Cyber Crime: The Next Challenge

An Overview of the Challenges Faced by Law Enforcement While Investigating Computer Crimes in the Year 2000 and Beyond

Paul A. Curtis

Sergeant – Arkansas State Police

Criminal Justice Institute

Director: Dr. Lee Colwell

School Of Law Enforcement Supervision

November 12, 2000

TABLE OF CONTENTS

Introduction

As the new millennium dawns, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element.

According to Donn Parker, www.infosecuritymag.com, "For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her own needs." Parker writes, "Since it could be tested repeatedly under predictable circumstances, it may become the perfect crime, one with no evidence and no basis for the victim and perpetrator to identify or confront each other. Neither would even know the crime method used and when and where it was done; it would happen before either could bat an eye (or click a mouse). The technology and know-how to launch the perfect crime are right around the corner. The only question that remains is, What can we do about it?"

This puts law enforcement squarely behind the 8-ball. We must anticipate our adversaries. They are intelligent and more than willing to use new technology that is at their disposal for the purpose of committing all manner of crimes. These unscrupulous persons will commit every imaginable crime from Trojan horse attacks, computer viruses, fraud, theft, impersonations, sabotage and logic bombs to the most unthinkable crime of exploiting our children through child pornography rings.

Climbing the Technology Mountain

Regrettably, the police have fallen behind in the computer age and must overcome a steep learning curve. To make matters worse, computer crime is sometimes difficult for police officials to comprehend and to accept as a major problem with a local impact, regardless of the size of their communities.

One of the major challenges facing law enforcement in this new era is keeping up with growing demands of technology. Computer technology changes are so rapid that if a department is up to date today, their equipment will probably be outdated in six months. Agencies are woefully behind in their acquisition and use of technology. Their budgets have not been increased to keep pace with the rapid change in technology. This makes its difficult for law enforcement agencies to keep up with this rapid change. The criminal element is not as challenged to keep pace. They are usually well financed and have the resources to continue purchasing this new technology.

Alfred Olsen, Chief, Warwick Township Police Department is quoted by the Editorial Staff of the Law Enforcement Internet Intelligence Report in their report on Computer Crime in the Year 2000 and Beyond, as saying, “Law Enforcement will always be behind because it is impossible to commit the time and resources to the computer crime issue. You are dealing with people, criminals, who have nothing else to do but work on-line all day, and have access to funds to buy the very best and the very latest in hardware and software. These people sit at their computers all day and do nothing but devise ways to defeat law enforcement. Law Enforcement still has to do everything else we have to do. We are always going to be playing catch up. Rank and file law enforcement just doesn't have the resources to commit to Internet investigations. People still have to look out for themselves, it's kind of like the Wild West" (p. 1).

In my personal attempts to bring my own agency in line with this new challenge, I have encountered the same situation. Budgets are considerably leaner due to services requiring all agencies to draw from the same tax dollar pool. It's not that the agency is not interested in the investigation of these types of crime. It's just that there does not seem to be enough money to go around or enough officers to conduct the investigations.

Thankfully, with the increase allocation of money from the federal and some state levels, and the use of seized computers this may be changing. If the law enforcement community is to keep pace with this growing problem of computer-related crime, it will have to have access to the very best and latest technology. That will require money and lots of it.

Definitions of Crimes Encountered

What is a computer crime?

A broad definition would be any crime committed that involves the use of a computer. In current times, this would mean just about every crime committed. Should a criminal use a computer to keep track of the robberies he's committed or the drugs he's sold, which means that even stick-ups, breaking and entering and every drug transaction could be considered a computer crime.

The Encyclopedia Britannica defines computer crime as any crime that is committed by means of the special knowledge or expert use of computer technology.

Since the first reported case of computer abuse in 1958, computers have been involved in most types of crimes, including theft, burglary, larceny, fraud, embezzlement, extortion, sabotage, espionage, kidnapping, and murder. Today, we must include the crime of child pornography as well. These systems can be the target of attacks themselves when a computer virus is surreptitiously introduced into the system to alter, damage or destroy data. With the introduction of modems (devices that allow computers to communicate over telephone lines) in 1960, breaking into private computers to destroy, steal, or alter information became much easier.

"Any crime on the books can have a computer element to it," says Lou Pacheco, Deputy Chief, Raynham, MA PD, as reported in Computer Crime in the Year 2000 and Beyond. "A bigger and bigger percentage of crimes committed are computer related, because of the nature of the way we live. 85% of all police investigations either involve the use of a computer, or you need a computer to help investigate them" (p. 2-3).

Computer Crime or Cyber Crime, as it is being called, is any crime that is committed or helped by the use of a computer. It could be as simple as fraud, or as complicated as stalking, murder, or child pornography and anything that lies between.

The Internet: A Joy and Curse

The Internet is both a joy and a curse for members of the law enforcement community. On one hand, if facilitates our ability to communicate and gather information. On the other hand, it enables the criminal element to do the same. The criminal element actually embraced the benefits of the Internet long before those of us in the law enforcement community did. In some ways, we still resist this tool.

Virtually everyone that I know is on line and with everyone on line we have created a huge pool of potential victims for the criminal who uses this technology tool. Criminals discovered the Internet long before the public did and they use it to their benefit. Child pornographers and pedophiles, which will be discussed later, know that it's perfect for them. They can trade pictures, and remain almost totally anonymous while conversing with children via the Internet. The criminals are just licking their lips at the possibilities.

"I liken it to the idea that Internet crime is today like when Alexander Graham Bell introduced the phone," says Jim McMahon, security consulting firm, McMahon and Associates, Computer Crime in the Year 2000 and Beyond. "Criminals use technology like businesses use it. We have been seeing an increasing use of the very same technology that helps businesses and others communicate. One of the reasons why Louis Freeh has strong feelings about the use of encryption methods is because it limits law enforcement from listening in. Federal law enforcement activities directed against criminal enterprises depend heavily on listening in on the crooks."

"Today, your standard issue criminal most likely is going to have access to and uses a computer system," continues McMahon. "Computers are being used to expand criminal operations. Most crooks involved in major crimes use cell phones, and mostly cloned phones. They also use pagers. The use of the Internet for communications—how can you tell if a message is involved in illegal activity without opening it? A lot of people use free e-mail to engage in criminal conduct, or for sending mail to people where you might not have the courage to send yourself (harassment, etc.)" (p. 3-4).

The virtual world of the Internet has arrived and caught most law enforcement totally off guard. Dave Johnston writes in the International Journal on Cyber Crime, "Limited resources must be stretched to provide some form of policing in the virtual world as well as support the traditional brick and mortar style of policing. Clear laws have not been written and precedents are not available to guide law enforcement and the judiciary. While law enforcement has been slow to respond, the criminal element is embracing this new medium whole-heartedly" (p. 3). This is as true in Arkansas as in the other states. Arkansas has only seven statutes in its criminal code that are intended to police the use of computers. None of these laws deal with the Internet and most don't address the problem related to other types of crime.

The Internet can be a huge misunderstood gray area, due to emerging technologies, new information and new crimes, and the naiveté of those who use the Web. "All the statistics show that cyber crime is increasing, and it makes sense that it is," says Patrick Taylor, VP, strategic marketing, Internet Security Systems, Year 2000 and Beyond. "To a degree, every company and every computer has some responsibilities for security. If you don't have 'no trespassing' signs, it's not against the law to walk on a piece of property. If the door is unlocked, and there are no signs up that say 'do not enter,' is someone breaking the law when they go in and look around? Conceptually speaking, there are a whole lot of computer doors that are unintentionally unlocked" (p.4).

This problem exists in most agencies today. Any department that has computers on a network or individual computers that have official data stored on them and those systems have access to the Internet have a security risk to that data unless they have put some security measures in place. Most departments have not accomplished this due to the expense of adding those protections.

"By cyber crime, we mean any kind of misuse of a computer system," Taylor continues. "The tricky parts come when you are looking at information I don't want you to. Is it happening? Yes, there is no question that people are being broken into every day. There are internal examples where someone inside a company copies material and sells it to a competitor. We are making it more compelling—more and more interesting things are being put into the electronic world. We are introducing more instances where we will have more problems" (p. 4-5)

White Collar Crime

Britannica.com defines White Collar Crime as crimes committed by persons of relatively high social or economic status in connection with their regular occupation. Though crimes such as stalking and pedophilia make the headlines, the majority of computer crime is white collar in nature, involving the theft of credit cards, money, identity, or intellectual property such as software or data.

As reported in the Computer Crime in the Year 2000 and Beyond report, Lee Altschuler, senior manager, Deloitte & Touche LLP, Fraud and Forensics says that "Computers as the tool of the crime, as the object of the crime, or as the place where the evidence from crime is stored is an accelerating, and it is a giant problem for the new millennium. It's virtually impossible to conduct sophisticated criminal activity involving large dollar amounts without using the computer. For example, we prosecuted with the FBI a check-kiting scheme. The amount of money in the kite was $310 million dollars, and the only way the defendants were able to keep track of the transactions was by using a commercially available accounting program" (p. 5)

We have experienced this same sort of crime in Arkansas where the criminal has used the computer to manufacture the actual check from businesses and then pass them through local businesses and be gone before the crime has been discovered.

Data Theft: Another Area of Concern

Law enforcement is charged with the investigation of the theft of data from companies, but of just as great a concern to the law enforcement community is the protection of their own data and unauthorized access to their files. This may require law enforcement agencies to bring in a security consultant to be sure that their own data is secure from unauthorized access.

The only way to ensure that your system is totally safe is to not have outside access to it. If you have access, you will have a security risk. If you are connected to the Internet through phone lines through a network or a modem, you cannot assume that your system will not be compromised at some point. Agencies can install fairly simple monitoring systems on their systems that will signal them when there has been a "knock" at the door. These security measures will also alert you to an actual intrusion. The Agency can run programs against these to track who has been in them, pinning it backwards to the keyboard.

One of the major threats to any system, whether it is a law enforcement agency or federal agency is the "Hacker". These individuals or groups can break into just about any system. They have unlimited resources, time, and in most cases motivation. All agencies must be vigilant in their security needs by continuously upgrading their security programs to battle the hacker. As soon as a new protocol is developed and announced, it seems that hackers have it figured out, and a more elaborate design must be developed.

"There have been reported cases of hackers accessing and manipulating federal court record systems," says Deloitte & Touche's Altschuler in Year 2000 and Beyond. "Everything is computerized now, it's even possible to hack into the Department of

Justice web page. The risks are: browsing and compromising sensitive information; altering information; destroying information. What's a reasonable protection level? One of the answers is periodic outside review by systems specialists specifically trained in intrusion techniques" (p. 6-7). This is expensive and most law enforcement agencies have not budgeted for this service.

I'm a retired Lieutenant Colonel with the United States Army Reserve and a member of an organization called The Reserve Officer's Association. While serving as the Arkansas Department President of this organization in 1999 and early 2000, the National Office in Washington D. C. experienced this problem of "hacking" when the National Office's Web Site was hacked and the entire system crashed causing untold damage to records and communication with the U. S. Congress. This disrupted membership endeavors and services and lobbying efforts for numerous National Defense Bills of which the organization had an interest. The cost to the organization to repair the damage ran in the thousands of dollars.

Imagine parts of the nations infrastructure being taken down by either cyber terrorists or hackers. I haven't heard of any documented cases as of this writing, but think of the panic it could cause. The risk is just as great from either cyber terrorist or hackers. Airport control towers have been shut down and 911 systems have been compromised. The potential for this to happen is there, and a lot of work has been done in the area of protecting our infrastructure. In this day and age when you go to war, you win by disrupting the enemies communications systems.

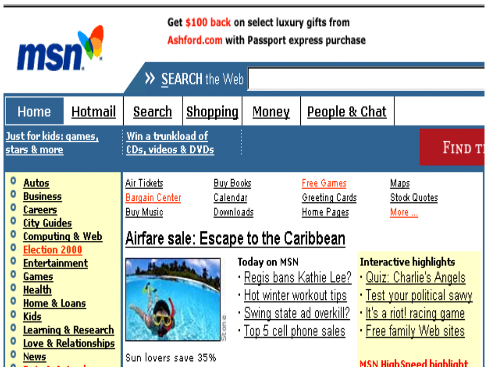
"Law enforcement should practice what they preach—check their own computer network security," Patrick Taylor, VP, strategic marketing, Internet Security Systems says in the Computer Crime in the Year 2000 and Beyond Report. "Managing security risks is a continuous process. Just like you check the doors before you go to bed, you do the same thing with computers. When it comes to computer crime investigations, the traditional tools of the trade haven't been adapted to the virtual world. You need to understand how to gather the evidence in cyber crime. You have to have the familiarity with how to gather evidence" (p.7)

From the training that I have received, I have learned that computers have logs and those can be examined. A computer literate criminal can alter these making it more difficult if not impossible to retrieve the evidence stored there. Just as in any crime scene, you have to think about where are the likely places someone would break in. That's relatively easy to do. You may have to bait a trap to catch an attack on your system in progress.

Computer security is a constant and changing process. Anything that you can lock can be unlocked. Just as in attempting to physically protect your home, you try to delay entry. You try to make it as difficult as possible and by doing so you will have more success. Computer security is no different.

Fraud: A Growing Concern

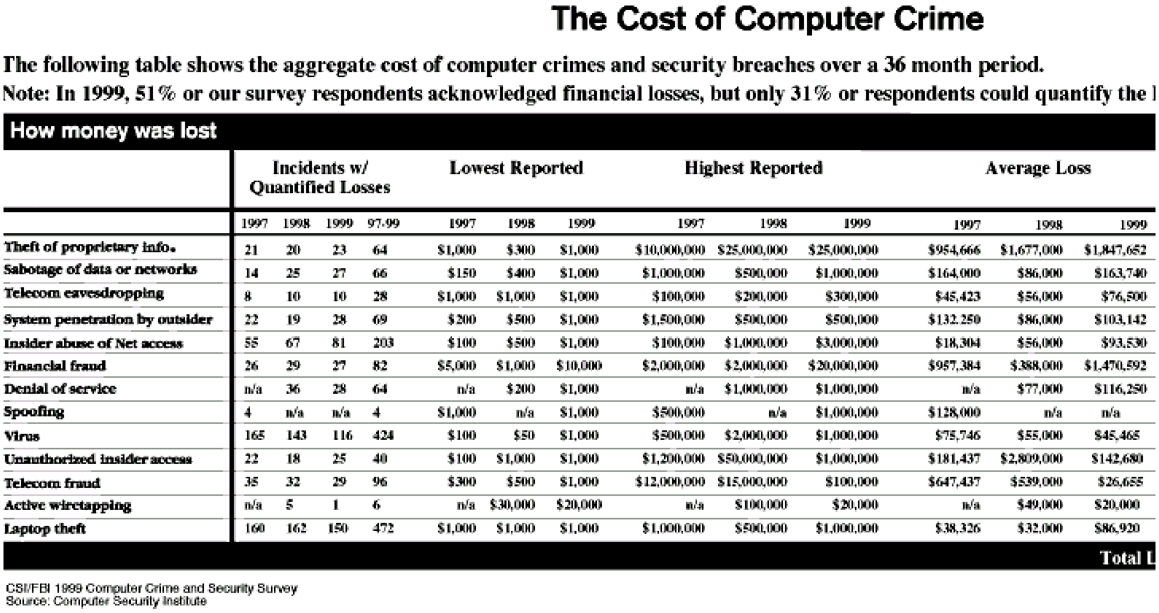
Due to the advances in technology, the use of computers to commit fraud by the use of another technology, The Internet, is growing at an alarming rate. Image is everything on the Internet. A company that is working out of an office in a home or a garage can appear to be much larger and more established simply because of the programming on its web page. This can be as elaborate as the MSN Web page shown here with all the links and search areas or as simple as the Aristotle Web page. These pages are what and who they appear to be, but it would be very easy for someone with less than honorable intention to display the same type pages.



"Computer crime is a huge problem, dollar wise and crime wise," says George Vinson, senior manager, Deloitte & Touche, LLP, Fraud and Forensics, Year 2000 and Beyond. "Any fraud that used to be conducted by fax and phone is now being conducted via the computer. Most smaller law enforcement agencies understand how overwhelming the problem is and how limited their resources are. They need to partner up with the state, county and federal agencies when they run across a fairly significant computer crime, so they can marshal the resources available" (p, 9)

On-line or e-commerce, as it is called today, is a growing area, with $7 billion in sales in the 1999 holiday season alone. "The biggest trend in computer crime that effects consumers has to do with electronic commerce, from the standpoint of fraud," says Jim McMahon, security consulting firm, McMahon and Associates, Year 2000 and Beyond. Its very difficult looking at a 10 meg Internet page to tell whether it's a multimillion-dollar company, or something out of a shoebox. The reality is that it is very easy to send money believing that you are dealing with a stand up business, and it really isn't anybody. One of the hot programs today is the use of the Internet for open bidding, auction type activities, and that whole area is ripe for fraud" (p. 10)

Working with this type crime and being one of only two contacts in the State of Arkansas for the Internet Fraud Complaint Center (IFCC), I receive complaints on a daily basis from persons in the State and from outside the state who have either been the victims of this type of fraud or who have perpetrated this type of fraud on others. The following chart will give an idea of how fraud and other types of crime on the Internet by use of a computer have increased over the past three years.



The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 36 month period.
Note: In 1999, 51% or our survey respondents acknowledged financial losses, but only 31% or respondents could quantify the l

How money was lost

	Incidents w/ Quantified Losses				Lowest Reported			Highest Reported			Average Loss		
	1997	1998	1999	97-99	1997	1998	1999	1997	1998	1999	1997	1998	1999
Theft of proprietary info.	21	20	23	64	$1,000	$300	$1,000	$10,000,000	$25,000,000	$25,000,000	$954,666	$1,677,000	$1,847,652
Sabotage of data or networks	14	25	27	66	$150	$400	$1,000	$1,000,000	$500,000	$1,000,000	$164,000	$86,000	$163,740
Telecom eavesdropping	8	10	10	28	$1,000	$1,000	$1,000	$100,000	$200,000	$300,000	$45,423	$56,000	$76,500
System penetration by outsider	22	19	28	69	$200	$500	$1,000	$1,500,000	$500,000	$500,000	$132.250	$86,000	$103,142
Insider abuse of Net access	55	67	81	203	$100	$500	$1,000	$100,000	$1,000,000	$3,000,000	$18,304	$56,000	$93,530
Financial fraud	26	29	27	82	$5,000	$1,000	$10,000	$2,000,000	$2,000,000	$20,000,000	$957,384	$388,000	$1,470,592
Denial of service	n/a	36	28	64	n/a	$200	$1,000	n/a	$1,000,000	$1,000,000	n/a	$77,000	$116,250
Spoofing	4	n/a	n/a	4	$1,000	n/a	$1,000	$500,000	n/a	$1,000,000	$128,000	n/a	n/a
Virus	165	143	116	424	$100	$50	$1,000	$500,000	$2,000,000	$1,000,000	$75,746	$55,000	$45,465
Unauthorized insider access	22	18	25	40	$100	$1,000	$1,000	$1,200,000	$50,000,000	$1,000,000	$181,437	$2,809,000	$142,680
Telecom fraud	35	32	29	96	$300	$500	$1,000	$12,000,000	$15,000,000	$100,000	$647,437	$539,000	$26,655
Active wiretapping	n/a	5	1	6	n/a	$30,000	$20,000	n/a	$100,000	$20,000	n/a	$49,000	$20,000
Laptop theft	160	162	150	472	$1,000	$1,000	$1,000	$1,000,000	$500,000	$1,000,000	$38,326	$32,000	$86,920

Total L

CSI/FBI 1999 Computer Crime and Security Survey
Source: Computer Security Institute

The calls and complaints that I receive from these auction type frauds are in small amounts ($15-$800), a lot of different victims, victims and criminals in different jurisdiction, and the amounts don't meet the threshold for federal crimes. These are crimes that cry out for task force type operations with US attorneys and local police officers being the most critical pieces.

As we see more and more people trading and buying on the Internet, including auctions and other type of purchases, the more crimes will be committed.

Theft: Also Growing

According to David L. Carter, Ph.D. and Andra J. Katz, Ph.D., Computer Crime: An Emerging Challenge for Law Enforcement, February 3, 1997, “Not surprisingly, the fastest growing computer related crime was theft. However, an interesting facet of this crime supports the most commonly stolen commodity was information. Respondents reported that thieves most frequently targeted intellectual property, which includes such things as new product plans, new product descriptions, research, marketing plans, prospective customer lists and similar information” http://www.info-sec.com/access/infoseczh.html-ssi).

Research indicates that the value of trade secrets and intellectual property is high. Persons committing this type of crime in the past have obtained such property by compromising employees, photocopying documents, committing burglary, or conducting surveillance of company personnel and practices. Now, thieves simply steal from computers because the more usable information is more accessible, it is easier and more reliable than other methods, and it presents less risk of detection and being caught. Carter and Katz, Computer Crime: An Emerging Challenge for Law Enforcement, research indicates that there is a significant relationship between the personal use of company computers and employees stealing or attempting to steal money. Businesses placed more security controls on monetary files and monitor them more closely than they do information files. Businesses usually have fewer monetary files than information files, which make them easier to monitor.

Despite the safeguards implemented by businesses, thefts have occurred. A case in Detroit, Michigan revealed that a small-time computer cracker penetrated a bank’s computer system, opened a new account, and methodically transferred small amounts of money into it from existing accounts. The small thefts totaled about $50,000 before anyone noticed a problem.

Child Pornography and Pedophilia: The Most Publicized

Child pornography distribution is a natural for the Internet. It offers anonymity and ease of transferring images and text. The use of the "Net" allows for the recruitment, harassment and abuse of minors by adults and is facilitated by the "I can be anyone" nature of the Internet.

Jay Bilchik, administrator, Internet Crimes Against Children, Office of Juvenile Justice and Delinquency Prevention, Year 2000 and Beyond, says "The Internet is almost tailor made preferential sex offenders—it's secret (anonymous), they can sit back in the privacy of their bedroom and engage in conversation with multiple targets with no risk of exposure. It's nothing like having to go to playgrounds. They can troll through chat rooms and look for easy victims. Preferential sex offenders have an all-encompassing need to feel good about themselves. The Internet gives them a way to talk with others who share their predilection. They can organize their information, share pictures, and keep fantasy journals" (p. 12)

The Internet helps the exchange and sharing of child pornography. The only way to not find child pornography on the Internet is not to look for it. Child Pornographers trade images of very young children, depending on their preferences, to other pornographers that will trade them to others or simply keep them for their own collection. In one case I have been involved with, the person lived in Arkansas and was actually running a server in his home and had over 20,000 images of children ages 10 to 15 years of age. He would allow anyone logged onto his server to download three of the images on his server if the person logged on would upload one of their images. This particular individual had traded as far away as Germany.

In Computer Crime in the Year 2000 and Beyond, the authors state, “There is increasing awareness that child pornography plays a significant role in the recruitment and control of additional victims. Not withstanding the image is a depiction of a sexual assault against a child it has farther-reaching implications. Child pornography is often used to decrease inhibition, used to introduce specific sex acts to the child/victim, it’s often used to characterize that sexual behavior between adults and children is normal. It is often used as controlling the victim into silence—blackmail” (p. 13)

Child pornography is illegal, but there are more ominous undertones than just passing pornography between two guys. Most of the safeguards that we tell our children about are designed to keep them from getting into trouble in the physical world. Individuals who are inclined to molest children could talk to a 10-year-old child in their bedroom, via the Internet, circumventing the traditional safeguards. These type criminals have access to an unlimited pool of potential victims. It is easy for them to develop relationships with their potential victim while chatting in chat rooms or exchanging e-mails. That is how many of these things begin. Because these types of criminals are migrating to the Internet, we must provide the proper equipment, training and tools to law enforcement to be effective in combating this threat to our children.

In my experience, I have encountered the problem of locating the perpetrator and determining where the crime occurred. We have seen the offender located in California and the victim located in Arkansas. Where do we say the crime occurred? If possible, the investigators attempt to set up a face-to-face meeting between the offender and the victim, then make a physical arrest. We are also encountering this same situation within the state. We may have an offender in one city contact a victim in another city and be willing to travel to the victim's city to engage in a sexual encounter. We have recently had some success in making arrest with the use of undercover officers and operations. The problem here is one of jurisdiction and resources. Agencies have to work together to combat this type of crime.

If we can determine, especially in enticement cases, where the offender is, we can forward that information to the local law enforcement officials. The case that was referred to earlier in this writing in regards to the child pornographer maintaining a server in his home was referred to us in that manner. The National Center for Missing and Exploited Children maintains a database of people who are involved in computer related cases.

There are more agencies that have realized that we must become involved with the investigation of this type crime. Some of these have started to go on-line, posing as youngsters, trying to bring the pedophiles and child pornographers to them. Those of us who are investigators can use the same anonymity that helps the criminals and convictions can be a result of this type operation.

Stalking, Hate Crimes and Harassment

The final area of crimes that we must learn to deal with on the computer and Internet are stalking, hate crimes, and harassment.

The Internet is a relatively new frontier, a brand new society, and with this society comes new dangers. The anonymity provided by the Internet has become a breeding ground for society's fringe elements, including stalkers. People might never say and do things face to face to another person that the Internet has made it easy for them to do because of the anonymity. People rarely use their real names on the "Net" so any name can be used and any persona that the person wishes can be assumed. The bottom line here is that you never know for sure whom you are dealing with.

An overweight pedophile can use a moniker of "SexyThing" and pass himself off as a nubile 14-year-old girl, and no one would know the difference.

On the Internet, things are never quite what they seem. Cyber stalking and harassment via the computer are becoming more and more common place. A woman recently filed a complaint with me asking for help at her company. It seems that she had been the target of numerous sexually explicit e-mails. She had not solicited this type of activity, but it had occurred and she had reported it to her company. This type of stalking is becoming very common and makes the work place uncomfortable for its victims. There are only a few statutes in place with strict penalties in Arkansas, although some new bills are in the works for the next legislative session.

It is very easy in this day for a harasser to assume your identity, cancel your credit cards, alter your credit history, create new credit card accounts, and cause you considerable trouble, all without leaving their computer. This may be done all because of some real or perceived slight of which you might not even be aware.

Hate groups can build web sites and virtual communities, which appeal to the disenfranchised. They can spread their message to more people than ever before, and don't have to stand on street corners dispensing their literature for all to see as in the past. These groups (right wing extremists, militias, etc.) can recruit openly on the Internet. It's not a crime and it is a great way to reach large numbers of people that would have been impossible in the past. These groups can dispense their type of rhetoric virtually unencumbered by any restriction.

The Internet is relatively inexpensive today and getting cheaper everyday. More and more of these type of groups will have access to a presence on the Internet and more people will receive whatever message they are sending. Web pages are becoming less expensive and more people will have access to these type groups than ever before.

"It is very difficult to track who is behind a website, group members hide behind the veil of anonymity, and it is nigh too impossible to find out who is signing onto these websites. Kids and other easily influenced people can get all the information they want, and even some they might not want, without fear of being "found out." No one will know what they're looking at, because they are anonymous," say the authors of Computer Crime in the Year 2000 and Beyond (p. 18).

There are numerous anonymous posting services in existence today and these fringe groups are getting much more sophisticated and using anonymous posting. This makes it increasingly difficult to track these groups. The heads of these fringe groups will make anonymous postings themselves using these services making it hard or impossible to track them down. Years ago the majority of the posting you would see on the Internet would be schools. Now they are anonymous.

Cyber Crime Units: An Expensive Proposition

Most law enforcement managers have come to dread the budget process. Law enforcement is continually being asked to do more with less. Arkansas is no different. We are constantly being asked to cut back on funds. With the reduction of funds come fewer resources to be put on the streets. Our managers are required to make painful decisions assigning budgetary priorities every day of the week. Some projects are going to fall by the way side due to the reduction in funding.

"Creating a cyber crime unit or a technological crime unit will require a large initial investment," says Dave Johnston in his article, Cyber Crime Units-An Expensive Proposition, for The International Journal on Cyber Crime. "This unit will also require on-going operational cash flow to ensure that training and equipment are maintained to acceptable standards" (p. 3). The forensic software is expensive and the various storage media, such as hard drives, will have to be maintained for the preservation of evidence.

The first responsibility of any Technological Crimes Unit is the forensic processing of the computer equipment seized. Regardless of the type of crime committed, the evidence will have to be recovered and preserved. The examiner will have to testify in court that his recovery procedures did not add, change, remove, or alter the data on the hard drive or other storage media in any fashion.

A combination of specialized software and training will be required at this point. This training will cover not only the basics of file structure and storage, but also the intricacies of operating systems. The investigator must be aware of techniques to bypass the operating system contained on the seized computer. Sometimes the seized computer system must be booted up from a "Boot Disk" containing an unaltered operating system. Training on how to use the special forensic software will be required. This training may be expensive, but without it there would be no purpose in starting a unit.

Once the training has been completed and the software purchased, the equipment must be purchased. This too can be expensive. A DOS/Windows lab may meet all of the basic needs of the investigator until the first time a LINUX or Macintosh system is encountered. The equipment required to preserve evidence on every type of system might sooner or later be required.

Each type of computer will require certain peripherals such as hard drives and printers to copy, capture and printout evidence.

Storage media that will be used to capture evidence, image the suspect drives and produce disclosure will be an ongoing expense. The original drive should never be worked on, but an exact bit for bit image created and that drive should be used to conduct the examination. This will require the investigator to maintain hard drives that are equal to or lager in size than the suspect drive.

Safeguarding computer evidence uses the same basic rules of evidence such as chain of custody and detailed documentation are critical. “It depends on the nature of the crime, because computer crime can be so diverse,” says Raynham PD’s Officer Thor Lundberg, Year 2000 and Beyond. “If you are talking about harassment vs. stalking, if they are in a chat room, you should save the log. If you are talking about child pornography, it’s different. Computer crime presents a whole set of new challenges. The handling of the evidence is pretty much the same, I try not to deviate from the set standards that have already been established. Since we are on the frontier in the move of law enforcement to the Internet, some adjustments to established protocols need to be made. I am trying to establish standards where standards do not exist. Chain of custody and documentation is very important” (p. 23-24).

Conclusion

A step in the right direction is the development of dedicated Computer Crimes Units, “Cyber Cops.” Officers cannot be expected to become experts at investigating computer type crimes in their spare time, especially when technology and criminal methods on the Internet change so quickly. Experts, who investigate only Cyber Crime, are necessary, if we in law enforcement are to make progress in the investigation and prosecution of computer crime.

We must become proactive in our efforts to combat the crime presented by this new challenge. Law Enforcement officers must learn to use the available technology to pursue criminals, to spread the word about computer crime, to arm potential victims with information and resources.

Law Enforcement must learn to use the Internet to their advantage. It can be an invaluable resource for us just like it has become a target rich environment for the criminal. We can post pictures of persons we are attempting to locate and the Internet will give us a million eyes looking for the person. It can be used in our efforts to locate missing children. We can eventually use the Internet and computers into a live worldwide network where it will be more difficult for people to hide.

Our officers are becoming more computer literate and we must continue to develop that trend. Law enforcement officers must understand that the computer is just another component of our investigations. We have already discussed to some degree the training that is needed for special units, but it is just as important train officers as they come through the various police academies in the use of the computer and the technology that is being used by the criminal mind to further their ability to commit crime.

Recruiting must target individuals who have a background in the use of computers and the changes in technology. In this way, law enforcement agencies can stay abreast of the changes in technology.

Law enforcement agencies should use the computer and the Internet to spread the word about what is working for them in the various type of investigations they are involved in, be they computer related or of the generic version. We must learn to work together in a cooperative effort to pool our resources to combat this very invasive new threat.

Task force type units should be formed to investigate crimes such as child pornography where jurisdictional lines may be crossed. There are so many facets of these type investigations that it only makes sense. Each agency involved could develop areas of expertise such as undercover, identifying suspects on line, encryption, and graphics. This would lead to a dozen or more cops that would contribute to solve these crimes.

The bottom line is that departments across the state have to commit resources to the computer side of law enforcement. As stated above, we must consider task force type operations to pool our resources and make the most of the expertise found in each of the departments involved.

Computer crime is not going to go away. Computers and the Internet are not some fad like the CB radio or bell-bottom pants. It is here to stay and the computer will continue to have a dramatic impact in the foreseeable future. As the use of computers and the Internet grows, so will computer related crime.

We in law enforcement must be ready.