

The Financial Impact of IT Security Breaches: What Do Investors Think?

Ashish Garg, Ph.D., Jeffrey Curtis, and Hilary Halper

Internet security is a pervasive concern for all companies. While many previous studies have attempted to quantify financial losses resulting from IT security breaches, reliance on self-reported survey data has undermined the credibility of their results. Using an event-study methodology, this article analyzes the financial impact of cyber-breaches, by measuring the stock market reaction, and reveals several new perspectives.

First, the actual losses on a per-incident basis are substantially greater than previous studies indicate. We estimate that security incidents can cost companies between \$17 and \$28 million per incident or 0.5 to 1.0 percent of annual sales for the average publicly listed company. Second, investor reactions to IT breaches extend to more than the breached party; they also “spill over” to Internet security vendors and insurance carriers. In general, security solution vendors experienced a share price increase in the range of 1 to 3 percent. In contrast, P&C (Property & Casualty) insurance carriers

experienced an initial fall in share price but more recently have experienced share price increases in the range of 1 to 2 percent.

Given the current economic environment, executive management teams are particularly sensitive to the preservation of shareholder value. This directive includes mitigating various types of corporate and business risk, including the E-security risk. However, a lack of credible estimates on the economic losses and financial impact of cyber-incidents has somewhat constrained the ability of decision makers and risk managers to make optimal decisions. By providing rigorous quantitative estimates, this study provides companies with a framework to better evaluate risk management investments. The empirical evidence presented here rejects the often-perceived dichotomy between insurance and security investments. The current market expectation is that “at-risk” companies will invest in *both* insurance and security to mitigate electronic commerce-related risk.



ASHISH GARG, PH.D., is a senior manager, and JEFFREY CURTIS and HILARY HALPER are senior consultants in Ernst & Young LLP's Economic and Business Analytics Practice. Garg has published extensively in the economics of IT and costing analytics solutions. Based in New York, their focus is on deploying robust financial analytics to validate strategy/business models and creating integrated solutions that drive value for global companies.

IMPORTANCE OF INFORMATION SECURITY

Without a doubt, information security is a pervasive concern for all companies and continues to rise in importance. IT security is now considered a mainstream operational concern as companies utilize the Internet as a key driver of E-business and greater collaboration. While the exigencies of E-commerce require that the Internet be safe and secure, the reality is drastically different. Various economy-wide surveys reveal that between 36 and 90 percent of organizations reported computer security breaches in the past year.¹

As adoption and dependence on the Internet grows, electronic collaboration will accelerate rapidly as organizations see the impact on their bottom lines. However, concerns over security and associated issues continue to be listed as a top challenge, hindering the multibillion dollar potential of B2B (business-to-business) and B2C (business-to-consumer) opportunities.² In addition to the growth of E-commerce, several significant changes driven by the forces of globalization and the regulatory environment make information security an even greater area of concern. Examples of such laws include the HIPAA (1996), COPPA (1998), and Gramm-Leach-Bliley Act (1999) that require thorough safeguards to protect the security and confidentiality of nonfinancial data, individual medical records, and the privacy of children on the Internet.

ECONOMIC IMPACT OF INFORMATION SECURITY

The degree to which you can express something in numbers is the degree to which you really understand it.

—William Thompson, “Lord Kelvin”
(1824–1907)

Despite the rise in information security incidents, few studies exist that satisfactorily quantify the economic impact of E-security incidents on the breached companies. Most of the estimates are based on self-reported surveys such as those conducted by the CSI/FBI, CERT, and other organizations.

As an illustration, according to the widely cited survey by the CSI/FBI, companies reported a total loss of \$456 million for IT security-related incidents in 2002. However, given that *only* between 10 and 20 percent of detected incidents are actually reported, while informative, this estimate could likely be a significant underestimate.³

Many macro studies similar to the CSI/FBI survey have estimated that security breaches cost companies between \$13 billion and \$1.6 trillion a year (explained in detail in [Exhibit 4](#)). For corporate policy makers, these surveys yield little utility as risk managers and IT decision makers are left with a wide range of estimates to intuit the financial impact of information security incidents. This is perhaps all the more surprising given that many of these studies use the identical self-reported survey methodology and analyze comparable samples in similar time periods. The lack of convergences in estimates from these surveys further highlights the issue that quantification of E-security has been quite challenging. One important obstacle has been that impact analysis requires estimating both tangible (loss to revenues, damages to computer systems, etc.) and intangible effects (loss of reputation, intellectual property, etc.).

As an alternative to self-reported surveys, this article proposes to analyze the financial impact of information breaches on corporations using an event-study methodology.⁴ If the markets are efficient (i.e., they react efficiently to all publicly available information), then *all the present and future effects of a publicly reported security breach are captured in the stock price*. The principal aim of this study is to provide policy makers and risk managers with more consistent estimates of the financial impact of security breaches, as an alternative to self-reported surveys. A comprehensive risk management framework entails that E-security breaches should extend to more than just the breached party. To test this hypothesis, this study analyses market reactions of information breaches on Internet security vendors and P&C insurance carriers.

EVENT-STUDY METHODOLOGY

Event-study methodologies have been used extensively in management science and finance to measure the impact of various corporate events, ranging from mergers to regulatory changes, on shareholder value. Event-study methodology is based on the *semistrong version* of the efficient markets hypothesis,⁵ which maintains that as new publicly available information is received, it is immediately absorbed by investors and incorporated into share prices. As such, *the current and future impact* of an event, for instance, a security breach, is measured by the abnormal change in the daily share price of the affected company.

Identification and Selection of Events

For this study, the relevant universe of events was compiled from a comprehensive review of security breach announcements available via Bloomberg, Dow Jones Interactive (DJI), and the few thousand publications in those archives. Both Bloomberg and DJI are widely considered to be the primary authoritative sources of significant news and real-time information to Wall Street traders and market investors. We searched these two popular financial data sources using keywords such as “security incident,” “hacker attack,” “IT incident,” “security breach,” and all variations and synonyms of these expressions to identify the widest universe of events possible from 1996 to 2002 and identified 49 events. By further screening these events for confounding news such as earnings announcements, analyst upgrades, and executive resignations, we arrived at 22 distinct events for our sample.

We chose not to include viruses in our universe. This is largely because viruses are systemic in nature; that is, they affect a large number of companies at the *same* time. Hence, it is difficult to accurately isolate the impact of a virus attack on an individual company. Including viruses, we are much more likely to pick up self-selection bias reporting than for distributed E-security incidents such as denial-of-service or Web site defacements.

EVENTS DESCRIPTION

The security incidents in this study can be divided into three main periods for the purposes of analysis (see [Exhibit 1](#)).

The Early Events:

December 1996 to February 2000

The earliest event in our study is August 1999 when the Microsoft Hotmail Web site was defaced and customer accounts were accessed (see [Exhibit 1](#)). Other events in this period include hacking of the Staples.com site and the more malicious attack on the Internet music store CD Universe, when a supposed Russian hacker stole over 300,000 customer credit card numbers. Until this point, hack attacks had been intermittent and had not received a great deal of public attention. This all changed in February of 2000.

The February 2000 Denial-of-Service Attacks: The Watershed

In February 2000, a series of well-orchestrated distributed denial-of-service (DDoS) attacks occurred that permanently changed the public perception of Internet attacks. The affected companies were some of the biggest icons of the Internet, such as Amazon, Yahoo, and eBay. Unlike earlier breached parties, the companies attacked either rely solely or heavily on the Internet for business. The first in the series of attacks occurred on February 7, 2000, when Yahoo suffered a deluge of service requests, a magnitude greater than its normal volume, in the span of seconds, in effect crippling the site. The following day, February 8, Buy.com, eBay, CNN, MSN, and Amazon were all attacked in a similar manner to Yahoo. Buy.com was making its IPO debut when its Web site crashed due to a denial-of-service (DoS) attack. To conclude the series, the attacks continued on Wednesday, February 9, with ZDnet and E*Trade experiencing difficulties in the early hours of the morning, and then Excite, which was affected in the evening.

According to many industry observers (and as results indicate), the wave of DoS

EXHIBIT 1 Company Reaction to Security Incidents

Company	Type of Breach	Date of Announcement	Cumulative Abnormal Return			Implied Change in Market Cap (\$ millions)
			T (%)	T to T+1 (%)	T to T+2 (%)	
Microsoft	Theft of customer information	8/30/99	1.4	2.1	0.7	6,765.1
Staples	Web site defacement	10/11/99 ^a	-0.3	4.6	0.9	(37.2)
eUniverse (CD Universe)	Theft of credit card information	1/10/00	-18.0	-20.7	-24.8	(15.4)
Yahoo	Denial-of-service	2/7/00	-3.4	-2.8	-2.7	(3,168.9)
eBay	Denial-of-service	2/8/00	-3.7	-4.8	-10.1	(815.0)
Microsoft	Denial-of-service	2/9/00 ^{a,b}	-3.1	-1.5	-0.1	(17,643.5)
Amazon	Denial-of-service	2/9/00 ^a	-0.5	-10.5	-4.4	(152.1)
Time Warner (CNN)	Denial-of-service	2/9/00 ^a	2.1	1.6	1.8	2,253.2
E*Trade	Denial-of-service	2/9/00	-2.0	-5.8	-4.7	(132.6)
ZDNet	Denial-of-service	2/9/00	2.6	-3.2	-3.3	12.0
Excite@Home	Denial-of-service	2/10/00	-3.3	-3.2	-5.9	(453.4)
RSA Security	Web site defacement	2/14/00 ^{a,b}	-9.5	-20.6	-17.2	(249.0)
National Discount Brokers	Denial-of-service	2/24/00	4.1	-1.8	-9.4	20.2
Nike	Web site defacement	6/21/00	-0.3	0.1	6.0	(26.7)
First Data (Western Union)	Theft of credit card information	9/8/00 ^b	-5.7	0.2	-0.8	(1,022.9)
Egghead.com	Theft of credit card information	12/18/00 ^b	-12.3	-15.5	-36.1	(6.4)
Travelocity	Theft of customer information	1/23/01	-2.3	-3.7	2.3	(23.2)
Microsoft	Denial-of-service	1/25/01	-0.9	3.0	3.0	(3,148.0)
Diageo (Burger King)	Web site defacement	3/2/01	1.9	2.5	-1.0	663.1
British Telecom	Web site defacement	4/2/01	-2.3	-1.5	5.4	(1,146.4)
HSBC	Web site defacement	9/21/00	-1.6	-1.2	-0.6	(1,869.0)
Playboy	Theft of credit card information	11/21/01	-1.1	-0.1	2.2	(3.7)
	Average		-2.7	-3.8	-4.5	(918.2)
	Significance level^c		95+	95+	90+	
	Implied total					(20,199.7)
	Average Market Cap (Excluding MSFT)					27,325.1
	Average Market Cap (Including MSFT)					86,346.7

^a Indicates that announcement was released after the close of trading on the previous trading day.

^b Indicates that the event is statistically significant.

^c Significance level of series of events using Wilcoxon test.

attacks in 2000 were the first to pop up on the radar screen of the business community and served as a wake-up call to technology-reliant companies, and to investors who derived clear implications for cyber-risk management. These attacks showed the true vulnerabilities of the Internet and heightened awareness on the financial impacts of security breaches, including the lost revenue due to downtime, systems recovery costs,

and damage to brand reputation and customer perception.

Other Recent Events: February 2000 to May 2002

Some of the more publicized events since the February 2000 DoS events have included the September 2000, theft of credit card data from the Western Union Web site. Also, internationally outside the United

The results of the event study show that the average abnormal fall in share price attributable to a security incident is estimated as 2.7 percent over one day.

States, Burger King and British Telecom had their Web sites defaced in early 2001.

DISCUSSION OF KEY RESULTS

Impact on the Breached Party

The results of the event study show that, for the 22 events studied (1996 to 2002), the average abnormal fall in share price attributable to a security incident is estimated as 2.7 percent over one day, increasing to 4.5 percent over a three-day period, indicating both persistence and delayed market reaction. Also, all these reactions were statistically significant.⁶ It is also noteworthy that stocks of impacted company in 17 of the 22 events (or 77 percent) had an initial negative, same-day reaction to an E-security breach. Combined, these events represent a combined loss of \$20.2 billion or, at an average loss of \$918 million per incident (see [Exhibit 1](#)), a significant loss in stock market value in a period of days.

A general caveat on the interpretation of these results is that these results are not representative of the wider population of non-public or non-Internet-dependent companies. The average company in the sample has a market cap in excess of \$86 billion and many of the companies are Internet pure-plays, companies such as Amazon, Yahoo, eBay, Travelocity, etc. While these results still reveal the market perception of publicly known breaches of security, they cannot be literally extrapolated to the domain of all major U.S. corporations (public or private, Internet, and brick-and-mortar alike).

Impact on Security Vendors and Insurance Carriers

In addition to the impact on the breached parties, *a priori* E-security incidents could have wider inter-industry impacts beyond just the breached party. In this study we specifically tested for the spillover impacts on two sectors: E-security vendors and P&C insurance carriers. This is because, from the

risk managers' point of view, increased investments in both Internet security and insurance are valid strategies for mitigating cyber-risk. Information security risk that cannot be completely alleviated by spending on Internet security solutions such as firewalls, intrusions detections systems, etc. can be diversified away by extra insurance. Hence, a comprehensive risk management framework entails implications (that are testable) on the spillovers effects of cyber-breaches on both the Internet security and the insurance sectors.

Internet Security

The magnitude of spillover impacts on E-security stocks depends critically on the market perception of the optimal level of investment in security technologies. For example, if financial markets perceived that the breached companies were investing optimally in security technologies, one would have expected a neutral response on the market value of security solution providers. In contrast, if investors perceived the attacks as a sign of suboptimal investments in IT security and a signal to increase E-security spending in the future, Internet security sector stock prices would rise perceptibly.

Our results indicate (see [Exhibit 2](#)) that Internet security stocks, in general, responded positively to security breaches, with increases between 0.9 and 3.3 percent on average for all events. However, data analysis confirms that the positive market reaction was further amplified *before* the DoS events of February 2000. The average (market weighted) reaction of Internet security stocks before these events was a positive 3.8 percent on the same day, increasing to 10.3 percent over three days.⁷ More formal regression analysis (not presented in this article) indicates that February 2000 was an empirical watershed — a clear delineation — when the markets dramatically adjusted their expectations. Thereafter,

EXHIBIT 2 E-Security Company Index Reaction to Security Incidents

Company	Type of Breach	Date of Announcement	Cumulative Abnormal Return			Total Index Market Cap (\$ millions)	Implied Change in Market Cap (\$ millions)
			T (%)	T to T+1 (%)	T to T+2 (%)		
Microsoft	Theft of customer information	8/30/99	2.2	5.9	9.7	15,909.8	1,543.2
Staples	Web site defacement	10/11/99	-1.5	-1.7	-2.4	25,545.7	(613.1)
eUniverse (CD Universe)	Theft of credit card information	1/10/00 ^b	4.5	0.7	1.1	43,697.9	480.7
Yahoo	Denial-of-service	2/7/00	1.4	1.2	9.6	47,470.8	4,557.2
eBay	Denial-of-service	2/8/00	-0.2	8.3	19.9	48,135.4	9,578.9
Microsoft, Amazon, Time Warner (CNN), E*Trade, ZDNet	Denial-of-service	2/9/00 ^b	8.5	20.1	20.9	50,921.9	10,642.7
Excite@Home	Denial-of-service	2/10/00 ^b	11.6	12.3	13.6	57,706.5	7,848.1
	Average		3.8	6.7	10.3	41,341.1	4,275.9
	Significance Level^c		90+	90+	95+		
RSA Security	Web site defacement	2/14/00	1.3	3.9	3.1	58,080.5	1,800.5
National Discount Brokers	Denial-of-service	2/24/00	0.1	3.3	2.2	59,342.9	1,305.5
Nike	Web site defacement	6/21/00	1.7	1.2	1.7	50,400.2	856.8
First Data (Western Union)	Theft of credit card information	9/8/00	-2.1	-5.6	-5.2	52,609.6	(2,735.7)
Egghead.com	Theft of credit card information	12/18/00	0.5	-6.1	-9.4	50,707.4	(4,766.5)
Travelocity	Theft of customer information	1/23/01	-0.5	-0.4	-1.3	43,932.9	(571.1)
Microsoft	Denial-of-service	1/25/01	-0.9	2.4	5.7	45,546.6	2,596.2
Diageo (Burger King)	Web site defacement	3/2/01*	-6.6	-13.3	-7.4	44,893.6	(3,322.1)
British Telecom	Web site defacement	4/2/01	-1.5	-1.6	0.3	32,666.2	98.0
HSBC	Web site defacement	9/21/00	-2.6	-3.1	-2.7	22,887.2	(618.0)
Playboy	Theft of credit card information	11/21/01	1.0	-1.4	-0.2	26,189.8	(52.4)
Midwest Express	Theft of customer information	4/26/02					
	Average		-0.9	-1.9	-1.2	44,296.1	(531.55)
	Significance Level^c		NM	NM	NM		
	Total						3,744.30

^a Indicates announcement was released after the close of trading on the previous trading day.

^b Indicates that the event is statistically significant.

^c Significance level of series of events using Wilcoxon test.

breaches would only marginally influence E-security-sector share prices as most of the news of increased security spending was *already factored-in* stock prices.

As expected past the turning point of February 2000, security breaches had a negative, albeit small impact on Internet security stocks. Also, none of these negative reactions are statistically significant at the appropriate level of confidence. This further reinforces the conjecture that most of the

news and information on the increased spending on Internet security was already factored in share prices.

Cyber-Insurance

As observed in the case of Internet security vendors, there is a possibility that cyber-attacks could have a potential spillover impact on insurance carriers. This is because, along with Internet security vendors, P&C insurance carriers have a crucial

role in cyber-risk management. Recognizing the business potential of E-risk services, P&C insurance carriers have been offering cyber-insurance policies at least since 1997. By most industry estimates, E-insurance is a high growth business and in 2001 alone, premium income was estimated to be in the \$100-million range.

For insurance carriers, the expected stock price reaction to IT security incidents depends on two opposing effects. First, there is the anticipation in the *increased* cyber-insurance business in the future. This effect is similar to that for the security solution providers and should lead to an unambiguous increase in share price. The countervailing effect is the investor perception of increased payouts by insurers on their *existing* commercial general liability (CGL) and business interruption (BI) policies. This is an understandable and genuine concern. According to many industry analysts, there is some debate within the insurance industry as to whether existing insurance policies cover Internet-related losses. In the view of an industry analyst:⁸

Many standard commercial insurance policies do not cover or recognize losses from denial-of-service attacks, virus infection or intellectual property violations — instead, insurance forms are increasingly offering dedicated ‘cyber’ policies. **However, there is very little awareness about this.**

Also to further muddy the waters, in recent decisions the courts have taken differing positions on whether or not lost computer data constitutes a physical loss to tangible property and hence is covered under existing CGL policies. For example, in the often-cited Ingram Micro case,⁹ an Arizona district judge ruled the loss of computer access and functionality caused by computer viruses, hacker attacks and power outages may be part of the business interruption policies. However, industry analysts claim that two recent court cases, popularly known as the AOL and Midwest Computer cases, have upheld insurance carriers’ claims that standard business policies do not

cover damages to data and other nontangibles.¹¹

Our results reveal (see [Exhibit 3](#)) that in security breaches up until the DoS attacks of February 2000, insurance company stocks were negatively impacted. The (market-weighted) average reaction was a –1.9 percent on the same day, –2.2 percent over two days, and –2.0 percent over a three-day period. All these reactions were statistically significant. On a market cap basis, the 23 P&C insurance carriers (in our sample) lost a total of \$16.6 billion in shareholder value — a significant loss of shareholder value in just four days. This negative reaction could have been driven by market perceptions of increased payout by carriers for first- and third-party losses due to ambiguity in existing CGL and BI contracts.

By comparison, the market reaction to the post-February 2000 events for the P&C insurance sector (see [Exhibit 3](#)) was generally positive. The market reaction to a cyber-breach to insurance-sector investors was a positive 0.7 percent, increasing to 1.4 percent over two days and 1.7 percent over three days.¹² This positive reaction is similar to that observed for the Internet security stocks (although smaller in magnitude) and could be explained by investor anticipation of increased cyber-insurance premiums. The 2000 DoS events have served to heighten awareness of cyber-incidents stimulating both the demand for special coverage and, on the supply side, the availability of coverage from P&C insurance carriers.

COMPARISON WITH OTHER STUDIES

This section contrasts our results with other comparable studies that have also measured economic impact of security incidents (see [Exhibit 4](#)). These studies have been sorted with respect to their event coverage, methodology, and grouped by category. As a general description on their methodology, most of these studies have relied on self-reported company surveys to report the financial impact of security breaches. As such, two concerns could dent the credibility of these

EXHIBIT 3 P&C Insurance Company Index Reaction to Security Incidents

Company	Type of Breach	Date of Announcement	Cumulative Abnormal Return			Total Index Market Cap (\$ millions)	Implied Change in Market Cap (\$ millions)
			T (%)	T to T+1 (%)	T to T+2 (%)		
Microsoft	Theft of customer information	8/30/99 ^b	-2.5	-2.5	-3.2	236,093.3	(7,555.0)
Staples	Web site defacement	10/11/99 ^b	-1.6	-2.4	-3.3	220,573.7	(7,278.9)
eUniverse (CD Universe)	Theft of credit card information	1/10/00 ^b	-2.7	-2.8	-0.1	245,119.1	(245.1)
Yahoo	Denial-of-service	2/7/00 ^b	-2.4	-5.6	-3.5	224,727.6	(7,865.5)
eBay	Denial-of-service	2/8/00 ^b	-3.1	-1.1	-4.0	220,335.2	(8,813.4)
Microsoft, Amazon, Time Warner (CNN), E*Trade, ZDNet	Denial-of-service	2/9/00 ^b	2.0	-0.9	1.7	219,522.2	3,731.9
Excite@Home	Denial-of-service	2/10/00	-2.9	-0.4	-1.7	214,003.2	(3,638.1)
	Average		-1.9	-2.2	-2.0	225,767.8	(4,547.6)
	Significance Level^c		95+	95+	95+		
RSA Security	Web site defacement	2/14/00	-1.2	0.6	0.2	212,500.6	425.0
National Discount Brokers	Denial-of-service	2/24/00 ^b	-1.9	-0.1	1.8	195,711.8	3,522.8
Nike	Web site defacement	6/21/00	0.1	1.3	3.6	260,548.5	9,379.7
First Data (Western Union)	Theft of credit card information	9/8/00 ^b	2.5	5.4	6.7	302,478.4	20,266.1
Egghead.com	Theft of credit card information	12/18/00	1.9	-0.4	1.1	303,395.7	3,337.4
Travelocity	Theft of customer information	1/23/01	0.7	3.5	4.4	340,706.7	14,991.1
Microsoft	Denial-of-service	1/25/01	0.5	2.0	2.8	305,590.0	8,556.5
Diageo (Burger King)	Web site defacement	3/2/01	0.9	0.0	-1.0	313,029.8	(3,130.3)
British Telecom	Web site defacement	4/2/01 ^b	0.7	-0.2	-2.1	300,041.4	(6,300.9)
HSBC	Web site defacement	9/21/00	2.8	1.9	-1.0	301,168.4	(3,011.7)
Playboy	Theft of credit card information	11/21/01	-0.3	-0.2	-0.4	315,317.0	(1,261.3)
Midwest Express	Theft of customer information	4/26/02					
	Average		0.7	1.4	1.7	286,408.0	4,725.73
	Significance Level^c		NM	90+	90+		
	Total						178.12

^a Indicates announcement was released after the close of trading on the previous trading day.

^b Indicates that the event is statistically significant

^c Significance level of series of events using Wilcoxon test

results. The first issue is that it is in the interest of the impacted company not to report, or to “underreport,” the actual financial impact of an IT security breach. In fact, the results from this study provide adequate support that publicly announced breaches can lower shareholder value quite significantly and hence the inherent incentive to underreport breach incidents. Second, in the determination of losses associated with a breach, a disproportionate emphasis has

been placed on immediate tangible losses, such as costs of replacing damaged systems and loss of income. The combination of these elements has generally been a significant obstacle in objectively and rigorously quantifying the impact of breaches in IT security.

Several other studies (from 2.1–2.4, listed in [Exhibit 4](#)) have focused exclusively on the February 2000 DoS attacks. Among them were the Yankee Group (2000), which

EXHIBIT 4 Comparison with Other Studies

	Study	Methodology/ Events Analyzed	Economic Impact
	Ernst & Young	Event study, all IT security incidents (excluding viruses) impacting U.S. public companies, 1996–2002	2.7%–4.5% fall in share price Loss of \$918MM in market cap. per incident \$17–\$28MM per incident for avg. publicly company
1.0	Riverhead Networks (2002)	1/2001 attack on Hotmail (MSFT)	\$500MM for the specific incident
2.1	Workforce (2000)	DoS events of February 2000	\$500K–\$1MM for each DoS attack
2.2	Yankee Group (2000)	DoS events of February 2000: Cumulative Loss	\$1.2 B for all attacks
2.3	Computer Economics Institute (2002)	DoS Events of February 2000: Cumulative Loss)	\$10.9 MM in lost revenue
2.4	Ettredge and Richardson (2001)	Event Study; DoS Events of February (2000) attacks	Loss in share price of 6% for B2B firms and 7.8% of B2C firms
3.1	Datamonitor (2000)	All E-security breaches, including virus attacks; 2000 survey	\$15B worldwide
3.2	Computer Economics Institute (2002)	All types of malicious attacks, including viruses; 2001 survey	\$13.2B worldwide
3.3	InformationWeek/PwC/Reality Research & Consulting (2001)	All E-security breaches including virus attacks; survey of 4900 firms in 30 countries in 2001	\$1.6 trillion dollars, worldwide annually U2.5% of GDP. \$266 billion for the U.S.
3.4	Prof. Frank Bernhard, UCD/Omni Consulting (2001)	All E-security breaches, including virus attacks; “economic leakage”; survey of 3000 businesses in the U.S. in 2001	5.7–7 % of annual revenue
4.1	DTI/PwC (2002)	All security breaches; survey of U.K. firms in 2002	\$50K (GBP 30K) per incident
4.2	KPMG (2002)	All security breaches; survey of 641 U.K. firms in 2002	\$120K (GBP 77K) per incident
4.3	CSI/FBI survey (2002)	All E-security breaches, including virus attacks; Survey of 503 U.S. firms in 2002	\$2.05MM per incident
5.1	Forrester Research (1998)	Tangible and intangible effects of a security breach; bottom-up study	\$21MM to \$106MM per incident
6.1	Cavusoglu et al. (2002)	Event study for all types of breaches	2.1% fall in share price of breached company

estimated a combined impact of \$1.2 billion, and the Workforce (2000) study that cited the losses as little as \$500,000 to \$1 million per event. Our study reveals that in terms of shareholder value, total losses were several times higher than either of these estimates. More specifically, our estimate of the loss of market value of the February 2000 events, is approximately \$20.5 billion, nearly 20 times greater than that estimated by the often-cited Yankee Group study.

Other broader surveys (from 3.1–3.4, listed in Exhibit 4) have estimated the financial loss to be between 2.5 percent¹³ and 5.7 percent¹⁴ of company revenue. Our results indicate that the stock market reaction to a security incident is on the order of

2.7 to 4.5 percent of market cap value. At an average market cap to sales ratio of 6 (from our sample), this translates to a 0.45 to 0.75 percent loss in equivalent annual revenue per incident. However, to compare this estimate with the others surveys, we factor in the probability of attacks and allow for the possibility of multiple incidents in the same year. Adjusting for both these variables, we compute that, in aggregate, security incident costs could be between 1.0 and 1.5 percent of sales for the corporate sector. This estimate places our results in a lower range than those obtained by self-reported surveys (2.5 to 7 percent). However, we believe that the 1.0 to 1.5 percent estimate is itself a kind of upward bound. This is

because the loss estimates are based on companies (eBay, Yahoo, Amazon) that are generally more Internet dependent than the average company.

In terms of per-incident costs, comparable surveys (from 4.2–4.3, see [Exhibit 4](#)) have been quite variable, with estimates ranging from \$50,000 per incident¹⁵ (PricewaterhouseCoopers/DTI) to \$2.05 million per incident for the CSI/FBI survey. An alternative approach by Forrester Research (1998)¹⁶ (5.1. in Exhibit 4) has been to estimate the impact from a bottom-up cost model. Using enterprise-specific parameters, Forrester estimates that the costs of a security breach range from \$21 million to \$106 million per incident. It is interesting to note that in this bottom-up analysis, the impact of breaches are calculated to be ten to fifty times higher than those estimated from self-reported surveys.

The estimate of studies 3.1 through 3.4 are based on economy-wide surveys and not just on publicly listed companies, such as those in our sample. To make the appropriate comparison, we have to make the necessary market adjustments.¹⁷ The adjustment estimates reveal that per-incident costs are estimated to be between \$17 and 28 million per incident for the average publicly listed company in the United States. Once again, it is worth reiterating that these estimates are based on the major publicized events and also on companies dependent on E-commerce revenues.

CONCLUSION

In the inexorable drive of companies to reduce costs and enhance productivity, there has been an increased reliance on the Internet. As such, information security is a pervasive concern for all companies, not simply those that rely either wholly or partially on the Internet to conduct business. While many studies have attempted to quantify the magnitude of losses resulting from IT security breaches, they have yielded little utility to policy makers. This is evidenced in the highly variable range of estimates obtained using the company-reported sur-

vey technique, ranging from \$50,000 to \$2 million of the per-incident cost of a security breach. Using a novel approach of event-study methodology, this study aims to provide a more objective view — a more accurately gauge — of losses resulting from IT security incidents.

This study contains several noteworthy results. First, we posit that losses on a per-incident basis are an order of magnitude greater than many previous studies and surveys have indicated. We conclude that, on average, the loss to a company is \$17 to 28 million per incident. This translates to a 0.5 to 1.0 percent loss of corporate revenue on an annual basis.

Second, we extend the spillover effects of E-security to include investor reactions to Internet security vendors and insurance carriers. For events inclusive and prior to February 2000, stocks of security companies reacted positively (from 4 to 10 percent) to security breaches. However, post February 2000 for Internet security companies, the market response was generally lukewarm and statistically insignificant. This suggests that by mid-2000, the market had already adequately factored in the possibility of a security breach into the share prices of the Internet security sector.

Similarly, insurance carriers reacted differently pre and post the DoS incidents of 2000. In this instance, insurance companies had a negative reaction of approximately 2.0 percent to incidents prior to the February 2000 events. By contrast, security incidents events post February 2000 have elicited a positive market reaction (between 0.7 and 1.7 percent) on the P&C insurance sector.¹⁸ Insurance-sector investors were perhaps reacting favorably in anticipation of increased cyber-insurance sales and the higher premiums as a result of heightened awareness of cyber-insurance.

Given the tight corporate budgets, IT managers, risk managers, and finance policy makers require reliable quantitative estimates to make tough decisions regarding enterprise IT security. However, existing studies, based largely on self-reported surveys and with

We conclude that on average the loss to a company is \$17 to \$28 million per incident. This translates to a 0.5 to 1.0 percent loss of corporate revenue on an annual basis.

wide dispersion in estimates, have provided little guidance to decision makers. This study fills a void in the literature. Evidence from an event study indicates that security incidents can cost companies (even non-Internet-dependent ones) between \$17 and \$28 million per incident or, in aggregate, 0.5 to 1.0 percent of annual sales. A comprehensive approach to cyber-risk mitigation requires not only increased Internet security spending (currently at a meager 2 percent of corporate IT spending), but additional investments in cyber-insurance policies. The empirical evidence presented rejects the often-perceived dichotomy between insurance and security investments. The study indicates that the market has factored in both of these approaches to cyber-risk management. ■

Notes

1. Three recent surveys estimate reported breaches by organizations differently. The CSI/FBI (2002) reported that nearly 90 percent of organizations (large corporations and government agencies) reported a computer security breach in the past 12 months. A survey by Ernst & Young (2002), focused only on corporations, found that more than 75 percent of businesses had experienced some interruption of their critical business systems related to IT security; while a Meta Group (2002) survey reported that 36 percent of organizations had reported a breach in the preceding two years.
2. According to surveys by Network World (2000), security is the *single most critical* concern of IT professionals in relation to E-business, a distinction it has claimed two years in a row.
3. For further reference on an extensive review, see Chapter 4 in Bosworth S. and Kabay, M.E., Eds., *Computer Security Handbook*, 4th edition, John Wiley & Sons, New York, 2002.
4. While the "Additional References" section mentions other similar studies, the authors of this study were unaware of other similar event studies and all the research was conducted independently.
5. For more details, see Fama, E.F., Fisher, L., Jensen, M., and Roll, R., "The Adjustment of Stock Prices to New Information," *International Economic Review*, 10, 1–21, February 1969.
6. The Wilcoxon is a popular nonparametric test that takes into account the sign and magnitude of the distribution of cumulative abnormal returns.
7. The positive reactions were all statistically significant using the Wilcoxon nonparametric tests outlined earlier.
8. As an example, see Alan McGibbon, Director of Scalable Networks, July 16, 2002.
9. The full reference: *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 WL 726789 (D. Arizona 4/18/2000).
10. These cases include *State Auto Property & Cas. Ins. Co. v. Midwest Computer & Moore*, 147 F. Supp.2d 1113 (Oklahoma, 2001) and *America Online v. St. Paul Mercury Insurance Co.* (Virginia, June 20th, 2002).
11. For more details, see Salkever, Alex, "E-Insurance for the Digital Age," *Business Week Online*, April 2, 2002.
12. All these effects were positive but statistically only weakly significant.
13. "Study Finds Computer Viruses and Hacking Take \$1.6 Trillion Toll on Worldwide Economy," *Information Week*, July 7, 2000.
14. UCSD/Omni Consulting.
15. Potter, Chris and Smith, Geoff, "Information Security Beaches Survey 2002," PricewaterhouseCoopers, 2002.
16. Howe, C., McCarthy, J.C., Buss, T., and Davis, A., "The Forrester Report: Economics of Security," February 1998.
17. The average publicly listed company in the United States has a market cap of \$1229 million (S&P 1500).
18. This positive effect is similar in sign and magnitude to the "Gaining for loss" effect observed in the response of P&C stocks to catastrophes such as hurricanes and earthquakes.

Additional References

- AtomicTangerine, "NPV: Information Security," 2000.
- Benston, G.J., "Accounting Numbers and Economic Values," *Antitrust Bulletin*, 27 (Spring), 161–215, 1982.
- Bosworth, S. and Kabay, M.E., Eds., *Computer Security Handbook*, 4th edition, John Wiley & Sons, New York, 2002.
- Cavusoglu, H. et al., "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers," The University of Texas at Dallas School of Management, February 2002.
- "Financial Impact and Background Information on Distributed Denial of Service Attacks," *Computer Economics*, 2000.
- D'Amico, A., "What Does a Computer Security Breach Really Cost?," *Secure Decisions*, a division of Applied Visions, September 7, 2000.
- DeLong, D., "Hackers Said to Cost U.S. Billions," *NewsFactor Network*, February 8, 2001.
- Ettredge, M. and Richardson, V., "Assessing the Risk in E-Commerce," University of Kansas, October 2001.
- Fama, E., "Efficient Capital Markets II," *Journal of Finance*, 46(5), 1575–1617, 1991.
- Figg, J., "Cyber Insurance to Cover E-Business," *Internal Auditor*, 57(4), August 1, 2000.
- Gordon, L. and Loeb, M., "Economic Aspects of Information Security," *Rainbow Technologies*, August 26, 2001.

Greengard, S., "You've Been Hacked!," *Workforce*, pp. 24–26, April 1, 2000.

Kayab, M.E., "Studies and Surveys of Computer Crime," *Computer Security Handbook*, 4th edition, 2001.

M2Presswire, "New Report from META Group Reveals Security Investments Are Reactionary and Technology Driven," March 15, 2002.

M2Presswire, "Digital Risk Insurance Ignored by UK Businesses; Survey from Scalable Networks Reveals Lack of Awareness over IT Insurance," July 16, 2002.

McCue, A., "Cost of Each Security Breach -- GBP 77,000," vnunet.com, March 18, 2002.

McWilliams and Siegel, "Event Studies in Management Research: Theoretical and Empirical Issues," *Academy of Management Journal*, 40, 626–657, 1997.

Paliotta, A.R., "Beyond the Maginot-Line Mentality: A Total-Process View of Information Security Risk Management," *Information Systems Security*, 10(3): 21–50 (July-August 2001).

Power, R., *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*, Que, Indianapolis, 2002.

QinetiQ, "Risky Business: Understanding the Impact of a Security Breach," 2002.

Research Concepts LLC, "Trends in the Networked World," *2002 Network World 500 Research Study*, May 2002.

Siegel, C., Sagalow, T.R., and Saritella, P., "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security," *Information Systems Security*, 11(5): 33–49 (September-October 2002).

Sigmond, S.H., Ed., *Safe and Sound: A Treatise on Internet Security*, RBC Capital Markets, November 2001.

Witty, J. et al., "The Price of Information Security," *Strategic Analysis Report*, Gartner Group, June 2001.

Yamori, N. and Kobayashi, T., "Is It True that Insurers Benefit from a Catastrophic Event? Market Reactions to the 1995 Hanshin-Awaji Earthquake," Center for Pacific Basin Monetary and Economic Studies, Federal Reserve Bank of San Francisco, September 1999.

APPENDIX

1. IT Security Vendor Index

ActivCard (ADR)	ACTI	SafeNet	SFNT
Aladdin Knowledge Systems	ALDN	SSP Solutions	SSPX
Authoriszor	AUTH	TTR Technologies	TTRE
Digimarc	DMRC	Verint Systems	VRNT
Network Asscoaites	NET	Bindview Development	BVEW
RSA Security	RSAS	CyberGuard	CFW
Secure Computing	SCUR	DataKey	DKEY
Trend Micro (ADR)	TMIC	Entrust	ENTU
Vasco Data	VDSI	McAfee	MCAF
Watchguard	WGRD	Rainbow Technologies	RNBO
CheckPoint Software	CHKP	Saflink	SFLK
Cylink	CYLK	Symantec	SYMC
Diversinet	DVNT	Valicert	VLCT
Internet Security Systems	ISSX	V-One	VONE
Network-1 Security Solutions	NSSI		

Source: Hoovers.com — Industry, Security Software & Services.

2. Property & Casualty Insurance Index

The P&C Insurance Index includes P&C insurers with market capitalization in excess of \$1 billion. Companies with less than \$1 billion in market capitalization are predominantly highly specialized, regional operations and thus were excluded due to a high potential to confound the results of this study.

American International Group	AIG	American National Insurance	ANAT
Allstate	ALL	Mercury General	MCY
Chubb	CB	21st Century Insurance Group	TW
St. Paul Companies	SPC	American Financial Group	AFG
CNA Financial	CNA	Alleghany	Y
ACE Limited	ACE	White Mountains Insurance	WTM
The Progressive Corporation	PGR	HCC Insurance Holdings	HCC
Cincinnati Financial	CINF	Commerce Group	CGI
SafeCo	SAFC	W.R. Berkley	BKLY
Allmerica Financial	AFC	Ohio Casualty	OCAS
Old Republic	ORI	Alfa	ALFA
Erie Indemnity	ERIE		

Source: Hoovers.com — Industry, Property & Casualty Insurance.