Communications of the Association for Information Systems

Volume 34 Article 3

1-2014

The Impact of Federal and State Notification Laws on Security Breach Announcements

Sanjay Goel
University at Albany, SUNY, goel@albany.edu

Hany A. Shawky
Department of Finance, School of Business, University at Albany, State University of New York

Recommended Citation
Goel, Sanjay and Shawky, Hany A. (2014) "The Impact of Federal and State Notification Laws on Security Breach Announcements," *Communications of the Association for Information Systems*: Vol. 34 , Article 3.
DOI: 10.17705/1CAIS.03403
Available at: https://aisel.aisnet.org/cais/vol34/iss1/3

Communications of the Association for Information Systems

CAIS

The Impact of Federal and State Notification Laws on Security Breach Announcements

Sanjay Goel

Department of Information Technology Management, School of Business, University at Albany, State University of New York, New York State Center for Information Forensics and Assurance (CIFA)

goel@albany.edu

Hany A. Shawky

Department of Finance, School of Business, University at Albany, State University of New York

Abstract:

Firms are under increasing regulatory pressures to protect consumers' confidential information. The focus of this article is to examine the impact of federal and state breach notification laws in coaxing organizations to improve security of customers' confidential information. Specifically, we use event-study methodology to examine the impact of security breach announcements on the market value of firms during the period before and after the enactment of this legislation. Our results show that the negative impacts of security breach announcements on stock prices have been reduced significantly after the enactment of federal and state security breach notification laws.

Keywords: information security; event study; security legislation; economics of security; security breaches

Volume 34, Article 3, pp. 37–50, January 2014

Communications of the Association for Information Systems

I. INTRODUCTION

Government and the states are responsible for introducing legislation that protects shareholder interests and ensures employee work safety. Such laws can have a significant impact on firms by adding constraints to their operations and requiring audits to demonstrate compliance [Bartel and Thomas, 1985].[1] The focus of this article is to examine the impact of federal and state breach notification laws in coaxing organizations to improve security of customers' confidential information. Specifically, we use event-study methodology to examine the impact of security breach announcements on the market value of firms during the period before and after the enactment of this legislation.

Security breach notification laws have been enacted in the United States since 2002. The first such law, the California data security breach notification law, Cal. Civ. Code 1798.82 and 1798.29, was enacted in 2002 and became effective on July 1, 2003. As related in the bill statement, the law requires "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The enactment of state and federal security breach notification laws is intended to compel firms to disclose to the public any incidence of a security breach regardless of its severity or its consequences. While the intended purpose is to protect the public, the impact of such laws may have important consequences on firms. We surmise that breach notification laws might have an impact similar to that of the Sarbanes-Oxley Act [Swartz, 2003; Zhang, 2007], where there is a reputational burden on firms resulting from the release of security breach incidents that would impact firms.

The rationale behind the breach notification statutes is twofold: (1) to give individuals a warning and a chance to protect themselves and (2) to encourage stronger security measures by requiring firms to publicize their breaches. Enacting such laws has significantly contributed to heightened awareness of the importance of information security throughout all levels of a business organization. Moreover, enacting these laws helped to inform consumers of the need to cautiously manage their identities online. One of the concerns, however, is that the current requirement for notifying customers of any breach generates too many breach disclosure letters, which may desensitize customers to such announcements.

The impact of negative events on a firm has been measured by estimating the changes in the market value of firms consequent to the event. Generalized conclusions based on specific types of events such as industrial accidents, lawsuits, and so on, can be drawn using event studies. Several such event studies are reported in the literature; for instance, Broder and Morrell [1991] have used event-study methodology to investigate the impact of industrial accidents on the market values of firms. They find a strong negative correlation between such accidents and firm valuation. Parmeswaran, Venkateshan, Gupta, Sharman, and Rao [2011] examine the impact of both positive and negative cloud computing announcements on the valuations of firms. Gupta, Sharman, and Rao [2010] have used event studies to examine the timing of Corporate Crisis Response to Security Breaches and find a significant correlation. Campell, Gordon, Loeb, and Zhou [2003] examined the impact of security breaches on market values and found that firms that experience a breach of "confidential information" experienced a 5 percent drop in market value while firms that experience a non-confidential breach had no such impact. Cavusoglu Mishra, and Raghunathan [2004] found that on average, firms lose approximately 2.1 percent of their market values within the two days surrounding the announcement of a security breach. However, Kannan, Rees, and Sridhar [2007] did not find a significant negative return on market valuations due to security breaches.

[1] For instance, the OSHA regulation introduced in 1970, designed to protect employee health and safety, costs industry over $2.7 billion each year [Weidenbaum and DeFina, 1978]. Similarly, an HIPAA regulation that was introduced in 1996 to protect patient information privacy is estimated to cost in the range from $3 billion to $43 billion in compliance and enforcement [Artnak and Benson, 2005]. Sarbanes-Oxley legislation was enacted in 2002 to improve internal controls and strengthen Corporate Governance practices. Estimates by Zhang [2007] suggest that the enactment of this legislation has cost corporations a total of $1.4 trillion in market value. In this particular case, the cost of implementing this legislation has been higher than expected [Braganza and Desouza, 2006; Swartz, 2003].

In another case, Goel and Shawky [2009] documented a significant negative impact on the market value of firms surrounding the announcement of a security beach, but indicated that the decline is in the order of 1 percent of firm value, an amount that is much lower than other studies have found. Hovav and D'Arcy [2004, 2005] have examined the impact of security breaches for a limited subset of breaches and conclude that the relative impact of the different types of breaches is not clear. Acquisti, Friedman and Telang [2006][2] investigated the impact of privacy breaches on firms and found a significant negative impact of such breaches on the market value of firms.

Gordon, Loeb and Zhou [2011] examined whether the impact of security breaches has been declining over time. They studied the impact of security breaches on firms in two distinct subperiods and concluded that there has been a significant downward shift in the impact of security breaches in the period following the 9/11 terrorist attacks relative to the pre-9/11 period. They attributed this downward shift to more effective remediation and disaster recovery by firms as well as to a perceived decrease in the tendency of customers to refrain from doing business with firms experiencing an information breach.

Our empirical results indicate that the negative impact of security breach announcements on the stock prices of publicly traded firms have been significantly reduced after the enactment of federal and state notification laws. The remainder of this article is organized into four sections. In Section II we develop our main hypothesis and our plan of testing it. In Section III we provide a detailed description of the data collection process. In Section IV we describe our event-study methodology, while in Section V we present our results and discuss their implications. A brief summary concludes the article.

II. HYPOTHESIS DEVELOPMENT

The incidence of security breaches continues to increase in both public and private organizations. In the past, many incidents went unreported due to the reticence of organizations to generate bad publicity or expose their vulnerability to potential hackers. To address this issue, mandatory security breach disclosure laws have been adopted by most states. These laws require companies to disclose the breaches publicly and inform their customers. Appendix A lists all fifty U.S. states plus the District of Columbia, showing their effective adoption dates. Many state regulations impose civil or criminal penalties for failure to disclose breach of public information. However, there is considerable variation in the laws across the different states [Bingisser, 2008] and there has been some support of a uniform federal breach notification law [Picanso, 2006-7]. In any case, the basic purpose remains the same (i.e., to give individuals a warning and a chance to protect themselves and to encourage firms to engage in better information security practices [Faulkner, 2007]).

Given the preponderance of empirical evidence regarding the negative impact of security breach announcements on firm value, we investigate whether this negative market impact on firm value has been affected by the enactment of federal and state security breach announcement laws. Since regulatory legislation can have a significant impact on a company's cash flows, event studies can be used as a metric for measuring the impact of such legislation on firm value.

Event-study methodology has been extensively used for policy analysis and for measuring the impact of legislation on firms in several areas including corporate law [Bhagat and Romano; 2002a, 2002b], gaming legislation [Bin, Puclik and He, 2009], energy tax legislation [Gilligan and Krehbiel, 1988], Sarbanes-Oxley [Chai, Kim and Rao, 2011; Chhaochharia and Grinstein, 2007; Li, Pincus and Rego, 2008 Litvak, 2007; Rezaee and Jain, 2005], and corporate governance [Bhagat and Romano, 2002b; Brown and Caylor, 2006; Durnev and Kim, 2005].

We hypothesize that the enactment of the security breach notification laws has the potential of influencing behavior and could therefore impact stock market prices of impacted firms in two ways. First, it is possible that firms may become more careful in preventing such breaches, which may in turn reduce the average aggregate negative effect of such breaches on firm value. Second, it is also possible that the increased disclosure of breaches due to these notification laws may desensitize investors and the public to such breach announcements, leading once again to a reduced impact on firm value. In this article, we test the specific hypothesis that the enactment of security breach notification laws might have actually reduced the impact of security breach announcements on firm value.

III. DATA COLLECTION

The data on security breach incidents was collected from public sources. A majority of the reported cases involved breach of confidentiality. Data collection was done in two steps. In the first step, we collected information on

[2] Telang and Wattal [2007] also conducted a study on disclosure of the vulnerabilities of software vendors and showed that firms lose around 0.6 percent of their market value when the vulnerability is reported.

breaches from online sources through the use of search engines.[3] Existing repositories of breaches were used in identifying incidents (e.g., Privacy Rights Clearing House). The incidents were then filtered to identify firms that were publicly traded in the United States. Once we obtained the filtered list of incidents, we then looked for company-specific information through search engine queries and online news repositories such as LexisNexis, Reuters, *New York Times*, and *Wall Street Journal*.

The critical data needed for this research included the identification of security breach announcement dates collected from various media outlets such as LexisNexis, *Wall Street Journal*, *PC Week*, Register, and others. Media reports that covered more than one individual security breach were associated with each of the security breaches reported. If the news was released on a holiday, we used the following day when the market was open as the event-study date.[4] If a single breach incident was published in numerous media outlets, it was considered a single report. To avoid contamination of the estimation period, we excluded from our sample any firm that experienced more than one security breach within a period of one year.

The other data needed for the study were the daily stock prices for the firms in our sample that were identified with security breach announcements for a period of thirteen months before the breach event and one month after the event date. This data was obtained from the Center for Research in Security Prices (CRSP). The remaining data needed to estimate the four factor market model parameters were the CRSP value-weighted market factor, the small firm factor, the value premium factor, and the momentum factor; all were obtained from the Kenneth French data library website.[5]

IV. METHODOLOGY

The efficient market hypothesis asserts that financial markets are informationally efficient, and that stock prices reflect all publicly available information.[6] Thus, using event-study methodology, the impact of security breaches can be measured by observing changes in the market value of firms in response to announcements of such incidents. This strategy is especially appropriate since market capitalization is a key indicator of firm performance and drives many business decisions.

McWilliams and Siegel [1997, 1999] point out that a well-crafted event study must clearly define the event that provides the new information with sufficient theoretic justification. They further note that confidence in the results can only be achieved when the abnormal returns associated with the event are correctly identified. Such identification relies on the following assumptions: (1) markets are efficient, (2) the event was unexpected by the market, and (3) there are no confounding effects during the event window.

In the context of our study, the new information that was unanticipated by the market was the announcements of security breaches. However, we went one step further in this study and attempted to distinguish between the impact of such announcements on firm value during the periods prior to and subsequent to the enactment of the security breach notification laws. When new information was released to the market, the true economic impact of such information was quickly and completely reflected on a firm's stock price [Fama, 1970].[7] Brown and Warner [1985] showed that the value adjustment process by the stock market would include any expected cost and benefit related to the new information.

The third assumption pertaining to potential confounding effects is quite important although it can be substantially addressed by choosing a very short event window, which we use in this study.[8] In essence, we assume that there are no other major confounding events such as the declaration of dividends, stock buy-backs, merger announcements, product announcements, or any impending forms of litigation. While such events cannot possibly be ruled out for each and every firm in our sample, it is highly unlikely that such effects would appear in any consistent pattern within our fairly short event window to impact our results.

Brown and Warner [1980, 1985] and MacKinlay [1997] provide a comprehensive review of event-study methodology and articulate several essential steps for the successful implementation of this approach. First, normal or expected

[3] We used several terms including "breaches," "security breaches," "security incidents." "data loss," and "Internet breach incidents."
[4] For instance, a security breach at Citibank was reported close to midnight on Friday, June 8, 2011, by Reuters. This was followed by a spate of announcements on Saturday. The event-study date for this incident was Monday, June 11, 2011, when the market opened.
[5] mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html
[6] Malkiel [2003] provides a comprehensive review of the efficient market hypothesis with supporting evidence of its robustness and centrality to our financial markets.
[7] Ball and Brown [1968] investigated the impact of earnings announcements on security prices and Fama, Fisher, Jensen, and Roll [1969] examined the market reaction to stock splits.
[8] The longer the event window, the more difficult it would be to control for events that might cause a confounding effect.

Communications of the Association for Information Systems

return performance for the firm must be reliably estimated. We use the three Fama-French [1993] factors plus the momentum factor in estimating expected returns:

$$R_t - R_t^{T-Bill} = \alpha + \beta_1 \cdot RMRF_t + \beta_2 \cdot SMB_t + \beta_3 \cdot HML_t + \beta_4 UMD + \varepsilon_t \qquad (1)$$

where R_t is the return on security in period t, $R_t^{T\text{-}Bill}$ is the return on U.S. Treasury bills in month t, and $RMRF_t$ is the CRSP value-weighted market portfolio minus the U.S. T-bill rate. The SMB_t and HML_t are the Fama-French factors that represent the small firm premium and the value premium, respectively, and *UMD* is the Carhart [1997] momentum factor that takes into account risk related to return persistence.[9]

Having estimated the expected return, abnormal returns can then be calculated by subtracting the normal return from the actual return, such that $AR_{it} = K_{it} - R_{it}$, where AR_{it} is the abnormal return on security i in period t and K_{it} is the actual return on security i in period t. We have chosen the length of the estimation window (255 days) to be sufficiently long such that, under the null hypothesis, the distribution of the sample abnormal returns of a given observation in the event window is approximately normally distributed: $AR_{it} \approx \mathrm{N}(0, \sigma^2(AR_{it}))$. The next step is to aggregate the abnormal returns through time to compute the cumulative abnormal return from period t_1 through t_2, as:

$$CAR_i(t_1, t_2) = \sum_{t=t_1}^{t=t_2} AR_{it} \qquad (2)$$

Although the event-study structure is relatively simple to implement, some statistical issues need to be carefully considered, especially when the event window is long (typically greater than twelve months). Kothari and Warner [1997, 2007] show that long-horizon studies typically lack the ability to detect abnormal performance and are particularly sensitive to the return generating process. However, short-horizon studies like the one we used in this article generally do not suffer from these limitations.

Since our primary focus was to examine the economic effect of enacting security breach notification laws on the documented negative market reaction to security breach announcements, we measured the impact of security breach announcements on firm value in the period prior to June 30, 2006, and again during the period after June 30, 2006. This date was a threshold in enacting breach notification laws; before this point, states were deliberate in enacting such laws, and after it most states rapidly adopted these laws. While it is not possible to identify a single date before which all states or after which all states enacted security breach notification laws, we note that before June 30, 2006, only sixteen states enacted such laws, whereas after that date forty-three states enacted such laws.[10] Thus, it is reasonable to expect that the impact of the enactment of these laws will be substantially reflected on the period after June 30, 2006, with insignificant effect, if any, reflected in the period prior to June 30, 2006. Using this as a cutoff date, we split our breach sample into two roughly equal data sets of about one-hundred incidents, which allowed us to get significant results in the before and after period.

Other possible sources of bias that can impact event-study results include non-synchronous trading, thinly traded securities, and some further liquidity issues related to small capitalization stocks. Fortunately, our sample was made up of mostly large firms that were actively traded on major exchanges. The average market capitalization of firms in our sample as of December 31, 2008, was $31.56 billion and the average beta for firms in the sample was 1.25. Finally, the choice of the appropriate market index was also critical. In our case, we used the CRSP value-weighted market index, which is the most comprehensive characterization of the U.S. equity markets.

V. EMPIRICAL RESULTS

Impact of Security Breaches Over Entire Sample Period

We used Eventus software for the event-study procedure in which we employed information on security breach incidents gathered in our database along with daily price information on each of the impacted firms obtained from

[9] The four factor market model is the premier return generating model used in estimating expected equity returns. The CRSP value-weighted market index is the most comprehensive representation of the U.S. equity markets. Further, the model adjusts for the size effect, the value premium, and the momentum effect, the three market anomalies empirically established in the finance literature.

[10] Henderson [1990] shows that although an event date is uncertain and in many cases may be impossible to identify precisely, the event methodology is still effective when reasonably short windows are considered.

CRSP.[11] The precise date in which the investing public was made aware of the security breach was of utmost importance in event-study analysis. While we have identified over 298 security breach incidents, we were able to identify an exact announcement date and obtain complete information for only 201 of the incidents, which constituted our final sample.

The total number of 201 incidents in our sample occurred over the period from January 2001 through December 2008. In order to study the impact of security breach notification laws on firms, we divided our sample of breach incidents into those that occurred prior to the enactment of the security notification laws and those that occurred after. Specifically, we divided the sample period into breaches that occurred before June 30, 2006, and those that occurred after June 30, 2006. We determined ninety-two breaches occurred between January 1, 2001, and June 30, 2006, and 109 breaches were announced after June 30, 2006, until December 31, 2008.

Before we turned our attention to examining the impact of the security breach notification laws on the two subperiods, we conducted a base case scenario which included all breaches over the entire period. Table 1 presents the average abnormal returns and cumulative abnormal returns for the entire sample of 201 observations estimated using the four factor market model. We estimated the normal model parameters using the 255 days prior to the event period, and then estimated AAR for (–30) days prior to the event and (+30) days after the event. The residuals were tested over a five-day event window prior to the event and two days after the event. It is important to note the increased number of significant negative abnormal residuals in the few days surrounding the event, which generated significant cumulative negative abnormal returns. This indicated the presence of important economic information that was being shown to the market.

In general, we observe a statistically significant negative AAR and CAR around the event date. A Patel Z value greater than 2 indicates that the estimated coefficient is statistically significant at the 5 percent level. The results show that in the three days surrounding the breach event, we found negative and statistically significant abnormal returns. Moreover, the results indicate that there is a negative effect on the returns of these firms on the day of the event and a highly significant negative impact occurring on the day following the breach incident. Our results are consistent with the literature regarding the negative market impact on firm value surrounding announcements of security breach incidents.

The significant cumulative abnormal returns surrounding the event date used in Table 1 show that the market anticipated the security breaches and reacted negatively to that information, as indicated by an average decline in the stock price of these firms. Such a negative reaction is characteristic of bad news. After these reports, investors will be concerned about the extent of the financial damage that might result from the security breach. Once the news of the breach is out, it is vital for firms to alleviate such fears and uncertainty by clearly delineating the extent of the breach and their immediate and long-term response to it.

Figure 1 depicts the behavior of both the AAR and the CAR for the four factor model residuals. There is clear evidence of a significant drop in the cumulative abnormal returns immediately prior to the announcement date. The magnitude of this cumulative decline in the abnormal returns around the announcement of the security breach is shown in Table 1 and Figure 1 to be in the order of 0.7 percent. This decline in the cumulative abnormal returns culminated from the significant negative average abnormal returns in the few days immediately preceding the incident. As expected, the average residuals returned to their normalcy immediately after the incident.[12]

Impact of Security Breaches Prior to Enactment of Notification Laws

After establishing the results for the impact of security breach announcements on the market value of firms for the entire period, we next focused on the period of January 1, 2001–June 30, 2006, which was the period prior to the enactment of state and federal security breach notification laws.[13] Table 2 and Figure 2 present the results for the ninety-two security breach incidents that occurred in that period. Essentially, the results were fairly similar, although more pronounced than the results for the entire period. The decline in the market value of firms during that period is shown in Table 2 and Figure 2 to be in the order of 1 percent of the market value of breached firms, which is higher than the estimated decline in the market value of firms (of 0.7 percent) when the entire period is considered.

[11] Eventus is a product of Cowan Research LC (http://www.eventstudy.com).
[12] It is significant to note that it takes about seven to eight days for the cumulative average residuals to return to the zero mean, suggesting that the full impact of security breach incidents remained for about a week after the event.
[13] While it is true that some states enacted the breach notification laws prior to that date, they were few in number and their impact on the total sample of firms breached across the country during that period is likely to be insignificant.

Table 1: Abnormal Residuals for Security Breach Announcements During Entire Sample Period, 2001-2008

The data show the average abnormal market model residuals and cumulative abnormal residuals for thirty days prior and thirty days after the announcement of a corporate security breach event. The results are for 201 security breaches that were announced during the period 2001 to 2008. Two asterisks indicate that average residuals are significantly different from zero at the 5 percent level.

Day	Average Residual	CAR	Patel Z	Day	Average Residual	CAR	Patel Z
-30	-0.24%	-0.24%	-1.910	1	-0.24%	-0.63%	-2.948**
-29	0.15%	-0.09%	1.247	2	0.11%	-0.52%	0.914
-28	-0.06%	-0.15%	-0.511	3	-0.05%	-0.57%	-0.406
-27	0.06%	-0.09%	0.528	4	0.08%	-0.49%	-0.700
-26	-0.09%	-0.18%	-0.802	5	-0.01%	-0.50%	-0.073
-25	0.05%	-0.13%	0.426	6	-0.03%	-0.53%	-0.296
-24	-0.12%	-0.25%	-1.034	7	0.14%	-0.39%	1.173
-23	0.15%	-0.10%	1.276	8	0.19%	-0.20%	1.463
-22	0.16%	0.06%	1.405	9	0.13%	-0.07%	-1.361
-21	0.08%	0.14%	0.712	10	-0.04%	-0.11%	-0.320
-20	-0.01%	0.13%	-0.049	11	0.08%	-0.03%	0.674
-19	-0.04%	0.09%	-1.031	12	-0.05%	-0.08%	-0.400
-18	-0.02%	0.07%	-0.160	13	0.06%	-0.02%	-0.551
-17	0.07%	0.14%	0.602	14	-0.08%	-0.10%	-0.648
-16	0.01%	0.15%	0.125	15	0.13%	0.03%	1.136
-15	0.00%	0.15%	0.025	16	-0.09%	-0.06%	-1.621
-14	0.07%	0.22%	0.573	17	-0.09%	-0.15%	-0.767
-13	-0.18%	0.04%	-1.903	18	0.05%	-0.10%	0.395
-12	-0.01%	0.03%	-0.114	19	0.13%	0.03%	1.095
-11	-0.14%	-0.11%	-1.163	20	-0.07%	-0.04%	-1.302
-10	0.06%	-0.05%	0.558	21	-0.13%	-0.17%	-1.105
-9	-0.05%	-0.10%	-0.455	22	0.05%	-0.12%	0.991
-8	0.12%	0.02%	1.031	23	0.14%	0.02%	1.237
-7	0.01%	0.03%	0.075	24	0.09%	0.11%	0.790
-6	0.01%	0.04%	0.114	25	-0.06%	0.05%	-0.540
-5	0.12%	0.16%	1.007	26	-0.20%	-0.15%	-1.721
-4	-0.05%	0.11%	-0.401	27	-0.03%	-0.18%	-0.236
-3	-0.05%	0.06%	-0.433	28	-0.06%	-0.24%	-0.550
-2	0.11%	-0.09%	0.970	29	0.08%	-0.16%	0.659
-1	-0.26%	-0.20%	-	30	0.01%	-0.15%	0.057
0	-0.30%	-0.39%	-				

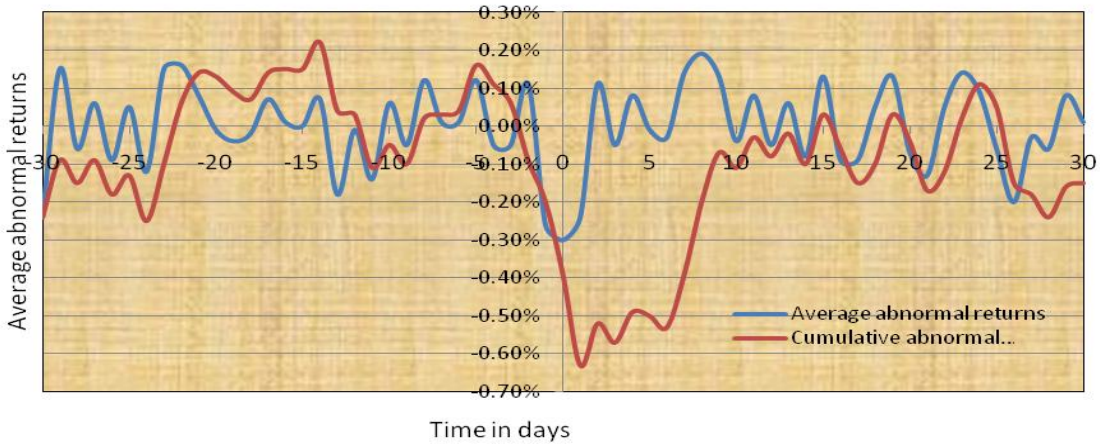

Figure 1. Average and Cumulative Abnormal Returns Around the Security Breach Events Occurring January 1, 2001, to December 31, 2008

Table 2: Abnormal Residuals Prior to Breach Notification Laws (Four Factor Market Model)

The data show the average abnormal four factor market model residuals and cumulative abnormal residuals for thirty days prior and thirty days after the announcement of a corporate security breach event. The results are for ninety-two breaches that occurred during the period from January 1, 2001, to June 30, 2006, prior to enactment of security breach notification laws in most states. Asterisks indicate that the average residual is significantly different from zero at the 5 percent level.

Day	AAR	CAR	Patel Z	Day	AAR	CAR	Patel Z
-30	-0.16%	-0.16%	-1.282	1	0.07%	-0.90%	0.571
-29	0.13%	-0.03%	1.025	2	-0.02%	-0.92%	-0.115
-28	0.01%	-0.02%	0.084	3	0.13%	-0.79%	-0.994
-27	-0.11%	-0.14%	-1.033	4	0.01%	-0.78%	0.057
-26	-0.06%	-0.20%	-1.235	5	0.14%	-0.64%	1.055
-25	-0.12%	-0.32%	-0.886	6	0.30%	-0.34%	-1.776
-24	0.17%	-0.15%	-1.339	7	0.19%	-0.15%	0.728
-23	0.02%	-0.13%	0.144	8	0.19%	0.04%	1.578
-22	0.17%	0.04%	1.342	9	-0.16%	-0.12%	-1.247
-21	-0.10%	-0.06%	-0.751	10	0.14%	0.02%	1.062
-20	0.12%	0.06%	-0.912	11	0.04%	0.06%	0.335
-19	-0.12%	-0.06%	-0.95	12	-0.17%	-0.11%	-1.269
-18	-0.10%	-0.16%	-0.764	13	0.11%	0.00%	0.859
-17	0.04%	-0.12%	0.336	14	0.12%	0.12%	0.932
-16	0.03%	-0.09%	0.195	15	-0.07%	0.05%	-0.533
-15	0.01%	-0.08%	0.056	16	-0.04%	0.01%	-0.332
-14	-0.15%	-0.23%	-1.164	17	0.04%	0.05%	0.297
-13	-0.13%	-0.36%	-1.036	18	-0.04%	0.01%	-0.335
-12	0.15%	-0.21%	1.116	19	-0.09%	-0.08%	-0.728
-11	-0.20%	-0.41%	-1.497	20	-0.15%	-0.23%	-1.149
-10	0.09%	-0.32%	0.721	21	0.18%	-0.05%	-1.388
-9	-0.03%	-0.35%	-0.22	22	0.20%	0.15%	1.513$
-8	0.12%	-0.23%	0.893	23	-0.02%	0.13%	-0.185
-7	0.15%	-0.08%	1.129	24	0.10%	0.23%	0.766
-6	0.06%	-0.02%	0.458	25	-0.02%	0.21%	-0.14
-5	-0.02%	-0.04%	-0.128	26	0.00%	0.21%	-0.037
-4	0.08%	0.04%	-0.612	27	-0.12%	0.09%	-1.655
-3	-0.14%	-0.10%	0.269	28	0.17%	0.26%	1.317
-2	-0.35%	-0.45%	-4.067***	29	0.06%	0.32%	0.475
-1	-0.40%	-0.85%	-3.071**	30	-0.10%	0.22%	-0.73
0	-0.12%	-0.97%	-0.155				

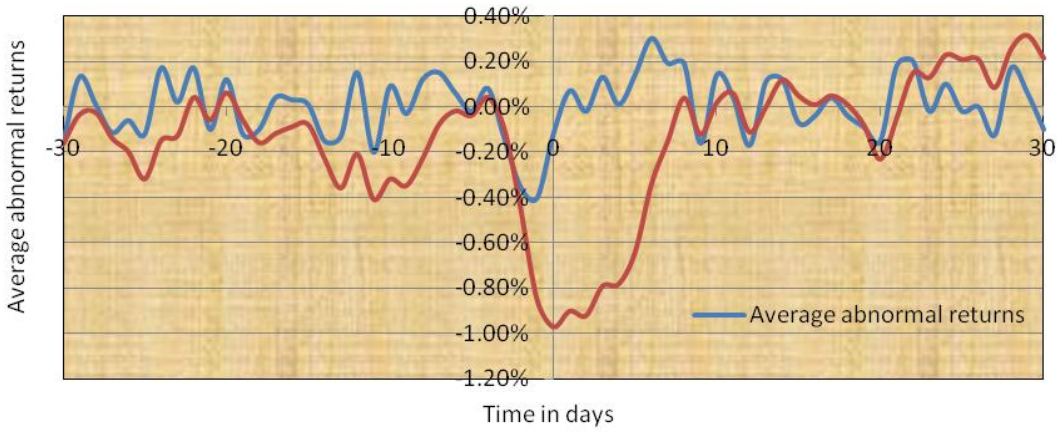

Figure 2. Average and Cumulative Abnormal Returns Around Security Breach Events for the Period Prior to Enactment of Enforcement Laws, January 1, 2001, to June 30, 2006

Impact of Security Breaches After Enactment of Notification Laws

We repeated the same procedure used in estimating the impact of security breach announcements for the security breaches that occurred after June 30, 2006, marking the enactment of the security breach notification laws. There were 109 breaches during the period from June 30, 2006, through December 31, 2008, which was the period after the enactment of the notification laws. It is interesting to note that the number of breach announcements that occurred in the past three years was more than the breach announcements that occurred in the prior seven years.

Table 3 and Figure 3 report the event-study results using the four factor market model to estimate the abnormal residuals. The results for this latter sample period appeared to be markedly different. While we still observed a statistically significant decline in the CAR on the event date (day 0), the overall market reaction was measurably reduced relative to what was documented in the earlier period. More specifically, during this time period in which we expected to observe the full impact of the enactment of the security breach notification laws, we found from Table 3 that the estimated decline in the market value of firms following an announcement of a security breach was only in the order of 0.5 percent of its market value.[14]

Table 3: Abnormal Residuals after Breach Notification Laws (Four Factor Market Model)

The data show the average abnormal four factor market model residuals and cumulative abnormal residuals for thirty days prior and thirty days after the announcement of a corporate security breach event. The results are for 109 breaches that occurred during the period from June 30, 2006, to December 31, 2008, after the enactment of security breach notification laws in most states. Asterisks indicate that the average residual is significantly different from zero at the 5 percent level.

Day	AAR	CAR	Patel Z	Day	AAR	CAR	Patel Z
-30	-0.14%	-0.14%	-1.592	1	0.13%	-0.41%	-1.572
-29	0.15%	0.01%	0.826	2	0.21%	-0.20%	1.114
-28	-0.12%	-0.11%	-0.634	3	0.12%	-0.08%	0.119
-27	0.23%	0.12%	1.211	4	0.12%	0.04%	-0.834
-26	-0.04%	0.08%	-0.193	5	-0.13%	-0.09%	-0.702
-25	0.19%	0.27%	1.008	6	0.09%	0.00%	0.996
-24	-0.07%	0.20%	-0.398	7	-0.01%	-0.01%	0.915
-23	0.01%	0.21%	1.376	8	0.14%	0.13%	1.893
-22	-0.15%	0.06%	0.821	9	-0.08%	0.04%	-1.513
-21	-0.12%	-0.06%	1.255	10	-0.19%	-0.15%	-0.99
-20	-0.09%	-0.15%	0.48	11	0.11%	-0.04%	0.575
-19	-0.11%	-0.26%	-1.767	12	0.05%	0.01%	0.287
-18	0.05%	-0.21%	0.265	13	-0.16%	-0.15%	-1.135
-17	0.09%	-0.12%	0.492	14	-0.02%	-0.17%	-1.297
-16	0.01%	-0.11%	0.029	15	0.01%	-0.16%	1.62
-15	-0.12%	-0.23%	-0.004	16	0.03%	-0.13%	-1.666
-14	0.15%	-0.08%	1.339	17	0.01%	-0.11%	-1.058
-13	-0.16%	-0.24%	-1.638	18	0.12%	0.01%	0.652
-12	0.15%	-0.09%	-0.785	19	0.22%	0.23%	1.69
-11	-0.08%	-0.17%	-0.453	20	-0.14%	0.09%	-1.965
-10	0.04%	-0.13%	0.215	21	-0.08%	0.01%	-0.448
-9	0.07%	-0.06%	-0.391	22	0.20%	0.21%	1.546
-8	0.12%	0.06%	0.655	23	-0.20%	0.01%	1.531
-7	-0.11%	-0.05%	-0.577	24	-0.09%	-0.08%	0.453
-6	-0.08%	-0.13%	-0.138	25	0.10%	0.02%	-0.54
-5	0.19%	0.06%	1.227	26	-0.07%	-0.05%	-1.472
-4	-0.02%	0.04%	-0.1	27	0.16%	0.11%	0.846
-3	-0.01%	0.03%	-0.654	28	-0.17%	-0.06%	-1.433
-2	-0.12%	-0.10%	-0.775	29	0.09%	0.03%	0.477
-1	-0.10%	-0.20%	-2.125*	30	0.09%	0.12%	0.506
0	-0.34%	-0.54%	-2.885**				

[14] A t-test of differences in means with unequal variance indicated that the difference between the decline in the market value of firms after June 30, 2006 (0.5 percent), and the decline in the market value of firms before June 30, 2006 (1 percent), is statistically significant at the 5 percent level.

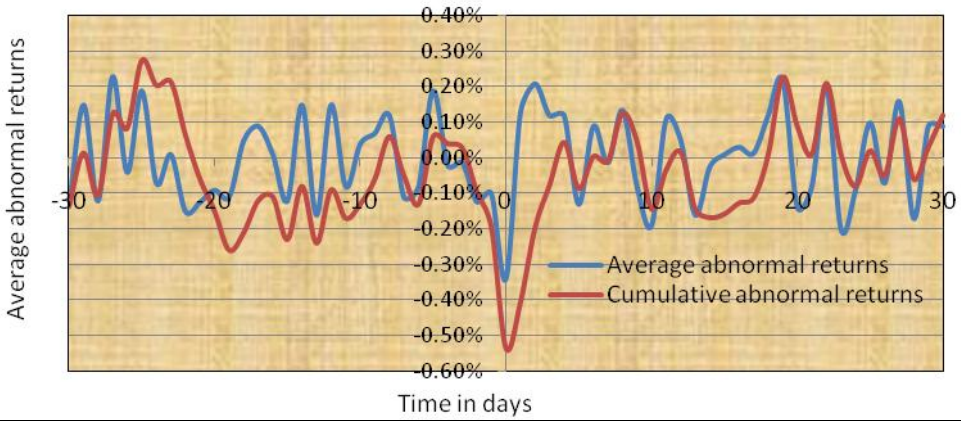

Figure 3. Average and Cumulative Abnormal Returns Around Security Breach Events for the Period After the Enactment of Enforcement Laws, June 30, 2006, to December 31, 2008

To put these results in the proper perspective, we should point out that our results for the overall period regarding the negative impact on firm value due to breach announcements is already lower than the average decline in market value of firms documented in earlier studies. Since some of these earlier studies used similar methodologies, it is reasonable to argue that our results for the overall period are also somewhat muted since they incorporate many of the breaches that occurred in the later period when security breach legislation was already enacted. Consequently, our findings that the negative impact of security breach announcements on the market value of firms has been reduced by the enactment of security notification laws corroborates earlier evidence and is consistent with our main contention.

VI. SUMMARY AND CONCLUSIONS

The intended purpose for enacting the security breach state notification legislation is to encourage both public and private organizations to implement better security measures in order to protect consumer information. Security breach notification laws impose a reputational cost on firms by mandating a public disclosure of security breaches. The economic effects of these notification laws have not been examined in the literature. Using event-study methodology, this article measures the effectiveness of these laws by estimating the impact of security breach incidents on firm value during the periods before and after the enactment of security breach notification laws.

Using a sample of over 200 breaches over the period 2001–2008, we found a statistically significant negative CAR in the order of 0.7 percent of firm value around the event date. The results showed negative and statistically significant abnormal returns in the three days surrounding the breach event. These findings corroborated other empirical evidence regarding the negative market impact on firm value surrounding announcements of security breach incidents. Moreover, such findings demonstrated the presence of significant economic incentives for firms to implement information security procedures.

In order to examine the economic impact of the security breach notification laws that were enacted in the latter part of 2006, we divided our sample of breach incidents into those that occurred prior to the enactment of these laws and those that occurred after. We found that the estimated decline in market value of firms due to security breach announcements was larger during the period prior to the enactment of the security breach notification laws than during the entire sample period. The decline in the market value of breached firms during the period prior to the enactment of notification laws was in the order of 1 percent, which was higher than the estimated decline in the market value of firms (of 0.7 percent) throughout the entire period.

For the period after the enactment of the notification laws, the results appeared to be significantly different. While we still observed a statistically significant decline in the CAR on the event date (day 0), the overall market reaction was measurably reduced relative to what was documented for the earlier period. In fact, the estimated decline in the market value of firms following an announcement of a security breach after the enactment of security breach notification laws was in the order of 0.5 percent of its market value, almost half the impact observed prior to the enactment of these security notification laws.

The reduced negative impact of security breach announcements on the market value of firms after the enactment of security notification laws provided some evidence in favor of the federal and state security breach notification legislation. Since the intended objective for enacting the state notification legislation was to encourage firms to implement better security measures, our findings of reduced negative impact on firm value was generally consistent

with the intended purpose of the legislation. It is also possible to conjecture that firms may have invested more resources in reducing the impact, if not the incidence, of security breaches.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Acquisti, A., A. Friedmann and R. Telang (2006, June 26–28) "Is There a Cost to Privacy Breaches? An Event Study", presentation at 27th International Conference on Information Systems (ICIS) 2006 / 5th Workshop on the Economics of Information Security (WEIS) 2006, Cambridge, England, http://weis2006.econinfosec.org/docs/40.pdf (current Oct. 18, 2012).

Artnak, K.E. and M. Benson (2005) "Evaluating HIPAA Compliance: A Guide for Researchers, Privacy Boards, and IRBs", *Nursing Outlook,* (53)2, pp. 79–87.

Ball, R. and P. Brown (1968) "An Empirical Evaluation of Accounting Income Numbers", *Journal of Accounting Research*, (6)2, pp. 159–178.

Bartel, A.P. and L.G. Thomas (1985) "Direct and Indirect Effects of Regulation: A New Look at OSHA's Impact", *Journal of Economics and Law,* (28)1, pp. 1–25.

Bhagat, S. and R. Romano (2002a) "Event Studies and the Law: Part I: Technique and Corporate Litigation", *American Law and Economics Review,* (4)1, pp. 141–168.

Bhagat, S. and R. Romano (2002b) "Event Studies and the Law: Part II: Empirical Studies of Corporate Law", *American Law and Economics Review,* (4)2, pp. 380–423.

Bin, F-S, M. Puclik and F. He (2009) "The Impact of Online Gaming Legislation Developments on Corporate Financial Performance: A Further Investigation", *International Research Journal of Finance and Economics*, (27)1, pp. 168–179.

Bingisser, G.M. (2008) "Data Privacy and Breach Reporting: Compliance with Varying State Laws", *Shidler J. L. Com. and Tech,* http://www.lctjournal.washington.edu/Vol4/a09Bingisser.html (current Oct. 18, 2012).

Braganza, A. and K.C. Desouza (2006) "Implementing Section 404 of the Sarbanes-Oxley Act: Recommendations for Information Systems Organizations", *Communications of the Association for Information Systems*, (18) Article 22, pp. 464–487.

Broder, I.E. and J.F. Morrell III (1991) "Incentives for Firms to Provide Safety: Regulatory Authority and Capital Market Reactions", *Journal of Regulatory Economics,* (3)4, pp. 309–322.

Brown, L.D. and M.L. Caylor (2006) "Corporate Governance and Firm Valuation", *Journal of Accounting and Public Policy,* (25)4, pp. 409–434.

Brown, S. and G.B. Warner (1980) "Measuring Security Price Performance", *Journal of Financial Economics*, (8)3, pp. 205–258.

Brown, S. and G.B. Warner (1985) "Using Daily Stock Returns: The Case of Event Studies", *Journal of Financial Economics*, (14)1, pp. 3–31.

Campbell, K., L.A. Gordon, M. Loeb and L. Zhou (2003) "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", *Journal of Computer Security*, (11)3, pp. 431–448.

Carhart, M. (1997) "On Persistence in Mutual Fund Performance", *Journal of Finance*, (52)1, pp. 57–92.

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, pp. 69–105.

Chai, S., M. Kim and H.R. Rao (2011) “Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior”, *Decision Support Systems*, (50)4, pp. 651–661.

Chhaochharia, V. and Y. Grinstein (2007) “Corporate Governance and Firm Value: The Impact of the 2002 Governance Rules”, *The Journal of Finance*, (62)4, pp. 1789–1825.

Durnev, A. and E.H. Kim (2005) “To Steal or Not to Steal: Firm Attributes, Legal Environment, and Valuation”, *Journal of Financ*e, (60)3, pp. 1461–1493.

Fama, E. (1970) “Efficient Capital Markets: A Review of Theory and Empirical Work”, *Journal of Finance*, (25)2, pp. 383–417.

Fama, E. and K. French (1993) “Common Risk Factors in the Returns on Stocks and Bonds”, *Journal of Financial Economics*, (33)1, pp. 3–56.

Fama, E., S. Fisher, M. Jensen and R. Roll (1969) “The Adjustment of Stock Prices to New Information”, *International Economic Review*, (10)1, pp. 1–21.

Faulkner, B. (2007) “Hacking into Data Breach Notification Laws”, *Florida Law Review,* (59)5, pp. 1097–1125.

Gilligan, T.W. and K. Krehbiel (1988) “Complex Rules and Congressional Outcomes: An Event Study of Energy Tax Legislation”, *The Journal of Politics,* (50)3, pp. 625–654.

Goel, S. and H.A. Shawky (2009) “Estimating the Impact of Security Breach Announcements on Firm Values”, *Information and Management,* (46)7, pp. 404–411.

Gordon, L., M. Loeb and L. Zhou (2011) “The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?”, *Journal of Computer Security*, (19)1, pp. 33–56.

Gupta, M., R. Sharman and H.R. Rao (2010, December) “Timing of Corporate Crisis Response to Security Breaches: Impact on Market Valuation”, *Workshop on Information Systems Security (WISP),* St. Louis, Missouri, USA.

Henderson, G.V., Jr. (1990) “Problems and Solutions in Conducting Event Studies”, *Journal of Risk and Insurance,* (57)2, pp. 282–306.

Hovav, A. and J. D'Arcy (2004) “The Impact of Virus Attack Announcements on the Market Value of Firms”, *Information Systems Security*, (13)3, pp. 32–40.

Hovav, A. and J. D’Arcy (2005) “Capital Market Reaction to Defective IT Products: The Case of Computer Viruses”, *Computers and Security*, (24)5, pp. 409–424.

Kannan, K., J. Rees and S. Sridhar (2007) “Market Reactions to Security Breach Announcements: An Empirical Analysis”, *International Journal of E-Commerce*, (12)1, pp. 69–91.

Kothari, S.P. and J.B. Warner (1997) “Measuring Long-Horizon Security Price Performance,” *Journal of Financial Economics,* (43)3, pp. 301–339.

Kothari, S.P. and J.B. Werner (2007) “Econometrics of Event Studies” in Eckbo, B.E. (ed.) *Handbook of Corporate Finance: Empirical Corporate Finance*, New York, NY: North-Holland, pp. 3–36.

Li, H., M. Pincus and S.O. Rego (2008) “Market Reaction to Events Surrounding the Sarbanes-Oxley Act of 2002 and Earnings Management”, *Journal of Law and Economics,* (51)1, pp. 111–134.

Litvak, K. (2007) “The Effect of the Sarbanes-Oxley Act on Non-US Companies Cross-Listed in the US”, *Journal of Corporate Finance*, (13)2–3, pp. 195–228.

MacKinlay, A.C. (1997) "Event Studies in Economics and Finance*", Journal of Economic Literature*, (35) March, pp. 13–39.

Malkiel, B.G. (2003) “The Efficient Market Hypothesis and Its Critics”, *Journal of Economic Perspectives,* (17)1, pp. 59–82.

McWilliams, A. and D. Siegel (1997) “Event Studies in Management Research: Theoretical and Empirical Issues”, *Academy of Management Journal*, (40)3, pp. 626–657.

McWilliams, A., D. Siegel and S.H. Teoh (1999) “Issues in the Use of the Event Study Methodology: A Critical Analysis of Corporate Social Responsibility Studies”, *Organizational Research Methods*, (2)4, pp. 340–365.

Parameswaran, S., S. Venkateshan, M. Gupta, R. Sharman and H.R. Rao (2011, Aug. 4-7) “Impact of Cloud Computing Announcements on Firm Valuation” proceedings of the 17th Americas Conference on Information

Systems (AMCIS), Detroit, MI, http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1320&context=amcis2011_submissions (current Oct. 18, 2012).

Picanso, K.E. (2006-7) "Protecting Information Security Under a Uniform Data Breach Notification Law", *Fordham Law Review*, (75)1, pp. 355–390.

Rezaee, Z. and P.K. Jain (2005) "The Sarbanes-Oxley Act of 2002 and Security Market Behavior: Early Evidence", *SSRN,* doi:10.2139/ssrn.498083 (current Oct. 18, 2012).

Swartz, N. (2003) "The Cost of Sarbanes-Oxley", *Information Management Journal*, (37)5, pp. 8–26.

Telang, R. and S. Wattal (2007) "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price", *IEEE Transactions on Software Engineering*, (33)8, pp. 544–557.

Weidenbaum, M. and R. DeFina (1978) *The Cost of Federal Regulation of Economic Activity,* Washington, DC: American Enterprise Institute.

Zhang, I.X. (2007) "Economic Consequences of the Sarbanes-Oxley Act of 2002", *Journal of Accounting and Economics,* (44)1–2, pp. 74–115.

APPENDIX A: EFFECTIVE ADOPTION DATES OF SECURITY BREACH NOTIFICATION LAWS BY STATE

Table A–1: Effective Adoption Dates of Security Breach Notification Laws by State

State	Effective Date	State	Effective Date
California	7/1/2003	Nebraska	7/14/2006
Arkansas	3/31/2005	Colorado	9/1/2006
Georgia	5/5/2005	Arizona	12/31/2006
North Dakota	6/1/2005	Hawaii	1/1/2007
Delaware	6/28/2005	New Hampshire	1/1/2007
Florida	7/1/2005	Utah	1/1/2007
Tennessee	7/1/2005	Vermont	1/1/2007
Washington	7/24/2005	Washington, DC	3/8/2007
Nevada	10/1/2005	Michigan	6/29/2007
North Carolina	12/1/2005	Wyoming	7/1/2007
New York	12/7/2005	Oregon	10/1/2007
Connecticut	1/1/2006	Massachusetts	10/31/2007
Illinois	1/1/2006	Maryland	1/1/2008
Louisiana	1/1/2006	West Virginia	6/8/2008
Minnesota	1/1/2006	Iowa	7/1/2008
New Jersey	1/1/2006	Virginia	7/1/2008
Maine	1/31/2006	Texas	4/1/2009
Ohio	2/17/2006	Alaska	7/1/2009
Montana	3/1/2006	South Carolina	7/1/2009
Rhode Island	3/1/2006	Missouri	8/28/2009
Wisconsin	3/31/2006	Mississippi	7/1/2011
Oklahoma	6/8/2006		
Pennsylvania	6/20/2006	Alabama	N/A
Idaho	7/1/2006	Kentucky	N/A
Indiana	7/1/2006	New Mexico	N/A
Kansas	7/1/2006	South Dakota	N/A

ABOUT THE AUTHORS

Sanjay Goel is an Associate Professor and Chair of the Information Technology Management Department in the School of Business, and the Director of Research at the NYS Center for Information Forensics and Assurance at UAlbany. He represents UAlbany in the Capital Region Cyber Crime Partnership. Dr. Goel received his PhD in Mechanical Engineering from RPI. His research includes information security, risk analysis, security policies, music piracy, cyber warfare and self-organization in complex systems. His latest research on self-organizing systems includes traffic light coordination, nano-bio computing and social networks. He and his team have worked with CSCIC in developing the information classification policy for New York. He is currently leading an effort launched by IEEE Communications Society and the IEEE Standards Association to create a vision for the Smart Grid future fifteen years ahead. He has over fifty articles in refereed journals and conference publications including top journals such as the *California Management Review*, *IEEE Journal of Selected Areas in Communication*, *Decision Support Systems*, and the *Information & Management Journal*.

Hany A. Shawky is Professor Finance and Economics and is Associate Dean of the School of at the University at Albany, State University of New York. He received his PhD degree in finance from the Ohio State University. He is the founder of the Center for Institutional Investment Management at the University at Albany and served as its director from September 2002 through December 2007. Hany specializes in investment management and portfolio performance evaluation and is widely published in academic and applied journals on issues dealing with asset pricing, stock market behavior, international financial markets and electricity markets. He has published over fifty refereed scholarly articles in finance and economics journals, and was the recipient of the School of Business Research Award in 1996, 2001 and 2004. He teaches investments and corporate finance and has regularly participated in executive training programs for bankers and corporate executives. He serves on a number of advisory boards and is a director on the board of trustees of small cap equity mutual fund. He has served as a consultant to many private and public organizations. Hany was recently listed among the “Most Prolific Authors in the Finance Literature: 1959-2008” with a percentile ranking in the top 2 percent of finance faculty worldwide (Heck and Cooley, 2009). He ranked 550 among the 17,601 finance faculty who has published at least one article in the top twenty-six core finance journals.

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems