The economic cost of publicly announced information security breaches: empirical evidence from the stock market [*]

Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou

Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland, College Park, MD 20742, USA

This study examines the economic effect of information security breaches reported in newspapers on publicly traded US corporations. We find limited evidence of an overall negative stock market reaction to public announcements of information security breaches. However, further investigation reveals that the nature of the breach affects this result. We find a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. Thus, stock market participants appear to discriminate across types of breaches when assessing their economic impact on affected firms. These findings are consistent with the argument that the economic consequences of information security breaches vary according to the nature of the underlying assets affected by the breach.

1. Introduction

Information security is concerned with protecting the confidentiality, integrity and accessibility of information [29]. Since even the best efforts cannot prevent all security breaches, information security breaches are ubiquitous. The 2002 Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI), reports that 90% of respondents detected computer security breaches within the past year [32]. Discussions concerning corporate information security breaches, however, provide conflicting views about the economic impact of such breaches. Some press reports and survey results suggest that firms experience significant financial losses as a result of information security breaches (e.g., [24,32]). Others, however, suggest that security systems effectively prevent breaches with severe economic consequences, and the breaches that do occur are nuisances with inconsequential economic effects on firms (e.g., [1,42]).

The above claims notwithstanding, the economic implications of corporate information security breaches remain an empirical issue. Our study examines the stock

[*] The study reported in this paper was partially supported by the DOD, Laboratory for Telecommunications Sciences, through a contract with the University of Maryland Institute for Advanced Computer Studies (UMIACS). Preliminary results of some data analyses reported in this paper were included in a working paper by Gordon et al. [21] and presented at the LTS May 2001 workshop.

0926-227X/03/$8.00 © 2003 – IOS Press. All rights reserved

market reaction to newspaper reports of information security breaches at publicly traded US corporations during the period January 1, 1995 to December 31, 2000. Our overall findings provide some limited support for a negative stock market reaction to these widely reported information security breaches. However, upon further investigation, we find that the nature of the breach affects this result. We find a highly significant negative market reaction to information security breaches involving unauthorized access to confidential data, but no significant market reaction when the breach does not involve access to confidential data. Thus, market participants discriminate across types of breaches in assessing the economic consequences of these events.

The remainder of our paper proceeds as follows. In the next section we review the relevant literature and develop our research hypotheses. The third section of the paper describes our research methodology including the sample selection process. We report the results of our empirical analysis in the fourth section of the paper. The fifth, and final, section of the paper provides concluding comments and some avenues for future research.

2. Hypothesis development

Corporate information security breaches take many forms including denial of service attacks, computer viruses, unauthorized access to private information such as customer lists and credit card data, and a variety of other attacks.[1] In contrast to the vast amount of literature on the technical and behavioral aspects of information security, the literature concerned with the economics of information security is rather small. Recent conceptual/theoretical studies by Anderson [2] and Gordon and Loeb [20] provide insights into the economics of information security, but do not investigate the actual magnitude of losses associated with information security breaches. Empirical research that examines the economic impact of corporate information security breaches is largely descriptive in nature, and has focused on the direct financial cost of information security breaches. This descriptive research is comprised largely of survey results compiled and analyzed by professional organizations (e.g., [16,25,32]). However, the quantity and quality of survey data on the cost of information security breaches is limited, since many firms are unwilling or unable to quantify their losses. Furthermore, it is unlikely that this approach could capture the full economic impact of information security breaches (especially in regard to indirect costs related to effects on the value of IT investments and other assets). Two recent reports published by the University of Michigan, the “Incident Cost Analysis and Modeling Project” and the “Incident Cost Analysis and Modeling

[1] The focus in this study is on security breaches that relate to the formal computer-based information systems rather than those that relate to breakdowns in the informal communication systems within an organization. Although beyond the scope of this paper, a much broader view would consider the contextual factors related to the entire information processing activities within an organization. Examination of this broader view of information security breaches would require in-depth case studies of individual organizations, as conducted by Dhillon [14].

Project I-CAMP II", however, attempt to address these indirect costs in their study of selected IT-related incidents at universities. The authors of the I-CAMP reports specifically incorporate estimates of user-side costs [33,34]. Of course, the problem in assessing the economic impact of information security breaches does not diminish the importance of such an assessment.

The prevalence of corporate information security breaches is well documented, as noted in the above-cited survey results. But, evidence on the frequency of information security breaches is not limited to survey results. Indeed, the popular press reports information security breaches. Press reports have described breaches at a broad spectrum of firms including both "new economy" firms (e.g., Amazon.com, Buy.com, and eBay) [47] and older well-established firms such as Ford and Estee Lauder [6]. The press has reported information security breaches even at icons of the information age such as Microsoft, Inc. For example, on January 26, 2001 *The Wall Street Journal* reported that:

> Microsoft Corp. blamed a malicious hacker for a second day of embarrassing failures involving its major Web services . . . For nearly five hours yesterday, the failures prevented millions of customers from sending e-mail, downloading software patches or searching online technical manuals. They also deprived Microsoft of revenue from online advertisements on some of its Web pages [8].

The combination of survey results and popular press reports leaves little doubt that information security breaches are commonplace among corporations. What is unclear, however, is the economic impact of these breaches. Competing arguments are often made regarding this question. One argument posits that the economic consequences of these breaches are highly consequential. This argument is intuitively appealing, as there is a variety of potential costs associated with information security breaches. These potential costs include: (1) lost business (both immediate and long term as a consequence of negative reputation effects), (2) activities associated with detecting and correcting the breaches, and (3) potential legal liability. There is also a substantial amount of anecdotal evidence and self-reported survey data that suggests substantial economic costs are associated with information security breaches. For example, on February 10, 2000 *The Wall Street Journal* reported that a denial of service attack against Yahoo!, "brought Yahoo!'s Web site to its knees, costing it an estimated $ 500 000 in a scant three hours" [24]. As reported in *CIO*, The Yankee Group estimated the total losses related to the February 2000 denial of service attacks were $ 1.2 billion [18]. The 2002 CSI/FBI Survey disclosed that 80% of respondents acknowledged financial losses related to computer crimes, although only 44% were willing and able to quantify these losses. For those firms reporting their losses, the aggregate financial loss in 2001 was close to $ 456 million [32]. Coverage of information security breaches by major newspapers in itself, suggests that they have substantial economic consequences and may result in reputation costs for the affected firms.

An alternative argument, however, suggests that the economic consequences of information security breaches are trivial over the long run. The intuition underlying this argument is that firms protect their most valuable information assets (e.g., secret formulas for key products, valuable customer data) at a higher level than their less valuable information. That is, since all information cannot be protected to the point where there is zero probability of a security breach, firms may allocate their security expenditures in a manner that minimizes the economic impact of security breaches [19]. Accordingly, there is reason to believe that most information security breaches that actually occur may have a small (or insignificant) economic impact on the value of a firm. Some popular press reports are consistent with the insignificant economic impact argument. One example is a *Wall Street Journal* article discussing the implications of the "love bug" virus, where the author argues:

> According to the headlines, an e-mail attachment called the "love bug" took the electronic world to the brink of destruction last Thursday . . . But for such an allegedly fierce creation, it was sure odd how the ILOVEYOU crisis was over in about 12 hours . . . My colleague, Rob Rosenberger, a computer-virus expert who has assisted in securing e-mail for both the Air Force and corporate America over the past decade, has watched this play out over and over . . . Mr. Rosenberger also rightly considers computer viruses little more than time-consuming nuisances . . . There's no evidence they noticeably hurt the private pocket or the economy . . . [42].

Additional anecdotal evidence consistent with the insignificant economic impact argument includes consequences of a series of hacker attacks resulting in shutdowns at companies such as Yahoo! and Amazon.com in February 2000. On the day of the attack Yahoo! was shut down for almost 3 hours, and its Web traffic dropped 11% relative to the same day the week before the breach. However, by the next day, the number of unique visitors to the site was back to normal, and up 9% from the same day the prior week. The trends were similar for other companies hit by this denial of service attack [48]. When asked about the economic impact of this attack on eBay, the firm's CEO, Meg Whitman, responded:

> Minimal. If people weren't able to list items during the time that our site was unavailable, they probably listed them soon afterward. Even if you make extreme assumptions that none of those deferred listings ever got made, the maximum we could be talking about is $ 50 000 of lost revenue to eBay [1].

When asked about the impact on eBay's reputation Whitman stated:

> Probably neutral. Most of our users were very supportive of us, and very angry at whoever did this [1].

The above statements are consistent with the argument that at least some varieties of information security breaches are viewed as a normal cost of business. For firms that are heavy users of information technologies, costs associated with the breaches that occur may be analogous to inventory shrinkage costs for a retailer. Certainly some efforts are taken to contain these types of costs, but by and large they are viewed as a cost of doing business. The cost of eliminating these events/losses altogether may exceed the benefits.[2] Data reported in the 2002 CSI/FBI survey are

[2] On a conceptual level, it is well known that expenditures on information security activities should not exceed the benefits from such activities (e.g., see [29] and [2]).

consistent with this view [32]. The average reported financial loss arising from computer security breaches in 2002 was $ 204 416, an immaterial amount relative to the asset base and annual net income of major US corporations.

Thus, there is anecdotal and self-reported survey evidence consistent with each of two competing arguments regarding the economic impact of information security breaches. One posits that information security breaches have a highly significant negative economic impact on firms. The other posits that most of these events have minimal economic consequences for firms. A third argument can also be made that information security breaches may have a net positive long-term economic impact on firms. This third argument is based on the premise that firms respond to breaches by making new investments in information security [7]. Thus, an information security breach may signal imminent, and previously unanticipated, investments in information security. These investments might have long-term economic benefits that exceed the cost of the breach that spurred the investment. If this were true, the expected net economic consequences of both the breach itself and the anticipated future benefits of information security investments signaled by the breach would have to be considered. It is possible that the net economic effect would be positive.

In order to investigate the competing arguments concerning the economic impact of information security breaches using a rigorous empirical analysis, one needs to identify both a sample of information security breaches and a measure of the economic impact of the breaches. In this study we use major newspaper reports to identify a sample of information security breach announcements and measure the economic impact of the reported incidents using a stock-market performance-based approach. We conduct an "event study" to assess the stock market reaction to publicly announced information security breaches.[3] If a reported information security breach were expected to have a negative (positive) effect on the firm's expected future cashflows, then the market reaction should be negative (positive). Alternatively, if the market views a particular breach as having negligible economic effects on the firm, there should be no market reaction. Since these are credible alternative hypotheses, we do not make a directional prediction and structure our analysis as an investigation of a null hypothesis stated as follows:

H1$_o$: There is no stock market reaction to public reports of corporate information security breaches.

Our discussion of security breaches leading up to the above null hypothesis has not considered the nature of the breach. Nevertheless, it seems reasonable to expect the market to react differently to various types of breaches. Indeed, while all information security breaches are potentially costly, those that involve access to confidential

[3] Bharadwaj and Keil [4] also use a stock market approach, but their study do not provide much guidance in determining the economic impact of information security breaches. They investigate the economic impact of IT failures using a sample that includes a broad set of events that include operational failures, implementation problems with new systems, system shutdowns, and some information security breaches. Their hypotheses and research design do not distinguish between information security breaches and the other types of IT failures included in their sample. Thus, the economic impact of information security breaches *per se* cannot be gleaned from their study.

firm and/or customer data may be the most costly. That is, customers, stockholders, and other stakeholders would likely be willing to accept some types of information security breaches (e.g., denial of service) as a routine risk and a normal cost of doing business. This would be consistent with the above quotations referring to the love bug virus and other denial of service attacks. These stakeholders, however, may be much more concerned when confidential information (e.g., credit card and other personal information) could be exposed to outsiders.

The underlying strategic asset affected by breaches involving unauthorized access to confidential information is quite different than that affected by attacks that do not involve access to confidential information. Once confidential information has been accessed, the value of such a strategic asset may be permanently compromised. For example, a firm's customer list may be an important proprietary asset. Once this list has been accessed without authorization, others may be able to use the list for marketing and other purposes. The firm that had invested in developing the customer list no longer has exclusive use of the list. This may permanently impair the list's value to the firm that created and owned it. In the case of breaches that do not involve unauthorized access to confidential information, the underlying assets generally relate to operations. While the firm may lose the ability to use these assets for some period of time, the loss is usually temporary. Consider the case of a denial of service attack. During the attack, the firm may not be able to conduct operations, take customer orders, etc. Once the attack ends and any necessary system changes are made, however, the firm can commence operations and the value of its operating systems is not permanently impaired.

This argument is consistent with the findings from the 2002 CSI/FBI Survey, which suggests that among information security breaches, the most serious financial losses were related to theft of proprietary information [32]. Thus, we investigate the stock market reaction to information security breaches involving unauthorized access to confidential information in contrast with other types of breaches by testing the following null hypotheses:

$H2_A$: There is no stock market reaction to public reports of corporate information security breaches involving unauthorized access to confidential information.

$H2_B$: There is no stock market reaction to public reports of corporate information security breaches that do not involve unauthorized access to confidential information.

3. Methodology

3.1. Sample selection

We identified information security breaches by electronically searching the full text of the *Wall Street Journal*, *New York Times*, *Washington Post*, *Financial Times*, and *USA Today* for the terms: “information security breach”, “computer system security”, “hacker”, “cyber attack”, “computer attack”, “computer break-in”, and “computer virus”. We chose these five newspapers for selecting our sample because we wanted to develop a sample that would allow a powerful test for a stock market reaction to security breaches. Breaches reported in these major newspapers are likely to be significant events at major corporations. Additionally, because they are highly visible media outlets, the investing community is likely to regularly follow reports in these newspapers. Thus, if there is a stock market reaction to information security breaches, this is the sample of events for which we are most likely to find it.

Of course, unless there is some publicly observable consequence such as shutdown of a Web site or litigation, the press may not become aware of a breach. Thus, some breaches with the most potentially severe economic consequences (such as employee initiated breaches that may compromise proprietary information) may not be reported in a timely fashion. In fact, our sample includes only two breaches that appear to involve insiders of the affected firms.[4] Thus, our sample of information security breaches largely represents external versus internal threats. Accordingly, our sample is likely not representative of the population of information security breaches. Nevertheless, the events in our sample do represent the publicly disclosed information security breaches, and as such, are the only information security breach events to which the stock market could respond.

Our search for information security breaches covers the period January 1995 through December 2000. We did not search periods prior to 1995 since the incidence of reported information security breaches is related to development of the Internet [32]. After reviewing the articles to identify those describing a firm-specific information security breach, an initial set of 84 events was identified.[5] Additional sample selection criteria are the availability of sufficient returns history (i.e., a minimum public trading history) on the Center for Research in Security Prices (CRSP) database for the estimation period necessary for our event study, continuity in the corporate entity’s identity over the period, and elimination of multiple events where estimation periods overlap earlier events for the same firm.[6] After imposing all sample selection criteria, our final sample consists of 43 events affecting 38 firms. Table 1 summarizes our sample selection procedure and Table 2 lists the events included in our sample along with a brief description of the reported security breach. Both new (e.g., Microsoft) and old economy (e.g., Ford) firms are included in our sample. Panel A of Table 3 provides descriptive statistics for sample firms measured at 1999. Panel B of Table 3 reports the industry distribution for our sample. While the 38 firms have 13 different two-digit primary SIC codes, there is evidence of some industry clustering, since 14 are business services firms (SIC 7300).

[4] The two sample events involving insiders are those affecting Raytheon and McGraw-Hill. As a sensitivity test, we conducted our tests excluding these two observations. Results after excluding these events are consistent with those reported for the full sample.

[5] When an information security breach event is reported by more than one newspaper, we include the earliest report in our sample.

[6] When the estimation period overlaps a prior event for the same firm, we include the earlier events.

Table 1

Sample selection criteria

Criterion	Impact on sample size	Firms remaining
Initial set of Corporate information security breaches reported in major newspapers	84	84
CRSP data availability	(28)	56
Merger	(2)	54
Sufficient returns data for estimation period computations	(4)	50
Overlapping Multiple information security breaches	(7)	43

In order to investigate implications of the nature of information security breaches, we partition our sample of events based on access to confidential information. Events that involve unauthorized access to confidential firm or customer data are classified as "confidential" events (e.g., access to customer credit card data, access to pricing or other firm proprietary information, etc.). Those that do not primarily involve access to confidential information are classified as "non-confidential" (e.g., denial of service attacks, website alteration, etc.). Our classification of events is annotated in Table 2.

3.2. Research design

We approach the question of the economic impact of information security breaches by examining the stock market reaction to major newspaper announcements of breaches at specific firms. Thus, we use an event study methodology where the event is the public announcement of an information security breach. In essence, our "event study" assesses investors' expectations regarding the long-term impact of publicly announced information security breaches, because a firm's market value of equity reflects the present value of its expected future cash flows. Thus, by using stock market returns as the basis of our proxy for economic impact, we are able to capture both direct and indirect costs of the information security breaches. This is an advantage since the indirect costs are difficult to quantify and are often ignored or, out of necessity, only crudely estimated in other research approaches. The stock market-based approach, however, does limit the analysis to publicly disclosed events.

We use two methodological approaches to conduct our event study. First, we use a standard market model-based event study methodology that has been widely used in the accounting and finance literature (e.g., [9]). This method is commonly used in the financial economics literature and has been used to examine the stock market reaction to public announcements related to information systems issues (e.g., [15] and [46]). The standard methodology uses Ordinary Least Squares (OLS) to estimate regression parameters. OLS assumes that the error terms from regressions are independent and identically distributed, have a mean of zero and are homoskedastic.

Table 2

Sample information security breach events

Company name	Source	Date	Confidentiality of event	Event description
Egghead.com	Washington Post	12/23/00	Confidential	Unauthorized access to credit card data
Disney	USA Today	09/27/00	Confidential	Unauthorized access to Disney World guest data
First Data Corp. (Western Union)	Wall Street Journal	09/11/00	Confidential	Unauthorized access to credit card data
Sabre Holdings Corp.	Wall Street Journal	06/27/00	Confidential	Unauthorized access to proprietary data
Nike Inc.	Wall Street Journal	06/22/00	Non-confidential	Unauthorized traffic re-direction
Ford Motor Co.	Wall Street Journal	05/05/00	Non-confidential	Love bug virus
Microsoft Corp.	Wall Street Journal	05/05/00	Non-confidential	Love bug virus
Estee Lauder Cos	Wall Street Journal	05/05/00	Non-confidential	Love bug virus
Bear Stearns Cos	USA Today	05/05/00	Non-confidential	Love bug virus
Trans World Airlines Inc.	USA Today	05/05/00	Non-confidential	Love bug virus
National Discount Brokers	Wall Street Journal	02/25/00	Non-confidential	Service interruption
McGraw-Hill Cos	Wall Street Journal	02/22/00	Confidential	Unauthorized access to confidential info facilitated by employee
Aastrom Biosciences Inc.	Wall Street Journal	02/18/00	Non-confidential	Unauthorized website entry & alteration
ZDNet	Wall Street Journal	02/10/00	Non-confidential	Denial of service attack
About.com	Wall Street Journal	02/10/00	Non-confidential	Denial of service attack
Time Warner Inc (CNN)	Washington Post	02/09/00	Non-confidential	Denial of service attack
Amazon.com Inc.	Wall Street Journal	02/09/00	Non-confidential	Denial of service attack
eBay Inc.	USA Today	02/08/00	Non-confidential	Denial of service attack
Lycos	Financial Times	02/08/00	Non-confidential	Denial of service attack
E-Trade Group	USA Today	02/08/00	Non-confidential	Denial of service attack
Yahoo!	Wall Street Journal	02/08/00	Non-confidential	Denial of service attack
Drug Emporium Inc.	Wall Street Journal	01/31/00	Confidential	Unauthorized access to credit card data
America Online	Wall Street Journal	01/27/00	Non-confidential	Flow in email system
Northwest Airline	Wall Street Journal	01/10/00	Confidential	Unauthorized access to credit card data
Dell Computer Corp.	Financial Times	11/19/99	Non-confidential	Production interruption by virus
Critical Path Inc.	Wall Street Journal	09/22/99	Non-confidential	Flow in email system
Symantec Corp.	Wall Street Journal	08/09/99	Non-confidential	Unauthorized website entry & alteration
Network Solutions Inc.	Washington Post	07/03/99	Non-confidential	Unauthorized website entry & traffic re-direction
AT&T Corp.	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
Lehman Brothers Holdings Inc.	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
Boeing Co.	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
General Electric Co.	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
Raytheon Co.	Wall Street Journal	04/05/99	Confidential	Unauthorized employee posting of confidential information
Merrill Lynch & Co. Inc.	USA Today	03/30/99	Non-confidential	Melissa virus
Intel Corp.	USA Today	03/30/99	Non-confidential	Melissa virus
Compaq Computer Corp.	USA Today	03/30/99	Non-confidential	Melissa virus
Lockheed Martin Corp.	USA Today	03/30/99	Non-confidential	Melissa virus
Microsoft Corp.	Wall Street Journal	10/27/98	Confidential	Unauthorized access to subscriber data
America Online	Wall Street Journal	10/19/98	Non-confidential	Unauthorized alteration of services address
New York Times Co.	Wall Street Journal	09/14/98	Non-confidential	Unauthorized website entry & alteration
America Online	Wall Street Journal	01/05/98	Confidential	Unauthorized access to passwords/credit card data
America Online	Washington Post	06/28/97	Confidential	Unauthorized access to users' accounts
Microsoft Corp.	Wall Street Journal	06/23/97	Non-confidential	Unauthorized service interruptions

Table 3

Descriptive statistics

Panel A: financial variables at FYE 1999

Variable	No. obs.	Mean	Median	Minimum	Maximum	Std. dev.
Total Assets ($mill.)	38	49 884.82	4 668.25	9.54	405 200.00	97 959.27
Book Value ($mill.)	38	8 670.74	1 570.07	−171.03	78 927.00	15 644.46
Sales ($mill.)	38	18 676.64	4 384.50	0.88	162 558.00	32 907.26
Net Income/Loss ($mill.)	38	1 379.02	393.00	−719.97	10 717.00	2 581.81
Market Value of Equity ($mill.)	38	64 468.57	8 775.77	13.28	602 432.92	131 966.17
Market to Book	38	12.81	5.96	−36.14	97.43	24.65

Panel B: sample industry distribution

SIC	Industry description	Number of firms
2700	Printing, Publishing & Allied	2
2800	Chemicals & Allied Prods	2
3000	Rubber & Misc. Plastic Prods	1
3500	Ind, Comm Mch, Computer Equip	1
3600	Electrical, Other Elec Equip	2
3700	Transportation Equipment	3
3800	Meas Instr, Photo Gds, Watches	1
4500	Transportation By Air	2
4800	Communications	1
5900	Misc. Retailers	1
6200	Security & Commodity Brokers	5
7300	Business Services	14
7800	Motion Pictures	3
	Total	38

However, there is some clustering of events in our sample (i.e., several firms were affected by virus or denial of service attacks from the same source on the same day), as well as some industry clustering. In addition, there is no reason to believe, on a priori grounds, that information security breaches have a similar effect on all firms. These concerns would violate the assumptions of OLS in that the regression residuals may suffer from contemporaneous cross-sectional correlation and/or heteroskedasticity. Thus, we also use a second, more rigorous, approach that takes into consideration the possible violation of some of the OLS assumptions. This method is a seemingly unrelated regression (SUR) approach.

3.2.1. *Standard OLS methodology*

To estimate the effect of the public disclosure of an information security breach, we first estimate what the firm's stock return would have been in the absence of the event. To do this, we assume that daily stock returns are consistent with the capital asset pricing model (CAPM), and estimate the market model for each firm over a 120-day estimation period.[7] The market model we estimate is specified as follows:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}, \tag{1}$$

where: R_{it} = return for firm i's stock on day t, net of the risk-free rate; R_{mt} = return for the market on day t, net of the risk-free rate; α_i, β_i = market model intercept and slope parameters, respectively, for firm i; and ε_{it} = disturbance term.

We use an estimation period that starts 121 days before the security breach announcement, and ends 2 days before that event date. We use the equally weighted NYSE/AMEX/NASDAQ market index return as our proxy for R_{mt}. This market index choice reflects the broad set of firms encompassed by our sample. Using the firm-specific parameters estimated for the market model over the estimation period, we are then able to compute abnormal returns for event days as follows:

$$AR_{it} = R_{it} - \left(\hat{\alpha}_i + \hat{\beta}_i R_{mt}\right). \tag{2}$$

The abnormal returns, *AR*, represent the extent to which realized returns on the event day deviate from the returns that would be expected based on the estimated firm-specific market model parameters. In this sense, the abnormal returns can be thought of as prediction errors.

In this study we use a three-day event window centered on the date of the newspaper report of the information security breach. The three-day window captures the market reaction on the announcement date as well as any that may occur on the previous or subsequent day. Although most of the information security breach events are short-term in nature, in the context of our study, it is important to include the two days around the announcement date. Including the day before the newspaper announcement captures any market reaction due to information leakage and allows for the case where an event such as a denial of service attack might begin before markets close, and although commonly known, might not be reported in a published newspaper until the next day. Including the day following the announcement date captures the market reaction to announcements made after the stock market closes on the announcement date.[8] We compute the cumulated abnormal returns (*CAR*) over the event window as follows:

$$\mathit{CAR}_i = \sum_{t=t_1}^{t_2} AR_{it}, \tag{3}$$

where: $[t_1, t_2]$ = the event interval; and all other terms as previously defined.

[7] A variety of estimation period lengths have been used in prior studies. The shortest of the commonly accepted estimation periods is 120 days. We chose this period in order to retain the most observations in our sample. Both Subramani and Walden [45] and Bharadwaj and Keil [4] used a 120-day estimation period.

[8] Given that newspaper articles are the sources of our announcements, the three-day window seems appropriate. Extending the window would increase the likelihood of confounding events. Nevertheless, results from a preliminary analysis with a seven-day window are consistent with those reported.

For our sample of 43 events, we compute the mean announcement effect as follows:

$$CAR = \frac{1}{N}\sum_{i=1}^{N} CAR_i, \tag{4}$$

where: $N =$ the number of events; and all other terms as previously defined.

Under the null hypothesis of no market reaction to the announcement of information security breaches, expected abnormal returns over the event window are zero. In testing our H1, we use a Z-statistic to assess the statistical significance of the abnormal returns over the event interval. In order to test our hypotheses regarding differential market reaction to information security breaches involving confidential information ($\mathrm{H2_A}$ and $\mathrm{H2_B}$), we examine abnormal returns over the event window for the two sub-samples of events partitioned based on confidentiality of information.

3.2.2. SUR methodology

As discussed above, because the sample included clustering of some events in our study (e.g., some viruses and denial of service attacks affected multiple firms) and industry clustering, as well as the fact there is no reason to assume that security breaches affect all firms in a similar manner, some OLS assumptions implicit in the standard methodology may not hold. Thus, as a sensitivity analysis to address these issues, we also use a seemingly unrelated regressions (SUR) model. The SUR methodology addresses the possibility of both contemporaneous correlation and heteroskedasticity of error terms across events. SUR models, which are a form of Generalized Least Squares (GLS) models, have been used for event studies in both the economics [5,36,41] and accounting literatures [22,39].

The SUR model used in our analysis is:

$$\begin{aligned}
&R_{1t} = \alpha_1 + \beta_1 R_{mt} + \gamma_1 D + e_{1t},\\
&R_{2t} = \alpha_2 + \beta_2 R_{mt} + \gamma_2 D + e_{2t},\\
&.\\
&.\\
&.\\
&R_{Nt} = \alpha_N + \beta_N R_{mt} + \gamma_N D + e_{Nt},
\end{aligned}$$

where: $D = 1$ if within the 3 day event period $[-1, +1]$, and 0 otherwise; R and R_{mt} as previously defined.

This specification allows us to operationalize tests of H1 and H2 two ways: first, as a joint hypothesis (i.e., whether all coefficients equal zero) and second, as an average hypothesis (i.e., whether the average coefficient equals zero). If stock market reactions have much variation in sign, the joint hypothesis test should be more powerful. If, however, the reaction to most events is in the same directions, the average hypothesis test may be more powerful [22]. A Theil's F statistic is used to test these hypotheses.

4. Results

Panel A of Table 4 presents the results of our test of H1 using the standard event study methodology. The mean CAR is -0.02, but is statistically insignificant ($p = 0.1393$) at conventional levels. While the p-value approaches marginal significance, we are not able to reject the H1 null hypothesis of no stock market reaction to reports of information security breaches. This result is inconsistent with the arguments that information security breaches adversely impact the future economic performance of affected firms.

The clustering in our sample may affect the validity of some OLS assumptions. Thus, we check the robustness of our result by using a SUR methodology. Results of this analysis using the full sample are presented in Panel A of Table 5. We reject the null joint hypothesis that all coefficients are equal to zero ($p = 0.0226$), but cannot reject the null average hypothesis that the average coefficient equals zero. The difference in the significance of the joint hypothesis results versus the average hypothesis results is consistent with observed variation in the signs of the stock market reactions across our sample events. Across the three-day event period, the CAR over the event period is negative for 47% of events (from Table 4). Due to the mixed signs of the stock market reaction to the events in our sample, the joint hypothesis test is more powerful than the average test. Thus, unlike the CAR results, the SUR results provide support for rejecting the null of no stock market reaction to our sample of information security breaches.

Although we find some support consistent with a negative stock market reaction to reported information security breaches, the findings are sensitive to the methodology used. Furthermore, the observed variation in the signs of the stock market reaction to the events is consistent with the competing arguments regarding the economic impact of such breaches. That is, there appear to be highly mixed reactions to the security breaches included in our study. In order to investigate further the impact of the nature of events that may affect stock market reaction, we partition our sample of events based on confidentiality. Panel B of Table 4 reports results of our test of $H2_A$ and $H2_B$. We find that 11 (i.e., 26%) of the sample events involve access of confidential information. For confidential (non-confidential) events, the CARs are negative in

Table 4

CAR results 3 day window $[-1, +1]$

	N	Mean CAR	Z-stat	p-value	% negative CARs
Panel A (full sample)					
Full Sample	43	-0.0188	-1.4783	0.1393	46.52
Panel B (sample partitions)					
Confidential Events	11	-0.0546	-2.7830	0.0053	63.64
Non-Confidential Events	32	-0.0065	-0.4142	0.6787	40.63.

Table 5

SUR results joint and average tests of H1

	Jt. Hypothesis (all coeff = 0)	Avg. Hypothesis (avg. coeff = 0)
Panel A (full sample)		
F-value	1.48	1.51
$Pr > F$	0.0226	0.2192
D.F.	43	1
	5160	5160
Panel B (confidential event sub-sample)		
F-value	3.68	12.40
$Pr > F$	0.0001	0.0004
D.F.	11	1
	5160	5160
Panel C (non-confidential event sub-sample)		
F-value	0.34	0.03
$Pr > F$	0.9998	0.8744
D.F.	32	1
	5160	5160

64% (41%) of cases. The mean CAR is significantly negative ($p = 0.0053$) for confidential events and insignificant for non-confidential events. Thus, for confidential events, we reject the null hypothesis $H2_A$, but we are unable to reject the null hypothesis $H2_B$ with respect to the non-confidential events. These results suggest that the confidential events drive the full-sample results presented in Panel A of Table 4.

Results using the SUR methodology to investigate market reactions to confidential and non-confidential event sub-samples are presented in Panels B and C of Table 5. For confidential events, we are able to reject both the null average hypothesis ($p = 0.0004$) and the null joint hypothesis ($p = 0.0001$). We can reject neither null hypothesis for the non-confidential sub-sample. Thus, these results are generally consistent with those reported for the CAR analysis where the mean CAR was significantly negative for the confidential sub-sample but insignificant for the non-confidential events.

5. Concluding comments

By using a stock market return framework to examine the economic implications of information security breaches, our study contributes to the literature examining the economic effects of information security breaches. We find some evidence of an overall negative stock market reaction to announcements of information security breaches in major newspapers, although this finding is not robust across all specifications. Nevertheless, these results provide some support for the argument that information security breaches adversely affect the future economic performance of affected firms.

When we partition the sample based on whether the breach involved access to confidential information, however, the results are more compelling. We find that all types of information security breaches are not viewed as having similar economic impacts. We do not find a significant market reaction when we examine security breaches that are not related to confidentiality. In contrast, we find a highly significant negative reaction for those breaches that relate to violations of confidentiality. Thus, it appears that stock market participants are discriminating when assessing the impact of information security breaches. Unlike breaches in our non-confidential sub-sample that largely affected the information infrastructure itself, breaches in our sample of confidential events involved unauthorized access to an underlying information asset (such as customer databases) in addition to the information technology infrastructure. Our results are consistent with the intuition that since information security protects a variety of firm assets, the economic consequence of a breach in security depends on the nature and value of the underlying assets compromised by the breach.

Some types of breaches, such as the denial of service attacks and other incidents included in our non-confidential sample, do not seem to be viewed as having a material impact on the firm's future economic performance. In this latter regard, it is interesting to note that many of the non-confidential events (i.e., love bug virus attacks) may have received more press coverage and affected more parties than the confidential events. Nevertheless, breadth of press coverage alone does not appear to drive the stock market's reaction (i.e., even highly publicized breaches may have little material economic implications for firms). This finding is consistent with the mixed results in the IT investment literature that, taken together, suggest stock market participants are discriminating when assessing the value of IT investments.

Our study extends the literature on the costs of information security breaches by introducing an empirical economics-based approach. Our findings are consistent with the logic underlying the argument that information security managers allocate investments in information security activities based on the potential economic benefits to be derived from such expenditures (i.e., stock market reactions seem to view differing types of information security breaches as having different consequences). Most security managers likely have realized that some types of information security breaches are both inevitable and acceptable as a normal on-going operating cost of the modern information environment.

Our study shares some limitations common to all event studies. First, our hypotheses and tests relate to the sign of stock market reaction, without making predictions about the absolute size of the reaction (although the statistical tests do consider the significance of such reactions). Second, the event methodology captures only the stock market's initial reaction to the event. Future revisions in beliefs related to the events under study may occur, but these are not easily observable and/or testable using this methodology. Finally, results of event studies may be sensitive to confounding events, clustering of events, and researcher decisions regarding event windows, estimation periods, and sample selection. We believe that our use of the SUR model adequately addresses some of these econometric concerns, but we are not able to address all of the inherent limitations of event studies.

The other major potential limitations of our study relate to our sample. Our sample represents only publicly disclosed information security breaches. Since firms have little or no incentive to publicly disclose information security breaches, and many (if not most) of these incidents cannot be externally observed, many information security breaches may not be reported in the media. Thus, our sample is probably not representative of the overall population of information security breaches. The nature of information security breaches that are reported in the press may be quite different than those that are not reported. The dominance of external threat events in our sample is consistent with this supposition. Thus, our results are likely not generalizable to information security breaches that are not publicly disclosed. Additionally, while our sample size is large enough to conduct statistical analysis, it is small in absolute terms. Given the frequency of information security breaches, it is interesting to note the limited number of firm-specific disclosures regarding information security breaches that appear in the major newspapers. We purposely chose the five high visibility outlets because we wanted to enhance the power of our tests in detecting stock market reactions to publicly announced security breaches. Even here, however, we found that breaches that did not involve unauthorized access to confidential information had no significant effect on the market value of the firms. Thus, it seems clear from our study that the market does not treat all breaches alike.

References

[1] G. Anders, eBay's CEO reacts to hacker attack, seeks joint action on Web security, *The Wall Street Journal* (February 10), B18 (2000).

[2] R. Anderson, Why information security is hard – an economic perspective, in: *Proceeding of 17th Annual Computer Security Applications Conference (ACSAC)*, New Orleans, Louisiana, 2001.

[3] A. Bharadwaj, S.G. Bharadwaj and B.R. Konsynski, Information technology effects on firm performance as measured by Tobin's q, *Management Science* **45**(6) (1999), 1008–1024.

[4] A. Bharadwaj and M. Keil, The effects of Information technology failures on the market value of firms: an empirical examination, Working paper, Emory University, 2001.

[5] J.J. Binder, Measuring the effects of regulation with stock price data, *Rand Journal of Economics* **16**(2) (1985), 167–183.

[6] T. Bridis, Virus gives 'love' a bad name – poisonous message's potential to destroy files prompted vast e-mail shutdown, *The Wall Street Journal* (May 5), B1 (2000).

[7] T. Bridis, E-Business: Microsoft takes steps to thwart hacker attacks, *The Wall Street Journal* (January 29), B4 (2001).

[8] T. Bridis and R. Buckman, Microsoft lays 2nd-day woes on hackers, *The Wall Street Journal* (January 26), A3 (2001).

[9] S.J. Brown and J.B. Warner, Measuring security price performance, *Journal of Financial Economics* **8**(3) (1980), 205–258.

[10] D. Chatterjee, V.J. Richardson and R.W. Zmud, Examining the shareholder wealth effects of announcements of newly created CIO positions, *MIS Quarterly* **25**(1) (2001), 43–70.

[11] T.E. Daniels and E.H. Spafford, Identification of host audit data to detect attacks on low-level IP vulnerabilities, *Journal of Computer Security* **7**(1) (1999), 3–36.

[12] D. Denning, An intrusion-detection model, *IEEE Transactions on Software Engineering* **SE-13**(2) (1987), 222–232.

[13] D. Denning and D. Branstad, A taxonomy for key escrow encryption systems, *Communications of the ACM* **39**(3) (1996), 34–40.

[14] G. Dhillon, *Managing Information System Security*, Macmillan Press LTD, London, 1997.

[15] B.L. Dos Santos, K. Peffers and D.C. Mauer, The impact of information technology investment announcements on the market value of the firm, *Information Systems Research* **4**(1) (1993), 1–23.

[16] Ernst and Young, Ernst and Young Information Security 2001, www.ey.com (2001).

[17] D. Frincke, Balancing cooperation and risk in intrusion detection, *ACM Transactions on Information and System Security* **3**(1) (2000), 1–29.

[18] A. Genusa, Conspiracy of silence, *CIO* **14**(10) (2001), 92–96.

[19] L.A. Gordon and M.P. Loeb, A framework for using information security as a response to competitor analysis systems, *Communications of the ACM* **44**(9) (2001), 70–75.

[20] L.A. Gordon and M.P. Loeb, The economics of information security investment, *ACM Transactions on Information and System Security* **5**(4) (2002), 438–457.

[21] L.A. Gordon, M.P. Loeb and L. Zhou, Stock market effects of information security, Working Paper, University of Maryland, 2001.

[22] L.A. Gordon and K.J. Silvester, Stock market reactions to activity-based costing adoptions, *Journal of Accounting and Public Policy* **18**(3) (1999), 229–251.

[23] L.M. Hitt and E. Brynjolfsson, Productivity, business profitability, and consumer surplus: Three different measures of information technology value, *MIS Quarterly* **20**(2) (1996), 121–142.

[24] P. Kedrosky, Hackers prey on our insecurities, *The Wall Street Journal* (February 10), A18 (2000).

[25] KPMG, KPMG Information Security Survey 2000, www.kpmg.co.uk (2000).

[26] K.D. Loch, H.H. Carr and M.E. Warkentin, Threats to information systems: todays reality, yesterday's understanding, *MIS Quarterly* **16**(2) (1992), 173–186.

[27] J. McHugh, Intrusion and intrusion detection, *International Journal of Information Security* **1**(11) (2001), 14–35.

[28] K. Muralidhar, D. Batra and P. Kirs, Accessibility, security, and accuracy in statistical databases: the case for the multiplicative fixed data perturbation approach, *Management Science* **41**(9) (1995), 1549–1564.

[29] NIST (National Institute of Technical Standards), An introduction to computer security: the NIST handbook, Special Publication 800-12, 1995.

[30] S. Osborn, R. Sandhu and Q. Munawer, Configuring role-based access control to enforce mandatory and discretionary access control policies, *ACM Transactions on Information and System Security* **3**(2) (2000), 85–106.

[31] M. Peyravian, A. Roginsky and N. Zunic, Hash-based encryption system, *Computers & Security* **18**(4) (1999), 345–350.

[32] R. Power, CSI/FBI 2002 Computer Crime and Security Survey, *Computer Security Issues and Trends* **18**(2) (2002), 7–30.

[33] Regents of the University of Michigan, Incident cost analysis and modeling project: A report from the CIC Security Working Group to the CIC chief information officers, 1998.

[34] Regents of the University of Michigan, Incident cost analysis and modeling project: I-CAMP II: A report to the USENIX association, 2000.

[35] V.J. Richardson and R.W. Zmud, Wealth effects accompanying appointments of outside directors to the boards of Internet companies, Working Paper, University of Kansas, 2000.

[36] N.L. Rose, The incidence of regulatory rents in the motor carrier industry, *Rand Journal of Economics* **16**(3) (1985), 299–318.

[37] R. Sandhu, V. Bhamidipati and Q. Munawer, The ARBAC97 model for role-based administration of roles, *ACM Transactions on Information and System Security* **2**(1) (1999), 105–135.

[38] B. Schneier, *Applied Cryptography*, 2nd ed., Wiley, New York, NY, 1996.

[39] K. Schipper and R. Thompson, The impact of merger-related regulations on the shareholders of acquiring firms, *Journal of Accounting Research* **21**(1) (1983), 184–221.

[40] G. Simmons, Cryptanalysis and protocol failures, *Communications of the ACM* **37**(11) (1994), 56–65.

[41] M. Smirlock and H. Kaufold, Bank foreign lending, mandatory disclosure rules, and the reaction of bank stock prices to the Mexican debt crisis, *Journal of Business* **60**(3) (1987), 347–364.

[42] G. Smith, ‘Love Bug’ victims don’t want a cure, *The Wall Street Journal* (May 8), A42 (2000).

[43] D.W. Straub, Effective IS security: an empirical study, *Information Systems Research* **1**(3) (1990), 255–276.

[44] D.W. Straub and R.J. Welke, Coping with systems risk: security planning models for management decision making, *MIS Quarterly* **22**(4) (1998), 441–469.

[45] M. Subramani and E. Walden, The impact of e-commerce announcements on the market value of firms, *Information Systems Research* **12**(2) (2001), 135–154.

[46] K.Y. Tam, The impact of information technology investments on firm performance and evaluation: Evidence from newly industrialized economies, *Information Systems Research* **9**(1) (1998), 85–98.

[47] K.T.L. Tran and R.L. Rundle, Hackers attack major Internet sites, cutting off Amazon, Buy.com, eBay, *The Wall Street Journal* (February 9), A3 (2000).

[48] *The Wall Street Journal*, Data show Web sites swiftly bounced back from hacker attacks (February 17), B8 (2000).

[49] P. Weill, The relationship between investment in information technology and firm performance: a study of the valve manufacturing sector, *Information Systems Research* **3**(4) (1992), 307–333.

Copyright © 2003 EBSCO Publishing