Fighting Crime in the Cyber-Age: A new Challenge for Law Enforcement

Bill Netterville

Abstract

Computers are becoming an increasingly important part of everyday life. They also provide new opportunities for criminal enterprise. The computer provides both new types of crime, and new ways of perpetrating traditional crimes. Computer crime investigation differs from more traditional crime investigation in several critical ways and will require law enforcement agencies to adopt new policies and practices. This paper documents the increasing rate of computer-based crime, points out several critical areas where it differs from more traditional crimes, and outlines some new problems and issues which law enforcement must address to combat computer crime. Finally, this paper suggests a plan of action suitable for many law enforcement agencies to prepare for dealing with computer based crime.

Introduction

The widespread adoption of the personal computer has changed the way we live. Every day personal computers (PCs) become more and more mainstream, performing various functions in our business, personal and recreational environments. They have automated many of the menial tasks of business, such as accounting, payroll, filing, record keeping, etc. This increased use of technology has caught the attention of the criminal element. The computer has become both target and tool to a new breed of cyber-criminal. These criminals utilize the evolving technology surrounding computers to commit crimes. They use the computer to more efficiently perpetrate traditional crimes, and also commit new types of crime made possible by the computer itself. A 1989 Florida Department of Law Enforcement (FDLE) survey of public and private sector businesses which utilized computers found “that of the 403 respondents, 25 percent reported that they had been victimized by computer criminals” (Carter & Katz, 1996, pg. 2).

From a law enforcement perspective, computer related crime differs significantly from more traditional criminal activity. Investigation of computer crime will require the law enforcement community to adopt new skills and practices and to learn to deal with a new criminal paradigm. The cyber-crime scene differs from the traditional crime scene, and poses several unique problems. This paper will address the increased use of computers in criminal activity. More specifically, it will explore how computer-based crimes fit into the traditional investigative methodologies utilized by most law enforcement agencies. If traditional methodologies are ineffective, what new methodologies should be adopted to properly investigate these crimes? Finally, some methods of addressing these problems by smaller law enforcement departments are suggested.

<u>The Emergence of Computer Crime</u>

There is no shortage of information on computer related security in the published press. However, most of these articles are primarily concerned with the prevention of computer crime; they do not deal with the aspect of identification of a suspect and the orderly building of a case to facilitate prosecution. For most of the business world, it is enough to identify that criminal access has occurred and then to thwart further access.

To this end, most of the literature which this author reviewed was lacking in those areas critical to law enforcement.

There is no arguing that computers are becoming an integral part of our society. Personal computers are in our schools, our homes and our businesses. It is possible to buy airline tickets, stocks and bonds, and other merchandise over the Internet. Several institutions offer banking services such as electronic fund transfer, loan applications and bill payment on-line. There are even sites which offer access to off-shore gambling and money laundering services just a click away. Perhaps even more sobering is the way the business world has accepted cyber-business. Industry experts estimate that electronic commerce already accounts for over $500 billion dollars worth of business to business transactions annually (Varney & McCarthy, 1996, pg. 43). This emerging market is largely without standards for security practices and policies. A study conducted by Infosecurity News of 1200 computer security professionals in 1996 found that “one quarter of organizations have no individual devoted exclusively to information security…. nearly 60 percent expect that staffing will not keep pace with future needs…. 30 percent felt that a lack of internal security policies and standards was a significant problem in their organizations” (Bernstein, 1997, pg.20).

This increased utilization of the computer for electronic commerce has not gone unnoticed by the criminal element. A study conducted in 1996 by Ernst and Young for Informationweek magazine reported that of 1300 companies surveyed “Some 54% had suffered a loss related to information security and disaster recovery in the past two years, a third cited losses due to malicious acts by company insiders, and 17% (25% in larger companies) cited malicious acts by people outside the company” (Violino, 1996, pg. 36-38). These reported losses may be just the tip of the iceberg. According to Richard Power, an analyst with the Computer Security Institute, “While some 75% of all U.S. corporations say they’ve experienced computer crime or a security breach, only 17% call the police, for fear of negative publicity” (Simons, 1997, pg. 57). As the Internet becomes more of a commercial medium, the reports of vandalized websites become more common. These sites are often used to distribute information on commercial products or services, and can even be purchase points for some products. Damage to these sites represent loss of potential sales and embarrassment to the site sponsor. Even government agency sponsored sites do not escape the vandals attention. Within the past year, the web sites for the CIA, Justice Department, and NASA have been “hacked” (Dugan, 1997; Morris, & Gold, 1997). In each case pornographic pictures or political propaganda was left in place of the legitimate site information.

An exhaustive treatise on types and methods of computer crime is beyond the scope of this paper. However, it is critical that the reader understands how computers fit into computer crime. According to Long, there are three basic methods in which the computer can be employed:

1. The computer is the target of the crime. The physical pieces of the machine may be taken for their intrinsic value. Hardware has few identifying numbers and can easily be broken down into individual components. These components, some of which may cost thousands of dollars, are then sold or rebuilt into a new computer - the computer equivalent of money laundering.

> The electronic information contained on the computer’s hard drive could also be the target. Trade secrets, financial information, personal correspondence, or other critical data could be utilized - sold to competitors, used to commit bank fraud, or even used for blackmail.
>
> 2. The computer is an instrument used in the commission of the crime. The advanced capabilities of the computer allow it to act in ways unique to the media. Computers can be used to intercept and alter or forge electronic bank transactions. Computer programs can be altered to affect accounting systems or inventories. Computer security systems can be electronically bypassed to access confidential records.
> 3. The computer is incidental to the crime. In this category, the computer provides more efficient automation of traditional tasks. An example of this would be a drug dealer keeping his customer and collection data on the computer. It could be kept on paper, but the computer is faster and more efficient. (p. 35)

Methods

This paper incorporates information found in the common press, technical literature, interviews with experts in the applicable fields of study, and extensive Internet based research.

The author conducted telephone interviews with both public and private sector experts in the field of computer based crime. The principle sources for these interviews were Brian Criste, a computer evidence crime analyst for the Florida Department of Law Enforcement Tampa office, and Winn Schwartau, a private security consultant with the firm of Interpact Inc. based in Seminole, Fl. Both are recognized experts in the field and are either published or referenced in other articles as well as this paper. Main topics covered in the interviews included: effectiveness of present law enforcement practices relating to computer crime; potential trends in computer crime for the coming years; and, what resources are required to combat computer crime, and training computer crime investigators.

This paper also includes data from a very limited telephone survey of law enforcement agencies documenting present staffing, training, and policies for computer crime investigation. While conducting research for this paper, the author found very little published information regarding present practices and staffing of computer crime investigators within law enforcement agencies. This is an area which could be fertile ground for future study, but was beyond the scope of this paper. The survey was directed at municipal law enforcement agencies within the state of Florida, serving populations of less than 50,000 citizens. The survey was of a structured response format and designed to discover whether the agency had experiences with computer crime, how they deal with it, how they train their investigators (if at all), and with what resources those investigators are provided. The survey was given to a small sample of the target population, and was not designed to statistically represent the entire group. However, useful inferences can be gained from the survey and are included elsewhere in this paper.

Results

Computer Crime Differs from Traditional Crime

Computer-based crimes differ in many ways from the traditional crimes normally investigated by law enforcement agencies. According the Florida's Office of Statewide Prosecution, traditional criminal investigations (and resultant successful prosecution) as conducted by sworn law enforcement personnel are based predominately on physical evidence (C. Broughan, personal communication, July 18, 1997). The fastest growing computer related crime is theft of information, so called intellectual property - such as new product plans, research, marketing plans, customer lists and similar data (Carter, & Katz, 1996). Unauthorized access of computer systems to acquire this data can often be done electronically. The criminal never comes into direct contact with the computer. The theft is of formless electronic data, and no physical evidence is left at the scene. If the thief is sophisticated enough to alter the computer's electronic user logs, there may not even be any record of his presence on the system. "The evidence of these crimes is neither physical nor human, but, if it exists, is little more than electronic impulses and programming codes" (Carter, & Katz, 1996, p. 1).

To compound matters, the ability to gain electronic access makes physical location immaterial to the cyber-criminal. Access to the computer system can be gained through company networks, the Internet, or via modem connection through phone lines. Jurisdictional concerns come into play and must be considered, if the location of the intruder can even be determined.

An excellent example of this is described in Stoll's book "The Cuckoo's Egg" (1989). During the late 1980's, East German spies used the ARPANET network (the predecessor of the Internet) to hack into over 400 military research sites within the U.S. Stoll, an astrophysicist at Lawrence Berkley Lab in California uncovered their activity by accident due to an inability to account for $2.34 of computer time at Berkley. The spies were able to break into computers all over the world from an apartment in Bremen, Germany. Even though their activity was uncovered, the FBI, CIA, NSA and DoD were unable to identify and locate the three cyber criminals for over a year. In fact, critical members of the FBI team admitted that they would not have been able to complete the investigation on their own. Once the criminals were identified, it took another six months of diplomatic wrangling to forge international cooperation to go forward with prosecution.

Computer crime is difficult to detect. Since there is a lack of physical evidence of a "break-in", operators may not realize that a crime has occurred for months. Additionally, many users view the computer as a "black box", neither understanding nor showing any interest in the methodology used to produce the computer's output. Many users take the attitude that computers don't make mistakes, so the computers output must be right. They have an unwillingness to validate or double-check the computers work product.

Even when they are aware of it, users are traditionally unwilling to report instances of computer crime. "While some 75% of all U.S. corporations say they've experienced computer crime or a security breach, only 17 percent call the police, for fear of negative publicity" (Simons, 1997, p. 57). This is contrary to more traditional crime where the victim is more likely to bring the police into the matter.

Cyber-criminals can use the computer's own systems to hide or destroy evidence of their work. Computer viruses - self replicating programs which can spread from computer to computer, similar to biological viruses in humans - can erase valuable data, render a computer unusable, or do other types of damage. These viruses can lay dormant on the computer system until activated by some specific (or random) condition. An example of this is the "Friday the 13th" virus which activates when the computer is used on a Friday the 13th. The payload or resultant instruction can be one of any number of computer instructions - anything from vandalism to some type of smoke screen to cover the cyber-criminal's activity.

Most recently, a new form of computer crime has emerged, cyber sabotage or cyber terrorism. Like their more traditional counterparts, these saboteurs work to deny access to vital computer systems, either through destruction of data, tampering with communications networks, viruses, or other methods. Like more traditional attacks, the motivation for these activities can be varied; political, financial, vindictive or other drives. This type of attack is most commonly seen today on the world wide web, a section of the vast Internet computer network.

Computer crime investigations require hardware and manpower not commonly available to many law enforcement agencies.

The tools and methods of computerized crime often differ from traditional criminal activity, even if the motives and gains are often the same. However, another critical consideration of computer based crime investigation involves the investigative personnel and the tools which are used in the investigation. The successful investigator will need a diverse group of skills, many of which are not common to the law enforcement community. Also needed will be a ready supply of computer hardware, software, and support manuals and expertise to cope with the wide spectrum of computer systems in common use.

> Computer crime must be approached in a cautious manner. Although it may seem that everyone has a computer, the old cliché, a little knowledge is a dangerous thing, must be remembered … In one case, an officer who ran a computer business on the side attempted to clean up a harddrive on a case. As a result, valuable evidence was lost (Laska, P., 1997,pg. 34).

Several aspects of the investigation require attention. As previously stated, many computer crimes involve little or no "hard" evidence. A case must be pieced together from circumstantial evidence, wiretap information, auditing trails, etc. "The nature of the crime brings together investigative techniques usually only utilized in organized crime investigations" (Laska, 1997, pg. 35). While larger agencies may possess personnel with this type of experience, most smaller agencies do not.

The sensitive nature of wiretaps, public phone system surveillance (computer systems often communicate with each other across public phone systems), potentially protected first amendment communications, and other legal issues will require extensive interaction with a competent legal advisor or department attorney. Failure to follow specific procedures and guidelines could taint any evidence and prevent it's use in future prosecution.

Once the case begins to build, the investigator will have to interact with the computer system. This may be in the form of interpreting surveillance data, discussion with informants or witnesses , or interrogation of seized articles such as diskettes, printer paper, or complete systems. The first challenge may be in taking possession of the hardware. Crafty criminals may have booby trapped the system to self destruct, either physically (explosives) or electronically (scramble or erase data from the hard drive) when common commands or actions are taken by an unsuspecting user. While researching this paper, the author found several "how to" papers in open circulation on the Internet on how to protect computer systems from tampering. Common computer commands, such as DIR can be remapped to produce uncommon results, such as formatting the hard drive. Power switches, or data cables can be rigged to detonate an explosive if turned on or disconnected. One example even described a pressure switch placed in the case which would ignite an incendiary within the computer if it were lifted or the cover removed.

Once in possession of the hardware, the investigator must be able to recover critical data from the system. It is critical that this be done in a non-destructive manner while preserving the devices for court presentation. The investigator must have at least a rudimentary knowledge of the hardware and software which he is dealing with. Given the fast pace of change in the computer field today, and the wide breadth of equipment available, merely keeping up on technological advances is a daunting task. More sophisticated systems such as networks, mainframe computers, and some communication systems may require the assistance of computer engineers or factory representatives to sort them out. According to FBI special investigator Hal Hendershot "Hackers are ahead of the average investigator. Several of our guys have master's degrees in information systems, but we are not studying computer systems 18 or 20 hours a day like some hackers are" (Panettieri, 1994, pg. 32). Various software and hardware utilities are available to help unlock the computer's data, requiring additional funding and expertise. This mix of computer expertise is often beyond the realm of the typical officer who has a computer in his home or office.

> This takes time and money and the right type of individuals to man this operation… It is very exacting work and training is essential for without a properly trained staff or access to computer experts who can provide needed assistance, important evidence could be lost, altered or destroyed" (Long, 1997, pg. 35).

The department must be willing to make a substantial commitment in time, training and manpower to successfully investigate computer crime. "Computer crime investigators are not interchangeable with other types of detectives. The learning curve is too steep. When you transfer one person out, it will take the new person two to three years to get the same level of expertise" (Pilant, 1997, pg. 38).

To compound matters, the requisite computer skills are in great demand in private sector as well. Our society is undergoing a computer revolution, and personnel with the knowledge and skills to run the machinery and master the technology are in high demand. The private sector, with its promise of greater financial rewards is in a position to siphon off knowledgeable personnel. This trend is very evident in the field of computer security consulting. "Information security remains a small specialized field, and professionals are not easy to come by. It is common practice for several companies to bid against each other to hire competent prospects" (Wilde, 1997, pg. 91). Computer crime investigators may find that they can get better pay, equipment, and training working elsewhere.

When investigators are present within a department, they are often poorly trained and equipped. In connection with this paper, the author conducted a survey of several

Florida agencies to determine what training and equipment they were supplied to combat computer crime. Among small to midsize agencies, the majority of municipal departments studied supplied no department sponsored training or equipment. Investigators tended to be self taught and worked with whatever resources existed within the department.

While Computer Crime is Becoming More Common, Agencies are not Developing Resources to Deal with It

A survey of Florida agencies found that about half of the agencies contacted had investigated instances of computer crime over the past two years. However, only half of those agencies contacted felt they had sufficient resources in-house to adequately handle the investigation. Based on this writer's research, the fifty percent capability may be optimistic. Of the agencies surveyed, none had provided any department sponsored training to investigators. Over 80% of the agencies surveyed relied on investigators who were self taught. Most departments utilized personnel who had computers at home and had developed their skills as a hobby. According to Winn Schwartau, an independent computer security consultant, "law enforcement in general is woefully unprepared to deal with computer crime. Typically, investigators are not trained to deal with these crimes, and administrators are not taking steps to prepare their departments for cyber-crime" (personal communication, October 2, 1997).

Resources Available

It appears that the law enforcement community is slowly becoming aware of the potential impact of computer related crime. At present, various federal and state agencies have taken steps to develop computer crime resources.

> The creation of computer crime units in the secret Service, Air Force Office of Special Investigations, FBI, and a small number of state and local agencies shows that law enforcement agencies are beginning to recognize the significance of computer crime. The growth of such groups as the Florida Association of Computer Crime Investigators and the High Tech Crime Investigators Association, as well as the proliferation of computer crime specialists in such agencies as the Royal Canadian Mounted Police, Royal Thai Police, and London Metropolitan Police Department, confirms the rising worldwide awareness of computer crime" (Carter, & Katz, 1996, pg. 1-2).

Florida is a leader in the technological battle against computer crime. FDLE has created the Computer Evidence Recovery section (CER) to provide expertise in computer forensics. As part of my research, I interviewed Brian Criste, a crime laboratory analyst for the Tampa based arm of CER. The CER program has four main goals: the examination of computer evidence; assistance in collection of computers and computer data from crime scenes; technical assistance to local agencies; and, training in computer forensics to local agencies. The CER has advanced tools and capabilities to do in depth research and analysis of computer systems. Criste stressed that they are also available to assist local agencies in conducting their own investigations as well. He stressed that another critical aspect of the forensic process was the local collection and packaging of evidence for submission to CER. Education and proper procedure on the local level is critical to the process.

Various federal and private sector agencies are available with extensive computer crime sections. The FBI and Secret Service have developed extensive expertise in computer crime investigation. CERT (Computer Emergency Response Team) is a government funded private entity run by Carnegie Mellon University in Pittsburgh. CERT is considered by many to be credited with “being the ultimate expert on the Internet and Internet security” (Panettieri, 1994, pg. 30). There are numerous private sector companies which specialize in computer security as well. Private sector consultants can provide a wide variety of services, and can either work on a per case or retainer basis.

These agencies provide the resources to deal with computer crime within their own jurisdictions; however, their existence does not completely answer the computer crime problem. Large state and federal agencies are far removed from local communities where crimes often occur. The Florida Department of Law Enforcement Computer Evidence Recovery Section (FDLE CER) cannot be called to investigate and prosecute all instances of computer crime in Florida. They have neither the resources or the personnel. Nor can most departments afford the luxury of bringing in a paid consultant to handle each case. To some extent, the problem must be dealt with on a more local level. Individual agencies must have the resources available in-house or near-house to first recognize the existence or involvement of computer crime, and then act in a professional manner to properly investigate, gather evidence, and provide a complete package for prosecution. The state and federal agencies can be called upon for their expertise and tools, but the burden of the investigation should fall to the local level as much as possible.

The coming computer crime epidemic is potentially most troublesome for smaller agencies, which may not have the breadth and experience of much larger departments to deal with computer crime. Physical location is meaningless when dealing with computer crime. Most communities, irrespective of size, have the businesses, individuals, and resources attractive to some type of computer crime. These communities may even be more appealing targets to the cyber-criminals since they are more likely to escape detection and sophisticated prosecution in the community with no computer crime investigation section.

The leaders of these communities may face an uphill battle preparing for the inevitable crimes to come. In an agency with limited resources, with no documented history of computer crime, and limited in-house expertise, the overwhelming temptation is to do nothing. The present percentage of agencies which have no or limited plans to deal with computer crime shows that this is often the case.

It is this author’s opinion that every agency should evaluate their potential exposure to computer crime, and take some steps to plan for it’s investigation. If nothing else, strategic plans should be made as a contingency for action. Local authorities and resources should be identified and arrangements made for their use. Future planning and budgetary considerations should be formulated to better address the issue in future budget cycles if they cannot be addressed at present.

Discussion

This paper has shown that computer based crime is different in many ways from the "traditional" crime law enforcement is used to dealing with. While in many instances the motivational factors are the same, the tools and methodologies are profoundly different from what agencies are used to seeing. Additionally, computers create opportunities for new types of crimes. They add factors and difficulties which law enforcement is not presently prepared to deal with.

Further, in dealing with the cyber-criminal, enforcement agencies are often lacking in knowledgeable staff and appropriate equipment to deal with the high technology used by the crooks. Computers are a fast paced, changing environment. Keeping up with the "electronic Jones's" is a costly, time consuming process. However, it is essential to keep up.

Computer crime is in it's infancy and for the most part has not reached a level where it is attracting wide spread attention. Agencies have limited resources, little history of computer criminal activity, and far more visible crime problems to address. Small to midsize agencies are especially vulnerable as they are even less likely to have the resources to combat this type of activity. However, we are becoming a nation of computer users. One need only look at the phenomenal growth of the Internet to see the widespread adoption of the computer age. As more and more people become computer literate, more criminals will attempt to seize opportunities to misuse the new media. Law enforcement must act now to get in front of the building wave of activity which is predicted. Agencies should take definite steps to prepare for the cyber age.

Recommendations

It is critical that agencies take steps to prepare for computer crime investigation. Agencies should take a realistic look at their resources and priorities. At this point, computer crime may take a back seat to more pressing matters such as gang crime, domestic abuse, and drugs. Even with only limited resources however, significant steps can be taken to prepare for the inevitable increase which will present itself. Based on this research, it is recommended the following steps be taken by all agencies as a minimum contingency plan for dealing with computer crime.

1. Identify local computer resources. Personnel within the agency and adjacent agencies who have significant computer skills or abilities should be identified. If personnel in-house are not competent, are there experts available in local businesses, college campuses, high schools, etc. who can act as sources of information for your internal needs?
2. Identify professional resources available to assist your agency in conducting local investigations. As previously discussed, state or regional agencies may have extensive capabilities which are available for department use. Contact points and procedures should be identified and documented before they are needed. Clarification should be obtained as to what resources are available and under what conditions they can be requested.
3. Department wide training should be conducted in the basics of common computer crimes. Street officers should be versed in what to look for in identifying computer crime. The first part of investigation is identification of the occurrence. To better

combat computer crime, we must first do a better job of recognizing it when we see it.

4. Provide selective specialized computer crime education. Key members of the department should be trained to handle computer crime investigations. The extent of the training should be based on the level of expertise and support. A small town with few resources and easy access to a regional computer crime investigative service such as FDLE's CER may only need to learn to properly collect evidence for outside analysis. Larger areas or those with more capable in-house staff may wish to do more in-depth training, or even develop their own in-house computer crimes section. At the least, one investigator and the crime scene technician should receive additional training in this area.
5. Educate the community. Computer crime is vastly under-reported at present. Departments should work to gain the trust of the business community to bring these crimes forward. This is an area where law enforcement has an opportunity to be proactive instead of merely reactive. Crime prevention units can educate citizens to prevent theft of hardware and critical systems, much as they are taught to protect their homes from burglary.
6. Monitor computer crime trends with an eye toward long range resource allocation. As computer crimes become more prevalent, additional resources will have to be allocated to their investigation. Agencies should look toward their future needs several years down the line when formulating budgets, manpower requests, and training.

Conclusion

Computer crime is a new area which should be of critical interest to law enforcement. For most agencies, it is an area which they are ill equipped to handle. At present, computer crimes are an oddity which attract curiosity and media attention. In the near future however, they may blossom to occupy a major portion of an agency's resources. While for many agencies, it is too soon to prepare fully for this new phenomenon, steps should be taken to prepare for a change in the way we do business. The change will occur. The question is; will we be ready for it, or will we scramble to catch up?

Bill Netterville is a 16 year veteran of the Ormond Beach Police Dept. He presently serves in the function of Patrol Sgt. Previous duties within the department have included Traffic Division Supervisor, Records/Communications Supervisor, and Data/Fiscal manager.
Bill has a masters degree in Business Administration, a bachelors degree in Communication and an A.S. degree in Computer Science. He is a member of the International Association of Law Enforcement Planners and is active in various civic organizations within his community. He is an advisor for a local Explorer post and is a past Eagle Scout.

References

Bernstein, D. (1997, May). Infosecurity News industry survey. Infosecurity News, 8,3.

Carter, D. & Katz, A. (1996,December). Computer Crime: An emerging challenge for law enforcement. FBI Law Enforcement Bulletin, 65,12.

Dugan, S. (1997, February). Cybersabotage. Infoworld, 19, 6.

Laska, P., (1997, April). Computer Crime, Investigations for the twenty first century. Law Enforcement Technology, 24, 4.

Long, W. (1997, May/June). Computer Crime. The Chief Of Police, 12,3.

Morris, P. & Gold, S. (1997, July). Cyber Terrorism. Secure Computing/Infosecurity News.

Panettieri, J., (1994, May). Guardian of the NET. Information Week

Pilant, L., (1997, August). Fighting crime in cyberspace. The Police Chief, 64,8.

Simons, J. (1997, May 12). Forget hackers; bar the door. U.S. News & World Report, 122,18.

Stoll, C., (1989). The Cuckoo's Egg. New York, New York: Doubleday

Varney, S. & McCarthy, V. (1996, October). Wired for profits. Datamation, 42,16.

Violino, B. (1996, October). The security facade. Information Week, 602.

Wilde, C., (1997, May). IT Management - Hunt for security. Information Week, 632.