

**Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?**

**L. Murphy Smith, D.B.A., CPA**

Professor of Accounting

Texas A&M University

4353 TAMU

College Station, TX 77843-4353

Phone: 979-845-3108

Fax: 979-845-0028

Email: [Lmsmith@tamu.edu](mailto:Lmsmith@tamu.edu)

**Jacob L. Smith**

Research Assistant

College Station, TX

## **Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?**

### **Abstract**

E-commerce has been a boon for business. A great deal of business activity now occurs in the realm of cyberspace on the Web. The downside of cyber-business is cyber crimes, also called electronic crime or simply e-crime. Cyber crime costs publicly traded companies billions of dollars annually in stolen assets and lost business. Further, when a company falls prey to cyber criminals, this may concern customers who worry about the security of their business transactions with the company. As a result, a company can lose future business if it is perceived to be vulnerable to cyber crime. Such vulnerability may even lead to a decrease in the market value of the company, due to legitimate concerns of financial analysts, investors, and creditors. This study first provides an overview of common cyber crimes. Second, a review is made of specific cases of publicly traded companies in news stories concerning cyber crime. Third and last, the impact of cyber crime news stories on companies' stock price is analyzed. Results suggest that not only can cyber crime cost a company directly in stolen assets, lost business, and reputation, but also can affect the company's stock performance, at least in the short run. Consequently, companies must do all that they can to avoid becoming a victim of cyber crime.

Key words: E-commerce, e-crime, cyber crime, computer fraud

## **Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?**

E-commerce has become a fundamental part of business activity. Most of this e-commerce occurs on the websites of publicly traded companies. The term 'cyberspace' refers to the electronic medium of computer networks, principally the Web, in which online communication takes place. One of the problems of e-business or cyber-business is that it is vulnerable to e-crime, also called cyber crime. Cyber crime costs publicly traded companies billions of dollars annually in stolen assets, lost business, and damaged reputations. Cash can be stolen, literally with the push of a button. If a company website goes down, customers will take their business elsewhere.

In addition to the immediate losses associated with cyber crime, when a company falls prey to cyber criminals, this may concern customers who worry about the security of their business transactions with the company. As a result, a company can lose future business if it is perceived to be vulnerable to cyber crime. Such vulnerability may even lead to a decrease in the market value of the company, due to legitimate concerns by financial analysts, investors, and creditors. This study first provides an overview of common cyber crimes. Second, a review is made of specific cases of publicly traded companies in news stories concerning cyber crime. Third and last, the impact of cyber crime news stories on companies' stock price is analyzed. Results suggest that not only can cyber crime cost a company directly in stolen assets, lost business, and reputation, but also can affect the company's stock market value, at least in the short run. Consequently, companies must do all that they can to avoid becoming a victim of cyber crime.

## **Motivation and Literature Review**

The corporate reputation or image of a company benefits from good news and suffers from bad news; the results are often a corresponding increase or decrease in the company's stock price. Prior accounting studies have examined stock market consequences of news regarding ethical behavior (McAnally et al. 2004), firm reputation and corporate governance characteristics (Fukami et al. 1997), workplace quality (Ballou et al. 2003), and firm environmental reputation (Clarkson et al. 2004).

With regard to e-commerce, prior studies have used event studies to evaluate the impact of e-commerce initiatives (Subramani and Walden 2001, Chen and Siems 2001) and to identify special characteristics of e-commerce firms to evaluate firm valuation or stock returns (Hand 2000; Trueman et al. 2000; Rajgopal et al. 2002). This study adds to the research literature regarding stock market performance and e-commerce, by investigating the effect of cyber crime on a company's stock price.

### **Types of Cyber Crime**

One example of a cyber crime involves Egghead.com. President of Egghead.com, Inc., Jeff Sheahan, emailed numerous customers and their credit card issuers, notifying them of an attack on the company's computer system. Following an FBI investigation and additional work by a forensic security firm (hired by Egghead), Egghead.com concluded that the company's security system apparently interrupted the intrusion in progress. Initial evidence indicated that several thousand credit card accounts in the system might have been affected. Cyber crimes, even when there are no direct losses to the company or its customer, can still be detrimental to a company's well-being (Luehlfiging et al. 2003).

Exhibit 1 lists several common cyber crimes. In general, cyber crimes are the modern-day counterparts of age-old crime. For example, prior to the electronic age, con artists went door-to-door and used verbal communication to gain the confidence of their victims. Today contemporary con artists use the Internet and online communications to perpetrate their crimes.

[Exhibit 1 about here.]

Perhaps the most well known of cyber crimes is the computer virus. A computer virus is a computer program that piggybacks or attaches itself to application programs or other executable system software; the virus subsequently activates, sometimes causing severe damage to computer systems or files. The basic steps in the computer virus infection process are shown in Exhibit 2.

[Exhibit 2 about here]

There are some indications that infections by computer viruses are decreasing. This may be due to better anti-viral software and anti-viral procedures. In addition, virus infections may be down as a result of new laws against computer viruses and criminal prosecution of perpetrators of computer viruses. The FBI and other investigators are cooperating more than ever to stop cyber crime. Local, state, and federal agencies routinely share information and team up for busts. The FBI and Secret Service have formed a joint cyber crime task force in Los Angeles (Grow and Bush 2005).

Following the 9-11 terrorist attack on the World Trade Center, cyber terrorism has become a high profile type of cyber crime. Cyber terrorism occurs when terrorists cause virtual destruction in online computer systems. Cyber terrorists employ devices such as computer viruses and online denial of service. The intention of the cyber terrorist is to incapacitate or

dramatically reduce the availability of an organization's computer resources. For a private company this results in loss of business; for a government entity this results in inability to carry out its mission.

E-fraud is the use of online techniques by a perpetrator to commit fraud. Popular forms of e-fraud include Email spoofing, phishing, and online credit card fraud. Email spoofing occurs when the perpetrator uses email to gain the confidence of an individual so that he or she provides personal information that is later used for unauthorized purposes such as fraudulent purchases, obtaining fraudulent loans, or identity theft. Spoofers are modern-day, tech-savvy con artists. Spam is a key method used by email spoofers to trick individuals into providing their personal information.

E-theft occurs when a perpetrator hacks into a banking system and diverts funds to accounts accessible to the criminal. To prevent e-theft, most major banks severely limit what clients can do online. Fraudulent Internet banking sites are often used to commit e-theft. The Internet can be used by criminals to establish fictitious online banks that attract customer deposits with promises of extremely high interest rates, after which the bank disappears with the money.

Netspionage occurs when perpetrators hack into online systems or individual PCs to obtain confidential information for the purpose of selling it to other parties (criminals). Offshore (foreign) online frauds are frauds perpetrated by persons in other countries. Foreign frauds are problematic as it is usually difficult for domestic law enforcement to apprehend and try individuals in a foreign country due to limited resources or extradition laws. Phishing is a popular technique used by foreign fraudsters.

Online credit card fraud results when the perpetrator illegally obtains a credit card number over the Internet and then uses it for unauthorized purposes such as fraudulent purchases. Alternatively, a fraudulent website can be used to fool the victim into voluntarily releasing credit card information.

Online denial of service is use of email barrages, computer viruses, or other techniques to damage or shut down online computer systems, resulting in loss of business. In some cases, online denial of service results in permanent damage to computer systems or files, requiring major expenditures to rebuild systems or recreate files.

Phishing is occurs when the perpetrator sends fictitious emails to individuals with links to fraudulent websites that appear official and cause the victim to release personal information to the perpetrator. This information is then used for unauthorized purposes such as fraudulent purchases, obtaining fraudulent loans, or identity theft.

Software piracy is the theft of intellectual assets associated with computer programs. Software piracy results in loss of profits to companies and individuals who own the software, while rewarding criminals who did not do the work or risk the resources necessary to develop the software.

Computer security is confronted with five basic threats: (1) natural disasters, (2) dishonest employees, (3) disgruntled employees, (4) persons external to the organization, and (5) unintentional errors and omissions (Smith et al. 2003). Historically, as show in Exhibit 3, the greatest threat was unintentional errors and omissions. However, this may be changing due to the increasing amount of personal and business activities done online.

[Exhibit 3 about here]

The direct costs of cyber crime for a sample of firms are shown in Exhibit 4. In just four years, for this sample, costs escalated from about 100 million to over \$250 million. Theft of proprietary information topped the list, going from about \$20 million to over \$60 million. Financial fraud increased from about \$25 million to about \$56 million.

[Exhibit 4 about here]

Preventive measures are available that help deter cyber criminals, such as passwords, firewalls, encryption, and other security policies and procedures. Since preventive measures are not always successful, cyber crime detection is a necessary last line of defense regarding loss prevention, or at least loss minimization. Detection techniques include: tripwires, configuration-checking tools, and anomaly detection systems. A brief overview of each of these intrusion detection techniques follows.

A tripwire is a software programs that take snapshots of critical system characteristics that can be used to detect critical file changes. Tripwires provide evidence of electronic crimes since most intruding hackers make modifications when they install backdoor entry points or alter file system and directory characteristics in the course of hacking the system.

A configuration-checking tool, also referred to as a “vulnerability assessment tool,” refers to software programs that detect insecure systems. Configuration-checking tools are primarily preventive in nature but used as a monitoring device they can also provide evidence regarding electronic crimes.

An anomaly detection system focuses on unusual patterns of system activity. Anomaly detection systems develop and analyze user profiles, host and network activity, or system programs in order to identify deviations from expected activity.

Unless properly and continuously “fine tuned,” a single intrusion detection technique may tend to under-report cyber crimes or over-report such as excessive false alarms. In most cases, companies find it necessary to employ multiple intrusion detection techniques to efficiently and effectively detect electronic crimes.

Experienced cyber criminals can obscure their actions through various methods. For example, cyber criminals may spread their intrusive behavior over a number of hosts on a network in order to defeat a single host intrusion detection procedure. Selecting and merging data from independent intrusion detection techniques, as well as the network itself, is necessary to identify this type of behavior.

Cyber crime is unlikely to be identified from random and intensive searches for evidence of criminal activity. If a cyber criminal can convince an intrusion detection system to continually and uselessly increase its use of computer resources, then the criminal has effectively accomplished denial of service, a particularly destructive type of cyber crime. In such a case, computer resources are wasted and cyber criminals are not detected.

### **Cyber Crime News Stories**

In February 2000, Amazon.com was one of many Internet sites affected by a group of cyber-terrorists who hacked into the site and made alterations to program coding. The problem was so severe that Amazon was forced to shut down in order to repair the damage and stop the unauthorized activity. As a result of the site closing, program changes were made to help prevent future break-ins (Kranhold 2000).

In October 2004 an individual gained access to the ChoicePoint Inc.’s database and thereby managed to pilfer 145,000 credit card files before leaving the system. The perpetrator did not have to crack the system with hacking procedures; however, he simply lied about his

identity over the phone and on a few forms. As a result, the data was simply handed over to him. As a normal course of business, companies like ChoicePoint Inc. distribute this type of information for a price to individuals for legitimate business purposes. In this case, the perpetrator made up false information about himself and was given access to the files. As a result of the incident, the company has taken steps to prevent this problem from recurring (Perez and Brooks 2005).

The Federal Trade Commission In November 2004 conducted a survey in which its operatives posed as distraught customers of numerous banks in order to gauge the banks' ability to respond to and prevent e-theft. Citizen's Financial Group was ranked among the bottom five banks in terms of preventing and fixing e-theft (Saranow 2004).

Like Amazon.com, eBay.com was the victim of a group of cyber-terrorists in February 2000. The company closed its site for a short period during which damage was repaired and actions were taken to prevent the problem from recurring (Kranhold 2000).

The Western Union branch of First Data Corp came under attack by a private hacker. In September 2000. The perpetrator hacked into the company site and stole credit-card information for 15,700 customers. Apparently, the theft was made possible during a routine maintenance process when an employee left the files unprotected and vulnerable to attack. First Data Corp immediately notified authorities and both the FBI and CIA became involved with the investigation (Colden 2000).

Like Citizen's Financial Group, Hibernia Corporation received very low ratings in the Federal Trade Commission survey conducted in November 2004. These ratings gave Hibernia a similarly low score and landed the company among the five worst ranked companies in terms of preventing and fixing e-theft (Saranow 2004).

In June 2005, a hacker accessed credit card files in the CardSystems Inc.'s database. The company processes credit card transactions for small to mid sized businesses. The hacker compromised the security of over 40 million cards issued by MasterCard, Visa USA Inc., American Express Co., and Discover. Because of the security breach, several banks were negatively affected. J.P. Morgan Chase was forced to investigate the security of its clients in June 2005. The company did not close any accounts immediately but began looking through the millions of potentially affected accounts (Sidel and Pacelle 2005).

A half million customers at Wachovia Inc. had confidential information illegally acquired by a professional criminal in May 2005. The criminal did not use a sophisticated hacking technique but employed traditional bribery to enlist eight former employees of Wachovia Corp. and Bank of America Corp. These former employees acquired and then sold the information to the criminal for \$10 a name. The criminal buyer subsequently sold the information to collection agencies and law firms. The New Jersey police are currently investigating the crime (Yuan 2005).

Washington Mutual Inc., like J.P. Morgan Chase, was affected by the security failure at CardSystems Inc. In Washington Mutual Inc.'s case, the company was forced to close down over 1,400 debit-card accounts (Sidel and Pacelle 2005).

In a pattern similar to other large websites, Yahoo.com came under the attack of cyber-terrorists in February 2000. Much like Amazon.com and eBay.com, Yahoo managed to avoid

any serious damage by shutting down its site to conduct repairs and modifications (Kranhold 2000).

### **Impact of Cyber Crime News on Company Stock Market Performance**

The ten cases used in the study (described above) were obtained by conducting a search of news stories regarding e-crime, cyber crime, and computer fraud on the ProQuest online database of current periodicals and newspapers (ProQuest 2005). These cases were used because they were listed at the top of the search, involved publicly traded companies, and included full news stories. Exhibit 5 provides the following information about the cases: company name, ticker symbol, type of crime, perpetrator, and damage sustained.

[Exhibit 5 about here]

In most of the cyber crime news stories, the perpetrator was a hacker. Types of crime included cyber-terrorism, e-theft, netspionage, online credit card fraud, and phishing. Affected companies include dot-com giants Yahoo!, Amazon, and eBay, and banks such as JP Morgan Chase and Washington Mutual. Damages vary from the closure of websites to stolen confidential information.

Exhibit 6 shows the effect of the cyber crime news story on the company's stock price. Shown in the exhibit are the company name, date of the news story pertaining to the cyber crime, the stock price on the date of the news story, the percent change in the company stock price for one and three days before the story, and the percent change for one and three days after the story. The short time period (three days before and after) was used, as is common in events studies, because wider time periods tend to be influenced by confounding events other than the one under investigation.

[Exhibit 6 about here]

To determine if the cyber crime news story had a significant impact on the company's stock price, a matched pair t-test was used. The change in the company stock price was compared to the percent change in the Standard & Poor's 500 stock market index. For -1 day and -3 days, there was no significant difference between the change in company stock price and the S&P 500 index. However, after the story, the change was significant for both +1 day (.01) and +3 days (.02). Thus, for this sample, a cyber crime news story results in a significant impact on the average company's stock price, at least in the short term.

### **Stopping Cyber Crime**

Since cyber crime is detrimental to business operations and to a company's stock market performance, business firms and their stakeholders clearly benefit from stopping cyber crime. A number of preventive measures can be employed to help prevent cyber crime. However, no matter how many preventive measures are used, unless properly and continuously "fine tuned," a single intrusion detection technique may tend to under-report cyber crimes or over-report such as excessive false alarms. In most cases, companies find it necessary to employ multiple intrusion detection techniques to efficiently and effectively detect electronic crimes.

Appropriate actions must be taken by qualified professionals to successfully resolve cyber crime. Since some business firms may lack qualified computer security personnel, hiring outside professionals e.g. forensic accountants may be necessary. For a company with computer security personnel, outside professionals may still be needed if the electronic crime resulted from negligence on the part of the company's computer security personnel. Law enforcement agencies can help with cyber crime investigations; although, many law enforcement agencies lack the technical expertise to investigate electronic crimes. Most can obtain warrants and seize computer equipment, but may be unable to find the evidence needed to resolve the cyber crime.

## **Conclusions**

This study described a number of common cyber crimes, identified specific cases in which publicly traded companies are the focus of news stories about cyber crime, and analyzed the impact of the cyber crime news stories on company stock prices. Results suggest that costs of cyber crime go beyond stolen assets, lost business, and company reputation, but also include a negative impact on the company's stock price, at least in the short run. Consequently, publicly traded companies must do all that they can to avoid becoming a victim of cyber crime.

To defend against cyber crime, intrusion detection techniques should be established. Techniques include tripwires, configuration-checking tools, and anomaly detection systems. Since prevention techniques are fallible, business firms should also establish procedures for investigation of and recovery from cyber crimes after they occur.

Future research could extend the current study by analyzing a larger sample of publicly traded companies that have been the victim of cyber crime. By employing a larger sample, future research might investigate the specific impact of different types of cyber crime on firms according to industry type. In addition, a longitudinal study might investigate whether different time periods affect the impact of the cyber crime. Perhaps as time goes by, investors may be less alarmed by news stories about cyber crime if such crimes become more commonplace.

## References

- Ballou, B., N. Godwin, and R. Shortridge. 2003. Firm Value and Employee Attitudes on Workplace Quality. *Accounting Horizons*, 17 (3): 329-341.
- Chen, A.H. and T. F. Siems. 2001. B2B e-marketplace announcements and shareholder wealth. *Economic and Financial Review*, First Quarter: 12-22.
- Clarkson, P, Y. Li, and G. Richardson. 2004. The Market Valuation of Environmental Capital Expenditures by Pulp and Paper Companies. *The Accounting Review* (April).
- Colden, Anne. 2000. Western Union reassures clients No financial fraud found since hacking. *Denver Post* (Sep 12): p. C1.
- Fukami, C., H. Grove and F. Selto. 1997. Market Value of Firm Reputation and Executive Compensation Structure. Working paper, University of Colorado at Boulder.
- Grow, Brian and Jason Bush. 2005. Hacker Hunters. *Business Week Online*, Website: [http://biz.yahoo.com/special/hacker05\\_article1.html](http://biz.yahoo.com/special/hacker05_article1.html) (June 8).
- Hand, J.R.M. 2000. Profit, losses and the non-linear pricing of Internet stocks. Working paper, University of North Carolina, Chapel Hill, NC.
- Kranhold, Kathryn. 2000. Handling Aftermath of Cybersabotage. *Wall Street Journal* (February 10): B22.
- Luehlfiging, M., C. Daily, T. Phillips, and LM Smith. 2003. Cyber Crimes, Intrusion Detection, and Computer Forensics. *Internal Auditing*, 18:5 (September-October): 9-13.
- McAnally, M., J. Blazovich, and L.M. Smith. 2004. Ethical Corporate Citizenship: Does it Pay? American Accounting Association Annual Meeting (August).
- Perez, Evan and Rick Brooks. 2005. File Sharing: For Big Vendor of Personal Data, A Theft Lays Bare the Downside; ChoicePoint Struggles to Gauge How Much Information Fell Into Wrong Hands; The Model: 'Small-Town Life.' *Wall Street Journal* (May 3): A1.
- ProQuest. 2005. Online information service. Website: <http://www.proquest.com/> (June 28).
- Rajgopal, S., M. Venkatachalam, and S. Kotha. 2002. Managerial actions, stock returns, and earnings: The case of business-to-business Internet firms. *Journal of Accounting Research* 40 (2): 529-557.
- Saranow, Jennifer. 2004. Guarding Identities: Banks Fall Short; Survey Finds Wide Gaps In Consumer Safeguards At Some Large Institutions. *Wall Street Journal* (Nov 17): D2.

Sidel, Robin and Mitchell Pacelle. 2005. Credit-Card Breach Tests Banking Industry's Defenses. *Wall Street Journal* (June 21): C1.

Smith, L.M., K. Smith, and D. Kerr. 2003. *Accounting Information Systems*, 4th Ed. Boston, Mass.: Houghton Mifflin.

Subramani, M. and E. Walden. 2001. The Impact of e-commerce announcements on the market value of firms. *Information System Research* 12 (2): 135-154.

Trueman, B., M. H. F. Wong and X. J. Zhang. 2000. The eyeballs have it: Searching for the value in Internet stocks. *Journal of Accounting Research* 38: 137-163.

Yuan, Li. 2005. Companies Face System Attacks From Inside, Too. *Wall Street Journal* (June 1): B1.

## Exhibit 1

### Examples of Cyber Crime

Cyber Crime	Description
Computer virus	A computer virus is a computer program that piggybacks or attaches itself to application programs or other executable system software; the virus subsequently activates, sometimes causing severe damage to computer systems or files.
Cyber terrorism	Cyber terrorism occurs when terrorists cause virtual destruction in online computer systems.
E-fraud	E-fraud is the use of online techniques by a perpetrator to commit fraud. Popular forms of e-fraud include Email spoofing, phishing, and online credit card fraud.
Email spoofing	Email spoof is use of email to trick an individual into providing personal information that is later used for unauthorized purposes.
E-theft	E-theft occurs when a perpetrator hacks into a banking system and diverts funds to accounts accessible to the criminal. To prevent e-theft, most major banks severely limit what clients can do online.
Netspionage	Netspionage occurs when perpetrators hack into online systems or individual PCs to obtain confidential information for the purpose of selling it to other parties (criminals).
Offshore Online Fraud	Offshore (foreign) online frauds are frauds perpetrated by persons in other countries.
Online credit card fraud	Online credit card fraud is illegal online acquisition of a credit card number and use of it for unauthorized purposes such as fraudulent purchases.
Online denial of service	Online denial of service is use of email barrages, computer viruses, or other techniques to damage or shut down online computer systems, resulting in loss of business.

**Exhibit 1 - Continued**

**Examples of Cyber Crime**

<b>Cyber Crime</b>	<b>Description</b>
Phishing	Phishing occurs when the perpetrator sends fictitious emails to individuals with links to fraudulent websites that appear official and thereby cause the victim to release personal information to the perpetrator.
Software piracy	Software piracy is the theft of intellectual assets associated with computer programs.

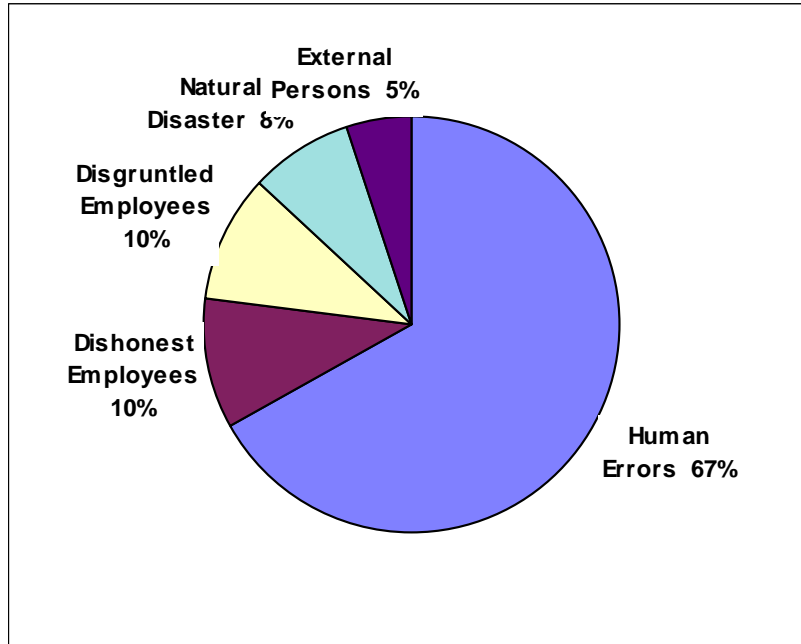
## **Exhibit 2**

### **Virus Infection Process**

1. Creation of virus by programmer; the virus program is typically an executable file, e.g. an exe, com, or vbs file.
2. The virus program is attached to an email (or alternatively attached to a public domain software program).
3. The email with the infected attachment file is sent to unwary recipients.
4. When the email message is opened, the infected program runs on the user's system and the virus replicates itself onto an operating system file.
5. In some cases, the virus spreads from the user's system to other user systems through infected diskettes. In other cases the virus gains access to the user's email system address book and sends itself to all the addresses.
6. At a predetermined point (e.g., a specific date), the virus activates, often leaving programs and data files unusable.

### Exhibit 3

#### Threats to Computer Security



Source: Smith et al. 2003.

## Exhibit 4

### The Cost of Cyber Crime

#### Total Annual Losses by Sample Respondents

<b>Year</b>	<b>1997</b>	<b>1998</b>	<b>1999</b>	<b>2000</b>
Theft of proprietary info.	\$20,048,000	\$33,545,000	\$42,496,000	\$66,708,000
Sabotage of data/networks	\$4,285,850	\$2,142,000	\$4,421,000	\$27,148,000
Telecom eavesdropping	\$1,181,000	\$562,000	\$765,000	\$991,200
Outside system penetration	\$2,911,700	\$1,637,000	\$2,885,000	\$7,104,000
Insider abuse of Net access	\$1,006,750	\$3,720,000	\$7,576,000	\$27,984,740
Financial fraud	\$24,892,000	\$11,239,000	\$39,706,000	\$55,996,000
Denial of Service	n/a	\$2,787,000	\$3,255,000	\$8,247,500
Spoofing	\$512,000	n/a	n/a	n/a
Virus	\$12,498,150	\$7,874,000	\$5,274,000	\$29,171,700
Unauthorized inside access	\$3,991,605	\$50,565,000	\$3,567,000	\$22,554,500
Telecom fraud	\$22,660,300	\$17,256,000	\$773,000	\$4,028,000
Active wiretapping	n/a	\$245,000	\$20,000	\$5,000,000
Laptop theft	\$6,132,200	\$5,250,000	\$13,038,000	\$10,404,300
<b>Total Annual Losses</b>	<b>\$100,119,555</b>	<b>\$136,822,000</b>	<b>\$123,779,000</b>	<b>\$265,586,240</b>
Source: Luehlfiing et al. 2003.				

## Exhibit 5

### Cyber Crime News Stories

Company	Ticker Symbol	Type of Crime	Perpetrator	Damage
Amazon.com Inc	AMZN	cyber-terrorist	hacker	Closed down the website
ChoicePoint Inc	CPS	netespionage	third party	145,000 individuals had confidential information stolen
Citizens Financial Group	CNFL	e-theft	potential hacker	Rated in the lowest 5 banks by the FTC in preventing e-theft
eBay Inc	EBAY	cyber-terrorist	hacker	Closed down the website
First Data Corp	FDC	netespionage, online credit card fraud	hacker	15,700 customers had confidential information stolen
Hibernia Corp	HIB	e-theft	potential hacker	Rated in the lowest 5 banks by the FTC in preventing e-theft
JP Morgan Chase	JPM	e-theft, netespionage, online credit card fraud	hacker	Investigating numerous possible breaches
Wachovia Corp	WB	netespionage	former employees	500,000 customers lost confidential information
Washington Mutual Inc	WM	e-theft, netespionage, online credit card fraud	hacker	Forced to close 1,400 debit-card accounts
Yahoo!	YHOO	cyber-terrorist	hacker	Closed down the website

## Exhibit 6

### Effect of Cyber Crime News on Stock Price

<b>Company</b>	<b>Date</b>	<b>Percent Change in Company Stock Price</b>				
		<b>Day</b>				
		-3	-1	0	+1	+3
Amazon.com Inc	02/10/00	(1.56)	5.33	0.00	(2.30)	(7.22)
ChoicePoint Inc	05/03/05	0.69	0.64	0.00	(1.36)	(1.00)
Citizens Financial Group	11/17/04	0.00	0.00	0.00	0.00	0.00
eBay Inc	02/10/00	4.42	1.00	0.00	(5.54)	(8.55)
First Data Corp	09/12/00	2.51	1.34	0.00	(3.94)	(2.91)
Hibernia Corp	11/17/04	0.72	(0.31)	0.00	(0.52)	(1.13)
JP Morgan Chase Co	06/21/05	0.11	0.03	0.00	0.61	(1.30)
Wachovia Corp	06/01/05	1.11	(1.17)	0.00	(0.19)	(1.36)
Washington Mutual Inc	06/21/05	(1.12)	(0.58)	0.00	(2.43)	(1.80)
Yahoo!	02/10/00	(3.01)	(1.33)	0.00	(6.37)	(9.18)
Avg % Change Stock Price		0.39	0.49	0.00	(2.20)	(3.45)
Avg % Change S&P 500 (match days)		0.21	(0.21)	0.00	(0.44)	(0.82)
Significance (prob.)		0.40	0.14	n.a.	0.01	0.02