

# **An Empirical Investigation of the Effect of Privacy Breaches on Firm Market Value**

## **I. Introduction**

According to many sources, 2005 was considered the worst year by far in terms of the sheer number of privacy breaches made by organizations.<sup>1</sup> Unfortunately this negative trend continued into 2006, and then nearly quadrupled in 2007 (AP 2007). “The dizzying pace of data-breach notifications in recent months shows no signs of slowing, as several more organizations have disclosed major data compromises ....”<sup>2</sup> According to Privacy Rights Clearinghouse, more than 100 million instances of data breaches have occurred in 2005 and 2006. Prior to 2005, the majority of reported privacy breaches (loss or disclosure of an individual’s personal information) affected governmental or non-profit entities. As these reported breaches become more pervasive in the for-profit environment, the interest in assessing the impact of them on market value becomes very relevant and interesting. Specifically, this research study investigates the impact of privacy breaches made by publicly traded organizations on consumers’ trust in the organization and the market value of the firm.

Analysis of stock market reactions to various types of events is certainly not new. Event study methodologies that assess whether events of all types affect capital markets have been popular for over three decades since Fama et al. (1969) put forth their efficient markets hypothesis. One stream of IT-related, stock market event studies examines whether announcements of IT investments affect firm market value (Dos Santos et al. 1993; Im et al. 2001; Chatterjee et al. 2002; Dehning et al. 2003; and Oh et al. 2006). While this research stream

---

<sup>1</sup> Lemos, Robert. 2005. “Data Security Moves Front and Center in 2005,” *Security Focus*, December 29, 2005. <http://www.securityfocus.com/news/11366>

<sup>2</sup> Vijayan, Jaikumar, and Todd Weiss. 2006. “Flurry of New Data Breaches Disclosed,” *Computerworld Online*, June 29, 2006. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001282>

began with assessing the basic question of whether such an association exists between IT investment and firm market value, it has progressed into examining which firm- and IT-specific characteristics moderate the market reaction to IT investment announcements (Oh et al. 2006). Recent research findings indicate that a firm's growth prospects, uncertainty, the strategic role of IT, and disclosure information are significantly related to cumulative abnormal returns, while asset-specificity of IT resources is not (Oh et al. 2006).

A second stream of event studies examines whether financial markets react positively to the announcement of newly created Chief Information Officer (CIO) positions (Chatterjee et al. 2001). Their results indicate that the market does indeed react positively to such information technology-related announcements. Guan et al. (2006), however, find that the results by Chatterjee et al. (2001) are driven by the subsample of firms not tracked by analysts. Specifically, they find that abnormal returns are found close to the announcement date primarily for those firms not tracked by the analysts. For the organizations tracked by the analysts, abnormal returns are found at earlier periods indicating information leakage and market adjustments being made prior to the formal CIO position announcement.

Relating to security breaches, little systematic study of capital market reaction has been conducted, and none thus far has evaluated the stock market consequences of privacy breaches. Although multiple sources (e.g., Cavoukian and Hamilton 2002; annual CSI/FBI Computer Crime and Survey Reports, and AICPA's *Understanding and Implementing Privacy Services* 2004) assert that organizations suffer significant financial losses due to such breaches, systematic examination of actual capital market reaction has been scarce. Ettredge and Richardson (2003) find, in a sample of four firms that suffered Distributed Denial of Service attacks, a statistically significant decrease in cumulative mean abnormal return of -5.2 percent for a three-day period.

They also find a contagion information transfer effect where Internet firms with similar business models also experienced a negative stock market reaction even though they were not directly attacked. Garg et al. (2003) examine whether security breaches caused a short-term stock market reaction. Their study includes six cases of web-site defacement, ten cases of Denial of Service Attacks, two cases of theft of customer information, and four cases of theft of credit card information. They find, overall, a 5.6 percent loss in share price over a 3-day period after the news of the event, although they do not report whether this is a statistically significant result. For the two cases of theft of customer information, they find no statistically significant losses. For the four cases of theft of credit information, they find a negative stock market reaction for two of the four companies, and an average stock market decline of 14.9 percent, although the overall statistical significance is not reported.

In a larger study, Cavusoglu et al. (2004) examine the capital market reaction to 66 IT security breaches experienced by publicly traded organizations. They find, overall, that the breached firms experienced a loss of 2.1 percent of their market value within two days of the announcement of the security breach. Their sample includes 34 cases of “availability” attacks and 32 “other attacks.” Thus, they do not specifically isolate privacy breaches. They do not find any significant differences in market reactions between the two categories of attacks. They also found, consistent with Ettredge and Richardson (2003), that breach cost is higher for “pureplay” or Internet only firms. They also find that security breaches cause a larger stock market reaction for smaller firms, which could be also correlated with whether they are followed by analysts as found by Guan et al. (2006), although they did not examine that aspect.

The small sample size (n=6) of privacy breaches examined by Garg et al. (2003) and Ettredge and Richardson (2003) (n=4) severely restricts the generalizability of such results. The

current study builds upon the Garg et al. (2003) and Cavusoglu et al. (2004) studies by employing a more recent data set that consists of a larger sample size of clearly identified privacy breaches and more comprehensive statistical analysis.

## **II. Theory and Hypotheses Development**

This research is guided by the efficient market hypotheses (Fama et al. 1969) and an adaptation of the four-dimensional model of IS Security developed by Loch et al. (1992), as well as previous findings by Ettredge and Richardson (2003), Garg et al. (2003), Guan et al. (2006), and Cavusoglu et al. (2004). The first hypothesis tests whether there is a stock market penalty for a firm's privacy breaches. According to Cavoukian and Hamilton (2002), "being exposed as a privacy misfit can damage your company's reputation, lead to costly litigation and send your customers running to the competition." Further, the Federal Trade Commission (FTC) has recently been investigating organizations that have not been adequately protecting personal information, and have required that some of them, such as Guidance Software, DSW Warehouse, CardSystems, BJ's Wholesale Club, Petco, Tower Records, and ChoicePoint, obtain a third party privacy assessment every two years for the next 10-20 years. Further, the FTC levied \$10 million in civil fines against ChoicePoint for their data breaches, in addition to a \$5 million customer restitution order (FTC 2006).

The stock market's reaction is a reflection of how the event ultimately affects the present value (PV) of its future expected cash flows (ECF). Prior to the announcement of the privacy breach (*time 1*), investors will value firm *i* at its market value per share of equity (MVE), and this relationship is expressed as:

$$MVE_{i1} = PV(ECF_{i1}). \quad (1)$$

When the announcement is made of the security breach, investors have new information that indicates future cash flows may be reduced due to the 1) need to increase IT spending on security, 2) cost of offering privacy monitoring services to affected customers, 3) loss of trust by consumers that may result in lower future sales, 4) litigation initiated by injured parties, and 5) possible sanctions by the FTC. Thus, at *time 2*, immediately following the announcement of the privacy breach, the value of firm *i*'s equity is expressed as:

$$MVE_{i2} = PV(ECF_{i2}). \quad (2)$$

The market value per share of equity at *time 2* equals the present value of previously expected cash flows to investors, less decreases in the cash flows due to the costs of mitigating the current attack and possible loss of future sales. This leads to the first hypothesis, which is stated in its alternative form:

*H<sub>1A</sub>: A publicly traded organization's announcement of a privacy breach is negatively associated with abnormal stock returns.*

### **Determinants of Cross-Sectional Variance**

This section is contingent upon finding statistically significant declines in the privacy breach firms' abnormal returns. Determinants of cross-sectional variation in abnormal returns are classified into two categories (Cavusoglu et al. 2004): firm specific and event specific.

#### ***Firm-Specific Mediating Factors***

Firm-specific factors that may mediate the abnormal returns around privacy breach announcements are examined by an investigation of firm type and firm size. Online consumer trust has been discussed and debated intensely in the IS literature (Gefen et al. 2003). These studies, however, only consider the trust relationships of online (web-based) scenarios. The

reality, however, is that most data breaches occur to corporate databases that were not created by web vendors. For example, the over 1 million DSW customers that had their credit card numbers stolen had made their purchases in traditional brick and mortar stores. Thus, consumers that do not make purchases online or submit their personal information online are still getting their electronically stored personal data stolen! Prior researchers studying security breaches and stock market reactions have typically categorized firms doing business on the Internet into two categories: conventional firms and internet firms (Ettredge and Richardson 2003; Cavusoglu et al. 2004). Cavusoglu et al. (2004) find that internet firms have a stronger stock market reaction to security breaches than do conventional firms. Because many businesses have morphed into integrated business models (Vasarhelyi and Greenstein 2003), we use the terms Conventional and Internet-integrated.

*H<sub>2A</sub>: The magnitude of abnormal negative returns is greater for firms more dependent on the Internet for revenue.*

Internet firms are expected to experience the largest market reaction.

Another firm-specific mediating factor examined is firm size. For a multitude of reasons given previously in the finance literature, the expected return for small firms exceeds the expected return for large firms even after accounting for market risk (Banz 1981; Fama et al. 1969). Specifically related to IT resources, Cavusoglu et al. (2004) discuss that large firms are likely to have more slack resources to deploy in case of a security breach. Cavusoglu et al. (2004) also find that smaller firms lose more market value than larger firms in the case of a security breach.

*H<sub>3A</sub>: The magnitude of abnormal negative returns is greater for smaller firms than for larger firms.*

### *Event Specific Mediating Factors*

This study also examines event-specific factors. Loch et al. (1992) present a four-dimensional model of IS Security, and this model is illustrated in Figure 1. Their model was developed prior to the “2005-2007 privacy storm” as a general security model, and it is not specific to privacy. For example, their “threats” examined did not include the possibility of accidental loss of data by employees or a third party, both of which are, unfortunately, common causes of privacy breaches. As such, we adapt their model to a Model of Privacy Breaches as illustrated in Figure 2. Specifically, we remove the distinction between human and non-human perpetrators because almost all privacy breaches contain a strong human element that cannot be ignored (Radcliffe 1998). Finally, all privacy breaches are some form of disclosure, so we do not include the other three consequences in Loch et al.’s (1992) model. Rather, we more specifically break out the characteristics of disclosure into further elements: size of breach, type of data compromised, data subject type, remediation by offering free credit monitoring, and number of days between incident and public disclosure. Thus, seven event-specific mediating factors are examined as illustrated in Figure 2. Additionally, two firm characteristics: Internet-dependency and size of firm are included as well based on the previous discussion leading to H2 and H3.

*Insert Figures 1 and 2 Here*

Privacy breaches can either stem from internal or external sources. An outsider can be considered to be either a hacker (intentional) or an external third party. External third parties may accidentally lose or disclose the data or intentionally disclose it to others. Loch et. al (1992) rank 13 security threats and they find that unauthorized access to data by employees is considered to be a bigger threat than access to data by outside hackers, however, recent CSI/FBI reports indicate that threats from external parties have increased in recent years. Loch et al. (1992) did

not consider the possibility of accidental loss of data by employees or a third party. Cannoy et al. (2006), in a meta-analysis of IS security research concerning internal vs. external threats, find that “research has largely ignored the distinction or, even more interesting, that there is no difference from an organizational perspective.” Loch et al. (1992) also discuss that security threats may either be intentional or unintentional, and this is a common categorization given by IT security professionals and academics. What is not clear, however, is which type of security threat poses the greatest risk. Since the relative “seriousness” of the source and intent of threat seems unclear, we formulate the following research questions:

*R1: The magnitude of abnormal returns for privacy breaches is no different for internal sources and external sources.*

*R2: The magnitude of abnormal returns is no different for accidental and intentional actions leading to privacy breaches.*

Size of breach is defined as the number of individuals affected by the breach. Because litigation risk and remediation costs increase with the number of individuals affected by the privacy breach, we expect, *ceteris paribus*, that the stock market reaction will be more pronounced for these organizations. Garg et al. (2003) observe, in their small sample of four companies, that the number of credit card numbers stolen is associated with the percentage drop in share price. This leads to the next hypothesis:

*H<sub>4A</sub>: The magnitude of abnormal returns is negatively related to the number of individuals affected by the breach.*

This study also examines whether the type of data exposed (credit card number, social security number, personal health information, and bank account number) affects the magnitude

of any found stock market reaction. Observations from Garg et al. (2003) indicate that the four cases of credit card data theft provided more pronounced drop in market share price than the two cases of theft of customer information. Customer information is not clearly defined, however, in their study. In an effort to understand which types of customer information may be of the most concern to consumers, we surveyed a group of individuals specifically charged with the enforcement and protection of consumers' information. This group is comprised of employees from one of Canada's *provincial* Information Privacy Commissioner's office. The results are presented in Table 1. Using a Chi-Square test of equal distributions, we find no significant differences in concern between the various types of data that are commonly exposed in data breaches. We use this information to guide us with the following hypothesis, in its null form:

*H<sub>5A</sub>: The magnitude of abnormal negative returns is not different for various types of breach of customer information.*

*Insert Table 1 Here*

Data that is exposed due to a privacy breach can be personal information for employees and/or consumers. The question is whether employee data breaches or consumer data breaches are considered more problematic. In both cases, the organizations may suffer from remediation for and litigation by the injured parties. However, for cases of consumer privacy breaches, the added potential cost of FTC or state Attorney General sanctions, as well as the loss of consumer trust, present greater consequences, *ceteris paribus*. This leads us to next hypotheses:

*H<sub>6A</sub>: The magnitude of abnormal negative returns is greater for consumer privacy breaches than for employee privacy breaches.*

The final event specific variable presented in our Model of Privacy Breaches is remediation offered in the form of free credit monitoring. While this remediation can be costly, it

averages about \$50 per individual affected, it can also restore consumer trust and good faith and reduce risk of litigation. Thus, *ceteris paribus*, we propose the following hypothesis:

*H<sub>7A</sub>: Firms that experience a privacy breach and offer free credit monitoring will have a smaller decline in their abnormal returns than firms that do not.*

Finally, we examine the number of days between the breach and the public announcement and/or media report. The longer the time a firm waits to notify its customers, the greater risk that the information may have been used to engage in identify theft. Further, if the organization sends private letters, the media tend to find out about the event and report it. Most companies at that point, within a day, issue a formal press release, so convergence of these two event dates are very, very close. Shareholders may also be concerned about the lack of transparency from management to the affected clients and to the shareholders themselves.

*H<sub>8A</sub>: The abnormal stock market returns for firms announcing privacy breaches will be negatively associated with the length of time between the privacy breach and the public announcement.*

### **III. Study Variables**

Daily abnormal returns are computed for a three-day period surrounding the privacy breach event date. Abnormal returns also are cumulated over the same three-day period. Abnormal returns are determined during the event period are based on the capital asset pricing model, and specified as follows:

$$R_{jt} = \alpha_j + \beta_j R_{mt} + \epsilon_{jt} \quad (3)$$

where:

$R_{jt}$  = the rate of return on the common stock of the  $j$ th firm on day  $t$ ;

- $R_{mt}$  = the market rate of return using the equally weighted NASDAQ index on day  $t$ ;  
 $\alpha_j$  = an intercept, and  $\beta_j$  is a slope parameter that measures the sensitivity of  $R_{jt}$  to the market index; and  
 $\varepsilon_{jt}$  = a disturbance term with the usual OLS properties.

The OLS market model is employed to estimate the abnormal return,  $AR$ , for the common stock of firm  $j$  on days  $t-1$ ,  $t=0$ , and  $t+1$  such that:

$$AR_{jt} = R_{jt} - (\alpha_j + \beta_j R_{mt}) \quad (4)$$

To estimate these returns, a 255-day estimation periods is used that begins 300 trading days before and ends 45 trading days before the event date ( $t=0$ ). To convert daily abnormal returns into cumulative abnormal returns, the daily  $AR$ s are averaged over the sample of  $N$  firms and over the three-day ( $T_1=-1$  to  $T_2=1$ ) period to yield cumulative abnormal returns,  $CAR_{T_1T_2}$ :

$$CAR_{T_1T_2}(=CAR_{1\sim 3}) = \frac{\sum_{j=1}^N \sum_{t=T_1}^{T_2} AR_{jt}}{N} \quad (5)$$

The measurement and coding of the explanatory variables examined in the analysis of cross-sectional variation are discussed in the following section.

#### IV. Sample and Descriptive Statistics

The sample of publicly traded organizations that experienced a security breach was initially identified from two sources: 1) the Privacy Rights Clearinghouse list of *A Chronology of Data Breaches*, and 2) SecureState's 2005 and 2006 Disclosures of U.S. Data Incidents. The event date is defined as the date the breach was first reported in the media. The event dates included in this study are between 1/1/2005 and 8/31/2006. News sources were checked for each company to make sure that the earliest possible publicly reported breach date is identified.

A total of 58 privacy breaches experienced by publicly traded organizations were identified that did not have any other significant press release announcements (earnings announcements, etc.) and also had return data available on CRSP. Two organizations in the sample, ADP and Wells Fargo, had more than one breach during this time period, and the breaches are considered as independent, separate events. Also, a couple of cases, a publicly traded third party (ADP) exposed or lost the data of another publicly traded organization. The stock price reaction is analyzed for both organizations in these cases. Notably absent from this list is DSW Warehouse, which has received much notoriety for its exposure of credit card information of 1.4 million customers and bank account information for over 90,000 customers. Interestingly, DSW was not publicly traded at the time of the privacy breach or the initial public notification of the breach, thus the event period cannot be examined. DSW issued its initial public offering just three months thereafter, and five months *before* the Federal Trade Commission announced its initial complaint against the company.

The organizations are listed by industry in Table 2. A wide number of industries are represented; however, just over one-third of the companies experiencing a breach are from the finance, insurance and real estate sector. Because of this clustering of firms in this one industry, the cumulative mean abnormal return will be examined by major industry classification to see if any specific industry is driving the results.

*Insert Table 2 Here*

Descriptive statistics for the variables used in the analysis of cross-sectional variance of any CARs found are given in Table 3. The variable, **Internet**, represents the firm's dependency on the Internet for revenue. In reviewing the revenue models for the organizations, the researchers classified the organizations into either Conventional=0 or Internet-Integrated=1. As

illustrated in Table 3, none of the firms in the sample are Internet only, thus supporting using an Internet-Integrated classification rather than Internet only.

*Insert Table 3 Here*

Many proxies for firm size are available, and we use the firm's market capitalization as of year-end 2005. As indicated in Table 3, the sample has a wide variety of organizations when considering size. However, the data is largely skewed, 70 percent of the organizations fall below the mean. Since this variable, **Size**, is not normally distributed, a natural log transformation is used in the analysis.

Privacy breaches can be caused by either internal or external sources, and they can be accidental or intentional. These variables are coded by reading the press releases and other media coverage to determine the coding of these variables. The variable, **ExtSource**, represents internal=0 or external source=1, and the data indicate that the majority of breaches (46 out of 58) are external. The variable, **Intent**, represents accidental=0 or intentional breach=1, and the data indicate that a majority (35 out of 58) are intentional.

The size of the privacy breach, **BreachSize**, is based on the number of individuals reported as affected by the breach. Again, this is determined by reading the press releases and other media coverage to determine the coding of these variables. The raw data is not normally distributed and is highly skewed towards relatively smaller breaches. The average breach affected over 600,000 individuals. After examining the data and taking into account that in eight of the cases, the number of individuals affected was not reported, we decided to use a categorical variable, with one category being that they chose, for whatever reason, not to report to the public how many individuals were affected. The coding of the ranges is given in Table 3.

The type of customer data exposed is also investigated. Again, this is determined by reading the press releases and other media coverage to determine the coding of these variables. This is not as precise, perhaps, as some of the other variables. Oftentimes, the press releases list a few data items that were compromised, and then proceed to mention “among other data” leaving the door open for not giving a complete list of data items. Thus, we could only code the data items that were specifically mentioned in the press releases. We created binary variables indicating whether the item was listed as compromised or not for four items: social security number (**SS**=1;otherwise=0), bank account information (**Bank**=1;otherwise=0), credit card number (**CC**=1;otherwise=0), and personal health information (**PHI**=1;otherwise=0). Although our survey results indicate the privacy regulators do not view a difference in severity of the various types of data breaches, we have no a priori theory or empirical data to indicate whether the “amount” of personal information compromised may be relevant to the firm valuation. Thus, we also create an exploratory “counting” variable, **NumbItems**, that counts the number of these items that are compromised during each breach. Table 3 indicates that social security number is most frequently compromised, while personal health information is far less frequently compromised. This may be due to strict regulation in the health care industry, which is subject to HIIIPAA regulations. Only four firms in the sample did not give some information regarding the type of data compromised. The vast majority of firms (40 out of 58) reported that only one of these four data elements was compromised.

Another variable examined in this study is the type of victim, **Victim**, and this is coded as employee=0 and customer=1. The sample events did not have any breaches where both customers and employees were affected. The majority (32 out of 58) of the breach victims were customers. Another item of interest is whether organizations can mitigate the consequences of

their privacy breach by offering the victims free credit monitoring. This variable, **FreeCredit**, is a binary variable that represents whether this is offered to the victims (1) or not (0). This seems to be a fairly popular approach as 25 of the 58 firms in the sample offered this to their victims.

Lastly, we examine whether firms are “punished” for waiting to notify the public of a breach by measuring the number of days, **Days**, between the actual breach and the press release date. As reported in Table 3, the average number of days between the event and the press release is 48 days (which would not generally meet many states’ current breach notification laws). Again, this data are not normally distributed, so the natural log of the data is used in the analysis.

We summarize our regression model as follows:

$$\mathbf{CAR} = \alpha_0 + \alpha_1 \mathbf{Internet} + \alpha_2 \mathbf{FirmSize} + \alpha_3 \mathbf{BreachSize} + \alpha_4 \mathbf{Victim} + \alpha_5 \mathbf{Freecredit} + \alpha_6 \mathbf{Days} + \alpha_7 \mathbf{ExtSource} + \alpha_8 \mathbf{Intent} + \alpha_9 \mathbf{SS} + \alpha_{10} \mathbf{Bank} + \alpha_{11} \mathbf{CC} + \alpha_{12} \mathbf{PHI} + \varepsilon \quad (6)$$

where:

**CAR** = Cumulative Abnormal Return over Days -1 to +1;  
**Internet** = 1 if the firm is Internet Integrated; 0 otherwise;  
**Firm Size** = natural log of market capitalization;  
**Breach Size** = Number of Individuals Affected by the Breach;  
**SS** = 1 if Social Security Number information is breached; 0 otherwise;  
**Bank** = 1 if Bank Account information is breached; 0 otherwise;  
**CC** = 1 if Credit Card information is breached; 0 otherwise;  
**PHI** = 1 if Personal Health information is breached; 0 otherwise;  
**Victim** = 1 if customer information is breached; 0 if employee information is breached;  
**Free Credit** = 1 if free credit monitoring is offered; 0 otherwise;  
**Days** = length of time in days from the privacy breach to the announcement of the privacy breach;  
**ExtSource** = 1 if External Source; 0= if Internal Source ; and  
**Intent** = 1 If Intentional; 0 if Accidental.

Table 4 provides a correlation matrix between the dependent variable and the cross-sectional variables. Highly significant correlations are indicated in bold in Table 4. NumItems is calculated based on SS, CC, Bank and PHI values, so those correlations are expected and are not listed here with the other highly significant correlations: 1) CAR and Days, 2) BreachSize and Victim, 3) SS and Bank, 4) SS and CC, 5) SS and Victim, 6) Bank and Victim, 7) CC and Victim, and 8) ExtSource and Intent.

*Insert Table 4 Here*

## **V. Results**

The CARs are calculated as described previously in Equation 5, and the results are presented in Table 5. We find a negative stock market reaction of -0.57 percent, which is significantly less than zero. Thus, H1 is rejected for the overall sample of firms in this study, and evidence is provided that a publicly traded organization's announcement of a privacy breach is negatively associated with its abnormal stock return.<sup>3</sup>

*Insert Table 5 Here*

### Cross-Sectional Analysis

In order to test H2 – H8 and the two research questions, regression analysis is used. The dependent variable is CAR, and the independent variables are Internet, FirmSize, BreachSize, Victim, FreeCredit, Days, ExtSource, Intent, SS, Bank, CC, and PHI.<sup>4</sup> We find that the coefficients on five of the variables are significantly different from

---

<sup>3</sup> We examine CAR by industry, and no statistical differences are found to indicate an industry effect. Also, due to high multi-collinearity with the four data types, NumItems, was excluded from the regression model.

<sup>4</sup> Variables that have a predicted direction are tested with two-tailed tests (Internet, FirmSize, BreachSize, Victim, FreeCredit and Days), while the research questions variables (ExtSource and Intent) and types of data breach variables (SS, Bank, CC PHI, and NumItems) are tested with one-tailed tests.

zero: Internet, FirmSize, Days, ExtSource, and Intent. We did not find any significance for the coefficients for the variables BreachSize, Victim, and FreeCredit.

Regarding the four data types, SS, Bank, CC, and PHI, we were really interested in whether the different types of data would cause different stock market reactions from one another. None of these variables are significant in the regression model. Because of the high correlations that exist between these data type variables, each of the four data type variables was entered into the model in isolation, and none of them was significant. Also, we conducted an ANOVA test of differences between these variables and found no differences in their relationship with cumulative abnormal returns.

*Insert Table 6 Here*

## **VI. Discussion**

A summary of the findings and how they relate to the test hypotheses and research questions is presented in Figure 3. A precursor to conducting the cross-sectional analysis is determining that a significant change (decline) occurred in stock market prices as measured by three-day CARs. The results indicate a significant decline in CAR for the firms in this sample indicating that, on average, firms suffer a decline in the stock market prices during the three-day period surrounding the public announcement of the privacy breach. The cross-sectional analysis is conducted to explore contributory factors to the magnitude of the change in CAR.

An interesting finding in this study is that, contrary to Cavusoglu et al. (2004), conventional firms experience a larger decline in stock market prices than do Internet firms. As mentioned earlier, Cavusoglu et al. do not study privacy breaches, rather they study “security” breaches. Conventional firms digitally store customer and employee

data, so perhaps it is more alarming to customers, analysts and firm shareholders when customer data are exposed. Some customers avoid online purchases because of their fear of identity theft, so unlike “availability attacks” studied in Cavusoglu et al., these customers, and ultimately investors, may have a heightened concern when a conventional firm exposes their data.

Consistent with Cavusoglu et al.’s findings, smaller firms experience a greater decline in CAR. While size can be a proxy for many things, some possible explanations are that the firm has a large customer base and strong enough reputation to weather the negative publicity. Larger firms can deploy greater resources into damage control, remediation, and additional marketing. It is also likely that the breach affects a smaller percentage of the large firm customers leading to a diminished impact on subsequent profitability as a percentage of firm sales.

As mentioned earlier, CSI/FBI reports have indicated that threats from external sources have increased in recent years. The findings in this study provide evidence that external breaches are considered to be more troubling as these types of breaches result in greater declines than do internal breaches. External breaches also include breaches by third parties. For the 46 firms in our sample that experienced a breach, 16 of these breaches were by third parties, such as data processing or shipping companies. We conducted additional testing and did not find any statistical differences between external breaches by external third parties and other external sources. Thus, for our sample at least, external breaches, of all types, result in a greater decline in CAR than do internal breaches. Thus, if an organization outsources an information processing component and a

breach occurs, that firm appears to have the potential for a more severe stock market reaction than if they insured that process and a breach occurred.

While prior researchers have discussed intentional vs. accidental breaches, no systematic empirical study has been conducted on this topic. Our findings suggest that accidental breaches are more severely punished in the stock market as evidenced by the greater decline in CAR for these firms. One possible explanation may be that people know hackers and thieves are a reality, however, they may expect that a firm's internal controls and operating procedures should protect them from errors made by employees, which to some extent may be considered negligent training and poor business practice.

Surprisingly, the number of individuals affected by a breach does not impact the CAR during the three-day announcement period. A data breach is apparently just a data breach, regardless of the number of individuals affected, according to the events examined in this sample. This result is somewhat surprising, but if recourse is sought by victims or free credit monitoring is offered to victims, then the costs of the breach are variable based on the number of individuals affected, but the results do not support this variable cost factor.

Based on a survey conducted with employees of a privacy regulator's office staff, we anticipated no difference in CAR for the four types of personal data breaches. For all four of the data elements, this proved to be true. Thus, our empirical findings corroborate the survey data we collected from a Canadian privacy regulator's office.

The results from this study indicate that no difference is perceived between disclosures of employee vs. customer data. Also, surprisingly, the risk mitigation tactic of providing free credit monitoring to customers does not apparently make a difference.

Businesses will most likely find this interesting. However, one possible explanation is that analysts consider the cost of providing this free credit monitoring service, and from a NPV perspective consider it a “wash” against customer backlash.

Finally, we find, as expected, that firms that wait to announce breaches experience a greater decline in CAR. Although the US has no federal data breach notification laws, 32 states have enacted various data breach notification laws, with California being the most stringent (Alexander 2007). Generally speaking, the various laws call for expedient notification to victims of theft of personal information that may be used in identity theft. Companies that wait to disclose may be found in violation of this requirement. The average days between the privacy breach and the public announcement is 48 days, which most privacy experts would agree is too long. “One of the primary causes of legal action is the accusation that you knew sooner than you told,” according to Rob Scott, managing partner at Scott & Scott LLP, a law and technology services firm in Dallas (Wood 2007). With the finding that it takes 48 days to disclose this to the public, firms may need to review their disclosure policies to minimize the damage to their firm’s reputation and stock price, as well as minimize the possibility of litigation.

## **VII. Limitations of the Study and Future Research Implications**

A few limitations should be noted. Despite our efforts to isolate the privacy breach announcements from all other announcements (see above), it is possible that the results are driven by other contemporaneous events not covered in the press announcement. Second, given the average delay of 48 days between the privacy breach and the public announcement, there exists a possibility of leakage to the financial

markets. In general, this would bias us against finding abnormal returns around the date of the breach announcement. There is also the possibility of a correlated omitted variable that could be driving the results which we have yet to discover. Only by conducting this sort of analysis can we begin to uncover other possible explanations for abnormal returns around privacy breach announcements.

There are several ideas for future research. Following Ettredge and Richardson (2003), it might be interesting to assess the contagion stock market reaction to competitors and others in the same industry. Future researchers could use case analysis techniques to determine more directly the costs of such privacy breaches, looking specifically at lost customers, lost revenues, increased security costs, increased marketing costs, and other increased costs that may not be as apparent in an archival study such as this one. In addition, as future privacy breaches proliferate, it may be interesting to examine the stock market reaction to FTC sanctions, although currently only a very small sample would be possible.

This study suggests that privacy breaches can be particularly costly to an organization. However, by following best practices and by considering some of the mediating factors studied in this paper, firms may be able to reduce their exposure to such breaches. The AICPA has provided the business community with Generally Accepted Privacy Principles. While this is designed as an assurance function, it is based on worldwide best practices and tangible guidance on reducing privacy risk. GAPP has recently been noted Cline (2007) as “likely to become the most important new source of requirements for your IT projects since Y2k and Sarbanes-Oxley.” Given the increasing number of data breaches, and the evidence provided here that stock market price is

affected by the announcement of such breaches, members of both industry and academia should embrace the concept of privacy risk mitigation.

## References

- AICPA. 2004. *Understanding and Implementing Privacy Services*, AICPA.
- Alexander, P. 2007. Data breach notification laws: A state by state perspective. *Intelligent Enterprise*. April 9, 2007.  
<http://www.intelligententerprise.com/showArticle.jhtml?articleID=198800638>.
- Associated Press. 2007. Data security breaches reach a record in 2007. December 31, 2007. *Wall Street Journal Online*,  
[http://online.wsj.com/article\\_print/SB119906141243958571.html](http://online.wsj.com/article_print/SB119906141243958571.html).
- Banz, R. 1981. The relationship between return and market value of common stocks. *Journal of Financial Economics* 9: 3-18.
- Cannoy, S., P. Palvia, and R. Schilhavy. 2006. A research framework for information systems security. *Journal of Information Privacy & Security* 2 (2): 3-29.
- Cavoukian, A., and T. Hamilton. 2002, *Privacy Payoff*, McGraw-Hill.
- Cavusoglu, H., B. Mishra, and S. 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): 69-104.
- Chatterjee, D., C. Pacini, and V. Sambamurthy. 2002. The shareholder-wealth and trading-volume effects of information technology infrastructure investments. *Journal of Management Information Systems* 19 (2): 7-42.
- Chatterjee, D., V. Richardson, and R. Zmud. 2001. Examining the shareholder wealth effects of announcement of newly created CIO positions. *MIS Quarterly* 25 (1): 43-70.
- Cline, Jay. 2007. "Mind the GAPP: Accountants bring GAAP-like principles to the privacy sphere," *Computerworld Online*, December 6, 2007.  
<http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9051459&pageNumber=1>
- Dehning, B., V. Richardson, and R. Zmud. 2003. The value relevance of announcements of transformational information technology investments. *MIS Quarterly* 27 (4): 637-656.
- Dos Santos, B, K. Peffers, and D. Mauer. 1993. The impact of information technology investment announcements on the market value of the firm. *Information Systems Research* 4 (1): 1-23.

- Ettredge, M., and V. Richardson. 2003. Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems* 17 (2): 71-82.
- Fama, E., L. Fisher, M. Jensen, and R. Roll. 1969. The adjustment of stock prices to new information. *International Economic Review* 10: 1-21.
- Federal Trade Commission. 2006. FTC File No. 052-3069; Civil Action No.: 1:06-cv-00198-GET
- Garg, A., J. Curtis, and H. Halper. 2003. Quantifying the financial impact of IT security breaches. *Information Management & Computer Security* 11 (2/3).
- Gefen, D., E. Karahanna, and D. W. Straub. 2003. Trust and TAM in online shopping: An integrated model. *MIS Quarterly* 21 (1): 51-90.
- Guan, L., S. Sutton, C. Chang, and V. Arnold. 2006. Further evidence on shareholder wealth effects of announcements for newly created CIO positions. *Database for Advances in Information Systems* 37 (2/3): 176-187.
- Im, K., K. Dow, and V. Grover. 2001. A reexamination of IT investment and the market value of the firm – An event study methodology. *Information Systems Research* 12 (1): 103-117.
- Loch, K. D., H. H. Carr, and M. E. Warkentin. 1992. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly* 16 (2): 173-186.
- Privacy Rights Clearinghouse. 2007. A chronology of data breaches. <http://www.privacyrights.org/ar/chrondatabreaches.htm>.
- Radcliffe, D. 1998. Physical security: The danger within. *Infoworld* 20 (16): 95-96.
- Vasarhelyi, M., and M. Greenstein. 2003. Underlying principles of the electronization of business: A research agenda. *International Journal of Accounting Information Systems* 4 (1).
- Wood, Lamont. 2007, "What, How, and When to Respond to a Data Breach," CIO, April 27, 2007, [http://www.cio.com/article/106551/What\\_When\\_and\\_How\\_to\\_Respond\\_to\\_a\\_Data\\_Breach/1](http://www.cio.com/article/106551/What_When_and_How_to_Respond_to_a_Data_Breach/1).

Table 1  
 Type of Data Compromised  
 Rankings of Importance

Type of Data	Provincial Information Privacy Commissioner's Office - Canada N=49		
	Mean	Std. Dev.	Chi- square test statistic
Social Security/Social Insurance Number	2.31	(1.122)	2.2
Bank Account Number	2.37	(1.112)	2.5
Credit Card Number	2.47	(1.209)	3.2
Personal Health Information	2.51	(1.063)	4.0

1 being the most upset  
 4 being the least upset

**Table 2**  
**Industry Classification by SIC Code**

<b>SIC Code</b>	<b>SIC Industry Name</b>	<b>Number of Companies</b>	<b>% of Sample</b>	
<b>Manufacturing</b>				
23	APPAREL AND OTHER TEXTILE PRODUCTS	1		
27	PRINTING AND PUBLISHING	1		
29	PETROLEUM AND COAL PRODUCTS	1		
36	ELECTRONIC & OTHER ELECTRIC EQUIPMENT	1		
37	TRANSPORTATION EQUIPMENT	5		
38	INSTRUMENTS AND RELATED PRODUCTS	1		
	<b>Total: Manufacturing</b>		10	17.2%
<b>Transportation, Communications, Electric, Gas And Sanitary</b>				
40	RAILROAD TRANSPORTATION	1		
45	TRANSPORTATION BY AIR	1		
48	COMMUNICATION	4		
49	ELECTRIC, GAS, AND SANITARY SERVICES	1		
	<b>Total: Trans., Comm., Ele., Gas&amp; San.</b>		7	12.1%
51	<b>Wholesale Trade - Nondurable Goods</b>	1	1	1.7%
<b>Retail Trade</b>				
53	GENERAL MERCHANDISE STORES	1		
54	FOOD STORES	2		
57	FURNITURE AND HOMEFURNISHINGS STORES	1		
	<b>Total: Retail Trade</b>		4	6.9%
<b>Finance, Insurance &amp; Real Estate</b>				
60	DEPOSITORY INSTITUTIONS	9		
61	NONDEPOSITORY INSTITUTIONS	2		
62	SECURITY AND COMMODITY BROKERS	3		
63	INSURANCE CARRIERS	5		
64	INSURANCE AGENTS, BROKERS, & SERVICE	1		
67	HOLDING AND OTHER INVESTMENT OFFICES	1		
	<b>Total: Finance, Ins.,&amp; Real Estate</b>		21	36.2%
<b>Services</b>				
70	HOTELS AND OTHER LODGING PLACES	1		
72	PERSONAL SERVICES	1		
73	BUSINESS SERVICES	8		
78	MOTION PICTURES	1		
79	AMUSEMENT & RECREATION SERVICES	1		
	<b>Total: Services</b>		12	20.7%
<b>Public Administration</b>				
80	HEALTH SERVICES	1		
87	ENGINEERING & MANAGEMENT SERVICES	1		
	<b>Total: Public Administration</b>		2	3.5%
99	<b>Nonclassifiable Establishments</b>	<u>1</u>	<u>1</u>	1.7%
		58	58	

**Table 3**  
**Descriptive Statistics**  
**Cross-Sectional Variables**

	<u>N</u>		<u>N</u>
Internet-Dependency ( <b>Internet</b> ):		Source of Breach( <b>ExtSource</b> ):	
Conventional	25	Internal	12
Internet-Integrated	<u>33</u>	External	<u>46</u>
	58		58
Intentional Breach ( <b>Intent</b> ):		Victim of Breach( <b>Victim</b> ):	
No (Accident)	23	Employee	26
Yes	<u>35</u>	Customer	<u>32</u>
	58		58
Offer of Free Credit Monitoring ( <b>FreeCredit</b> ):			
Yes	25		
No	<u>33</u>		
	58		
Types of Customer Data Exposed (Breaches may expose more than 1 data type):			
Social Security Number ( <b>SS</b> )	48		
Bank Account Number ( <b>Bank</b> )	12		
Credit Card Number ( <b>CC</b> )	7		
Personal Health Information ( <b>PHI</b> )	4		
<u>No. of Data Items Exposed (<b>NumItems</b>)</u>			
1	40		
2	11		
3	3		
4	0		
Data type not reported	<u>4</u>		
	58		
<hr/>			
Size – Market Capitalization ( <b>FirmSize</b> ):		Days between breach & event ( <b>Days</b> ):	
Mean	\$ 46,890 M		48
Std. Dev.	(71,614 M)		(108)
Max	\$367,473 M		720
Min	\$ 55 M		0
Size of Breach-number of individuals affected ( <b>BreachSize</b> ):			
Less than 10,000	12	Mean	620,368
10,000 – 99,999	19	Std. Dev.	( 2,368,332)
100,000 – 999,999	14	Max	16,300,000
Greater than 1 million	5	Min	80
Not reported	<u>8</u>		
	58		

**Table 4**  
**Correlation Matrix of Variables**  
**Pearson Correlations**

	CAR	Internet	Firm Size	Breach Size	SS	Bank	CC	PHI	Numb Items	Victim	Free Credit	Days	ExtSource	Intent
CAR	1													
Internet	.19	1												
Firm Size	.02	-.09	1											
Breach Size	.01	-.02	-.16	1										
SS	.15	-.12	.01	-.08	1									
Bank	.02	.02	-.10	.24	<b>-.33*</b>	1								
CC	-.06	-.10	-.04	.19	<b>-.34*</b>	.22	1							
PHI	.11	.03	.00	.08	.11	-.02	-.11	1						
Numb Items	.12	-.13	-.09	.26	.19	<b>.63***</b>	<b>.47***</b>	<b>.45***</b>	1					
Victim	-.01	.20	-.21	<b>.40**</b>	<b>-.35**</b>	<b>.30**</b>	<b>.36**</b>	-.03	.20	1				
Free Credit	.05	-.23	.04	.25	-.13	-.05	.23*	.12	.08	.10	1			
Days	<b>-.48***</b>	-.16	.08	.26	-.19	-.08	.13	-.06	-.12	.27	.13	1		
ExtSource	-.17	.16	.23	-.10	.08	-.07	.06	-.03	.02	-.03	-.12	.12	1	
Intent	-.12	-.14	.25	-.11	-.08	.05	-.05	.23	.07	.05	.05	.04	<b>-.37**</b>	1

**\*\*\*, \*\*, \* significantly respectively at .001, .01 and .05**

**Variable Definitions:**

**CAR** = Cumulative Abnormal Return over Days -1 to +1; **Internet** = 1 if the firm is Internet Integrated; 0 otherwise. **Firm Size** = natural log of market capitalization; **Breach Size** = Categorical representing ranges of Individuals Affected by the Breach; **SS** = 1 if Social Security Number information is breached; 0 otherwise; **Bank** = 1 if Bank Account information is breached; 0 otherwise; **CC** = 1 if Credit Card information is breached; 0 otherwise; **PHI** = 1 if Personal Health information is breached; 0 otherwise; **Victim** = 1 if customer information is breached; 0 if employee information is breached; **Free Credit** = 1 if free credit monitoring is offered; 0 otherwise; **Days** = length of time in days from the privacy breach to the announcement of the privacy breach; **ExtSource** = 1 if External Source; = if Internal Source ; **Intent** = 1 If Intentional; 0 if Accidental

**Table 5**  
**Mean Abnormal Returns of Firms Experiencing Privacy Breaches**  
**Market Adjusted Returns**

<b>Days</b>	<b>N</b>	<b>Mean Cumulative Abnormal Return</b>	<b>Positive: Negative</b>	<b>Portfolio Time-Series (CDA) t</b>
(-1,+1)	58	-0.57%	24:34	1.99*

\* denotes statistical significance at the .05 level

**Table 6**  
**Regression - Full Sample**  
**N=58**

$$CAR = \alpha_0 + \alpha_1 \text{Internet} + \alpha_2 \text{FirmSize} + \alpha_3 \text{BreachSize} + \alpha_4 \text{Victim} + \alpha_5 \text{Freecredit} + \alpha_6 \text{Days} + \alpha_7 \text{ExtSource} + \alpha_8 \text{Intent} + \alpha_9 \text{SS} + \alpha_{10} \text{Bank} + \alpha_{11} \text{CC} + \alpha_{12} \text{PHI} + \varepsilon \quad (6)$$

R	R Square	Adjusted R Square	Std. Error of the Estimate
.679	.46	.266	.0190

**ANOVA**

	Sum of Squares	df	Mean Square	F	Sig.
Regression	.010	12	.001	2.357	.026
Residual	.012	33	.000		
Total	.022	45			

**Coefficients**

	Unstandardized Coefficients			
	B	Std. Error	t	Sig.
(Constant)	-.039	.025	-1.547	.131
<b>Internet</b>	<b>.012</b>	<b>.006</b>	<b>1.849</b>	<b>.037</b>
<b>FirmSize</b>	<b>.004</b>	<b>.002</b>	<b>1.726</b>	<b>.047</b>
BreachSize	.003	.004	.819	.210
Victim	-.002	.008	-.279	.391
Freecredit	-.001	.006	-.145	.443
<b>Days</b>	<b>-.008</b>	<b>.002</b>	<b>-3.056</b>	<b>.002</b>
<b>ExtSource</b>	<b>-.018</b>	<b>.008</b>	<b>-2.174</b>	<b>.037</b>
<b>Intent</b>	<b>.013</b>	<b>.007</b>	<b>1.919</b>	<b>.064</b>
SS	.012	.010	1.176	.248
Bank	.003	.008	.395	.695
CC	.008	.010	.791	.435
PHI	-.015	.013	-1.201	.238

Dependent Variable: CAR

Note:

The p-values reflect one-tailed tests with the exception of ExtSource and Intent, which are two-tailed tests, since no sign was predicted in the hypotheses.

Figure 1  
Loch et al. (1992) Model of IS security

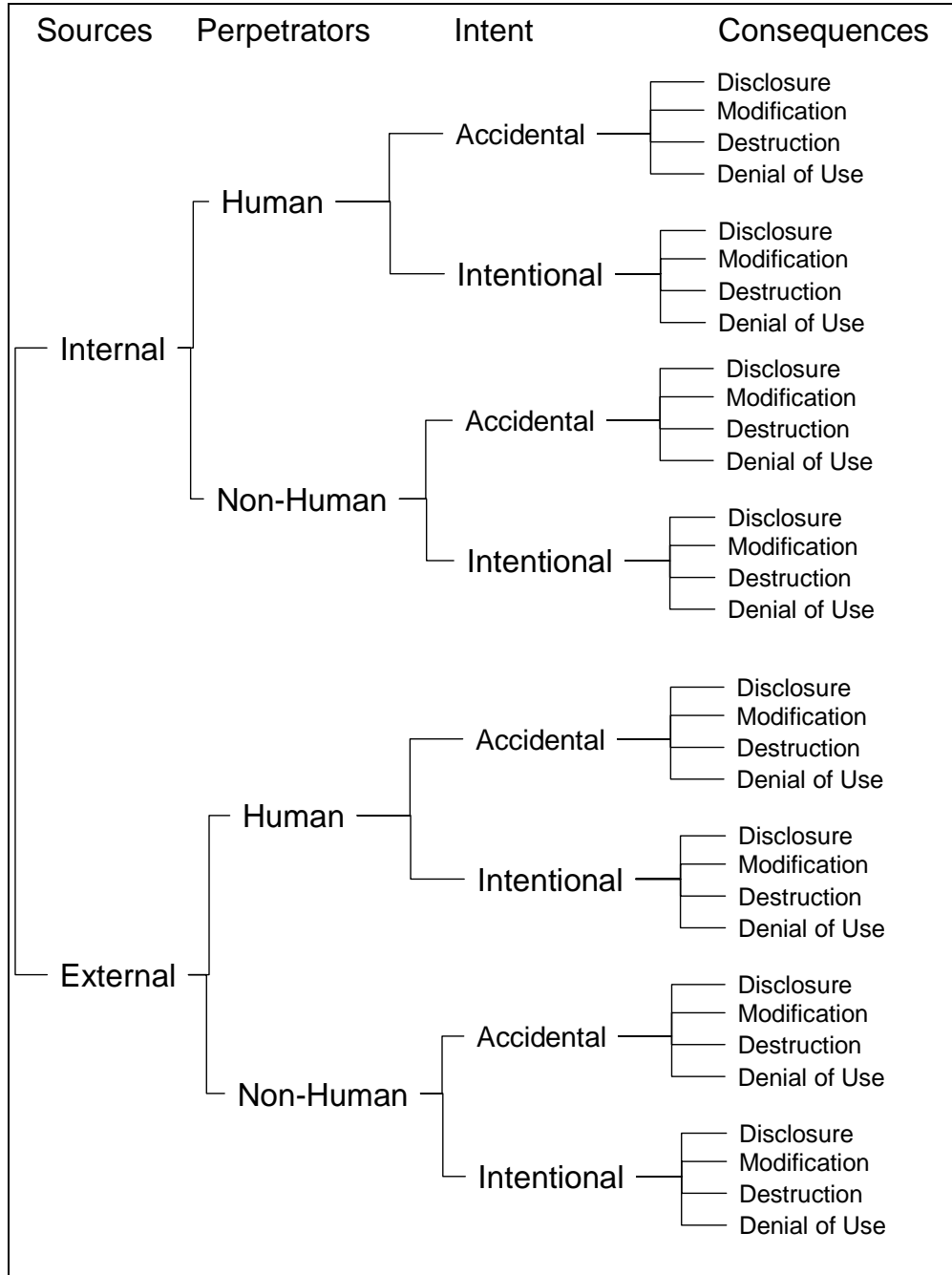


Figure 2  
Model of Privacy Breaches

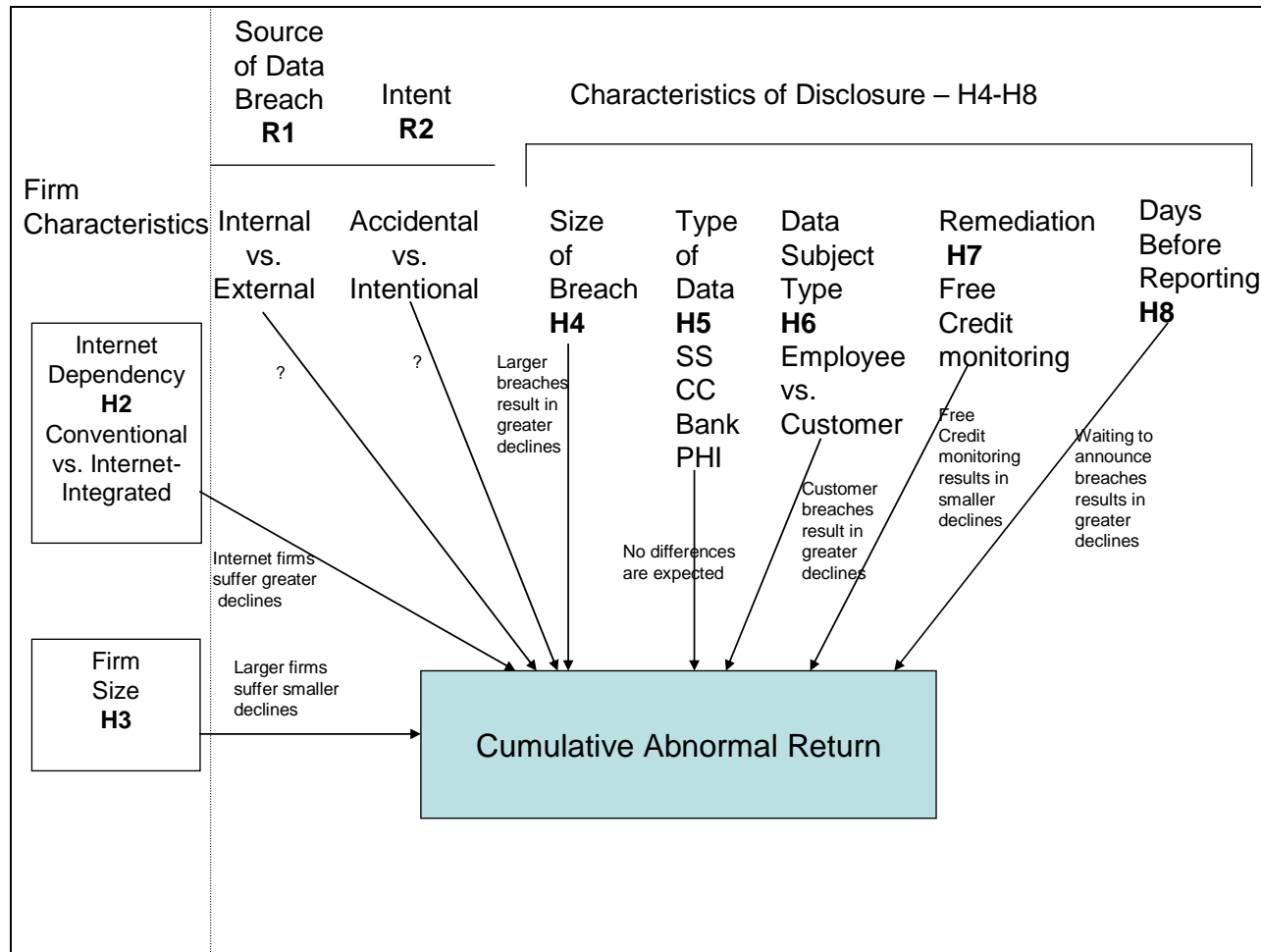


Figure 3  
Summary of Findings

