Corporate Computer Crime: Collaborative Power in Numbers

Lynne M. Wiggins
Project Manager, Information Systems, GT Systems, Inc.

Introduction

Technology advances have given corporations the capability to store and retrieve massive amounts of data, offering connections to just about anyone, anywhere, at anytime. Advances have brought blessings to many, as corporations have benefited from increased productivity from e-mail connectivity, online messaging, computerized training and ebusiness. Accompanying these benefits, advances have also increased corporate risks. They have created an infrastructure in which the corporation itself can easily become the victim. Large volumes of data, having been reduced to bits and bytes and held within complex yet accessible systems, make corporations increasingly vulnerable to corporate computer crime. Corporations affected by computer crime are then left to determine whether or not to report the incident and what remedies should be utilized to resolve the problem and minimize future risks. Collaborative information sharing and working alliances between corporations and law enforcement are needed to prevent a parallel between corporate computer crime rates and the technological advances.

Types of Corporate Computer Crime

Corporate computer crimes are not much different from conventional white-collar crimes. Carelessness, greed, revenge, life-style, crisis, and need for a sense of superiority, ego, or power can cause either. High technology, when integrated into conventional white-collar crimes such as fraud, illegal infiltration, piracy, bootlegging, and counterfeiting, has created four general categories of corporate computer crime: innocent hackers; computers as a tool; computers as a target; and computer-related crime.

The first category of corporate computer crime involves innocent hackers. In the 1960s, "hacking" referred to intellectual student pranks intended to find ingenious ways to use computers. Students performing the hacks were known to be hackers. During these early days, hacker intentions were to enter, learn, and leave quietly without doing damage to the compromised system. Hackers were skilled programmers without motivation to steal or commit crime but fueled by the need to satisfy egos and prove intellectual power. Hackers of today's computer environment continue in this quest as pranksters perpetrating tricks without intending any particular or long-lasting harm. Prefabricated hacking tools, available at many hacker websites, help further hacking exuberance. These tools are used to intrude on and explore corporate computers for largely innocent motives such as education, curiosity, social justice, and competition with peers. Even with this innocuous definition, innocent hackers, while viewed by most as a nuisance, are still criminals.

At a minimum, vandalism produced during hacking incidents lowers corporate productivity. Increased manpower costs to tighten holes within insecure systems are required to prevent future trespass capabilities. No matter how innocent the hacker's motives may be,

> unauthorized use of others' computers, information and networks is a crime in most legal jurisdictions in the Western world. The greatest losses from hacking are usually the costs of the victim's staff to repair the damage done to computer stored information and to restore the integrity and authenticity of computer and communication systems (Parker, D., 1998, pp. 44, 174).

The second category of corporate computer crime consists of use of the computer as a tool or weapon to help commit a crime that could be committed without it. In this category, the computer facilitates the crime by making the crime easier to commit. For corporate computer crime, examples of such facilitated crime are forgery of documents, intrusion, stalking, fraud, embezzlement, and theft of proprietary information. Any misuse of computer technology for illegal gain can impede the corporation's pursuit of objectives or create chaos.

The human factor cannot be ignored. Faced with the need to come up with quick cash, some find the use of computers as a tool to commit a crime too hard to resist. "Take the case of a branch manager who embezzled over $20 million from his bank over the course of 18 months. [Previously a data processing department worker, he] knew that the main computer would notify auditors if more than one million dollars were transferred from an account" (Parker, D., pg. 5). Additional crimes where the computer is used as a tool include harassing employees, stopping business dealings or hiding other thefts.

In the third category of corporate computer crime, the computer itself (or data contained within it) becomes the target. Attacks may be subtle, targeting individual files saved

on storage devices ranging from floppies to disk arrays, or bold, targeting business-critical systems such as e-mail, documentation, accounting, and payroll systems.

This category of corporate computer crime involves criminals known as crackers. The crackers target computers by cracking into systems with intent to sabotage and cause chaos to the corporation. Crackers may change or delete files, redirect websites or tie things up to keep out others. Methods to target computers for corporate computer crime include: the virus, which infects executable files and causes harm after infection; the worm, which copies itself and consumes space and time; the Trojan horse, which enters the target system and releases a virus or worm; and the logic bomb, which detonates at some future event and releases a virus, or causes other damage.

The final category of corporate computer crime is computer-related crime. Computer related crimes are crimes occurring to computer-related objects such as hardware or software. Hardware crimes include theft of computers, laptops, peripherals, internal chips, and other computer hardware. Software crimes include theft, counterfeiting, copyright violation and piracy of software.

Computer-related crime has become very lucrative for criminals. "In the 1980s, for example, the FBI estimated that the average computer heist took in between $400,000 and $560,000, whereas the average bank robbery netted between $4,000 and $19,000" (Friedrichs, D., 1996, pg. 178). The category of computer-related crime also includes the infiltration of a corporation's saved information contained within laptops and hard drives to utilize programming techniques only available through sales of licensed software.

Origins of Corporate Computer Crime

Each of the four categories of corporate computer crime can originate from either external or internal unauthorized access to anything computer related within a company. Many times a name, password, location of a key or an unlocked door is all that is needed to infiltrate a corporation's computer-related areas.

External criminals, outside of the corporate circle of employees and investors, tend to be technically knowledgeable about the potential value of the computer-related theft. Tactics used by criminals can initiate all four types of corporate computer crimes from as close as next door to as far as around the world.

The innocent hacker, while sometimes hard to differentiate from intentional crackers, has high success rates of reaching into a corporation's system and retrieving information. In a recent Internet Security Systems Seminar (2002), Gerulski quoted a client: "I get scanned dozens of times everyday. Less than 20 percent of those scans are U.S. based." Gerulski also noted many university computer systems are scanned within the first 15 minutes of putting a new computer on the network. While these scans may not cause damage, the results of the innocent hacking can be days or weeks of man-hours to guarantee the systems are secure from bigger cracker-type threats (Gerulski, D., 2002).

The external criminal using the computer as a tool appears in cases such as extortion. A recent case featured a cracker who was able to retrieve names, addresses and bank account numbers, which he later used in an attempt to extort funds from a large banking firm. "The intrusion into the server happened in early 2001, though the Russian did nothing for nearly eight months with the data he obtained…[in] 2001, the hacker began sending e-mail to ORCC's client bank, saying that he would post the data he'd obtained from the server on the Internet if he was not paid $10,000." Luckily, in this case, the incident ended with the hacker being caught prior to damage to both the bank and its customers (Costello, S., 2002).

When the external criminal uses the computer as a target, the computers are broken into similar to an intruder breaking into a home. This type of crime usually involves crackers who are either angry with the owners of the corporation or are acting as industrial spies. In the first instance, the cracker may initiate a Denial of Service (DoS) attack. Conry-Murray (2001) describes a DoS attack using an analogy of a mosquito attack: While in bed, and doing nothing, "[h]ad I just lain there, the bug would've come at me all night until it got what it wanted: my blood…Squash these bugs before they bite." One such attack he reported targeted the White House web site, www.whitehouse.gov. "In July 2001, Code Red 1 worm wriggled its way to prominence with a one-two security punch…Fortunately, the attack was easily thwarted… highlight[ing] the importance of good security administration" (2001, pp. 36, 38).

When the computer is a target of an industrial spy, individuals employed by the corporation's competitor conduct the crimes. In these cases, the theft of proprietary information can be extremely damaging to the corporation. In a 1996 documentary, cracking in the spying arena was estimated to have increased by142 percent per year. For the year of 1996 alone, 122 countries were caught spying against United States corporations through online espionage (CBS, 1996).

In the final category, computer-related crime, the external criminal is the thief of hardware or software. As technology advances, the external theft of computer-related items is increasing. Internal chips for computers, being extremely light, can be worth more by weight than diamonds. Theft of laptops and other hardware can be a two-fold prize, as both the device and the data contained within the device can be sold for cash to the black market or competitors. In 1996 Wallace described computer-related theft as the "new criminal," with software theft alone totaling losses of "5 to 25 billion dollars per year" (CBS, 1996).

While external criminals create major havoc for corporations, internal criminals may be even more destructive and cause higher monetary losses. Internal criminals tend to be disgruntled employees or greedy executives. As Cabot of Cabot Computer Consultants stated, "Internal sources have always been the major source" (personal communication, January 15, 2002). Because corporations rely on their infrastructure, the technology is at the internal criminal's fingertips on a daily basis. In many cases, resentment, mistrust, low moral or revenge are causes of this increased crime. According to Anne Chen (2002) in her recent article for eWeek, "Hacker exploits and denial-of service attacks may be snatching the headlines, but the biggest threats to security may be inside your company's network. They're employees who, either out of carelessness or malice, leave vital assets open to exploitation" (Chen, A., 2002, pg. 37).

Like external criminals, internal criminals can also initiate all four types of corporate computer crime. Innocent hacking may occur by internal criminals accessing areas they are not authorized to penetrate. Insufficient monitoring of employees can prevent most innocent hacking via internal criminals from being identified, unless inadvertent damage results. In these cases, offenders may incorrectly believe they are solving problems by finding out all information needed to complete the job requirements. When incidents are discovered, depending on corporate policy, internal hackers may face demotion, termination or criminal charges.

When internal criminals use the computer as a tool, crimes such as Salami fraud, in which trusted employees slice off small portions of numerous accounts and keep the proceeds, can occur.

"In a 1989 case, an accountant employed by New York City used a loophole in the city's computerized accounting system to divert $1 million to his own bank account" (Friedrichs, D., 1996, pg. 179).

When the computer is the target, internal criminals can search for information easily retrieved with access from written passwords posted on computer terminals or simple programs designed to crack passwords. Information such as trade secrets and personal information can be easily zipped or FTP'd to a competitor's computer in an attempt to sabotage the corporation when revenge is wanted. In 1993, one such case charged a consultant with "attempting to destroy a client's program by introducing a virus into it in the aftermath of a billing dispute"(Friedrichs, D., 1996, pg. 178). Ex-employees can also be dangerous, as exemplified in a recent report from the *New York Times* of an "IT executive who caused up to $20 million in damage when he sabotaged the computer systems of the New Jersey chemical company that had laid him off" (Scalet, S., 2001, pg. 60).

When there is computer-related crime by internal criminals, physical assets such as laptops, discs and chips, and software are blatantly taken through access naively granted by the corporation. Internal knowledge of auditing procedures, inattentive security, negligent licensing standards and questionable policies leave loopholes allowing internal criminals to go undiscovered for indefinite periods. Software piracy and copyright violations are extremely hard for the corporation to control. Many employees take advantage of this and believe they are entitled to software intended for work use only. Those taking software for home use do not hesitate to steal software for installation on one or multiple PCs outside of the office or share software with others.

Causes of Corporate Computer Crime

The causes of corporate computer crime are as numerous as the types of crime and can change on a case-by-case basis. Many cases of corporate computer crime can be traced to corporations inadequately protected as computer technology advances and reliance upon it increases. Additionally, many non-technical executives tend to see computer and information security differently than they do physical security. Because of this, the majority of causes of corporate computer crimes generally fall within two categories: technological advances and corporate standards.

Today's corporations must be aware that while the advancement in the technology available to them is increasing, so is the advancement of technology available to criminals. As e-mail has become a requirement for the corporation, attacks against e-mail systems have increased. As distributed computing has increased and become more available, so have the attacks against it.

Wireless computing, the latest trend in corporate information technology standards, has also opened new avenues for criminals. According to Symantec's Clyde, "there are now so many free tools on the Internet that hackers needn't be experts to cause problems; all they have to do is run readily available scripts" (Scott, K., 2001, pg. 56).

While the reach of technology has expanded, the lack of regulated corporate standards has become key to successful computer crime. Intending to create user-friendly interfaces for workers or to share data with customers and suppliers, many corporations have created an environment equally user-friendly to the corporate computer criminals. As systems get easier to use and administer, and corporations become more global and international, the added confusion of merged policies fails to keep standard access defined and regulated. Conry-Murray quotes Creed, the director of network security for Goodrich, as stating: "When you have 23,000 people and a hundred plus locations, policy gets all over the map really quickly"(2002, pp. 44).

To Report or Not to Report Corporate Computer Crime

When faced with corporate computer crime, the corporation must not only look at the types, origins and causes of the crime, but also weigh the negative against the positive aspects of reporting a criminal incident. "When an employee receives a threat via e-mail or trade secrets have been compromised, calling the cops is the obvious choice. However, if an employee is suspected of accessing information that's considered off-limits, it could be a matter best dealt with in-house" (Duffy, D., 2001, pg. 8). In most cases, however, the decision comes down to a matter of apprehension versus necessity.

Apprehension Elicits Corporate Silence

In many cases, the victimized corporation is afraid or apprehensive about reporting corporate computer crime. Both safeguarding corporate positioning and preventing investigative scrutiny force many corporations to deal with this crime on their own. Damian (2001), a computer science engineer from India, responding to whether incidents should be made public, expressed this viewpoint:

> Any security problem with regards to a firm should be dealt within it and it should not be let to the knowledge of others to have a hand at it to solve the problems as this could provide them additional advantage to explore (Damian, G., 2001).

The 2001 CSI/FBI survey indicates ninety percent of those responding agreed with Damian by avoiding reporting occurrences due to expected negative publicity. Seventy-five percent also responded with the belief that competitors would use the occurrences to their advantage (Power, R., 2001).

Many companies are concerned with publication of names and confiscation of computers, which could interrupt business. Some believe exposure of corporate computer crime can result in public embarrassment for the corporation and possible loss of competitive advantage to other corporations able to reap the benefits of the crime. Businesses do not want to be depicted as vulnerable and, in some cases, they have little faith in authorities to resolve the issues.

When asked in a survey questionnaire if all incidents are reported to the applicable authorities, Roy, Director of Security, Bombardier Transportation Group, answered:

> No, because most of the time a company doesn't want to be associated with the legal process and get that kind of publicity. It also depends on the security officer's background. If it is military or law enforcement chances are higher that the crime be reported. The IT background officers have a tendency to cover up because they feel (wrongfully) that their technical expertise will be challenged and they will look bad (personal interview, February 4, 2002).

While management should be alerted and legal council questioned, few corporations are aware of whom they should report to and others are afraid of surveillance or increased scrutiny of computer systems. Skeptical business leaders, suspicious of what authorities may help themselves to, are afraid of a possible

shut-down of entire systems and interruption of operations for an indefinite period of time.

> There's a prevailing misconception that as soon as you pick up the phone to call the FBI, teams of agents will swoop down on you with guns drawn to confiscate your computers and seize control—effectively closing down your business (Mayor, T., 2001, pg. 1).

Whether lack of first-hand knowledge or rumors of past incidents have fostered this view, corporations taking the stand of nondisclosure are left to fend for themselves when it comes to security.

Positive Resolution Necessitates Corporate Disclosure

In contrast to proponents of corporate silence, some experts believe a secure system is one widely open to peer review. This would apply even to small cracks in security. According to Scalet (2001), "not admitting that you have a problem is the first step to not recovering." An incident illustrating this:

> [A] large brokerage company got a call from hackers who claimed to have planted a logic bomb that would crash the company's computers at a certain time—unless the company paid them big bucks. The technical staff found no evidence of tampering, so the company ignored the call. Sure enough, the company's systems, which processed millions of dollars of transactions an hour, crashed at the appointed time. The next time the extortionists rang, the company knew that the threat was real and got law enforcement involved (Scalet, S., 2001, pg. 62).

Keeping quiet does not make the system more secure. In many cases, there is a social obligation to inform the public. This informative approach can help show how the corporation is prepared to respond. It will show shareholders procedures are in place to lessen the possibility of future crimes and show detection policies are in force. According to Roy's experience, he asserted "that it is possible to control these problems and most of the time turn them around as an advantage for the company" (personal interview, February 4, 2002).

Failing to cooperate with authorities and report the incident may permit the culprit to continue and eventually create adverse publicity or affect the bottom line for the corporation if released at a later date. In one well-known case, Egghead.com kept a corporate computer crime occurrence to itself. This crime involved the cracking of its systems, which enabled the criminals to access credit card account numbers of its customers. Egghead.com failed to notify these customers for four months. Although customers had lodged numerous complaints regarding illegal activities on their accounts, Egghead.com remained silent. Divulging the problem when it occurred and offering a rebate or coupon might have offset the customer's losses and kept them loyal to the company, but today, Egghead.com is no longer in existence (Gerulski, D., 2002).

In many cases, corporations do not have the opportunity to choose whether to report or not. In these cases, the crime violates a criminal code. The act of concealing knowledge of a felony is punishable and the corporation would be the criminal if it kept quiet. Due to the sensitivity of data, regulatory standards are common in banking and health care when dealing with security breaches or losses of data. Many contract requirements include information security disclosure clauses as well.

Whether required by law, contract or corporate policy, disclosing corporate computer crime has more benefits than corporate silence. Without disclosure and getting authorities involved, corporate computer crime cannot be aggressively prosecuted. If a corporation is successful in thwarting the advances of the culprit without legal action, the culprit is free to continue the pattern. According to Desmond's (2001) article on computer crime, "it should be clear that companies have far more to gain than lose by working with law enforcement… Law enforcement is getting better at finding and prosecuting perpetrators, but the process works far better if the victims cooperate" (pg. 2). If there is any chance of loss of trade secret data which may risk competition getting the information or not knowing who is attacking or what is being stolen, reporting may deter others by permitting authorities to investigate, locate, and facilitate prosecution and subsequent punishment.

Reporting Realities

Possibly surprising to many, the first federally prosecuted case of corporate computer crime took place 35 years ago, in 1966, before many of us knew anything about computers.

> The perpetrator was a young computer programmer working under contract with a Minneapolis bank to program and maintain its computer system…he changed the checking account program in the bank's computer so that it would not react to—and would not report—any naturally occurring overdraft condition in his account. (Parker, D., pg. 8)

While the programmer expected this to last only long enough to get him through a tough time, the embezzlement continued until it totaled $14,000. While small in comparison to more current large dollar corporate computer crimes, this original prosecution gave us a glimpse of the potential in this new avenue of crime.

During the 1970s and 1980s, most corporate computer crimes were nuisances. The 1980s changed that. With the advent of the PC era, many individuals were now able to have the computer power they enjoyed at work in the comfort of their homes. In August 1983, the face of corporate computer crime changed drastically as described by Standler (1999):

> [A] group of young hackers in Milwaukee hacked into a computer at the Sloan-Kettering Cancer Institute in New York City. That computer stored records of cancer patients' radiation treatment. Altering files on that computer could have killed patients, which reminded everyone that hacking was a serious problem. This 1983 incident was cited by the U.S. Congress in the legislative history of a federal computer crime statute (pg. 4).

When determining whether corporate computer crime is a nuisance or substantially damaging, one must consider the nature of the crime. According to Smith, Special Agent of the FBI Pittsburgh division and Awareness of National Security Issues and Response (ANSIR) coordinator, there is "greater volume [of] low dollar-nuisance. [But an] increasing number of high dollar matters" (personal communication, January 31, 2002).

By 1993, more than 100 viruses were being reported each month. Estimates recorded by Friedrichs in 1996 reported "annual losses due to computer crime…from $100 million to $5 billion…[with] estimate[s]…that only 1 percent of computer thefts [being] detected, and perhaps as few as 15 percent of these [being] reported" (Friedrichs, D., 1996, pg. 177).

When looking at today's statistics, the 2001 CSI/FBI survey indicated 64 percent of respondents reported unauthorized use of computer systems within the last 12 months. The two most likely sources of these attacks included independent hackers and disgruntled

TABLE 1

CERT Incident Log Data

	Number of incidents reported	Vulnerabilities Reported	Security alerts published	Security notes published	Mail messages handled	Hotline calls received
1995	2,412	171	31	N/A	32,084	3,428
1996	2,573	345	53	N/A	31,638	2,062
1997	2,134	311	50	N/A	39,626	1,058
1998	3,734	262	34	15	41,871	1,001
1999	9,859	417	22	1	34,612	2,099
2000	21,756	1090	26	57	56,365	1,280+
2001	52,658	2437	41	341	118,907	1,417+

(CERT/CC Statistics, 2002, pp. 1-3)

employees, with U.S. competitors, foreign corporations, and foreign governments also being stated. Total annual losses from corporate computer crime of those responding in 2001 were reported to be $377,838,700 (up $112,242,460 from last year) (Power, R., pp. 6,9,11). The Computer Emergency Response Team (CERT) (2002) also shows steady increases in computer crime activity as shown in Table 1.

Sample cases of corporate computer crime include a $10 million dollar theft from Citibank and the catching of Kevin Mitnik in 1994, and multiple Denial of Service attacks in 2000. Attacks feared today as a result of the September 11, 2001 terrorist attacks have increased the awareness of security risks and needs:

> Skirmishes in the hills of southern Afghanistan grab today's headlines, but there are pitched battles occurring on other fronts that don't always make the news. In the last two months, a bout of work attacks has struck untold numbers of companies around the globe. In November W32.BadTrans.B-mm swept through 50 countries, as did Nimda.E, the latest version of the Nimda worm. During the past couple of weeks, the Goner worm has successfully infected about 840,000 machines worldwide. Computer Economics estimates damages from this latest worm total at least $7.5 million. (D'Antoni, H., 2001, pg. 72.)

Recent reported and prosecuted cases found within the CCIPS section of the U.S. Department of Justice (2002) continue to illustrate the increasing corporate computer crime statistics (as shown in Table 2).

Existing Laws and Regulations

While the chart identifies some of the prosecuted cases within the past few years, corporate computer crime can be difficult to prosecute under traditional laws and regulations. In traditional crimes, taking someone's property is considered larceny. Breaking and entering into a building is considered burglary. In many corporate computer crime cases, however, no one is breaking into a building. Entering a system through a telephone line is not the same. While computer hardware theft is covered by traditional laws, the electronic information contained within a computer "represents a new form of 'property' less clearly protected by traditional laws" (Friedrichs, D., 1996).

Larceny, theft of services, trespass, embezzlement, destruction of property, copyright violations and mail and wire fraud are traditional legal categories used to prosecute some corporate computer crimes. In many cases, civil review is needed to bridge the gaps of traditional laws. Many corporate computer crimes fall under traditional financial crimes, as most affect financial assets. Traditional laws are also appropriate when dealing with computer-related crime and thefts of computer-related objects. In most cases, state and federal laws exist for these crimes.

The nature of computer crimes, however, makes it hard for traditional laws to cover the entire offense. When a computer is destroyed, destruction of property is apparent. When someone destroys or illegally accesses or copies files on a computer, the damage is harder to identify and when identified, it may not constitute destruction of property or theft.

The first federal computer statute, enacted in 1984, was rewritten into the Computer Fraud and Abuse Act of 1986 (CFAA) when the 1984 statute was found to be inadequate. By the end of the '80s, most states had passed computer crime laws. Although each state's statutes were based on the 1986 federal statute, each also contain fundamental differences, making interstate prosecution difficult. Most states have since taken the initiative to update their statutes, as has the federal government.

According to Horoski, Highmark Systems Engineer Specialist and Special Deputy Uniform Division, Allegheny County Sheriff's Department,

> lately more and more prosecutions ARE occurring. This is true even in the case of minor incidents. There are several reasons for this. Case law has been established, PA crimes codes have been amended to address these crimes, prosecutors are becoming more educated in technology based crimes and the subsequent ways to prosecute them successfully. (personal interview, February 8, 2002)

Enforcing these laws, however, is the problem. Schwartau stated support for a national policy resolution in a 1996 documentary:

> We have the technology, we have the solutions to protect against breaking and entering into computer systems. We have this entire suite of capabilities but we've chosen not to do anything about it through apathy, through arrogance, through a reluctance to invest in our future. We have to overcome that and part of that's gonna come through national policy. (CBS, 1996)

In 1992, punishment for damage to information contained on the computer or prevention of use of a system was added to national law and in 1996, criminal penalties listed were added to electronic espionage. However, work remains to be done.

> Laws specifically prohibiting computer crime are quite recent and not easily enforced. In addition to federal statutes, local laws and procedures at the state levels exist, but in some opinions, "most state statutes are not adequate to punish computer criminals" (Friedrichs, D., 1996, pg. 180).

TABLE 2

Recent prosecuted corporate computer crime cases

Case name and date	Type of breach	Loss estimate	Sentence in months	Restitution	Explanation of crime
U.S. v. Osowski 11/26/01	Confidentiality	6.3M	34	7.8M	Cisco accountant stole stock from company
U.S. v. Torricelli 9/5/01	Confidentiality Integrity	N/A	8	4K	"#conflict" hacking group member
U.S. v. McKenna 6/18/01	Confidentiality Integrity Availability	13K	6	13K	Disgruntled former employee
U.S. v. Sullivan 4/13/01	Integrity Availability	100K	24	194K	Disgruntled former employee
U.S. v. Morch 3/21/01	Confidentiality	5K	36 (probation)	0	Employee theft of proprietary company info.
U.S. v. Ventimilia 3/20/01	Integrity Availability	209K	60 (probation)	233K	Disgruntled GTE employee
U.S. v. Sanford 12/6/00	Confidentiality Integrity Availability	45K	60 (probation)	45K	"HV2K" hacking group member
U.S. v. Gregory 9/6/00	Confidentiality	1.5M	26	154K	"Global Hell" hacking group member
U.S. v. Smith 12/9/99	Integrity Confidentiality	90K	21	3K	Member of "The Darkside Hackers"

(Computer intrusion cases, 2002, pp.1-2)

Most recently, however, H.R. 3162, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001," passed on October 26, 2001, gives more power to authorities in dealing with computer crime, including:

> [Authority to arrest] and charge a hacker who breaks into a computer, even if the hacker's Internet traffic merely travels through U.S. computers or routers… Previously, the United States could prosecute hackers only if they attacked U.S. systems. Under Section 814 of the Patriot bill, any activity deemed illegal by the United States involving "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" is considered a crime (Hulme, G., 2001, pg. 22).

This recent bill resulted in a mandate to establish nationwide Electronic Crimes Task Forces to create a backbone of support for public and private sectors. These taskforces, along with the bill itself, recognized the Secret Service philosophy of "bringing academia, law enforcement and private industry together to combat crime in the information age" (USS Electronic Crimes Task Force Regional Locations, pg. 1).

Even with the PATRIOT bill, issues remain unresolved relating to the international corporate computer crime. Foreign-based prosecutions are very different from those contained within the United States. When dealing with foreign criminals, differences in laws regarding collections of evidence, local jurisdiction, extradition, territoriality, language, and time zones are only a few of the problems faced in legal battles. Outside of the United States, few countries have existing cyber-crime laws, and most are mainly interested in protecting their own. Additionally, activity viewed as illegal in one country may be legal in another. While the United States recognizes the existence of this global threat, the limitations of existing treaties still need to be addressed.

The nature of corporate computer crime crosses borders, complicating investigations and prosecutions. A well-known recent case involved the "Philippine government's decision to drop all charges against 'Love Bug' suspect Onel De Guzman." While the Philippines had entered a Mutual Legal Assistance Treaty with the United States, this was not a "conviction law." The "commitment of each individual country to enforce computer crimes" is needed. Without commitment, "treaties won't be worth a whole hell of a lot," stated Toren, former prosecutor in the U.S. Department of Justice's Computer Crimes and Intellectual Property section. (Burke, L. 2000, pp. 1-2)

Although international regulations are rare and corporate computer criminals have succeeded in committing billions of dollars in damage internationally, it is enlightening to see there is some push for coordination. A new treaty in Europe, if successful, may be one of the first steps to collaboration:

> Last May, the Council of Europe, working with Canada, Japan, South Africa and the United States, approved the 27th draft of the Convention on Cybercrime, the first international treaty on crime in cyberspace…participating countries will be required to create laws that coincide

> with regulations in the treaty…The treaty will also allow one country to obtain information…from another country, possibly leading to the arrest and extradition of the hacker. (Wall, B., 2002, pg. 102)

Global consensus of what defines a computer crime is the first step. Defining the differences in the types of laws and constituting a common framework is needed.

Corporate Computer Crime Remedies

When looking at corporate computer crime, the numerous types of crime and the issues involved in coming to a decision to report an incident or not, it seems obvious the remedies involve both the authorities and the corporations. Not unlike individual persons, however, each believes its way is the right way to do things. Each belief can be valid and must be considered as part of the total solution to the problem, but combined, they may be able to create a greater wall of defense against and attack upon the corporate computer crime predator.

Authorities

Upon first assessment, many authorities view corporate computer crime as less of a priority because it is not a violent crime. "The principal training of police personnel is oriented toward conventional crime… and [corporate crime is] likely to require a greater investment of time than typical conventional crime cases" (Friedrichs, D., 1996, pg. 272). Local authorities have a hard time seeing corporate computer crime as a major impactor on their local jurisdictions. If a physical component is involved, they can normally handle it. However, "[in] local jurisdictions in which special computer crime investigative units have been established, they must compete for finite resources with other units (such as a drug enforcement unit) that have a higher priority" (Friedrichs, D., 1996, pg. 180).

Protocols must be enacted to address training needs to bring local authorities up to date with the technology. Inter-agency coordination and cooperation is crucial. Because of the complexity of corporate computer crimes, often local agencies are unable to handle these cases, but once they get the first call, their calls for help to other authorities can help uncover trends in incidents.

While some believe the authorities are incapable of preventing corporate computer crime, in certain cases they have successfully combined state and federal strengths, resulting in competent responses. This combination comes as no surprise, as many corporate computer crime cases cross state and national lines. Federal agencies seem most appropriate for these cases, with the FBI becoming the focal point of reporting. Unfortunately, lines demarking areas of jurisdiction among the federal government authorities are not well enough defined at this point, preventing adequate integration. For instance:

> [T]he NIPC was to include the FBI and Secret Service agents as well as other investigators with experience in computer crime and infrastructure protection [however] contrary to Secret Service expectations, neither of the agents was allowed to participate in investigative activities or assigned responsibilities…as a result, the Secret Service withdrew its detailees in October 1999 (Critical Infrastructure Protection, 2001, pg. 83).

Enlarging the problem is the present fact that not all authorities are required to report to one central agency.

While the authorities work through the process of determining the best protocols for notification, technologies are advancing. Authorities must take the time to keep abreast of technological advances, because the criminals are quick to take advantage of advances on a daily basis. For example, "data scrambling technology that allows consumers to send their credit card numbers across the Internet or send commercial e-mails in complete privacy, also makes it harder for governmental authorities to catch criminals" (National Business Institute, 2001, pg. 327). Training courses, such as the Law Enforcement Training Session from the DOJ/FBI (CFP96), stress awareness of electronic crime as crime and the changes in federal legislation to deal with it.

While national authorities lead the charge within both the FBI and DOJ, some states have set up their own task forces and local agencies have begun requesting assistance from industry professionals. The hope is that they will "boost their cybercrime savviness and win the trust of corporate America" (Mayor, T., 2001, pg. 4).

Even with this increase in awareness, and the hopeful statistics of increased reporting of corporate computer crimes by local business, the state continues to decide whether or not to pursue investigation of individual cases. Selection and prioritization of crimes reported can easily result in a criminal case being declined for prosecution. According to Scalet (2001), the FBI seems interested only in cases where there is business loss of more than $5,000 and where stores located in more than one state are affected by the loss (Scalet, S., 2001). Shore, Special Agent, FBI Pittsburgh and Infraguard, clarified this better by stating the FBI won't "get into a case if no prosecution is expected or without federal interest." (personal interview, January 16, 2002).

Quantifying the loss is not always the roadblock to prosecution. At times, local authorities are limited by their technical, budgetary and personnel resources. In addition, the resources of the whole judicial system must be considered (from the judges to the correctional system). Violent criminal cases have qualities that may attract the attention of politicians, and the electorates they depend on. Selection and prioritization is the only way authorities can devote what little time, effort and money that is available to corporate computer crime (Shover, N. & Wright, J., 2001).

Although prevention and detection is the responsibility of the corporation, law enforcement officers, once involved in an investigation, "can look for patterns, collect evidence and sometimes put hackers behind bars" (Scalet, S., 2001, pg. 62). Forensic methods for investigating corporate computer crime can often be productive. While many corporate computer criminals believe their crimes are erased by deleting files, the evidence obtainable through proper forensic investigative procedures can prove them wrong. The recent Enron bankruptcy case has highlighted this fact. "It is impossible that [congressional investigators] cannot find data on those hard drives. There are too many computers involved…[They] will find enough to make a story," according to Sanders, a computer forensics expert from New Technologies Inc. (DiSabatino, J., 2002, pg. 65).

The proper forensic investigative procedure is key to recovering admissible evidence. Protecting data integrity and the chain of custody are imperative. In any case, corporations must realize that by changing the slightest bit of data, their evidence may be disallowed in court. "The original evidence must be locked up and have a clear chain of custody" for use in forensic investigations (Scalet, S., 2001, pg. 62). Five steps have been identified and are being followed by many investigators: Isolate and secure, copy, investigate, evaluate and document. During this sequence, all "standard forensic and procedural principles must be applied." Evidence must not be accessed or altered and

it must be preserved for later review. Individuals who investigate corporate computer crime must be trained and held responsible for all actions "while such evidence is in their possession" (Gottfried, G., 2001, pg. 90).

Gathering, sharing, and disseminating information related to corporate computer crime can be as important as the forensic chain of custody. The goal should be more coordination with the police authorities and less duplication. Currently, no national clearinghouse exists for dealing with corporate computer crime, and, in many cases, lack of information may perpetuate self-policed businesses reluctant to report. Authoritative use of new technologies (such as surveillance) and sharing of incident information across the multiple agencies may assist in the prosecution of corporate computer crimes.

Corporations

Similar to the authorities, corporations have had the history of viewing corporate computer crime as a small problem in the scope of making a profit. Gerulski (2002) quoted Forrester: "Enterprises spend more on coffee supplies than on IT security" (2002). Most corporations do not believe corporate computer crime will happen to them and security is viewed as something needing to be focused on physical assets only.

This position is not new to corporations. An example from the past demonstrates that corporations have not changed much in their response to cutting technologies in the past 100 years. In 1882, when sprinkler systems were introduced into the marketplace, few corporations saw the value in securing their business assets from something they believed would not happen to them. "Sprinklers were considered to be as dubious an investment as information security is today," but once the businesses had them, they "could stop thinking about fires and start thinking about their business" (Berinato, S., 2002, pp. 43, 52).

History has shown that corporations can be slow to see the value in security, but the recent events of September 11, 2001 may change this. While computer and information security is complex, constantly changing, and requires training, experience, and justification of expenses, computer and information security is essential to business survival. According to Roy, "the process and tools exist, it is more a matter of getting the companies and different organizations aware of the problem so they invest more money and resources" (personal interview, February 2, 2002).

Most businesses are not immune to "the threats of system downtime and data loss. In large organizations, a major computer outage can halt work across a broad swath of the enterprise" (Merchantz, B., 2002, pg. 31). A plan of action created in advance of an attack is needed. Scalet (2001) explains:

> When business and IT employees think they're under attack, they panic. They call all the wrong people. They start rebooting or unplugging computers, and in the process they often do more damage—either to data, business continuity or to the organization's reputation—than the intruder would have done. (Scalet, S., 2001, pg. 60)

Identifying crucial information, strategic direction, potential confidentiality issues, and protection levels is the first step. To do this, many corporations put security in the hands of systems specialists. Knowledgeable security experts familiar with the corporation's industry can address account creations, administrative access and permissions as well as potential holes in the system. If a business is to recover following a computer crime occurrence, however, it must have stringent insurance and backup processes, and a willingness to pursue criminal and civil damages where applicable.

Insurance coverage comes into play when dealing with a loss of corporate identity or proprietary information. Unfortunately, while security concerns are now at a peak within corporations, insurance coverage for information security may be harder to find and come at higher rates since September 11, 2001. "Many insurers will exclude online assets from standard commercial insurance policies this year, shifting the coverage to costlier supplemental policies." Some policies will offer no coverage if damage is terrorist-related. This supplemental insurance comes at a great cost to the corporation. Policies covering "viruses, security breaches…can range from 2 percent to 8 percent of the overall premium's cost…[often with the requirement of an] audit of security systems and policies…" (Hulme, G., 2002, pg. 24). Because of the increased cost and increased scrutiny of systems, many corporations have concluded that this added insurance is unnecessary.

Insurance coverage may not be the answer for all corporations, but all corporations must avoid complacency about securing their computer systems. Even a good cybercrime insurance policy does not remove the responsibility for diligence by the corporation. Keeping the management informed, maintaining an organized system administration standard, and educating employees is crucial. Many prepared corporations have computer systems and websites recoverable from corporate computer crime by just restoring systems from backups. At the time of a security breach, the administration must improve security and then reopen as soon as possible.

Improving security, either before a corporate computer crime or after, includes controlling restricted access to information as well as physical assets. Raising the awareness of technological changes and the need for computer forensics standards and education among all employees is needed. Use of technologies, from basic to high-tech, is imperative to secure the corporation. These technologies include:

- Securing locations where computer hardware is used and stored by maintaining control of laptops and access to all hardware as well as securing hard disks and data media.
- Securing on-line data by installing software security packages requiring passwords, installing network firewalls, installing and using virus protection software, and safeguarding confidential information.
- Preventing employee downloads of pirated software, shareware or freeware, preventing unauthorized capabilities to download from the Internet, and utilizing encryption for email.
- Utilizing internal auditing systems to direct internal software developers to develop software without vulnerabilities; utilizing network and host intrusion detection to prove the need for spending on security; utilizing proven security models (such as ISO 17799 focused on best practices for information security); and becoming more concerned about partners that access your systems.

(National Business Institute, 2001)

Identifying how much corporate computer crime can cost the corporation is imperative in determining how much to spend on security. Knowing the importance of the assets involved and being aware of the information technology available to the corporation and valued suppliers and partners are the first steps. Preventing misuse of access and information is a necessity. The corporation should never overestimate the loyalty of its employees or partners. Once access is given, it can easily be transferred to others.

This heightened awareness, respect and reliance on security must be maintained. Cor-

porate computer security should be a habit, but people "fall into and out of habits. People get blasé" (Conry-Murray, A., 2001, pg. 44). David Gerulski stressed that people should be first, then planning, then technology (2002). With this in mind, informing the employee population of the corporation about security policies should be addressed first. The employees should be made aware of the policies of the corporation. Awareness is a virtually cost-free proposal to most corporations. Electronic mailing lists, weekly or monthly newsletters or bulletins on a company Intranet can encourage security measures without additional cost to the corporation.

These security measures should be based on a standard policy for information technology for the corporation. To succeed in getting corporate acceptance of the policy, the policy should be implemented from the top down, beginning with acceptance and utilization by top management in the corporation and following down the ladder with strict requirements. A checklist of things to incorporate into a security policy document given by Wood, CISA, CISSP, independent information security consultant included:

1. "Perform background checks for all workers"
2. "Maintain a low profile in the public's eyes" (keeping computer centers out of reach)
3. "Wear a badge when inside company offices"
4. "Update and test information systems contingency plans"
5. "Store critical production data securely at offsite location"
6. "Install latest patches on systems located on network periphery"
7. "Install and monitor intrusion detection systems"
8. "Turn on minimum level of systems event logging"
9. "Assign explicit responsibility for information security tasks"
10. "Perform periodic risk assessments for critical systems"

(Conry-Murray, A., 2002, pg. 48).

Self-regulation through tough policies is imperative. When determining what safeguards to address, Parker (1998) suggests: "Common sense and organization objectives" for keeping it focused and yet secure; "Good advice from experienced experts" whose knowledge and competence can be priceless; Utilizing "security controls at reasonable cost from trusted vendors" to keep the security tight and assume best practices; and looking at benchmark cases and "practices of other organizations under similar circumstances" to determine the best route to follow for the corporation's specific needs (Parker, D., 1998, pg. 24).

These pre-defined policies for security control and for "responding to disaster— whatever shape it takes—can help guide a company through a crisis" (Conry-Murray, A., 2002, pg. 49). Along with these policies, Carnegie Mellon's CERT team believes response plans should take the following into account: "1. Triage: Identify, categorize and assign informing information" through which trends may be identified, and intrusions prioritized; "2. Analyze: Examine the report and identify actions to be taken," permitting investigation and evaluation of the seriousness of the threat; and "3. Respond: Will your team report to other[s]," permitting predefined communication channel alerts, whether corporate only, or including authorities, for further preventive actions (Bragg, R. 2001, pg. 27).

Creation of a corporate incident response team can be beneficial. The team should include representation from executives, IS, all business units, public relations, the legal department and human resources to create a functional team willing and able to respond in a crisis. Training and having all on board prior to the crisis will streamline the discussion on whether or not to report and how to deal with any issues while protecting the corporate reputation (Duffy, D., 2001).

With no response team, at a minimum, maintenance of internal incident reports and outside reports is "crucial for determining the effectiveness of security and monitoring trends over a period of time"(Parker, D., pg. 472). Keeping aware of local or market-related threats is also important, because even the best security rigidly identified and followed can have holes.

Because damage often involves the loss of intellectual property, losses may not be easy to calculate or identify. When the crime is reported to authorities and prosecution results, corporations can sue the perpetrator for civil or tort damages. For example, when dealing with a computer virus, there "is also a possibility of a class action by corporate and personal victims against a person who wrote and initially released a computer virus" (Standler, R., 1999, pg. 8).

Unfortunately, most criminals using viruses are young, with few assets, or else outside the jurisdiction of notified authorities. Smith, FBI, stated that even with "civil proceedings you may never truly know what the full scope of the damage was, or if the cancer has even been fully identified. Still the civil process is appropriate, as opposed to criminal, in certain cases" (personal interview, January 31, 2002).

Cooperation with authorities

Today, with the threat of cyber terrorism, every alliance available can be important. Varon quotes Vatis, a former FBI official and current director of the Institute for Security Technology Studies at Dartmouth College: "It's important [that CIOs] look at the government as a partner…In turn…government can share information about IT security threats and vulnerabilities that might be difficult for CIOs to learn on their own" (2002, pg. 41).

Through trusted relationships between private sector and government entities, alerts of potential threats can be shared. One such successful collaboration was that between the Electric Power Industry and the NIPC, in which "information gathered through the electric power industry led to detection of a potentially damaging computer exploit and issuance of a warning to industry members and the public" (Critical Infrastructure Protection, 2001, pg. 74). In some cases, participating corporations "already voluntarily exchange security incident and vulnerability data with Infraguard, a partnership among businesses, the FBI, various government agencies and academic institutions" (Colkin, E., 2001, pg. 23).

The U.S. government recognizes these potential benefits for both the private and public sectors. November, 2001 recommendations to Congress included "development of a 'top to bottom' national approach to dealing with potential cyber security issues, which involves federal, state and local agencies as well as private sector cooperation" (The cyberterrorism threat, 2001, pg. 1). It is then left to corporate leaders to determine whether collaboration will benefit them.

As the government begins to realize the potential benefits of information sharing, corporations look back at the government for assistance. Many corporations, recalling incentives given to corporations for the Y2k preparedness initiatives, hope the federal government will intercede by minimally requiring "security vendors to provide better products," and offering government subsidized "loans for small to medium-sized busi-

nesses for equipment and training"(Carlson, C., 2001, pg.17).

While the degree of involvement has not been defined completely, many government entities are willing to work with corporations to prevent corporate computer crime. Many companies have yet to realize the usefulness of the tools available to various policing authorities. These include negotiation power between nations, time zones, languages, "investigative skills, forensic knowledge, access to attachés in foreign countries, and established relationships with Internet players as big as Cisco Systems and as small as the local ISPs." (Mayor, T., 2001, pp. 2-3).

In one case involving innocent hackers, calling the FBI was the solution to the problem. The authorities were able to use their resources to turn "several of the group members into informants…[while they] tracked entry points, contacted ISPs, pored over logs, monitored hacking channels and contacted owners of each machine that had been hit." The result was prosecution of the one non-juvenile member (Mayor, T., 2001, pg. 2).

A foundation of trust is needed. Most corporations face the unknown when dealing with criminal issues and most government authorities face the unknown when dealing with corporate issues. Without the sharing of information, corporations and governmental agencies cannot determine whether the threat has occurred to only one victim or multiple victims. Having access to databases containing logs of reported corporate computer crimes as well as remedies utilized to correct damaged systems can initiate warnings, prevent recurrence and help prosecute the criminals. With this information, corporations can better understand the risks and the civil authorities can better understand both the nature and number of crimes committed.

The differences between corporate and governmental motivations, which result in differing perceptions about threats, vulnerabilities, and risks, can only be addressed when information is shared between the two. Some associations have been created to deal with information sharing on corporate computer crimes. These include:

- CERT—Computer Emergency Response Team—federally funded incident reporting alerting, research, and training
- CIAO—Critical Infrastructure Assurance Office—outreach to private sector, state and local governments to share information, coordinate incident response, training, R&D and help with legislation and creation of a national plan.
- ECSAP—Electronic Crimes Special Agent Program—United States Secret Service Electronic Crimes Taskforce—training for forensic investigation of computer crimes and public/private information sharing effort.
- Infraguard—run by FBI and NIPC in cooperation with private sector in which interests and knowledge in both sectors are combined to enable information flowing between them on threats and attacks of infrastructures.
- Internet Security Alliance—best standard practices for both legislators and industries
- ISACS—Information Sharing and Analysis Centers—industry specific info for critical infrastructure sectors such as electric, financial, information technology, oil & gas, telecom, U.S. government and water.
- NIPC—National Infrastructure Protection Center—government agencies, state, local government and private sector issuing attack warnings and guidance.
- SANS Institute—analysts and forensic handles—cooperative research between education and organizations, system administrators and professionals.

While this listing is in no way comprehensive, it exemplifies organizations currently available to assist in the reporting, investigation and assistance of cooperation between authorities and corporations. The problem lies, however, in not knowing which organizations should be contacted in a given case. As with border jurisdiction conflicts, possible turf wars and lack of collaboration is possible with so many associations attempting to do the same thing. While competition can often be good, and is very appropriate for sector-driven issues, over-duplication can be extremely wasteful.

Conclusion

Whether internal or external, innocent or not, corporate computer crimes occur on a daily basis. Advances in technology have created an environment in which criminals would be stupid not to take advantage of existing holes in the corporate infrastructure. Corporations, concerned about possible negative impact on their companies, face the perplexing dilemma of whether to take chances and report computer crimes or omit reporting them and risk further assaults.

Potential damages because of corporate computer crime are almost beyond comprehension. Criminal prosecutions, while paling in comparison to the number of corporate computer crimes committed, can only occur if reported to authorities. Legal statutes can also only be modified if the economic risks resulting from corporate computer crimes are identified. At that point, law enforcement agencies can be made aware of the magnitude of the problem and attempt to train and staff accordingly. Until then, authorities maintain jurisdiction to the best of their abilities through selection, prioritization as well as procedures and use of technology.

Corporations must respond to news of corporate computer crime by reverting to recovery policies. Those able to prepare sufficiently for the multitude of possible corporate computer crimes will be able to respond quickly to crisis situations. With the aid of insurance coverage, support from management, awareness of technology advances and security policies, corporations may be able to minimize their risks.

Through the power in numbers, cooperation between governmental entities and corporations open the door to greater resolution of the problem. Trusting relationships between the two are needed to promote a working relationship that benefits both and to share a broader awareness of the problem and possible solutions.

Corporate computer crimes are likely to continue in unanticipated ways. With the threat of digital catastrophe at our doorsteps because of the September 11 terrorist attacks, well-defined policies are necessary. Future possibilities may include legislation forcing corporate disclosure while protecting corporate anonymity, as both authorities and corporations stay one step ahead of the criminal. Additional future focus should be placed on strengthening agreements, treaties and associations across interstate and international borders.

Short of returning corporations to pencil and paper and totally eliminating computer systems, corporate computer crime is here to stay. Continuation of corporate silence, while possibly protecting a small piece of the economy, hurts the whole by keeping the information secluded. Today's growing computer crime statistics suggest a matching need for increased realization that computer security is vital to the continuity of a corporation. Information sharing and alliances between corporations and the government will be nec-

essary to create an environment that is hostile to the growth of corporate computer crime. Utilization of an Infraguard-style organization can serve to bridge the gap between corporations and civil authorities. This collaborative power in numbers can then facilitate the common goal of corporate computer crime prevention.

References

———. (2002). *CERT/CC Statistics 1988-2001.* Retrieved January 31, 2002, from http://www.cert.org/stats/cert_stats.html, pp. 1-3.

———. (2001). Critical infrastructure protection: Significant challenges in developing national capabilities. *United States General Accounting Office report to the subcommittee on technology, terrorism and government information, committee on the judiciary, U.S. Senate.* Retrieved January 31, 2002, from http://www.gao.gov/new.items/d01323.pdf, pp. 1-108.

———. (2002). Computer intrusion cases. *Computer crime and intellectual property section (CCIPS).* Retrieved January 3, 2002 from http://www.usdoj.gov/criminal/cybercrime/cccases.html, pp.1-7.

———. (2001). The cyberterrorism threat: All too real. *Technobabble.* 2 (6), pg. 1.

———. (n.d.) *USS Electronic Crimes Task Force Regional Locations.* Retrieved February 13, 2002, from http://www.ectaskforce.org/Regional_Locations.htm, pp. 1-5.

Bernato, S. (2002). Finally, a real return on security spending. *CIO magazine*, 15 (9): 42-52.

Bragg, R. (2001). Critical response teamwork. *Enterprise systems journal*, 16 (12): 22-28.

Burke, L. (2000). Love bug case dead in Manila. [Electronic version] *Wired news.* Retrieved January 9, 2002, from http://www.wired.com/news/politics/0,1283,38342,00.html, pp. 1-2.

Carlson, C. (2001). Cybersecurity: Striving for public/private pact. *eWeek*, 18 (41): 1, 17.

CBS (Producer). (1996). *20th century with Mike Wallace: Criminals in cyberspace.* New York, NY: A&E Home Video.

Chen, A. (2002). Watching your back: The biggest threats to security may already be inside your network. *eWeek*, 19 (3): 37-38.

Colkin, E. (2001). IT security and the law. *Information week*, 865: 22-24.

Conry-Murray, A. (2002). Security policies in a time of terror. *Network magazine*, 17 (1): 44-49.

Conry-Murray, A. (2001). Swatting persistent security pests. *Network magazine*, 16 (12): 36-42.

Costello, S. (2002). Russian hacker arrested in bank extortion case. [Electronic version] *InfoWorld.* Retrieved February 7, 2002, from http://www.infoworld.com/articles/hn/xml/02/02/06/020206hnrussian.xml?0207thunknown.

D'Antoni, H. (2001). As the worm turns: Disclosing a hack. *Information week*, 868: 72.

Damian, G. (2001, December 6). *Encryption is not to let known to others.*[#6 of 10]. Message posted to http://cwforums.computerworld.com/WebX?50@@.ee9af0d.

Desmond, P. (2001). Take a bite out of computer crime. [Electronic version] *Datamation.* Retrieved January 9, 2002, from http://www.wired.com/news/politics.0,1283,38342,00.html, pp. 1-4.

DiSabatino, J. (2002). Enron bankruptcy case highlights e-mail's lasting trail. *Computerworld*, 36 (4): 65.

Duffy, D. (2001). Don't press the panic button. [Electronic version] *Darwin magazine.* Retrieved February 13, 2002, from http://www.darwinmag.com/read/090101/panic_content.html, pg. 1-13.

Friedrichs, D. (1996). *Trusted criminals: White collar crime in contemporary society.* Belmont, CA: Wadsworth publishing company.

Gerulski, D. *Are you vulnerable? (Internet Security Systems Seminar),* January 30, 2002. Pittsburgh, PA.

Gottfried, G. (2001, February). Taking a byte out of crime. *Network magazine*, 16 (2): 90-94.

Hulme, G. (2001). Antiterrorism law targets hackers around the world. *Information week*, 866: 22.

Hulme, G. (2002). Insuring against cybercrime gets tougher. *Information week*, 870: 24.

Mayor, T. (2001). Break glass, pull handle, call FBI. [Electronic version] *CIO magazine.* Retrieved January 9, 2002, from http://www.cio.com/archive/060101/fbi_content.html.

Merchantz, B. (2002). Adopting a managed availability philosophy. *Contingency planning and management*, 7 (1): 31-33.

National Business Institute. (2001). *The law of the internet in Pennsylvania.* Eau Claire, WI: Author, pg. 327.

Parker, D. (1998). *Fighting computer crime: A new framework for protecting information.* New York, NY: Wiley computer publishing.

Power, R. (2001). 2001 CSI/FBI computer crime and security survey. *Computer security issues and trends*, 7(1): 1-20.

Scalet, S. (2001). How not to recover from getting hacked: A loser's guide to failure. *CIO magazine*, 15 (5): 60-64.

Scott, K. (2001). Zeroing in. *Information week*, Issue 862, pp. 50-57.

Shover, N. & Wright, J. (Ed.) (2001). Crimes of privilege. New York, NY: Oxford University Press, pp. 381-390.

Standler, R. (1999). *Computer crime.* Retrieved January 3, 2002, from http://www.rbs2.com/ccrime.html, pp. 1, 4-8.

Varon, E. (2002). Homeland defense: New rules of war. *CIO magazine.* 15 (7): 40-44.

Wall, B. (2002). An imperfect cybercrime treaty. *CIO magazine*, 15 (9): 102-104.