Case Studies of Cybercrime and its Impact on Marketing Activity and Shareholder Value

Article *in* Academy of Marketing Studies Journal · December 2010

CITATIONS
25

READS
49,105

3 authors:

Katherine Taken Smith
Texas A&M University - Corpus Christi
71 PUBLICATIONS **1,784** CITATIONS
SEE PROFILE

Murphy Smith
Texas A&M University - Corpus Christi
156 PUBLICATIONS **2,035** CITATIONS
SEE PROFILE

Jacob Lawrence Smith
2 PUBLICATIONS **41** CITATIONS
SEE PROFILE

Case Studies of Cybercrime and Its Impact on Marketing Activity and Shareholder Value

Katherine T. Smith
Department of Marketing
Texas A&M University
4112 TAMU
College Station, TX 77843-4112
Tel: 979-845-1062
Fax: 979-862-2811
Email: Ksmith@mays.tamu.edu

L. Murphy Smith, CPA*
Mays Business School
Texas A&M University
4353 TAMU
College Station, TX 77843-4353
Phone: 979-845-3108
Fax: 979-845-0028
Email: Lmsmith@tamu.edu

Jacob L. Smith
Grace Bible Church
College Station, TX 77845
JacobSmith@grace-bible.org

*Corresponding author

Forthcoming in
Academy of Marketing Studies Journal

CASE STUDIES OF CYBERCRIME AND ITS IMPACT ON MARKETING ACTIVITY AND SHAREHOLDER VALUE

Katherine T. Smith, Texas A&M University
L. Murphy Smith, Texas A&M University
Jacob L. Smith, Grace Bible Church

ABSTRACT

Cybercrime, also called e-crime, costs publicly traded companies billions of dollars annually in stolen assets and lost business. Cybercrime can totally disrupt a company's marketing activities. Further, when a company falls prey to cyber criminals, this may cause customers to 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 cybercrime. Such vulnerability can lead to a decrease in the market value of the company, due to legitimate concerns of financial analysts, investors, and creditors. This study examines 10 case studies of publicly traded companies affected by cybercrime, and its impact on marketing activity and shareholder value. The study also describes some of the major types of cybercrime. Results indicate that costs of cybercrime go beyond stolen assets, lost business, and company reputation; cybercrime has a significant negative effect on shareholder value.

INTRODUCTION

E-commerce is a fundamental part of marketing activity. Most e-commerce takes place 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. A challenge facing e-business or cyber-business is that it is vulnerable to e-crime, also called cybercrime. Cybercrime can totally disrupt a company's marketing activities. Cybercrime costs publicly traded companies billions of dollars annually in stolen assets, lost business, and damaged reputations. Cybercrime costs the US economy over $100 billion per year (Kratchman et al. 2008, Mello 2007). 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 direct losses associated with cybercrime, a company that falls prey to cyber criminals may lose the confidence of customers who worry about the security of their business transactions. As a result, a company can lose future business if it is perceived to be vulnerable to cybercrime. 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 examines types of cybercrime and how they affect marketing activity. In addition, the study reviews 10 case studies of publicly traded companies affected by cybercrime, and its impact on shareholder value.

The research questions addressed by this study include: (1) What are some ways that cybercrime affects marketing activity? and (2) Do cybercrime news stories negatively affect shareholder value? Results suggest that there are a number of types of cybercrime that have detrimental effects on marketing activity. Furthermore, the costs of cybercrime go beyond stolen

assets, lost business, and company reputation, but also include a negative impact on the company's stock price.

E-BUSINESS AND E-RISK

Corporate managers must consider e-risks, that is, potential problems associated with e-business. Precautions must be taken against e-fraud, malicious hackers, computer viruses, and other cybercrimes. To some extent, electronic business (e-business) began with the early computers in the 1950s. However, not until development of the World Wide Web in the 1990s did e-business really take off. E-business is exchanging goods or services using an electronic infrastructure.

Only a short time ago, using the Internet as a primary way to do business was considered too risky. Today, e-business is simply business; it's the way business is done in the twenty-first century. The Internet is widely used for both business-to-business (B2B) transactions and business-to-consumer (B2C) transactions. The B2B market is from five to seven times larger than B2C. The B2B market is predicted to exceed $5 trillion in the early 21st century. The B2C market is growing as fast but is characterized by a much smaller average transaction size (Kratchman et al. 2008).

In a span of about 50 years, computers transformed the way people work, play, and communicate. The first electronic computer was built in 1946. The computer network that would evolve into the Internet was established in 1969. By the mid-1990's, millions of people were using their personal computers to "surf the web." A brief history of the Web and e-commerce is shown in Exhibit 1.

Insert Exhibit 1 about here

E-risk is the potential for financial and technological problems resulting from doing business on the Web (e-business). Changes in economic, industrial, and regulatory conditions mean new challenges. Troublemakers in cyberspace seek systems to infiltrate and misuse. Just for the fun of it, there are some people who try to hack into a business firm's computer system. Once access to the system is achieved, intruders can potentially cause major problems by deleting or changing data. Poorly developed accounting systems threaten a company's survivability and profitability of e-business operations.

Risks related to e-business on the Web include the following (Smith et al. 2003):

- The changing e-business environment alters risks, so old solutions may no longer work.
- International business activity expands the scale and scope of risks.
- Computing power, connectivity, and speed can spread viruses, facilitate system compromise, and compound errors in seconds potentially affecting interconnected parties.
- Hackers never stop devising new techniques; thus, new tools mean new vulnerabilities.
- Digitization creates unique problems for digital information and transactions.

LITERATURE REVIEW

There have been many research studies on the topic of e-commerce marketing and some specifically related to cybercrime. A selection of representative studies will be briefly reviewed here. Smith (2009) identified the annual growth rate of e-commerce to be as high as 28%, while individual countries may have much higher growth rates. In India, for example, which has a younger market, the e-commerce growth rate has been projected as high as 51%. Kotabe et al. (2008) evaluate the role of e-commerce, performance, and outsourcing. Gregory et al. (2007) study the impact of e-commerce on marketing strategy.

E-commerce websites are vulnerable to various risks, including cybercrime. These risks can be minimized by establishing effective controls. In addition, Web assurance services can be used to provide various levels of assurances that controls are in place (Runyan et al. 2008). Cybercrime is distinct from other threats facing business today, as described by Speer (October 2000), and contains unique characteristics. Zomori (2001) examines potential and real risks of e-business, caused by cyber-crime and money laundering. He emphasizes that trust is fundamental to doing e-business. Loss of trust and the ability to conduct e-business would not only represent a financial loss of e-business companies, but in society at large.

Smith (2008) identifies widespread use of e-commerce in all types of business, including manufacturing companies, retail stores, and service firms. This study reviews prior research, examines the origins of e-commerce, identifies e-risks, describes retail trade on the Internet, defines virtual business, identifies aspects of website design, and describes types of cybercrime that hamper e-commerce. Smith (2010) examines various marketing strategies often used in digital media to identify those preferred by Millennials, and which are effective in influencing behavior. Millennials are identified as a driving force behind online shopping. Results indicate a preference for online coupons and side-panel ads; Millennials do not like pop-up advertising. Graphics are effective in gaining their attention. Further, if given an incentive, such as a discount or reward, Millennials will write an online product review.

Oates (2001) stresses the importance of preventing, detecting, investigating, and prosecuting cybercrimes with the goal of reducing their impact on business and the public's confidence. In order to stop cybercrime, the private, public, and international sectors must openly share information on the methods they are successfully using to detect and prevent these crimes.

Kshetri (2005) draws upon literatures of psychology, economics, international relations and warfare to examine the behavior of cyber criminals. He finds that countries across the world differ in terms of regulative, normative and cognitive legitimacy regarding different types of Web attacks. The cyber criminal’s selection criteria for the target network include symbolic significance and criticalness, degree of digitization of values and weakness in defense mechanisms.

Riem (2001) found that the greatest threat to computer security comes from employees, consultants and contractors working within the company, rather than from outside hackers attempting to obtain access. Yapp (2001) agrees that the greatest threat to security is still from the inside, which is where nearly 70% of all frauds, misuses and abuses originate. Inadequate password policies and controls are the root of the most problems.

The corporate reputation or image of a company benefits from good news and suffers from bad news; the results often include a corresponding increase or decrease in the company’s

stock price. Prior studies have examined stock market consequences of news regarding ethical behavior (Blazovich and Smith 2008), firm reputation and corporate governance characteristics (Fukami et al. 1997), workplace quality (Ballou et al. 2003), and firm environmental reputation (Clarkson et al. 2004). Smith et al. (2010) find that a positive corporate reputation is associated with a significant market value premium, superior financial performance, and lower cost of capital. Given these findings, marketing managers would do well to strive to build and maintain a positive reputation.

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 cybercrime on a company's stock price and e-commerce marketing activity.

TYPES AND COSTS OF CYBERCRIME

Cybercrimes are the modern-day counterparts of age-old crime. Before the electronic age, con artists went door-to-door and used verbal communication to gain the confidence of their victims. The modern con artist uses the Internet and online communications to commit crimes. Exhibit 2 lists some of the common types of cybercrime.

Insert Exhibit 2 about here

The problems caused by the various cybercrimes vary over time. For example, computer viruses are not regarded as serious a threat as they once were. Infections by computer viruses are decreasing, most likely as a result of better anti-viral software and anti-viral procedures. In addition, the decrease in computer virus infections may be partly due to new laws against computer viruses and criminal prosecution of perpetrators of computer viruses. Federal, state, and local agencies share information and team up for operations. For example, the Secret Service and Federal Bureau of Investigation created a joint cybercrime task force in Los Angeles (Grow and Bush 2005).

The direct costs of cybercrime for a sample of firms are shown in Exhibit 3. In just four years, for this sample, the cost of cybercrimes 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 was second on the list, almost doubling in four years. Also incurring a substantial increase was "Insider abuse of Net access." Sabotage became a major problem in the final year.

Insert Exhibit 3 about here

CASE STUDIES OF CYBERCRIME

The following cases were obtained by conducting a search of news stories regarding e-crime, cybercrime, and computer fraud on the ProQuest online database of current periodicals

and newspapers. The ProQuest Research Library provides online access to a wide range of academic subjects. The ProQuest database includes over 4,070 tiles, nearly 2,800 in full text, from 1971 forward (ProQuest 2010). These cases examined in this study were used because they were listed at the top of the search, involved publicly traded companies, and included full news stories.

In February 2000, Amazon.com, Ebay.com, and Yahoo.com were among many Internet sites affected by a group of cyber-terrorists who hacked into the company websites and made alterations to program coding. The problem was so severe that the companies were 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).

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).

In October 2004, the perpetrator 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 and Hibernia Corporation were ranked among the bottom five banks in terms of preventing and fixing e-theft (Saranow 2004).

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 investigated the crime (Yuan 2005).

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).

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).

Exhibit 4 provides the following information about the cases previously described: company name, ticker symbol, type of crime, perpetrator, and damage sustained.

Insert Exhibit 4 about here

IMPACT OF CYBERCRIME ON COMPANY STOCK MARKET PERFORMANCE

In many cybercrime news stories, the perpetrator is a hacker. In other stories, the perpetrator has relatively little computer expertise. 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 5 shows the effect of the cybercrime news story on the company's stock price. Shown in the exhibit are the company name, date of the news story pertaining to the cybercrime, 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.

Insert Exhibit 5 about here

To determine if the cybercrime 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 (prob>.01) and +3 days (prob>.02). Thus, for this sample, the cybercrime results in a significant impact on the average company's stock price in the short term.

The Internet companies, Amazon, Ebay, and Yahoo, were affected most by the cybercrime news stories. Their stock prices dropped from 2 to 6 percent on +1 day and 7 to 9 percent on +3. The research question addressed by this study was: Do cybercrime news stories negatively affect shareholder value? The answer appears that cybercrime and resulting news stories do affect shareholder value, at least in the short term, via significant decreases in stock price. Since this is an event study, based on cybercrime news stories, it does not investigate the longer-term impact. Such analysis would be problematic given other factors, beyond the event of the cybercrime, which would affect stock market performance.

STOPPING CYBERCRIME

Cybercrime is detrimental to marketing operations and to a company's stock market performance; consequently, business firms and their stakeholders clearly benefit from stopping cybercrime. Preventive measures can be employed to help prevent cybercrime. 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 cybercrimes or over-report such as excessive false alarms. Companies generally find it necessary to employ multiple intrusion detection techniques to efficiently and effectively detect electronic crimes. Intrusion detection 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 cybercrimes after they occur.

Qualified professionals can help resolve cybercrimes. Business firms often lack qualified computer security personnel; thus, 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 cybercrime 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 cybercrime.

ADDITIONAL THREATS TO COMPUTER SECURITY

Based on movies and television shows, many people think that the greatest threat to computer security is intentional sabotage or unauthorized access to data or equipment. While sabotage and unauthorized access are serious problems, they are not the main threat to computer security. There are five basic threats to computer security: (1) natural disasters, (2) dishonest employees, (3) disgruntled employees, (4) persons external to the organization, and (5) unintentional errors and omissions. The extent that each of these threats is actually realized is shown in Exhibit 6.

Insert Exhibit 6 about here

As shown in the exhibit, human errors cause the great majority of the problems concerning computer security. Unintentional errors and omissions are particularly prevalent in systems of sloppy design, implementation, and operation. However, if the systems development process is done properly, errors and omissions will be minimized. An effective internal control structure is an integral part of any reliable information system.

The key to computer security and the success of any control structure is in the people of the organization. Research has shown that systems development is most effective when the users are involved, and most likely to fail when they are not. The following steps by management are integral to effective computer security (Kratchman et al. 2008):

- Design controls and security techniques to ensure that all access to and use of the information system can be traced back to the user.
- Restrict access by users to the parts of the system directly related to their jobs.
- Conduct periodic security training.
- Assign an individual or committee to administer system security in an independent manner.
- Clearly communicate and consistently enforce security policies and procedures.

Marketing information systems should be well defended against internal and external threats, including interruptions to information processing, whether resulting from natural disasters or manmade sabotage. According to the AICPA's 2009 Top Technology Initiatives, information security management is the top-rated key factor in doing business. In fact, in most recent years, information security management has been identified as the technology initiative likely to have the greatest effect in the upcoming year (AICPA 2009). While not in the top ten, another important technology initiative identified in the study was customer relationship management, which includes sales force automation, sales history, and campaign marketing, applications.

CONCLUSIONS

This study identifies types and costs of cybercrimes, how they interrupt marketing and business activity, and specific cases in which publicly traded companies are affected by cybercrime. In addition, the study analyzes the impact of the cybercrime news stories on shareholder value. Results suggest that costs of cybercrime go beyond stolen assets, lost business, and company reputation, but also include a negative impact on the company's stock price. Consequently, publicly traded companies must do all that they can to avoid becoming a victim of cybercrime and its negative impact on marketing activity and shareholder value.

To defend against cybercrime, 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 cybercrimes 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 cybercrime. By employing a larger sample, future research might investigate the specific impact of different types of cybercrime on firms according to industry type and/or specific categories of marketing activity (e.g. customer order processing, supply chain, etc.). In addition, a longitudinal study might investigate whether different time periods affect the impact of the cybercrime. Perhaps as time goes by, investors may be less alarmed by news stories about cybercrime if such crimes become more commonplace.

REFERENCES

AICPA (American Institute of CPAs). 2009. 2009 Top Technology Initiatives and Honorable Mentions. AICPA, website: aicpa.org (December).

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.

Gregory, Gary, Munib Karavdic, and Shaoming Zou. 2007. The Effects of E-Commerce Drivers on Export Marketing Strategy. *Journal of International Marketing*, Vol. 15, No. 2: 30-57.

Grow, Brian and Jason Bush. 2005. Hacker Hunters. *Business Week Online*, Website: 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.

Kotabe, Masaaki, Michael J. Mol, Janet Y. Murray. 2008. Outsourcing, performance, and the role of e-commerce: A dynamic perspective. *Industrial Marketing Management*. Vol. 37, No. 1 (January): 37-45.

Kranhold, Kathryn. 2000. Handling Aftermath of Cybersabotage. *Wall Street Journal* (February 10): B22.

Kratchman, Stan, J. Smith, and L.M. Smith. 2008. Perpetration and Prevention of Cyber Crimes. *Internal Auditing*. Vol. 23, No. 2 (March-April): 3-12.

Kshetri, Nir. 2005. Pattern of Global Cyber War and Crime: A Conceptual Framework. *Journal of International Management*, Vol. 11, No. 4 (December): 541-562.

Luehlfing, M., C. Daily, T. Phillips, and LM Smith. 2003. Cyber Crimes, Intrusion Detection, and Computer Forensics. *Internal Auditing*, 18:5 (September-October): 9-13.

Blazovich, Janell and L. Murphy Smith. 2008. Ethical Corporate Citizenship: Does it Pay? Working Paper. Available at http://ssrn.com/abstract=1125067.

Mello, John, Jr. 2007. Cybercrime Costs US Economy at Least $117B Each Year. TechNewsWorld, Website: ecommercetimes.com (July 26).

Oates, Brad. 2001. Cyber Crime: How Technology Makes it Easy and What to do About it. *Information Systems Management*, 18 (3) (June): 92–96.

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. 2010. Online information service. Website: http://www.proquest.com/ (February 25).

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.

Runyan, B., K. Smith, and L.M. Smith. 2008. Implications of Web Assurance Services on E-Commerce. *Accounting Forum*, Vol. 32: 46-61.

Riem, A. 2001. Cybercrimes Of The 21st Century. *Computer Fraud & Security* (April): 12-15.

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, K.T. 2008. An Analysis of E-Commerce: E-Risk, Global Trade, and Cybercrime. Working Paper. Available at SSRN: http://ssrn.com/abstract=1315423.

Smith, K.T. 2010. Digital Marketing Strategies that Millennials Find Appealing, Motivating, or Just Annoying. *Journal of Strategic Marketing*, forthcoming. Available at SSRN: http://ssrn.com/abstract=1692443.

Smith, K.T. 2009. Worldwide Growth of E-Commerce. *E-Business* (March): 29-34.

Smith, K.T., Murphy Smith, and Kun Wang. 2010. Does Brand Management of Corporate Reputation Translate into Higher Market Value? *Journal of Strategic Marketing*, Vol. 18, No. 3 (June): 201-222. Available at SSRN: http://ssrn.com/abstract=1135331.

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

Speer, David L. 2000. Redefining borders: The challenges of cyber crime. *Crime, Law and Social Change* 34 (3): 259-273.

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.

Yapp, P. 2001. Passwords: Use and Abuse. *Computer Fraud & Security* (September): 14-16.

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

Zombori, Gyula. 2001. e + Finance + Crime, A Report on Cyber-Crime and Money. Laundering Nathanson Centre for the Study of Organized Crime and Corruption, York University (Canada). Working Paper.

Exhibit 1

Information Technology: Historical Timeline
Pertaining to the Web and E-Commerce

1946 The first electronic computer, ENIAC, is constructed at the University of Pennsylvania.

1958 To counter Soviet technological advances, the U.S. forms the Advanced Research Projects Agency (ARPA), with the Department of Defense, to develop U.S. prominence in science and technology applicable to the military.

1969 ARPANET, the forerunner of the Internet, established with four nodes: UCLA, Stanford, UC-Santa Barbara, and University of Utah.

1970 First applications of electronic data interchange (EDI).

1984 Science fiction author William Gibson coins the term "cyberspace" in his novel, Neuromancer. Internet host computers exceed 1,000.

1988 Internet worm disables 6,000 of 60,000 Internet hosts. The worm was created by a Cornell University graduate student; infected computers were connected through ARPAnet and other E-mail networks in the Internet loop. Some of the US's top science and research centers were affected.

1991 Tim Berners-Lee, working at CERN in Geneva, develops a hypertext system to provide efficient information access. He posts the first computer code of the World Wide Web in a relatively innocuous newsgroup, "alt.hypertext." Later, people refer to the Internet itself as the Web.

1994 Inception of business to consumer (B2C) e-commerce.
Pizza Hut sells pizza on its Web site.
First Virtual, the first cyberbank, opens.

1995 *The Bottom Line is Betrayal* authored by K.T. Smith, D.L. Crumbley, and L.M. Smith: the first business educational novel focused on international trade, global marketing, and emerging technologies.

1997 Inception of business-to-business (B2B) e-commerce.
US Postal Service issues electronic postal stamps.

2009 Internet host computers (i.e., computers with a registered IP address) exceed 200 million. Users in over 150 countries are connected.

Exhibit 2

Common Types of Cybercrime

Cybercrime	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.
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.
Botnet	A Botnet infection occurs when a hacker transmits instructions to other computers for the purpose of controlling them, and then using them for various purposes such as spam distribution or phishing.
Spoofing	Spoofing 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 financial institution e.g. a bank 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).
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 2 - Continued

Common Types of Cybercrime

Cybercrime	Description
Software piracy	Software piracy is the theft of intellectual assets associated with computer programs.
Spam	Spam refers to unsolicited email; spam is illegal if it violates the Can-Spam Act of 2003, such as by not giving recipients an opt-out method.
E-fraud	E-fraud is the use of online techniques by a perpetrator to commit fraud. Popular forms of e-fraud include spoofing, phishing, and online credit card fraud.
Cyber terrorism	Cyber terrorism occurs when terrorists cause virtual destruction in online computer systems.

Exhibit 3

Costs of Cybercrime

Total Annual Losses by Sample Respondents

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

Source: Luehlfing et al. 2003.

Exhibit 4

Cybercrime News Stories

Company	Ticker Symbol	Type of Crime	Perpetrator	Damage
Amazon.com Inc	AMZN	cyber-terrorism	hacker	Closed down the website
ChoicePoint Inc	CPS	netspionage	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-terrorism	hacker	Closed down the website
First Data Corp	FDC	netspionage, 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, netspionage, online credit card fraud	hacker	Investigating numerous possible breaches
Wachovia Corp	WB	netspionage	former employees	500,000 customers lost confidential information
Washington Mutual Inc	WM	e-theft, netspionage, online credit card fraud	hacker	Forced to close 1,400 debit-card accounts
Yahoo!	YHOO	cyber-terrorism	hacker	Closed down the website

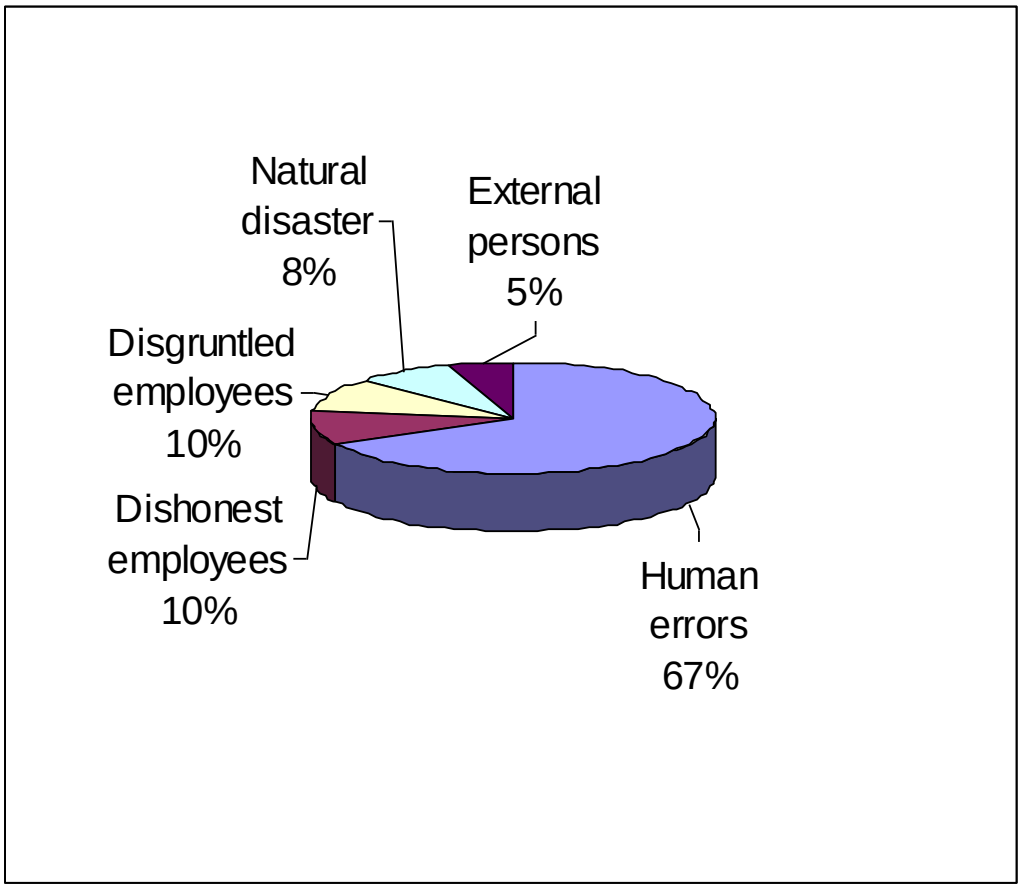
Exhibit 5

Effect of Cybercrime News on Stock Price

		Percent Change in Company Stock Price				
		Day				
Company	**Date**	-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

Exhibit 6

Threats to Computer Security



Source: Smith et al. 2003.