

## DATA SECURITY MANAGEMENT

# COMPUTER CRIME INVESTIGATION AND COMPUTER FORENSICS

Thomas Welch

## INSIDE

Computer Crime Defined, Rules of Evidence, Conducting Investigations, Surveillance,  
Legal Proceedings, Forensics

Incidents of computer-related crime and telecommunications fraud have increased dramatically over the past decade. However, because of the esoteric nature of this crime, there have been very few prosecutions and even fewer convictions. The new technology that has allowed for the advancement and automation of many business processes has also opened the door to many new forms of computer abuse. Although some of these system attacks merely use contemporary methods to commit older, more familiar types of crime, others involve the use of completely new forms of criminal activity that evolved along with the technology.

Computer crime investigation and computer forensics are also evolving sciences that are affected by many external factors, such as continued advancements in technology, societal issues, and legal issues. Many gray areas need to be sorted out and tested through the courts. Until then, the system attackers will have an advantage, and computer abuse will continue to increase. Computer security practitioners must be aware of the myriad technological and legal issues that affect systems and users, including issues dealing with investigations and enforcement.

**COMPUTER CRIME DEFINED**

According to the *American Heritage Dictionary*, a crime is any act committed or omitted in violation of the

**PAYOFF IDEA**

The move towards open, distributed systems has created many new ways in which information can be compromised. Data security managers need to be aware of the changing legal and technological issues as they relate to users, and the issues that misuse and crime can bring up. This article covers the areas of computer crime investigation and computer forensics, providing the data security professional with an overview of the legal issues involved, and the tools available to analyze and substantiate computer crime.

---

law. This definition causes a perplexing problem for law enforcement when dealing with computer-related crime, because much of today's computer-related crime is without violation of any formal law. This may seem to be a contradictory statement, but traditional criminal statutes in most states have only been modified over the years to reflect the theories of modern criminal justice. These laws generally envision applications to situations involving traditional types of criminal activity, such as burglary, larceny, and fraud. Unfortunately, the modern criminal has kept pace with the vast advancements in technology and has found ways to apply such innovations as the computer to his criminal ventures. Unknowingly and probably unintentionally, he or she has also revealed the difficulties in applying older traditional laws to situations involving computer-related crimes.

In 1979, the Department of Justice established a definition for computer crime, stating that a computer crime is any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution. This definition was too broad and has since been further refined by new or modified state and federal criminal statutes.

### **Criminal Law**

Criminal law identifies a crime as being a wrong against society. Even if an individual is victimized, under the law society is the victim. A conviction under criminal law normally results in a jail term or probation for the defendant. It could also result in a financial award to the victim as restitution for the crime. The main purpose of prosecuting under criminal law is punishment for the offender. This punishment is also meant to serve as a deterrent against future crime. The deterrent aspect of punishment only works if the punishment is severe enough to discourage further criminal activity. This is certainly not the case in the U.S., where very few computer criminals ever go to jail. In other areas of the world, very strong deterrents exist. For example, in China in 1995, a computer hacker was executed after being found guilty of embezzling \$200,000 from a national bank. This certainly will have a dissuading value for other hackers in China.

To be found guilty of a criminal offense under criminal law the jury must believe, beyond a reasonable doubt, that the offender is guilty of the offense. The lack of technical expertise, combined with the many confusing questions posed by the defense attorney, may cause doubt for many jury members, thus rendering a not guilty decision. The only short-term solution to this problem is to provide simple testimony in laymen's terms and to use demonstrative evidence whenever possible. Even with this, it will be difficult for many juries to return a guilty verdict.

Criminal conduct is broken down into two classifications depending on severity. A felony is the more serious of the two, normally resulting in a jail term of more than one year. Misdemeanors are normally punishable

---

---

by a fine or a jail sentence of less than a year. It is important to understand that to deter future attacks, stricter sentencing must be sought, which only occurs under the felonious classification. The type of attack or the total dollar loss has a direct relationship to the crime classification.

Criminal law falls under two main jurisdictions: federal and state. Although there is a plethora of federal and state statutes that may be used against traditional criminal offenses, and even though many of these same statutes may be applied to computer-related crimes with some measure of success, it is clear that many cases fail to reach prosecution or fail to result in conviction because of the gaps that exist in the federal criminal code and the individual state criminal statutes.

Because of this, almost every state, along with the federal government, have adopted new laws specific to computer-related abuses. These new laws, which have been redefined over the years to keep abreast of the constant changes in the technological forum, have been subjected to an ample amount of scrutiny due to many social issues that have been affected by the proliferation of computers in society. Some of these issues, such as privacy, copyright infringement, and software ownership, are yet to be resolved. More changes to the current collection of laws can be expected. Some of the computer-related crimes that are addressed by the new state and federal laws are:

- Unauthorized access.
- Exceed authorized access.
- Intellectual property theft or misuse of information.
- Pornography.
- Theft of services.
- Forgery.
- Property theft (e.g., computer hardware and chips).
- Invasion of privacy.
- Denial of services.
- Computer fraud.
- Viruses.
- Sabotage (i.e., data alteration or malicious destruction).
- Extortion.
- Embezzlement.
- Espionage.
- Terrorism.

All but one state, Vermont, have created or amended laws specifically to deal with computer-related crime; 25 states have enacted specific computer crime statutes, and the other 24 states have merely amended their traditional criminal statutes to confront computer crime issues. Vermont has announced legislation under Bill H.0555 that deals with the theft of

---

---

computer services. The elements of proof, which define the basis of the criminal activity, vary from state to state. Security practitioners should be fully cognizant of their state laws, specifically the elements of proof. In addition, traditional criminal statutes, such as theft, fraud, extortion, and embezzlement, can still be used to prosecute computer crime.

Just as there has been abundant new legislation at the state level, there have also been many new federal policies, such as the *Electronic Communications Privacy Act* and the *Computer Fraud and Abuse Act* of 1986. They have been established to deal precisely with computer and telecommunications abuses at the federal level. Moreover, many modifications and updates have been made to the Federal Criminal Code, Section 1030, to deal with a variety of computer-related abuses. Even though these new laws have been adopted for use in the prosecution of a computer-related offense, some of the older, proven federal laws discussed later in this article offer a simpler case to present to judges and juries:

- Wire fraud.
- Mail fraud.
- Interstate transportation of stolen property.
- Racketeer influenced and corrupt organizations (RICO)

#### **Civil Law**

Civil law (or tort law) identifies a tort as a wrong against an individual or business which normally results in damage or loss to that individual or business. The major differences between criminal and civil law is the type of punishment and the level of proof required to obtain a guilty verdict. There is no jail sentence under the civil law system. Victims may receive financial or injunctive relief as restitution for their loss. An injunction against the offender will attempt to thwart any further loss to the victim. In addition, a violation of the injunction may result in a contempt of court order, which places the offender in jeopardy of going to jail. The main purpose of seeking civil remedy is for financial restitution, which can be awarded as follows:

- Compensatory damages.
- Punitive damages.
- Statutory damages.

In a civil action, if there is no culpability on the part of the victim, the victim may be entitled to compensatory (i.e., restitution) and punitive damages. Compensatory damages are actual damages to the victim and include attorney fees, lost profits, and investigation costs. Punitive damages are damages set by the jury with the intent to punish the offender. Even if the victim is partially culpable, an award may be made on the vic-

---

---

tims behalf, but may be lessened due to the victim's culpable negligence. Statutory damages are damages determined by law. Mere violation of the law entitles the victim to a statutory award.

Civil cases are much easier to convict under because the burden of proof required for the conviction is much less. To be found guilty of a civil wrong, the jury must believe, based only on the preponderance of the evidence, that the offender is guilty of the offense. It is much easier to show that the majority (i.e., 51%) of the evidence is pointing to the defendant's guilt.

Finally, just as a search warrant is used by law enforcement as a tool in the criminal investigation, the court can issue an impoundment order, which is a court order to take back the property in question. The investigator should also keep in mind that the criminal and civil case can take place simultaneously, thus allowing items seized during the execution of the search warrant to be used in the civil case.

### **Insurance**

An insurance policy is generally part of an organization's overall risk mitigation or management plan. The policy transfers the risk of loss to the insurance company in return for an acceptable level of loss (i.e., the insurance premium). Because many computer-related assets (i.e., software and hardware) account for the majority of an organization's net worth, they must be protected by insurance. If there is a loss to any of these assets, the insurance company is usually required to pay out on the policy. An important factor is the principle of culpable negligence. This places part of the liability on the victim if the victim fails to follow "a standard of due care" in the protection of its assets. If a victim organization is held to be culpably negligent, the insurance company may be required to pay only a portion of the loss.

### **RULES OF EVIDENCE**

Before delving into the investigative process and computer forensics, it is essential that the investigator have a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceeding generally amounts to a significant challenge, but when computers are involved, the problems are intensified. Special knowledge is needed to locate and collect evidence and special care is required to preserve and transport the evidence. Evidence in a computer crime case may differ from traditional forms of evidence inasmuch as most computer-related evidence is intangible — in the form of an electronic pulse or magnetic charge.

Before evidence can be presented in a case, it must be competent, relevant, and material to the issue, and it must be presented in compliance

---

---

with the rules of evidence. Anything that tends to prove directly or indirectly that a person may be responsible for the commission of a criminal offense may be legally presented against him. Proof may include the oral testimony of witnesses or the introduction of physical or documentary evidence.

By definition, evidence is any species of proof or probative matter, legally presented at the trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, and objects for the purpose of inducing belief in the minds of the court and jurors as to their contention. In short, evidence is anything offered in court to prove the truth or falsity of a fact in issue. This section describes each of the Rules of Evidence as it relates to computer crime investigations.

### **Types of Evidence**

Many types of evidence exist that can be offered in court to prove the truth or falsity of a given fact. The most common forms of evidence are direct, real, documentary, and demonstrative. Direct evidence is oral testimony, whereby the knowledge is obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue. Direct evidence is called to prove a specific act (e.g., an eyewitness statement).

Real evidence, also known as associative or physical evidence, is made up of tangible objects that prove or disprove guilt.

Physical evidence includes such things as tools used in the crime, fruits of the crime, or perishable evidence capable of reproduction. The purpose of the physical evidence is to link the suspect to the scene of the crime. It is the evidence that has material existence and can be presented to the view of the court and jury for consideration.

Documentary evidence is evidence presented to the court in the form of business records, manuals, and printouts, for example. Much of the evidence submitted in a computer crime case is documentary evidence.

Finally, demonstrative evidence is evidence used to aid the jury. It may be in the form of a model, experiment, chart, or an illustration offered as proof.

When seizing evidence from a computer-related crime, the investigator should collect any and all physical evidence, such as the computer, peripherals, notepads, or documentation, in addition to computer-generated evidence. Four types of computer-generated evidence are

- Visual output on the monitor.
  - Printed evidence on a printer.
  - Printed evidence on a plotter.
  - Film recorder (i.e., a magnetic representation on disk and optical representation on CD).
-

---

A legal factor of computer-generated evidence is that it is considered hearsay. The magnetic charge of the disk or the electronic bit value in memory, which represents the data, is the actual, original evidence. The computer-generated evidence is merely a representation of the original evidence; but in *Rosenberg v. Collins*, the court held that if the computer output is used in the regular course of business, the evidence shall be admitted.

#### **Best Evidence Rule**

The best evidence rule, which had been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.

#### **Exclusionary Rule**

Evidence must be gathered by law enforcement in accordance with court guidelines governing search and seizure or it will be excluded as set in the Fourth Amendment. Any evidence collected in violation of the Fourth Amendment is considered to be "Fruit of the Poisonous Tree," and will not be admissible. Furthermore, any evidence identified and gathered as a result of the initial inadmissible evidence will also be held to be inadmissible. Evidence may also be excluded for other reasons, such as violations of the *Electronic Communications Privacy Act* (ECPA) or violations related to provisions of Chapters 2500 and 2700 of Title 18 of the *United States Penal Code*.

Private citizens are not subject to the Fourth Amendment's guidelines on search and seizure, but are exposed to potential exclusions for violations of the ECPA or *Privacy Act*. Therefore, internal investigators, private investigators, and CERT team members should take caution when conducting any internal search, even on company computers. For example, if there is no policy explicitly stating the company's right to electronically monitor network traffic on company systems, internal investigators

---

---

would be well advised not to set up a sniffer on the network to monitor such traffic. To do so may be a violation of the ECPA.

### **Hearsay Rule**

Hearsay is secondhand evidence: evidence that is not gathered from the personal knowledge of the witness but from another source. Its value depends on the veracity and competence of the source. Under the federal Rules of Evidence, all business records, including computer records, are considered hearsay, because there is no firsthand proof that they are accurate, reliable, and trustworthy. In general, hearsay evidence is not admissible in court. However, there are some well-established exceptions (e.g., Rule 803) to the hearsay rule for business records.

### **Business Record Exemption to the Hearsay Rule**

*Federal Rules of Evidence* 803(6) allow a court to admit a report or other business document made at or near the time by or from information transmitted by a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the [report or document], all as shown by testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

To meet Rule 803(6) the witness must:

- Have custody of the records in question on a regular basis.
- Rely on those records in the regular course of business.
- Know that they were prepared in the regular course of business.

Audit trails meet the criteria if they are produced in the normal course of business. The process to produce the output will have to be proven to be reliable. If computer-generated evidence is used and admissible, the court may order disclosure of the details of the computer, logs, and maintenance records in respect to the system generating the printout, and then the defense may use that material to attack the reliability of the evidence. If the audit trails are not used or reviewed — at least the exceptions (e.g., failed log-on attempts) — in the regular course of business, they do not meet the criteria for admissibility.

*Federal Rules of Evidence* 1001(3) provide another exception to the hearsay rule. This rule allows a memory or disk dump to be admitted as evidence, even though it is not done in the regular course of business. This dump merely acts as statement of fact. System dumps (in binary or hexadecimal) are not hearsay because they are not being offered to prove the truth of the contents, but only the state of the computer.

---



---

### **Chain of Evidence: Custody**

Once evidence is seized, the next step is provide for its accountability and protection. The chain of evidence, which provides a means of accountability, must be adhered to by law enforcement when conducting any type of criminal investigation, including a computer crime investigation. It helps to minimize the instances of tampering. The chain of evidence must account for all persons who handled or who had access to the evidence in question.

The chain of evidence shows:

- Who obtained the evidence.
- Who secured the evidence.
- Who had control or possession of the evidence.

It may be necessary to have anyone associated with the evidence testify at trial. Private citizens are not required to maintain the same level of control of the evidence as law enforcement, although they are well advised to do so. Should an internal investigation result in the discovery and collection of computer-related evidence, the investigation team should follow the same, detailed chain of evidence as required by law enforcement. This will help to dispel any objection by the defense that the evidence is unreliable, should the case go to court.

### **Admissibility of Evidence**

The admissibility of computer-generated evidence is, at best, a moving target. Computer-generated evidence is always suspect, because the ease of which it can be tampered with, usually without a trace. Precautionary measures must be taken to ensure that computer-generated evidence has not been tampered with, erased, or added to. To ensure that only relevant and reliable evidence is entered into the proceedings, the judicial system has adopted the concept of admissibility:

- *Relevancy of evidence*: evidence tending to prove or disprove a material fact. All evidence in court must be relevant and material to the case.
- *Reliability of evidence*: the evidence and the process to produce the evidence must be proven to be reliable. This is one of the most critical aspects of computer-generated evidence.

Once computer-generated evidence meets the business record exemption to the hearsay rule, is not excluded for some technicality or violation and follows the chain of custody, it is held to be admissible. The defense will attack both the relevancy and reliability of the evidence, so that great care should be taken to protect both.

---

---

### **Evidence Life Cycle**

The evidence life cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:

- Collection and identification.
- Storage, preservation, and transportation.
- Presented in court.
- Returned to the victim (i.e., the owner).

**Collection and Identification.** As the evidence is obtained or collected, it must be properly marked so that it can be identified as being that particular piece of evidence gathered at the scene. The collection must be recorded in a log book identifying that particular piece of evidence, the person who discovered it, and the date, time, and location discovered. The location should be specific enough for later recollection in court. When marking evidence, these guidelines should be followed:

- The actual piece of evidence should be marked if it will not damage the evidence by writing or scribing initials, the date, and the case number if known. This evidence should be sealed in an appropriate container, then the container should be marked by writing or scribing initials, the date, and the case number, if known.
- If the actual piece of evidence cannot be marked, the evidence should be sealed in an appropriate container and then that container marked by writing or scribing initials, the date, and the case number, if known.
- The container should be sealed with evidence tape and the marking should write over the tape, so that if the seal is broken it can be noticed.

When marking glass or metal, a diamond scribe should be used. For all other objects, a felt-tip pen with indelible ink is recommended. Depending on the nature of the crime, the investigator may wish to preserve latent fingerprints. If so, static-free nitrile gloves should be used if working with computer components, instead of standard latex gloves.

**Storage, Preservation, and Transportation.** All evidence must be packed and preserved to prevent contamination. It should be protected against heat, extreme cold, humidity, water, magnetic fields, and vibration. The evidence must be protected for future use in court and for return to the original owner. If the evidence is not properly protected, the person or agency responsible for the collection and storage of the evidence may be held liable for damages. Therefore, the proper packing materials should be used whenever possible.

---

---

Documents and disks (e.g., hard, floppy, and optical) should be seized and stored in appropriate containers to prevent their destruction. For example, hard disks should be packed in a static-free bag within a cardboard box with a foam container. It may be best to rely on the system administrator or a technical advisor on how to best protect a particular type of system, especially mini-systems or mainframes.

Finally, evidence should be transported to a location where it can be stored and locked. Sometimes, the systems are too large to transport, thus the forensic examination of the system may need to take place on site.

**Evidence Presented in Court.** Each piece of evidence that is used to prove or disprove a material fact must be presented in court. After the initial seizure, the evidence is stored until needed for trial. Each time the evidence is transported to and from the courthouse for the trial, it must be handled with the same care as with the original seizure. In addition, the chain of custody must continue to be followed. This process will continue until all testimony related to the evidence is completed. Once the trial is over, the evidence can be returned to the victim (i.e., owner).

**Evidence Returned to Victim.** The final destination of most types of evidence is back with its original owner. Some types of evidence, such as drugs or paraphernalia are destroyed after the trial. Any evidence gathered during a search, even though maintained by law enforcement, is legally under the control of the courts. Even though a seized item may be the victim's and may even have the victim's name on it, it may not be returned to the victim unless the suspect signs a release, or after a hearing by the court. However, many victims do not want to go to trial. They just want to get their property back.

Many investigations merely need the information on a disk to prove or disprove a fact in question, thus there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying. Mirror copies of the suspect disk are obtained by using forensic software and then one of those copies can be returned to the victim so that he or she can resume business operations.

## **CONDUCTING COMPUTER CRIME INVESTIGATION**

The computer crime investigation should start immediately following the report of any alleged criminal activity. Many processes ranging from reporting and containment to analysis and eradication should be accomplished as soon as possible after the attack. An incident response plan should be formulated, and a Computer Emergency Response Team (CERT) should be organized before the attack. The incident response

---

---

plan will help set the objective of the investigation and will identify each of the steps in the investigative process.

The use of a corporate CERT is invaluable. Due to the numerous complexities of any computer-related crime, it is extremely advantageous to have a single group that is acutely familiar with the incident response plan to call upon. The CERT team should be a technically astute group, knowledgeable in the area of legal investigations, the corporate security policy (especially the incident response plan), the severity levels of various attacks, and the company position on information dissemination and disclosure.

The incident response plan should be part of the overall corporate computer security policy. The plan should identify reporting requirements, severity levels, and guidelines to protect the crime scene and preserve evidence. The priorities of the investigation will vary from organization to organization, but the issues of containment and eradication are reasonably standard, which is to minimize any additional loss and resume business as quickly as possible.

#### **Detection and Containment**

Before any investigation can take place, the system intrusion or abusive conduct must first be detected. The closer the detection is to the actual intrusion not only helps to minimize system damage, but also assists in the identification of potential suspects.

To date, most computer crimes have either been detected by accident or through the laborious review of lengthy audit trails. Although audit trails can assist in providing user accountability, their detection value is somewhat diminished because of the amount of information that must be reviewed and because these reviews are always postincident. Accidental detection is usually made through the observation of increased resource utilization or inspection of suspicious activity. However, this is not effective due to the sporadic nature of this type of detection.

These types of reactive or passive detection schemes are no longer acceptable. Proactive and automated detection techniques must be instituted to minimize the amount of system damage in the wake of an attack. Real-time intrusion monitoring can help in the identification and apprehension of potential suspects, and automated filtering techniques can be used to make audit data more useful.

Once an incident is detected, it is essential to minimize the risk of any further loss. This may mean shutting down the system and reloading clean copies of the operating system and application programs. However, failure to contain a known situation (i.e., a system penetration) may result in increased liability for the victim organization. For example, if a company's system has been compromised by an external attacker and the company failed to shut down the intruder, hoping to trace him or

---

---

her, the company may be held liable for any additional harm caused by the attacker.

### **Report to Management**

All incidents should be reported to management as soon as possible. Prompt internal reporting is imperative to collect and preserve potential evidence. It is important that information about the investigation be limited to as few people as possible. Information should be given on a need-to-know basis, which limits the possibility of the investigation being leaked. In addition, all communications related to the incident should be made through an out-of-band method to ensure that the intruder does not intercept any incident-related information. In other words, E-mail should not be used to discuss the investigation on a compromised system. Based on the type of crime and type of organization it may be necessary to notify:

- Executive management.
- The information security department.
- The physical security department.
- The internal audit department.
- The legal department.

### **The Preliminary Investigation**

A preliminary internal investigation is necessary for all intrusions or attempted intrusions. At a minimum, the investigator must ascertain if a crime has occurred; and if so, he or she must identify the nature and extent of the abuse. It is important for the investigator to remember that the alleged attack or intrusion may not be a crime. Even if it appears to be some form of criminal conduct, it could merely be an honest mistake. There is no quicker way to initiate a lawsuit than to mistakenly accuse an innocent person of criminal activity.

The preliminary investigation usually involves a review of the initial complaint, inspection of the alleged damage or abuse, witness interviews, and, finally, examination of the system logs. If during the preliminary investigation, it is determined that some alleged criminal activity has occurred, the investigator must address the basic elements of the crime to determine the chances of successfully prosecuting a suspect either civilly or criminally. Further, the investigator must identify the requirements of the investigation (i.e., the dollars and resources). If it is believed that a crime has been committed, neither the investigator nor any other company employees should confront or talk with the suspect. Doing so would only give the suspect the opportunity to hide or destroy evidence.

---

---

### **Determine if Disclosure Is Required**

Determine if a disclosure is required or warranted due to laws or regulations. Disclosure may be required by law or regulation or may be required if the loss affects the corporation's financial statement. Even if disclosure is not required, it is sometimes better to disclose the attack to possibly deter future attacks. This is especially true if the victim organization prosecutes criminally or civilly. Some of these attacks would probably result in disclosure:

- A large financial loss by a public company.
- A bank fraud.
- An attack on a public safety systems (e.g., air traffic control).

The Federal Sentencing Guidelines also require organizations to report criminal conduct. The stated goals of the commission were "to provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct." The guidelines also state that organizations have a responsibility to "maintain internal mechanism for preventing, detecting, and reporting criminal conduct." The Federal Sentencing Guidelines do not prevent an organization from conducting preliminary investigations to ascertain if, in fact, a crime has been committed.

### **Investigation Considerations**

Once the preliminary investigation is complete and the victim organization has made a decision related to disclosure, the organization must decide on the next course of action. The victim organization may decide to do nothing, or it may attempt to eliminate the problem and just move on. Deciding to do nothing is not a very effective course of action, because the organization may be held culpably negligent should another attack or intrusion occur. The victim organization should at least attempt to eliminate the security hole that allowed the breach, even if it does not plan to bring the case to court. If the attack is internal, the organization may wish to conduct an investigation that might only result in the dismissal of the subject. If it decides to further investigate the incident, the organization must also determine if it is going to prosecute criminally or civilly, or merely conduct an investigation for insurance purposes. If an insurance claim is to be submitted, a police report is usually necessary.

When making the decision to prosecute a case, the victim must clearly understand the overall objective. If the victim is looking to make a point by punishing the attacker, a criminal action is warranted. This is one way in which to deter potential future attacks. If the victim is seeking financial restitution or injunctive relief, a civil action is appropriate. Keep in mind

---

---

that a civil trial and criminal trial can happen concurrently. Information obtained during the criminal trial can be used as part of the civil trial.

The key is for the victim organization to know what it wants to do at the outset, so all activity can be coordinated. The evidence, or lack thereof, may also hinder the decision to prosecute. Evidence is a significant problem in any legal proceeding, but the problems are compounded when computers are involved. Special knowledge is needed to locate and collect the evidence, and special care is required to preserve the evidence.

There are many factors to consider when deciding on whether to further investigate an alleged computer crime. For many organizations, the primary consideration is the cost associated with an investigation. The next consideration is probably the effect on operations or the effect on business reputation. The victim organization must answer these questions:

- Will productivity be stifled by the inquiry process?
- Will the compromised system have to be shut down to conduct an examination of the evidence or crime scene?
- Will any of the system components be held as evidence?
- Will proprietary data be subject to disclosure?
- Will there be any increased exposure for failing to meet a “standard of due care”?
- Will there be any potential adverse publicity related to the loss?
- Will a disclosure invite other perpetrators to commit similar acts, or will an investigation and subsequent prosecution deter future attacks?

The answers to these questions may have an effect on who is called in to conduct the investigation. Furthermore, these objectives must be addressed early on, so that the proper authorities can be notified if required. Prosecuting an alleged criminal offense is a time-consuming task. Law enforcement and the prosecutor expect a commitment of time and resources for:

- Interviews to prepare crime reports and search warrant affidavits.
  - Engineers or computer programmers to accompany law enforcement on search warrants.
  - Assistance of the victim company to identify and describe documents, source code, and other found evidence.
  - A company expert who may be needed for explanations and assistance during the trial.
  - Documents which may need to be provided to the defendant’s attorney for discovery. They may ask for more than the organization may want to provide. The plaintiff’s (i.e., victim’s organization) attorney
-

---

will have to argue against broad-ranging discovery. Defendants are entitled to seek evidence that they need for their defense.

- Company employees will more than likely be subpoenaed to testify.

### **Who Should Conduct the Investigation?**

Based on the type of investigation (i.e., civil, criminal, or insurance) and extent of the abuse, the victim must decide who is to conduct the investigation. This used to be a straightforward decision, but high-technology crime has altered the decision-making process. Inadequate and untested laws, combined with the lack of technical training and technical understanding, has severely hampered the effectiveness of the criminal justice system when dealing with computer-related crimes.

In the past, society would adapt to change, usually at the same rate of that change. Today, this is no longer true. The information age has ushered in dramatic technological changes and achievements, which continue to evolve at exponential rates. The creation, the computer, is being used to create new technologies or advance existing ones. This cycle means that changes in technology will continue to occur at an increasing pace. What effect does this have on the system of law? How new laws will be established must be examined. The process must be adapted to account for the excessive rate of change. While this is taking place, if an investigation is launched, the victim must choose from these options:

- Conduct an internal investigation.
- Bring in external private consultants or investigators.
- Bring in local, state, or federal law enforcement officials.

**Exhibit 1** identifies each of these tradeoffs. Law enforcement officers have greater search and investigative capabilities than private individuals, but they also have more restrictions than private citizens. For law enforcement to conduct a search, a warrant must first be issued. Issuance of the search warrant is based on probable cause (i.e., reason to believe the something is true). Once probable cause has been identified, law enforcement officers have the ability to execute search warrants, subpoenas, and wire taps. The warrant process was formed to protect the rights of the people. The Fourth Amendment established:

*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

There are certain exceptions to this. The “exigent circumstances” doctrine allows for a warrantless seizure, by law enforcement, when the de-

---



**EXHIBIT 1 — Tradeoffs for Each Group Conducting an Investigation**

Group	Cost	Legal Issues	Information Dissemination	Investigative Control
Internal Investigators	Time/People Resources	Privacy Issues		
		Limited Knowledge of Law and Forensics	Controlled	Complete
Private Consultants	Direct Expenditure	Privacy Issues	Controlled	Complete
Law Enforcement Officers	Time/People Resources	Fourth Amendment Issues		
		Jurisdiction	Uncontrolled Public Information (FOIA)	None
		Miranda Privacy Issues		

struction of evidence is impending. In *United States v. David* the court held that “When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity.”

Internal investigators (i.e., nongovernment) or private investigators, acting as private citizens, have much more latitude in conducting a warrantless search, due to a ruling by the Supreme Court in *Burdeau v. McDowell*. In this case, the Court held that evidence obtained in a warrantless search could be presented to a grand jury by a government prosecutor, because there was no unconstitutional government search and hence no violation of the Fourth Amendment.

Normally, a private party or citizen is not subject to the rules or laws governing search and seizure, but a private citizen becomes a police agent, and the Fourth Amendment applies, when:

- The private party performs a search for which the government would need a search warrant to conduct.
- The private party performs that search to assist the government, as opposed to furthering its own interest.
- The government is aware of that party’s conduct and does not object to it.

The purpose of this doctrine is to eliminate the opportunity for government to circumvent the warrant process by eliciting the help of a private citizen. If a situation required law enforcement to obtain a warrant, due to the subject’s expectations of privacy, and the government knowingly allowed a private party to conduct a search to disclose evidence, the court would probably rule that the private citizen acted as a police agent.

---

A victim acting to protect his or her property by assisting police to prevent or detect a crime does not become a police agent.

The largest issues affecting the decision on what to bring in (in order of priority) are information dissemination, investigative control, cost, and the associated legal issues. Once an incident is reported to law enforcement, information dissemination becomes uncontrolled. The same holds true for investigative control. Law enforcement controls the entire investigation, from beginning to end. This does not always have a negative effect, but the victim organization may have a different set of priorities.

Cost is always a concern, and the investigation costs only add to the loss initially sustained by the attack or abuse. Even law enforcement agencies, which are normally considered “free,” add to the costs because of the technical assistance that they require during the investigation.

Another area that affects law enforcement is jurisdiction. Jurisdiction is the geographic area where the crime had been committed and any portion of the surrounding area over or through which the suspect passed, en route to or going away from the actual scene of the crime. Any portion of this area adjacent to the actual scene over which the suspect, or the victim, might have passed, and where evidence might be found, is considered part of the crime scene. When a system is attacked remotely, where did the crime occur? Most courts submit that the crime scene is the victim’s location. What about “en route to”? Does this suggest that the crime scene also encompasses the telecommunication’s path used by the attacker? If so, and a theft occurred, is this interstate transport of stolen goods? There seem to be more questions than answers, but only through cases being presented in court can a precedence be set.

There are advantages and disadvantages for each of these groups previously identified. Internal investigators will know the victim’s systems the best, but may lack some of the legal and forensic training. Private investigators who specialize in high-technology crime also have a number of advantages, but usually result in higher costs. Private security practitioners and private investigators are also private businesses and may be more sensitive to business resumption than law enforcement.

If the victim organization decides to contact the local police department, the detective unit should be called directly. If 911 is called, a uniformed officer will arrive and possibly alert the attacker. Furthermore, the officer must create a report of the incident that will become part of a public log. Now, the chances for a discretionary dissemination of information and a covert investigation are gone. The victim organization should ask the detective to meet with it in plainclothes. When they arrive at the workplace, they should be announced as consultants. If it is appropriate for federal authorities to be present, the victim organization should inform the local authorities. Be aware that a local law enforcement agency may not be well equipped to handle high-tech crime. The majority of

---

---

law enforcement agencies have limited budgets and place an emphasis on problems related to violent crime and drugs. Moreover, with technology changing so rapidly, most law enforcement officers lack the technical training to adequately investigate an alleged intrusion.

The same problems hold true for the prosecution and the judiciary. To prosecute a case successfully, both the prosecutor and the judge must have a reasonable understanding of high-technology laws and the crime in question, which is not always the case. Moreover, many of the current laws are woefully inadequate. Even though an action may be morally and ethically wrong, it is still possible that no law is violated (e.g., the *LaMacchia* case). Even when there is a law that has been violated, many of these laws remain untested and lack precedence. Because of this, many prosecutors are reluctant to prosecute high-technology crime cases.

Many recent judicial decisions have indicated that judges are lenient towards the techno-criminal just as they are with other white-collar criminals. Furthermore, the lack of technical expertise may cause “doubt,” thus rendering “not guilty” decisions. Because many of the laws concerning computer crime are new and untested, many judges have a concern with setting precedence that may later be overturned in an appeal. Some of the defenses that have been used, and accepted by the judiciary, are

- If an organization has no system security or lax system security, that organization is implying that no company concern exists. Thus, there should be no court concern.
- If a person is not informed that access is unauthorized, it can be used as a defense.
- If employees are not briefed and do not acknowledge understanding of policy and procedures, they can use it as a defense.

### **The Investigative Process**

As with any type of criminal investigation, the goal of the investigation is to know the who, what, when, where, why, and how. It is important that the investigator log all activity and account for all time spent on the investigation. The amount of time spent on the investigation has a direct effect on the total dollar loss for the incident, which may result in greater criminal charges and, possibly, stiffer sentencing. Finally, the money spent on investigative resources can be reimbursed as compensatory damages in a successful civil action.

Once the decision is made to further investigate the incident, the next course of action for the investigative team is to establish a detailed investigative plan, including the search and seizure plan. The plan should consist of an informal strategy that will be employed throughout the investigation, including the search and seizure:

---

- 
- Identify what type of system is to be seized.
  - Identify the search and seizure team members.
  - Determine if there is risk that the suspect will destroy evidence or cause greater losses.

**Identify the Type of System.** It is imperative to learn as much as possible about the target computer systems. If possible, the investigator should obtain the configuration of the system, including the network environment (if any), hardware, and software. The following questions should be answered before the seizure:

- Who are the system experts? They should be part of the team.
- Is a security system in place on the system? If so, what kind? Are passwords used? Can a root password be obtained?
- Where is the system located? Will simultaneous raids be required?
- What are the required media supplies to be obtained in advance of the operation?
- What law has been violated? Are there elements of proof? If yes, these should be the focus of the search and seizure.
- What is the probable cause? Is a warrant necessary?
- Will the analysis of the computer system be conducted on site, in the investigator's office, or in a forensics lab?

**Identify the Search and Seizure Team Members.** There are different rules for search and seizure based on who is conducting the search. Under the Fourth Amendment, law enforcement must obtain a warrant, which must be based on probable cause. In either case, a team should be identified and should consist of these members:

- The lead investigator.
- The information security department.
- The legal department.
- Technical assistance — the system administrator as long as he or she is not a suspect.

If a corporate CERT team is already organized, this process is already complete. A chain of command must be established, and who is to be in charge must be determined. This person is responsible for delegating assignments to each of the team members. A media liaison should be identified if the attack is to be disclosed, to control the flow of information to the media.

**Obtaining and Serving Search Warrants.** If it is believed that the suspect has crucial evidence at his or her home or office, a search war-

---

---

rant will be required to seize the evidence. If a search warrant is going to be needed, it should be done as quickly as possible before the intruder can do further damage. The investigator must establish that a crime has been committed and that the suspect is somehow involved in the criminal activity. He or she must also show why a search of the suspect's home or office is required. The victim may be asked to accompany law enforcement when serving the warrant to identify property or programs.

If it is necessary to take documents when serving the search warrant, they should be copied onto a colored paper to prevent the defense from inferring that what might have been found was left by the person serving the warrant.

**Is the System at Risk?** Before the execution of the plan, the investigative team should ascertain if the suspect, if known, is currently working on the system. If so, the team must be prepared to move swiftly, so that evidence is not destroyed. The investigator should determine if the computer is protected by any physical or logical access control systems and be prepared to respond to such systems. It should also be decided early, what will be done if the computer is on at the commencement of the seizure. The goal of this planning is to minimize any risk of evidence contamination or destruction.

### **Executing the Plan**

The first step in executing the plan is to secure the scene, which includes securing the power, network servers, and telecommunications links. If the suspect is near the system, it may be necessary to physically remove him or her. It may be best to execute the search and seizure after normal business hours to avoid any physical confrontation. Keep in mind that even if a search is conducted after hours, the suspect may still have remote access to the system through a LAN-based modem connection, PC-based modem connection, or Internet connection.

The area should be entered slowly so as not to disturb or destroy evidence. The entire situation should be evaluated. In no other type of investigation can evidence be destroyed more quickly. The keyboard should not be touched, because this action may invoke a Trojan horse or some other rogue or malicious program. The computer should not be turned off unless it appears to be active (i.e., formatting the disk, deleting files, or initiating some I/O process). The disk activity light should be looked at, as well as listening for disk usage. If the computer must be turned off, the wall plug should be pulled, rather than using the On/Off switch. Notes, documentation, passwords, and encryption codes should be looked for. The following questions must be answered to control the scene effectively:

---

- 
- Is the computer system turned on?
  - Is there a modem attached? If so,
    - Are there internal modems?
    - Are telephone lines connected to the computer?
  - Is the system connected to a LAN?

The investigator may wish to videotape the entire evidence collection process. There are two different opinions on this. The first is that if the search and seizure is videotaped, any mistakes can nullify the whole operation. The second opinion is that if the evidence collection process is videotaped, many of the claims by the defense can be silenced. In either case, investigators should be cautious about what is said if the audio is turned on.

The crime scene should be sketched and photographed before anything is touched. Sketches should be drawn to scale. Still photographs of critical pieces of evidence should be taken. At a minimum, the following should be captured:

- The layout of desks and computers.
- The configuration of the all computers on the network.
- The configuration of the suspect computer.
- The suspect computer's display.

If the computer is on, the investigator should capture what is on the monitor. This can be accomplished by videotaping what is on the screen. The best way to do this, without getting the "scrolling effect" caused by the video refresh, is to use an NTSC adapter. Every monitor has a specific refresh rate (i.e., horizontal: 30–66 KHz, vertical: 50–90 Hz) that identifies how frequently the screen's image is redrawn. It is this redrawing process that causes the videotaped image to appear as if the vertical hold is not properly adjusted. The NTSC adapter is connected between the monitor and monitor cable and directs the incoming signal into the camcorder directly. Still photos are a good idea, too. A flash should not be used, because it can "white out" the image. Even if the computer is off, the monitor should be checked for burnt-in images. This does not happen as much with the new monitors, but it may still help in the discovery of evidence.

Once the investigator has reviewed and captured what is on the screen, he or she should pull the plug on the system. This is for PC-based systems only. Minisystems or mainframes must be logically powered down. A forensic analysis (i.e., a technical system review with a legal basis focused on evidence gathering) should be conducted on a forensic system in a controlled environment. If necessary, a forensic analysis can be conducted on site, but never by using the suspect systems operating system or system utilities. The process that should be followed is discussed later in this chapter.

---

---

The investigator should identify, mark, and pack all evidence according to the collection process under the Rules of Evidence. He or she should also identify and label all computer systems, cables, documents, and disks. Then, he or she should also seize all diskettes, backup tapes, optical disks, and printouts, making an entry for each in the evidence log. The printer should be examined, and if it uses ribbons, at least the ribbon should be taken as evidence. The investigator should keep in mind that many of the peripheral devices may contain crucial evidence in their memory or buffers.

Some other items of evidence to consider are LAN servers and routers. The investigator must check with the manufacturer on how to output the memory buffers for each device, keeping in mind that most buffers are stored in volatile memory. Once the power is cut, the information may be lost. In addition, the investigator must examine all drawers, closets, and even the garbage for any forms of magnetic media (i.e., hard drives, floppy diskettes, tape cartridges, or optical disks) or documentation.

Moreover, it seems that many computer-literate individuals conduct most of their correspondence and work product on a computer. This is an excellent source of leads, but the investigator must take care to avoid an invasion of privacy. Even media that appears to be destroyed can turn out to be quite useful. For example, one criminal case involved an American serviceman who contracted to have his wife killed and wrote the letter on his computer. In an attempt to destroy all the evidence, he cut up the floppy disk containing the letter into 17 pieces. The Secret Service was able to reconstruct the diskette and read almost all the information.

The investigator should not overlook the obvious, especially hacker tools and any ill-gotten gains (i.e., password or credit card lists). These items help build a case when trying to show motive and opportunity. The State of California has equated hacker tools to that of burglary tools; the mere possession constitutes a crime. Possession of a Red Box, or any other telecommunications instrument that has been modified with the intent to defraud, is also prohibited under U.S.C. Section 1029.

Finally, phones, answering machines, desk calendars, day-timers, fax machines, pocket organizers, and electronic watches are all sources of potential evidence. If the case warrants, the investigator should seize and analyze all sources of data — electronic and manual. He or she should also document all activity in an activity log and, if necessary, secure the crime scene.

### **Surveillance**

Two forms of surveillance are used in computer crime investigations: physical and computer. Physical surveillance can be generated at the time of the abuse, through CCTV security cameras, or after the fact. When after the fact, physical surveillance is usually performed undercov-

---

---

er. It can be used in an investigation to identify a subject's personal habits, family life, spending habits, or associates.

Computer surveillance is achieved in a number of ways. It is done passively through audit logs or actively by way of electronic monitoring. Electronic monitoring can be accomplished through keyboard monitoring, network sniffing, or line monitoring. In any case, it generally requires a warning notice or explicit statement in the corporate security policy indicating that the company can and will electronically monitor any and all system or network traffic. Without such a policy or warning notice, a warrant is normally required.

Before conducting any electronic monitoring, the investigator should review Chapters 2500 and 2700 of the *Electronic Communications Privacy Act* (ECPA), Title 18 of the U.S. Code. (These chapters relate to key-stroke monitoring or system administrators looking into someone's account.) If the account holder has not been properly notified, the system administrator and the company can be guilty of a crime and liable for civil penalties. Failure to obtain a warrant could result in the evidence being suppressed, or worse yet, litigation by the suspect for invasion of privacy or violation of the ECPA.

One other method of computer surveillance that is used is "sting operations." These operations are established so as to continue to track the attacker, on-line. By baiting a trap or setting up "Honey Pots," the victim organization lures the attacker to a secured area of the system. The system attackers were enticed into accessing selected files. Once these files or their contents are downloaded to another system, their mere presence can be used as evidence against the suspect. This enticement is not the same as entrapment because the intruder is already predisposed to commit the crime. Entrapment only occurs when a law enforcement officer induces a person to commit a crime that the person had not previously contemplated.

It is very difficult to track and identify a hacker or remote intruder unless there is a way to trace the call (e.g., caller ID or wire tap). Even with these resources, many hackers meander through communication networks, hopping from one site to the next, through a multitude of telecommunications gateways and hubs, such as the Internet. In addition, the organization cannot take the chance of allowing the hacker to have continued access to its system, potentially causing additional harm.

Telephone taps require the equivalent of a search warrant. Moreover, the victim will be required to file a criminal report with law enforcement and must show probable cause. If sufficient probable cause is shown, a warrant will be issued and all incoming calls can be traced. Once a trace is made, a pen register is normally placed on the suspect's phone to log all calls placed by the suspect. These entries can be tied to the system intrusions based on the time of the call and the time that the system was accessed.

---



---

**EXHIBIT 2 — Investigative and Forensic Tools Currently Available**

---

**Investigative Tools**

Investigation and Forensic Toolkit Carrying Case	Static Charge Meter
Cellular Phone	EMF/ELF Meter (Magnetometer)
Laptop Computer	Gender Changer (9 Pin and 25 Pin)
Camcorder w/NTSC adapter	Line Monitor
35mm Camera (2)	RS232 Smart Cable
Polaroid Camera	Nitrile Antistatic Gloves
Tape Recorder (VOX)	Alcohol Cleaning Kit
Scientific Calculator	CMOS Battery
Label Maker	Extension Cords
Magnifying Glass 3 1/4"	Power Strip
Crime Scene/Security Barrier Tape	Keyboard Key Puller
PC Keys	Cable Tester
IC Removal Kit	Breakout Box
Compass	Transparent Static Shielding Bags (100 Bags)
	Antistatic Sealing Tape
Felt Tip Pens	
Diamond Tip Engraving Pen	Serial Port Adapters (9 Pin - 25 Pin & 25 Pin - 9 Pin)
Extra Diamond Tips	Foam-Filled Carrying Case
	Static-Dissipative Grounding Kit w/Wrist Strap
Inspection Mirror	Foam-Filled Disk Transport Box
Evidence Seals (250 Seals/Roll)	Printer and Ribbon Cables
	9 Pin Serial Cable
Plastic Evidence Bags (100 Bags)	25 Pin Serial Cable
Evidence Labels (100 Labels)	Null Modem Cable
Evidence Tape — 2"×165'	Centronics Parallel Cable
Tool Kit containing:	50 Pin Ribbon Cable
Screwdriver Set (inc. Precision Set)	LapLink Parallel Cable
Torx Screwdriver Set	Telephone Cable for Modem
25' Tape Measure	
Razor Knife	
Nut Driver	
Pliers Set	
LAN Template	
Probe Set	
Neodymium Telescoping Magnetic Pickup	
Allen Key Set	
Alligator Clips	
Wire Cutters	
Small Pry Bar	
Hammer	
Tongs and/or Tweezers	
Cordless Driver w/Rechargeable Batteries (2)	Batteries for Camcorder, Camera, Tape Recorder, etc. (AAA, AA, 9-volt)
Pen Light Flashlight	
Computer Dusting System (Air Spray)	
Small Computer Vacuum	

**Investigative and Forensic Tools**

[Exhibit 2](#), although not exhaustive, identifies some of the investigative and forensic tools that are commercially available. Exhibit 2 identifies the

---

---

**EXHIBIT 3 — Forensic Software and Utilities Currently Available**

---

Computer Supplies	Software Tools
Diskettes: 3 1/2" Diskettes (Double and High-Density Format) 5 1/4" Diskettes (Double and High-Density Format) Diskette Labels 5 1/2" Floppy Diskette Sleeves 3 1/2" Floppy Diskette Container CD-ROM Container Write Protect labels for 5 1/4" Floppies Tape Media 1/4" Cartridges 4 mm DAT 8 mm DAT Travan 9-Track/1600/6250 QIC  Hard Disks IDE SCSI Paper 8 1/2 × 11 Laser Paper 80 Column Formfeed 132 Column Formfeed	Sterile O/S Diskettes  Virus Detection Software SPA Audit Software Little-Big Endian Type Application Password Cracking Utilities Disk Imaging Software Auditing Tools Test Data Method Integrated Test Facility (ITF) Parallel Simulation Snapshot Mapping Code Comparison Checksum File Utilities (DOS, Windows, 95, NT, UNIX)  Zip/Unzip Utilities
Miscellaneous Supplies	Miscellaneous Supplies
Paper Clips Scissors Rubber Bands Stapler and Staples Masking Tape Duct Tape Investigative Folders Cable Ties/Labels Numbered and Colored Stick-on Labels	MC60 Microcassette Tapes Camcorder Tapes 35mm Film (Various Speeds) Polaroid Film Graph Paper Sketch Pad Evidence Checklist Blank Forms — Schematics Label Maker Labels

hardware and software tools that should be part of the investigators tool-kit, and [Exhibit 3](#) identifies forensic software and utilities.

**Other Investigative Information Sources**

When conducting an internal investigation, it is important to remember that the witness statements and computer-related evidence are not the only sources of information useful to the investigation. Personnel files provide a wealth of information related to an employee's employment history. It may show past infractions by the employee or disciplinary action by the company. Telephone logs can possibly identify any accom-

---

---

plices or associates of the subject. At a minimum, they will identify the suspects most recent contacts. Finally, security logs, time cards, and check-in sheets will determine when a suspected insider had physical access to a particular system.

### **Investigative Reporting**

The goal of the investigation is to identify all available facts related to the case. The investigative report should provide a detailed account of the incident, highlighting any discrepancies in witness statements. The report should be a well-organized document that contains a description of the incident, all witness statements, references to all evidentiary articles, pictures of the crime scene, drawings and schematics of the computer and the computer network (if applicable), and finally, a written description of the forensic analysis. The report should state final conclusions, based solely on the facts. It should not include the investigator's opinions. The investigator should keep in mind that all documentation related to the investigation is subject to discovery by the defense, so that he or she should exercise caution in any writings associated with the investigation.

### **COMPUTER FORENSICS**

Computer forensics is the study of computer technology as it relates to the law. The objective of the forensic process is to learn as much about the suspect system as possible. This generally means analyzing the system by using a variety of forensic tools and processes, and that the examination of the suspect system may lead to other victims and other suspects. The actual forensic process is different for each system analyzed, but the guidelines in [Exhibit 4](#) should help the investigator or analyst conduct the forensic process.

### **Searching Access Controlled Systems and Encrypted Files**

During a search, an investigator may be confronted with a system that is secured physically or logically. Some physical security devices such as CPU key locks prevent only a minor obstacle, whereas other types of physical access control systems may be harder to break.

Logical access control systems may pose a more challenging problem. The analyst may be confronted with a software security program that requires a unique user name and password. Some of these systems can be simply bypassed by entering a Control-C or some other interrupt command. The analyst must be cautious that any of these commands may invoke a Trojan horse routine that may destroy the contents of the disk. A set of "password cracker" programs should be part of the forensic toolkit. The analyst can always try to contact the publisher of the software program in an effort to gain access. Most security program publishers leave a back door to enter their systems.

---

**Forensics Analysis**

**1. Conduct a Disk Image Backup of Suspect System**

Remove the internal hard disks from suspect machine and label:

- Which disk is being removed (checking the cables C and D)?
- What type of disk is it? IDE or SCSI?
- What is the capacity of the disk, making a note of cylinders, heads, and sectors?

Place each disk in a clean forensic examination machine as the next available drive, beware that the suspect disk may have a virus (keep only the minimal amount of software on the forensic examination machine and log all applications).

Backup (i.e., disk image) the suspect disks to tape:

- Make at least four copies of the affected disk.
- Put the original disk into evidence along with a backup tape.
- Return a copy back to the victim.
- Use the other two copies for the investigation (one is used for new utilities).

Pack the original suspect disks, along with one of the backup tapes in the appropriate containers, seal, mark, and log into evidence.

Restore one of the backup tapes to a disk equal in capacity (identical drive, if possible).

Analyze the data (in a controlled environment) on the restored disk.

**2. System Analysis and Investigation (Forensic System)**

Everything on the system must be checked.

If files or disk are encrypted:

- Try to locate or obtain the suspects password (which may be part of evidence collected).
- Attempt to obtain the encryption algorithm and key.
- Attempt to crack the password by using brute force or cracking tools.
- Compel the suspect to provide the password or key.

If the disk is formatted:

- Attempt to use the unformat commands.

Check for viruses.

Create an organization chart of the disk:

- Use the commands from the primary forensic host disk.

Chkdsk — displays the number of hidden files on the DOS system.

Search for hidden and deleted files with Norton Utilities:

- Change the attributes of hidden files.
- Un-erase deleted files.

If necessary, use data recovery techniques to recover:

- Hidden files (hidden by attributes or steganography).
- Erased files.
- Reformatted media.
- Overwritten files.
- Review slack space. (The amount of slack space for each file will vary from system to system based on cluster size that expands as hard disk capacity increases. The cluster, the basic allocation unit, is the smallest unit of space that DOS uses for a file.)

Inventory all files on the disk.

Review selected files and directories with Outside/In:

- Conduct a keyword search with a utility program or custom search program.
  - Check word processing documents (\*.doc), text files (\*.txt), spreadsheets (\*.xls), and databases (keep in mind that the file names may be camouflaged and may not relate to the content).
-

---

## EXHIBIT 4 — Guidelines for Forensic Analysis (*Continued*)

---

### Forensics Analysis

Review communications programs to ascertain if any numbers are stored in the application.

Search for electronic pen pals and target systems:

- Communications software setup.
- Caller ID files.
- War dialer logs.

Review the slack space on the suspect disk:

- Amount of slack space is dependent on disk capacity.

### 3. Reassemble the Suspect System (exact configuration)

Re-install a copy of the suspect disk onto the suspect system.

Check the CMOS to make sure that the boot sequence is floppy first, hard disk second.

If the system is password protected at the CMOS level, remove or reinstall or short out the CMOS battery.

Boot the system from a clean copy of the operating system (i.e., from floppy disk)

Pay particular attention to the boot-up process:

- Modified BIOS or EPROM.
- Possibly during the self test or boot-up process.

At first, do not use the affected systems operating system (OS) utilities on the original disks:

- Many times these utilities contain a Trojan Horse or logic bomb that will do other than what is intended (i.e., conducting a delete with the Dir command).
- If necessary to boot from the suspect system, check to ensure that the system boots from the floppy drive and not the suspect drive. This may mean using a clean DOS operating system floppy and then using the `command.com` file from that floppy.

Check the system time:

- Always check to see if the clock was reset on the system.

Run a complete systems analysis report:

- System summary, which contains basic system configuration.
- Disk summary.
- Memory usage with task list.
- Display summary.
- Printer summary.
- TSR summary.
- DOS driver summary.
- System interrupts.
- CMOS summary.
- List all environment variables as set by `autoexec.bat`, `config.sys`, `win.ini`, and `system.ini`.

Check system logs for account activity:

- Print out an audit trail, if available.
- Is the audit trail used in the normal course of business?
- What steps are taken to ensure the integrity of the audit trail?
- Has the audit trail been tampered with? If so, when?

### 4. Reassemble the suspect system (exact configuration)

Use the affected systems OS utilities on the original disks:

- Let the system install all background programs (set by `autoexec.bat` and `config.sys`).

What has been done to the system? Any Trojan Horses?

---

### Forensics Analysis

What rogue programs were left on the system?

- Check the system interrupts and TSRs for rogue programs (i.e., keystroke monitoring).

**5. Restore and review all data on PCMCIA flash disks, floppy disk, optical disk, ditto tapes, zip drives, kangaroo drives, and all backup media.**

Repeat the procedures one through four for all data.

**6. Notes and reminders**

The investigator must use an anti-static wrist-band and mat before conducting any forensic analysis.

The investigator must make notes for each step in the process, especially when restoring hidden or deleted files or modifying the suspect system (i.e., repairing a corrupted disk sector with Norton Utilities).

The investigator must note that what has happened on the system may have resulted from error or incompetence rather than a malicious user.

The investigator must remember the byte ordering sequence when conducting a system dump.

The investigator must write-protect all floppies before analyzing.

When analyzing databases, the data structures must be compared. The data may have been changed or the structure itself, which would totally invalidate the data.

The investigator should remember, even if the data is not on the hard disk, that it may be on backup tapes or some other form of backup media.

The investigator should look around the suspect's work area for documents that may provide a clue to the proper user name and password combination. The investigator should also check desk drawers and rolodexes to find names of acquaintances and friends, for example. It is possible to compel a suspect to provide access information. The following cases set a precedence for ordering a suspect, whose computer was in the possession of law enforcement, to divulge password or decryption key:

- *Fisher v. U.S.* (1976), 425 U.S. 391, 48 LED2 39.
- *U.S. v. Doe* (1983), 465 U.S. 605, 79 LED2d 552.
- *Doe v. U.S.* (1988), 487 U.S. 201, 101 LED2d 184.
- *People v. Sanchez* (1994) 24 CA4 1012.

The caveat is that the suspect might use this opportunity to command the destruction of potential evidence. The last resort may be for the investigator to hack the system, which can be done as follows:

- Search for passwords written down.
  - Try words, names, or numbers that are related to the suspect.
  - Call the software vendor and request their assistance (some vendors may charge for this).
-

- 
- Try to use password-cracking programs that are readily available on the net.
  - Try a brute force or dictionary attack.

### **Steganography**

One final note on computer forensics involves steganography, which is the art of hiding communications. Unlike encryption, which uses an algorithm and a seed value to scramble or encode a message to make it unreadable, steganography makes the communication invisible. This takes concealment to the next level: that is, to deny that the message even exists. If a forensic analyst were to look at an encrypted file, it would be obvious that some type of cipher process had been used. It is even possible to determine what type of encryption process was used to encrypt the file, based on a unique signature. However, steganography hides data and messages in a variety of picture files, sound files, and even slack space on floppy diskettes. Even the most trained security specialist or forensic analyst may miss this type of concealment during a forensic review.

Steganography simply takes one piece of information and hides it within another. Computer files, such as images, sound recordings, and slack space contain unused or insignificant areas of data. For example, the least significant bits of a bitmap image can be used to hide messages, usually without any material change in the original file. Only through a direct, visual comparison of the original and processed image can the analyst detect the possible use of steganography. Because many times the suspect system only stores the processed image, the analyst has nothing to use as a comparison and generally has no way to tell that the image in question contains hidden data.

### **LEGAL PROCEEDINGS**

The victim and the investigative team must understand the full effect of their decision to prosecute. The postincident legal proceedings generally result in additional cost to the victim until the outcome of the case, at which time they may be reimbursed.

### **Discovery and Protective Orders**

Discovery is the process whereby the prosecution provides all investigative reports, information on evidence, list of potential witnesses, any criminal history of witnesses, and any other information except how they are going to present the case to the defense. Any property or data recovered by law enforcement will be subject to discovery if a person is charged with a crime. However, a protective order can limit who has access, who can copy, and the disposition of the certain protected docu-

---

---

ments. These protective orders allow the victim to protect proprietary or trade secret documents related to a case.

### **Grand Jury and Preliminary Hearings**

If the defendant is held to answer in a preliminary hearing or the grand jury returns an indictment, a trial will be scheduled. If the case goes to trial, interviews with witnesses will be necessary. The victimized company may have to assign someone to work as the law enforcement liaison.

### **The Trial**

The trial may not be scheduled for some time, based on the backlog of the court that has jurisdiction in the case. In addition, the civil trial and criminal trial will occur at different times, although much of the investigation can be run in parallel. The following items provide guidance for courtroom testimony:

- The prosecutor does not know what questions the defense attorney will ask.
- The questions should be listened to carefully to understand and determine that it is not a multiple-part or contradictory question.
- The question should not be answered quickly. The prosecutor should be given time to object to the defense questions that are inappropriate, confusing, contradictory, or vague.
- If the question is not understandable, the defense attorney should be asked to provide an explanation, or the question can be answered by stating: "I understand your question to be ...."
- Hearsay answers should not be given, which generally means that testimony as to personal conversations cannot be given.
- Witnesses should not get angry, because it may affect their credibility.
- Expert witnesses may need to be called.

### **Recovery of Damages**

To recover the costs of damages, such as reconstructing data, reinstalling an uncontaminated system, repairing a system, or investigating a breach, a civil law suit can be filed against the suspect in either a superior court or a small claims court.

### **Post-Mortem Review**

The purpose of the post-mortem review is to analyze the attack and close the security holes that led to the initial breach. In doing so, it may also be necessary to update the corporate security policy. All organizations should take the necessary security measures to limit their exposure and potential liability. The security policy should include an:

---



- 
- Incident response plan.
  - Information dissemination policy.
  - Incident reporting policy.
  - Electronic monitoring statement.
  - Audit trail policy.
  - Inclusion of a warning banner that should:
    - Prohibit unauthorized access.
    - Give notice that all electronic communications will be monitored.

Finally, many internal attacks can be avoided by conducting background checks on potential employees and consultants.

## **SUMMARY**

Computer crime investigation is more an art than a science. It is a rapidly changing field that requires knowledge in many disciplines. Although it may seem esoteric, most investigations are based on traditional investigative procedures. Planning is integral to a successful investigation. For the internal investigator, an incident response plan should be formulated before an attack occurs. The incident response plan helps set the objective of the investigation and identifies each of the steps in the investigative process. For the external investigator, investigative planning may occur postincident. It is also important to realize that no individual has all the answers and that teamwork is essential. The use of a corporate CERT team is invaluable, but when no team is available the investigator may have the added responsibility of building a team of specialists.

The investigator's main responsibility is to determine the nature and extent of the system attack. From there, with knowledge of the law and forensics, the investigative team may be able to piece together who committed the crime, how and why the crime was committed, and more importantly, what can be done to minimize the potential for any future attacks. For the near term, convictions will probably be few, but as the law matures and as investigations become more thorough, civil and criminal convictions will increase. In the meantime, it is extremely important that investigations be conducted so as to understand the seriousness of the attack and the overall effect on business operations.

Finally, to be successful the computer crime investigator must, at a minimum, have a thorough understanding of the law, the rules of evidence as they relate to computer crime, and computer forensics. With this knowledge, the investigator should be able to adapt to any number of situations involving computer abuse.