Legal, Regulations, Compliance, and Investigations

This chapter presents the following:
- Computer crimes and computer laws
- Motives and profiles of attackers
- Various types of evidence
- Laws and acts put into effect to fight computer crime
- Computer crime investigation process and evidence collection
- Incident-handling procedures
- Ethics pertaining to information security professionals and best practices

Computer and associated information crimes are the natural response of criminals to society’s increasing use of, and dependence upon, technology. However, crime has always taken place, with or without a computer. A computer is just another tool and, like other tools before it, it can be used for good or evil.

Fraud, theft, and embezzlement have always been part of life, but the computer age has brought new opportunities for thieves and crooks. A new degree of complexity has been added to accounting, recordkeeping, communications, and funds transfer. This degree of complexity brings along its own set of vulnerabilities, which many crooks are all too eager to take advantage of.

Companies are being blackmailed by cybercriminals who discover vulnerabilities in their networks. Company trade secrets and confidential information are being stolen when security breaches take place. Online banks are seeing a rise in fraud, and retailers’ databases are being attacked and robbed of their credit card information. In addition, identity theft is the fastest growing white-collar crime as of the writing of this book.

As e-commerce and online business become enmeshed in today’s business world, these types of issues become more important and more dangerous. Hacking and attacks are continually on the rise, and companies are well aware of it. The legal system and law enforcement seem to be behind in their efforts to track down cybercriminals and successfully prosecute them. New technologies to fight many types of attacks are on the way, but a great need still exists for proper laws, policies, and methods in actually catching the perpetrators and making them pay for the damage they cause. This chapter looks at some of these issues.
The Many Facets of Cyberlaw

Legal issues are very important to companies because a violation of legal commitments can be damaging to a company’s bottom line and its reputation. A company has many ethical and legal responsibilities it is liable for in regards to computer fraud. The more knowledge one has about these responsibilities, the easier it is to stay within the proper boundaries.

These issues may fall under laws and regulations pertaining to incident handling, privacy protection, computer abuse, control of evidence, or the ethical conduct expected of companies, their management, and their employees. This is an interesting time for law and technology because technology is changing at an exponential rate. Legislators, judges, law enforcement, and lawyers are behind the eight ball because of their inability to keep up with technological changes in the computing world and the complexity of the issues involved. Law enforcement needs to know how to capture a cybercriminal, properly seize and control evidence, and hand that evidence over to the prosecutorial and defense teams. Both teams must understand what actually took place in a computer crime, how it was carried out, and what legal precedents to use to prove their points in court. Many times, judges and juries are confused by the technology, terms, and concepts used in these types of trials, and laws are not written fast enough to properly punish the guilty cybercriminals. Law enforcement, the court system, and the legal community are definitely experiencing growth pains as they are being pulled into the technology of the twenty-first century.

Many companies are doing business across state lines and in different countries. This brings even more challenges when it comes to who has to follow what laws. Different states can interpret the same law differently. One country may not consider a particular action against the law at all, whereas another country may determine that the same action demands five years in prison. One of the complexities in these issues is jurisdiction. If a cracker from another country steals a bunch of credit card numbers from a U.S. financial institution and he is caught, a U.S. court would want to prosecute him. His homeland may not see this issue as illegal at all or have laws restricting such activities. Although the attackers are not restricted or hampered by country borders, the laws are restricted to borders in many cases.

Despite all of this confusion, companies do have some clear-cut responsibilities pertaining to computer security issues and specifics on how companies are expected to prevent, detect, and report crimes.

The Crux of Computer Crime Laws

Computer crime laws (sometimes referred to as cyberlaw) around the world deal with some of the core issues: unauthorized modification or destruction, disclosure of sensitive information, unauthorized access, and the use of malware (malicious software).

Although we usually only think of the victims and their systems that were attacked during a crime, laws have been created to combat three categories of crimes. A computer-assisted crime is where a computer was used as a tool to help carry out a crime. A computer-targeted crime concerns incidents where a computer was the victim of an attack crafted to harm it (and its owners) specifically. The last type of crime is where a computer is not necessarily the attacker or the attackee, but just happened to be in-
volved when a crime was carried out. This category is referred to as "computer is incidental."

Some examples of computer-assisted crimes are:

- Attacking financial systems to carry out theft of funds and/or sensitive information
- Obtaining military and intelligence material by attacking military systems
- Carrying out industrial spying by attacking competitors and gathering confidential business data
- Carrying out information warfare activities by attacking critical national infrastructure systems
- Carrying out hactivism, which is protesting a government or company’s activities by attacking their systems and/or defacing their web sites

Some examples of computer-targeted crimes include:

- Distributed Denial-of-Service (DDoS) attacks
- Capturing passwords or other sensitive data
- Installing malware with the intent to cause destruction
- Installing rootkits and sniffers for malicious purposes
- Carrying out a buffer overflow to take control of a system

**NOTE** The main issues addressed in computer crime laws are: unauthorized modification, disclosure, destruction, or access; and inserting malicious programming code.

Some confusion typically exists between the two categories, “computer-assisted crimes” and “computer-targeted crimes,” because intuitively it would seem any attack would fall into both of these categories. One system is carrying out the attacking, while the other system is being attacked. The difference is that in computer-assisted crimes, the computer is only being used as a tool to carry out a traditional type of crime. Without computers, people still steal, cause destruction, protest against companies (for example, companies that carry out experiments upon animals), obtain competitor information, and go to war. So these crimes would take place anyway, it is just that the computer is simply one of the tools available to the evildoer. One way to look at it is that a computer-targeted crime could not take place without a computer, while a computer-assisted crime could. Thus, a computer-targeted crime is one that did not, and could not, exist before computers became of common use. In other words, in the good old days, you could not carry out a buffer overflow on your neighbor, or install malware on your enemy’s system. These crimes require that computers be involved.

If a crime falls into the “computer is incidental” category, this means a computer just happened to be involved in some secondary manner, but its involvement is still insignificant. For example, if you had a friend that worked for a company that runs the state lottery and he gives you a printout of the next three winning numbers and you type them into your computer, your computer is just the storage place. You could have just kept the piece of paper and not put the data in a computer. Another example is child
pornography. The actual crime is obtaining and sharing child pornography pictures or graphics. The pictures could be stored on a file server or they could be kept in a physical file in someone’s desk. So if a crime falls within this category, the computer is not attacking another computer, and a computer is not being attacked, but the computer is still used in some significant manner.

You may say, “So what? A crime is a crime. Why break it down into these types of categories?” The reason these types of categories are created is to allow current laws to apply to these types of crimes, even though they are in the digital world. Let’s say someone is on your computer just looking around, not causing any damage, but she should not be there. Should the legislation have to create a new law stating, “Thou shall not browse around in someone else’s computer” or should we just use the already created trespassing law? What if a hacker got into a system that made all of the traffic lights turn green at the exact same time? Should the government go through the hassle of creating a new law for this type of activity, or should the courts use the already created (and understood) manslaughter and murder laws? Remember, a crime is a crime and a computer is just a new tool to carry out traditional criminal activities.

By allowing the use of current laws, this makes it easier for a judge to know what the proper sentencing (punishments) are for these specific crimes. Sentencing guidelines have been developed by the government to standardize punishments for the same types of crimes throughout federal courts. To use a simplistic description, the guidelines utilize a point system. For example, if you kidnap someone, you receive 10 points. If you take that person over state boundary lines, you get another 2 points. If you hurt this person, you get another 4 points. The higher the points, the more severe the punishment.

So if you steal money from someone’s financial account by attacking a bank’s mainframe, you may get 5 points. If you use this money to support a terrorist group, you get another 5 points. If you do not claim this revenue on your tax returns, there will be no points. The IRS just takes you behind a building and shoots you in the head.

Now, this in no way means countries can just depend upon the laws on the books and that every computer crime can be countered by an existing law. Many countries have had to come up with new laws that deal specifically with different types of computer crimes. For example, the following are just some of the laws that have been created or modified in the United States to cover the various types of computer crimes:

- 18 USC 1029: Fraud and Related Activity in Connection with Access Devices
- 18 USC 1030: Fraud and Related Activity in Connection with Computers
- 18 USC 2510 et seq.: Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC 2701 et seq.: Stored Wire and Electronic Communications and Transactional Records Access
- The Digital Millennium Copyright Act
- The Cyber Security Enhancement Act of 2002

**NOTE** You do not need to know these laws for the CISSP exam; they are just examples.
Complexities in Cybercrime

Since we have a bunch of laws to get the digital bad guys, this means we have this whole cybercrime thing under control, right?

Alas, hacking, cracking, and attacking have only increased over the years and will not stop anytime soon. Several issues deal with why these activities have not been properly stopped or even curbed. These include proper identification of the attackers, the necessary level of protection for networks, and successful prosecution once an attacker is captured.

Most attackers are never caught because they spoof their addresses and identities and use methods to cover their footsteps. Many attackers break into networks, take whatever resources they were after, and clean the logs that tracked their movements and activities. Because of this, many companies do not even know they have been violated. Even if an attacker’s activities trigger an intrusion detection system (IDS) alert, it does not usually find the true identity of the individual, though it does alert the company that a specific vulnerability was exploited.

Attackers commonly hop through several systems before attacking their victim so that tracking them down will be more difficult. Many of these criminals use innocent people’s computers to carry out the crimes for them. The attacker will install malicious software on a computer using many types of methods: e-mail attachments, a user downloading a Trojan horse from a web site, exploiting a vulnerability, and so on. Once the software is loaded, it stays dormant until the attacker tells it what systems to attack and when. These compromised systems are called zombies, the software installed on them are called bots, and when an attacker has several compromised systems, this is known as a botnet. The botnet can be used to carry out DDoS attacks, transfer spam or pornography, or do whatever the attacker programs the bot software to do. These items are covered more in-depth in Chapter 11, but are discussed here to illustrate how attackers easily hide their identity.

Local law enforcement departments, the FBI, and the Secret Service are called upon to investigate a range of computer crimes. Although each of these entities works to train its people to identify and track computer criminals, collectively they are very far behind the times in their skills and tools, and are outnumbered by the number of hackers actively attacking networks. Because the attackers use tools that are automated, they can perform several serious attacks in a short timeframe. When law enforcement is called in, its efforts are usually more manual—checking logs, interviewing people, investigating hard drives, scanning for vulnerabilities, and setting up traps in case the attacker comes back. Each agency can spare only a small number of people for computer crimes, and generally they are behind in their expertise compared to many hackers. Because of this, most attackers are never found, much less prosecuted.

This in no way means all attackers get away with their misdeeds. Law enforcement is continually improving its tactics and individuals are being prosecuted every month. The following site shows all of the current and past prosecutions that have taken place in the U.S.: www.cybercrime.gov. The point is that this is still a small percentage of people who are carrying out digital crimes. Some examples of what is posted at this site are listed in Table 10-1.
### Table 10-1  Examples of Computer Crimes in Less Than Two Months in the U.S.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 16, 2007</td>
<td>Three Individuals Indicted for Conspiracy to Sell More than $5 Million in Counterfeit Software</td>
</tr>
<tr>
<td>August 9, 2007</td>
<td>Guilty Plea Entered in Federal Copyright Infringement Case</td>
</tr>
<tr>
<td>August 7, 2007</td>
<td>Chicago-Area Man Sentenced to One Year and One Day in Prison for Criminal Copyright Infringement as Part of Operation Copycat: Movies Downloaded from Internet-Warez Site Were Sold in Defendant's Retail Outlets</td>
</tr>
<tr>
<td>August 6, 2007</td>
<td>Operation Higher Education: Maryland Man Involved in Online Piracy Ring Is Sentenced</td>
</tr>
<tr>
<td>August 7, 2007</td>
<td>Remaining Two Defendants Sentenced in Largest CD and DVD Manufacturing Piracy and Counterfeiting Scheme Prosecuted in the United States to Date: Three Defendants Used Expensive Replication Equipment and Fake FBI Anti-Piracy Labels as Part of a Massive Copyright and Trademark Infringement Scheme to Manufacture Pirated and Counterfeit Software and Music CDs and DVDs for Retail Distribution Around the Country</td>
</tr>
<tr>
<td>August 2, 2007</td>
<td>Eighteen Charged with Racketeering in Internet Drug Distribution Network</td>
</tr>
<tr>
<td>August 2, 2007</td>
<td>Former Chinese National Convicted for Committing Economic Espionage to Benefit China Navy Research Center in Beijing and for Violating the Arms Export Control Act: First Conviction in the Country Involving Source Code Under the Arms Export Control Act; and Second Conviction in the Country Under the Economic Espionage Act of 1996</td>
</tr>
<tr>
<td>July 31, 2007</td>
<td>Third Conviction for Camcording Movies in a Theater and Third Conviction for Violating the Digital Millennium Copyright Act as Part of Operation Copycat: Thirty-Sixth Copyright Conviction in Case</td>
</tr>
<tr>
<td>July 23, 2007</td>
<td>International Investigation Conducted Jointly by FBI and Law Enforcement Authorities in People's Republic of China Results in Multiple Arrests in China and Seizures of Counterfeit Microsoft and Symantec Software</td>
</tr>
<tr>
<td>July 2, 2007</td>
<td>Illinois Man Pleads Guilty to Posting &quot;24&quot; Television Show on Internet Prior to First Broadcast on Fox</td>
</tr>
<tr>
<td>June 26, 2007</td>
<td>Twenty-Nine Defendants in New York, New Jersey, and California Charged with Conspiracy to Smuggle over 950 Shipments of Merchandise into the United States: Defendants Include Merchandise Distributors, Freight Forwarders, Customs Brokers, Owners and Managers of Customs-Bonded Warehouses, and Managers of a Customs Exam Site</td>
</tr>
<tr>
<td>June 25, 2007</td>
<td>Two Convicted of Selling $6 Million Worth of Counterfeit Software on eBay</td>
</tr>
<tr>
<td>June 22, 2007</td>
<td>Extradited Software Piracy Ringleader Sentenced to 51 Months in Prison</td>
</tr>
<tr>
<td>June 14, 2007</td>
<td>“Phisher” Sentenced to Nearly Six Years in Prison After Nation’s First Can-Spam Act Jury Trial Conviction</td>
</tr>
<tr>
<td>June 12, 2007</td>
<td>Man Pleads Guilty to Conspiring to Commit Trade Secret Theft from Corning Incorporated</td>
</tr>
<tr>
<td>June 12, 2007</td>
<td>Valley Couple Charged with Criminal Copyright and Trademark Violations for Distributing Counterfeited Microsoft Software: Defendants Obtained Software and Distributed It Throughout the United States</td>
</tr>
<tr>
<td>June 8, 2007</td>
<td>Moorpark Man Sentenced to Five Years in Prison for Conducting a Multimillion Dollar International Cable Piracy Business</td>
</tr>
</tbody>
</table>
Really only a handful of laws deal specifically with computer crimes, making it more challenging to successfully prosecute the attackers who are caught. Many companies that are victims of an attack usually just want to ensure that the vulnerability the attacker exploited is fixed, instead of spending the time and money to go after and prosecute the attacker. This is a huge contributing factor as to why cybercriminals get away with their activities. Most companies do not report the crime, as illustrated in the 2006 CSI/FBI Figure 10-1. Some regulated organizations—for instance, federal institutions—by law, must report breaches. However, most organizations do not have to report breaches or computer crimes. No company wants their dirty laundry out in the open for everyone to see. The customer base will lose confidence, as will the shareholders and investors. We do not actually have true computer crime statistics because most are not reported.

Although regulations, laws, and attacks help make senior management more aware of security issues, though not necessarily motivated by them, when their company ends up in the headlines and it’s told how they lost control of over 100,000 credit card numbers, security suddenly becomes very important to them.

**CAUTION** Even though financial institutions must, by law, report security breaches and crimes, that does not mean they all follow this law. Some of these institutions, just like many other organizations, often simply fix the vulnerability and sweep the details of the attack under the carpet.

![Figure 10-1](image)

**Figure 10-1** Many companies just fix their vulnerabilities instead of reporting breaches.
Electronic Assets

Another complexity that the digital world has brought upon society is defining what has to be protected and to what extent. We have gone through a shift in the business world pertaining to assets that need to be protected. Fifteen years ago and more the assets that most companies concerned themselves with protecting were tangible ones (equipment, building, manufacturing tools, inventory). Now companies must add data to their list of assets, and data are usually at the very top of that list: product blueprints, Social Security numbers, medical information, credit card numbers, personal information, trade secrets, military deployment and strategies, and so on. Although the military has always had to worry about keeping their secrets secret, they have never had so many entry points to the secrets that had to be controlled. Companies are still having a hard time not only protecting their data in digital format, but defining what constitutes sensitive data and where that data should be kept.

NOTE
In many countries, to deal more effectively with computer crime, legislative bodies have broadened the definition of property to include data.

As many companies have discovered, protecting intangible assets (data, reputation) is much more difficult than protecting tangible assets.

The Evolution of Attacks

About five years ago, and even further back, hackers were mainly made up of people who just enjoyed the thrill of hacking. It was seen as a challenging game without any real intent of harm. Hackers used to take down large web sites (Yahoo, MSN, Excite) so their activities made the headlines and they won bragging rights among their fellow hackers. Back then, virus writers created viruses that simply replicated or carried out some benign activity, instead of the more malicious actions they could have carried out. Unfortunately, today, these trends have taken on more sinister objectives.

Although we still have script kiddies and people who are just hacking for the fun of it, organized criminals have appeared on the scene and really turned up the heat regarding the amount of damage done. In the past, script kiddies would scan thousands and thousands of systems looking for a specific vulnerability so they could exploit it. It did not matter if the system was on a company network, a government system, or a home user system. The attacker just wanted to exploit the vulnerability and “play” on the system and network from there. Today’s attackers are not so noisy, however, and they certainly don’t want any attention drawn to themselves. These organized criminals are after specific targets for specific reasons, usually profit-oriented. They try and stay under the radar and capture credit card numbers, Social Security numbers, and personal information to carry out fraud and identity theft.

NOTE
Script kiddies are hackers who do not necessarily have the skill to carry out specific attacks without the tools provided for them on the Internet and through friends. Since these people do not necessarily understand how the attacks are actually carried out, they most likely do not understand the extent of damage they can cause.
Chapter 10: Legal, Regulations, Compliance, and Investigations

Common Internet Crime Schemes

- Auction fraud
- Counterfeit cashier’s check
- Debt elimination
- Parcel courier email scheme
- Employment/business opportunities
- Escrow services fraud
- Investment fraud
- Lotteries
- Nigerian letter or “419”
- Ponzi/pyramid
- Reshipping
- Third-party receiver of funds

Find out how these types of computer crimes are carried out by visiting www.ic3.gov/crimeschemes.aspx.

In 20% of cases, information was used to open new accounts in the victim’s name.

Source: Federal Trade Commission, Identity Theft Survey Report
We have already seen a decrease in the amount of viruses created just to populate as many systems as possible, and it is predicted that this benign malware activity will continue to decrease, while more dangerous malware increases. This more dangerous malware has more focused targets and more powerful payloads—usually installing backdoors or bots, and/or loading rootkits.

So while the sophistication of the attacks continues to increase, so does the danger of these attacks. Isn’t that just peachy?

**Do You Trust Your Neighbor?**

Because an attacker must have access to the systems that hold the wanted resources, it is usually easier for insiders than outsiders to access resources that companies fight to protect. In this sense, employees present a greater potential for computer crimes than outsiders trying to get in. Many statistics and security professionals have indeed indicated that employees cause more security breaches and computer fraud than outside attackers, but the media usually only touts stories about external hackers and crackers. Therefore, fighting off that group of people receives more attention and effort than fighting the threat of employees taking advantage of their position and access.

Up till now, we have listed some difficulties of fighting cybercrime: the anonymity the Internet provides the attacker; attackers are organizing and carrying out more sophisticated attacks; the legal system is running to catch up with these types of crimes; and companies are just now viewing their data as something that must be protected. All these complexities aid the bad guys, but what if we throw in the complexity of attacks taking place between different countries?

**Different Countries**

If a hacker in Ukraine attacked a bank in France, whose legal jurisdiction is that? How do these countries work together to identify the criminal and carry out justice? Which country is required to track down the criminal? And which country should take this person to court? Well, we don’t really know. We are still working this stuff out.

When computer crime crosses international boundaries, the complexity of such issues shoots up exponentially, and the chances of the criminal being brought to any court decreases. This is because different countries have different legal systems, some countries have no laws pertaining to computer crime, jurisdiction disputes may erupt, and some governments may not want to play nice with each other. For example, if someone in Iran attacked a system in Israel, do you think the Iranian government would help Israel track down the attacker? What if someone in North Korea attacked a military system in the U.S.? Do you think these two countries would work together to find the hacker? Maybe or maybe not—or perhaps the attack was carried out by the government.

There have been efforts to standardize the different countries’ approach to computer crimes, because they happen so easily over international boundaries. Although it is very easy for an attacker in China to send packets through the Internet to a bank in Saudi Arabia, it is very difficult (because of legal systems, cultures, and politics) to motivate these governments to work together.
Also, many companies communicate internationally every day through e-mail, telephone lines, satellites, fiber cables, and long-distance wireless transmission. It is important for a company to research the laws of different countries pertaining to information flow and privacy.

Global organizations that move data across other country boundaries must be aware of and follow the Organisation for Economic Co-operation and Development (OECD) Guidelines and transborder information flow rules, which were addressed in Chapter 3. Since most countries have a different set of laws pertaining to the definition of private data and how it should be protected, international trade and business gets more convoluted and can negatively affect the economy of nations. The OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so data are properly protected and everyone follows the same type of rules.

NOTE Information on OECD Guidelines can be found at www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Although the OECD is a great start, we still have a long way to go to standardize how cybercrime is dealt with internationally.

Organizations that are not aware of and/or do not follow these types of rules and guidelines can be fined and sued, and business can be disrupted. If your company is expecting to expand globally, it would be wise to have legal counsel that understands these types of issues so this type of trouble does not find its way to your company’s doorstep.

If the organization is exchanging data with European entities, it may need to adhere to the Safe Harbor requirements. Europe has always had tighter control over protecting privacy information than the U.S. and other parts of the world. So in the past when U.S. and European companies needed to exchange data, confusion erupted and business was interrupted because the lawyers had to get involved to figure out how to work within the structures of the differing laws. To clear up this mess, a “safe harbor” framework was created, which outlines how any entity that is going to move privacy data to and from Europe must go about protecting it. U.S. companies that deal with European entities can become certified against this rule base so data transfer can happen more quickly and easily.

The European Union (EU) takes individual privacy much more seriously than most other countries in the world, so they have strict laws pertaining to data that are considered private, which are based on the European Union Principles on Privacy. This set of principles has six areas that address using and transmitting information considered sensitive in nature. All states in Europe must abide by these six principles to be in compliance.

The European Privacy Principles:

1. The reason for the gathering of data must be specified at the time of collection.
2. Data cannot be used for other purposes.
3. Unnecessary data should not be collected.
4. Data should only be kept for as long as it is needed to accomplish the stated task.
5. Only the necessary individuals who are required to accomplish the stated task should be allowed access to the data.
6. Whoever is responsible for securely storing the data should not allow unintentional “leaking” of data.

References

- Stanford Law University  http://cyberlaw.stanford.edu
- Cyber Law in Cyberspace  www.cyberspace-law.org
- Organisation for Economic Co-operation and Development  www.oecd.org

Types of Laws

As stated earlier, different countries often have different legal systems. In this section, we will cover the core components of these systems and what differentiates them.

- **Civil (code) Law**
  - System of law used in continental European countries such as France and Spain.
  - Different from the common law used in the United Kingdom and United States.
  - Civil law is rule-based law not precedence-based.
  - The civil law system is mainly focused on codified law—or written laws.
  - The history of civil laws dates to the sixth century when the Byzantine emperor Justinian codified the laws of Rome.
  - Civil legal systems should not be confused with the civil (or tort) laws found in the U.S.

- **Common Law**
  - Developed in England
  - Based on previous interpretations of laws
    - In the past, judges would walk throughout the country enforcing laws and settling disputes.
    - They did not have a written set of laws, so they based their laws on custom and precedent.
• Today it uses judges and juries of peers
• Broken down into:
  • Criminal
  • Civil
  • Administrative (regulatory)
• Responsibility is on the prosecution to prove guilt beyond a reasonable
doubt (innocent until proven guilty)
• Used in Canada, United Kingdom, Australia, United States, New Zealand

• Customary Law
  • Deals mainly with personal conduct and patterns of behavior
  • Based on traditions and customs of the region
  • Emerged when cooperation of individuals became necessary as
    communities merged
  • Not many countries work under a purely customary law system, but instead
    use a mixed system where customary law is an integrated component.
    (Codified civil law systems emerged from customary law.)
  • Mainly used in regions of the world that have mixed legal systems (e.g.,
    China, India)

• Religious Law Systems
  • Based on religious beliefs of the region
  • In Islamic countries, the law is based on the rules of the Koran.
  • The law, however, is different in every Islamic country.
  • Commonly divided into:
    • Responsibilities and obligations to others
    • Religious duties
  • Knowledge and rules as revealed by God, which define and govern human
    affairs.
  • Law, in the religious sense, also includes codes of ethics and morality which
    are upheld and required by God. For example, Hindu law, Sharia (Islamic
    law), Halakha (Jewish law), and so on.

• Mixed Law Systems
  • Two or more legal systems are used together and apply cumulatively or
    interactively.
  • A combination of systems is used as a result of more or less clearly defined
    fields of application.
Civil law may apply to certain types of crimes, while religious law may apply to other types within the same region.

Civil law deals with wrongs against individuals or companies that result in damages or loss. This is referred to as tort law. A civil lawsuit would result in financial restitution and/or community service instead of jail sentences. When someone sues another person in civil court, the jury decides upon liability instead of innocence or guilt. If the jury determines the defendant is liable for the act, then the jury decides upon the punitive damages of the case.

Criminal law is used when an individual’s conduct violates the government laws, which have been developed to protect the public. Jail sentences are commonly the punishment for criminal law cases, whereas in civil law cases the punishment is usually an amount of money that the liable individual must pay the victim. For example, in the O.J. Simpson case, he was first tried and found not guilty in the criminal law case, but then was found liable in the civil law case. This seeming contradiction can happen because the burden of proof is lower in civil cases than in criminal cases.

NOTE

Civil law generally is derived from common law (case law), cases are initiated by private parties, and the defendant is found “liable” or “not liable” for damages. Criminal law typically is statutory, cases are initiated by government prosecutors, and the defendant is found guilty or not guilty.

Administrative/regulatory law deals with regulatory standards that regulate performance and conduct. Government agencies create these standards, which are usually applied to companies and individuals within those specific industries. Some examples of

Source: University of Ottawa Faculty of Law, www.droitcivil.uottawa.ca/world-legal-systems/eng-monde.php
administrative laws could be that every building used for business must have a fire detection and suppression system, must have easily seen exit signs, and cannot have blocked doors, in case of a fire. Companies that produce and package food and drug products are regulated by many standards so the public is protected and aware of their actions. If a case was made that specific standards were not abided by, high officials in the companies could be held accountable, as in a company that makes tires that shred after a couple of years of use. The people who held high positions in this company were most likely aware of these conditions but chose to ignore them to keep profits up. Under administrative, criminal, and civil law, they may have to pay dearly for these decisions.

The people who want to be successful in fighting crime over computer wires and airwaves must understand the mentality of the enemy, just as the police officers on the street must understand the mentality of the traditional types of criminal.

Many times, when figuring out a computer crime, or any type of crime, one has to understand why and how crimes are committed. To be a good detective, one would need to know how a criminal thinks, what motivates him to do the things he does, what his goals and demons are, and how these are reflected in the crimes he commits. This is how the detective gets inside the criminal’s mind so she can predict his next move as well as understand what circumstances and environments are more prone to fraud and illegal acts. This is true with cybercrime. To properly stop, reduce, or prohibit cybercrime, it is best to know why people do what they do in the first place.

**Intellectual Property Laws**

Intellectual property laws do not necessarily look at who is right or wrong, but rather how a company can protect what it rightfully owns and what it can do if these laws are violated.

A major issue in many intellectual property cases is what the company did to protect the resources it claims have been violated in one fashion or another. A company must go through many steps to protect resources that it claims to be intellectual property and must show that it exercised due care in its efforts to protect those resources. If an employee sends a file to a friend and the company attempts to terminate the employee based on the activity of illegally sharing intellectual property, it must show the court and jury why this file is so important to the company, what type of damage could be or has been caused as a result of the file being shared, and, most importantly, what the company had done to protect that file. If the company did not secure the file and tell its employees that they were not allowed to copy and share that file, then the company will most likely lose the case. However, if the company went through many steps to protect that file, explained to its employees that it was wrong to copy and share the information within the file, and that the punishment could be termination, then the company could not be charged with falsely terminating an employee.

Intellectual property can be protected by several different laws, depending upon the type of resource it is.

**Trade Secret**

Trade secret law protects certain types of information or resources from unauthorized use or disclosure. For a company to have its resource qualify as a trade secret, the
resource must provide the company with some type of competitive value or advantage. A trade secret can be protected by law if developing it requires special skill, ingenuity, and/or expenditure of money and effort. This means that a company cannot say the sky is blue and call it a trade secret.

A trade secret is something that is proprietary to a company and important for its survival and profitability. An example of a trade secret is the formula used for a soft drink, such as Coke or Pepsi. The resource that is claimed to be a trade secret must be confidential and protected with certain security precautions and actions. A trade secret could also be a new form of mathematics, the source code of a program, a method of making the perfect jelly bean, or ingredients for a special secret sauce.

Many companies require their employees to sign a nondisclosure agreement, confirming that they understand its contents and promise not to share the company’s trade secrets with competitors. Companies require this both to inform the employees of the importance of keeping certain information secret and to deter them from sharing this information. Having them sign the nondisclosure agreement also gives the company the right to fire the employee or bring charges if the employee discloses a trade secret.

**Copyright**

In the United States, copyright law protects the right of an author to control the public distribution, reproduction, display, and adaptation of his original work. The law covers many categories of work: pictorial, graphic, musical, dramatic, literary, pantomimes, motion picture, sculptural, sound recording, and architectural. Copyright law does not cover the specific resource, as does trade secret law. It protects the expression of the idea of the resource instead of the resource itself. A copyright law is usually used to protect an author’s writings, an artist’s drawings, a programmer’s source code, or specific rhythms and structures of a musician’s creation. Computer programs and manuals are just two examples of items protected under the Federal Copyright Act. The item is covered under copyright law once the program or manual has been written. Although including a warning and the copyright symbol (©) is not required, doing so is encouraged so others cannot claim innocence after copying another’s work.

The protection does not extend to any method of operations, process, concept, or procedure, but it does protect against unauthorized copying and distribution of a work. It protects the form of expression rather than the subject matter. A patent deals more with the subject matter of an invention; copyright deals with how that invention is represented.

Computer programs can be protected under the copyright law as literary works. The law protects both the source and object code, which can be an operating system, application, or database. In some instances, the law can protect not only the code, but also the structure, sequence, and organization. The user interface is part of the definition of a software application structure; therefore, one vendor cannot copy the exact composition of another vendor’s user interface.

**Trademark**

My trademark is my stupidity.
Response: Good for you!

A trademark is slightly different from a copyright in that it is used to protect a word, name, symbol, sound, shape, color, or combination of these. The reason a company
would trademark one of these, or a combination, is that it represents their company to a group of people or to the world. Companies have marketing departments that work very hard in coming up with something new that will cause the company to be noticed and stand out in a crowd of competitors, and trademarking the result of this work is a way of properly protecting it and ensuring others cannot copy and use it.

**Patent**

*Patents* are given to individuals or companies to grant them legal ownership of, and enable them to exclude others from using or copying, the invention covered by the patent. The invention must be novel, useful, and not obvious—which means, for example, that a company could not patent air. Thank goodness. If a company figured out how to patent air, we would have to pay for each and every breath we took!

After the inventor completes an application for a patent and it is approved, the patent grants a limited property right to exclude others from making, using, or selling the invention for a specific period of time. For example, when a pharmaceutical company develops a specific drug and acquires a patent for it, that company is the only one that can manufacture and sell this drug until the stated year in the patent is up. After that, all companies are allowed to manufacture and sell this product, which is why the price of a drug drops substantially after its patent expires.

This also takes place with algorithms. If an inventor of an algorithm acquires a patent, she has full control over who can use it in their products. If the inventor lets a vendor incorporate the algorithm, she will most likely get a fee and possibly a royalty fee on each instance of the product that is sold.

**Internal Protection of Intellectual Property**

Ensuring that specific resources are protected by the previously mentioned laws is very important, but other measures must be taken internally to make sure the resources that are confidential in nature are properly identified and protected.

The resources protected by one of the previously mentioned laws need to be identified and integrated into the company’s data classification scheme. This should be directed by management and carried out by the IT staff. The identified resources should have the necessary level of access control protection, auditing enabled, and a proper storage environment. If it is deemed secret, then not everyone in the company should be able to access it. Once the individuals who are allowed to have access are identified, their level of access and interaction with the resource should be defined in a granular method. Attempts to access and manipulate the resource should be properly audited, and the resource should be stored on a protected server with the necessary security mechanisms.

Employees must be informed of the level of secrecy or confidentiality of the resource, and of their expected behavior pertaining to that resource.

If a company fails in one or all of these steps, it may not be covered by the laws described previously, because it may have failed to practice due care and properly protect the resource that it has claimed to be so important to the survival and competitiveness of the company.
Software Piracy

Software piracy occurs when the intellectual or creative work of an author is used or duplicated without permission or compensation to the author. It is an act of infringement on ownership rights, and if the pirate is caught, he could be sued civilly for damages, be criminally prosecuted, or both.

When a vendor develops an application, it usually licenses the program rather than sells it outright. The license agreement contains provisions relating to the use and security of the software and the corresponding manuals. If an individual or company fails to observe and abide by those requirements, the license may be terminated and, depending on the actions, criminal charges may be leveled. The risk to the vendor that develops and licenses the software is the loss of profits it would have earned. Many companies and their employees do not abide by their software licenses, and the employees use the company’s software for their home use.

Some software vendors sell bulk licenses, which enable several users to use the product simultaneously. Other vendors incorporate a monitoring system that keeps track of the usability to ensure that the customer does not go over the license limit. The security officer should be aware of all of these types of contractual commitments required by software companies. This person needs to be educated on the restrictions the company is under and make sure proper enforcement mechanisms are in place. If a company is found guilty of illegally copying software or using more copies than its license permits, the security officer in charge of this task will be primarily responsible.

The Software Protection Association (SPA) has been formed by major companies to enforce proprietary rights of software. The association was created to protect the founding companies’ software developments, but it also helps others ensure that their software is properly licensed. These are huge issues for companies that develop and produce software, because a majority of their revenue comes from licensing fees.

Other international groups have been formed to protect against software piracy, including the Federation Against Software Theft (FAST), headquartered in London, and the Business Software Alliance (BSA), based in Washington, D.C. They provide similar functionality as the SPA and make efforts to protect software around the world.

One of the offenses an individual or company can commit is to decompile vendor object code. This is usually done to figure out how the application works by obtaining the original source code, which is confidential, and perhaps to reverse-engineer it in the hope of understanding the intricate details of its functionality. Another purpose of reverse-engineering products is to detect security flaws within the code that can later be exploited. This is how some buffer overflow vulnerabilities are discovered.

Many times, an individual decompiles the object code into source code and either finds security holes and can take advantage of them or alters the source code to produce some type of functionality that the original vendor did not intend. In one example, an individual decompiled a program that protects and displays e-books and publications. The vendor did not want anyone to be able to copy the e-publications its product displayed and thus inserted an encoder within the object code of its product that enforced this limitation. The individual decompiled the object code and figured out how to cre-
ate a decoder that would overcome this restriction and enable users to make copies of
the e-publications, which infringed upon those authors’ and publishers’ copyrights.

The individual was arrested and prosecuted under the new Digital Millennium
Copyright Act (DMCA), which makes it illegal to create products that circumvent copy-
right protection mechanisms. As of this writing, this new act and how it will be en-
faced have caused many debates and controversy because of its possible negative
effects on free speech and legitimate research.

Interestingly enough, many computer-oriented individuals protested this person’s
arrest—something which included several marches—and the company prosecuting
(Adobe) quickly decided to drop all charges.

References

- United States Copyright Office  www.copyright.gov/
- Electronic Frontier Foundation, Intellectual Property Online: Patent,
  Trademark, Copyright  www.eff.org/IP/
- Caltech Office of the Intellectual Property Counsel  www.caltech.edu/ott/
  security/OIPC_Home.htm
- Find Law  http://news.corporate.findlaw.com
- TracReports  http://trac.syr.edu/tracreports/bulletins/white_collar_crime/
  monthlyjul06

Privacy

Privacy is becoming more threatened as the world relies more and more on technology.
In response, countries have enacted privacy laws. For example, although the United
States already had the Federal Privacy Act of 1974, it has enacted new laws, such as the
Gramm-Leach-Bliley Act of 1999 and the Health Insurance Portability and Account-
ability Act (HIPAA), in response to an increased need to protect personal privacy infor-
mation.

The Federal Privacy Act was put into place to protect U.S. citizens’ sensitive informa-
tion that is collected by government agencies. It states that any data collected must be
done in a fair and lawful manner. The data are to be used only for the purposes for which
they were collected and held only for a reasonable amount of time. If an agency collects
data on a person, that person has the right to receive a report outlining data collected
about him if it is requested. Similar laws exist in many countries around the world.

Many of the privacy principles addressed in most countries’ privacy laws state that
the information must be accurate, kept up-to-date, and cannot be disclosed to a third
party unless authorized by statute or consent of that individual. People also have the
right to make a correction to their personal information. If data is to be transmitted to
a location where the equivalent security protection cannot be ensured, then transmis-
sion is prohibited.

Technology is continually advancing in the amount of data that can be kept in data
warehouses, data mining and analysis techniques, and distribution of this mined data.
Companies that are data aggregators compile in-depth profiles of personal information on millions of people, even though many individuals have never heard of these specific companies, have never had an account with them, nor have given them permission to obtain personal information. These data aggregators compile, store, and sell personal information. One company (ChoicePoint) has approximately 19 billion records of personal information.

It seems as though putting all of this information together would make sense. It would be easier to obtain, have one centralized source, be extremely robust in the information it contained—and be the delight of identity thieves everywhere...because all they have to do is hack into one location and get enough information to steal thousands of identities. One U.S.-based company, LexisNexis, compiles and sells personal and financial data on U.S. consumers. In 2005, the company claimed that personal information on 310,000 people nationwide may have been stolen. Also in 2005, identity thieves stole the personal information for around 140,000 people from ChoicePoint.

### The Increasing Need for Privacy Laws

The following issues have increased the need for more privacy laws and governance:

- **Data aggregation and retrieval technologies advancement**
  - Large data warehouses are continually being created full of private information
- **Loss of borders (globalization)**
  - Private data flows from country to country for many different reasons
  - Business globalization
- **Convergent technologies advancements**
  - Gathering, mining, distributing sensitive information

Since companies, countries, and individuals have increased needs for privacy, we must deal with these needs through government laws, industry regulations, self-regulation, and individual actions.

### Laws, Directives, and Regulations

Regulation in computer and information security covers many areas for many different reasons. Some issues that require regulation are data privacy, computer misuse, software copyright, data protection, and controls on cryptography. These regulations can be implemented in various arenas, such as government and private sectors for reasons dealing with environmental protection, intellectual property, national security, personal privacy, public order, health and safety, and prevention of fraudulent activities.

Security professionals have so much to keep up with these days, from understanding how the latest worm attacks work and how to properly protect against them, to how new versions of DoS attacks take place and what tools are used to accomplish them. Professionals also need to follow which new security products are released and how they com-
pare to the existing products. This is followed up by keeping track of new technologies, service patches, hotfixes, encryption methods, access control mechanisms, telecommunications security issues, social engineering, and physical security. Laws and regulations are now ascending the list of things that security professionals also need to be aware of. This is because organizations must be compliant with more and more laws and regulations, and noncompliance can result in a fine or a company going out of business, with certain executive management individuals ending up in jail.

Laws, regulations, and directives developed by governments or appointed agencies do not usually provide detailed instructions to follow to properly protect computers and company assets. Each environment is too diverse in topology, technology, infrastructure, requirements, functionality, and personnel. Because technology changes at such a fast pace, these laws and regulations could never successfully represent reality if they were too detailed. Instead, they state high-level requirements that commonly have companies scratching their heads on how to be compliant with them. This is where the security professional comes to the rescue. In the past, security professionals were expected to know how to carry out penetration tests, configure firewalls, and deal only with the technology issues of security. Today, security professionals are being pulled out of the server rooms and asked to be more involved in business-oriented issues. As a security professional, you need to understand the laws and regulations that your company must comply with and what controls must be put in place to accomplish compliance. This means the security professional now must have a foot in both the technical world and the business world.

Over time, the CISSP exam has become more global in nature and less U.S.-centric. Specific questions on U.S. laws and regulations have been taken out of the test, so you do not need to spend a lot of time learning them and their specifics. Be familiar with why laws are developed and put in place and their overall goals, instead of memorizing specific laws and dates.

Thus, the following sections on laws and regulations contain information you do not need to memorize, because you will not be asked questions on these items directly. But remember that the CISSP exam is a cognitive exam, so you do need to know the different reasons and motivations for laws and regulations, which is why these sections are provided. This list covers U.S. laws and regulations, but almost every country either has laws similar to these or is in the process of developing them.

**The Sarbanes-Oxley Act (SOX)**

The Public Company Accounting Reform and Investor Protection Act of 2002, generally referred to as the Sarbanes-Oxley Act (named after the authors of the bill), was created in the wake of corporate scandals and fraud which cost investors billions of dollars and threatened to undermine the economy.

The law, also known as SOX for short, applies to any company that is publicly traded on United States markets. Much of the law governs accounting practices and the methods used by companies to report on their financial status. However, some parts, Section 404 in particular, apply directly to information technology.

SOX provides requirements for how companies must track, manage, and report on financial information. This includes safeguarding the data and guaranteeing its integrity and authenticity. Most companies rely on computer equipment and electronic storage
for transacting and archiving data, therefore there must be processes and controls in place to protect the data.

Failure to comply with the Sarbanes-Oxley Act can lead to stiff penalties and potentially significant jail time for company executives, including the Chief Executive Officer (CEO), the Chief Financial Officer (CFO), and others.

The Health Insurance Portability and Accountability Act (HIPAA)
The Health Insurance Portability and Accountability Act (HIPAA), a U.S. federal regulation, has been mandated to provide national standards and procedures for the storage, use, and transmission of personal medical information and health care data. This regulation provides a framework and guidelines to ensure security, integrity, and privacy when handling confidential medical information. HIPAA outlines how security should be managed for any facility that creates, accesses, shares, or destroys medical information.

People’s health records can be used and misused in different scenarios for many reasons. As health records migrate from a paper-based system to an electronic system, they become easier to maintain, access, and transfer, but they also become easier to manipulate and access in an unauthorized manner. Traditionally, health care facilities have lagged behind other businesses in their information and network security mechanisms, architecture, and security enforcement because there was no real business need to expend the energy and money to put these items in place. Now there is.

HIPAA mandates steep federal penalties for noncompliance. If medical information is used in a way that violates the privacy standards dictated by HIPAA, even by mistake, monetary penalties of $100 per violation are enforced, up to $25,000 per year, per standard. If protected health information is obtained or disclosed knowingly, the fines can be as much as $50,000 and one year in prison. If the information is obtained or disclosed under false pretenses, the cost can go up to $250,000 with ten years in prison if there is intent to sell or use the information for commercial advantage, personal gain, or malicious harm. This is serious business.

The Gramm-Leach-Bliley Act of 1999 (GLBA)
The Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to develop privacy notices and give their customers the option to prohibit financial institutions from sharing their information with nonaffiliated third parties. The act dictates that the board of directors is responsible for many of the security issues within a financial institution, that risk management must be implemented, that all employees need to be trained on information security issues, and that implemented security measures must be fully tested. It also requires these institutions to have a written security policy in place.

The Computer Fraud and Abuse Act
The Computer Fraud and Abuse Act, written in 1986 and amended in 1996, is the primary U.S. federal antihacking statute. It prohibits seven forms of activity and makes them federal crimes:

- The knowing access of computers of the federal government to obtain classified information without authorization or in excess of authorization
The intentional access of a computer to obtain information from a financial institution, the federal government, or any protected computer involved in interstate or foreign communications without authorization or through the use of excess of authorization.

The intentional and unauthorized access of computers of the federal government, or computers used by or for the government when the access affects the government's use of that computer.

The knowing access of a protected computer without authorization or in excess of authorization with the intent to defraud.

Knowingly causing the transmission of a program, information, code, or command and, as a result of such conduct, intentionally causing damage without authorization to a protected computer.

The knowing trafficking of computer passwords with the intent to defraud.

The transmission of communications containing threats to cause damage to a protected computer.

These acts range from felonies to misdemeanors with corresponding small to large fines and jail sentences.

The Federal Privacy Act of 1974

In the mid-1960s, a proposal was made that the U.S. government compile and collectively hold in a main federal data bank each individual’s information pertaining to the Social Security Administration, Census Bureau, the Internal Revenue Service, the Bureau of Labor Statistics, and other limbs of the government. The committee that made this proposal saw this as an efficient way of gathering and centralizing data. Others saw it as a dangerous move against individual privacy and too “Big Brother.” The federal data bank never came to pass because of strong opposition.

To keep the government in check on gathering information on U.S. citizens and other matters, a majority of its files are considered open to the public. Government files are open to the public unless specific issues enacted by the legislature deem certain files unavailable. This is what is explained in the Freedom of Information Act. This is different from what the Privacy Act outlines and protects. The Privacy Act applies to records and documents developed and maintained by specific branches of the federal government, such as executive departments, government corporations, independent regulatory agencies, and government-controlled corporations. It does not apply to congressional, judiciary, or territorial subdivisions.

An actual record is information about an individual’s education, medical history, financial history, criminal history, employment, and other similar types of information. Government agencies can maintain this type of information only if it is necessary and relevant to accomplishing the agency’s purpose. The Privacy Act dictates that an agency cannot disclose this information without written permission from the individual. However, like most government acts, legislation, and creeds, there is a list of exceptions.

So what does all of this dry legal mumbo-jumbo mean? Basically, agencies can gather information about individuals, but it must be relevant and necessary for its approved cause. In addition, that agency cannot go around town sharing other people’s
private information. If it does, private citizens have the right to sue the agency to protect their privacy.

This leaks into the computer world because this information is usually held by one type of computer or another. If an agency’s computer holds an individual’s confidential information, it must provide the necessary security mechanisms to ensure it cannot be compromised or copied in an unauthorized way.

**Basel II**

The Bank for International Settlements devised a means for protecting banks from overextending themselves and becoming insolvent. The original Basel Capital Accord implemented a system for establishing the minimum amount of capital that member financial institutions were required to keep on hand.

In November 2006, the Basel II Accord went into effect. Basel II takes a more refined approach to determining the actual exposure to risk of each financial institution and taking risk mitigation into consideration to provide an incentive for member institutions to focus on and invest in security measures.

Basel II is built on three main components, called “Pillars.” Minimum Capital Requirements measures the risk and spells out the calculation for determining the minimum capital. Supervision provides a framework for oversight and review to continually analyze risk and improve security measures. Market Discipline requires member institutions to disclose their exposure to risk and validate adequate market capital.

Information security is integral to Basel II. Member institutions seeking to reduce the amount of capital they must have on hand must continually assess their exposure to risk and implement security controls or mitigations to protect their data.

**Payment Card Industry Data Security Standards (PCI DSS)**

Identity theft and credit card fraud are increasingly more common. Not that these things did not occur before, but the advent of the Internet and computer technology have combined to create a scenario where attackers can steal millions of identities at a time.

The credit card industry took proactive steps to curb the problem and stabilize customer trust in credit cards as a safe method of conducting transactions. Visa began their own program, the Cardholder Information Security Protection (CISP) program, while other vendors began similar initiatives.

Eventually, the credit card brands joined forces and devised the Payment Card Industry Data Security Standard (PCI DSS). The PCI Security Standards Council was created as a separate entity to maintain and enforce the PCI Data Security Standard.

The PCI DSS applies to any entity that processes, transmits, stores, or accepts credit card data. Varying levels of compliance and penalties exist and depend on the size of the customer and the volume of transactions. However, credit cards are used by millions and accepted almost anywhere, which means just about every business in the world must comply with the PCI DSS.

The PCI Data Security Standard is made up of 12 main requirements broken down into six major categories. The six categories of PCI DSS are: Build and Maintain a Secure Network, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Monitor and Test Networks, and Maintain an Information Security Policy.
PCI DSS is a private-sector industry initiative. It is not a law. Noncompliance or violations of the PCI DSS may result in financial penalties or possible revocation of merchant status within the credit card industry, but not jail time. However, Minnesota recently became the first state to mandate PCI compliance as a law, and other states, as well as the United States federal government, are considering similar measures.

**NOTE** As mentioned before, privacy is being dealt with through laws, regulations, self-regulations, and individual protection. PCI is an example of a self-regulation approach. It is not a regulation that came down from the government and that is being governed by a government agency. It is an attempt by the credit card companies to reduce fraud and govern themselves so the government does not have to get involved.

**The Computer Security Act of 1987**
The Computer Security Act of 1987 requires U.S. federal agencies to identify computer systems that contain sensitive information. The agency must develop a security policy and plan for each of these systems and conduct periodic training for individuals who operate, manage, or use these systems. Federal agency employees must be provided with security-awareness training and be informed of how the agency defines acceptable computer use and practices.

Because the U.S. federal government deals with a lot of important, confidential, and secret information, it wants to make sure all individuals and systems within all federal government agencies meet a certain level of awareness and protection.

**The Economic Espionage Act of 1996**
Prior to 1996, industry and corporate espionage was taking place with no real guidelines for who could properly investigate the events. The Economic Espionage Act of 1996 provides the necessary structure when dealing with these types of cases and further defines trade secrets to be technical, business, engineering, scientific, or financial. This means that an asset does not necessarily need to be tangible to be protected or be stolen. Thus, this act enables the FBI to investigate industrial and corporate espionage cases.

**Employee Privacy Issues**
Within a corporation, several employee privacy issues must be thought through and addressed if the company wants to be properly protected. An understanding that each state may have different privacy laws should prompt the company to investigate exactly what it can and cannot monitor before it does so.

**Review on Ways of Dealing with Privacy**
Current methods of privacy protection and examples are listed next:

- **Government regulations**  SOX, HIPAA, GLBA, BASEL
- **Self-regulation**  Payment Card Industry (PCI)
- **Individual user**  Passwords, encryption, awareness
If a company has learned that the state the facility is located in permits keyboard, e-mail, and surveillance monitoring, it must take the proper steps to ensure that the employees know that these types of monitoring may be put into place. This is the best way for a company to protect itself, make sure it has a legal leg to stand on if necessary, and not present the employees with any surprises.

The monitoring must be work-related, meaning that a manager may have the right to listen in on his employees’ conversations with customers, but he does not have the right to listen in on personal conversations that are not work-related. Monitoring also must happen in a consistent way, such that all employees are subjected to monitoring, not just one or two people.

If a company feels it may be necessary to monitor e-mail messages and usage, this must be explained to the employees, first through a security policy and then through a constant reminder such as a computer banner or regular training. It is best to have an employee read a document describing what type of monitoring they could be subjected to, what is considered acceptable behavior, and what the consequences of not meeting those expectations are. The employees should sign this document, which can later be treated as a legally admissible document if necessary.

A company that wants to be able to monitor e-mail should address this point in its security policy and standards. The company should outline who can and cannot read employee messages, describe the circumstances under which e-mail monitoring may be acceptable, and specify where the e-mail can be accessed. Some companies indicate that they will only monitor e-mail that lives on the mail server, whereas other companies declare the right to read employee messages if they reside on the mail server or the employee’s computer. A company must not promise privacy to employees that it does not then provide, because that could result in a lawsuit.

Although IT and security professionals have access to many parts of computer systems and the network, this does not mean it is ethical and right to overstep the bounds that could threaten a user’s privacy. Only the tasks necessary to enforce the security policy should take place, and nothing further that could compromise another’s privacy.

Many lawsuits have arisen where an employee was fired for doing something wrong (downloading pornographic material, using the company’s e-mail system to send out...
confidential information to competitors, and so on), and the employee sues the company for improper termination. If the company has not stated that these types of activities were prohibited in its policy and made reasonable effort to inform the employee (through security awareness, computer banners, the employee handbook) of what is considered acceptable and not acceptable, and the resulting repercussions for noncompliance—the employee could win the suit and receive a large chunk of money from the company. So policies, standards, and security awareness activities need to spell out these issues, otherwise the employee’s lawyer will claim the employee had an assumed right to privacy.

**Liability and Its Ramifications**

As legislatures, courts, and law enforcement develop and refine their respective approaches to computer crimes, so too must corporations. Corporations should develop not only their preventive, detective, and corrective approaches, but also their liability and responsibility approaches. As these crimes increase in frequency and sophistication, so do their destruction and lasting effects. In most cases, the attackers are not caught, but there is plenty of blame to be passed around, so a corporation needs to take many steps to ensure that the blame and liability do not land clearly at its doorstep.

The same is true for other types of threats that corporations have to deal with today. If a company has a facility that burns to the ground, the arsonist is only one small piece of this tragedy. The company is responsible for providing fire detection and suppression systems, fire-resistant construction material in certain areas, alarms, exits, fire extinguishers, and backups of all the important information that could be affected by a fire. If a fire burns a company’s building to the ground and consumes all the records (customer data, inventory records, and similar information that is necessary to rebuild the business), then the company did not exercise due care to ensure it was protected from such loss (by backing up to an offsite location, for example). In this case, the employees, shareholders, customers, and everyone affected could successfully sue the company. However, if the company did everything expected of it in the previously listed respects, it could not be successfully sued for failure to practice due care (negligence).

Figure 10-2 illustrates the results of a real-world story where a company was found guilty of negligence and fraud.

In the context of security, **due care** means that a company did all it could have reasonably done, under the circumstances, to prevent security breaches, and also took reasonable steps to ensure that if a security breach did take place, proper controls or countermeasures were in place to mitigate the damages. In short, due care means that a company practiced common sense and prudent management and acted responsibly. **Due diligence** means that the company properly investigated all of its possible weaknesses and vulnerabilities.

Before you can figure out how to properly protect yourself, you need to find out what it is you are protecting yourself against. This is what due diligence is all about—researching and assessing the current level of vulnerabilities so the true risk level is understood. Only after these steps and assessments take place can effective controls and safeguards be identified and implemented.
The same type of responsibility is starting to be expected of corporations pertaining to computer crime and resource protection. Security is developed and implemented to protect an organization’s valuable resources; thus, appropriate safeguards need to be in place to protect the company’s mission by protecting its tangible and intangible resources, reputation, employees, customers, shareholders, and legal position. Security is a means to an end and not an end within itself. It is not practiced just for the sake of doing it. It should be practiced in such a way as to accomplish fully understood, planned, and attainable goals.

Senior management has an obligation to protect the company from a long list of activities that can negatively affect it, including protection from malicious code, natural disasters, privacy violation, infractions of the law, and more.

The costs and benefits of security should be evaluated in monetary and nonmonetary terms to ensure that the cost of security does not outweigh the expected benefits. Security should be proportional to potential loss estimates pertaining to the severity, likelihood, and extent of potential damage.

Figure 10-2 One example of the consequences of corporate fraud in 2002

![WorldCom Share Price Chart](chart)

2002
Security mechanisms should be employed to reduce the frequency and severity of security-related losses. A sound security program is a smart business practice.

Senior management needs to decide upon the amount of risk it is willing to take pertaining to computer and information security, and implement security in an economical and responsible manner. (These issues are discussed in great detail in Chapter 3.) These risks do not always stop at the boundaries of the organization. Many companies work with third parties, with whom they must share sensitive data. The main company is still liable for the protection of this sensitive data that they own, even if it is on another company’s network. This is why more and more regulations are requiring companies to evaluate their third-party’s security measures.
When companies come together to work in an integrated manner, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability, and responsibility, which should be clearly defined in the contracts each party signs. Auditing and testing should be performed to ensure that each party is indeed holding up its side of the bargain.

If one of the companies does not provide the necessary level of protection and its negligence affects a partner it is working with, the affected company can sue the upstream company. For example, let’s say company A and company B have constructed an extranet. Company A does not put in controls to detect and deal with viruses. Company A gets infected with a destructive virus and it is spread to company B through the extranet. The virus corrupts critical data and causes a massive disruption to company B’s production. Therefore, company B can sue company A for being negligent. Both companies need to make sure they are doing their part to ensure their activities, or the lack of them, will not negatively affect another company, which is referred to as downstream liability.

### NOTE

Responsibility generally refers to the obligations and expected actions and behaviors of a particular party. An obligation may have a defined set of specific actions that are required, or a more general and open approach, which enables the party to decide how it will fulfill the particular obligation. Accountability refers to the ability to hold a party responsible for certain actions or inaction.

Each company has different requirements when it comes to their list of due care responsibilities. If these steps are not taken, the company may be charged with negligence if damage arises out of its failure to follow these steps. To prove negligence in court, the plaintiff must establish that the defendant had a legally recognized obligation, or duty, to protect the plaintiff from unreasonable risks, and that the defendant’s failure to protect the plaintiff from an unreasonable risk (breach of duty) was the proximate cause of the plaintiff’s damages.

The following are some example scenarios in which a company could be held liable for negligence in its actions and responsibilities.

### Personal Information

A company that holds medical information, Medical Information Inc., does not have strict procedures on how patient information is disseminated or shared.

A person pretends to be a physician, calls into Medical Information Inc., and requests medical information on the patient Don Hammy. The receptionist does not question the caller and explains that Don Hammy has a brain tumor. A week later, Don Hammy does not receive the job he interviewed for and finds out that the employer called Medical Information Inc. for his medical information.

So what was improper about this activity and how would liability be determined? If and when this case went to court, the following items would be introduced and addressed:
- **Legally recognized obligation**
  - Medical Information Inc. does not have policies and procedures in place to protect patient information.
  - The employer does not have the right to make this kind of call and is not able to use medical information against potential employees.

- **Failure to conform to the required standard**
  - Sensitive information was released to an unauthorized person by a Medical Information Inc. employee.
  - The employer requested information it did not have a right to.

- **Proximate causation and resulting injury or damage**
  - The information provided by Medical Information Inc. caused Don Hammy great embarrassment and prevented him from obtaining a specific job.
  - The employer made its decision based on information it did not have a right to inquire about in the first place. The employer’s illegal acquisition and review of Don’s private medical information caused it to not hire him.

The outcome was a long legal battle, but Don Hammy ended up successfully suing both companies, recovered from his brain tumor, bought an island, and has never had to work again.

### Hacker Intrusion

A financial institution, Cheapo Inc., buys the necessary middleware to enable it to offer online bank account transactions for its customers. It does not add any of the necessary security safeguards required for this type of transaction to take place over the Internet.

Within the first two weeks, 22 customers have their checking and savings accounts hacked into, with a combined loss of $439,344.09.

What was improper about this activity and how would liability be determined? If and when this case went to court, the following items would be introduced and addressed:

- **Legally recognized obligation**
  - Cheapo Inc. did not implement a firewall or IDS, harden the database holding the customer account information, or use encryption for customer transactions.
  - Cheapo Inc. did not effectively protect its customers’ assets.

- **Failure to conform to the required standard**
  - By not erecting the proper security policy and program and implementing the necessary security controls, Cheapo Inc. broke 12 federal regulations used to govern financial institutions.

- **Proximate causation and resulting injury or damage**
  - The financial institution’s failure to practice due care and implement the basic requirements of online banking directly caused 22 clients to lose $439,344.09.
Eventually, a majority of the accounts were attacked and drained, a class action suit was brought against Cheapo Inc., a majority of the people got most of their money back, and the facility Cheapo Inc. was using as a financial institution is now used to sell tacos.

These scenarios are simplistic and described in a light-hearted manner, but failure to implement computer and information security properly can expose a company and its board of directors to litigation and legal punishment. Many times people cannot hide behind the corporation and are held accountable individually and personally. The board of directors can compromise its responsibilities to the stockholders, customers, and employees by not ensuring that due care is practiced and that the company was not being negligent in any way.

Resources

- U.S. Department of Justice  www.cybercrime.gov/cccases.html
- State Laws  www.cybercrimes.net/State/state_index.html
- Cornell Law University  www4.law.cornell.edu/uscode/18/1030.html

Investigations

Since computer crimes are only increasing and will never really go away, it is important that all security professionals understand how computer investigations should be carried out. This includes legal requirements for specific situations, understanding the “chain of custody” for evidence, what type of evidence is admissible in court, incident response procedures and escalation processes, and that security professionals are not robo-cops.

When a potential computer crime takes place, it is critical that the investigation steps are carried out properly to ensure that the evidence will be admissible to the court and that it can stand up under the cross-examination and scrutiny that will take place. As a security professional, you should understand that an investigation is not just about potential evidence on a disk drive. The whole environment will be part of an investigation, including the people, the network, connected internal and external systems, federal and state laws, management’s stance on how the investigation is to be carried out, and the skill set of whomever is carrying out the investigation. Messing up on just one of these components could make your case inadmissible or at least damaging if it is brought to court. So, make sure to watch many more episodes of CSI and Law & Order!

Incident Response

Many computer crimes go unreported because the victim, in many cases, is not aware of the incident or wants to just patch the hole the hacker came in through and keep the details quiet in order to escape embarrassment or the risk of hurting the company’s reputation. This makes it harder to know the real statistics of how many attacks hap-
pen each day, the degree of damage caused, and what types of attack and methods are being used.

Although we commonly use the terms “event” and “incident” interchangeably, there are subtle differences between the two. An event is a negative occurrence that can be observed, verified, and documented, while an incident is a series of events that negatively affects the company and/or impacts its security posture. This is why we call reacting to these issues “incident response,” because something is negatively affecting the company and causing a security breach.

Many types of incidences (virus, insider attack, terrorist attacks, and so on) exist and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting “weird.” The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned JavaScript and rolled out some code that caused mayhem and confusion.

When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whoever has been delegated to investigate these types of situations. Someone who is unfamiliar with the proper process of collecting data and evidence from a crime scene could instead destroy that evidence, and thus all hope of prosecuting individuals and achieving a conviction would be lost. Companies should have procedures for many issues in computer security such as enforcement procedures, disaster recovery and continuity procedures, and backup procedures. It is also necessary to have a procedure for dealing with computer incidents. Many companies do not have a clue as to who to call or what to do right after they have been the victim of a cybercrime. This means the company should have an incident response policy and procedures set up just for this type of event before it actually takes place.

The incident response policy should indicate if systems can be taken offline to try to save evidence or if systems have to continue functioning at the risk of destroying evidence. Each system and functionality should have a priority assigned to it. For instance, if the file server is hit, it should be removed from the network, but not shut down. However, if the mail server is hit, it should not be removed from the network or shut down because of the priority the company attributes to the mail server over the file server. Trade-offs and decisions will have to be made, but it is better to think through these issues before the situation occurs, because better logic is usually possible before a crisis, when there’s less emotion and chaos.

All organizations should develop an incident response team to respond to the large array of possible security incidents. The team should have someone from senior management, the network administrator, security officer, possibly a network engineer and/or programmer, and a liaison for public affairs. The purpose of having an incident response team is to ensure that there is a group of people who are properly skilled, who follow a standard set of procedures, and who are singled out and called upon when this type of event takes place.

NOTE In reality, usually the technical team members are called to the scene to carry out their functions, and the other team members may be called to update them on the situation and possibly ask them for direction pertaining to specific issues of the situation.
The team should have proper reporting procedures established, be prompt in their reaction, work in coordination with law enforcement, and be an important element of the overall security program.

The incident response team should have the following basic items:

- A list of outside agencies and resources to contact or report to
- Roles and responsibilities outlined
- A call tree to contact these roles and outside entities
- A list of computer or forensics experts to contact
- Steps on how to secure and preserve evidence
- A list of items that should be included on the report for management and potentially the courts
- A description of how the different systems should be treated in this type of situation (for example, the systems should be removed from both the Internet and the network and powered down)

When a suspected crime is reported, the incident response team should follow a set of predetermined steps to ensure uniformity in their approach and make sure no steps are skipped. First, the incident response team should investigate the report and determine that an actual crime has been committed. If the team determines that a crime has been carried out, senior management should be informed immediately. If the suspect is an employee, a human resources representative must be called right away. The sooner the documenting of events begins, the better. If someone is able to document the starting time of the crime, along with the company employees and resources involved, it would provide a good foundation for evidence. At this point, the company must decide if it wants to conduct its own forensics investigation or call in the big guns. If experts are going to be called in, the system that was attacked should be left alone in order to try and preserve as much evidence of the attack as possible. If the company decides to conduct its own forensics investigation, it must deal with many issues and address tricky elements. (Forensics will be discussed in the next section.)

Computers and networks face many types of threats, each requiring a specialized type of recovery. However, an incident response team should draft and enforce a basic outline of how all incidents are to be handled. This is a much better approach than the way many companies deal with these threats, which is usually in an ad hoc, reactive, and confusing manner. A clearly defined incident-handling process is more cost-effective, enables recovery to happen more quickly, and provides a uniform approach with certain expectation of its results.

Incident handling should be closely related to disaster recovery planning and should be part of the company’s disaster recovery plan, usually as an appendix. Both are intended to react to some type of incident that requires a quick response so the company can return to normal operations. Incident handling is a recovery plan that responds to malicious technical threats. The primary goal of incident handling is to contain and mitigate any damage caused by an incident and to prevent any further damage.

Without an effective incident-handling program, individuals who have the best intentions can sometimes make the situation worse by damaging evidence, damaging
systems, or spreading malicious code. Many times, the attacker booby-traps the compromised system to erase specific critical files if a user does something as simple as list the files in a directory. A compromised system can no longer be trusted because the internal commands listed in the path could be altered to perform unexpected activities. The system could now have a backdoor for the attacker to enter when he wants, or could have a logic bomb silently waiting for a user to start snooping around only to destroy any and all evidence.

Incident handling should also be closely linked to the company’s security training and awareness program to ensure that these types of mishaps do not take place. Past issues that the incident recovery team encountered can be used in future training sessions to help others learn what the company is faced with and how to improve response processes.

Employees need to know how to report an incident to the incident-handling team. The process must be centralized, easy to accomplish (or the employees won’t bother), convenient, and welcomed. Some employees feel reluctant to report incidents because they are afraid they will get pulled into something they do not want to be involved with or accused of something they did not do. There is nothing like trying to do the right thing and getting hit with a big stick. Employees should feel comfortable about the process, and not feel intimidated by reporting suspicious activities.

A sound incident-handling program works with outside agencies and counterparts. The members of the team should be on the mailing list of the Computer Emergency Response Team (CERT) so they can keep up-to-date about new issues and can spot malicious events, hopefully before they get out of hand. CERT is an organization that is responsible for monitoring and advising users and companies about security preparation and security breaches.

NOTE Resources for CERT can be found at www.cert.org/certcc.html and www.cert.am.

**Incident Response Procedures**

In the preceding sections, we repeatedly stated there should be a standard set of procedures for the team to follow, but what are these procedures? While different organizations define these procedures (or stages) a little differently, they accomplish the exact same thing. (ISC)² has chosen the following set of procedures for incidence response:

- Triage
- Reaction
  - Containment
  - Analysis
  - Tracking
- Follow-up
- Repair
- Recovery
- Prevention
First, we start with **triage**, just as the medics do with people who are injured. The crux of it is, “Is this person really hurt?” “How bad is this person hurt?” “What type of treatment does this person need (surgery, stitches, or just a swift kick in the butt)?”

So that’s what we do in the computer world, too. We take in the information available, investigate its severity, and set priorities on how to deal with the incident.

Once we understand the severity of the incident taking place, we move on to the next stage, which is **containment**. In the medical world, if you were found to have tuberculosis, you would be put in an isolation room because no one wants to catch your cooties. In the containment phase, the damage must be mitigated. In the computer world, this could mean that an infected server is taken off the network, firewall configurations are changed to stop an attacker, or the system that is under attack is disconnected from the Internet.

Once the incident has been contained, we need to figure out what just happened by putting the available pieces together. This is the stage of **analysis**, where more data are gathered (audit logs, video captures, human accounts of activities, system activities) to try and figure out how this incident happened. The goals are to figure out who did this, how they did it, when they did it, and why. Management must be continually kept abreast of these activities because they will be the ones making the big decisions on how this whole mess is to be handled.

Once we have as much information as we can get in the last stage and answered as many questions as we can, we then move to the **tracking** stage. We determine if the source of the incident was internal or external and how the offender penetrated and gained access to the asset. If the attacker was external, the team would contact their ISP to help them in gathering data and possibly help in finding the source of the attack. Many times this is difficult because attackers move from one system to the next, so several ISPs may have to get involved.

**NOTE** All of this data needs to be documented and carried out in a manner that will be admissible in court.
Once the incident is understood, we move into the follow-up stage, which means we implement the necessary fix to ensure this type of incident cannot happen again. This may require blocking certain ports, deactivating vulnerable services or functionalities, switching over to another processing facility, or applying a patch. This is properly called “following recovery procedures,” because just arbitrarily making a change to the environment may introduce more problems. The recovery procedures may state that a new image needs to be installed, backup data needs to be restored, the system needs to be tested, and all configurations are properly set.

**CAUTION** An attacked or infected system should never be trusted because you do not necessarily know all the changes that have taken place and the true extent of the damage. Some malicious code could still be hiding somewhere. Systems should be rebuilt to ensure that all of the potential bad mojo has been released by carrying out a proper exorcism.

What Can We Learn from This?

Once operations return to normal, it is a good idea to have a team briefing to answer the following questions:

- What happened?
- What did we learn?
- How can we do it better next time?

The team should review the incident and how it was handled and carry out a postmortem analysis. The information that comes out of this meeting should indicate what needs to go into the incidence response process and documentation, with the goal of continual improvement.

The previous model did not indicate that any type of forensics was to take place. As stated previously, management must decide if law enforcement should be brought in to carry out the investigation, if evidence should be collected for the purposes of prosecution, or if the hole should just be patched. Most companies do not have a forensics team on staff to carry out those tasks. In such situations, if a suspected crime has occurred and management does not want law enforcement involved but does want a forensics investigation carried out, external forensics experts will be called in.

Figure 10-3 outlines the same basic steps just described.
Cops or No Cops?
Management needs to make the decision as to whether law enforcement should be called in to handle the security breach. The following are some of the issues to understand if law enforcement is brought in.

- Company loses control over investigation once law enforcement is involved.
- Secrecy of compromise is not promised; it could become part of public record.
- Effects on reputation need to be considered (the ramifications of this information reaching customers, shareholders, and so on).
- Evidence will be collected and may not be available for a long period of time. It may take a year or so to get into court.

Other issues to think through when a company is developing incident response procedures include deciding how the incident will be explained to the press, customers, and shareholders. This could require the collaboration of the public relations department, management, human resources (if employees are involved), IT department, and the legal department. A cybercrime may have legal ramifications that are not immediately apparent and must be handled delicately. The company should decide how it will report the matter to outsiders, to ensure that the situation is not perceived in a totally different light.

References

- CERT Coordination Center  www.cert.org
- 6 Steps to Incident Handling  www.giac.org/resources/whitepaper/network/17.php
- The University of Georgia Computer Security and Ethics  www.uga.edu/compsec
- Bibliography of Computer Security Incident Handling Documents, by Klaus-Peter Kossakowski, DFN-CERT (Germany)  www.cert.dfn.de/eng/pre99papers/certbib.html
- NIST Incident Handling Information  http://csrc.nist.gov/topics/inchand.html

Computer Forensics and Proper Collection of Evidence

_I just spilled coffee on our only evidence._
Response: Case closed. Let’s all go home.

_Forensics_ is a science and an art that requires specialized techniques for the recovery, authentication, and analysis of electronic data for the purposes of a criminal act. Specific processes exist relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical
features of data, and computer usage. This is not something the ordinary network administrator should be carrying out.

**NOTE** Digital Forensics Science (DFS) is the study of computer technology and how it relates to law.

The people conducting the forensics investigation must be properly skilled in this trade and know what to look for. If someone reboots the attacked system or inspects various files, it could corrupt viable evidence, change timestamps on key files, and erase footprints the criminal may have left. In most situations, it is best to remove the system from the network, dump the contents of the memory, power down the system, and make a sound image of the attacked system and perform forensic analysis on this copy. Working on the copy instead of the original drive will ensure that the evidence stays unharmed on the original system in case some steps in the investigation actually corrupt or destroy data. Dumping the memory contents to a file before doing any work on the system or powering it down is a crucial step because of the information that could be stored there. This is another method of capturing fragile information.

**NOTE** The forensics team needs specialized tools, an evidence collection notebook, containers, a camera, and evidence identification tags. The notebook should not be a spiral notebook, but a notebook that is bound in a way that one can tell if pages have been removed.

### International Organization on Computer Evidence

When we covered laws earlier in the chapter, we discussed how important it is to standardize different countries’ attitudes and approaches to computer crime since computer crimes often take place over international boundaries. The same thing is true with forensics. Thus, digital evidence must be handled in a similarly careful fashion so it can be used in different courts, no matter what country is prosecuting a suspect. The *International Organization on Computer Evidence (IOCE)* was created to develop international principles dealing with how digital evidence is to be collected and handled so various courts will recognize and use the evidence in the same manner. The international principles developed by IOCE for the standardized recovery of computer-based evidence are governed by the following attributes:

- Consistency with all legal systems
- Allowance for the use of a common language
- Durability
- Ability to cross international boundaries
- Ability to instill confidence in the integrity of evidence
- Applicability to all forensic evidence
- Applicability at every level, including that of individual, agency, and country
The IOCE principles are listed next:

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing, or transferring digital evidence, is responsible for compliance with these principles.

So, there you go. Do all of that and we will finally achieve world peace.

**Motive, Opportunity, and Means**

*MOM did it.*

To understand the “whys” in crime, it is necessary to understand the motive, opportunity, and means—or MOM.

*Motive* is the “who” and “why” of a crime. The motive may be induced by either internal or external conditions. A person may be driven by the excitement, challenge, and adrenaline of committing a crime, which would be an internal condition. Examples of external conditions might include financial trouble, a sick family member, or other dire straits. Understanding the motive for a crime is an important piece in figuring out who would engage in such an activity. For example, many hackers attack big-name sites because when the sites go down, it is splashed all over the news. However, once technology advances to the point where attacks cannot bring down these sites, or once these activities are no longer so highly publicized, the individuals will eventually stop initiating these types of attacks because their motive will have been diminished.

*Opportunity* is the “where” and “when” of a crime. Opportunities usually arise when certain vulnerabilities or weaknesses are present. If a company does not have a firewall, hackers and attackers have all types of opportunities within that network. If a company does not perform access control, auditing, and supervision, employees may have many opportunities to embezzle funds and defraud the company. Once a crime fighter finds out why a person would want to commit a crime (motive), she will look at what could allow the criminal to be successful (opportunity).

*Means* pertains to the capabilities a criminal would need to be successful. Suppose a crime fighter was asked to investigate a complex embezzlement that took place within a financial institution. If the suspects were three people who knew how to use a mouse, keyboard, and a word processing application, but only one of them was a programmer and system analyst, the crime fighter would realize that this person may have the means to commit this crime much more successfully than the other two individuals.
Incident Investigators

Incident investigators are a breed of their own. Many people suspect they come from a different planet, but to date that hasn’t been proven. Good incident investigators must be aware of suspicious or abnormal activities that others might normally ignore. This is because, due to their training and experience, they may know what is potentially going on behind some abnormal system activity, while another employee would just respond, “Oh, that just happens sometimes. We don’t know why.”

The investigator could identify suspicious activities, such as port scans, attempted SQL injections, or evidence in a log that describes a dangerous activity that took place. Identifying abnormal activities is a bit more difficult, because it is more subtle. These activities could be things like increased network traffic, an employee staying late every night, unusual requests to specific ports on a network server, and so on. As an analogy, if a mother of a teenage boy smelled smoke on his jacket, she might suspect he had taken up smoking. If the teenage boy, who usually plays Xbox games all night, starts going to the library every night, the mother would notice this abnormal activity and, upon snooping around, perhaps discover her son has a new girlfriend he is meeting at the park each night.

On top of being observant, the investigator must understand forensics procedures, evidence collection issues, how to analyze a situation to determine what is going on, and know how to pick out the clues in system logs.

Different Types of Assessments an Investigator Can Perform

- Network analysis
- Communication analysis
- Log analysis
- Path tracing
- Media analysis
- Disk imaging
- MAC time analysis (Modify, Access, Create)
- Content analysis
- Slack space analysis
- Steganography
- Software analysis
- Reverse engineering
- Malicious code review
- Exploit review
The Forensics Investigation Process

To ensure that forensics activities are carried out in a standardized manner, it is necessary for the team to follow specific laid-out steps so nothing is missed and thus ensure the evidence is admissible. Each team or company may commonly come up with their own steps, but all are essentially accomplishing the same things.

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

Figure 10-4 fills in many of the steps that take place in each phase of the investigation process.

During the examination and analysis process of a forensics investigation, it is critical that the investigator works from an image that contains all of the data from the original disk. It must be a bit-level copy, sector by sector, to capture deleted files, slack spaces, and unallocated clusters. These types of images can be created through the use of specialized tools or the -dd Unix utility. A file copy tool does not recover all data areas of the device necessary for examination.

<table>
<thead>
<tr>
<th>Identification</th>
<th>Preservation</th>
<th>Collection</th>
<th>Examination</th>
<th>Analysis</th>
<th>Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event/crime detection</td>
<td>Case management</td>
<td>Preservation</td>
<td>Preservation</td>
<td>Preservation</td>
<td>Documentation</td>
</tr>
<tr>
<td>Resolve signature</td>
<td>Imaging technologies</td>
<td>Approved methods</td>
<td>Traceability</td>
<td>Traceability</td>
<td>Expert testimony</td>
</tr>
<tr>
<td>Profile detection</td>
<td>Chain of custody</td>
<td>Approved software</td>
<td>Validation techniques</td>
<td>Statistical</td>
<td>Clarification</td>
</tr>
<tr>
<td>Anomalous detection</td>
<td>Time synchronization</td>
<td>Approved hardware</td>
<td>Filtering techniques</td>
<td>Protocols</td>
<td>Mission impact statement</td>
</tr>
<tr>
<td>Complaints</td>
<td>Legal authority</td>
<td>Pattern matching</td>
<td>Data mining</td>
<td>Recommended countermeasure</td>
<td></td>
</tr>
<tr>
<td>System monitoring</td>
<td>Lossless compression</td>
<td>Hidden data discovery</td>
<td>Timeline</td>
<td>Statistical interpretation</td>
<td></td>
</tr>
<tr>
<td>Audit analysis</td>
<td>Sampling</td>
<td>Hidden data extraction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc.</td>
<td>Data reduction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recovery techniques</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 10-4 Characteristics of the different phases through an investigation process
Chapter 10: Legal, Regulations, Compliance, and Investigations

The original media should have two copies created: a primary image (a control copy that is stored in a library) and a working image (used for analysis and evidence collection).

Before creating these images, the investigator must make sure the new media has been properly purged, meaning it does not contain any residual data. Some incidents have occurred where drives that were new and right out of the box (shrink-wrapped) contained old data not purged by the vendor.

The investigator works from the duplicate image because it preserves the original evidence, prevents inadvertent alteration of original evidence during examination, and allows re-creation of the duplicate image if necessary. Most media are “magnetic-based” and the data are volatile, and can be contained in:

- Registers and cache
- Process tables and ARP cache
- Contents of system memory
- Temporary file systems
- Data on the disk

So, great care and precision must take place to capture clues from any computer or device. Remember that PDAs, cell phones, USB jump drives, laptops, and memory cards could be holding evidence also.

To ensure that the original image is not modified, it is important to create message digests for files and directories before and after the analysis to prove the integrity of the original image.

NOTE Logs should be kept detailing all activities, systems, peripherals and their serial numbers, and each team’s actions. This will help ensure that the evidence, or the process of collection, can stand up to scrutiny and be used in a court of law. Also be sure to document the role of the system(s) in the organization.

Controlling the Crime Scene

Just like any other type of crime, it is important to control who comes in contact with the evidence of the crime to ensure its integrity. The following are just some of the steps that should take place:

- Only allow authorized individuals access to the scene.
- Document who is at the crime scene.
- In court, the integrity of the evidence may be in question if there are too many people milling around.
- Document who were the last individuals to interact with the systems.
In most cases, an investigator’s notebook cannot be used as evidence in court. It can only be employed by the investigator to refresh his memory during a proceeding.

The next crucial piece is to keep a proper chain of custody of the evidence. Because evidence from these types of crimes can be very volatile and easily dismissed from court because of improper handling, it is important to follow very strict and organized procedures when collecting and tagging evidence.

When copies of data need to be made, this process must meet certain standards to ensure quality and reliability. Specialized software for this purpose can be used. The copies must be able to be independently verified and must be tamperproof.

Each piece of evidence should be marked in some way with the date, time, initials of the collector, and a case number if one has been assigned. Magnetic disk surfaces should not be marked on, and floppy disks should only be marked with a felt-tip pen. Reel-to-reel magnetic tape can be marked on the nonshiny side of the tape within the...
first portion, also known as the *leader* part. The piece of evidence should then be sealed in a container, which should be marked with the same information. The container should be sealed with evidence tape and, if possible, the writing should be on the tape so a broken seal can be detected.

**NOTE** The chain of custody of evidence dictates that all evidence be labeled with information indicating who secured and validated it.

Wires and cables should be labeled, and a photograph of the labeled system should be taken before it is actually disassembled. Media should be write-protected. Storage should be dust free, kept at room temperature without much humidity, and, of course, not stored close to any strong magnets or magnetic fields.

If possible, the crime scene should be photographed, including behind the computer if the crime involved some type of physical break-in. Documents, papers, and devices should be handled with cloth gloves and placed into containers and sealed. All storage media should be contained, even if it has been erased, because data still may be obtainable.

Because this type of evidence can be easily erased or destroyed and is complex in nature, identification, recording, collection, preservation, transportation, and interpretation are all important. After everything is properly labeled, a chain of custody log should be made of each container and an overall log should be made capturing all events.

For a crime to be successfully prosecuted, solid evidence is required. Computer forensics is the art of retrieving this evidence and preserving it in the proper ways to make it admissible in court. Without proper computer forensics, hardly any computer crimes could ever be properly and successfully presented in court.

The most common reasons for improper evidence collection are: no established incident response team, no established incident response procedures, poorly written policy, and a broken chain of custody.

**NOTE** A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented as evidence in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

**Resources**

- To Catch a Thief  [www.logicalsecurity.com/resources/resources_articles.html](http://www.logicalsecurity.com/resources/resources_articles.html)
- Introduction to Forensics  [www.albany.edu/~gangolly/digitalforensics661.ppt](http://www.albany.edu/~gangolly/digitalforensics661.ppt)
What Is Admissible in Court?

He is guilty because I don’t like him.
Response: Um, I need more than that.

Computer logs are important in many aspects of the IT world. They are usually used to troubleshoot an issue or to try to understand the events that took place at a specific moment in time. When computer logs are to be used as evidence in court, they must be collected in the regular course of business. Most of the time, computer-related documents are considered hearsay, meaning the evidence is secondhand evidence. Hearsay evidence is not normally admissible in court unless it has firsthand evidence that can be used to prove the evidence’s accuracy, trustworthiness, and reliability, such as the testimony of a businessperson who generated the computer logs and collected them. This person must generate and collect logs as a normal part of his business activities and not just this one time for court. The value of evidence depends upon the genuineness and competence of the source.

It is important to show that the logs, and all evidence, have not been tampered with in any way, which is the reason for the chain of custody of evidence. Several tools are available that run checksums or hashing functions on the logs, which will allow the team to be alerted if something has been modified.

When evidence is being collected, one issue that can come up is the user’s expectation of privacy. If an employee is suspected of, and charged with, a computer crime, he might claim that his files on the computer he uses are personal and not available to law enforcement and the courts. This is why it is important for companies to conduct security-awareness training, have employees sign documentation pertaining to the acceptable use of the company’s computers and equipment, and have legal banners pop up on every employee’s computer when they log on. These are key elements in establishing that a user has no right to privacy when he is using company equipment. The following banner is suggested by CERT Advisory:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring an individual improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

This explicit warning strengthens a legal case that can be brought against an employee or intruder, because the continued use of the system after viewing this type of warning implies that the person acknowledges the security policy and gives permission to be monitored.

Evidence has its own life cycle, and it is important that the individuals involved with the investigation understand the phases of the life cycle and properly follow them.

The life cycle of evidence includes:

- Collection and identification
- Storage, preservation, and transportation
- Presentation in court
- Return of the evidence to the victim or owner
Several types of evidence can be used in a trial, such as written, oral, computer-generated, and visual or audio. Oral evidence is testimony of a witness. Visual or audio is usually a captured event during the crime or right after it.

Not all evidence is equal in the eyes of the law and some types of evidence have more clout, or weight, than others. The following sections quickly describe the different ways evidence can be categorized and valued.

**Best Evidence**

*Best evidence* is the primary evidence used in a trial because it provides the most reliability. An example of something that would be categorized as best evidence is an original signed contract. Oral evidence is not considered best evidence because there is no firsthand reliable proof that supports its validity, and it therefore does not have as good a standing as legal documents. Oral evidence cannot be used to dispute a legal document, but it can be used to interpret the document.

**Secondary Evidence**

*Secondary evidence* is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence. Oral evidence, such as a witness’s testimony, and copies of original documents are placed in the secondary evidence category.

**Direct Evidence**

*Direct evidence* can prove a fact all by itself and does not need backup information to refer to. When using direct evidence, presumptions are not required. One example of direct evidence is the testimony of a witness who saw a crime take place. Although this oral evidence would be secondary in nature, meaning a case could not rest on just it alone, it is also direct evidence, meaning the lawyer does not necessarily need to provide other evidence to back it up. Direct evidence often is based on information gathered from a witness’s five senses.

**Conclusive Evidence**

*Conclusive evidence* is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration.

**Circumstantial Evidence**

*Circumstantial evidence* can prove an intermediate fact that can then be used to deduce or assume the existence of another fact. This type of fact is used so the judge or jury will logically assume the existence of a primary fact. For example, if a suspect told a friend he was going to bring down eBay’s web site, a case could not rest on that piece of evidence alone because it is circumstantial. However, this evidence can cause the jury to assume that because the suspect said he was going to do it, and hours later it happened, maybe he was the one who did the crime.

**Corroborative Evidence**

*Corroborative evidence* is supporting evidence used to help prove an idea or point. It cannot stand on its own but is used as a supplementary tool to help prove a primary piece of evidence.
Opinion Evidence
When a witness testifies, the opinion rule dictates that she must testify to only the facts of the issue and not her opinion of the facts. This is slightly different from when an expert witness is used, because an expert is used primarily for his educated opinion. Most lawyers call in expert witnesses to testify and help the defending or prosecuting sides better understand the subject matter so they can help the judge and jury better understand the matters of the case.

Hearsay Evidence
Hearsay evidence pertains to oral or written evidence presented in court that is second-hand and has no firsthand proof of accuracy or reliability. If a witness testifies about something he heard someone else say, it is too far removed from fact and has too many variables that can cloud the truth. If business documents were made during regular business routines, they may be admissible. However, if these records were made just to be presented in court, they could be categorized as hearsay evidence.

The foundation of admissibility is based on the following items:

- Procedures for collecting and maintaining evidence
- Proof of how errors were avoided
- Identification of custodian and skill set
- Reasonable explanations for:
  - Why certain actions were taken
  - Why specific procedures were bypassed

It is important that evidence be sufficient, reliable, and relevant to the case at hand. These characteristics of evidence provide a foundation for a case and help ensure that the evidence is legally permissible.

For the evidence to be sufficient, it must be persuasive enough to convince a reasonable person of the validity of the evidence. This means the evidence cannot be subject to personal interpretation. Sufficient evidence also means it cannot be easily doubted.

For evidence to be reliable, or competent, it must be consistent with the facts. Evidence cannot be reliable if it is based on someone’s opinion or copies of an original document, because there is too much room for error. Reliable evidence means it is factual and not circumstantial.

For evidence to be relevant, it must have a reasonable and sensible relationship to the findings. If a judge rules that a person’s past traffic tickets cannot be brought up in a murder trial, this means the judge has ruled that the traffic tickets are not relevant to the case at hand. Thus, the prosecuting lawyer cannot even mention them in court.

If a piece of evidence is found to be sufficient, reliable, and relevant to the case, it must also be legally permissible, meaning it was obtained in a legal way. The evidence must not have been obtained through an unlawful search and seizure, recorded illegally, or obtained through a coerced confession. All of these steps must be taken to ensure that the evidence will not be thrown out once it gets to court. (This section not only will help you on the CISSP exam, but will also come in handy the next time you watch Law & Order.)
Surveillance, Search, and Seizure

Two main types of surveillance are used when it comes to identifying computer crimes: physical surveillance and computer surveillance. Physical surveillance pertains to security cameras, security guards, and closed-circuit TV (CCTV), which may capture evidence. Physical surveillance can also be used by an undercover agent to learn about the suspect's spending activities, family and friends, and personal habits in the hope of gathering more clues for the case.

Computer surveillance pertains to auditing events, which passively monitors events by using network sniffers, keyboard monitors, wiretaps, and line monitoring. In most jurisdictions, active monitoring may require a search warrant. In most workplace environments, to legally monitor an individual, the person must be warned ahead of time that her activities may be subject to this type of monitoring.

Search and seizure activities can get tricky depending on what is being searched for and where. For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search. The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.

In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant.

After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.

A thin line exists between enticement and entrapment when it comes to capturing a suspect's actions. Enticement is legal and ethical, whereas entrapment is neither legal nor ethical. In the world of computer crimes, a honeypot is always a good example to show the difference between enticement and entrapment. Companies put systems in their screened subnets that either emulate services that attackers usually like to take advantage of or actually have the services enabled. The hope is that if an attacker breaks into the company's network, she will go right to the honeypot instead of the systems that are actual production machines. The attacker will be enticed to go to the honeypot system because it has many open ports and services running and exhibits vulnerabilities that the attacker would want to exploit. The company can log the attacker's actions and later attempt to prosecute.
The action in the preceding example is legal unless the company crosses the line to entrapment. For example, suppose a web page has a link that indicates that if an individual clicks it, she could then download thousands of MP3 files for free. However, when she clicks that link, she is taken to the honeypot system instead, and the company records all of her actions and attempts to prosecute. Entrapment does not prove that the suspect had the intent to commit a crime; it only proves she was successfully tricked.

**Interviewing and Interrogating**

Once surveillance and search and seizure activities have been performed, it is very likely that suspects must be interviewed and interrogated. When this is needed, there should be one person in charge of the interview or interrogation, with one or two others present. Both the topics of discussion and the questions should be prepared beforehand and asked in a systematic and calm fashion, because the purpose of an interrogation is to obtain evidence for a trial.

The employee interrogator should be in a position that is senior to the employee suspect. A vice president is not going to be very intimidated or willing to spill his guts to the mailroom clerk. The interrogation should be held in a private place, and the suspect should be relatively comfortable and at ease. If exhibits are going to be shown to the suspect, they should be shown one at a time, and otherwise kept in a folder. It is not necessary to read a person their rights before questioning unless law enforcement officers do the interrogation.

What the interrogators do not want to happen during an interrogation is to be deceived by the suspect, to relinquish important information pertaining to the investigation, or to have the suspect flee before a trial date is set.

**A Few Different Attack Types**

Several categories of computer crimes can be committed and different methods exist to commit those crimes. The following sections go over some of the types of computer fraud and abuses.

**Salami**

*I will take a little bit of your salami, and another little bit of your salami, and a bit more of your salami, and no one will ever notice.*

A *salami* attack is one in which the attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. Salami attacks usually take place in the accounting departments of companies, and the most common example of a salami attack involves subtracting a small amount of funds from many accounts with the hope that such an insignificant amount would be overlooked. For example, a bank employee may alter a banking software program to subtract 5 cents from each of the bank’s customers’ accounts once a month and move this amount to the employee’s bank account. If this happened to all of the bank’s 50,000 customer accounts, the intruder could make up to $30,000 a year.
Data Diddling

*Can I just diddle the data a little?*

*Response: Nope, it’s illegal.*

Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer’s loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20.

In 1997 in Maryland, a Taco Bell employee was sentenced to ten years in jail because he reprogrammed the drive-up window cash register to ring up every $2.99 order as one penny. He collected the full amount from the customer, put the penny in the till, and pocketed the other $2.98. He made $3600 before his arrest.

There are many reasons to enter false information into a system or application, but the usual reason is to overstate revenue and assets and understate expenses and liabilities. Sometimes managers do this to deceive shareholders, creditors, superiors, and partners.

This type of crime is common and one of the crimes easiest to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits. This is just one example of how insiders can be more dangerous than outsiders.

Excessive Privileges

Excessive privileges is a common security issue that is extremely hard to control in vast complex environments. It occurs when a user has more computer rights, permissions, and privileges than what is required for the tasks she needs to fulfill. If a user only needs to be able to read and print materials on the file server, she should not be granted full control. A common example of this is when a manager in accounting is granted full control of all files on a specific server, including payroll information. When this person is moved from accounting to the research department, his rights should be revoked or at least reduced, but most companies do not have procedures in place to make sure this happens. (This is referred to as authorization creep.) Now he has full control over the account records and the research records, and thus has excessive privileges. If he ever becomes disgruntled with the company for one reason or another, the company could have much more damage to deal with than if it had properly restricted his access.

Password Sniffing

*I think I smell a password!*

Password sniffing is just what it sounds like—sniffing network traffic with the hope of capturing passwords being sent between computers. Several tools are available on the Internet that provide this functionality. Capturing a password is tricky, because it is a piece of data that is usually only used when a user wants to authenticate into a domain or access a resource. Some systems and applications do send passwords over the network in cleartext, but a majority of them do not anymore. Instead, the user’s workstation performs a one-way hashing function on the password and sends only the resulting value...
to the authenticating system or service. The authenticating system has a file containing all users’ password hash values, not the passwords themselves, and when the authenticating system is asked to verify a user’s password, it compares the hashing value sent to what it has in its file.

Many of the tools used to capture passwords can also break the encryption of the password. This is a common way that a computer crime starts.

**IP Spoofing**

I couldn’t have carried out that attack. I have a different address!

Response: I’m not convinced.

Networks and the Internet use IP addresses like we use building numbers and street names to find our way from one place to another. Each computer is assigned an IP address so packets know where they came from and where they are going. However, many attackers do not want anyone to know their real location, so they either manually change the IP address within a packet to show a different address or, more commonly, use a tool that is programmed to provide this functionality for them. This type of activity is referred to as **IP spoofing**. Several attacks that take place use spoofed IP addresses, which give the victim little hope of finding the real system and individual who initiated the attack.

One reason that IP spoofing is so easily accomplished is that the protocol of the Internet, IP, was developed during a time when security was rarely considered. Back then, developers were much more focused on functionality, and probably could not have imagined all the various types of attacks that would be carried out using the protocols they developed.

IPv6 and IPv4 using IPSec, described in Chapter 8, can be used to help fight IP spoofing, but for this to be successful, everyone would need to use this protocol. Change is hard to implement when it means millions of people will need to modify the way they do things.

---

**NOTE** Spoofing can be considered a masquerading attack. Masquerading is the act of trying to pretend to be someone else.

**Dumpster Diving**

I went through your garbage and found your Social Security number, credit card number, network schematics, mother’s maiden name, and evidence that you wear funny underwear.

**Dumpster diving** refers to the concept of rummaging through a company’s or individual’s garbage for discarded documents, information, and other precious items that could then be used in an attack against that person or company. The intruder would have to gain physical access to the premises, but the area where the garbage is kept is usually not highly guarded. Dumpster diving is unethical, but it’s not illegal. Trespassing is illegal, however, and may be done in the process of dumpster diving. (Laws concerning this may vary in different states.)

Industrial spies can raid corporate dumpsters to find proprietary and confidential information. Credit card thieves can go through dumpsters to retrieve credit card infor-
mation from discarded receipts. Phreakers have been known to dumpster dive at telephone companies, hoping to find manuals on how the internals of the telephone systems work.

**Emanations Capturing**

*Do you think we should be worried about that white van in the parking lot with the huge antenna, large amount of power cords, and the pizzas continually being delivered to it?*

*Response: Nope.*

Emanations, and the way attackers eavesdrop on them, are addressed in Chapter 4 in the "Tempest" section. Basically, every electrical device emits electrical waves into the surrounding environment. These waves contain information, comparable to how wireless technologies work. These waves can be carried over a distance, depending on the strength of the signals and the material and objects in the surrounding area. Attackers have used devices to capture these waves and port them to their own computer systems so they can access information not intended for them.

Attackers need to have specialized tools that tune into the frequency these waves are carried over. They also have to be within close proximity to the building that is emitting the waves. Companies that have information of such sensitive nature that attackers would go through this much trouble usually have special computer systems with shielding that permit only a small amount of electrical signals to be emitted. The companies can also use material within the walls of the building to stop these types of electrical waves from passing through them.

These types of attacks are usually the stuff of spy novels, with three guys in a service van full of high-grade technological devices in the parking lot of a company. However, a certain technology has caused this type of eavesdropping to happen without such spy-like activities: wireless networks. When a company installs a wireless network, certain configurations can be set to prevent outsiders from being able to eavesdrop on its employees' network traffic. Unfortunately, some companies do not employ these configurations for one reason or another. This enables anyone with a laptop and a wireless network interface card (NIC) to drive into a company's parking lot and eavesdrop on network traffic. (Wireless technology and its security ramifications are covered in Chapter 7.)

**Wiretapping**

Most communications signals are vulnerable to some type of wiretapping or eavesdropping. It can usually be done undetected and is referred to as a passive attack. Tools used to intercept communications include cellular scanners, radio receivers, microphone receivers, tape recorders, network sniffers, and telephone-tapping devices.

---

**NOTE** A passive attack is non-intrusive, as in eavesdropping or wiretapping. An active attack, on the other hand, is intrusive, as in DoS or penetration attacks.
It is illegal to intentionally eavesdrop on another person’s conversation under many countries’ existing wiretap laws. In many cases, this action is only acceptable if the person consents or there is a court order allowing law enforcement to perform these types of activities. Under the latter circumstances, the law enforcement officers must show probable cause to support their allegation that criminal activity is taking place and can only listen to relevant conversations. These requirements are in place to protect an individual’s privacy rights.

References

- Security Focus  www.securityfocus.com/

Ethics

*Just because something is not illegal does not make it right.*

Ethics are based on many different issues and foundations. They can be relative to different situations and interpreted differently from individual to individual. Therefore, they are often a topic of debate. However, some ethics are less controversial than others, and these types of ethics are easier to expect of all people.

(ISC)² requires all certified system security professionals to commit to fully supporting its Code of Ethics. If a CISSP intentionally or knowingly violates this Code of Ethics, he or she may be subject to a peer review panel, which will decide whether the certification should be relinquished.

The full set of (ISC)² Code of Ethics for the CISSP is listed on the (ISC)² site at https://www.isc2.org/cgi-bin/content.cgi?category=12. The following list is an overview, but each CISSP candidate should read the full version and understand the Code of Ethics before attempting this exam:

- Act honorably, honestly, justly, responsibly, and legally, and protect society.
- Work diligently, provide competent services, and advance the security profession.
- Encourage the growth of research—teach, mentor, and value the certification.
- Discourage unnecessary fear or doubt, and do not consent to bad practices.
- Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures.
- Observe and abide by all contracts, expressed or implied, and give prudent advice.
- Avoid any conflict of interest, respect the trust that others put in you, and take only those jobs you are fully qualified to perform.
• Stay current on skills, and do not become involved with activities that could injure the reputation of other security professionals.

An interesting relationship exists between law and ethics. Most often, laws are based on ethics and are put in place to ensure that others act in an ethical way. However, laws do not apply to everything—that is when ethics should kick in. Some things may not be illegal, but that does not necessarily mean they are ethical.

Corporations should have a guide developed on computer and business ethics. This can be part of an employee handbook, used in orientation, posted, and made a part of training sessions.

Certain common ethical fallacies are used by many in the computing world to justify their unethical acts. They exist because people look at issues differently and interpret (or misinterpret) rules and laws that have been put into place. The following are examples of these ethical fallacies:

• Hackers only want to learn and improve their skills. Many of them are not making a profit off of their deeds; thus, their activities should not be seen as illegal or unethical.
• The First Amendment protects and provides the right for U.S. citizens to write viruses.
• Information should be shared freely and openly; thus, sharing confidential information and trade secrets should be legal and ethical.
• Hacking does not actually hurt anyone.

**The Computer Ethics Institute**

The Computer Ethics Institute is a nonprofit organization that works to help advance technology by ethical means.

The Computer Ethics Institute has developed its own Ten Commandments of Computer Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people’s computer work.
3. Thou shalt not snoop around in other people’s computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people’s computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people’s intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.
The Internet Architecture Board

The Internet Architecture Board (IAB) is the coordinating committee for Internet design, engineering, and management. It is responsible for the architectural oversight of the Internet Engineering Task Force (IETF) activities, Internet Standards Process oversight and appeal, and editor of Request for Comments (RFCs). Figure 10-5 illustrates the IAB’s place in the hierarchy of entities that help ensure the structure and standardization of the Internet. Otherwise, the Internet would be an unusable big bowl of spaghetti and we would all still be writing letters and buying stamps.

The IAB issues ethics-related statements concerning the use of the Internet. It considers the Internet to be a resource that depends upon availability and accessibility to be useful to a wide range of people. It is mainly concerned with irresponsible acts on the Internet that could threaten its existence or negatively affect others. It sees the Internet as a great gift and works hard to protect it for all who depend upon it. The IAB sees the use of the Internet as a privilege, which should be treated as such and used with respect.

Figure 10-5  Agencies responsible for maintaining order for the components of the Internet
The IAB considers the following acts as unethical and unacceptable behavior:

- Purposely seeking to gain unauthorized access to Internet resources
- Disrupting the intended use of the Internet
- Wasting resources (people, capacity, and computers) through purposeful actions
- Destroying the integrity of computer-based information
- Compromising the privacy of others
- Conducting Internet-wide experiments in a negligent manner

The IAB vows to work with federal agencies to take whatever actions are necessary to protect the Internet. This could be through new technologies, methods, or procedures that are intended to make the Internet more resistant to disruption. A balance exists between enhancing protection and reducing functionality. One of the Internet’s main purposes is to enable information to flow freely and not be prohibited; thus, the IAB must be logical and flexible in its approaches, and in the restrictions it attempts to implement. The Internet is everyone’s tool, so everyone should work together to protect it.

**Corporate Ethics Programs**

More regulations are requiring organizations to have an ethical statement and potentially an ethical program in place. This has been brought on by a lot of slimy things that have taken place in the past that were known about and encouraged by executive management, even if they don’t admit it. The ethical program is to serve as the “tone at the top,” which means that the executives need to not only ensure that their employees are acting ethically, but that they themselves are following their own rules. The main goal is to ensure that the motto “succeed by any means necessary” is not the spoken or unspoken culture of a work environment. Certain structures can be put into place that provide a breeding ground for unethical behavior. If the CEO gets more in salary based on stock prices, then he may find ways to artificially inflate stock prices, which can directly hurt the investors and shareholders of the company. If managers can only be promoted based on the amount of sales they bring in, these numbers may be fudged and not represent reality. If an employee can only get a bonus if a low budget is maintained, he might be willing to take shortcuts that could hurt company customer service or product development. Although ethics seem like things that float around in the ether and make us feel good to talk about, they have to be actually implemented in the real corporate world through proper business processes and management styles.

The *Federal Sentencing Guidelines for Organizations (FSGO)* created an outline for ethical requirements, and in some cases will reduce the criminal sentencing and liability if ethical programs are put in place. This was updated in 2004 with requirements that made it much more important for the senior executives and board members of an organization to actively participate and be aware of the ethics program in an organization. The intent is to enforce and foster a sense of due diligence that will detect criminal activity as well as protect against it and deter it from happening. Aspects of the Sarbanes-Oxley Act of 2002 are intended to function in much the same manner but with regards to accounting and truthfulness in corporate reporting.
References

- Internet Architecture Board  www.iab.org
- Computer Security Institute  www.gocsi.com
- Corp-Ethics  www.corp-ethics.com/
- Society of Corporate Ethics  www.corporatecompliance.org/CCN/ccn_vIII23.htm

Summary

Law, ethics, and investigations are very important parts of computer and information security. They are elements that do not usually come to mind when one speaks of information security, but they are a must if a society is serious about controlling this type of crime and punishing the guilty.

In many ways, the laws and courts are in their infancy stages when attempting to deal with computer crimes. They are faced with not having many precedents to fall back on when interpreting what is legal and illegal and what the proper punishments are for each type of computer crime. However, the legal system is quickly developing laws and providing ways to properly interpret them to help all law enforcement agencies and the victims. Over the last few years, hacking and attacking have been performed for fun, mainly by curious computer individuals, but as the punishments increase, such fun may quickly come to an end.

Security professionals should be aware of, and be well-versed in, computer security laws and regulations that apply in their environments. They should be able to properly inform their management and customers of expected responsibilities, as well as know what boundaries they are expected to work within themselves.

Quick Tips

- Dumpster diving refers to going through someone's trash to find confidential or useful information. It is legal, unless it involves trespassing, but in all cases it is considered unethical.
- Wiretapping is a passive attack that eavesdrops on communications. It is only legal with prior consent or a warrant.
- Social engineering is the act of tricking or deceiving a person into giving confidential or sensitive information that could then be used against him or his company.
- Civil Law System
  - Uses prewritten rules and is not based on precedence
  - Is different than civil (tort) laws, which works under a common law system
Common Law System
- Made up of criminal, civil, and administrative laws

Customary Law System
- Addresses mainly personal conduct, and uses regional traditions and customs as the foundations of the laws
- Is usually mixed with another type of listed legal system rather than being the sole legal system used in a region

Religious Law System
- Laws are derived from religious beliefs and address an individual’s religious responsibilities; commonly used in Muslim countries or regions

Mixed Law System
- Using two or more legal systems
- Data diddling is the act of willfully modifying information, programs, or documentation in an effort to commit fraud or disrupt production.
- Excessive privileges means an employee has more rights than necessary to complete her tasks.
- Criminal law deals with an individual’s conduct that violates government laws developed to protect the public.
- Civil law deals with wrongs committed against individuals or companies that result in injury or damages. Civil law does not use prison time as a punishment, but usually requires financial restitution.
- Administrative, or regulatory, law covers standards of performance or conduct expected by government agencies from companies, industries, and certain officials.
- A patent grants ownership and enables that owner to legally enforce his rights to exclude others from using the invention covered by the patent.
- Copyright protects the expression of ideas rather than the ideas themselves.
- Trademarks protect words, names, product shapes, symbols, colors, or a combination of these used to identify products or a company. These items are used to distinguish products from the competitors’ products.
- Trade secrets are deemed proprietary to a company and often include information that provides a competitive edge. The information is protected as long as the owner takes the necessary protective actions.
- Crime over the Internet has brought about jurisdiction problems for law enforcement and the courts.
- Privacy laws dictate that data collected by government agencies must be collected fairly and lawfully, must be used only for the purpose for which they were collected, must only be held for a reasonable amount of time, and must be accurate and timely.
If companies are going to use any type of monitoring, they need to make sure it is legal in their business sector and must inform all employees that they may be subjected to monitoring.

Employees need to be informed regarding what is expected behavior pertaining to the use of the company’s computer systems, network, e-mail system, and phone system. They need to also know what the ramifications are for not meeting those expectations. These requirements are usually communicated through policies.

Logon banners should be used to inform users of what could happen if they do not follow the rules pertaining to using company resources. This provides legal protection for the company.

Countries differ in their view of the seriousness of computer crime and have different penalties for certain crimes. This makes enforcing laws much harder across country borders.

The three main types of harm addressed in computer crime laws pertain to unauthorized intrusion, unauthorized alteration or destruction, and using malicious code.

Law enforcement and the courts have a hard time with computer crimes because of the newness of the types of crimes, the complexity involved, jurisdictional issues, and evidence collection. New laws are being written to properly deal with cybercrime.

If a company does not practice due care in its efforts to protect itself from computer crime, it can be found to be negligent and legally liable for damages.

Elements of negligence include not fulfilling a legally recognized obligation, failure to conform to a standard of care that results in injury or damage, and proximate causation.

Most computer crimes are not reported because the victims are not aware of the crime or are too embarrassed to let anyone else know.

Theft is no longer restricted to physical constraints. Assets are now also viewed as intangible objects that can also be stolen or disclosed via technological means.

The primary reason for the chain of custody of evidence is to ensure that it will be admissible in court by showing it was properly controlled and handled before being presented in court.

Companies should develop their own incident response team, which is made up of people from management, IT, legal, human resources, public relations, security, and other key areas of the organization.

Hearsay evidence is secondhand and usually not admissible in court.

To be admissible in court, business records have to be made and collected in the normal course of business, not specially generated for a case in court.
Business records can easily be hearsay if there is no firsthand proof of their accuracy and reliability.

- The life cycle of evidence includes identification and collection of the evidence, storage, preservation, transportation, presentation in court, and its return to the owner.
- Collection of computer evidence is a very complex and detail-oriented task. Only skilled people should attempt it; otherwise, evidence can be ruined forever.
- When looking for suspects, it is important to consider the motive, opportunity, and means (MOM).
- For evidence to be admissible in court, it needs to be relevant, sufficient, and reliable.
- Evidence must be legally permissible, meaning it was seized legally and the chain of custody was not broken.
- All evidence should be marked and stored in a container, which also should be marked.
- In many jurisdictions, law enforcement agencies must obtain a warrant to search and seize an individual’s property, as stated in the Fourth Amendment. Private citizens are not required to protect the Fourth Amendment rights of others unless acting as a police agent.
- Enticement is the act of luring an intruder and is legal. Entrapment induces a crime, tricks a person, and is illegal.
- The salami attack is executed by carrying out smaller crimes with the hope that the larger crime will not be noticed. The common salami attack is the act of skimming off a small amount of money.
- Phreakers are hackers who specialize in committing telephone fraud.
- After a computer system is seized, the investigators should make a bit mirror image copy of the storage media before doing anything else.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. Which of the following does the IAB consider unethical?
   A. Creating a computer virus
   B. Entering information into a web page
   C. Performing a penetration test on a host on the Internet
   D. Disrupting Internet communications
2. What is the study of computers and surrounding technologies and how they relate to crime?
   A. Computer forensics
   B. Computer vulnerability analysis
   C. Incident handling
   D. Computer information criteria

3. Which of the following does the IAB consider unethical behavior?
   A. Internet users who conceal unauthorized accesses
   B. Internet users who waste computer resources
   C. Internet users who write viruses
   D. Internet users who monitor traffic

4. After a computer forensics investigator seizes a computer during a crime investigation, what is the next step?
   A. Label and put it into a container, and then label the container.
   B. Dust the evidence for fingerprints.
   C. Make an image copy of the disks.
   D. Lock the evidence in the safe.

5. A CISSP candidate signs an ethics statement prior to taking the CISSP examination. Which of the following would be a violation of the (ISC)² Code of Ethics that could cause the candidate to lose his or her certification?
   A. E-mailing information or comments about the exam to other CISSP candidates
   B. Submitting comments on the questions of the exam to (ISC)²
   C. Submitting comments to the board of directors regarding the test and content of the class
   D. Conducting a presentation about the CISSP certification and what the certification means

6. If your company gives you a new PC and you find residual information about confidential company issues, what should you do based on the (ISC)² Code of Ethics?
   A. Contact the owner of the file and inform him about it. Copy it to a disk, give it to him, and delete your copy.
   B. Delete the document because it was not meant for you.
   C. Inform management of your findings so it can make sure this type of thing does not happen again.
   D. E-mail it to both the author and management so everyone is aware of what is going on.

7. Why is it difficult to investigate computer crime and track down the criminal?
A. Privacy laws are written to protect people from being investigated for these types of crimes.
B. Special equipment and tools are necessary to detect these types of criminals.
C. Criminals can hide their identity and hop from one network to the next.
D. The police have no jurisdiction over the Internet.

8. Protecting evidence and providing accountability for who handled it at different steps during the investigation is referred to as what?
   A. The rule of best evidence
   B. Hearsay
   C. Evidence safety
   D. Chain of custody

9. If an investigator needs to communicate with another investigator but does not want the criminal to be able to eavesdrop on this conversation, what type of communication should be used?
   A. Digitally signed messages
   B. Out-of-band messages
   C. Forensics frequency
   D. Authentication and access control

10. Why is it challenging to collect and identify computer evidence to be used in a court of law?
    A. The evidence is mostly intangible.
    B. The evidence is mostly corrupted.
    C. The evidence is mostly encrypted.
    D. The evidence is mostly tangible.

11. The chain of custody of evidence describes who obtained the evidence and
    ____________.
    A. Who secured it and stole it
    B. Who controlled it and broke it
    C. Who secured it and validated it
    D. Who controlled it and duplicated it

12. Before shutting down a system suspected of an attack, the investigator should do what?
    A. Remove and back up the hard drive
    B. Dump memory contents to disk
    C. Remove it from the network
    D. Save data in the spooler queue and temporary files
13. Why is computer-generated documentation usually considered unreliable evidence?
   A. It is primary evidence.
   B. It is too difficult to detect prior modifications.
   C. It is corroborative evidence.
   D. It is not covered under criminal law, but it is covered under civil law.

14. Which of the following is a necessary characteristic of evidence for it to be admissible?
   A. It must be real.
   B. It must be noteworthy.
   C. It must be reliable.
   D. It must be important.

15. In the United States, what agency usually works with the FBI when investigating computer crimes?
   A. (ISC)²
   B. The Secret Service
   C. The CIA
   D. The state police

16. If a company deliberately planted a flaw in one of its systems in the hope of detecting an attempted penetration and exploitation of this flaw, what would this be called?
   A. Incident recovery response
   B. Entrapment
   C. Illegal
   D. Enticement

17. If an employee is suspected of wrongdoing in a computer crime, what department must be involved?
   A. Human resources
   B. Legal
   C. Audit
   D. Payroll

18. When would an investigator’s notebook be admissible in court?
   A. When he uses it to refresh memory
   B. When he cannot be present for testimony
   C. When requested by the judge to learn the original issues of the investigations
   D. When no other physical evidence is available
19. Disks and other media that are copies of the original evidence are considered what?
   A. Primary evidence
   B. Reliable and sufficient evidence
   C. Hearsay evidence
   D. Conclusive evidence

20. If a company does not inform employees that they may be monitored and does not have a policy stating how monitoring should take place, what should a company do?
   A. Don’t monitor employees in any fashion.
   B. Monitor during off-hours and slow times.
   C. Obtain a search warrant before monitoring an employee.
   D. Monitor anyway—they are covered by two laws allowing them to do this.

21. What is one reason why successfully prosecuting computer crimes is so challenging?
   A. There is no way to capture electrical data reliably.
   B. The evidence in computer cases does not follow best evidence directives.
   C. These crimes do not always fall into the traditional criminal activity categories.
   D. Wiretapping is hard to do legally.

22. When can executives be charged with negligence?
   A. If they follow the transborder laws
   B. If they do not properly report and prosecute attackers
   C. If they properly inform users that they may be monitored
   D. If they do not practice due care when protecting resources

23. To better deal with computer crime, several legislative bodies have taken what steps in their strategy?
   A. Expanded several privacy laws
   B. Broadened the definition of property to include data
   C. Required corporations to have computer crime insurance
   D. Redefined transborder issues

24. Many privacy laws dictate which of the following rules?
   A. Individuals have a right to remove any data they do not want others to know.
   B. Agencies do not need to ensure that the data is accurate.
   C. Agencies need to allow all government agencies access to the data.
   D. Agencies cannot use collected data for a purpose different from what it was collected for.
25. Which of the following is not true about dumpster diving?
   A. It is legal.
   B. It is illegal.
   C. It is a breach of physical security.
   D. It is gathering data from places people would not expect to be raided.

Answers

1. D. The Internet Architecture Board (IAB) is a committee for Internet design, engineering, and management. It considers the use of the Internet to be a privilege that should be treated as such.
   The IAB considers the following acts unethical and unacceptable behavior:
   • Purposely seeking to gain unauthorized access to Internet resources
   • Disrupting the intended use of the Internet
   • Wasting resources (people, capacity, and computers) through purposeful actions
   • Destroying the integrity of computer-based information
   • Compromising the privacy of others
   • Negligence in the conduct of Internet-wide experiments

2. A. Computer forensics is a field that specializes in understanding and properly extracting evidence from computers and peripheral devices for the purpose of prosecution. Collecting this type of evidence requires a skill set and understanding of several relative laws.

3. B. This question is similar to question 1. The IAB has declared wasting computer resources through purposeful activities unethical because it sees these resources as assets that are to be available for the computing society.

4. C. Several steps need to be followed when gathering and extracting evidence from a scene. Once a computer has been confiscated, the first thing the computer forensics team should do is make an image of the hard drive. The team will work from this image instead of the original hard drive so it stays in a pristine state and the evidence on the drive is not accidentally corrupted or modified.

5. A. A CISSP candidate and a CISSP holder should never discuss with others what was on the exam. This degrades the usefulness of the exam to be used as a tool to test someone’s true security knowledge. If this type of activity is uncovered, the person could be stripped of their CISSP certification.

6. C. When dealing with the possible compromise of confidential company information or intellectual property, management should be informed and be involved as soon as possible. Management members are the ones who
are ultimately responsible for this data and who understand the damage its leakage can cause. An employee should not attempt to address and deal with these issues on his own.

7. C. Spoofing one’s identity and being able to traverse anonymously through different networks and the Internet increase the complexity and difficulty of tracking down criminals who carry out computer crimes. It is very easy to commit many damaging crimes from across the country or world, and this type of activity can be difficult for law enforcement to track down.

8. D. Properly following the chain of custody for evidence is crucial for it to be admissible in court. A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to establish that it is sufficiently trustworthy to be presented as evidence in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

9. B. Out-of-band communication means to communicate through some other type of communication channel. For example, if law enforcement agents are investigating a crime on a network, they should not share information through e-mail that passes along this network. The criminal may still have sniffers installed and thus be able to access this data.

10. A. The evidence in computer crimes usually comes straight from computers themselves. This means the data are held as electronic voltages, which are represented as binary bits. Some data can be held on hard drives and peripheral devices, and some data may be held in the memory of the system itself. This type of evidence is intangible in that it is not made up of objects one can hold, see, and easily understand. Other types of crimes usually have evidence that is more tangible in nature, and which is easier to handle and control.

11. C. The chain of custody outlines a process to ensure that under no circumstance was there a possibility for the evidence to be tampered with. If the chain of custody is broken, there is a high probability that the evidence will not be admissible in court. If it is admitted, it will not carry as much weight.

12. B. If the computer was actually attacked or involved in a computer crime, there is a good possibility that useful information could still reside in memory. Specific tools can be used to actually dump this information and save it for analysis before the power is removed.

13. B. It can be very difficult to determine if computer-generated material has been modified before it is presented in court. Since this type of evidence can be altered without being detected, the court cannot put a lot of weight on this evidence. Many times, computer-generated evidence is considered hearsay in that there is no firsthand proof backing it up.

14. C. For evidence to be admissible, it must be sufficient, reliable, and relevant to the case. For evidence to be reliable, it must be consistent with fact and must not be based on opinion or be circumstantial.
15. **B.** The FBI and Secret Service are both responsible for investigating computer crimes. They have their own jurisdictions and rules outlining who investigates which types of crimes.

16. **D.** Companies need to be very careful about the items they use to entice intruders and attackers, because this may be seen as entrapment by the court. It is best to get the legal department involved before implementing these items. Putting a honeypot in place is usually seen as the use of enticement tools.

17. **A.** It is imperative that the company gets human resources involved if an employee is considered a suspect in a computer crime. This department knows the laws and regulations pertaining to employee treatment and can work to protect the employee and the company at the same time.

18. **A.** Notes that are taken by an investigator will, in most cases, not be admissible in court as evidence. This is not seen as reliable information and can only be used by the investigator to help him remember activities during the investigation.

19. **C.** In most cases, computer-related evidence falls under the hearsay category, because it is seen as copies of the original data that are held in the computer itself and can be modified without any indication. Evidence is considered hearsay when there is no firsthand proof in place to validate it.

20. **A.** Before a company can monitor its employees, it is supposed to inform them that this type of activity can take place. If a company monitors an employee without telling him, this could be seen as an invasion of privacy. The employee had an expected level of privacy that was invaded. The company should implement monitoring capabilities into its security policy and employee security-awareness programs.

21. **C.** We have an infrastructure set up to investigate and prosecute crimes: law enforcement, laws, lawyers, courts, juries, judges, and so on. This infrastructure has a long history of prosecuting “traditional” crimes. Only in the last five years have computer crimes been prosecuted more regularly; thus, these types of crimes are not fully rooted in the legal system with all of the necessary and useful precedents.

22. **D.** Executives are held to a certain standard and are expected to act responsibly when running and protecting a company. These standards and expectations equate to the due care concept under the law. Due care means to carry out activities that a reasonable person would be expected to carry out in the same situation. If an executive acts irresponsibly in any way, she can be seen as not practicing due care and be held negligent.

23. **B.** Many times, what is corrupted, compromised, or taken from a computer is data, so current laws have been updated to include the protection of intangible assets, as in data. Over the years, data and information have become many companies’ most valuable asset, which must be protected by the laws.
24. D. The Federal Privacy Act of 1974 and the European Union Principles on Privacy were created to protect citizens from government agencies that collect personal data. These acts have many stipulations, including that the information can only be used for the reason for which it was collected.

25. B. Dumpster diving is the act of going through someone’s trash with the hope of uncovering useful information. Dumpster diving is legal if it does not involve trespassing, but it is unethical.