The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers

Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan

ABSTRACT: Assessing the value of information technology (IT) security is challenging because of the difficulty of measuring the cost of security breaches. An event-study analysis, using market valuations, was used to assess the impact of security breaches on the market value of breached firms. The information-transfer effect of security breaches (i.e., their effect on the market value of firms that develop security technology) was also studied. The results show that announcing an Internet security breach is negatively associated with the market value of the announcing firm. The breached firms in the sample lost, on average, 2.1 percent of their market value within two days of the announcement—an average loss in market capitalization of $1.65 billion per breach. Firm type, firm size, and the year the breach occurred help explain the cross-sectional variations in abnormal returns produced by security breaches. The effects of security breaches are not restricted to the breached firms. The market value of security developers is positively associated with the disclosure of security breaches by other firms. The security developers in the sample realized an average abnormal return of 1.36 percent during the two-day period after the announcement—an average gain of $1.06 billion in two days. The study suggests that the cost of poor security is very high for investors.

KEY WORDS AND PHRASES: Capital markets, event study, information technology security, information technology security management, Internet security, security breach announcements.

The number of companies that conduct business over the Internet is steadily increasing, but the massive growth of e-business has not been an unmitigated boon. The Internet provides great advantages to firms, facilitating the exchange of vast amounts of information, goods, and services that can increase efficiency and thus customer awareness and loyalty, but these advantages can also turn into threats: Customers may be delighted to flip through dozens of virtual sales racks and make immediate on-line purchases, but they certainly do not want unauthorized parties to appropriate their credit card numbers and other personal data, or interfere with their ability to access the Web site in the first place. This problem is a very serious one for many companies. A recent survey by CSI-FBI found that the Internet was the point of attack in 74

An earlier version of this paper was presented at WISE 2002 (Workshop on Information Systems and Economics), Barcelona, and AAA-IS 2003 (American Accounting Association–Information Systems), San Diego. The authors thank the workshop participants as well as Hal Varian, Rajiv Banker, Ross Anderson, Radha Mahapatra, Hasan Cavusoglu, and seminar participants at the University of Texas at Dallas for encouraging them to pursue this study and for their comments on earlier drafts of the paper.

International Journal of Electronic Commerce / Fall 2004, Vol. 9, No. 1, pp. 69–104.

1086-4415/2004 $9.50 + 0.00.

percent of hacking incidents in 2002, a rise from 38 percent in 1996 [61]. According to the Computer Emergency Response Team (CERT) Coordination Center, the number of Internet attacks on business has almost doubled every year since 1997 [16]. Not surprisingly, companies that do e-business are seeking ways to exploit the interconnectivity of networks, encouraging and even improving "open access," but still maintain a security firewall.

Public awareness of security breaches increased dramatically when high-profile Internet companies like Amazon, eBay, and Yahoo were hit by denial-of-service (DOS) attacks in February 2000. Software developers are cognizant of the need for secure products. In 2002, Microsoft took the unprecedented step of ceasing development of new Windows operating system software for an entire month and sending the company's 7,000 systems programmers to a special security training program [49]. In a memo addressing the incident, the company's president, Bill Gates, announced that security is now "more important than any other part of our work. If we don't do this, people simply won't be willing—or able—to take advantage of all the great work we do. When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box" [15]. Gates's memo did not estimate the cost of security breaches to Microsoft, but it shows that a major software developer values features related to security in its products.

Even as firms have come to recognize the importance of security, assessing its economic value has proved to be challenging. Traditionally, organizations have regarded security as a kind of insurance policy that mitigates consequences rather than prevents them. According to Ron Knode, Computer Sciences Corporation's global director of managed security services, "While most IS professionals recognize the benefits of protecting and securing data, the business leadership in the organization still sees security as a 'nice to have' rather than 'need to have.' It is not until something goes wrong before perceptions change. The fact is, it costs far less to establish the right security measures at the outset than it does to recover from a breach in security" [25]. His words proved true—three months later—when the February 2000 DOS attack struck several firms.

The true cost of a security breach is manifold. Security lapses can lead to the loss of consumer confidence and trust, over and above the lost business and exposure to third-party liability. In a recent survey by Media Metrix, only 12.1 percent of U.S. companies with a Web presence cited direct financial loss as a concern in security breaches, but more than 40 percent cited consumer trust and confidence [58]. Although it may be impossible to directly quantify the costs associated with the breaching of consumer trust and confidence, an indirect estimate is possible on the basis of the capital market valuations of firms.

The present research has the following specific objectives:

1. To quantify the costs associated with IT security breaches using market valuation data.
2. To explain the factors that affect the cross-sectional variations related to breach costs.
3. To document the information-transfer effect of security breaches on security developers' market valuations.

The research in this paper is related to two previous studies of IT failures and capital markets. Ettredge and Richardson investigated the stock market reaction to the February 2000 DOS attacks and found that Internet firms suffered market reactions more severely than did traditional firms [30]. Theirs was the first study to measure the effects of security breaches on capital markets. Bharadwaj and Keil, who studied the impact of announcements of IT failures, including DOS attacks on capital markets, found a significant drop in the market value of firms that experienced such failures [10]. The present research, like the work of the aforementioned authors, employs the event-study method, but as far as is known, it is the first large-scale examination of the effect of security breaches on capital markets. It differs from these two earlier works in the following respects. First, unlike Ettredge and Richardson, it does not restrict the analysis to DOS attacks, but considers security breaches of all types. This makes it possible to investigate the differential effects of DOS as compared with other types of attack. Although the February 2000 incident is a landmark in the IT security domain because of the wide scope and publicity of the attack, the paper analyzes the impact of security breaches in 1996–2001 and does not isolate the February 2000 incident. Next, whereas Bharadwaj and Keil study security breaches among several other types of IT failure (they also consider DOS attacks only), the present paper focuses exclusively on security breaches. For the purposes of the study, a security breach is defined as a malicious attempt to interfere with a company's business and its information. Thus, the study does not consider accidental events and glitches that may affect the firm. In what is, perhaps, its most important departure from the aforementioned two studies, the present analysis is not limited to one segment of the market but also looks at certain repercussions of an attack beyond the breached companies. The effects of security breaches on breached firms are analyzed and so are the information-transfer effects produced by the breaches on security technology firms. The present paper is the first study in the information systems (IS) literature to investigate information-transfer effects.[1]

The research found that announcements of Internet security breaches were negatively associated with the market value of the announcing firms. The breached firms, on average, lost 2.1 percent of their market value within two days of the announcement. This translated into a $1.65 billion average loss in market capitalization per breach based on the mean market value of the firms in the data set. The research also found that

1. Breach cost is higher for "pure play," or Internet-only, firms than for conventional firms.
2. Breach cost increased during the study period.
3. Security breaches are costlier for smaller firms than larger firms.
4. Breach cost is not significantly different across breach types.

The effects of security breaches were not restricted to the breached firms, however. The market value of security technology firms was positively associated with the disclosure of a security breach. The security firms in the sample realized, on average, an abnormal return of 1.36 percent within two days after the announcement. This produced, on average, a total gain for security firms of $1.06 billion in a two-day period.

	Transitory	Long-term
Tangible	*Low*	*High*
Intangible	*High*	*Very high*

Table 1. Degree of Uncertainty in Estimation of Costs.

Theory and Hypotheses Development

In order to derive hypotheses, the study identified the different types of costs associated with security breaches and their relationship to firm value under the efficient market hypothesis.

Cost of Security Breaches

The costs of security breaches can be broadly classified as transitory (or short-term) costs, incurred only during the period in which the breach occurs, and permanent (or long-term) costs, incurred over several periods.

The transitory costs of security breaches include lost business and decreased productivity resulting from the unavailability of the breached resources; labor and material costs required to detect, contain, repair, and reconstitute breached resources; costs associated with evidence collection and prosecution of the attacker; costs related to providing information to customers and the public; and other media-related costs [26].

Permanent, or long-term, costs have more far-reaching effects on the breached firm's future cash flow. These costs are related to the loss of customers who switch to competitors, inability to attract new customers due to perceived poor security, loss of trust of customers and business partners, legal liabilities arising from the breach, and the cost of attackers' access to confidential or proprietary information. Perceptions of increased business risk may also translate into increased insurance costs for the firm and higher capital costs in debt and equity markets.

The costs incurred as a result of breaches can be further classified as tangible or intangible. It is possible to estimate the cost of lost sales, material and labor, and insurance, but costs related to trust are difficult to calculate. Nonetheless, these intangibles are extremely important in the measurement of the overall cost of security for business. Table 1 blocks out the four types of costs and the degree of uncertainty associated with dollar estimates of each type. The magnitude of the four types of costs is likely to vary based on the breach type and business type.

Investors' Beliefs and Firm Values Under an Efficient Market Hypothesis

The study constructed a model for valuating firms based on the efficient market hypothesis and investors' belief revision. Consider a firm whose value at a

time period t is denoted by V_t. Assuming that the firm will liquidate at the terminal period T, the value of the firm can be expressed as the discounted value of expected future cash flows at time t conditioned on all the information available to the market until time t.[2] Thus,

$$V_t = E_t\left(\sum_{i=t}^{T}\frac{c_i\,|\vec{\eta}_t}{\prod_{j=t}^{i}\left(1+r_j^t\right)}\right), \tag{1}$$

where $c_i\,|\vec{\eta}_t$ is the net cash flow in period i conditioned on all the information available to the market until date t from the beginning of the firm's existence. $\vec{\eta}_t = \{\vec{\eta}_{t-1}, \eta_t\}$, with η_t the new information flow to the market during a time from $t-1$ to t. (Note that η_t itself can be multidimensional.) r_j^t represents the term structure of the interest rate for the firm in a period j at some time t. E_t acts as the expectation operator at a time t (i.e., expectation with respect to investor belief about cash flow distribution at time t).

The change in firm value between periods t and $(t+1)$ is

$$\Delta V = E_{t+1}\left(\sum_{i=t+1}^{T}\frac{c_i\,|\vec{\eta}_{t+1}}{\prod_{j=t+1}^{i}\left(1+r_j^{t+1}\right)}\right) - E_t\left(\sum_{i=t}^{T}\frac{c_i\,|\vec{\eta}_t}{\prod_{j=t}^{i}\left(1+r_j^t\right)}\right). \tag{2}$$

Given that the definition of period is arbitrary, if the length of the period is shrunk such that η_{t+1} is simply the breach information during periods t and $t+1$, then ΔV represents the change in the firm's value because of this firm-specific event. Because the firm is part of a market, ΔV includes any change in firm value that is related to market forces. Let ΔV_b be the change in value produced by a firm-specific security breach event, and let ΔV_m be the change in firm value because of a concomitant market event. Thus, for a breached firm,

$$\Delta V_b = \Delta V - \Delta V_m. \tag{3}$$

Several interesting observations are obtained from this model. First, both the change in the breached firm's value and the change in the market value are observable during the event period. The change in firm value is derived due to breach from these two observed values. Second, the change in the breached firm's value subsumes all types of breach costs mentioned above, and the different types of costs cannot be distinguished. However, an indirect approach can be used to get an estimate of these costs: The types of costs likely to be associated with the breach event are specified *ex ante* for the firm

under consideration using specific information about the type of breach and the attributes of the firm and rational arguments. For example, it is reasonable to assume that most of the costs associated with a DOS attack will be tangible short-term costs related to loss of business due to unavailability of the breached information resources. However, in most cases, it may be nearly impossible to separate the different types of breach costs. Third, in view of the fact that investors change their beliefs based on all the information that is known to date, the breach value will be correlated with the known characteristics of the firm and breach type and any other information available to the investors. Thus, in a cross-sectional analysis, the calculated breach cost can be regressed against these attributes to better determine their effects on the breach cost. In addition, it is important to note that because investors revise their beliefs based on their most current information, the same information event can generate different belief revisions for investors at different times.

Development of Hypotheses

In keeping with the discussion of breach costs and firm value under the efficient market hypothesis, several testable propositions are derived in the discussion that follows.

Impact of Security Breaches on Market Value of Breached Firm

As discussed above, a security breach is multifaceted and can have both tangible and intangible costs. Whereas most tangible costs are immediate or short-term, the intangible costs can have a long-term effect on the firm's expected future cash flows. Anecdotal evidence suggests that the impact of a security breach on the breached firm's value can be significant. For example, immediately following the February 2000 DOS attack, Yahoo, eBay, and Buy.com lost 15 percent, 24 percent, and 44 percent, respectively, of their market value [4].

The relationship between IT security and market valuations of firms doing business on the Internet can be traced to the trust of customers who do business with the firm through the Internet. Customer trust assumes more significance in e-business because of concerns related to data privacy. A customer may be unwilling to transact business with sites perceived to be insecure. A security breach can irrevocably damage the trust and confidence necessary to build a long-term relationship with the customer. In the Internet era, characterized by much competition and little loyalty, dissatisfied customers can switch to competitors that are just a click away. Thus, perceptions of lax security can have a profound financial impact on a firm. Security problems may signal to the market that the firm is not concerned about customer privacy or that its internal security practices are poor, and this may lead investors to question the firm's long-term performance [32].

As described in the model given above, investors revise their expectations based on new information in announcements. Investor expectations are reflected in the value of the firm. If investors view a security breach negatively,

believing that the transitory and long-term costs resulting from it will substantially reduce expected future cash flows [31], then one may expect a negative abnormal stock market return near the day of the announcement.

> *H1: A firm's announcement of an Internet security breach is negatively associated with its abnormal stock return.*

Determinants of Cross-Sectional Variance

The discussion in this section develops hypotheses to explain the cross-sectional variation in abnormal returns caused by security breaches. The determinants of cross-sectional variation in abnormal returns are classified into three categories: firm-specific factors, context-specific factors, and event-specific factors. Firm-specific factors, such as firm type and firm size, affect the magnitude of reaction in capital markets. Time (i.e., date security breach occurred), defined here as a context-specific factor, is used as a variable to control for changes in investor beliefs correlated with the passage of time. Breach type is defined as an event-specific factor. Because investors presumably know these factors when they revise their expectations of future cash flows, these variables will correlate to the cross-sectional variation in the change in firm value triggered by a breach event.

1. Firm-specific factors comprise the first group of determinants to be discussed.

Firm type. Firms doing business on the Internet are typically grouped into two categories: conventional firms and net firms. Conventional firms, sometimes referred to as brick-and-mortar or click-and-mortar firms, have a customer base in traditional markets and thus do not rely solely on the Internet to conduct business. Brick-and-mortar firms (e.g., Coca-Cola) do not use the Internet as an additional channel to sell their products, but they use it as a marketing tool to communicate with their customers. Click-and-mortar firms (e.g., Borders) use the Internet as another channel—in addition to their physical stores—to sell their products. Internet firms, also called pure play or Internet-only companies, include firms like Amazon and eBay, which rely exclusively on the Internet to sell their products and services.

Although security breaches can impose short- and long-term costs on both types of firms, the intangible long-term costs are more severe for Internet firms. These firms rely solely on the Internet for their survival, so information security is not an attractive optional feature but an essential ingredient for success. Outages caused by DOS attacks mean lost revenues and lost opportunities, because customers cannot make intended purchases. Attacks that penetrate the confidentiality and integrity of customer information may lead to liability suits and long-term competitive disadvantage. All of these costs are nearly impossible to estimate *ex ante*.

Consumer concern about on-line security has been confirmed in several surveys. Respondents in a Rockbridge Associates study expressed suspicions about the security of on-line transactions: 58 percent did not consider any on-line transaction safe, 67 percent were not confident about conducting business with a company that could only be reached on-line, and 77 percent thought

it was unsafe to provide a credit card number over a computer [7]. A study by the Angus Reid Group revealed that many Internet users have never shopped on-line, because they fear their credit card information will be leaked or stolen [2]. Consumer fears about security and security breaches impose intangible costs on firms, because they contribute to the loss of consumer confidence.

Conventional firms are relatively less affected than net firms by security breaches on the Internet. Firms that use the Internet simply to provide information to the public will incur little damage from DOS attacks on their Web sites, and even those that conduct business over the Internet will not be completely shut down by such attacks. If, for example, a security problem shuts down the Borders Web site, the company can continue to sell books through its physical stores. This is not true for Amazon. If its Web site is down, there is no other way for customers to transact business with the company. Besides, the intangible costs in terms of customers' and partners' loss of trust in the organization would probably be much more severe for net firms. Thus, even if the dollar cost is the same in terms of time and other resources spent on fixing the breach and getting the system up and running, intangible long-term costs are likely to be far greater for Internet firms than for non-net firms. Based on the above arguments, one may expect the impact of security breaches to be higher for net firms than for conventional firms. Because the change in a firm's value due to a breach captures both the short- and long-term tangible and intangible costs, one may posit a significant long-term intangible cost to net firms, a cost that will be reflected in stock price returns. In other words, cumulative negative abnormal returns are higher for Internet firms than for non-net firms.

> *H2: The magnitude of abnormal negative returns for Internet security breaches is larger for net firms than for conventional firms,* ceteris paribus.

Firm size. It is well documented in the finance literature that the expected return for small firms exceeds the expected return for large firms even after accounting for beta, or market, risk [6, 33, 63]. Fama and French attribute this discrepancy to possible distress risks in small firms [33]. With greater access to capital markets, lower costs for capital, multiple sources of income, diversified market products, and brand-name recognition, large firms can absorb negative economic and financial shocks more easily than small firms. Security breaches can be viewed as negative economic shocks. Large firms are likely to handle these shocks better than small firms.

In the strategic management literature, the resource-based theory of firms is widely used to explain competitive advantage. This definition of a firm as a broader set of resources that can be used to accomplish organizational goals can be traced to the seminal work of Penrose [59].[3] Resources are broadly defined as tangible or intangible assets that are tied semipermanently to the firm and may include brand names, skilled personnel, technological skills, patents, machinery, capital, and efficient procedures [14]. Large firms are likely to have more of these resources than small firms: more capital to work with, more slack resources to deploy in case of a security breach, such as backup Web servers and IT staff, perhaps even more highly skilled IT personnel than small firms. These differences can produce asymmetries in the impact of secu-

rity breaches. Both the distress risk issues cited by Fama and French and the resource-based theory indicate that large firms may be better able to withstand the negative impacts of security breaches than small firms.

In addition, empirical studies in the IS domain have documented similar relationships between firm size and abnormal returns. Bharadwaj and Keil found an inverse relationship between firm size and (negative) abnormal stock returns when they examined the effects of IT failures [10]. Hendricks and Singhal reported similar results for supply-chain problems [39]. In a study of the impact of IT investments, Im and colleagues observed that (positive) abnormal returns were negatively related to firm size [40].

> *H3: An abnormal (negative) stock market return due to an Internet security breach is larger for smaller firms than for larger firms,* ceteris paribus.

2. The discussion of determinants now proceeds to event-specific factors.

Nature of attack (breach type). IT security breaches are associated with three primary categories of attack: access attacks, modification attacks, and DOS attacks [51]. Each type of attack compromises one or more of a company's security objectives: confidentiality of customer information, integrity of information, and availability of applications and services.

In an access attack, the attacker attempts to gain unauthorized access to information. Access attacks may occur through technical means that exploit a vulnerability in the system, so that the attacker gains access to customer information purely electronically. They may also be made through "social engineering"—ploys or scams by which the attacker attempts to extract unauthorized information from the customer (e.g., by posing as a customer representative on the telephone and requesting credit card or other information).[4]

A modification attack is one in which the attacker attempts to make illegal insertions or deletions of information. This type of attack compromises the integrity of the information.

DOS attacks deny the use of resources, applications, or information to legitimate users of the system.[5] They are arguably the most critical security issue on the Internet, particularly for e-commerce services.[6] If the site is not available, revenue is lost, resulting in a direct hit to the bottom line. Customer dissatisfaction can grow quickly.

On the upside, DOS attacks have relatively brief durations and do not destroy data. Although obviously disruptive, attacks on availability only affect site accessibility, making them less damaging than other forms of attack that destroy, manipulate, or expose programs and sensitive information on a wide scale. DOS attacks do not expose firms to the potentially large third-party liability associated with breaches of privacy and unauthorized leaks of customer information. Thus, although tangible costs resulting from lost business can be substantial after a DOS attack, the intangible costs are likely to be higher with other types of attack. Because the overall cost of a breach includes both types of cost, it is difficult to determine whether capital markets consider availability breaches more serious than other breach types. Thus, a directional result is not proposed in the next hypothesis.

H4: The magnitude of abnormal negative returns that result from Internet security breaches will differ between availability and all other types of attack, ceteris paribus.

3. Context-specific factors are the final body of determinants to be discussed.

Time. In the early days of the Internet, few security-related incidents occurred, and firms and investors paid little heed to the possibilities of access, integrity, or availability attacks. However, where once security was considered an unnecessary burden, in recent years, these issues have become a primary concern, as more firms experience security breaches. The pattern of increase can easily be seen in the number of security incidents reported to CERT. In 1996, there were only 2,573 reports of security-related incidents. This number jumped to 21,756 in 2000, and to 52,658 in 2001 [16]. The popular press has begun to publish more news about Internet security. A key word search of the term "Internet security" in Lexis/Nexis revealed 97 articles in 1996, 696 articles in 2000, and 625 in 2001. Recent attacks on high-profile Web sites like Amazon, eBay, Yahoo, and Etrade have contributed to heightened awareness of Internet security.

Investors cannot have perfect insight into the exact costs of a particular security breach, but as more is discovered about the cost of security breaches in general, investors in due course may revise their beliefs about the costs. The eventual change in reaction to similar events has been documented by several IS researchers. Bharadwaj and Keil find that (negative) abnormal returns due to IT-related project failures are positively associated with the passage of time [10]. Similarly, Subramani and Walden show that market reactions to e-commerce announcements changed from positive to negative over time [69]. In light of this, the research design controls for time. If a learning curve is involved in investors' gaining understanding of the implications of security breaches, one would expect the response to security breaches to change over a time interval [1].[7] Time is used as a control variable to proxy for such belief revision over time.[8] Earlier researchers, such as Mikhail, Walther, and Willis [52], used this variable to control for similar effects.

Relationship Between Internet Security Breaches and Market Value of Internet Security Firms (Information Transfer)

Announcements of security breaches convey information to investors about Internet security developers. Anecdotal evidence suggests that there is a link between security breaches and the market value of Internet security firms. Following the news of the February 2000 DOS attacks, five different Internet security stocks climbed more than 20 percent, and one firm, WatchGuard Technologies, gained 46 percent. When Microsoft was hacked almost a year later, the stock prices of security firms also increased [55]. A series of attacks against Web firms in the last few years proves that this is not a temporary issue. As firms invest more in security, demand for security products increases. An estimate by IDC predicts that the worldwide market for IT security products will reach $21 billion in 2005, from $6.7 billion in 2001. Gartner predicts that investments by U.S. companies in information security will increase from the

current 0.4 percent of revenue to 4 percent of revenue by 2011, a 1,000 percent increase [64].

Information transfers are said to occur if announcements made by one group of firms contemporaneously affect the returns of another group of non-announcing firms [66]. Previous studies have documented information transfers in various settings, such as earnings announcements, sales announcements, and management forecasts [3, 5, 20, 34, 35, 37, 56]. Most information-transfer studies concentrate on intra-industry information transfer, but Olsen and Dietrich, and Chang, Mishra, and Huang consider interindustry information transfers [17, 56]. Olsen and Dietrich show that monthly sales announcements by retailers lead to statistically significant changes in the stock prices of retailers and their suppliers. Chang, Mishra, and Huang studied information transfer across industries in the supply chain and the characteristics of the supply chain, such as relative dependence, level of vertical integration, and type of news (i.e., good vs. bad) that affects the magnitude of information transfer.

The notion of information transfer in the present paper is similar to the one used by Olsen and Dietrich and by Chang, Mishra, and Huang in that it posits information transfer between firms that suffer from breaches and firms that are potential suppliers of security products to breached firms [17, 56]. Following both empirical and anecdotal evidence, it is expected that announcements of security breaches will have a positive impact on the valuation of the stocks of security firms.

> *H5: Announcements of Internet security breaches are positively associated with abnormal stock market returns of Internet security firms.*

Data Set and Methodology

Sample Selection

For the purpose of analyzing how announcements of security breaches affect capital markets, "event" is defined in this study as the first public disclosure to the media of a security breach of a firm. The study covered security breaches that occurred between January 1, 1996, and December 31, 2001. The samples of announcements of security breaches came from three different news sources: Lexis/Nexis, and the technology portals CNET and ZDNET. Lexis/Nexis was chosen because the databases it covers includes the major U.S. newspapers. CNET and ZDNET were chosen as alternative databases to supplement the articles found in Lexis/Nexis, because they are highly regarded global sources of information for the technology industry. After careful examination of several articles about Internet security breaches, the on-line search features of these sources were used to search for announcements using the key words "attack," "breach," and "break-in" in the same search string as the words "hacker," "Internet," and "security." This search resulted in 2,563 articles for potential events.

Every news article that mentioned specific breaches was considered in the study. A news article might refer to a press release by a breached firm or might include news about an apparent security breach, such as a DOS attack or a

Web defacement (see Appendix A for an illustrative sample). Consistent with the literature, an announcement that contained news about security breaches at multiple firms was counted as announcing multiple events, each one relating to one of the firms involved [70]. The data search included duplicate items, because data were gathered from different sources. When there was more than one announcement about the same security breach, the earliest announcement was retained, and the others were eliminated. Also eliminated were announcements related to IT project failures, such as implementation and operation system failures resulting from sudden malfunctions in software or hardware, because these were unrelated to security. At the end of this step, 225 events corresponding to security breaches were identified from the 2,563 articles.

The next step eliminated announcements of attacks against firms that were not publicly traded—government agencies, nonprofit organizations, and privately held companies. Also removed from the data set were publicly held companies not traded in the United States. These steps reduced the number of events in the database to 78.

After these screenings, the remaining data set only included announcements pertaining to firms traded on U.S. capital markets. These firms were then matched with data available on the University of Chicago's Center for Research in Security Prices (CRSP) daily common-stocks returns tapes. Firms that did not have return data in CRSP, such as those traded in the OTCBB market [23], were matched with return data in either the NASDAQ Quote or Yahoo Quote archives. A few announcements were eliminated from the data set because sufficient historical return data necessary for a meaningful analysis were unavailable. The remaining announcements were checked against confounding factors, such as dividends, mergers and acquisitions, earnings, or other significant public announcements, that could undermine the results of the study. Consistent with the literature, the check for confounding factors was conducted on the day before, the day of, and the day after the security breach announcement. After this last check, the final database consisted of 66 security breach announcements in the period 1996–2001.

Sample Coding

Each announcement and all related firm characteristics were carefully examined to operationalize a classification scheme to test hypotheses 2 through 5. Following the convention in other event studies, market value was used as a surrogate for *firm size* [10, 40]. The natural logarithm of market value (in million dollars) of the firm at the end of the year immediately preceding the event date was used as a measure of firm size. Market value data were collected from the Compustat database.

Internet.com's Internet Stock List™ and Morgan Stanley Dean Witter's Internet Companies List were used to code the firms in each announcement as either conventional or net firms. These two lists are the most comprehensive lists of Internet firms. They only include companies that are solely in Internet-related business. The same lists were used in prior studies [30, 38, 71]. In the present study, a firm was classified as a net firm if it was listed on

both lists. If it did not appear in either list, it was coded as a conventional firm. There were two firms, listed in one list but not the other. They were classified as conventional firms because a detailed examination revealed that they generated a significant portion of their revenues from non-Internet channels. Of the 66 events, 31 were coded as announcements by Internet firms, and the remaining 35 as announcements by conventional firms.

To code the nature of the breach as either an availability breach or other breach, each announcement was carefully examined to determine whether the security breach resulted in the loss of availability of a service, application, or information. Two of the authors independently categorized the security breaches. The coders were in agreement in 96.96 percent of the cases. This level of agreement indicates a very high level of intercoder reliability. Inconsistencies in categorization were resolved through discussions. Of the 66 events, 34 were coded as announcements for availability attacks, and the remaining 32 as announcements for other attacks.

Sample Description

Table 2 presents the distribution of security breach announcements in the final data set. The frequency of security breaches ultimately increased. There were only two announcements in 1996. The number jumped to 21 in 2000 and 26 in 2001. About 29 percent of the 66 announcements were made between 1996 and 1999, and the remaining 71 percent between 2000 and 2001. The increase in the number of announcements may be attributed to several reasons, including an increase in the number of firms with a presence on the Internet, greater awareness of security, and an increase in the media coverage of IT security.

Table 3 shows descriptive statistics for firms in the sample of 66 events based on data from the most recent year before the announcement date of security breach. The mean asset value was $38.5 billion, and the mean market value was $78.3 billion. Higher mean values compared to median values indicates that the sample is skewed toward larger firms.

Selection of Internet Security Product Firms

The list of Internet security firms was compiled from two sources: INFOSYSSEC, the security portal for information system security, and *Information Security Magazine,* the leading magazine for the security industry. INFOSYSSEC provides a section about top security companies and their stock quotes that lists more than 40 publicly traded security firms [42]. This list was augmented with the list of security firms nominated for the 2002 Information Security Excellence Awards by *Information Security Magazine* [41]. These awards are given to companies that offer products and services recognized as leaders in the information security field.

A total of 128 security firms was identified after the firms in these two sources were combined. When the duplicates were removed, the list contained

Year	Number of security breaches
1996	2
1997	5
1998	6
1999	6
2000	21
2001	26

Table 2. Security Breach Announcements, 1996–2001.

99 unique firms. The list was screened to identify the private firms and foreign security firms not traded in the United States—this process eliminated 43 firms from the list. After a careful investigation, any of the remaining firms whit core business that was not Internet security were also removed. The business description of each firm provided in Yahoo Finance was used for this purpose. If security was not mentioned in the description, the firm was dropped from the list. This process removed 16 firms from the list. The final list after all these checks comprised 40 security firms traded in U.S. capital markets (see Appendix B for details).

In the next step, a security firm sample was compiled for each event—that is, for each announcement of a security breach. We included a security firm in an event's security firms sample only if it had been a publicly traded company for at least 160 days before the day of the event. The exact composition of events' security firm samples varied with time, because the number of security firms that qualified for inclusion (out of 40 firms) in the security firm sample varied with time. The mean number of security firms for each event was 31.12, the minimum was 17, the median was 36, and the maximum was 38. As in the case of the breached firms, these firms were then matched with their return data in CRSP.

Statistical Methodology

The event-study methodology was used to assess the impact of announcements of security breaches on capital markets. An event study seeks to determine the effect of an announcement (the event) on the stock prices of firms. This method has been employed extensively in the accounting and finance literature to study the effects of an assortment of events, ranging from corporate acquisitions to joint venture formation to CEO successions [28, 36, 43, 47, 67, 68]. The first application of this methodology in the IS literature was the study by Dos Santos, Peffers, and Mauer, who examined the effect of IT investment announcements on market values of firms [29]. More recently, the effects of various types of IS-related announcements on capital markets have been examined, including e-commerce initiatives, IT failures, IT investments, dot-com name changes, and newly created CIO positions [10, 18, 23, 40, 70].

	Mean	Median	Standard deviation	Minimum	Maximum
Total assets (in million $)	38,558.9	5,348.0	109,158.2	37.8	642,191.0
Sales (in million $)	12,199.6	4,357.2	16,282.5	11.0	64,826.0
Net income (in million $)	1,655.1	344.7	3,134.2	-1,457.6	11,797.0
Market value (in million $)	78,327.0	23,333.7	113,928.2	158.7	460,770.5
Number of employees (in thousands)	38.5	12.7	54.8	0.1	260.0

Table 3. Descriptive Statistics for Breached Firms.

The event of interest in the present study is the announcement of an Internet security breach in a firm. To determine whether an announcement affects a firm's stock price, for each firm, the study first estimated what the return of the stock would have been had the event not occurred, that is, the normal return. Consistent with other event studies, the market model used in the study was one that predicts a linear relationship between the market return and the return of a stock.[9] The model is specified as

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t}, \quad (4)$$

where $R_{i,t}$ is the return of stock i on day t; $R_{m,t}$ represents the return on the market portfolio on day t; α_i and β_i stand for the intercept and slope parameters, respectively, for firm i; and $\varepsilon_{i,t}$ symbolizes a disturbance term for stock i on day t, with the usual ordinary least squares (OLS) properties.

The NASDAQ composite index was chosen as the market index. It includes more than 4,000 companies, more than most other stock market indices. Because it is broad-based, the composite is one of the most widely followed and quoted market indices. Most of the firms in the sample were technology firms, so the use of the NASDAQ composite index (characterized as a technology index) as the market index was appropriate. Previous event studies on Internet firms also used the NASDAQ as the market index (e.g., [62]).[10]

The market model was used to estimate the intercept and slope parameters for each firm in the sample. The sizes selected for the estimation window and the event window were based on previous event studies. The estimation period ranges typically from 120 days to 200 days [10, 29, 40, 70]. The study used an estimation window of 160 days. The estimation window started 160 days before the announcement day and ended one day before the announcement day. In event studies, the selection of the event window over which the effects of an announcement are examined is crucial [50].[11] A one-day event window is usually preferred. In practice, the event window is often expanded to two days, the day of announcement ($t = 0$) and the day after the announcement ($t = 1$) [13, p. 151]. This is done to capture the price effects of announcements that occur after the stock markets close on the announcement day. If the announcement is made before the markets close, any response to new information in it will be reflected on the announcement day. However, if the announcement is made after the markets close, the effects will be reflected in the stock price on the day following the announcement. Some studies included the period before the announcement day in the event window in order to capture the possibility of information leakage to markets before the announcement day [70]. Because security breaches are generally unanticipated, however, the event window in the present study did not incorporate any period before the announcement. Consistent with the above arguments, a two-day event window was used in the analysis. To the extent that the actual announcement day preceded the day used in the sample, the tests were biased toward accepting the null hypothesis of no abnormal returns in the event window.

The coefficient estimates, $\hat{\alpha}_i$, $\hat{\beta}_i$, from regression of Equation 4 were used to predict the expected return over the event window. Then the abnormal return

for firm i on day t of the event window was calculated, following McWilliams and Siegel [50]

$$AR_{i,t} = R_{i,t} - \left(\hat{\alpha}_i + \hat{\beta}_i R_{m,t}\right). \tag{5}$$

Abnormal returns (also called excess returns) are deviations of realized returns from normal returns. They are unbiased estimates (in the return form) of changes in the market value of the firm during the event period that are attributed to investors' reactions to information contained in an announcement [29]. The standard errors are calculated as in Subramani and Walden [70]:

$$\operatorname{var}\left(AR_{i,t}\right) = \left(s_i^2 \left[1 + \frac{1}{160} + \frac{\left(R_{m,t} - \bar{R}_m\right)^2}{\sum_{t=-160}^{-1} \left(R_{m,t} - \bar{R}_m\right)^2} \right] \right) \tag{6}$$

where s_i^2 is the residual return variance from the estimation of the market model on the interval of 160 days before the event window, $\bar{R}_m$ is the mean market return on the market index over the estimation window, and $R_{m,t}$ is the return on the market index on day t in the estimation window.

Assuming that abnormal returns are independent of time, for firm i, the cumulative abnormal return (CAR) and the variance of the cumulative abnormal return are the sum of the individual abnormal returns and variances over the event window, respectively. Thus,

$$CAR_i = \sum_{t=0}^{1} AR_{it} \tag{7}$$

and

$$\operatorname{var}\left(CAR_i\right) = \sum_{t=0}^{1} \operatorname{var}\left(AR_{it}\right). \tag{8}$$

These are aggregated across all events to draw an overall inference as

$$\overline{CAR} = \frac{1}{N} \sum_{i=1}^{N} CAR_i \tag{9}$$

along with

$$\operatorname{var}\left(\overline{CAR}\right) = \frac{1}{N^2} \sum_{i=1}^{N} \operatorname{var}\left(CAR_i\right). \tag{10}$$

	Abnormal returns		Cumulative abnormal returns
	$t = 0$	$t = 1$	$(t = 0, t = 1)$
Mean	-0.0086	-0.0123	-0.0209
Minimum	-0.1806	-0.1803	-0.3609
First quartile	-0.0225	-0.0207	-0.0294
Median	-0.0025	-0.0050	-0.0144
Third quartile	0.0141	0.0067	0.0185
Maximum	0.0655	0.0394	0.0892

Table 4. Descriptive Statistics of Abnormal Returns and Cumulative Abnormal Returns ($n = 66$).

A student's *t*-test was used to test the alternative hypothesis that the mean *CAR* over the event period significantly differed from zero:

$$t = \frac{\overline{CAR}}{\sqrt{\text{var}\left(\overline{CAR}\right)}} t_{(a,df=N-1)}. \tag{11}$$

Results

Effect of Security Breach Announcements on Announcing Firms

Table 4 presents the abnormal returns for each day in the event window and the cumulative abnormal returns over the event window resulting from the announcements of Internet security breaches. The median and mean cumulative abnormal return over the event period and the median and mean abnormal return for each day in the event window were negative. On announcement day ($t = 0$), an average of –0.86 percent abnormal returns was observed. The stocks realized, on average, an abnormal return of –1.23 percent on the day following the announcement ($t = 1$). This gave rise to a –2.09 percent cumulative abnormal return over the event window. Compromised firms lost, on average, around 2.1 percent of their market value within the two days surrounding the events.[12] This translated into a $1.65 billion average loss in market capitalization per incident, based on the mean market value of the firms in the data set.[13]

Table 5 presents the results to test H1. The mean abnormal returns are negative and statistically significant for each day in the event period. Over the event window, the *t*-statistic for the mean cumulative abnormal return is almost 3, with a *p*-value of 0.00192, indicating that the mean cumulative abnormal return is significantly different from zero. Thus, the null hypothesis of a zero-mean cumulative abnormal return is rejected in favor of the alternative hypothesis 1.

Event window	Mean	*t*-value	*p*-value[a]	Frequency of negative returns[c]	*z*-value[b]	*p*-value[a]
0	-0.008638	-1.74985	0.04243	36	-0.948630	0.171404
1	-0.012282	-2.49133	0.0076442	39	-1.894067	0.029108
0,1	-0.02092	-2.99862	0.00192	41	-1.823797	0.034091

Table 5. Event Study Results for Breached Firms.

[a] *p*-values of one-tailed significance.
[b] If T^+ is the sum of the ranks assigned to positive CARs, and N is the sample size, then the test statistic is given by $(T^+ - a)/b$, which is distributed as $N(0, 1)$ for large samples, where $a = N*(N + 1)/4$, and $b = N*(N + 1)*(2N + 1)/24$.
[c] Of 66 observations.

The results given above are based on the assumption that abnormal returns and cumulative abnormal returns are normally distributed random variables. The Wilcoxon signed-rank test—a nonparametric test—was employed to check the robustness of the results [53, p. 534]. As McWilliams and Siegel pointed out, nonparametric tests are important to control for the effects of outliers on the significance of results, because most event-study parametric test statistics are sensitive to outliers [50]. The results in Table 5 indicate that the signed-rank test statistic is negative ($z = -1.8238$) and significant ($p = 0.0341$), confirming the results of the parametric test.

Determinants of Cross-Sectional Variance in Cumulative Abnormal Returns

A multiple linear regression model, given in Equation 12, was set up to study the relationship between cumulative abnormal returns and characteristics of events. The model regressed the cumulative abnormal returns on hypothesized variables and control variables, namely, firm type, firm size, nature of attack, and time. This made it possible to test hypotheses 2 through 4.

$$CAR_i = \beta_0 + \beta_1 \left(FirmType\right)_i + \beta_2 \left(FirmSize\right)_i + \beta_3 \left(AttackType\right)_i + \beta_4 \left(Time\right)_i + \varepsilon_i . \quad (12)$$

The independent variables were operationalized as follows. Using the coding scheme discussed above, firm type was labeled using an indicator variable. A value of 1 was assigned if the firm type was Internet , and 0 otherwise. The size of the firm was coded as the log of the market value of the firm (in millions) at the end of the year immediately before the event. The nature of the attack was labeled 1 if the security breach was an availability attack, and 0 otherwise. Finally, time was captured using the number of years from the first announcement date. That is, the date on which the first breach announcement was made in the data set was chosen as the reference point and coded as zero, and the time for each successive announcement was captured as the difference between the date of the successive event and the date of the first event in units of year.[14] Descriptive statistics and a correlation matrix for independent variables are shown in Table 6.

Table 7 presents the results of the regression analysis. The overall model is significant ($F = 4.63$; $p = 0.0025$) with an R^2 of 0.2311 and an adjusted R^2 of 0.1828. H2 is supported by the results reported in Table 7. The coefficient for firm type is negative and significant ($t = -1.71$; $p = 0.0461$), indicating that abnormal (negative) stock market returns due to Internet security breaches are larger for net firms than for conventional firms. The results show, other things being equal, that compared to conventional firms, the stocks of net firms, on average, experience an additional 2.83 percent negative abnormal returns.

In contrast to expectations, no support was found for H4. The supposition that availability attacks have a different impact from other types of attacks was

Variable	Mean	Standard deviation	Minimum	Maximum	(1)	(2)	(3)	(4)
(1) Firm type	0.47	N/A	0	1	1.00			
(2) Firm size	9.88	2.09	5.07	13.04	-0.25	1.00		
(3) Nature of attack	0.52	N/A	0	1	-0.18	0.21	1.00	
(4) Time	3.30	1.34	0	5.03	-0.20	0.32	-0.06	1.00

Table 6. Descriptive Statistics and Pearson Product–Moment Correlations.

	Predicted sign	Parameter estimate	Standard error	*t*	*p*[a]
Intercept	-/+	-0.1141	0.0433	-2.64	0.0106
Firm type (H2)	–	-0.0283	0.0166	-1.71	0.0461
Firm size (H3)	+	0.0150	0.0042	3.60	0.0003
Nature of attack (H4)	-/+	-0.0122	0.0164	-0.74	0.4597
Time	–	-0.0107	0.0064	-1.68	0.0488
Model R^2	0.2331				
Adj. R^2	0.1828				
F-value	4.63	(0.0025)[b]			

Table 7. Results of Cross-Sectional Regression to Predict Variability in Cumulative Abnormal Returns.

[a] *p* represents one- (two-)tailed significance when sign is (is not) hypothesized.
[b]Number in parentheses specifies the significance of *F*.

not supported by the data. The parameter estimate was negative but not significant ($t = -0.74$; $p = 0.4597$). This implies that markets do not distinguish between different types of security breaches. In other words, market participants apply a similar negative premium to all attacks regardless of type. H3, which relates firm size to abnormal return, was strongly supported by the data. The parameter estimate for the firm size was positive and highly significant ($t = 3.60$; $p = 0.0003$), as expected. The result confirmed that smaller firms lose more than larger firms in case of a security breach. The estimate of time coefficient was negative and significant ($t = -1.68$; $p = 0.0488$), indicating that investors reacted more harshly to the recent attacks.

Effect of Security Breach Announcements on Internet Security Firms

The study assumed that the abnormal returns were uncorrelated in the cross-section in order to analyze the effect of security breaches on announcing firms. This was a reasonable assumption, because most of the announcements occurred at different time intervals. The assumption made it possible to calculate the variance of aggregated sample cumulative abnormal returns as the sum of the variances of individual sample cumulative abnormal returns. The assumption is not defensible, however, when the event windows overlap. Because all the security firms experienced the same signal for possible information transfer (i.e., an announcement of a security breach) on the same day, the event windows overlapped perfectly. In this case, the assumption of no covariance between the residuals (abnormal returns) of the security firms would have been problematic [9]. Therefore, in this instance, it was undesirable to aggregate the estimated variances of the cumulative abnormal returns of individual Internet security firms for a given security breach announcement to estimate the variance of the mean cumulative abnormal return for that event. Ignoring the contemporaneous correlation of residuals is even more dangerous if the sample firms come from the same industry, as in this case,

because of the presence of positive industry cross-sectional return covariation [57]. Hence, it is crucial to consider cross-sectional dependencies to avoid incorrect inferences.

It was decided, because of these concerns, not to estimate the variance of mean cumulative abnormal return from the estimated variances of sample cumulative abnormal returns for each information-transfer event. Instead, only the mean cumulative abnormal return was calculated for each event, $\overline{CAR}_i$. Assuming that all $\overline{CAR}_i$s were random samples from an infinite population with the same mean and variance, the following procedures were used to estimate mean and variance:[15]

$$\overline{\overline{CAR}} = \frac{1}{N}\sum_{i=1}^{N}\overline{CAR}_i \tag{13}$$

$$\text{var}\left(\overline{\overline{CAR}}\right) = \frac{1}{N*(N-1)}\sum_{i=1}^{N}\left(\overline{CAR}_i - \overline{\overline{CAR}}\right)^2, \tag{14}$$

where $\overline{CAR}$ is the mean cumulative abnormal return of security firms for security breach i, and $\overline{\overline{CAR}}$ is the average of all $\overline{CAR}_i$s. Therefore, the test statistic is

$$t = \frac{\overline{\overline{CAR}}}{\sqrt{\text{var}\left(\overline{\overline{CAR}}\right)}}t_{(\alpha,df=N-1)}. \tag{15}$$

Table 8 presents the abnormal returns for each day in the event window and the cumulative abnormal returns over the event window resulting from the announcements of Internet security breaches. Both the median and the mean of the cumulative abnormal returns over the interval and the abnormal returns for each day in the event window are positive. An average of 0.71 percent abnormal stock return was observed on the announcement day (t = 0). The stocks realized, on average, an abnormal return of 0.65 percent on the day after the announcement (t = 1). This gave rise to a 1.1356 percent cumulative abnormal return over the event window. In other words, each security developer realized, on average, a 1.36 percent return above the return expected by a market model. Thus, in the two-day period, a total average gain of $1.06 billion could be attributed to the information-transfer effects of security breach announcements on the market values of security developers.

The information-transfer effects of security breach announcements are reported in Table 9. The positive abnormal return is significant (t = 2.712). The nonparametric test is also significant (z = 2.028). These results support the hypothesis that security breach announcements affect the values of announcing firms and also of Internet security developers. The market value of security firms increased in anticipation of the expected future gains from such incidents.

	Abnormal returns		Cumulative abnormal returns
Statistics	**$t = 0$**	**$t = 1$**	**($t = 0$, $t = 1$)**
Mean	0.0071	0.0065	0.0136
Minimum	-0.0268	-0.0443	-0.0598
First quartile	-0.0084	-0.0085	-0.0113
Median	0.0018	0.0030	0.0041
Third quartile	0.0168	0.0160	0.0302
Maximum	0.0789	0.1226	0.1349

Table 8. Descriptive Statistics of Abnormal Returns and Cumulative Abnormal Returns ($n = 66$).

Sensitivity Analysis of Results

The robustness of the results to influential observations and model assumptions was evaluated by a series of sensitivity analyses. The first analysis dealt with the effect of outliers on the *t*-tests (H1, H5). Following convention, data points (events) that were outside the range of the mean, plus and minus three standard deviations, were removed [19]. For breached firms, this resulted in the elimination of one event from the data set. The cumulative abnormal return after this event was deleted turned out to be –1.57 percent and was significantly greater than zero ($t = –2.29$; $p = 0.012$). For security developers, no points were outside the limits. The nonparametric test controls for outliers, so there was good reason for confidence that the results are not driven by outliers.

The validity of the results concerning H2, H3, and H4 was checked by addressing three statistical issues associated with regression analysis: multicollinearity, heteroscedasticity, and influential points. The testing for multicollinearity began by first calculating the correlation matrix of all the independent variables in the regressions (see Table 6). All the coefficients were found to be below the threshold level of 0.7 [75]. Two other popular diagnostics were also calculated: the variance inflation factor (VIF) and the condition number (CN). VIF was below the threshold level of 10 for the regression on abnormal returns, and CN was below the threshold level of 30 [8, 19]. Thus, multicollinearity was not a problem in the data set.

Because the data set includes cross-sectional data, variance of disturbances may not be constant among all the data points because of different event-specific or firm-specific factors related to data points. As a quick check, residuals were plotted against independent variables, and no indication of trend was found in the regression (i.e., the residuals did not increase or decrease with the value of the independent variable). In addition, the White test was performed [74]. Heteroscedasticity was not detected at the 5 percent level.

The question of whether results are driven by a set of influential observations is crucial. Removal of those observations may cause substantial changes in the estimated coefficients and therefore in the test results. Cook's distance is the statistic usually employed to detect influential observations [22]. Several researchers suggest that instead of using limits, a scree plot of Cook's

Event window	Mean	*t*-value	*p*-value[a]	Frequency of positive returns[c]	*z*-value[b]	*p*-value[a]
0	0.007061	2.3671	0.010458	36	1.440512	0.07486
1	0.006540	2.0011	0.024780	35	1.357467	0.08732
0,1	0.013560	2.7123	0.004271	37	2.028216	0.02127

Table 9. Information-Transfer Effect on Security Firms.

Note: A total of 2,054 security firms were identified for 66 information-transfer events. The combination of the sample security firms varies with the timing of the events, because the number of security firms that qualified for inclusion in the sample varies with time. The mean number of security firms per information-transfer event was 31.12; the minimum was 17; the median was 36; and the maximum was 38.

[a] *p*-values of one-tailed significance.

[b] If T^+ is the sum of the ranks assigned to positive CARs, and N is the sample size, then the test statistic is given by $(T^+ - a)/b$, which is distributed as $N(0,1)$ for large samples, where $a = N^*(N + 1)/4$, and $b = N^*(N + 1)^*(2N + 1)/24$.

[c] Of 66 observations.

distances should be drawn to separate out the influential observations so that they can be dropped [19, 21]. For the regression on cumulative abnormal returns, the scree plot suggested the removal of five observations from the data set. When the model was refitted without these points, firm type was still significant at the 1 percent level, and attack type was still not significant.

The time variable in the regression analysis controlled for any change in volatility through time, as suggested by earlier research. However, stock betas can provide a firm-specific control for volatility. The regression was rerun with betas included to control for firm-specific volatility in order to check whether the results in Table 7 were confounded or not. Table 10 presents the results of the new regression. Beta was significant at the 5 percent level. The time variable that was a control variable became insignificant. This implies that beta was a better control for volatility than time. However, the main results were still significant (firm type was even more significant than before). The attack type was still insignificant. Therefore, the results of the cross-sectional analysis were not confounded by stock betas. Thus, the results were robust against every sensitivity and robustness check that was conducted.

Implications, Limitations, and Conclusions

Implications

According to the CSI-FBI Computer Crime and Security Survey 2002, which polled 503 respondents from organizations throughout the United States, 80 percent reported financial losses, but only 44 percent (223) were able to quantify them. The total reported loss was $455,848,000, and the average estimated loss was $2,044,161 per organization across all types of breaches. The highest reported loss was for theft of proprietary information, reported by 41 organizations, with an average of $4,166,512 per organization. The sabotage of data networks cost an average of $351,953, and DOS attacks resulted in a $244,940 loss per organization. The reported losses included the firms' estimates of direct and tangible costs associated with security breaches only.

The results of the present study show that the announcement of an Internet security breach is negatively associated with the market value of the announcing firm. In the study, breached firms lost an average of 2.1 percent of their market value within the two days surrounding the events, which is roughly a $1.65 billion average loss in market capitalization per incident across breach types. This figure is orders of magnitude above the average loss estimate reported in the CSI-FBI survey. The huge difference in the estimates of firm losses because of a security breach may be explained by the fact that firms in the CSI-FBI survey estimated only direct costs, such as lost productivity or sales, and expenditure on restoring the breached system, whereas the loss estimated in the present event study may also include investors' expectations about the impact on future cash flows, which requires considerations of intangible costs, such as the loss of consumer confidence. Investors may also anticipate that the firm will be breached again in the future. The estimates based on the event study may be noisy because of the uncertainties. Even if the esti-

	Predicted sign	Parameter estimate	Standard error	*t*	*p*[a]
Intercept	-/+	-0.1389	0.0435	-3.19	0.0022
Firm type (H2)	–	-0.0539	0.0198	-2.72	0.0043
Firm size (H3)	+	0.0131	0.0041	3.16	0.0013
Nature of attack (H4)	-/+	-0.0126	0.0159	-0.79	0.4306
Time	–	-0.0053	0.0067	-0.79	0.2169
Beta	-/+	0.0416	0.0189	2.20	0.0318
Model R^2	0.2902				
Adjusted R^2	0.2311				
F-value	4.91	(0.0008)[b]			

Table 10. Results of Cross-Sectional Regression by Firm Betas.

[a]*p* represents one- (two-)tailed significance when a sign is (is not) hypothesized.
[b]Number in parentheses specifies the significance of *F*.

mates are discounted, however, there is an order of magnitude of difference between the firms' reported estimates in the CSI-FBI survey and the market value loss in the study. One possible implication of this finding is that the intangible costs of security breaches may be much larger than the tangible costs, and therefore, firms that ignore the intangible costs grossly underestimate the loss from security breaches. Because investments in IT security are directly dependent on the extent of potential loss from breaches, firms are likely to underinvest in IT security if they make investment decisions based only on tangible costs. The study offers proponents of IT security a much-needed economic justification to get firms to invest in security.

The finding that the average (negative) cumulative abnormal return associated with announcements decreases with the size of the firm suggests that investors penalize smaller firms more than larger firms when a security breach occurs. This implies that managers of small firms must understand the importance of security for their survival, and goes against the common argument, "We are a small firm, and we cannot invest much in IT security." In fact, managers of small firms should view IT security as a key issue for survivability.

Another important finding is that the market penalizes all firms for security breaches, but Internet firms are penalized more than conventional firms. A possible explanation for this effect is the differential degree to which firms depend on the Internet to generate revenues and survive in the long run. This result is intuitive—firms that rely solely on the Internet for their revenue (so-called pure-play firms) have more to lose from poor IT security infrastructure than firms that have multiple sales channels. Security of IT systems is a matter of the utmost importance for the success of Internet firms.

The results show that negative effects of security problems have been increasing. A possible explanation for this progression is that the role of the Internet in commerce has increased along with the risks. As investors come to understand Internet-based business models, security breach events assume more significance in their minds. An implication for managers is that the risk of security breaches should be periodically reassessed, and the necessary steps should be taken to mitigate the risk. The finding that firms experience similar

cumulative abnormal returns regardless of the nature of the attack is somewhat puzzling. One possible explanation is that investors regard any kind of security breach as a failure of the IT security program and penalize firms for not having taken adequate steps to prevent security problems. This explanation implies that managers should focus on minimizing all types of breaches to the fullest extent possible. Another possible explanation is that the intangible costs associated with security breaches are quite difficult to estimate. The large errors in these estimates obfuscate any differences between various types of security breaches in investors' minds. The study could not classify attacks into more than two categories, because there were not enough observations. Additional insights require further investigation. To increase the power of testing, future research should focus on more general classification of attack types in a larger data set.

The finding that security firms realize significant positive returns as a reaction to security breach announcements shows that security and e-commerce go hand in hand. There can be no e-commerce unless there is adequate security. The general rise in the stock prices of Internet security firms further justifies this argument, because security can be improved only with a series of security controls. Investors believe that firms will react to security breaches by investing more in security technology. The study does not offer any insights into what types of breaches will be prevented by particular technologies (e.g., firewalls, intrusion detection systems, disaster recovery systems). An effort to answer this question would be an interesting extension of the study.

Limitations and Conclusions

The study and research design had several limitations. Event-study methodology was used to estimate the cost of security breach events for firms. This methodology relies on the assumptions that markets are efficient and investors are rational. Thus, the present research, like all other event studies, suffers from the fact that real markets can deviate from such an ideal characterization. The time period used for the study was characterized by high market valuation and market volatility. This by itself does not invalidate the event-study methodology, but it may increase the errors in the estimates of breach cost. Although it is difficult to quantify these effects, the study tried to control them with the time variable.[16] The time variable is only weakly significant. However, to the extent that time does not capture the effects mentioned above, the results should be interpreted with caution. An effort was made to eliminate all known confounding events from the sample, but other, unknown factors that may affect a firm's market valuation during the event window may increase the error in the estimates of breach cost. Another limitation is the focus on publicly traded U.S. firms. This limits the generalization of the results to other countries but increases the internal validity of the research design. Future researchers may study the issue with samples from other nations.

Another significant limitation of the study relates to the categorization of breach types. Breaches were classified as either availability attacks or attacks of some other type. Clearly, it would be beneficial to classify the breaches that

belong to the second category more precisely. The reason for the primitive classification was the unavailability of data in the announcements. In addition, a finer classification would require more sample data to have sufficient statistical power. Further research can provide additional insights into the impact of breach type on capital markets.

The results of the study summarized in this paper should be reassuring to firms that have invested in information security. They should, as well, be a source of encouragement supporting implementation for firms that doubt the value of adopting sound security practices.

NOTES

1. Subsequent to the study, Ettredge and Richardson extended their analysis to include information-transfer effects associated with the February 2000 DOS attacks [30].

2. Without loss of generality, the terminal period can be chosen to be infinity, based on the going-concern assumption.

3. Subsequent work in this area has been done by Peteraf, Rubin, and Wenderfelt [60, 65, 73].

4. Such attacks have been especially painful for AOL. Its customers have been scammed several times using e-mail, telephone, and other means [44].

5. It is estimated that Internet traffic slowed by 26 percent because of DOS attacks in February 2000 [45]. A study at the University of California at San Diego estimated that nearly 4,000 such attacks per week are launched against Web sites [24].

6. CloudNine Communications, one of Britain's oldest Internet service providers, went out of business because its network was down for too long a time after a DOS attack [72].

7. It is also possible that there may not be any adjustment in time if investors have, on average, perfect insight into breach costs.

8. Note that the use of market-adjusted abnormal returns and time as a control variable makes it possible to control for market- and time-specific volatility.

9. The market model is good in terms of detecting event effects. The variance of abnormal return is reduced if the portion of the return related to variation in the market's return is removed. This improves the ability to detect event effects [46].

10. The use of other indices does not change our results qualitatively.

11. Unless there is a specific reason to keep the event window long, it should be kept short. Using a long event window severely reduces the power of the test statistics, which can cause false inferences about the significance of an event [11, 12]. Empirical evidence suggests that markets react to new information and adjust stock prices almost instantaneously [27, 54]. Another reason to keep the event window short is that it is almost impossible to control for confounding effects in long windows, which, in turn, influences the robustness of the test results. The methodology herein assumes that abnormal returns are the result of the announcement, and not of the other events occurring in the event window.

12. The cumulative abnormal return values are comparable to the cumulative abnormal return values found in other event studies. For example, Bharadwaj and Keil found that the mean cumulative abnormal return for IT failure announcements was –1.79 percent [10]. Menzar, Nigh, and Kwok, who analyzed the effect of the withdrawal of multinational firms from South African markets, observed that the mean cumulative abnormal return was –2.0 percent [51].

13. The average market capitalization loss per incident was calculated as the average market capitalization of breached firms times the average cumulative abnormal return over the event window.

14. The choice of the first announcement date as the reference point does not affect the results, nor does the choice of year as the time unit.

15. We thank Yexiao Xu, professor of finance at the University of Texas at Dallas, for suggesting these procedures. They do not assume that the cross-sectional error terms are independent for each event date. We also did a simple *t*-test of the mean that assumes that the cross-sectional error terms are independent for each event date. The result was highly significant ($t = 4.95$; $p < 0.0001$).

16. Researchers like Mikhail, Walther, and Willis have used this variable to control for similar effects [52].

REFERENCES

1. Agrawal, D.; Bharath, S.T.; and Viswanathan, T. Technological change and stock market volatility: Evidence from e-commerce **a**doptions. Working Paper. University of Maryland at College Park, Robert H. Smith School of Business, March 2003. Available at www.rhsmith.umd.edu/ceme/research/TechnologicalChange-April14-2003.pdf.

2. Angus Reid Group. *Security and Privacy Issues Keeping Millions from Shopping Online.* Angus Reid Group, April 27, 2000 (www.ipsos-na.com/news/pdf/media/ap000426.pdf).

3. Asthana, S.C., and Mishra, B.K. The differential information hypothesis, firm size, and earnings information transfer: An empirical investigation. *Journal of Business Research, 53* (2001), 37–47.

4. Atomic Tangerine. *NPV: Information Security.* Atomic Tangerine, Pittsburgh, 2000 (www.ttivanguard.com/risk/netpresentvalue.pdf).

5. Baginski, S.P. Information transfer associated with management forecasts of earnings. *Journal of Accounting Research, 25* (1987), 196–216.

6. Banz, R. The relationship between return and market value of common stocks. *Journal of Financial Economics, 9* (March 1981), 3–18.

7. Beale, M. Survey reveals consumer concern over e-commerce security issues. *E-Commerce Times*, June 21, 1999 (www.ecommercetimes.com/story/1981.html).

8. Belsley, D.; Kuh, E.; and Welsch, R. *Regression Diagnostics.* New York: John Wiley, 1980.

9. Bernard, V.L. Cross-sectional dependence and problems in inference in market-based accounting research. *Journal of Accounting Research, 25,* 1 (1987), 1–48.

10. Bharadwaj, A., and Keil, M. The effect of information technology failures on the market value of firms: An empirical examination. *INFORMS 2001 Miami,* November 2001 (www.informs.org/Conf/Miami2001/TALKS/Sponsor-13.html).

11. Brown, S., and Warner, J. Measuring security price performance. *Journal of Financial Economics, 8* (1980), 205–258.

12. Brown, S., and Warner, J. Using daily stock returns: The case of event studies. *Journal of Financial Economics, 14* (1985), 3–31.

13. Campbell, J.Y.; Lo, A.W.; and MacKinlay, A.C. *The Econometrics of Financial Markets.* Princeton: Princeton University Press, 1997.

14. Caves, R.E. Industrial organization, corporate strategy and structure. *Journal of Economic Literature, 58* (1980), 64–92.

15. CBS News.com. Locking Windows. Associated Press, January 16, 2003. Available at www.cbsnews.com/stories/2002/01/16/tech/main324663.shtml.
16. CERT Coordination Center. *CERT/CC Statistics 1988–2003.* Carnegie-Mellon University, Software Engineering Institute, January 22, 2004. Available at www.cert.org/stats/cert_stats.html.
17. Chang, H.; Mishra, B.; and Huang, C. Manager's earnings forecast and information transfer in supply chains. Working Paper, University of California at Riverside, 2003.
18. Chatterjee, D.; Richardson, V.J.; and Zmud, R.W. Examining the shareholder wealth effects of announcements of newly created CIO positions. *MIS Quarterly, 25,* 1 (2001), 43–70.
19. Chatterjee, S., and Price, B. *Regression Analysis by Example.* New York: John Wiley, 1991.
20. Clinch, G.J., and Sinclair, N.A. Intra-industry information releases: A recursive system approach. *Journal of Accounting and Economics, 9* (1987), 89–106.
21. Coenders, G., and Saez, M. Collinearity, heteroscedasticity and outlier diagnostics in regression. In A. Ferligoj and A. Mrvar (ed.), *New approaches in applied statistics.* Ljubljana: FDV, 2000, pp. 79–94.
22. Cook, R.D. Detection of influential observations in linear regression. *Technometrics, 19* (1977), 15–18.
23. Cooper, M.J.; Dimitrov, O.; and Rau, P.R. A rose.com by any other name. *Journal of Finance, 56,* 6 (December 2001).
24. Costello, S. Study: Nearly 4000 DOS attacks occur per week. CNN.com/IDG.net. Available at www.cnn.com/2001/TECH/internet/05/24/dos.study.idg/.
25. CSC (Computer Sciences Corporation). CSC survey reveals inadequate information security practices among companies worldwide (November 19, 2001). Available at www.csc.com/newsandevents/news/1584.shtml.
26. D'Amico, A.D. What does a computer security breach really cost? Secure Decisions, a Division of Applied Visions, Northport, NY, September 7, 2000.
27. Dann, L.; Mayers, D.; and Raab, R. Trading rules, large blocks and the speed of price adjustment. *Journal of Financial Economics, 4* (1977), 3–22.
28. Davidson, W.; Worrell, D.; and Dutia, D. The stock market effects of CEO succession in bankrupt firms. *Journal of Management, 16* (1993), 517–533.
29. Dos Santos, B.L.; Peffers, D.C.; and Mauer D.C. The impact of information technology investment announcements on the market value of the firm. *Information Systems Research, 4,* 1 (1993), 1–23.
30. Ettredge, M., and Richardson, V.J. Assessing the risk in e-commerce. In R.H. Sprague, Jr. (ed.), *Proceedings of the Thirty-fifth Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 2002.
31. Fama, E. Efficient capital markets II. *Journal of Finance, 46,* 5 (1991), 1575–1617.
32. Fama, E.; Fisher, L.; Jensen, M.C.; and Roll, R. The adjustment of stock prices to new information. *International Economic Review, 10,* 1 (1969), 1–21.
33. Fama, E., and French, K. The cross-section of expected stock returns. *Journal of Finance, 47,* 2 (1992), 427–465.

34. Foster, G. Intra-industry information transfer associated with earnings releases. *Journal of Accounting and Economics, 3* (1981), 201–231.
35. Freeman, R., and Tse, S. An earnings prediction approach to examining intercompany information transfers. *Journal of Accounting and Economics, 15* (1992), 509–523.
36. Friedman, S.D., and Singh, H. CEO succession and stockholder reaction: The influence of organizational context and event context. *Academy of Management Journal, 32* (1989), 718–744.
37. Han, J.C.Y.; Wild, J.J.; and Ramesh, K. Managers earnings forecast and intra-industry information transfers. *Journal of Accounting and Economics, 11* (1989), 1–33.
38. Hand, J. Profits, losses, and non-linear pricing of internet stocks. In J. Hand and B. Lev (eds.), *Intangible Assets: Values, Measures, and Risks.* New York: Oxford University Press, 2003.
39. Hendricks, K.B., and Singhal, V.K. The effect of supply chain glitches on shareholder wealth. Paper presented at INFORMS 2001, Miami, November 2001.
40. Im, K.S.; Dow, K.E.; and Grover, V. Research report: A reexamination of IT investment and the market value of the firm: An event-study methodology. *Information Systems Research, 12,* 1 (March 2001), 103–117.
41. *Information Security.* Information Security 2002 Excellence Awards Listing of Categories and Semi-Finalists. Available at www.infosecuritymag.com/awards2002/listproducts.html.
42. INFOSYSSEC, The Security Portal for Information System Security (http://infosyssec.com).
43. Koh, J., and Venkatraman, N. Joint venture formations and stock market reactions: An assessment in information technology sector. *Academy of Management Journal, 34* (1991), 869–892.
44. Kornblum, J. AOL users conned for credit data. CNET News.com, May 20, 1997. Available at http://news.com.com/2100–1033_3–279948.html.
45. Lemos, R. A year later, DOS attacks still a major Web threat. CNET News.com, February 7, 2001. Available at http://news.com.com/A+year+later percent2C+DDoS+attacks+still+a+major+Web+threat/2009-1001_3-252187.html.
46. MacKinlay, C.A. Event studies in economics and finance. *Journal of Economic Literature, 35* (1997), 13–39.
47. Mahdawan, R., and Prescott, J.E. Market value impact of joint venture: The effect of industry information-processing load. *Academy of Management Journal, 38* (1995), 900–915.
48. Maiwald, E. *Network Security: A Beginner's Guide.* Berkeley: Osborne/McGraw-Hill, 2001.
49. Markoff, J. Stung by security flaws, Microsoft makes software safety a top goal. *New York Times,* January 17, 2002, C1.
50. McWilliams, A., and Siegel, D. Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal, 40,* 3 (1997), 626–657.
51. Menzar, M.B.; Nigh, D.; and Kwok, C.C.Y. Effect of announcements of withdrawal from South Africa on stockholder wealth. *Academy of Management Journal, 37,* 6 (1994), 1633–1648.

52. Mikhail, M.; Walther, B.; and Willis, R. Do security analysts improve their performance with experience? *Journal of Accounting Research, 35* (Suppl.) (1997), 131–157.
53. Miller, I., and Miller, M. *John E. Freund's Mathematical Statistics* (6th ed.). Upper Saddle River, NJ: Prentice Hall, 1999.
54. Mitchell, M., and Netter, J. Triggering the 1987 stock market crash: Antitakeover provisions in the proposed house ways and means tax bill? *Journal of Financial Economics, 24* (1989), 37–68.
55. Nersey, C. Hacker scare again boosts security stocks. Available at www.internetnews.com/bus-news/article.php/573961.
56. Olsen, C., and Dietrich, R. Vertical information transfers: The association between retailers' sales announcements and suppliers' security returns. *Journal of Accounting Research, 23* (1985), 144–166.
57. Otchere, I. Two decades of information transfer studies: A review. *Accounting Research Journal, 15,* 1 (2002), 21–38.
58. Pastore, M. Companies lack understanding of information security. ClickZ, October 10, 2001. Available at http://cyberatlas.internet.com/big_picture/hardware/article/0,1323,5921_900911,00.html.
59. Penrose, E.T. *The Theory of the Growth of the Firm.* New York: John Wiley, 1959.
60. Peteraf, M.A. The cornerstones of competitive advantage: A resource-based view. *Strategic Management Journal, 14* (1984), 179–191.
61. Power, R. 2002 CSI/FBI computer crime and security survey. *Computer Security Issues and Trends, 8,* 1 (2002).
62. Rajgopal, S.; Venkatachalam, M.; and Kotha, S. Managerial actions, stock returns, and earnings: The case of business-to-business internet firms. *Journal of Accounting Research, 40,* 2 (May 2002).
63. Reinganum, M.R. Misspecification of capital asset pricing: Empirical anomalies based on earnings yield and market values. *Journal of Financial Economics,* 9 (March 1981), 19–46.
64. Rombel, A. Internet security in an insecure world. *Global Finance, 15,* 13 (December 2001), 28–32.
65. Rubin, P.H. The expansion of firms. *Journal of Political Economy, 81* (1973), 936–949.
66. Schipper, K. Information transfers. *Accounting Horizons, 4* (1990), 94–107.
67. Seth, A. Value creations in acquisitions: A reexamination of performance issues. *Strategic Management Journal, 11* (1990), 99–115.
68. Shelton, L. Strategic business fits and corporate acquisition: Empirical evidence. *Strategic Management Journal, 9* (1988), 278–288.
69. Subramani, M., and Walden, E. The game of the name: A comparison of capital market reactions to dotcom vs. traditional name changes. MISRC Working Paper No. 00-15. University of Minnesota, Carlson School of Management, July 18, 2001. Available at http://misrc.umn.edu/workingpapers/fullPapers/2000/0015_071800.pdf.
70. Subramani, M., and Walden, E. The impact of e-commerce announcements on the market value of firms. *Information Systems Research, 12,* 2 (June 2001), 135–154.
71. Trueman, B.; Wong, M.H.; and Zhang, X.J. The eyeballs have it: Search-

ing for the value in internet stocks. *Journal of Accounting Research, 38* (2000), 137–162.
72. Warner, B. Internet firm hacked out of business. Reuters, February 1, 2002. Available at http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2844881,00.html.
73. Wenderfelt, B. A resource based view of the firm. *Strategic Management Journal, 5* (1984), 171–180.
74. White, H. A heteroscedasticity-consistent covariance matrix estimator and a direct test for heteroscedasticity. *Econometrica, 48,* 4 (1980), 817–838.
75. Zhu, K., and Kraemer, K.L. E-commerce metrics for net-enhanced organizations: Assessing the value of e-commerce to firm performance in the manufacturing sector. *Information Systems Research, 13,* 3 (2002), 275–295.

Appendix A: Illustrative Samples of Internet Security Breach Announcements

Example of a Single Security Breach Announcement

Source: CNet News.Com
Time: January 10, 2000
Title: FBI Probes Extortion Case at CD Store

> Taking advantage of an apparent security breach in CD Universe's database, a hacker posted links to potentially thousands of customer names, addresses, and credit card numbers after purportedly failing to extort money from the on-line music store. The hacker, who goes by the name "Maxus," claimed to have tapped into an estimated 350,000 user names and credit cards from CD Universe. Before posting access to the information through a Web site identified only by its IP address, he demanded $100,000 from the Connecticut-based Web store. In a statement issued today, eUniverse, which owns CD Universe, acknowledged that a portion of its customer data had been stolen. The company said it had notified the FBI after the hacker attempted blackmail. The FBI shut Maxus' Web site Saturday after it was discovered, the company said.

Example of a Multiple Security Breach Announcement

Source: CNet News.Com
Time: February 15, 2001
Title: Hackers Attack HP, Compaq, Others

> A group of Internet vandals calling themselves Sm0ked Crew has hit the Web sites of technology giants such as Hewlett-Packard, Compaq Computer, Gateway. Late Wednesday, Attrition.org, an independent organization that records hacking incidents, reported that Sm0ked Crew had defaced HP's e-learning site, a Compaq Europe, Middle East, and Africa page. Wednesday morning, the affected HP and Compaq sites still carried a message from the hackers: "Admin, You just got Sm0ked. This site was hacked by Sm0ked crew. Hacked by splurge and The-Rev. Greetz

dislexik, nouse, system33r, italguy, B_Real and anyone I forgot, sm0kedcrew@hushmail.com."

Appendix B: List of Internet Security Firms

This is a list of security firms traded in the United States. The list was compiled from two sources: INFOSYSSEC, the security portal for information system security, and *Information Security Magazine,* the leading magazine of the security industry. A careful investigation of the firms on the list found that IT security was not the core business for some of them. The business description of each firm was checked in Yahoo Finance. If security was not mentioned there, the firm was dropped from the list. Sixteen firms were dropped because their core businesses did not include security. An asterisk indicates that the firm was dropped from the list.

ID	Company	ID	Company
1*	Hewlett Packard Co.	29*	Lucent Technologies Inc.
2*	International Business Machines Co.	30	Axent Technologies Inc.
3*	National Service Industries Inc.	31*	S1 Co.
4*	Schlumberger Ltd.	32*	Electronic Data Systems Co.
5*	Unisys Co.	33	Check Point Software Tech Ltd.
6	Computer Associates Intl Inc.	34	V-One Co.
7	Datakey Inc.	35	Sac Technologies Inc.
8*	3COM Co.	36	Verisign Inc.
9*	Novell Inc.	37	Internet Security Systems Inc.
10*	Sun Microsystems Inc.	38	Bindview Development Co.
11*	Microsoft Co.	39	Pilot Network Services Inc.
12	Rainbow Technologies Inc.	40	Entrust Technologies Inc.
13	Netegrity Inc.	41	Network1 Security Solutions Inc.
14	Symantec Co.	42	Hifn Inc.
15	ZixIt Co.	43	Trend Micro Inc.
16*	Cisco Systems Inc.	44	Netiq Co.
17	Identix Inc.	45	Watchguard Technologies Inc.
18*	Bmc Software Inc.	46	Tumbleweed Communications Co.
19	Intrusion Com Inc.	47*	Red Hat Inc.
20	Networks Associates Inc.	48	Baltimore Technologies Pl
21	Safenet Inc.	49	Predictive Systems Inc.
22	Saflink Co.	50*	Akamai Technologies Inc.
23	Wave Systems Co.	51	Sonicwall Inc.
24	Cyberguard Co.	52	Mcafee Com Inc.
25	Rsa Security Inc.	53	ActivCard S.A.
26	Secure Computing Co.	54	Vasco Data Sec Intl Inc.
27	Aladdin Knowledge Systems	55	Gemplus International S.A
28	Cylink Co.	56	Jawz Inc.

HUSEYIN CAVUSOGLU (huseyin@tulane.edu) is an assistant professor of information and operations management at the A.B. Freeman School of Business at Tulane University. He received his Ph.D. in management science with a specialization in MIS from the University of Texas at Dallas. He has presented his work at the International Conference on Information Systems (ICIS), Workshop on Information Systems and Economics (WISE), Workshop on Information Technology and Systems (WITS), Americas Conference on Information Systems (AMCIS), and other conferences, and has pa-

pers forthcoming in *Communications of the ACM* and *Decision Analysis.* His major research interests are in the areas of information economics, assessment of the value of IT security, and IT security management. He is a member of AIS and INFORMS.

BIRENDRA MISHRA (barry.mishra@ucr.edu) is an assistant professor of accounting in the School of Management at the University of California, Riverside. He received his Ph.D. in business with a specialization in accounting from the University of Texas at Austin. His research areas include management accounting and management control issues, disclosure, policy-making and regulatory issues, information sharing in supply chains, and IT security. He has published in *Journal of Accounting Research, Marketing Science, Management Science, Journal of Accounting and Public Policy, Journal of Management Accounting Research, Journal of Business Research,* and *American Institute of Chemical Engineers Journal.*

SRINIVASAN RAGHUNATHAN (sraghu@utdallas.edu) is an associate professor of management information systems in the School of Management at the University of Texas at Dallas. He received his Ph.D. in business from the University of Pittsburgh. His research interests concern the economics of information systems. He has published in *Management Science, Information Systems Research, Journal of Management Information Systems,* and *IEEE Transactions.*