Global Information Assurance Certification Paper

Successful Partnerships for Fighting Computer Crime

Beth Binde

August 11, 2001

Introduction

Computer crimes are crimes in which computers are:

- a tool to facilitate or enable an illegal activity
- a target of criminal activity
- incidental to a criminal offense

Criminals use computers to facilitate "traditional" crimes. Examples include prostitution rings, loan sharking, illegal drug distribution, stalking and harassment. This is in addition to the computer worms, viruses, network intrusions and denial of service attacks that receive substantial attention from the news media. Other avenues that target computers include theft of hardware, software and services, counterfeiting of hardware, and software piracy. Closely related crimes in the high technology area include identity theft, telephone and phone card fraud, as well as other criminal uses of technology.

Given the wide range of possible criminal activities in the high technology arena, computer security officers need to be prepared to respond to computing incidents that are not only against the local acceptable use policy for computers and networks, but also violate federal, state or local statutes. The SANS Institute publication Computer Security Incident Handling Step by Step: A Survival Guide for Computer Security Incident Handling provides excellent guidance for incident handling. The pamphlet focuses on the preparation needed prior to an incident and the plans that need to be in place well ahead of time. Step 1.9 on page 14 recommends developing interfaces to law enforcement agencies and suggests how to facilitate the process, advising on the following:

- What to report and where to report it
- Establishing relationships with law enforcement
- Evidence collection

What to report and where to report it

As noted in the **Incident Handling** guide, law enforcement is primarily interested in arresting and prosecuting criminals and investigating violations of the law. As annoying as spam (unsolicited bulk email) can be, the Federal Bureau of Investigation will probably not open a case on the matter. Their mandate is to investigate crimes that meet specific criteria. Examples include financial loss over a certain (statutory) amount, breaches of national security, or distribution of child pornography. At the same time, email death threats to the President of the United States may warrant an investigation by the United States Secret Service. There may be violations of state statutes, indicating that the state police have jurisdiction. Many areas have local police departments and while universities may depend on municipal police departments, some have their own separate and distinct police departments with fully certified officers and detective

bureaus. To complicate matters even further, laws on more than one level (federal, state, local) may have been broken. It is important to know where to call, but figuring that out is a challenge.

A seminar on computer crime law geared to computer security officers is a good investment of time. For example, as of this writing, federal law differentiates between email that has been read by the intended recipient and email that has not yet been read; and between unread email more than 180 days old and unread email less than 180 days old. A general acquaintance with computer crime laws is helpful. See the **References** for a link to the full text of federal statutes, as provided by the Department of Justice. Interpretive guidance on *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* is available on the same site. State statutes as well as federal can be located through American Law Sources On-Line (http://www.lawsource.com/also/). In addition, the SANS Institute Information Security Reading Room includes an introductory overview of legal issues as presented by Jimmy Staggs (http://www.sans.org/infosecFAQ/legal/law.htm).

Be advised that it is particularly wise to consult your legal counsel with regard to interpretations of the law and applicability to the situation at hand. Depending on the policy in your institution, your legal counsel may wish to provide instructions on what evidentiary materials can be provided to law enforcement and what can be discussed with outside investigators as well as provide advice on what legal instruments (subpoena, search warrant, court order and so forth) may be needed in order to pursue the investigation. The interests of no one are well served if evidence is collected improperly and cannot be used in the prosecution of a case, especially if your institution is the victim of a crime.

The best solution to the question of knowing who to call is to establish working relationships with local law enforcement agencies. This will allow you to learn about the different agencies and their jurisdictions. When questions of jurisdiction arise, the resources for getting correct answers will be known to you.

Establishing relationships with law enforcement

Besides getting answers to questions about jurisdiction, good working relationships with law enforcement agencies are helpful during critical computer incidents. Working with a known law enforcement agency, hopefully a welcome ally, is far superior to the already stressful situation brought on by the criminal investigation of a critical computer incident. But where are the high technology crime units located? What are some good ways to approach a law enforcement agency?

The first challenge is to find the computer investigation units in your area and get in touch with

them. A good resource for contact information is a publication of the National Institute of Justice publication, Electronic Crime Scene Investigation: A Guide for First Responders available online (http://www.ojp.usdoj.gov/nij/pubs.htm). The body of the manual is an excellent guide to police procedures for collecting electronic evidence at a crime scene. Reviewing the document will acquaint you with investigative procedures and provide insight into law enforcement concerns. The appendices include a comprehensive listing of high technology crime units across the United States as well as a few other countries. There is an excellent bibliography of references and resources for training opportunities and a list of organizations that received a draft of the manual.

A number of the listed organizations open membership to law enforcement personnel as well as civilians interested in this area. Such organizations provide an excellent opportunity to meet law enforcement personnel who specialize in computer investigations and the chance to mingle with other institutional computer security officers. Three prominent organizations have been chosen for review. Each of them offer full and equal membership privileges to members of the private sectors as well as members of the public sector, including law enforcement personnel. These organizations (and their associated acronyms by which they are commonly known) are:

- High Tech Crime Consortium (HTCC)
- High Technology Crime Investigation Association (HTCIA)
- New York Electronic Crimes Task Force (NYECTF)

The HTCC (http://www.hightechcrimecops.org/) exists primarily in the virtual setting of cyberspace. The vision of HTCC is to assist law enforcement agencies in the fight against computer crime. Many lack the appropriate hardware, software, funding and training for the challenge of investigating computer crime. HTCC provides a forum for the sharing of information and expertise in these areas. There is an active mailing list for the exchange of information and ideas. HTCC also sponsors training opportunities for all members of the organization, including law enforcement personnel and those without law enforcement affiliations.

The HTCIA (http://www.htcia.org/index.html) is an organization similar to HTCC. HTCIA sponsors training opportunities and mailing lists as well. In addition, there are regional chapters that sponsor meetings on a regular basis and an annual convention that provides additional training opportunities. The local meetings provide the chance for face-to-face interactions with others that have interest in computer crime.

A unique partnership of public and private sectors is embodied in the NYECTF. A succinct description of the organization is found in a pamphlet published by and about the organization:

> The New York Electronic Crimes Task Force (NYECTF) represents a confederation of law enforcement agencies, public prosecutors, academia and private industry institutions in a strategic alliance to pool their core competencies to address electronic crimes. Its participants have very clear common goals…

The organization is headed by the New York office of the United States Secret Service (USSS), but membership is not geographically restricted. In fact, the membership is multinational in scope. The structure of the NYECTF allows the organization to take advantage of expertise wherever it can be found. It extends the activities beyond the more traditional law enforcement investigative activities to address the systemic issues underlying crimes. These activities include the development of educational and training programs for children and parents and facilitating research and development of tools and methodologies.

The results achieved by the NYECTF are impressive. In the period from January 1995 through July 2001, the NYECTF was responsible for 832 arrests (199 Federal, 633 State). In addition, they dealt with 2063 missing and exploited children issues, 3271 identity takeovers/subscription fraud issues, recovered 60 handguns/machine guns and 2 crossbows and seized 13.31 kilos of illegal drugs (heroin, crack cocaine or pot). There were 535 forensic examinations and 605 computers seized. Asset forfeiture (real property not included) totaled $7,026,625 with actual/potential fraud loss totaling $516,151,304.64.

While accomplishing all of the above, there were 252 presentations/demonstrations, 8,007 instances of assistance to outside agencies, and electronic crimes training for 11.978 people. Significant and major cases handled by the NYECTF include the first investigation into computer and satellite intercepts and eavesdropping of law enforcement Mobile Data Terminals (1998), the indictment of organized crime figure John Gotti Jr. (1999), the first hacker arrest on Wall Street (2000), a telecommunications hacker case that threatened the complete 911 emergency system as well as the communications for a large portion of the United States (2001) and a CEO identity take-over case targeting individuals listed in the Forbes listing of the *Richest People in America* (2001). These statistics were reported in the same pamphlet referenced above.

Despite all of the above accomplishments, the NYECTF considers its greatest achievement to be government and private sector partnerships – the cornerstone and trademark of the New York Electronic Crimes Task Force. The partnership benefits the NYECTF because it surrounds itself with some of the best people in technology, which usually means joining forces with the private sector. Members of the private sectors also assist law enforcement in cultivating information and in seeing the "bigger picture" in criminal behavior. The private sector benefits from better intelligence, information about countermeasures, and working relationships with law enforcement.

Organizations such as the three that have been reviewed here provide invaluable resources in a number of areas—the opportunity for personal networking being one of the primary areas. Sponsored training opportunities abound in the three that were reviewed here. Each provides a possible forum for a seminar (formal or informal) on techniques in evidence collection and chain of custody issues.

Evidence collection

Another recommendation from the SANS **Incident Handling** document is to become familiar with evidence collection techniques and chain of custody issues. An excellent treatment introduction to this topic is available in the SANS Institute Information Security Reading Room in an article by Franklin Witter on *Legal Aspects of Collecting and Preserving Computer Forensic Evidence.* A chain of custody shows how evidence was collected, analyzed and preserved so that it can be presented in a court or at another hearing procedure. Since electronic evidence can be easily altered, a clear chain of custody is necessary to demonstrate that the evidence is trustworthy.

The first (and best) rule offered by Mr. Witter should always be kept in mind when dealing with computer incidents is this**: do not rush**. Otherwise, mistakes will be made and evidence will be lost. Information should be recorded in an evidence collection notebook reserved for this incident alone. The best kind is bound (so that pages cannot be removed without someone noticing) and with pre-numbered pages. The information must be as detailed as possible. Examples of the kinds of information that should be kept are:

- who first reported the incident, when was it reported, and what were the surrounding circumstances
- names of all investigators
- reasons for the investigation
- all computer equipment that is a target of the investigation, including hardware specifications, any inventory tracking numbers, operating system and patch levels and installed application software
- names of systems administrators responsible for maintenance of the system
- a detailed listing of the procedure used in collecting and analyzing the data and the result of the analysis
- a list of all who had access to the collected evidence

Evidence should be transported to the forensic lab or to secure safekeeping under the control of two people. Control of access to the evidence is vital. If it can be shown that unauthorized persons have had access, the evidence may not be admissible to the court or hearing.

The SANS **Incident Handling** document further cautions (page 35)

> Just be sure that you take notes that you would be proud to see displayed in a courtroom six months later. That means never doodle or write sarcastic remarks in your notebook!

Similar advice should be kept in mind if audio or video equipment is used to record information.

Mr. Witter emphasizes that planning and documented procedures are an important aspect of

evidence handling procedures. He recommends practicing evidence recovery techniques on test systems in advance of critical incidents, following the procedures in place. This encourages familiarity with the procedures as well as giving an opportunity for review and revision. He notes that the plan needs to be developed along with the advise of legal counsel and will benefit from input by law enforcement. The importance of working with your legal counsel cannot be stressed too often.

Conclusion

The overarching concept to remember is that planning and preparation are fundamentally important to the handling of computer related crimes and to partnering successfully with law enforcement. To review the major aspects of working with law enforcement agencies:

- Know the types of cases law enforcement will be interested in
- Contact local law enforcement before there is an incident
- Arrange for a briefing on evidence collection
- Work closely with your legal counsel

References

American Law Sources On-Line. LawSource.com. URL: http://www.lawsource.com/also/ (11 Aug. 2001).

Computer Crime and Intellectual Property Section (CCIPS), United States Department of Justice. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." Jan. 2001 URL: http://www.usdoj.gov/criminal/cybercrime/searchmanual.html (11 August 2001).

Computer Security Incident Handling Step by Step: A Survival Guide for Computer Security Incident Handling. [Bethesda, MD]: SANS Institute, 1998.

Department of Justice. "Federal Code Related to Cybercrime." Department of Justice, Computer Crime and Intellectual Property Section (CCIPS). September 25, 2000. URL: http://www.usdoj.gov/criminal/cybercrime/fedcode.htm (11 August 2001).

High Tech Crime Consortium. High Tech Crime Consortium Home Page. URL: http://www.hightechcrimecops.org/ (8 August 2001).

High Technology Crime Investigation Association. High Technology Crime Investigation Association International Home Page. 21 July 2001 URL: http://www.htcia.org/index.html (11 August 2001).

National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First

Responders. July, 2001. URL: http://www.ojp.usdoj.gov/nij/pubs.htm (11 August 2001).

New York Electronic Crimes Task Force. Some things are worth defending...Your Country is One of Them. [New York], [2001].

Radcliff, Deborah. "Cyber-Mod Squad Sets Out After Crackers." Computerworld 19 June 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO45927,00.html (8 August 2001).

Staggs, Jimmy. "Computer Security and the Law." 1 Dec. 2000 URL: http://www.sans.org/infosecFAQ/legal/law.htm (8 August 2001).

Witter, Franklin. "Legal Aspects of Collecting and Preserving Computer Forensic Evidence." 10 Apr. 2001 URL: http://www.sans.org/inforsecGAW/incident/evidence.htm (8 August 2001).