

TELEMASP BULLETIN

TEXAS LAW ENFORCEMENT MANAGEMENT AND ADMINISTRATIVE STATISTICS PROGRAM

April/May 2000

Vol. 7, No. 1

An Overview of Computer-Related Crime

Anecdotes available from reported offenses provide strong support that computer-related crime has increased dramatically in recent years. Indeed, both the character and nature of these offenses and their frequency of occurrence have changed notably since about 1995 when the Internet experienced explosive growth. One simply needs to search the phrase "computer crime" on a web search engine and find a plethora of incidents and commentary on the problem. How much computer crime is occurring? It is simply unknown. Not only is there significant inconsistency in defining computer crime offenses, there is a void of any attempt to collect offense data.

Offenses vary in character from clear criminality (e.g., theft, fraud, or destruction of data files) to acts where criminal culpability is less clear, such as violations of privacy (e.g., unauthorized access to credit reports or medical records). Similarly, types of criminal behavior by web site users also varies (e.g., pornography, black marketeering, or gambling). This is complicated by the global character of networking offenses—transactions and behavioral interactions can occur between people worldwide from their homes with no scrutiny by immigration, customs, or other government entity. The gravity of the problem is illustrated by the Computer Crime and Intellectual

Property Section of the U.S. Department of Justice which estimates cybercrime costs as high as \$10 billion annually (Williams 1999). This *TELEMASP Bulletin* reviews the fundamentals of computer crime to place it in a contemporary perspective.

The Changing Character of Cyber Victimization

The extent and nature of computer crime appears to be on a rapidly ascending curve. A study conducted by the American Bar Association in 1987 found that of the 300 corporations and government agencies surveyed, 72 (24%) claimed to have been the victim of a computer-related crime in the 12 months prior to the survey (ABA 1987). The estimated losses from these crimes ranged from \$145 million to \$730 million over the one year period. This broad range is illustrative of the problem in estimating losses. Not

**Special Bulletin
Co-Sponsored by the
Texas Regional Community
Policing Institute,
Funded by the
Office of Community Oriented
Policing Services**

*Bill Blackwood Law Enforcement Management Institute of Texas
Texas Regional Community Policing Institute*



only is it difficult to identify and document these crimes, it is even more difficult to place a monetary value on the loss of intellectual property wherein the actual value may not be known for months or years.

Two years later, the Florida Department of Law Enforcement (FDLE) surveyed 898 public and private sector organizations which conducted business by computer. Of the 403 (44.9%) respondents, 25% reported they had been victimized by computer criminals (FDLE 1989). The Florida study found embezzlement of funds by employees to be a major source of the crimes; however, no attempt to estimate losses was made because, according to one of the researchers interviewed, "losses would have been nothing more than a guess."

In 1991, a survey was conducted of 3,000 Virtual Address Extension (VAX) sites in Canada, Europe, and the United States to assess computer security threats and crimes. The results show that 72% of the respondents reported a security incident had occurred within the previous 12 months, with 43% reporting the incident was criminal in nature (U.N. Commission on Crime and Criminal Justice 1995). The ABA and FDLE studies scarcely even mentioned this "external threat" and gave little attention to it as a growing problem. This is not surprising, however, since networking in the late 1980s was predominantly used by the military, academics, and researchers. Access was comparatively limited and networking technology was both more expensive and more cumbersome. However, the 1991 United Nations study suggested that external threats via remote access was a problem which would grow in the years to come. Despite this concern, past research suggests that threats of computer crime generally come from employees, just like much of the theft in retail businesses.

The data from Carter and Katz (1998) show a trend of victimization which increased significantly over previous studies, with 98.5% of the respondents reporting they had been victimized—43.3% reported being victimized more than 25 times. While these numbers seem dramatic, security professionals with whom these results were discussed stated they were

surprised at the frequency of admitted victimization, not actual victimization. One respondent stated, "Do we know the national or even local scope of the computer crime threat? Probably not; but it has to be higher than anyone wants to admit."

The 1998 joint survey by the FBI and Computer Security Institute found that for the third year in a row, corporate security directors reported an increase of computer system penetration by outsiders. This represented a 20% increase of successful system incursions since 1996 (Computer Security Institute, 1999). Collectively, these data provide empirical support for the anecdotal evidence: Not only is unauthorized access to and theft from computer systems increasing, but the number of system incursions committed by "outsiders" is increasing.

Hacking and thefts are the best documented offenses; however, other forms of cybercriminality are emerging also. Fraud through investment web sites, theft of identity, and telecommunications are all examples of expanding areas of criminality (*see* Computer Security Institute 1999; Public Interest Research Group 1999). Nor is cybercrime limited to crimes against property. A recent initiative by the U.S. Department of Justice explored the problem of cyberstalking, noting the rapidly increasing nature of the problem, which is aggravated by the increasing amount of personal information available on the Internet (U.S. Department of Justice 1999). While largely anecdotal information has been collected on these crimes, little is known about offense patterns and offender characteristics.

What Is Computer Crime?

Since computer crimes can vary widely, a single definition—beyond criminal behavior wherein a computer is involved—is insufficient. Rather, it is more accurate to describe computer crime based on the different, albeit overlapping, methods a computer is involved in (or associated with) criminal acts (*see* Figure 1).

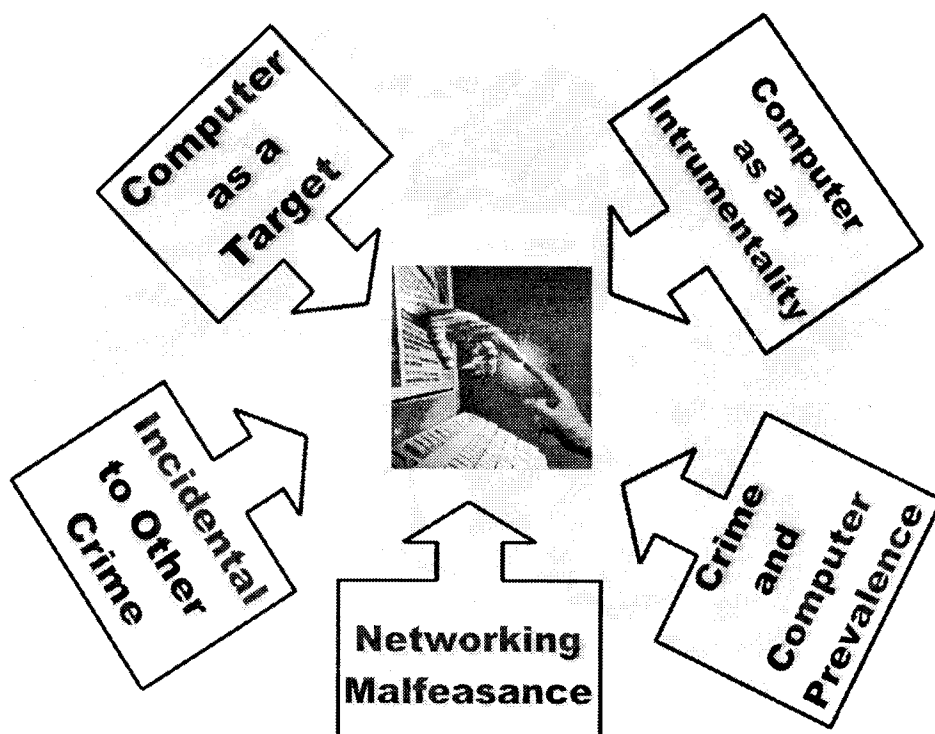


Figure 1

Characterizations of Computer Crime

The computer is the target. In these cases, the intent of the offender is either (1) to take information from the computer's memory, or (2) intentionally damage hardware, programs, or data files. Essential to these offenses is the unauthorized access to stored memory by either a network incursion (i.e., hacking/cracking), a violation of trust (i.e., an employee or otherwise authorized user violates the conditions of access to the computer); or unauthorized direct access to the computer (i.e., a person who has no lawful access to a computer surreptitiously accesses the machine to commit the offense). Also essential in this category is that the theft or damage is intentional. Offenses may include theft of intellectual property, theft of marketing information (e.g., price lists, etc.), sabotage of intellectual property, sabotage of software applications or data files, or the unlawful access to or tampering with personal, business, or government records.

One area which has experienced notable growth since the rapid expansion of networking is referred to as hactivism. This is the practice of hacking into a web site of a person, group, government, organization, or business whom the hacker defines as a political (or ideological) opponent. The intent of the incursion is typically to deface a web page, cause disruption of the web site's function, incur expenses for the web site owner for repairs, and/or to articulate an opposing viewpoint. For example, animal rights activists have hacked web pages of research organizations and businesses which use animals to test products. During the conflict in the former Yugoslavia, the web sites of NATO, U.S. Department of Defense, and the British Ministry of Defence were hacked a number of times with protest messages left by the hackers.



The computer as an instrumentality of a crime. In these cases, the processes of the computer are used to facilitate the crime. Just like a burglar may use a screw driver as a criminal instrument to break into a home, the computer may be used as a criminal instrument to commit crimes. Crimes may include frauds from use of ATM cards and accounts, theft of money through “round-off” schemes on interest calculations or currency conversions, credit card fraud, fraud from transactions in the computer, or telecommunications fraud.

The computer is incidental to other crimes. These are circumstances where a pattern or incident of criminality uses a computer simply for ease in maintaining the efficacy of criminal transactions. Importantly, the computer is not essential to the crime, but the technology is being used to more easily facilitate the crime. Crimes may include money laundering, pornography distribution, facilitation of pedophilia, book making, child abductions, and even murder.

Crime which is associated with the prevalence of computers. Just as computers may be targets and instrumentalities, computers and related technologies may also be crime commodities. The crime may be committed without a computer; however, the advent of micro-computers have produced new crime targets. Crimes may include software piracy and counterfeit, copyright violations of software, counterfeit equipment, and black market trafficking of stolen computer memory, processors, peripherals, and software.

Networking malfeasance. These offenses are committed explicitly as a result of the communications and access afforded by networking. It includes a wide array of behaviors, including some which are “improper” but not criminal, *per se*, (e.g., privacy violations) and others at the opposite end of the continuum which may be considered as crimes against persons. Examples of networking malfeasance include harassment, defamation of an individual or an organization via networking messages, luring minors to meet with sexual offend-

ers, use of a computer’s access and dissemination abilities as a threat, use of the computer in newly developed or adapted con games (fraud), cyberstalking, criminal inducement (i.e., pedophiles, illegal gambling, inciting hate crimes), and the unauthorized access to a computer system including the viewing of files just to “explore” the system. This is sometimes referred to as “walking through a computer.” In some cases, there may be a criminal violation—depending on the nature of the information which is accessed—but in many cases this is most likely to be a civil matter.

Computer Hacking

According to the on-line “new hacker’s dictionary,” a hacker is a person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. Hackers have a great deal of expertise and knowledge about computer systems and software capacity but use their skills for solving computing problems, identifying security holes, and to “push” systems beyond their intended use or design. Within this techno-culture, hackers maintain they do not violate privacy, nor do they take the property of another or disrupt systems.

A cracker is one who breaks the security of a computer system to explore private files, download information, and/or disrupt the intended operation and use of a computer system. Contrary to widespread belief, this does not usually involve some ingenious application or insightful brilliance, but rather persistence and the dogged repetition of techniques which exploit common weaknesses in the security of target systems.

While hackers and crackers are insistent on the distinction between these two, the media and the general culture use the terms synonymously. Indeed, on web sites which have been defaced by system intruders, it is common to see statements such as “you’ve been hacked” (rather than “you’ve been cracked.”)



Another important player in the techno-culture is the “phreaker.” These are individuals who have developed knowledge and expertise to crack telecommunications systems. This practice has changed significantly over a very short time due to the growth of digital telecommunications networks and the use of computers in voice mail and as telecommunications switches. Thus, contemporary phreakers are those individuals with hacking knowledge as specifically *applied to telecommunications systems*.

Organized Crime

Interpol defines organized crime as any enterprise or group of persons engaged in a continuing illegal activity which has as its primary purpose the generation of profits and continuance of the enterprise regardless of national boundaries (Carter 1994). Key factors in this definition with respect to the forecast is that organized crime groups are *entrepreneurial* and that they exist for the purposes of making a profit. Just like legitimate businesses, organized crime groups have consistently used methods which will enhance efficiency and effectiveness to achieve profits. Many methods are illegal—such as use of violence, corruption or fraud—yet legal methods are also used such as stock investments, purchase of real estate and other principles common to legitimate businesses for distribution and marketing of a commodity. Globally, the character of organized crime is evolving into this entrepreneurial model. Traditional images of organized crime as a “Mafia-like” entity are dated, not reflecting the vast amount of organized criminal activity occurring around the world today. To neither recognize nor respond to this change is to perpetuate a myth.

Just as computerization is used to enhance the efficacy of legitimate businesses, organized crime groups follow similar methods. Further, since many organized crime groups have demonstrated creativity in furthering their enterprises, it is reasonable to assume that they will also embrace the capabilities available through technology.

Computerization has been used by organized crime groups in a number of ways (see Figure 2).

Record keeping. Evidence by law enforcement and intelligence organizations have found crime groups keeping computerized spreadsheets and databases. Records which have been discovered include contraband shipment schedules; income and expenses of contraband or commodities; databases of conspirators and “customers”; locations, account numbers, and status of monetary transactions (typically money being laundered); records of monetary transfers and payments; databases and “status” of bribed or vulnerable officials; and database dossiers of officials, conspirators, and others with whom the crime group has an interest.

Counterfeit currency and documents. Computer technology has provided a revolution in the counterfeit currency and document business. With color scanners, color printers, sophisticated word processing and graphics software suites, and computer-driven color photocopiers, successful counterfeiting has not only significantly broadened, but also become much more difficult to detect. As one example, within one month after the release of the new “counterfeit-proof” U.S. \$100 bill, good counterfeits of the currency were discovered in Eastern Europe.

The same scanning process and graphics software are used for counterfeit passports. Counterfeiters maintain scanned “masters” of various passports in computer files and are then able to readily enter appropriate names, photographs and identity information in the files to prepare a high quality counterfeit. Because the counterfeits are near the quality of legitimate documents and the process of creating the counterfeits is fast, the enterprise yields high profits.

Illegal immigration. Outside of refugees fleeing into countries such as Zambia and Thailand from neighboring countries embroiled in civil war, the European Union countries have experienced some

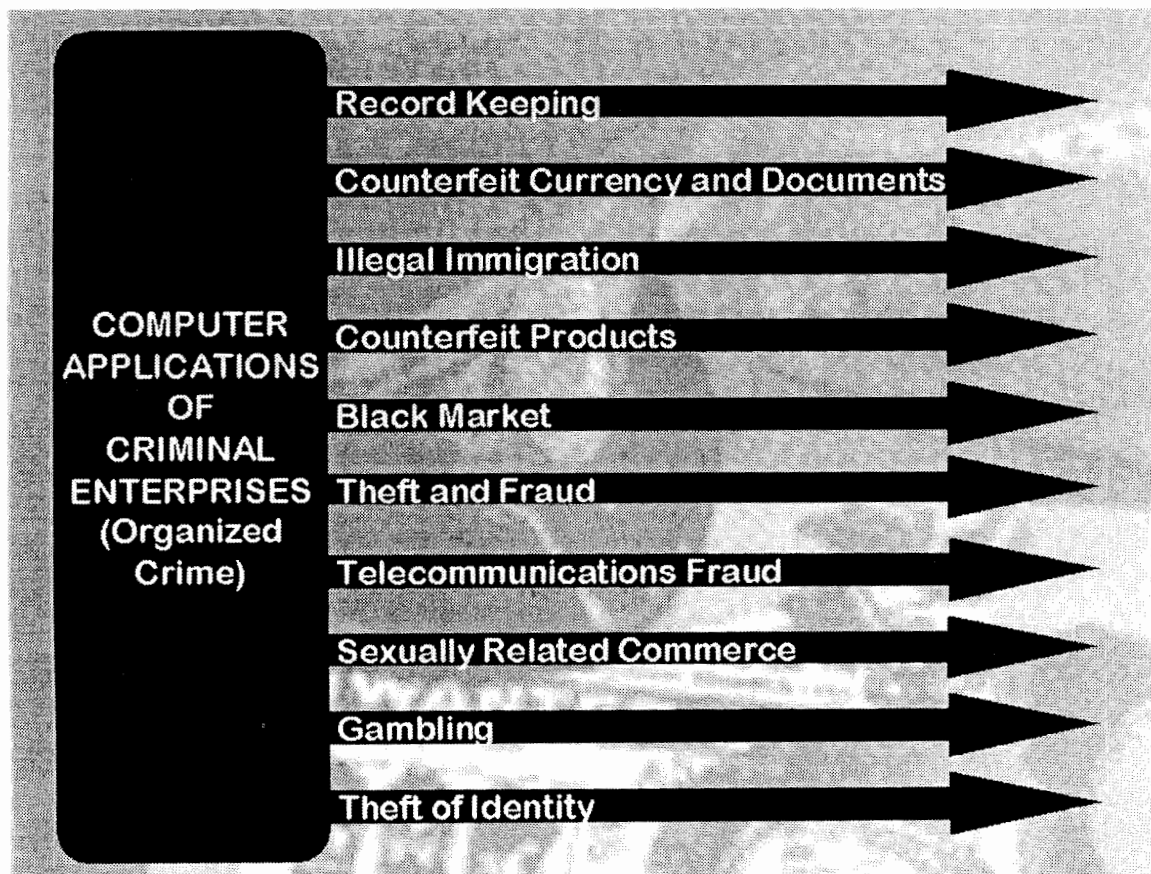


Figure 2

Uses of Computers by Organized Crime Groups

of the largest influx of illegal immigrants (notably from Central and Eastern Europe). Seeking both peace and economic opportunity, the new immigrants have made many sacrifices—including financial ones—to achieve their goals. As in other cases when governments are slow in responding to a crisis—if they respond at all—criminal enterprises will fill the void.

In these cases, evidence has indicated that organized crime groups previously involved mostly in black market smuggling have created new processes to smuggle immigrants into Western countries with “appropriate” documentation, typically for a substantial fee. While computers play a comparatively smaller role in these enterprises,

they nonetheless help expedite the scheme through the use of such processes as logistics and arrangements via e-mail; computer forged immigration documents; and general record keeping related to this enterprise.

Black market. In virtually every country in the world, there is a Black Market available to provide people with products they need or desire but simply cannot obtain (or sometimes afford) through the legitimate open market. The Black Market trades in any commodity which will turn a profit, particularly if the commodity is contraband (ranging from prohibited pharmaceuticals to Cuban cigars), counterfeit (Rolex watches have remained a long-standing popular Black Market item), or stolen



property (anything which is popular but either too expensive to purchase or difficult to obtain). In nearly every Black Market, organized crime is omnipresent.

Outside of its illegal commodities and avoidance of licensing and taxes, the Black Market operates much like any business. It is market-driven; requires suppliers, transportation and distribution networks; it has a payroll; it must remain competitive; and it is obliged to keep its customers satisfied in order to maintain repeat clientele. Because of the similarities with legitimate businesses, organized crime groups involved in the Black Market have increasingly operated much like legitimate businesses.

Just as in any business, the Black Market needs to make its inventory descriptions known to both the "sales staff" and potential clients. Photographs, product descriptions, costs, inquiry processes and related information for a wide variety of "commodities" have been found in computer files; in a few cases the files are accessible through a restricted server or web site. Additionally, some Black Market merchandise is increasingly available for order through the Internet (under the guise of a legitimate business), vastly expanding the enterprises' market, hence profits. In addition, computerization via networking provides increased anonymity to specific individuals in the criminal group.

Counterfeit products. The marketing of counterfeit products—ranging from Nikon cameras to Microsoft software to Levi jeans—is well documented. The extent to which "traditional" organized crime is involved is debated; however, there is strong evidence that such groups are strongly involved in the "marketing" and distribution of these products.

As in the case of counterfeit currency and documents, criminal enterprises have been using color scanners and computer-driven color printers to scan legitimate logos, product tags, and such

things as "jackets" and labels of videotapes, audio tapes, and software. Using the scanned images as masters, skilled printers are able to prepare these materials to legitimize the appearance of the counterfeit products. Counterfeit packaging of black market products is also being used to make the product look more legitimate to the consumer. With packaging that makes the product appear authentic, the enterprise could sell more of their counterfeit products at higher prices and still undercut the legitimate manufacturer's sales.

Sexually related commerce. Most people have heard news accounts about various forms of individual sexually related misconduct (such as child pornography) occurring via the Internet. Organized crime has virtually no involvement with such incidents. Keeping in mind that the sole purpose of a criminal enterprise is to make a profit, the role of organized crime in this venue is to promote sexually related commerce.

Using the Internet to arrange for prostitution is one of the more common enterprises. This includes not only logistical arrangements (i.e., appointments) but even payment by credit card using e-commerce protocols. The process is discreet and safer for both the "service provider" and "customer." In one case, a criminal enterprise using a server based in Amsterdam was arranging for prostitutes in both London and Frankfurt. Although the enterprise has been closed, it was difficult because of limitations inherent in dealing with multi-national jurisdictions. One investigator stated that if the enterprise had been based in a non-European Union country, it would probably still be in operation.

Gambling. Gambling has always been a favorite—and profitable—activity for organized crime. At this point it appears most unlawful computerized gaming operations—notably in North America and Asia—are not on the Internet but accessible via modem directly into a server (albeit using Internet protocols). However, accessibility to such operations are increasingly available through the



Internet using Virtual Private Network (VPN) access for security (largely from authorities) and to ensure payment for services. The expanded capacity for multimedia hardware and software is particularly fueling sites by enabling more effective simulation of video gaming machines.

Typically, the user must "join a club" to be given access to the site for gambling. Part of the membership ruse is to pay "dues" which are used as bets. Most typically gamblers supply a credit card number wherein they can purchase "units" to wager—"units" are essentially electronic poker chips. (Most typically, all wagers and transactions are converted to U.S. dollars regardless of the country of origin.)

In some cases, when a member joins and is given his/her personal identification number, they can then make a deposit—either by wire or money order—to a front company which serves as the "bank" for the gambling operation. All bets and communications are then conducted via the computer link. When the gambler wins, he/she is typically given credits which can be used for further wagers or he/she can request payment, typically through the front company which serves as a bank. Credit card "credits" are not used for two reasons: (1) the gamblers want their winnings quickly in a readily convertible form, and (2) it is feared that the issuance of too many credits to a given card number would raise questions leading to investigations.

Theft and fraud. As computers are increasingly used to account for and make financial transactions, criminals are increasingly accessing them unlawfully to transfer funds, defraud, or steal information. Many anecdotes are available concerning employees or hackers who have committed such crimes. One of the most frequently cited is the case of a Russian organized crime group which stole \$12 million from Citibank via computer (all but around \$400,000 was recovered). This, however, is currently the exception rather than the rule for criminal enterprises.

The most common computer-assisted thefts by organized crime groups target intellectual property. As information becomes an increasingly valuable commodity, organized criminals have learned how to market stolen information for high profits and substantially less risk than more traditional illicit commodity trafficking. Theft of information such as trade secrets, new product specifications, product pricing plans, and customer lists have proven to be highly profitable. While these transactions typically do not have the violence and emotional daring associated with more traditional organized crime activities, the economic toll can be far higher.

The second area of computer-assisted theft by organized crime is fraud. The Florida Division of Insurance Fraud has discovered fraud through altered computer programs which underreport insurance agency incomes. Medical and pharmaceutical overpayments through Medicare/Medicaid have also been fraudulently made in many ways through the altering of computer records and, more commonly, the use of shell companies billing the government for medical services, equipment, and pharmaceuticals. While these forms of theft net significant amounts of money, they typically are not products of broad-based organized crime, although they frequently meet the technical definition of a criminal enterprise. Such offenses are difficult to detect, difficult to investigate, and difficult to prosecute. Moreover, they engender little emotional outcry from the public. As a result, they offer little risk and high profits—an appealing combination of factors for the entrepreneurial offender.

Telecommunications fraud. There are four types of telecommunications fraud which criminal enterprises appear to be most involved. First is the theft of telephone credit card numbers which can be gained by accessing computer records, some computerized voice mail boxes, and telephone billing files. Prime targets are large multi-national corporations because discovery of the fraudulent billings takes longer. The billing numbers are either sold "on the street" (using "pushers" in the



same method as drug dealers) or, as is increasingly the case, sold to other crime groups for their use.

The second type of telecommunications fraud, which has actually decreased, involves hacking into telecommunications “switches” (which are computers) for the purpose of routing calls and changing billing numbers. While individual hackers still break into the switches, organized efforts to do this have largely stopped as a result of more aggressive security precautions by telecommunications carriers and comparatively little profit to be made.

The third area is the largest and fastest growing—wireless phone theft and fraud. This too was started by individuals and small groups but is increasingly involving organized crime groups. The process originally involved the capture of wireless Electronic Identification Numbers (EINs) being transmitted from users’ telephones. Using a device which detects and records the number, it could then be sold and programmed into a person’s wireless phone. The number is typically usable for about one month before being detected as stolen. The fraudulent user would then need to purchase a new number.

The fourth type—which has increased significantly—is where organized crime groups have compromised Private Automatic Branch Exchanges (PABX) of companies to use telecommunications services for their own benefit (FBI 1999). A PABX is the heart of a digital telecommunications system which can include a company’s internal phone system, its wireless network, voice mail, e-mail, and internal data network. A criminal enterprise using this system can call anywhere in the world without costs. Moreover, using a compromised system makes it more difficult for investigators to gain a wiretap order or to follow a trail of telephone calls. The unlawful use of a PABX not only constitutes a real monetary loss to the victim, it also makes investigations of organized crime groups more difficult.

Theft of identity. A rapidly growing type of crime is the theft of identity. While there are numerous variations, essentially it occurs when someone uses personal information about an individual—usually the Social Security Number, a credit card number, address and phone number—to represent him or herself as that person for fraudulent purposes. Examples include obtaining credit cards and loans in someone else’s name and then not paying the bills; opening utility accounts; renting an apartment; obtaining a wireless telephone; and so forth. In some instances cars have also been purchased with false identities. Another type of identity theft—a worst case scenario—is when the perpetrator commits a crime in the victim’s name and gives that person a criminal record (Public Interest Research Group 1999). Stolen identities have also been used by people for flight to avoid prosecution as well as to hide in order to avoid such things as the civil process or creditors.

Organized crime groups have long been involved in the trafficking of stolen merchandise. The evidence from this research suggests that criminal enterprises are using identity theft for fraudulent purposes; however, the greatest and easiest profit is trafficking in stolen identities, *per se*. Given the earlier discussion on the ease of counterfeiting official documents coupled with the ability to obtain a great deal of personal information quite easily, it is likely that there will be a significant growth of identity theft supported by sophisticated documentation which will produce a legitimate appearance.

Responding to Computer Crime in Texas

While there are some computer crime initiatives in Texas, they are being overwhelmed by the number of cases where computers are involved. In the Dallas/Fort Worth Metroplex, there are only three police employees trained as computer forensic analysts—two at the Dallas Police Department and one at the Irving Police Department—all of whom attempt to help agencies in the region when



possible. The forensic analyst has the tedious task of creating a "mirror image" of a seized computer's hard drive in order to search the mirror for incriminating evidence. The analyst must have the expertise to break security measures on the original hard drive and avoid "traps" set by the computer's owner that would destroy files. Once gaining access to the hard drive, each file must be opened—many of which may be password protected—and reviewed for evidence. Each computer hard drive can take three or four days to completely analyze. Given the Metroplex population, and particularly in light of the number of high technology firms located there, the caseload has quickly become overwhelming. The Irving forensic analyst estimated his backlog to be six months.

Beyond the Metroplex, there are forensic analysts in the Austin and Houston Police Departments with forensic personnel being trained for the Texas Department of Public Safety. In many cases, all of these specialists must also do investigative work as well as forensic analysis resulting in even greater delays for processing cases. Despite this limited staffing, only California, New York, and the federal

government have more computer crime investigative expertise than Texas.

In the area of child pornography via computer, there is a North Texas Task Force with federal, state, and local investigators focusing investigations on Internet-based child pornography distribution networks. The Task Force has had good success as a computer-related investigative initiative in the state.

Policy Implications

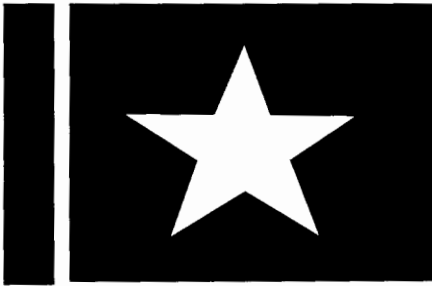
Police agencies must recognize computer crime as a problem to be addressed. This recognition has implications for staffing, training, and perhaps prioritizing duties. While computer crime does not have the emotional impact of predatory crime, its effects are costly—perhaps larger than all other crimes against property combined. Given the growth of the Internet for e-commerce and entertainment, it was inevitable that criminals would find ways to exploit the web for power and profit. Law enforcement must be prepared to respond with the same resilience.

References

- American Bar Association. (1987). *Report on Computer Crime*. Chicago: American Bar Association.
- Carter, D.L. (1994). "International Organized Crime: Emerging Trends in Entrepreneurial Crime." *Journal of Contemporary Criminal Justice*, 10(4):239-266.
- Carter, D.L. and Katz, A.J. (1998). "Computer Crime Victimization: An Assessment of Criminality in Cyberspace." *Police Research Quarterly*, Vol. 1, No. 1.
- Computer Security Institute. (1999). *Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey*. San Francisco: Computer Security Institute.
- Florida Department of Law Enforcement. (1989). *Computer Crime in Florida*. An unpublished report prepared by the Florida Department of Law Enforcement, Tallahassee, Florida.
- Public Interest Research Group. (1999). *Identity Theft II: Return to the Consumer X-Files*. PIRG Report online at <http://www.igc.org/pirg/consumer/xfiles/index.htm>.
- U.N. Commission on Crime and Criminal Justice. (1995). *United Nations Manual on the Prevention and Control of Computer-Related Crime*. New York: United Nations.
- U.S. Department of Justice. (1999). *Cyberstalking: A New Challenge for Law Enforcement and Industry*. A report to the Vice-President. <http://www.usdoj.gov/ag/cyberstalkingreport.htm>.
- Williams, Wayne. (1999). "The National Cyberterrorism Training Partnership." *The Informant*, 25(3):7-11.

Note

Figures 1 and 2 are used with permission of David L. Carter and Andra J. Bannister. (2000). *Computer Crime: A Forecast of Emerging Trends*. Paper presented at the Annual Meeting of the Academy of Criminal Justice Sciences. (New Orleans, LA).



BILL BLACKWOOD

Law
Enforcement
Management
Institute of
Texas

Randy Garner, Ph.D.
Executive Director

Kay Billingsley
Publications Manager

For information about LEMIT
programs, call (800) 477-9248



A Member of The Texas State University System

TELEMASP Monthly Bulletins,
ISSN 1075-3702, are produced
under an agreement with the

Police Research Center
Sam Houston State University
Larry T. Hoover, Ph.D., Director
Jamie L. Tillerson, Program Manager

© Sam Houston State University

For information about TELEMASP
Bulletins, call (936) 294-1704

This Bulletin was authored by Dr. David Carter, professor in the School of Criminal Justice and director of the National Center for Community Policing at Michigan State University. Dr. Carter participates in LEMIT's LCC program and Executive Issues Seminars.

This project was co-sponsored by cooperative agreement #97-CK-WX-0020 awarded by the Office of Community Oriented Policing Services, U.S. Department of Justice. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

**Bill Blackwood Law Enforcement
Management Institute of Texas**
Criminal Justice Center
Sam Houston State University
Huntsville, TX 77341-2296

Non-Profit
Organization
U.S. POSTAGE
PAID
Permit No. 26
Huntsville
Texas