case study

Information Age.
Vol. 9, #1 Jan 87

Combatting computer crime

Ken McLeod gives an overview of the setting up and operation to date of Maricopa County Sheriff's Office Computer Crimes Unit

The first two years' operation of a computer crimes unit is reviewed. The various categories of high-technology crime encountered are outlined, and cases of them given. The skills, background and expertise of a high-technology investigator are described.

Keywords: crime investigation, computer crime, telecommunications fraud, computer fraud

The Maricopa County Sheriff's Office Computer Crimes Unit was formed on 27 July 1984, with more than a little consternation. After many months of trying to convince the administration that such a unit was necessary, permission was given to form the unit. However, once the go ahead had been given, the question was raised, 'Okay, what now?'

We had no one to go for help in setting up our unit, so, with little hesitation, we set out to determine the best course of action in forming it. Although the deputies assigned to the unit had many years of computer and telecommunications experience, little or no literature existed on computer fraud investigation procedure.

We soon found that our small unit was on the leading edge of computer fraud investigations: when we sought advice from other police agencies, little was available. We were breaking new ground and few police agencies could help.

Nevertheless, we soon found an abundance of high-technology crime taking place right on our doorstep, in Arizona. Within two days of forming the unit, we had our first computer fraud arrest; or at least we thought we did. It turned out somewhat differently. One of the projects we started during the formation of the Computer Crimes Unit was the development of a computerized public access bulletin board system. We believed that, if we opened up a high-technology form of communications with the public, someone might use it to report high-technology crime!

On 29 July 1984, a young man called into the bulletin board and posted a message to all users. In this message the youth offered to modify the decoders of the local cable television companies for a fee, allowing the users of the decoders to receive the premium pay TV channels free of charge.

Needless to say, we were excited at the prospect of investigating this possible crime; surprise was the least of our feelings at seeing this message posted on a bulletin board system clearly identified as being run by the police! We took the young man up on his offer, giving him the address of our apartment, which was actually a small apartment rented just for the occasion by the cable TV company.

The cable company provided a colour TV and two decoders. One was 'mine' and the other belonged to my neighbour 'Bud' (my partner). At the prearranged time, the young man showed up with considerable precision, and the young man (who was 15 years old) proceeded to open the decoders and modify one part which defeated the scrambling software of the device. He demonstrated how we could now receive all the premium channels without 'lining the pockets of the cable company'. The youth told us that he learned the secret from his brother, an engineer with a local electronics firm. He also told us how he had been convicted of burglary just the day before, for breaking into a school.

We paid him the agreed price, and, just before he left the apartment, we arrested him, later charging him with burglary and two counts of tampering with a cable TV decoder. Just a few months before, the Arizona legislature had made it a felony, punishable by 18 months in prison and a $150 000 fine, to tamper with a cable TV decoder. Since the young man entered a structure for the purpose of committing a felony therein, he was charged with burglary. He later pleaded guilty to all charges.

Maricopa County Sheriff's Office, Maricopa County, Phoenix, Arizona, USA

While this is clearly not a computer fraud, the incident started with a young man using his home computer to initiate contacts for his illegal enterprise. We felt this was the type of crime that was well within our mission to investigate and prosecute.

A few months later, again with information provided to us through our bulletin board system (BBS), we made the first arrests of bulletin board system operators (SYSOPs), who were alleged to have passed computer access codes and other information through their BBS for other users to obtain and use to defraud computer companies.

The Computer Crimes Unit is generally responsible for the detection and apprehension of persons who commit crimes in which technically complicated devices or methods are used to commit or facilitate the criminal activity or are the object of the crime. The unit differs somewhat from other traditional investigatory units in that very little criminal activity is referred to the unit from within the Sheriff's office. What this means is that most of the crimes investigated by the unit are started through the actions of the personnel assigned to the unit, i.e. through undercover investigations or covert sources. Some of the main areas of investigatory concentration are as follows.

TELECOMMUNICATIONS FRAUD

Telecommunications fraud is the theft of computer or telecommunications services and/or the dissemination of information by individuals or groups for the purpose of defrauding telecommunications or computer companies. This includes all forms of transmission, radio (RF), microwave, lightwave (laser and fibreoptics), and twisted-pair (electromagnetic).

Telecommunications fraud is usually investigated by employing electronic surveillance, interception or monitoring. This does not necessarily mean an aural wiretap, but instead, a trap and trace of all calls coming into a specific location, or a pen register to track all telephone calls leaving a specific telephone.

At times this may also mean a level of cooperation from a third party common carrier or victim which may heretofore not have been available. Many providers of communications services have been reluctant to cooperate with law enforcement agencies, necessitating a change in the methods of acquiring electronic data.

For example, one of the methods used by the Computer Crimes Unit to obtain information from third party keepers of records and common carriers (Mountain Bell) is the grand jury subpoena. However, in a recent case in the District of Columbia, GTE Communications successfully fought a grand jury subpoena issued upon the company for the production of electronic mail between one narcotics dealer and another. GTE argued that, as a carrier of electronic mail, they were simply a provider of a service and not a keeper of records. Therefore, they had no authority to go into the electronic mail box of a subscriber and retrieve e-mail without the permission of the sender. Although many law enforcement officers would not agree with the GTE position, personally I see merit in their position and support it.

The ramifications of the GTE position are that the Computer Crimes Unit has used and will continue to use a greater number of search warrants to obtain information related to criminal activity in telecommunications cases. The advantage of a search warrant, besides the obvious benefit of judicial review prior to issuance, is that the person or place subject to search has no authority to resist the search. This will impact other investigatory details and units as a greater reliance is placed on the transmission and reception of electronic mail by suspects. This will also mean a need for greater specificity on the part of investigators seeking information from third party common carriers and uncooperative victims.

The Computer Crimes Unit is responsible for a number of firsts in the prosecution of telecommunications fraud:

- the first prosecution under the computer fraud statutes for the use of long-distance switching services without authorization,
- the first prosecution of a person using a computerized blue box to obtain long-distance switching services illegally,
- the first prosecution of a person for disseminating long-distance access codes from one person to another via computer.

COMPUTER FRAUD

The Computer Crimes Unit has, to date, handled a broad number of crimes which were prosecuted under the computer fraud statute, ARS 13-2316, et seq. These investigations have usually involved unauthorized access into a computer system or computer network, or the dissemination of the means to gain unauthorized computer access. The sources of information used as a foundation for these investigations come, for the most part, from three sources: informants, the public access bulletin board system and undercover investigations.

The informants have been developed over the last two years by the members of the Computer Crimes Unit, much the same as any other investigator would

Note: there is a fine line between ARS 13-3707, *Telecommunications Fraud* and ARS 13-2316(A), (B), *Computer Fraud.* Computer fraud is often the statute of choice and has successfully been charged in quite a few telecommunications fraud cases, the primary reason being that computer fraud is a felony and a part of the organized crime statutes, and telecommunications fraud is only a misdemeanour.

develop sources. The bulletin board system has been instrumental in providing a source of high-technology information flow between computer users and law enforcement. Several cases were developed through tips provided through the bulletin board system.

The undercover operations of the Computer Crimes Unit have consisted of infiltrating the groups of people who are attempting to gain, or have succeeded in gaining, unauthorized computer access. Avoiding specifics, this involves investigators posing as computer criminals by calling into the computer systems operated by criminals and gaining the trust of the person or persons possessing or disseminating the entry authorizations of target computer systems.

The investigation of computer crime requires a high level of intensity and knowledge on the part of investigators. While it may seem simple to a casual observer, the ease by which investigators understand the complaints of the victims comes not from law enforcement training, but from extensive backgrounds in computer systems and telecommunications.

Investigators handling high-technology cases must research their cases in the world of high-technology jargon and acronyms. Investigators are acting in an environment into which law enforcement has not stepped: the internal sanctuaries of high-technology research and manufacturing organizations. For this reason, persons assigned the responsibility of investigating high-technology crimes must be comfortable interviewing, for example, a computer scientist who possesses such a fundamental understanding of his subject that little consideration is given to explanation. This requires that investigators remain current on the dynamism inherent in the rapidly changing electronics field.

It is difficult to quantify the exact skills required of a high-technology investigator, except that the person needs to be highly conversant in the fundamentals of computer and electronic theory. Another area of required expertise is the ability to search for and seize highly technical evidence and to subsequently examine the evidence. To date, the Computer Crimes Unit has relied either on the personal expertise of the investigator or the expertise of persons not affiliated with the victim. This has created problems with the timely seizure or examination of evidence and therefore the possibility of losing the case. However, a recent decision in California may change this.

In People v. Superior Court (Moore & Gopal) (1980) 104 Cal. App. 3rd 1001, the California Court of Appeals there held that the police may use expert witnesses, including the victim's own expert employees, to actually do the physical searching of the suspects' premises under strict police supervision. In that case, the police had a search warrant and were searching for stolen integrated circuit design documents. The Court held that the items sought were so complex and technical as to be outside of the possible realm of experience of the police. Therefore, the court reasoned, the police were justified in relying totally upon the opinions of the experts, and were not required to have the experts explain everything to them before seizing the material.

This is a very good case for the prosecution, and a leading case on the subject. Also, in People v. Superior Court (Meyers) (1979) 25 Cal. 3rd 67, where burglary victims supplied a probable cause for a search warrant on a neighbour's garage, then were invited to help police search in both the garage and the house of the suspect. They identified 75 items not listed in the search warrant, which were seized. The California Supreme Court (on all people) upheld this practice as valid (See also Miller v. United States (9th Cir. 1982) 688 F2d 652, in accord.)

The Computer Crimes Unit has scored a number of firsts in the apprehension of computer fraud suspects:

- the first prosecution of a bulletin board SYSOP (system operator) for facilitation of computer fraud for allowing his bulletin board system to be used for the distribution of information on the methods for gaining unauthorized computer access, and the first authorization for a search warrant to search and seize the computer operated by a suspect,
- the first prosecution of any person, anywhere in the world for committing the wiretap of a computer to computer transmission,
- the first prosecution of any person for the crime of fraudulent schemes for operating a computer system with the intent that others believe the computer is actually another computer system and with the intent to obtain confidential information from the victims.

OTHER OFFENCES

The Computer Crimes Unit has undertaken investigations, which, at first glance, seem to be outside the parameters of the unit. However, the use of high-technology methods to pass illegal information is growing at such an alarming rate, it is now quite common to find computer crime suspects involved in other areas of more traditional criminal activity. Some of these investigations are as follows.

Trafficking in stolen property

It has become common for computer criminals to be selling the information or items they have unlawfully acquired. In many cases, the information about how to compromise a computer system can be worth substantially more in dollar value than the amount that the

largest sting operations recover in stolen property. For example, the US Bureau of Justice Statistics reported that the average loss in financial institutions in 1984, per computer fraud incident, was $500 000. Information on how to break in a financial computing system is hot property on the computer criminal market.

The Computer Crimes Unit was responsible for the first prosecution of a person(s) for the acquisition and distribution of computer information in which Trafficking was charged successfully.

Credit card fraud

The Computer Crimes Unit has uncovered several cases of persons trading credit card numbers via computer and then purchasing computer products or other items with those credit card numbers. While credit card fraud is certainly not a new crime, it is, nevertheless, prevalent among younger computer criminals. The Computer Crimes Unit has recovered many thousands of dollars in stolen property as a result of investigations originally commenced as computer fraud cases.

ADDITIONAL DUTIES

The Computer Crimes Unit has loaned its high-technology experience to many other sections of the Sheriff's office and outside agencies. This assistance generally involves consultation on the acquisition, installation or use of high-technology monitoring equipment. This also includes the necessary court orders authorizing these devices.

The unit has also been consulted when the need arises for rapid search warrant development. Because the unit is one of the most prolific users of search warrants, the detail has developed a computerized system to issue search warrants. This has allowed other sections to use the search warrant system when a warrant is needed quickly.

Investigators regularly seek forums from which new experience can be gained. Since the law enforcement community itself lacks the methods by which high-technology information is transferred to investigators, interaction between investigators and the high-technology community has been developed. This has been in the form of presentations by investigators to all types of groups, from social clubs to scientists at the Los Alamos National Laboratory. In return, investigators have been allowed to participate, as peers, in many types of proprietary and high-level training courses offered by electronic and computer companies.

Investigators assigned to the Computer Crimes Unit also possess a number of professional certifications, and are members of various information- and computer-oriented professional organizations.

In summary, the duties of a high-technology investigator involve the development of new skills and levels of understanding, accompanied by the traditional skills of a competent criminal investigator.