Financial Analysis Of Information Security Breaches*

Faramarz Damanpour, (E-mail: damanpfx@jmu.edu), James Madison University
M. Hossain Heydari, (E-mail: heydari@jmu.edu), James Madison University

Abstract

Each year, due to hacker attacks and virus infections billions of dollars are wasted. The impacts are globally felt and are not restricted to a single industry or agency, but it includes academia, individual, industry, and government agencies. In fact, hackers and viruses are becoming more and more sophisticated and are increasingly harder to detect. In this paper an attempt has been made to present Internet security and vulnerability, security policies, financial impacts, remedies, and a model to evaluate the opportunity costs of variables involve in security breaches.

1.0 Introduction

In recent years, international business and commerce have been experiencing dramatic changes via economic integration and globalization. Internet and computer technology have played a key role in the way companies do business, and synergism has been created between Internet technology and global business operations. Electronic business is no longer an alternative, but it is an imperative. Dot-com startups are grabbing market share online and competition between the leading computer and software producers and innovators are heating-up. While Internet clock ticks, many companies still struggle to find the best strategy.

Many companies are struggling with the most basic problem because there is no unique model or formula to deal with the best possible business strategy. Truth is, there is no simple prescription. Even companies in the same industry, of the same size, or with similar cultures are finding that a single E-commerce strategy does not fit all. Furthermore, the Internet has sprawled a wide variety of issues related to international trade, law, policies and intellectual property rights. In addition, the cost of a strategy implementation and security breaches created a difficult task for corporate managers in these downturn economy and competitive environment.

2.0 Internet Security and Vulnerability

Since no single authority runs the Web, it is difficult to make it secure. The first week of February 2000 crash of mysterious attacks against Web sites such as Yahoo Inc. and E*Trade Group Inc. has called for the Internet architectural needs to be redesigned to prevent malicious tampering. But how do you control and upgrade a network with no boss and no central authority, just a loose confederation of self-government standard-setters and rule makers?

On the other hand, billions of dollars are wasted each year due to hacker attacks and virus infections. A hacker with enough resources, time, and money can compromise almost any computer system and network, including government agencies, industry, academia, and individually owned computers. In fact, hackers and viruses are becoming more and more sophisticated and are becoming increasingly harder to detect.

According to a recent study by the American Society for Industrial Security (ASIS) and the consulting firm of PricewaterhouseCoopers (PwC), Fortune 1000 companies sustained losses of more than $45 billion from the theft of Property information. The loss has nearly doubled in 2001 in comparison with the FBI report of $24 billion in 1999.

Readers with comments or questions are encouraged to contact the authors via email.

On the average, the Fortune 1000 companies reported 2.45 incidents with an estimated loss per incident of over $500,000. More troubling is that of the 97 companies that participated in the ASIS survey, 44 reported a total of more than 1000 separate incidents of thefts. Tech companies reported the majority of those incidents. The average tech firm reported 67 individual attacks. The average theft was pegged at $15 million in loss business. These incidents are occurring despite the passage of the U.S. Economic Espionage Act of 1996, which considers theft of trade secrets a federal offense with prison sentences of up to 15 years and fines of up to $500,000 for individuals. Domestic thieves who sing to corporate rivals, face fines of up to $250,000 and jail sentences of up to 10 years. According to ASIS, the top five countries cited as security risks are the United States, China, Japan, France, and the United Kingdom. Mexico and Russia have the highest increase in spy activities. [1,2,3]

3.0 The Statement of Purpose

This paper addresses five issues. First, it presents the Internet security and vulnerability, and difficulties associated with strategies to implement information security. Second, it presents e-commerce evolution and perspective, Internet thefts and frauds, with several examples of businesses that have been subject to security breaches. Third, it reviews the importance of the information security, the ways and means of dealing with the hackers and virus infections and introduces several Web sites who deal with computer fraud and preventions. Fourth, the paper addresses various surveys results, the cost of electronic fraud, and corporate security policy and resources, with recommendations on security software. Finally, it introduces a flexible model and input variables for firms of different size to deal with the financial costs of Internet breaches and provide ideas to help Internet security. An attempt has been made to pre-test market by conducting a survey of 20 companies with security breaches to gather information regarding the costs of security intrusions.

4.0 E-Commerce Evolution and Perspective

The Internet has changed the way companies communicate, how they share information with business partners, and how they buy and sell. It also changed the way they view their Internet technology investments. One should not ignore the fact that the value proposition of E-commerce includes the creation of new market opportunities through electronic channels. These electronically channeled market opportunities enable companies to lower transaction costs, reduce delivery times, improve customer services, and add convenience. Increasingly, electronic sales, marketing, and distribution channels will grow at the expense of traditional channels for business. The bottom line is that E-business is seen increasingly as something that must be pursued at all costs.

The benefits are multi-dimensional, and given the strategy, it may include six dimensions:

- Better management information
- Lower transaction costs
- Better integration of suppliers and venders
- Better market understanding
- Better channel partnership
- Expand geographical coverage

There are three business areas that find the most benefit from online trading: automobiles, online lending, and travel. Of course with more use of Internet and electronic commerce, companies found that not only the costs of electronic implementation increased, but also frauds and thefts have been increasing in a form that they were not accustomed to. Now they are faced with the Internet security and vulnerability, and how to deal with these problems.

5.0 Internet Thefts and Frauds

It is very difficult and may not be possible to present all different examples of electronic frauds and misuse. Thus, we would like to consider a few examples and cases to shed light into recent Internet crimes.

Case 1 - Bank Crime*:* The traditional format of ski-mask wearing, gun-brandishing thieves dashing out of banks with cash-stuffed moneybags are a dying breed. Only 2 percent of mounting bank crime losses is now from physical robberies, according to the Oregon Bankers Association, as reported by Bob Sullivan of MSNBC. Now the crimes are more in form of stolen financial data and bank information walking out of the door. This is known as "electronic and paper fraud." There is almost no risk to the crime that cannot be spotted by security cameras, and even may not live in the same community, state or even the same country. Bank fraud appears in six formats:

- Wire Transfer
- Credit card fraud
- Creation of fake bank website
- Skimming ATM
- Car loans and equity loans identity theft
- Stolen information about bank customer

Wire transfer can be done by re-routing wire transfer from one bank to another bank, or by tricking a bank employee by a phone call. Other frauds in some respects are easier by depositing a fraudulent check from a credit card company, then withdrawing the money immediately, or by skimming ATM card numbers right from the machine. Often the banks' fraud start with a telephone call to a bank requesting information, such as bank account, or via identity theft resulting in car loans or even equity loans. Since September 11, 2001, a new form of bank fraud technique has been introduced by criminals acting as FBI agents who approach banks to collect information about an individual account or accounts to prevent terrorism activities.

To deal with this type of crimes, banks took several actions from installing special security software to add campaigns. For example Bank of America kicked off a new add campaign in 2001 entitled " Invasion of the ID snatchers" with the National Consumer League warning customers about the hazards of ID theft. Nevertheless, complains are mounting. Bank crime stories tell us that banking system has become a convenient database for criminals. Fraud expert Rob Douglas argued in his presentation to the Oregon Bankers Association in June 2002 that "the nation's banking system has become a playground for criminals – and now, terrorists – who know how to turn stolen financial data into steady income." One of the problems is the lack of prosecutions, despite the passage of Gramm-Leach-Bililey Act of 1999. The legislation declared "surrendering private financial information is a federal crime." Mike Foglio, Oregon Bankers Association Chairman complained that "we have cases we tie up with a bow and give them to federal authorities, and we cannot get them interested unless the loss is at least $50,000." Thus, criminals know that they can risk a $10,000 fraud with almost no fear of jail time. [2]

Case 2 – Microsoft*:* Hackers gained access to some of Microsoft Corporation's essential product secrets including latest versions of Windows 2000 and Offices in June 2000. What appears they had access to is the source code for products in development, creating a major embarrassment for the software company and its chairman, Bill Gates. A person close to the matter told CNNfn.com that the hackers could have had access to internal systems for as many as 60 days, and a London spokesman for Microsoft found signs that the intrusion may have come from St. Petersburg in Russia. The Wall Street Journal who first reported the Microsoft intrusion said that the electronic intruders entered into Microsoft's system and, thus, into the company network by e-mail software known as QAZ Trojan , which can be then used to delete files or deliver passwords. But industry experts said that Trojan is a relatively unsophisticated hackers' tool, which is not likely to have duped Microsoft's systems on its own. Another report indicated that the Microsoft attack started on October 14, 2000, when an employee -- possibly a temporary or contract worker -- received e-mail that automatically installed nefarious software into the corporate system. The software then gave access to the employee's computer and its protected passwords, and eventually to those of other computers in the network. Invaders may have then tweak Microsoft's original source code for Windows, adding "back doors" or other malicious code that provide easy access for future attacks. [1,3]

Getting access to confidential information from Microsoft's internal network could theoretically be of benefit to the software giant's competitors. But there is no indication that this was the case here. It is true that Microsoft's credibility has been damaged by this hack, but financially it did not hurt Microsoft at all. On the same day that the news was broadcasted, shares of Microsoft were up $3.88 at $68.31. If this intrusion were as negative as it appeared on the surface, Microsoft stock would be dropped like a rock. In general, one may think that it is possible that the hacker(s) was planning to create and sell a bootleg version of Windows or try to pass off the copies as new counterfeit packaging or include it as preload software on new computers. It is also possible that hackers could be eager to jump on new Microsoft products before they hit the stores. In a study and a survey conducted by Computer Security Institute and published in March 2000, it was found that 90 percent of respondents, mainly big corporations and government agencies, detected computer security breaches over the previous 12 months. Twenty five percent of respondents detected penetration from outside the organization. [1,3]

Citing figures from the Computer Security Institute, the San Francisco FBI survey, and the Business software Association reports that one in four pieces of software is pirated, Microsoft has given high profile to the legal maneuvers against software pirates. In October 2000, the company filed suits against three businesses in Atlanta area for distributing counterfeit copies of Window 2000, Window 98 and NT, and the BackOffice server software. In September 2000, Microsoft sued a number of California computer resellers for allegedly hawking pirated software. [2, 3]

If the attack was piracy-related, Microsoft incident could result in international legislations. Russia and China have long been atop the list of countries with piracy and hacking problems. Weak copyright -protection enforcement, combined with strong educational programs in computer programming and mathematics, had made these nations ideal labs for unauthorized copyright and tinkering. Of course, there are many theories about the Microsoft's hackers. Professor Eugene Spafford, Director of the Center for Education and Research in Information Assurance and Security at Purdue University, speculated that the hackers could be looking for information that could help prove the government's case against the software giant. Another scenario involves hackers tied to organize crime. As it was mentioned previously, according to the Wall Street Journal, the Microsoft hackers had an email address based in St. Petersburg, Russia – a hotbed of activities for the Russian mafia. Ira Winkler, president of the Internet Security Advisors Group (ISAG) made a good argument about the political issue related to these types of piracies. Would the U.S. government going to prosecute this person (s) just because he hacked into Microsoft? How much of a crime is it and how do you punish the person? Who is going to convince the Russians or another country to extradite this person, assuming he is not in the United State? [3]

Case 3 – Credit Card Fraud: MSNBC broke the story of one hacker who gathered the details of nearly a half-million credit cards that he stored on a US government computer. Another hacker named 'Curador' claimed to have gathered 23,000 credit card numbers, many of which he published on Web sites across the Net. [4] Most of these types of crime originated from retail stores' Webs, banks, stolen credit cards, and those sites with adult contents. The frauds associated with credit cards are recently run via a scanner. A scanner small enough to fit in a pocket can easily read and write a credit card's magnetic strips when a card is unobserved for a few minutes, in retail stores, restaurants, or any merchandise stores. The fraudster swipes the card through the scanner, which records all the necessary information, such as the cardholder's name, address and account details. Later, the device can be used to write on the strips of out-dated or cancelled cards, converting them to working copies of the originals.

The retail industry is in denial of credit card piracy and other security threats. They are concern about the loss of customers' confidence in online trading, and they are faced with a dilemma on how to handle the situations. An online crime rate below 1 percent is considered good for a commercial Web site; the rate for adult web sites is in the range of 8 percent to 12 percent. [4] But the true losses are concealed from the public. The question is that if you turned away 5 percent of revenues to keep your charge back rate at 1 percent and below, are you really doing yourself a favor?

This brings us to corporate risk management position. A very good security is a very expensive security. Most small merchants simply cannot afford the sophisticated security that large corporations and banks use. ICVerify a popular billing software for online credit card transactions marketed by Cybercash , was exploited for the 300,000 account score at CD Universe. Merchants need to manage fraud to a cost that makes business sense to them. Vitessa and the partner HNC Software provide services that enable merchants to select the level of fraud protection that makes the most business sense in their market. The services try to match the actual needs of an individual merchant with the likelihood of encountering fraudulent purchases. HNC has a fraud detection service for small online merchants called e-HNC, which is modeled on its more expensive, corporate oriented Falcon service. Merchants can buy into it at a cost of only a few pennies per transaction. [4]

Case 4 – Universities, Hospitals and Government agencies: In June through mid-July 2000, a sophisticated hacker took command of large portions of the University of Washington Medical Center's internal network, and downloaded computerized admissions records for 4,000 heart patients. One of the files contained the name, address, birth date, social security number, height and weight of patients along with each medical procedure they underwent. Interesting enough, the Seattle teaching hospital did not detect the fraud for over four weeks, and then elected not to notify immediately law enforcement agencies of the intrusions. [5,6] The hacker, a 25 years Dutch man who calls himself "Kane" did it for fun after a conversation with a friend about how well sensitive computers were protected. He later indicated that he also tried to crack a university center in New York, and one in the Netherlands, but neither of those penetrations gave him significant access. He was so surprised that the University of Washington Medical Center machines were exposed without any firewalls of any kind. Of course, there are those who believe that firewall would not fix the problem, when one deals with the complexity of the medical center, the rapidly increasing rate of new technology, and when the organization is too big to survive from intrusions. Another problem is that universities cannot lock down their computers in the same way a company could. Because universities typically have to provide an academic research network, and many have high speeds Internet connections, they become ideal for hackers. Another problem is that universities cannot immediately detect hacking. This was the case with the University of Washington, as well as Indiana University – with 55,000 Internet connected computers.

In regard to the Indiana University, hackers have broken into the network twice in one year, once two weeks after the school pledged to tighten its computer security policies. The University's network was hacked in January 2000 when 3,000 student records containing sensitive data were compromised. It was hacked so that it could be used as a storage site. It was later discovered that a Swedish man was storing his music and video files on the server. Another hacker broke into a database on May 24, 2000, and the breach was discovered on June 4, 2000. The file contained the names, addresses, and social security numbers of 1700 people who had requested information about the university's music program. Furthermore, hackers also used the university's servers as a private chat room and to store hacking tools and other files on the servers. [7]

Another example is the case of Benjamin Breuninger, a 22 year Minnesota man who in November 1999 intruded into an unclassified network at Lawrence Livermore National Laboratory (a nuclear laboratory), and planted in the system a backdoor that allowed him to reenter over the course of the next 10 days. The intrusion cost the laboratory $20,000 for the time workers spent re-securing the network. The hacker pleaded for a deal with the federal prosecutors and indicated that he cracked the lab's network to combat depression and suicidal tendencies. [5] The most recent vandalism reported by the CBS News and CNN occurred on January 26, 2003, when a hacker broke into the Bank of America cash machine control center and created disruption and financial crises which effected Bank of America's operation and other financial institutions for a day.

Pentagon computer were hacked 215 times in the year 2000. Overall, an estimate shows that 23,662 incidents involving unclassified networks occurred in 2000, up slightly from 22,144 in 1999. According to Michael Rasmussen, a senior industry analyst for Giga Information Group, most of the DOD's unclassified system breaches were via port scans. He cited ignorance and a lack of qualified security personnel for problems like those the Department of Defense has been experiencing. The most notable intrusion in the year 2000 was on the FBI's network by hackers from the former Soviet Union. This hacker was watching for vulnerability for a while, and when FBI's employers did not maintain the proper security, the hacker penetrated into the system. [8]

6.0 Russian Roulette

Russia has growing reputation as home base for some of the Net's most notorious hackers. In December 2000, the FBI began investigating a Russian link in the theft of 55,000 credit card numbers from merchant card processor CreditCards.com. After the site refused to pay $100,000, the hackers posted almost half of the numbers on the Web. Consumers whose card numbers were stolen incurred unauthorized charges from a Russian-base site. Almost the same happened in December1999. It involved the theft of approximately 300,000 card numbers from CDUUniverse.com. In that episode, a teenage Russian hacker released thousands of the numbers online when the music e-tailer refused to meet his $100,000 extortion demand. [9]

In March 2001, FBI issued an advisory warning that several organized Russian hacker groups operating out of Eastern Europe, Russia and Ukraine have stolen proprietary information from hundreds of e-commerce and online banking sites, including customer databases and more than 1 million credit card numbers. Overall, 40 e-commerce firms, located in 20 states, have had their computer systems penetrated by hackers who exploited vulnerabilities in un-patched Microsoft Windows NT operating systems. Hackers also were involved in the theft of nearly 100,000 credit card numbers from Amazon-owned book vender Bibliofind.com. After successfully invading consumer data, hackers either offered Internet security services for a large fee to patch the system against other hackers, or release the information online when the firms refused to pay the fees. [9]

One of the interesting case was the cases of Vasiliy Gorshkov, age 26, from Chelyabinsk, Russia, on 20 counts of conspiracy, computer crimes, and fraud against Speakeasy network of Seattle, Washington, Nara Bank of Los Angeles, California, Central National Bank of Waco, Texas, and the online credit card payment company PayPal of Palo Alto, California. Gorshkov and partner, Alexey Ivanov, were persuaded to travel to Seattle, Washington as part of the FBI undercover operation. Here, the FBI created a computer security company named "Invita" and asked the two men to show their skill in hacking. They successfully demonstrated their skills and indicated that they were willing to work with Invita from Russia where the FBI could not get them. They were arrested immediately, and after the FBI got access to their computers, found large databases of stolen credit card information (56,000), stolen bank account and other personal financial information of customers of online banking at Nara bank, Central National Bank of Waco, Texas, and Internet service providers like Lightrealm of Kirkland, Washington. In addition, the FBI found that hackers had broken into computers of school district in St. Clair County, Michigan, to infiltrate Paypal and e-Bay. At e-Bay, hackers acted as both seller and winning bidder in the same auction and pay themselves with the stolen credit cards. The jury in the United States District Court in Seattle returned guilty verdicts against them on October 10, 2002, and Gorshkov faces a maximum sentence of five years in prison on each account (for a total statutory maximum of 100 years in prison) and a maximum fine of $250,000 on each account. [10]

7.0 CSI Survey Results

CERT is a center of Internet security expertise at the Software Engineering Institute, operated by Carnegie Mellon University, Pittsburgh, Pennsylvania. The center studies Internet security vulnerabilities and publishes security alerts. In April 2002, CERT coordination Center reported that the speed of attack tools is increasing and they are more difficult to detect via anti-virus software and intrusion detection systems. The same sentiment was expressed by the Computer Security Institute (CSI), based in San Francisco, which conducts surveys and provides information on the security breaches for the past seven years. The latest CSI survey conducted in 2001 and reported in 2002, with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad provides valuable information. The survey polled 503 computer security professionals in U.S. corporations, government agencies, financial institutions, medical institutions and universities. The following are the major results [11,12]:

- Ninety percent of respondents, primarily large corporations and government agencies, reported experiencing computer security breaches in the last 12 months, 80 percent acknowledged financial losses due to security breaches, and 64 percent reported unauthorized use of their computer systems.

- Forty four percent of respondents (223) were able to quantify financial losses, and reported a total of $445.8 million losses. In regard to the theft of proprietary information, 5 percent (26 respondents) reported a total of $170.8 million losses, and for the financial fraud, 5 percent (25 respondents) reported a total of $115.7 million losses.

- For the fifth year in a row in 2001, more respondents (74%) cited their Internet connection as a frequent point of attack versus 70 percent in the year 2000, and 33 percent cited their Internet system as the point of attack in

2001versus 31 percent in the year 2000. This indicates that outside attacks are growing. In addition, 85 percent of the respondents said they have detected computer viruses.

- Seventy percent reported some vandalism to their Web sites in 2001, as compared to 64 percent in 2000.

What is interesting is that all these attacks occurred despite the wide deployment of security technologies. The survey in 2000-2001 shows that 95 percent of companies have firewalls, 61 percent have IDS, nearly 90 percent have access control of some sort, and 42 percent digital IDS. The survey points to the rapid expansion of e-commerce, vulnerabilities of systems, more technologically advanced scanning tools, and the ability of hackers to bypass the firewalls that are the primary line of defense against intrusion for most companies.

Many articles have been written about hackers and how to deal with them in the last several years, but none were really effective. The following is a sample of a few useful sites from vnunet.com [13]:

- Anti-hacking squads could help corporations: http://www.vnunet.com/News/1112675 (10-18-2000)
- Malicious code targets Palm users: http://www.vnunet.com/News/1109769 (08-29-2000)
- Bug watch: how to deal with hoax viruses: http://www.vnunet.com/News/1108144 (08-04-2000)
- Bug watch: a real can of worms: http://www.vnuney.com/News/1105950 (07-07-2000)
- Web page virus prompts security concerns: http://www.vnunet.com/News/1105489 (07-03-2000)
- Small firms at risk from hackers: http://www.vnunet.com/News/1105297 (06-30-2000)
- Viruses hoax prey on nervous users: http://www.vnunet.com/News/1104251 (06-22-2000)
- Viruses pose no risk to mobile phones: http://www.vnunet.com/News/1102850 (06-08-2000)
- Love Bug prompts Microsoft security update: http://www.vnunet.com/Specials/1101157 (05-16-2000)
- Counting the cost of the Love Bug: http://www.vnunet.com/Analysis/11101015 (05-09-2000)
- DTI survey uncovers security complacency: http://www.vnunet.com/News/601816 (04-06-2000)

8.0 The Cost of Electronic Fraud

The true estimate of the costs of security fraud is very difficult. The existing estimates and reports vary in a wide range. The Business Software Association, a Washington-based software industry consortium, estimated in a May 2000 report that losses due to piracy topped $12 billion worldwide in 1999, and today one in four pieces of software in circulation is pirated. As reported previously, a study by the American Society for Industrial Security (ASIS) and consulting firm PricewaterhouseCoopers reported that Fortune 1000 companies sustained losses of more than $45 billion in 1999 from the theft of proprietary information -- up from the mid-90's estimate by the FBI that pegged the cost at roughly $24 billion a year. Another study/survey by Reality Research for PricewaterhouseCoopers indicated that hack attacks would cost the world economy $1.6 trillion in the year 2000 (the study covering 30 countries and 4,900 Information Technology companies), and viruses were expected to add an additional $1.5 trillion to the tab. The survey also indicated that in the year 2000 alone, 39,363 human years productivity worldwide have been lost because of viruses. The experts also believe that Love Bug hit 60 percent to 80 percent of American businesses, costing companies worldwide an estimated $2.61 billion. Meanwhile, according to the FBI, 9 out of 10 companies have reported computer security breaches since March 1999. The study was based on more than 600 companies and government agencies. Lack of proper security has been given as the main reason for the break-ins. [1, 2, 3, 13, 14,15]

9.0 Corporate Security Policy

It is important for corporations to establish security policy, security objectives and procedures that prepare their organization to detect signs of intrusion. Preparation procedures include the actions necessary to observe systems and networks for signs of unexpected behavior by monitoring, inspecting, and auditing both hardware and software systems. Security policies and procedures must be documented, well known, visible and enforceable. All sensitive documents must be restored and protected. The type of threats that a company may encounter include:

- Attempts to gain unauthorized access to a system or its data
- Unintended and unauthorized disclosure of information

- Disruption or denial of service
- Unauthorized use of a system to process, store, or transmit data
- Unauthorized changes to system hardware and software

In order to deal with these intrusions, companies have to document and publicize the roles, responsibilities, authority, and conditions for the testing of intrusion detection tools and procedures. For further information about policy and procedures, contact Carnegie Mellon software Engineering Institute, CERT Coordinator Center [16], and SANS Institute Resources, which provide security policy project and resources. [17] The following are the security policy resources on the Web, courtesy of SANS Institute.

http://www.sans.org/infosecFAQ/policy/policy_list.htm This site contains articles and papers written by GIAC certified professionals.
http://www.ietf.org/rfc/rfc2196.txt?Number=2196 This site contains security policies procedures handbook.
http://www.securityfocus.com/data/library/Why_Security_Policies_fail.pdf A white paper.
http://www.security.kirion.net/securitypolicy/
http://www.network-and-it-security-policies.com/
http://www.brown.edu/Research/Unix_Admin/cuisp
http://iatservices.missouri.edu/security/
http://www.utoronto.ca/security/policies.html
http://irm.cit.nih.gov/security/sec_policy.html
http://w3.arizona.edu/~security/pandp.htm
http://secinf.net/ipolicye.html
http://ist-socrates.berkekey.edu:2002/pols.html
http://www.ruskwig.com/security_policies.htm
http://razor.bindview.com/presentations.InfoCarePart2.html
http://www.jisc.ac.uk/pub01/security_policy.html

OECD and IT Security. In May 2002, the Organization for Economic Cooperation and Development (OECD), an international body representing 30 nations, met to upgrade the guidelines for information system and IT security issued in 1992, in part due to the September 11, 2001 terrorist attacks in the United States. The new guidelines, which are not binding for any nation or company, set out an awareness principle that calls for owners or users of IT to understand security and handle it in a way that respects the rights and legitimate interests of others. The OECD's intent is to create a document that is accessible to all participants and set a framework from which a company develops best practices. While the guideline may have no technological impact, it puts the companies on notice. Kimberly Kiefer, a Washington-based attorney, who is co-chairwoman of the American Bar Association's Information Security Committee, said companies face legal peril when information security breaches compromise customer data. [18]

Because government agencies and military lag behind private enterprises in dealing with security breaches, they started to cope with the problem by hiring consultants to infiltrate their computers and provide them with advise on how to prevent security breaches. It is no doubt that security policies underpin the security and well being of information resources. A directory of information security policies and resources has been developed to help those in need. [19, 20] The fundamental question is how to deploy the policies at the most effective way and cost. Again, let me remind you that the relationship between information security policies and risk analysis is by its nature complex. But it needs to be considered and evaluated if one is concerned with unauthorized security breath.

10 Security Software

Many experts reported and many articles have been written about hackers and how to deal with them. Since September 11, 2001, in this new era of terrorism, corporate America is on high alert to help secure their own operations and the nation's critical infrastructure. To be truly effective, security best practices must address all dimensions of enterprise IT security: e-commerce, applications, network infrastructure, and content. Cheryl Krivda of Fortune magazine with the help of Carnegie Mellon University conducted a study and reported that enterprises must use anti-virus, intrusion detection, firewall, and virtual private network solutions to protect their network perimeter. Access control, encryption, authentication, and digital credential technology are some of the effective solutions available to protect applications, messaging, and databases. [21]

The scope of our study does not permit a presentation of all available security software. We chose to introduce two software that have been widely recommended. One deals with passwords and the second one deals with Digital Right Management (DRM). Both have received endorsement from IT experts.

Entrust's Software: This software gives a full-proof ID card or a backstage pass for doing digitally encrypted signatures across the Internet. It is reported that 90 percent of Web financial transactions are currently protected by only passwords. When you log into your online bank or trading accounts, you enter a password via Internet to connect. The server has a copy or image of your password, and check to see whether your user ID and password match. The problem is that back-end systems are favored targets of hackers and they hold not only your securities but also other vital information like credit card and ATM card numbers.

With Entrust's software, when you type your password into your PC, Entrust's technology verifies the password locally, rather than sending it to a server across the net. This give you access to a so-called private key, which is stored on your computer. One can use the private key to create a digital signature or decrypt information. Your bank or broker would set you up with a private key. It is immune to hacking even by a super computer because it features about 100 digits and steps contained in about 2KB of algorithm. The private key has a corresponding "public Key," which is made available as an address for transactions in a kind of outline phone book. Your private key is authenticated for the public key through an intermediary or interpreter. It consists of an encrypted digital certificate on a server hosted by your broker, which tells the public key that you have a trustworthy real world identity. Entrust's is currently applying this technology into the wireless equipment, starting with the next generation products from Nokia, Motorola, Waterloo, and Research In Motion (RIM). [22]

Digital Rights Management (DRM): DRM enables secure transaction of valuable files – audio, video, or text – across digital networks. Currently, it is a darling of consumer media, but the technology can be extended to cover financial services, the health care sector, law firms, and anyone who want to send confidential information over digital networks. DRM technologies were invented by a small Santa Clara, California company called InterTrust technologies in 1990. The inventor, Victor Shear envisioned a world in which most commercial transactions would be conducted electronically between a wide variety of hardware and software devices that would interact. The technology permits trust between hardware and software devices, and enables them to handle valuable information via digital property in accordance with predictable rules.

The key problem was how to provide persistent protection to digital files. The past technology permits encryption to protect a document or copyright movie when it is transferred from point "A" to point "B." But it did not provide any further protection thereafter. The recipient at point "B" once received the document made digital copies and distributed them globally. To protect this, one had to wrap the file in a secure digital container and tag it with rules describing how it could be used. DRM provided such a protection. To play or read the encryption file, recipient would need hardware or software that could trust the content that the originator sent to enforce the rules. DRM would enable both senders/producers and receivers/consumers to have a relationship that was impossible in the past. On February 13, 1995, Victor Shear on behalf of InterTrust filed a 1000-page patent application, referred to as the "Big Book." Thereafter, this small 39 employees company acquired 25 additional patents, and had 85 more pending. But the honeymoon did not last that long. As clients lined up including Universal Music Group, Bertelsman, National Westminster Bank, Mitsubishi, Sony Music Entertainment and McGraw-Hill, the trouble started. First, Sony and Philip offered to buy InterTrust for $453 million in cash, then, Xerox and IBM started to develop the same technology, and in the summer of 1999, Microsoft after visiting the InterTrust lab, offered $140 million for a 20 percent stake in the company plus a commitment to begin shipping the company's software in every copy of Windows starting in 2002. [23]

The deal apparently was not completed. But Microsoft had already insight about the technology and used it to its advantage. In 2000, Microsoft launched its .NET initiative, with its focus on networking computing and began introducing DRM and trust features on nearly all its products. Meanwhile the InterTrust stocks fell from $97 in February 2000 to under $1 in august 2001, and its workforce fell from 376 to 39. By the April 2002, InterTrust stopped selling its products and became a pure intellectual-property company with limited cash flow. In May 2002, Sony licensed InterTust patent's, agreeing to pay an upfront fee of $28.5 million, as well as, royalties. This gave the InterTrust a vote of confidence and the first quarter of profit in its life. InterTrust sued Microsoft, saying that its patents are infringed every time Microsoft ships its Window XP operating system, Office XP suite, Word 2002 processor, Excel 2002 spread sheet, Outlook 2002 e-mail client, Power Point 2002 slide presentation software, Windows Media Player, Xbox videogame console, Microsoft software servers, mobile phones, pocket computers, and consumer electronics devices and tool kits. Interesting enough the Microsoft negotiator, Will Poole, indicates: "Dreams without implementation are fairly easy to come by, especially in the software industry," and he added that Microsoft wanted to do a deal with InterTrust, despite the fact that the owner did not take it. [23]

11. A Model to Estimate the Cost of Security Breaches

One aim of this study is to develop a model to calculate the cost of the security breaches, given the parameters in which companies operate. Because companies are different by nature of their works and sizes, to develop one model that fits all is not possible. However, we identified eleven input variables involved in security breaches. Of course all companies are not subject to all these variables, and the regression model for companies of different size and scope are different.

The following are the input variables involve in estimating the cost of security breaches:

- Financial
- Security
- Loss of data
- Operation efficiency
- Legal
- Recuperation and loss due to down time
- Competitors' benefits
- Impact on stock price
- Loss of credibility and trust
- Access to technology for business use by outsiders
- Hacking by organized crime groups

Financial costs are associated with the opportunity cost of security breaches and the loss of benefits as the result of intrusion. This cost varies widely among the corporations based on the size and type of the activities involved. It is substantially higher for consumer-oriented businesses, such as banks, credit card companies, telephone and communication companies and government agencies, than other type of businesses. The ***security cost*** is associated with the costs of security policy application and implementation, security hardware and software, and training procedures and durations. The ***loss of data cost*** is subject to depth and damages as a result of security breaches. This cost is also a function of the company's size and the field of activities. Similarly, ***recuperation cost*** varied based on the depth and size of damage. Naturally, this cost is substantially higher for the consumer-oriented firms. The ***legal costs*** are associated with the costs of prosecution, court fees, and other legal aspects of pursuing hackers legally for the breaches of privacy and stolen data, as well as costs of lawsuits from victims.

While the extent of security breaches by a ***competitor and for competitive benefit*** is not clearly obvious or investigated, the cost of such security intrusion cannot be ignored, especially if the outcome is an access to an advance technology or new research methodology. The costs associated with the ***impact of hacking on the companies' stock price*** and ***loss of credibility*** and trust is interrelated. An extensive damage or breach of security will directly damage the reputation of the company and may damage the stock price. In addition, the loss due to downtime may impact both the employee's resources and the system, while security breaches are being fixed. A***ccess to technology for business use*** (but not by competitors) by a person let's say from China or Russia to develop counter-fit software has a direct business impact via loss of revenue and profit, and contributes to over-supply of product in a given market. ***Hacking by organized crime groups*** for business-economic benefit not only has negative business implication, but it also creates credibility problem. This type of security breaches is harder to crack than the ones by a teenager intrusion for fun.

To calculate these input variables costs, one needs to have access to two factors: cost of each input components, and weight assigned to each input variable. No study exists to reveal the actual costs of input variables, because in part, it is difficult to measure, and in part corporations who had security breaches in the past refuse to cooperate in order to safeguard credibility and prevent damage to their business activities and products. Therefore, any calculation of these costs would be subject to speculation and inaccurate forecasting. We made an attempt to pretest the outcome by surveying 20 corporations whose names appeared in the press as the ones with some form of security breaches. But not even one responded to the questionnaire. The weight assigned to each input variables is far easier to accomplish, because it is a function of the firm's size, type of business activity, security policy, and hardware and software in use for this purpose. Thus, this phase of our intention - - a development of a model to estimate the cost of security breaches – is left for future research and for times in which more information can be available.

12. Conclusion

Communication networks are vulnerable and any person with enough time and resources can compromise almost any system. While the purpose and intention of hackers may vary, the result is the same. This paper, with the help of several examples, tried to shed light on the high cost of the security breaches and damages. Furthermore, it addressed e-commerce evolution and perspective to show the inter-connection between technology advancement and increase in security breaches. Several businesses, such as banks, credit card companies, telecommunication firms, hardware and software businesses, and customer-oriented agencies are the most to lose and are more subject to security intrusions. More importantly, we dealt with the security prevention tools and introduced two software which may present partial solution to the security breaches. Finally, an analysis of the cost of security breaches and parameters of input variables to create a financial model and to estimate the costs of security breaches, were introduced. We sincerely hope that we contributed sufficient information to encourage further research in the development of a financial model to suit various firms.

This research is supported in part by a grant from the Department of Defense.

References

1. Microsoft: Big Hack Attack," CNNmoney, October 27, 2000; http://money.cnn.com/2000/10/27/technology/micosoft/
2. Sullivan, Bob, "Bank Crime Data Theft on the Rise," June 26, 2000; http://www.msnbc.com/news/772723.asp
3. Conrad, Rachel, "Hack Attacks a Global Concern," CNET.com, October 29, 2000.
4. Greene, Thomas C., "Hacking Credit Cards Is Preposterously Easy," The Register, July 30, 2002; http://www.theregister.co.uk/content/archive/9978.htm
5. Poulsen, Kevin, "Hospital Records Hacked," Security Focus, December 6, 2000; http://online.securityfocus.com/news/122
6. "Security Computers Prime Targets For Hackers," USA TODAY, June 6, 2001; http://www.usatoday.com/life/cyber/2001-06-01-hackers-college.htm
7. Delio, Michelle, "Hoosier favorite Hack Victim?", WebMD Newsletter, September 12, 2002.
8. Weisman, Robyn, "Pentagon Computers Hacked 215 Times in Past Year," News Factor Network, May 18, 2001; http://newsfactor.com/perl/story/9862.html
9. Saliba, Clare, "Russian Hackers Blackmail U.S. E-Commerce Sites," E-Commerce Times, March 9, 2001; http://www.ecommercetimes.com/perl/story/8063.html
10. "Russian Computer Hacker Convicted by Jury," U.S. Department of Justice, Press Release, Western District of Washington, Seattle, Washington, October 10, 2001; http://www.usdoj-crm/mis/jam
11. "Security Incidents," Counterpane, August 2002; http://www.counterpane.com/incidents.html and http://www.gocsi.com/press/20020407.html

12. “Attacks Grow More Sophisticated as Cyber Crime Bleeds U.S. Companies,” Overseas Security Advisory Council (OSAC) – Cyber News, June 26,2002; http://www.ds-osac.org/edb/cyber/news/story.cfm?KEY=8404
13. Leyden, John, “Hackers and Viruses To Cost Business,” November 7, 2000; http://www.vnunet.com/News/1106282
14. Enos, Lori, “Report: Security Software sales To Surge,” E-Commerce Tomes, October 4, 2000; http://www.ecommercetimes.com/perl/story/4460html
15. McDonald, Tim, “Report: Year’s Hack Attacks To Cost $1.6 Trillion,” E-Commerce Times, July 11, 2002; http://www.ecommercetimes.com/perl/story/3741.html
16. “Establish a Policy and Procedures that prepare Your Organization to detect Signs of Intrusion,” CERT Coordination Center, Software Engineering Institute, Carnegie Mellon, 2000.
17. “The SANS Security Policy Project,” SANS Institute resources, 2002; http://www.sans.org/newlook/resources/policies/policies.htm
18. Thibodeau, Patrick, “International Group Eyeing IT Security Principles, Standards,” IDG net, Computerworld, May 21, 2002.
19. O’Harrow Jr., Robert, “Sleuths Invade Military PCs with Ease,” Washington Post, August 16, 2002, page A01.
20. “The Information Security Policies/Computer Security policies Directory,” 2002; http://www.information-security-policies-and-standards.com/
21. Krivda, Cheryl, “Double Jeopardy,” Fortune, February 3, 2003, page 48. Produced in cooperation with Carnegie Mellon University.
22. Kaihla, Paul, “Securing the Ether,” Business 2.0, Web Article, February 14, 2001; http://www.business2.com/articles/web/0,1653,9458,00.html
23. “Can This Man Bring Down Microsoft?”, Fortune Magazine, December 30, 2002, pages 144-152.