there is no support for Hypothesis 4, that is, the market value loss of firms is not different based on the magnitude of the breach. It should be noted that only about half the firms in our sample reported the number of customer records breached. This small sample size may have impacted the analysis. As an alternate approach, in conducting the regression, a dummy variable for whether the impact was known or unknown for reported incidents was used instead of impact size variable in regression equation. There was no statistically significant difference in market value loss of firms based on whether the magnitude of impact was known or unknown.

As can be seen from Model 3 in Table 3, the coefficient associated with the interaction term—Size of the Firm × Magnitude of Breach—is statistically significant ($\beta = 0.26$, $t = 2.13$). Therefore, Hypothesis 5 is supported. Next, as suggested by Aiken and West (1991, p. 12), it is important to probe any significant interaction effect to fully understand its meaning. One of the most powerful means of probing is to plot the relationship between the predictor variable and the dependent variable for different levels of the moderator variable. In the figure below, we plotted NPVLoss as a function of size of the firms for two levels of magnitude of breach. The two-level categorizations (median split of magnitude of impact) and firm size were done only for the graph, not for the analysis. Looking at the plot (Figure 1), one can surmise that when large breaches occur at larger firms, the firms face a greater market value loss vis-à-vis when small breaches occur. For smaller firms, the market value loss is not significantly different for different magnitudes of the breach.

Finally, focusing on our exploratory questions, as shown in Table 3 Model 2, the coefficient for dummy variable associated with the financial service industry firms is statistically significant ($\beta = 0.34$, $t = 2.54$). However, the coefficient associated with the retail sector firms was not significant ($\beta = 0.12$, $t = 0.77$). Also, the coefficient for the dummy variable associated with the type of information compromised—financial

Table 3. Regression Results

Independent Variables	Dependent Variable: NPVLoss			
	Model 1 β Coefficient (*t* value)	Model 2 β Coefficient (*t* value)	Model 3 β Coefficient (*t* value)	Model 4 β Coefficient (*t* value)
Control variable				
Number of previous breaches	0.33* (2.59)	0.17 (1.76)	0.21 (1.74)	0.22 (1.72)
Main effects				
Firm size		0.32* (2.55)	0.30* (2.33)	0.37** (2.81)
Magnitude of impact		0.02 (0.21)	0.09 (0.72)	0.08 (0.66)
Financial industry firm		0.34* (2.54)	0.30* (2.33)	0.29* (2.05)
Retail sector firm		0.12 (0.77)	0.13 (0.87)	0.17 (0.86)
Type of information breached (1 = *Financial Information*, 0 = *Personal Information*)		−0.01 (−0.08)	−0.03 (−0.25)	−0.08 (−0.38)
Interaction effects				
Firm Size × Magnitude of Impact			0.26* (2.13)	0.26* (2.09)
Financial Sector Firm × Type of Information Breached				0.04 (0.26)
Retail Sector Firm × Type of Information Breached				−0.03 (−0.22)
R^2	.11	.29	.36	.36
F ratio	6.73*	3.52**	3.87**	2.91**
ΔR^2		.18	.07	
F ratio		2.67*	4.54*	

Note. NPV = net present value.
* $p < .05$.
** $p < .01$.

information (i.e., credit card numbers) or personal information (i.e., social security numbers) —is not statistically significant ($\beta = -0.01$, $t = -0.08$). The coefficients associated with the two interaction terms related to Type of Industry Sector and Type of Information Breached are not significant (Model 4 in Table 3).

Managerial Implications and Future Research Directions

The results of this study clearly demonstrate that reports of a customer information breach negatively impact the market value of firms in the immediate (short) window as well as the long window. The stocks of the impacted firms show a decline of almost 3% in CARs over the entire time window explored in this study [−1, +30]. Interestingly, the decline in market value is higher in the long window [+2, +30] than in the immediate (short) window [−1, +1]. The decline in market value (significant negative CAR) sets in as soon as the breach is reported. However, the results show that investors (the market) take time in assessing the "true" impact of breach of the firm. Then, once the investors gain and absorb more information about the reported breach, they begin to express concerns about the long-term health of the breached firms. This concern manifests itself in higher depreciation in stock value of the firms in the long window as compared to the short window. A closer look at some of the reports in our sample shows that the details about the number of customers (potentially) affected, source of the breach, and containment strategies are very unclear in the initial reports. Sometimes, the details about the true impact in terms of costs and lost opportunity of the breached firms do not unfold immediately (i.e., the short window). Appendix C shows an example of this evolutionary nature of breach reports. The short window [−1, +1] may be too short a window for investors to ascertain the full nature of the breach. However, as the details start to emerge, investors truly understand the long-term impact of the breach. The market then reacts rationally rather than displaying severe immediate "irrational antipathy" based on initial breach reports.

Counter to what previous researchers have proposed and empirically discovered (Cavusoglu, Mishra, and Raghunathan 2004), the results of our study show that larger firms suffer a greater market value loss than smaller firms after a customer information security breach. Even more interesting is the significant interaction effect that emerged between the Size of the Firm and Magnitude of the Breach on market performance. This result confirms that larger firms have much more to lose when they suffer large breaches (i.e., more number of customers affected by the breach). In other words, larger breaches at larger firms result in much more market value loss than when larger firms suffer from smaller breaches. This may be the case for a couple of reasons. First, customers may expect that larger firms will expend more resources to protect customer information vis-à-vis smaller firms. Second, larger breaches at large firms may signal to the customer that a large firm was grossly negligent rather

than it being an isolated incident that is out of control of the company. Consequently, at the time of failure, there may be a more severe backlash from customers who feel that the large firm skimped in customer protection.

By affecting a larger set of customers, larger breaches can result in proportionally more severe implications for the firm and thus require much more involved recovery efforts. Conventional thinking has been that larger firms have more slack resources to recover from customer information breaches, and thus would be more successful in their recovery efforts than smaller firms. However, this is a very information system centric view, that is an information security breach is a technology systems issue and one that is about technical fixes rather than image fixes. In reality, a large customer base will quickly engage in negative word-of-mouth and exhibit negative repurchase intentions (Kalamas, Laroche, and Makdessian 2008). Additionally, larger firms face a much larger potential of class action suits from angry customers especially when a large set of customers is affected. Lastly, large magnitude customer information breaches at large firms will receive a lot of media scrutiny, which can magnify the negative opinions of not only current customers, but also prospective ones. Thus, even with more resources, larger firms have more at risk given customer expectations and subsequent reactions to a data loss incident.

As proposed earlier, a customer information breach is a "service failure" issue rather than a "systems failure" one. Large firms may be better served in being pro-active in customer information security measures, making it a strategic service priority rather than a technical systems consideration. Given that the greatest negative impact on market value occurs when large companies compromise significant amounts of consumer data, these are exactly the companies that have the most to lose. To mitigate this risk, it is imperative that these companies have a "best in class" service recovery plan. A well-designed and executed recovery plan may help the company respond more quickly and effectively post breach. Such a response may help slow the network effects and lessen the overall negative impact on the market value of the firm post breach.

Interestingly, the results show that it is not the type of information that is compromised (financial or personal), but rather the industry sector to which the breached firm belongs that significantly impacts the market valuation of the firm. From our results, it appears that the market reacts more negatively to breach incidents in the financial services sector. It can be surmised that financial service firms are held to a much higher standard than with regard to security of customer information. Consequently, they bear a greater responsibility in recovery efforts related to customer information breach incidents. Financial service firms may also be better served by expending more resources in preventing customer information breaches in the first place. Given consumers' high expectations of financial service firms and the general distrust with financial service practices subsequent to recent financial crisis, these firms must proactively communicate to customers about their information security investments and delineate their stringent security policies as part of the renewed emphasis on ethical practices.

Future research studies are needed to further explore customer information security breach incidents in the context of service failures and recovery. While this study examined indirect implications of data loss on customer perceptions through the impact on the market value of the firms, researchers can explore the direct impact of information breaches on customers' perceptions and reactions. Specifically, studies can examine the impact of data breach reports on service quality perceptions. One interesting question is how different types of information breaches may differentially impact consumers' perceptions.

Researchers may also want to look at the specific recovery efforts of firms suffering the breach (e.g., T. J. Maxx CEO's letter of concern to customers) and the consequent impact on customers' perception of breached firms. In addition to the recovery actions themselves, the timing of these actions is another area for future research to explore, especially how the timing impacts consumers' perceptions of the firm post breach. In future studies, research may benefit by exploring how the recovery strategy delivers procedural, distributive, and interactional justice in the breach context. Different service recovery efforts have been argued to impact customers' perceptions of the firms' brand and reputation differently (Zhu, Sivakumar, and Parasuraman 2004). It is hard to obtain reliable and accurate information pertaining to the firm's timing of service recovery efforts as most recovery efforts are done through private communications between the firm and its customers. Therefore, through experimental and survey methods, future research can focus on the direct one-to-one relationship between information breach service recovery efforts and customer evaluations of recovery efforts in terms of customer confidence/trust levels, preferences, satisfaction, repurchase intentions, and customer loyalty.

Conclusion

Given our results, we hope to focus the attention of researchers and practitioners on customer information breaches as a type of service failure (more importantly a macro-service failure that impacts a large number of customers simultaneously). Like all other service failure incidents, customer information breaches have the potential to impact customer satisfaction and customer behavior (Bitner, Booms, and Tetreault 1990; Smith, Bolton, and Wagner 1999). Well-conceived and well-executed recovery strategies can overcome customers' emotional and rational response to service failure incidents (Tax and Brown 2000). A good "breach recovery" strategy may be the reason why some of the companies in our sample manage to turn short-window negative CARs into long-window positive CARs. Companies that only see market value drop in a short burst (short-window) may be the ones that handle the customer information breach with a well thought out plan and are able to assuage the customers' negative sentiments and concerns. While the companies that "bleed" market value over a long

window may be the ones that either do not have a great service recovery plan in place and/or botch up the recovery from customer information breach incidents through missteps (such as the example of T. J. Maxx that took over a week to send out a formal letter to the customers).

Additionally, the intention of this study is to draw the attention of executives to the importance of investing in information systems security, especially when such systems pertain to customer information. Strategic attention to customer information systems security is even more critical when there is proliferating attempt to collect more and more customer information to compete on analytics and segmentation. Customer information breaches have to be thought of as severe negative critical service incidents. Any severe negative critical incident can have significant impact on customer satisfaction and market share (van Doorn and Verhoef 2008). Simply put, customer information security is a more than an information systems/technology issue. It requires that companies establish corporate policies and procedures that guide tactical actions (Dutta and McCrohan 2002). It is not practical to suggest or to plan for the fact that all information can be protected at all times. Companies must expend strategic efforts on continuity and recovery plans, especially focusing on the needs of the customer. Recovery plans should specifically focus on how to publicly address breaches (Dutta and McCrohan 2002).

Finally, customer consent is absolutely essential when collecting information. But, firms must go beyond that and make efforts to explain to customers why they are collecting information. What is the value that is passed back to the customers (the reverse transaction)? Additionally, if companies have fair procedures in place to protect customers' privacy, customers will be willing to disclose more information about themselves (Culnan and Armstrong 1999). That said, perhaps firms should take a step back and think whether they need to collect all the information they are collecting, even if consumers are willing to disclose it. More may not be better! If firms collect only that is absolutely essential, they would have less information to secure (making it easier to secure), and they may even get customers to give them limited but high-quality information. That would be a win-win proposition.

Appendix A

Table A1. Example of Data Breach Reports

Laptop Stolen With 22,000 Kaiser Patients' Data By Sherry Hu (http://cbs5.com/wrapper_consumer/seenon/consumer/stolen.laptop.kaiser.2.452422.html) OAKLAND (CBS 5)—In yet another instance of laptop theft potentially endangering personal data, Kaiser Permanente is in the process of notifying as many as 22,000 patients of a possible breach of their private medical information. The personal information was located on a doctor's laptop computer stolen from the Medical Center in Oakland at the end of last November.
TJX breach involved 45.7m cards, company reports March 28, 2007 By Jenn Abelson, Boston Globe Staff (http://www.boston.com/business/ticker/2007/03/tjx_breach_invo.html) At least 45.7 million credit and debit card numbers were stolen by hackers who broke into the computer systems at the TJX Cos. in Framingham and the United Kingdom and siphoned off data over a period of several years, making it the biggest breach of personal data ever reported, according to security specialists.
JPMorgan Chase's Private Bank Has Computer Breach August 30, 2005 By Liz Moyer (http://www.forbes.com/markets/2005/08/30/jpmorgan-chase-breach-0830markets18.html) JPMorgan Chase & Co. now has to contend with calming customers after a laptop computer containing account information was stolen from its Dallas private banking office. These aren't just any customers, either. They are wealthy individuals, mostly from Texas, who are clients of the firm's storied private bank, which has been trying to boost its image and branch out nationally for the last few years.
Medicare chastises Humana June 3, 2006 By Patrick Howington, The Courier-Journal (http://www.courier-journal.com/apps/pbcs.dll/article?AID=/20060603/BUSINESS/606030358/1003) A computer file containing Social Security numbers and other personal information on approximately 17,000 people enrolled in Humana Medicare plans was left unsecured in a hotel computer after a Humana employee called up the data, the Louisville insurer disclosed yesterday.

(continued)

Table A1 (continued)

Appendix B

Table B1. Announcement Effect in Alternative Short-Term and Long-Term Window

			Tests		
Event Windows	Mean CAR (All Firms)	Positive: Negative	Patell *Z*	Standard Cross-Sectional *Z*	Rank Test *Z*
Alternative short-term windows					
[−5 to +5]	−0.85%	41:52	−1.84*	−1.67*	−0.89
[−3 to +3]	−0.45%	46:47	−0.174*	−1.49$	−0.84
[−10 to +10]	−0.97%	44:49	−1.35$	−1.19	−0.51
Alternative long-term windows					
[+4 to +18]	−0.60%	38:55	−1.31$	−1.19	−1.41$
[+4 to +25]	−1.01%	39:54	−1.54$	−1.38$	−1.79*
[+4 to +30]	−1.82%	41:52	−2.42**	−2.07*	−2.17*
[+6 to +20]	−0.71%	41:52	−1.76*	−1.58$	−1.92*
[+6 to +30]	−1.73%	43:50	−2.36**	−1.98*	−2.18*
[+11 to +20]	−0.69%	34:59	−2.21*	−2.19*	−2.45**
[+11 to +30]	−1.70%	35:58	−2.61**	−2.38**	−2.52**

$$^{\$}p < .1$$ level. $$^{*}p < .05$$ level. $$^{**}p < .01$$ level. $$^{***}p < .001$$ level.

Appendix C

Table C1. Evolution of Breach Information

Initial Report
Fraudsters steal details on 2,000 credit
April 26, 2006
By Andy McCue, Special to CNET News.com
http://news.com.com/2100-7349_3-6065267.html
Fraudsters stole the credit card details of 2,000 MasterCard holders in a major security breach last week. Silicon.com was contacted by one customer of the Clydesdale Bank, who was told that her MasterCard details, along with those of 2,000 other people, were "in the hands of a fraudster." The theft was detected and the card stopped before it could be used by the fraudster. The Clydesdale Bank would not comment except to say it was advised of the problem by MasterCard.
Follow-Up Report
MasterCard security breach hits Morgan Stanley
But company still refuses to reveal scale or source of the credit card hack...
By Andy McCue
April 27, 2006
http://www.silicon.com/financialservices/0,3800010322,39158448,00.htm
Morgan Stanley customers in the UK are the latest to have been hit by a major security breach that has resulted in thousands of MasterCard credit card details being stolen by fraudsters. silicon.com yesterday exclusively revealed how at least 2,000 MasterCard holders have had their credit card details compromised. MasterCard notified card issuers of the breach last week and they have been calling affected customers to cancel their cards, close accounts and issue new cards and details.

... A Morgan Stanley spokeswoman told silicon.com: "The breach is something that has affected lots of issuers not just us. MasterCard informed Morgan Stanley [about the breach] and we are taking action to contact all cardholders affected, shut their accounts and issue new cards." Speculation is now growing that the UK incident could be linked to a massive security breach in the US earlier this month, which resulted in hundreds of thousands of card details and PIN numbers being compromised by hackers. MasterCard has so far declined to comment on the scale or source of the credit card security breach beyond issuing a statement saying it took immediate action as soon as the breach was discovered.

Web Appendix: Test Statistics Used in the Event Study

Boehmer, Musumeci, and Poulsen (1991) have used the following notations and formula (Equation W5) to compute the test statistics fundamental for an event study:

N number of stocks (firms) in the sample;
A_{jE} stock (firm) j's abnormal return on event day (E);
A_{jt} stock (firm) j's abnormal return on day t;
T_j number of trading days in stock j's estimation period, equal to 200 if there is no missing return;
R_m average market index return (m = market) during the estimation period;
$\hat{S}_j$ stock j's estimated standard deviation of abnormal return during the estimation period;
SR_{JE} stock j's standardized abnormal return on the event day (E).

$$= \frac{A_{jE}}{\hat{S}_j \sqrt{1 + \frac{1}{T_j} + \frac{\left(R_{mE} - \overline{R_m}\right)^2}{\sum_{t=-256}^{-2} \left(R_{mt} - \overline{R_m}\right)^2}}} \quad \text{(W1)}$$

In this study, three test statistics were utilized based on the work of Cowan and Sergeant (1996, pp. 5-9): (a) The Patell (1976) standardized residual test as used by Brown and Warner (1985) in their study, (b) Standardized cross-sectional test (Boehmer, Musumeci, and Poulsen 1991), and (c) Rank test (Corrado 1989). In each of the tests, the null hypothesis is that the mean abnormal return is equal to zero. Since each of these tests has its distinct advantages and disadvantages, we utilize all three tests to demonstrate robustness of the results of this study.

The Patell test standardizes the event-date prediction error for each stock by its standard deviation. The essence of the test is that the individual prediction errors are assumed to be cross-sectionally independent and normally distributed. Therefore, each standardized prediction error has a Student t distribution. The test statistic is computed using Equation W2.

$$Z = \frac{\sum_{j=1}^{N} SR_{jE}}{\sqrt{\sum_{j=1}^{N} \frac{T_j - 2}{T_j - 4}}} \quad \text{(W2)}$$

The Patell test is considered more powerful than the tests that do not assume cross-sectional independence (Brown and Warner 1985). The downside of Patell test is that if the variance of stock returns increases on the event date, the Patell test rejects the null hypothesis more often than the nominal significance level.

An alternative to Patell test is the standardized cross-sectional test (Cowan and Sergeant 1996). It is similar to the Patell test, but instead of using the theoretical variance of t distribution, the variance is estimated from the cross-section of event-date standardized prediction errors. When using a standardized cross-sectional test, a procedural assumption that has to be made is that the event-date variance is proportional to the estimation period variance. The test statistic can be calculated using Equation W3 (Boehmer, Musumeci, and Poulsen 1991).

$$Z = \frac{1}{N} \sum_{j=1}^{N} SR_{JE} \Bigg/ \frac{1}{N(N-1)} \sqrt{\sum_{j=1}^{N} \left(\sum_{j=1}^{N} \frac{SR_{jE}}{N}\right)^2} \quad \text{(W3)}$$

As reported by Boehmer, Musumeci, and Poulsen (1991) the test is correctly specified in NYSE-AMEX samples under null

hypothesis even when there is an increase in variance of stock returns on the event date.

The third and final test—the Rank test was developed by Corrado (1989). The procedure treats the 255-day estimation period and the event-day as a single 256-day time series. The procedure ranks each daily return for each firm. As per Corrado's (1989) notation:

K_{jt} represents the rank of abnormal return AR_{jt} in the time series of 256 daily abnormal returns of stock j. The smallest abnormal return is assigned the rank of 1. The missing returns can be adjusted for by dividing each rank by number of non-missing returns in each firm's time series plus one (Cowan and Sergeant 1996) as shown in Equation W4:

$$U_{jt} = \frac{K_{jt}}{(M_j + 1)}, \tag{W4}$$

where M_j is the number of nonmissing abnormal returns for stock j. The rank test statistic then is:

$$Z = \frac{1}{\sqrt{N}} \sum_{j}^{N} \frac{(U_{j0})}{S_u} \tag{W5}$$

The standard deviation S_u is calculated as showing in Equation W6:

$$S_u = \frac{1}{\sqrt{256}} \sum_{t=-255}^{0} \left[\frac{1}{\sqrt{N_t}} \sum_{j=1}^{N_t} (U_{jt} - 0.5) \right] \tag{W6}$$

Acknowledgments

We would like to sincerely thank *JSR*'s editor Katherine N. Lemon as well as three anonymous reviewers for their helpful comments and suggestions. We are also very grateful for the methodological guidance and assistance we received from Jennifer Conrad, Wayne Landsman, and Adam Reed.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interests with respect to the authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research and/or authorship of this article.

Notes

1. http://www.wwpi.com/index.php?option=com_content&task=view&id=3871&Itemid=128.
2. Consistent with previous research (Murphy, Daley, and Knemeyer 1999), we have used the U.S. Small Business Administration's (SBA) classification to operationalize firm size as the number of employees of a firm. Firm size has been shown to be a better explanatory variable for firm's performance than other variables such as market size, working capital, and cash flow (Johannisson and Lindström 1971).
3. Previous studies have measured the magnitude of the breach as the number of people affected (Acquisti, Friedman, and Telang 2006). However, it can be argued that the magnitude is relative to the total customer base of the affected firm. Therefore, in this study, we measure the magnitude of the breach as a ratio (the number of customers affected by a breach/total revenue of the breached firm). We used the total revenue of the breached firm as a surrogate for the number of customers a firm serves because companies are not required to publicly report customer base (number of customers) information in their annual filing.
4. http://attrition.org/dataloss/dldos.html.
5. We thank the reviewers for their suggestions for the robustness check.

References

Acquisti, Alesandro, Allan Friedman, and Rahul Telang (2006), "Is There a Cost to Privacy Breaches? An Event Study," proceedings of the Twenty-Seventh International Conference on Information Systems, Milwaukee, WI.

Aiken, Leona S. and Stephen G. West (1991), *Multiple Regression: Testing and Interpreting Interactions*. Newbury Park, CA: SAGE.

Anand, Bharat N. and Tarun Khanna (2000), "Do Firms Learn to Create Value? The Case of Alliances," *Strategic Management Journal,* 21 (3), 295-315.

Banking Technology (2008), "Data Breaches Cost FS Firms 17% More Than in Other Industries," *Banking Technology*, March 8.

Berry, Leonard (1995), *On Great Service: A Framework for Action.* New York: The Free Press.

Bitner, Mary Jo, Bernard H. Booms, and Tetreault, M. (1990), "The Service Encounter: Diagnosing Favourable and Unfavourable Incidents," *Journal of Marketing*, 54 (1), 71-84.

Bitner, Mary Jo, Stephen W. Brown, and Matthew L. Meuter (2000), "Technology Infusion in Service Encounters," *Journal of the Academy of Marketing Science*, 28 (1), 138-149.

Blattberg, Robert C. and John Deighton (1991), "Interactive Marketing: Exploiting the Age of Addressability," *Sloan Management Review,* 33 (1), 5-14.

Bloom, Paul N., George R. Milne, Robert Adler (1994), "Avoiding Misuse of Information Technologies: Legal and Societal Considerations," *Journal of Marketing*, 58 (January), 98-110.

Boehmer, Ekkehart, Jim Musumeci, and Annette B. Poulsen (1991), "Event-study Methodology Under Conditions of Event-induced Variance," *Journal of Financial Economics,* 30 (2), 253-272.

Brown, Stephen J. and Jerold B. Warner (1985), "Using Daily Stock Returns: The Case of Event Studies," *Journal of Financial Economics* 14 (March), 3-31.

Brown, Steven P. and Ricard F. Beltramini (1989), "Consumer Complaining and Word of Mouth Activities: Field Evidence," *Advances in Consumer Research*, 16 (1), 9-16.

Bunker, Matthew P. and A. Dwayne Ball (2008), "Causes and Consequences of Grudge-holding in Service Relationships," *Journal of Services Marketing*, 22 (1), 37-47.

Cable, John, Andrew Henley, and Kevin Holland (2002), "Pot of Gold or Winner's Curse? An Event Study of the Auctions of 3G Mobile Telephone Licenses in the UK," *Fiscal Studies*, 23 (4), 447-462.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou (2003), "The Economic Cost of Publicly Announced

Information Security Breaches: Empirical Evidence from the Stock Market,'' *Journal of Computer Security*, 11 (3), 431-448.

Capron, Laurence and Jung-Chin Shen (2007), ''Acquisitions of Private vs. Public Firms: Private Information, Target Selection, and Acquirer Returns,'' *Strategic Management Journal,* 28 (9), 891-911.

Carhart, Mark M. (1997), ''On Persistence in Mutual Fund Performance,'' *Journal of Finance*, 52 (1), 57-82.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan (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 (1), 70-104.

Chan, Su Han, John W. Kensingerc, Arthur J. Keown, and John D. Martin (1997), ''Do Strategic Alliances Create Value?'' *Journal of Financial Economics,* 46 (2), 199-222.

Conrad, Jennifer, Bradford Cornell, and Wayne R. Landsman (2002), ''When Is Bad News Really Bad News?'' *Journal of Finance*, 57 (6), 2507-2532.

Conrad, Jennifer and Gautam Kaul (1993), ''Long-term Market Overreaction or Biases in Computed Returns?,'' *Journal of Finance,* 48 (1), 39-63.

Corrado, Charles J. (1989), ''A Nonparametric Test for Abnormal Security-price Performance in Event Studies,'' *Journal of Financial Economics*, 23 (2), 1989, 385-395.

Cowan, Arnold R. and Anne M. A. Sergeant (1996), ''Trading Frequency and Event Study Test Specification,'' *Journal of Banking & Finance*, 20 (10), 1731-1757.

Culnan, Mary J. and Pamela K. Armstrong (1999), ''Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation,'' *Organization Science*, 10 (1), 104-115.

Dos Santos, Brian L., Ken Peffers, and David C. Mauer (1993), ''The Impact of Information Technology Investment Announcements on the Market Value of the Firm,'' *Information Systems Research*, 4 (1), 1-23.

Dutta, Amitava and Kevin McCrohan (2002), ''Management's Role in Information Security in a Cyber Economy,'' *California Management Review*, 45 (1), 67-87.

Fama, Eugene F. (1970), ''Efficient Capital Markets: A Review of Theory and Empirical Work,'' *Journal of Finance*, 25 (2), 383-417.

Fama, Eugene F. and Kenneth R. French (1993), ''Common Risk Factors in the Returns on Stocks and Bonds,'' *Journal of Financial Economics*, 33 (February), 3-56.

Glazer, Rashi (1991), ''Marketing in an Information-intensive Environment: Strategic Implications of Knowledge as an Asset,'' *Journal of Marketing,* 55 (October), 1-19.

Graddy, Duane B. and Thomas H. Strickland (2007), ''Public Information as a Deterrent to Environmental Infractions,'' *Applied Economics*, 39 (15), 1961-1972.

Hoffman, Donna L., Thomas P. Novak, and Marcos A. Peralta (1999), ''Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web,'' *Information Society*, 15 (2), 129-139.

Hovav, Anat and John D'Arcy (2003), ''The Impact of Denial-of-service Attack Announcements on the Market Value of Firms,'' *Risk Management & Insurance Review*, 6 (2), 97-121.

Hsu, Hung-Chia, Adam V. Reed, and Jörg Rocholl (2010), ''The New Game in Town: Competitive Effects of IPOs.'' *Journal of Finance*, 65 (2), 495-528.

Johannisson, Bengt and Christian Lindström (1971), ''Firm Size and Inventive Activity,'' Swedish Journal of Economics, 73 (4), 427-442.

Kalaignanam, Kartik, Venkatesh Shankar, Rajan Vardarajan (2007), ''Asymmetric New Product Development Alliances: Win-win or lose-lose Partnerships?,'' *Management Science*, 53 (3), 357-374.

Kalamas, Maria, Michael Laroche, and Lucy Makdessian (2008), ''Reaching the Boiling Point: Consumers' Negative Affective Reactions to Firm-attributed Service Failures,'' *Journal of Business Research*, 61 (8), 813-824,.

Kannan, Karthik, Jackie Rees, and Sanjay Sridhar (2007), ''Market Reactions to Information Security Breach Announcements: An Empirical Analysis,'' *International Journal of Electronic Commerce,* 12 (1), 69-91.

Kothari, S. P. and Jerold B. Warner (2006), ''Econometrics of Event Studies,'' in *Handbook of Corporate Finance: Empirical Corporate Finance*, volume A (*Handbooks in Finance Series*), B. Espen Eckbo, ed. , chapter 1. North Holland: Elsevier.

Kwansa, Francis A. (1994), ''Acquisitions, Shareholder Wealth and the Lodging Sector: 1980-1990,'' *International Journal of Contemporary Hospitality Management*, 6 (6), 16-20.

Kuykendall, Lavonne (2004), ''BJ's Case Shows Issuers' Data-breach Cost Fatigue,'' *American Banker*, 169 (165), 5.

Lewicki, Roy J. and Barbara B. Bunker (1996), ''Developing and Maintaining Trust in Work Relationships,'' in *Trust in Organizations: Frontiers of Theory and Research*, R. M. Kramer and T. R. Tyler, eds. . Thousand Oaks, CA: SAGE, 114-139.

MacKinlay, A. Craig (1997), ''Event Studies in Economics and Finance,'' *Journal of Economic Literature*, 35 (1), 13-39.

McCollough, Michael A., Leonard L. Berry, and Manjit S. Yadav (2000), ''An Empirical Investigation of Customer Satisfaction After Service Failure and Recovery,'' *Journal of Service Research*, 3 (2), 121-137.

Montoya-Weiss, Mitzi M., Glenn B. Voss, and Dhruv Grewal (2003), ''Determinants of Online Channel Use and Overall Satisfaction with a Relational, Multichannel Service Provider,'' *Journal of the Academyof Marketing Science*, 31 (4), 448-458.

Murphy, Paul R., James M. Daley, and A. Michael Knemeyer (1999), ''Comparing Logistics Management in Small and Large Firms: An Exploratory Study,'' *Transportation Journal*, 38 (4), 18-25.

Parasuraman, A. and George M. Zinkhan (2002), ''Marketing To and Serving Customers Through the Internet: An Overview and Research Agenda,'' *Journal of Academy of Marketing Science,* 30 (4), 286-295.

Parasuraman, A., Valarie A. Zeithaml, and Arvind Malhotra (2005), ''E-S-QUAL: A Multiple-item Scale for Assessing Electronic Service Quality,'' *Journal of Service Research,* 7 (3), 213-233.

Patell, James M. (1976), ''Corporate Forecasts of Earnings Per Share and Stock Price Behavior: Empirical Tests,'' *Journal of Accounting Research,* 14 (2), 246-276.

PGP Research Report (2006), ''2006 Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions,'' http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf. (accessed on March 16, 2009).

Pine II, B. Joseph (1992), *Mass Customization: The New Frontier in Business Competition.* MA: Harvard Business School Press.

Ponemon Institute (2008), "Consumers' Report Card on Data Breach Notification." April 15, 2008, Research Report by Ponemon Institute, LLC.

Robinson, Sandra L. and Denise M. Rousseau (1994), "Violating the Psychological Contract: Not the Exception but the Norm," *Journal of Organizational Behavior*, 15 (3), 245-259.

Roos, Inger (1999), "Switching Processes in Customer Relationships," *Journal of Service Research*, 2 (1), 376-393.

Smith, Amy K., Ruth N. Bolton, and Janet Wagner (1999), "A Model of Customer Satisfaction with Service Encounters Involving Failure and Recovery," *Journal of Marketing Research*, 36 (3), 356-373.

Smith, Don A. (2006), "The Still Growing Problem of Data Breach and Identity Theft," *Banking Law Journal,* 123 (10), 919-924.

Subramani, Mani and Eric Walden (2001), "The Impact of e-commerce Announcements on the Market Value of Firms," *Information Systems Research*, 12 (2), 135-154.

Swaminathan, Vanitha and Christine Moorman (2009), "Marketing Alliances, Firm Networks, and Firm Value Creation," *Journal of Marketing*, 73 (5), 52-69.

Swaminathan, Vanitha, Feisal Murshed, and John Hulland (2008), "Value Creation Following Merger and Acquisition Announcements: The Role of Strategic Emphasis Alignment," *Journal of Marketing Research*, 45 (1), 33-47.

Tax, Stephen S. and Stephen W. Brown (2000), "Service Recovery, Research Insights and Practices," in *Handbook of Services Marketing and Management*, T.A. Swartz and D. Iacobucci, eds., Thousand Oaks, CA: SAGE, 271-285.

Ting-Heng, Chu, Lin Che-Chun, and Larry J. Prather (2005), "An Extension of Security Price Reactions Around Product Recall Announcements," *Quarterly Journal of Business & Economics*, 44 (3/4), 33-48.

van Doorn, Jenny and Peter C. Verhoef (2008), "Critical Incidents and the Impact of Satisfaction on Customer Share," *Journal of Marketing*, 72 (4), 123-142.

Wall Street & Technology (2007), "Businesses Still Lack Data Security," July 16.

Wang, Sijun and Lenard Huff (2007), "Explaining a Buyer's Response to a Seller's Violation of Trust," *European Journal of Marketing*, 41 (9-10), 1033-1052.

Wirtz, Jochen, May O. Lwin, and Jerome D. Williams (2007), "Causes and Consequences of Consumer Online Privacy Concern," *International Journal of Service Industry Management*, 18 (4), 326-348.

Wolfe, Daniel (2007), "Data Breach Tab Higher at Financial Firms," *American Banker*, 172 (229), 10.

Zhu, Zhen, K. Sivakumar, and A. Parasuraman (2004), "A Mathematical Model of Service Failure and Recovery Strategies," *Decision Sciences*, 35 (3), 493-525.

Bios

Arvind Malhotra's research is focused in the areas of market impact of digital innovations and evolving organizational forms. His research projects include studying successful innovative structures, adoption of innovative technologies, and knowledge management in interorganizational contexts. Arvind's work has been published in leading journals like *Harvard Business Review*, *Sloan Management Review*, *MIS Quarterly*, *Information Systems Research*, *Journal of Service Research*, and *Journal of Academy of Marketing Science*. He received his PhD in business administration and his MS in industrial and systems engineering from the University of Southern California and his BE in electronics and communications engineering from the University of Delhi.

Claudia Kubowicz Malhotra's research interests are in the area of consumer behavior. Specifically, her research focus is on service failures and service recovery strategies, consumer privacy issues, and new product marketing. She has also examined how consumers adopt and use web and mobile technologies with a focus on the evolution and effectiveness of advertising in these contexts. Her work has been published in *Communications of the ACM*. She received her PhD and MBA from UNC's Kenan-Flagler Business School and her BSBA from Georgetown University.