**Operational Investigations**

Operational investigations have the loosest standards for collection of information. They are not intended to produce evidence because they are for internal operational purposes only. Therefore, administrators conducting an operational investigation will only conduct analysis necessary to reach their operational conclusions. The collection need not be thorough or well-documented, because resolving the issue is the primary goal. In addition to resolving the operational issue, operational investigations also often conduct a *root cause analysis* that seeks to identify the reason that an operational issue occurred. The root cause analysis often highlights issues that require remediation to prevent similar incidents in the future.

**Criminal Investigations**

Criminal investigations, typically conducted by law enforcement personnel, investigate the alleged violation of criminal law. Criminal investigations may result in charging suspects with a crime and the prosecution of those charges in criminal court. Most criminal cases must meet the beyond a reasonable doubt t standard of evidence. Following this standard, the prosecution must demonstrate that the defendant committed the crime by presenting facts from which there are no other logical conclusions. For this reason, criminal investigations must follow very strict evidence collection and preservation processes.

**Civil Investigations**

Civil investigations typically do not involve law enforcement but rather involve internal employees and outside consultants working on behalf of a legal team. They prepare the evidence necessary to present a case in civil court resolving a dispute between two parties.

Most civil cases do not follow the beyond a reasonable doubt standard of proof. Instead, they use the weaker preponderance of the evidence standard. Meeting this standard simply requires that the evidence demonstrate that the outcome of the case is more likely than not. For this reason, evidence collection standards for civil investigations are not as rigorous as those used in criminal investigations.

**Regulatory Investigations**

Government agencies may conduct regulatory investigations when they believe that an individual or corporation has violated administrative law. Regulators typically conduct these investigations with a standard of proof commensurate with the venue where they expect to try their case. Regulatory investigations vary widely in scope and procedure and are almost always conducted by government agents.

**Electronic Discovery**

In legal proceedings, each side has a duty to preserve evidence related to the case and, through the discovery process, share information with their adversary in the proceedings. This discovery process applies to both paper records and electronic records and the electronic discovery (or eDiscovery) process facilitates the processing of electronic information for disclosure. The Electronic Discovery Reference Model describes a standard process for conducting eDiscovery with nine steps.

**Information Governance** ensures that information is well organized for future eDiscovery efforts

**Identification** locates the information that may be responsive to a discovery request when the organization believes that litigation is likely.

**Preservation** ensures that potentially discoverable information is protected against alteration or deletion.

**Collection** gathers the responsive information centrally for use in the eDiscovery process

**Processing screens** the collected information to perform a “rough cut” of irrelevant information, reducing the amount of information requiring detailed screening.

**Review** examines the remaining information to determine what information is responsive to the request and removing any information protected by attorney-client privilege.

**Analysis** performs deeper inspection of the content and context of remaining information.

**Production places** the information into a format that may be shared with others.

**Presentation displays** the information to witnesses, the court and other parties.

Conducting eDiscovery is a complex process and requires careful coordination between information technology professionals and legal counsel.

**Evidence**

**Admissible Evidence**

There are three basic requirements for evidence to be introduced into a court of law. To be considered admissible evidence , it must meet all three of these requirements, as determined by the judge, prior to being discussed in open court:

**■ The evidence must be relevant t to determining a fact**

**The fact that the evidence seeks to determine must be material l (that is, related) to the case.**

**■ The evidence must be competent , meaning it must have been obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.**

**Types of Evidence**

Three types of evidence can be used in a court of law: real evidence, documentary evidence, and testimonial evidence. Each has slightly different additional requirements for admissibility.

**Real Evidence Real evidence** (also known as **object evidence** ) consists of things that may actually be brought into a court of law. In common criminal proceedings, this may include items such **as a murder weapon, clothing, or other physical objects. In a computer crime case, real evidence might include seized** computer equipment, such as a keyboard with fingerprints on it or a hard drive from a hacker’s computer system. Depending on the circumstances, **real evidence may also be conclusive evidence** , such as DNA, that is incontrovertible.

**Documentary Evidence** Documentary evidence includes any written items brought into court to prove a fact at hand. This type of evidence must also be authenticated. For example, if an attorney wants to introduce a computer log as evidence, they must bring a witness (for example, the system administrator) into court to testify that the log was collected as a routine business practice and is indeed the actual log that the system collected.

Two additional evidence rules apply specifically to documentary evidence:

■ The best evidence rule states that, when a document is used as evidence in a court proceeding, **the original document must be introduced. Copies or descriptions of original evidence (known as secondary evidence** ) will not be accepted as evidence unless certain exceptions to the rule apply.

■ **The parol evidence rule states that, when an agreement between parties is put into written form, the written document is assumed to** contain all the terms of the agreement and no verbal agreements may modify the written agreement. If documentary evidence meets the materiality, competency, and relevancy requirements and also complies with the best evidence and parol evidence rules, it can be admitted into court.

**Chain of Evidence**

In many cases, it is not possible for a witness to uniquely identify an object in court. In those cases, a chain of evidence (also known as a chain of custody ) must be established. This documents everyone who handles evidence—including the police who originally collect it, the evidence technicians who process it, and the lawyers who use it in court. The location of the evidence must be fully documented from the moment it was collected to the moment it appears in court to ensure that it is indeed the same item. This requires thorough labeling of evidence and comprehensive logs noting who had access to the evidence at specific times and the reasons they required such access.

When evidence is labeled to preserve the chain of custody, the label should include the following types of information regarding the collection:

■ General description of the evidence

■ Time and date the evidence was collected

■ Exact location the evidence was collected from

■ Name of the person collecting the evidence

■ Relevant circumstances surrounding the collection

Each person who handles the evidence must sign the chain of custody log indicating the time they took direct responsibility for the evidence and the time they handed it off to the next person in the chain of custody. The chain must provide an unbroken sequence of events accounting for the evidence from the time it was collected until the time of the trial.

**Testimonial Evidence** Testimonial evidence is, quite simply, evidence consisting of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition. Witnesses must take an oath agreeing to tell the truth, and they must have personal knowledge on which their testimony is based. Furthermore, witnesses must remember the basis for their testimony (they may consult written notes or records to aid their memory). Witnesses can offer direct evidence : oral testimony that proves or disproves a claim based on their own direct observation. The testimonial evidence of most witnesses must be strictly limited to direct evidence based on the witness’s factual observations. However, this does not apply if a witness has been accepted by the court as an expert in a certain field. In that case, the witness may offer an expert opinion based on the other facts presented and their personal knowledge of the field.

**Testimonial evidence must not be hearsay evidence**. That is, a witness cannot testify as to what someone else told them outside court. **Computer log fi les that are not authenticated by a system administrator can also be considered hearsay evidence.**

**Evidence Collection and Forensic Procedures**

Collecting digital evidence is a tricky process and should be attempted only by professional forensic technicians. The International Organization on Computer Evidence (IOCE) outlines six principles to guide digital evidence technicians as they perform media analysis, network analysis, and software analysis in the pursuit of forensically recovered evidence:

■ When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

■ Upon seizing digital evidence, actions taken should not change that evidence.

■ When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

■ All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.

■ An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

■ Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

As you conduct forensic evidence collection, it is important to preserve the original evidence. Remember that the very conduct of your investigation may alter the evidence you are evaluating. Therefore, when analyzing digital evidence, it’s best to work with a copy of the actual evidence whenever possible. For example, when conducting an investigation into the contents of a hard drive, make an image of that drive, seal the original drive in an evidence bag, and then use the disk image for your investigation.

**Media Analysis** Media analysis, a branch of computer forensic analysis, involves the identify cation and extraction of information from storage media. This may include the following:

**■ Magnetic media (e.g., hard disks, tapes)**

**■ Optical media (e.g., CDs, DVDs, Blu-ray discs)**

**■ Memory (e.g., RAM, solid state storage)**

Techniques used for media analysis may include the recovery of deleted fi les from unallocated sectors of the physical disk, the live analysis of storage media connected to a computer system (especially useful when examining encrypted media), and the static analysis of forensic images of storage media.

**Network** Analysis Forensic investigators are also often interested in the activity that took place over the network during a security incident. This is often difficult to reconstruct due to the volatility of network data—if it isn’t deliberately recorded at the time it occurs, it generally is not preserved.

Network forensic analysis, therefore, often depends on either prior knowledge that an incident is underway or the use of preexisting security controls that log network activity. These include:

Intrusion detection and prevention system logs

■ Network flow data captured by a flow monitoring system

■ Packet captures deliberately collected during an incident

■ Logs from firewalls and other network security devices

The task of the network forensic analyst is to collect and correlate information from these disparate sources and produce as comprehensive a picture of network activity as possible.

**Software** Analysis Forensic analysts may also be called on to conduct forensic reviews of applications or the activity that takes place within a running application. In some cases, when malicious insiders are suspected, the forensic analyst may be asked to coduct a review of software code, looking for back doors, logic bombs, or other security vulnerabilities.

**Hardware/Embedded Device Analysis** Finally, forensic analysts often must review the contents of hardware and embedded devices. This may include a review of

■ Personal computers

■ Smartphones

■ Tablet computers

■ Embedded computers in cars, security systems, and other devices

Analysts conducting these reviews must have specialized knowledge of the systems under review. This often requires calling in expert consultants who are familiar with the memory, storage systems, and operating systems of such devices. Because of the complex interactions between software, hardware, and storage, the discipline of hardware analysis requires skills in both media analysis and software analysis.

**Calling in Law Enforcement**

One of the first decisions that must be made in an investigation is whether law enforcement authorities should be called in. This is a relatively complicated decision that should involve senior management officials. There are many factors in favor of calling in the experts. For example, the FBI now maintains a National Computer Crime Squad that includes individuals with the following qualifications:

■ Degrees in the computer sciences

■ Prior work experience in industry and academic institutions

■ Basic and advanced commercial training

■ Knowledge of basic data and telecommunications networks

■ Experience with Unix and other computer operating systems

On the other hand, two major factors may cause a company to shy away from calling in the authorities. First, the investigation will more than likely become public and may embarrass the company. Second, law enforcement authorities are bound to conduct an investigation that complies with the Fourth Amendment and other legal requirements that may not apply if the organization conducted its own, private investigation.

**Conducting the Investigation**

Never conduct your investigation on an actual system that was compromised. Take the system offline, make a backup, and use the backup to investigate the incident.

■ Never attempt to “hack back” and avenge a crime. You may inadvertently attack an innocent third party and find yourself liable for computer crime charges.

■ If in doubt, call in expert assistance. If you don’t want to call in law enforcement, contact a private investigations firm with specific experience in the field of computer security investigations.

Computer crimes are generally classified as one of the following types:

■ Military and intelligence attacks

■ Business attacks

■ Financial attacks

■ Terrorist attacks

■ Grudge attacks

■ Thrill attacks

**Military and Intelligence Attacks**

Military and intelligence attacks are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources

An attacker may be looking for the following kinds of information:

■ Military descriptive information of any type, including deployment information, readiness information, and order of battle plans

■ Secret intelligence gathered for military or law enforcement purposes

■ Descriptions and storage locations of evidence obtained in a criminal investigation

■ Any secret information that could be used in a later attack

**Business Attacks**

Business attacks focus on illegally obtaining an organization’s confidential information. This could be information that is critical to the operation of the organization, such as a secret recipe, or information that could damage the organization’s reputation if disclosed, such as personal information about its employees. **The gathering of a competitor’s confidential information, also called industrial espionage ,**

**Financial Attacks**

Financial attacks are carried out to unlawfully obtain money or services. They are the type of computer crime you most commonly hear about in the news. The goal of a financial attack could be to steal credit card numbers, increase the balance in a bank account, or place “free” long-distance telephone calls. You have probably heard of individuals breaking into telephone company computers and placing free calls. **This type of financial attack is called phone phreaking.**

**Terrorist Attacks**

Terrorist attacks are a reality in modern society. Our increasing reliance on information systems makes them more and more attractive to terrorists. Such attacks differ from military and intelligence attacks. The purpose of a terrorist attack is to disrupt normal life and instill fear, whereas a military or intelligence attack is designed to extract secret information.

**Grudge Attacks**

Grudge attacks are attacks that are carried out to damage an organization or a person. The damage could be in the loss of information or information processing capabilities or harm to the organization or a person’s reputation. The motivation behind a grudge attack is usually a feeling of resentment, and the attacker could be a current or former employee or someone who wishes ill will upon an organization. The attacker is disgruntled with the victim and takes out their frustration in the form of a grudge attack.

**Thrill Attacks**

Thrill attacks are the attacks launched only for the fun of it. Attackers who lack the ability to devise their own attacks will often download programs that do their work for them. These attackers are often called script kiddies because they run only other people’s programs, or scripts, to launch an attack.

Incident Handling

**Event** Any occurrence that takes place during a certain period of time

**Incident** An event that has a negative outcome affecting the confidentiality, integrity, or availability of an organization’s data

**Common Types of Incidents**

An incident occurs when an attack, or other violation of your security policy, is carried out against your system. There are many ways to classify incidents; here is a general list of categories:

■ Scanning

■ Compromises

■ Malicious code

■ Denial of service

**Scanning**

Scanning attacks are reconnaissance attacks that usually precede another, more serious attack. They’re comparable to a burglar casing a neighborhood for targets, looking for homes with unlocked doors or where nobody is home on guard.

**Compromise**

A system compromise is any unauthorized access to the system or information the system stores. A compromise could originate inside or outside the organization. To make matters worse, a compromise could come from a valid user.

**Malicious Code**

When malicious code is mentioned, you probably think of viruses and spyware. Although a virus is a common type of malicious code, it is only one type of several. Detection of this type of a malicious code incident comes from either an end user reporting behavior caused by the malicious code or an automated alert reporting that scanned code containing a malicious component has been found. The most effective way to protect your system from malicious code is to implement virus and spyware scanners and keep the signature database up to date

**Denial of Service**

The final type of incident is a denial of service (DoS) . This type of incident is often the easiest to detect. A user or automated tool reports that one or more services (or the entire machine) are unavailable. Although they’re simple to detect, avoidance is a far better course of action. It is theoretically possible to dynamically alter firewall rules to reject DoS network traffic, but in recent years the sophistication and complexity of DoS attacks make them extremely difficult to defend against. Because there are so many variations of the DoS attack, implementing this strategy is a nontrivial task.

**Response Teams**

Many organizations now have a dedicated team responsible for investigating any computer security incidents that take place. These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs). When an incident occurs, the response team has four primary responsibilities:

■ Determine the amount and scope of damage caused by the incident.

■ Determine whether any confidential information was compromised during the incident.

■ Implement any necessary recovery procedures to restore security and recover from incident-related damages.

■ Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

Potential team members include the following:

■ Representative(s) of senior management

■ Information security professionals

■ Legal representatives

■ Public affairs/communications representatives

■ Engineering representatives (system and network)

**Incident Response Process**

Intrusion detection/prevention systems ■ Antivirus software ■ Firewall logs ■ System logs ■ Physical security systems ■ File integrity monitoring software

**Step 2: Response and Reporting**

Once you determine that an incident has occurred, the next step is to choose an appropriate response. Your security policy should specify steps to take for various types of incidents. Always proceed with the assumption that an incident will end up in a court of law. Treat any evidence you collect as if it must pass admissibility standards. Once you taint evidence, there is no going back. You must ensure that the chain of evidence is maintained.

**Isolation and Containment** The first actions you take should be dedicated to limiting the exposure of your organization and preventing further damage. In the case of a potentially compromised system, you should disconnect it from the network to prevent intruders from accessing the compromised system and also to prevent the compromised system from affecting other resources on the network.

**Gathering Evidence** It is common to confiscate equipment, software, or data to perform a proper investigation. The manner in which the evidence is confiscated is important. The confiscation of evidence must be carried out in a proper fashion. There are three basic alternatives.

**First,** the person who owns the evidence could voluntarily surrender it. This method is generally appropriate only when the attacker is not the owner. Few guilty parties willingly surrender evidence they know will incriminate them. Less experienced attackers may believe they have successfully covered their tracks and voluntarily surrender important evidence. A good forensic investigator can extract much “covered-up” information from a computer. In most cases, asking for evidence from a suspected attacker just alerts the suspect that you are close to taking legal action.

**Second**, you could get a **court to issue a subpoena** , or court order, that compels an individual or organization to surrender evidence and then have the subpoena served by law enforcement. Again, this course of action provides sufficient notice for someone to alter the evidence and render it useless in court.

**The last option** is a search **warrant**. This option should be used only when you must have access to evidence without tipping off the evidence’s owner or other personnel. You must have a strong suspicion with credible reasoning to convince a judge to pursue this course of action.

**Analysis and Reporting** Once you finish gathering evidence, you should analyze it to determine the most likely course of events leading up to your incident. Summarize those findings in a written report to management. In your report, you should be careful to distinguish fact from opinion. It is acceptable to theorize about possible causes, but you should be certain to state which of your conclusions are based entirely on fact and which involve a degree of estimation.

**Step 3: Recovery and Remediation**

After completing your investigation, you have two tasks remaining: restoring your environment to its normal operating state and completing a “lessons learned” process to improve how you handle future incidents.

**Restoration** The goal of the restoration process is to remediate any damage that may have occurred to the organization and limit the damage incurred by similar incidents in the future. These are some of the key actions you should take during this phase:

■ Rebuild compromised systems, taking care to remediate any security vulnerabilities that may have contributed to the incident.

■ Restore backup data, if necessary, to replace data of questionable integrity.

■ Supplement existing security controls, if necessary, to fill gaps identified during the incident analysis.

Once you have completed the restoration process, your business should be back up and running in the state it was in prior to the incident

**Lessons** Learned The final stage of the incident response process is to conduct a “lessons learned” session.

**Interviewing Individuals**

**(ISC) 2 Code of Ethics**

The safety and welfare of society and the common good, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

■ Therefore, strict adherence to this Code is a condition of certification.

**Code of Ethics Canons**

The Code of Ethics includes the following canons:

**Protect society, the common good, necessary public trust and confidence, and the infrastructure.** Security professionals have great social responsibility. We are charged with the burden of ensuring that our actions benefit the common good.

**Act honorably, honestly, justly, responsibly, and legally.** Integrity is essential to the conduct of our duties. We cannot carry out our duties effectively if others within our organization, the security community, or the general public have doubts about the accuracy of the guidance we provide or the motives behind our actions.

**Provide diligent and competent service to principals.** Although we have responsibilities to society as a whole, we also have specific responsibilities to those who have hired us to protect their infrastructure. We must ensure that we are in a position to provide unbiased, competent service to our organization.

**Advance and protect the profession.** Our chosen profession changes on a continuous basis. As security professionals, we must ensure that our knowledge remains current and that we contribute our own knowledge to the community’s common body of knowledge.

Internet Advisory Board (IAB) issued a statement of policy concerning the proper use of the Internet. The contents of this statement are valid even today. It is important that you know the basic contents of the document, titled “Ethics and the Internet,” Request for Comments (RFC) 1087, because most codes of ethics can trace their roots back to this document…