

Chapter 5

Legal Issues in Information Security

CRITICAL SKILLS

- 5.1** Understand U.S. Criminal Law
- 5.2** Understand State Laws
- 5.3** Understand Laws of Other Countries
- 5.4** Understand Issues with Prosecution
- 5.5** Understand Civil Issues
- 5.6** Understand Privacy Issues

There are many legal issues with regard to information security. The most obvious issue is that breaking into computers is against the law—well, most of the time it is. Depending on where you are in the world, the definition of a computer crime differs, as does the punishment for engaging in such activity. No matter how the activity is defined, if the perpetrators of the crime are to be punished, information security professionals must understand how to gather the information necessary to assist law enforcement in the capture and prosecution of the individuals responsible.

However, computer crime is not the only issue that must be dealt with by information security professionals. There are also the civil issues of liability and privacy that must be examined. Organizations must understand their risks with regard to employees and other organizations on the network if internal security is lax. New laws have been passed that address banking customers and medical privacy. Violations of these laws may pose a significant risk to an organization, including criminal penalties. All of these issues must be understood and examined by information security professionals in conjunction with the legal advisors of the organization.

**NOTE**

I am not an attorney and this chapter is not meant to be legal advice. The purpose of this chapter is to highlight some of the legal issues surrounding information security. Laws change over time and thus it is best to consult your organization's general counsel on all legal issues.

CRITICAL SKILL**5.1**

Understand U.S. Criminal Law

The United States criminal law forms the basis for computer crime investigations by federal authorities (mainly the FBI and the Secret Service). While 18 US Code 1030 is the primary computer crime statute, other statutes may form the basis for an investigation. The following sections discuss the statutes that are most often used. For the applicability of these statutes to a particular situation or organization, please consult your organization's general counsel.

Computer Fraud and Abuse (18 US Code 1030)

As I mentioned, **18 US Code 1030** forms the basis for federal intervention in computer crimes. There are a few things about the statute that should be understood by security professionals, beginning with the types of computer crime that are covered by the statute.

Section (a) of the statute defines the crime as the intentional access of a computer without authorization to do so. A second part of the statute adds that the individual accessing the computer has to obtain information that should be protected. Close reading of this statute gives the impression

that only the computers of the U.S. government or financial institutions are covered. However, later in the text, **protected computers** is defined to include computers used by financial institutions, the U.S. government, or any computer used in interstate or foreign commerce or communication.

Based on this definition, most of the computers connected to the Internet will qualify, as they may be used in interstate or foreign commerce or communication. One other important point must be made about 18 US Code 1030: there is a minimum amount of damage that must occur before this statute may be used. The damage amount is \$5,000, but this may include the costs of investigating and correcting anything done by the individual who gains unauthorized access. It should also be noted that the definition of damage does not include any impairment to the confidentiality of data even though Section (a) does discuss disclosure of information that is supposed to be protected by the government.

This statute then does not specifically prohibit gaining access to a computer if the damage that is done does not exceed \$5,000. Other activity that is commonly performed by intruders may not be illegal. For example, it was ruled in Georgia (see *Moulton v. VC3, N.D. Ga.*, Civil Action File No. 1:00-CV-434-TWT, 11/7/00) that scanning a system did not cause damage and thus could not be punished under federal or Georgia state law.

**NOTE**

18 US Code 1030 was modified by the Patriot Act. This act is discussed later in this chapter.

Credit Card Fraud (18 US Code 1029)

Many computer crimes involve the stealing of credit card numbers. In this case, **18 US Code 1029** can be used to charge the individual with a federal crime. The statute makes it a crime to possess fifteen or more counterfeit credit cards.

An attack on a computer system that allows the intruder to gain access to a large number of credit card numbers to which he does not have authorized access is a violation of this statute. The attack will be a violation even if the attack itself did not cause \$5,000 in damage (as specified in 18 US Code 1030) if the attacker gains access to fifteen or more credit card numbers.

Copyrights (18 US Code 2319)

18 US Code 2319 defines the criminal punishments for copyright violations where an individual is found to be reproducing or distributing copyrighted material where at least ten copies have been made of one or more works and the total retail value of the copies exceeds \$1,000 (\$2,500 for harsher penalties). If a computer system has been compromised and used

as a distribution point for copyrighted software, the individual who is providing the software for distribution is likely in violation of this statute. Again, this is regardless of whether the cost of the compromise exceeded \$5,000.

**NOTE**

The victim of this crime is not the owner of the system that was compromised but the holder of the copyright.

Interception (18 US Code 2511)

18 US Code 2511 is the wiretap statute. This statute outlaws the interception of telephone calls and other types of electronic communication and prevents law enforcement from using wiretaps without a warrant. An intruder into a computer system that places a “sniffer” on the system is likely to be in violation of this statute, however.

A reading of this statute may also indicate that certain types of monitoring performed by organizations may be illegal. For example, if an organization places monitoring equipment on its network to examine electronic mail or to watch for attempted intrusions, does this constitute a violation of this statute? Further reading in this statute shows that there is an exception for the provider of the communication service. Since the organization is the provider of the service, any employee of the organization can monitor communication in the normal course of his or her job for the “protection of the rights or property of the provider of that service.” This means that if it is appropriate for the organization to monitor its own networks and computer systems to protect them, that action is allowed under this law.

**TIP**

Make sure that your organization’s internal policies and procedures cover the monitoring of the network. The policies and procedures should identify which employees are authorized to perform this monitoring and also inform all employees that such monitoring will take place (see the section “Understand Privacy Issues” of this chapter for more information).

Access to Electronic Information (18 US Code 2701)

18 US Code 2701 prohibits unlawful access to stored communications, but it also prohibits preventing authorized users from accessing systems that store electronic communications. This statute also has exceptions for the owner of the service so that the provider of the service may access any file on the system. This means that if an organization is providing the communications service, any file on the system can be accessed by authorized employees of the organization.

Other Criminal Statutes

When a crime occurs through the use of a computer, violations of computer crime laws are not the only statutes that can be used to charge the perpetrator. Other laws such as mail and wire fraud can and are also used. Keep in mind as well that a computer may be used to commit a crime totally unrelated to computer crimes. The computer or the information stored on it may constitute evidence in the case, or the case may be investigated using computers as a means to the end.

Patriot Act

The **USA-Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)** was passed in response to the terrorist attacks of September 11, 2001. Several parts of the act have a direct impact on the federal computer crime statutes. These impacts are discussed below.

Changes to 18 US Code 1030

The Patriot Act increased the maximum penalties for violations of 18 US Code 1030 to ten years for the first offense and twenty years for subsequent offenses. With the new law, state offenses will count as prior offenses for sentencing.

One of the biggest issues with the original 18 US Code 1030 was the requirement to show \$5,000 worth of damage. The Patriot Act modifies the wording of this section of the law to define damage as “any impairment of the integrity or availability of data, a program, a system, or information.” This simple change makes reaching the \$5,000 minimum much easier. The new version of the law also allows for the combination of damages to multiple systems as long as the events or attacks occurred within a one-year time frame.

The term “loss” is also broadened to include any reasonable cost to the victim. This includes the cost of responding, determining the damage, and restoring the systems to operation. Also included are revenue losses or other costs due to an interruption of service. This change will also make it easier to reach the \$5,000 minimum.

A new offense has been added to 18 US Code 1030. An individual has violated federal law if the actions taken affect a computer system used by the government for justice, national defense, or national security regardless of the loss incurred. With this change, it is no longer required to compute damages for attacks against Department of Defense computer systems.

Finally, an individual in the United States who attacks computers outside of the United States can be prosecuted under federal law. This change means that such attacks are now included under 18 US Code 1030.

Trap and Trace Changes

In the past, the Pen Register Statute (18 US Code 3127) allowed law enforcement to gain access to the phone numbers that were called from a particular telephone. This statute did not allow for access to the content of the phone call but only the numbers that were called. The statute had very specific technical language that limited the information that could be obtained to telephone numbers.

The Patriot Act of 2001 modified the language of the law to include any device or process that records dialing, routing, addressing, or signaling information. The act does continue the prohibition on the recording of content. With these changes, it is possible to collect the following information:

- E-mail header information
- Source and destination IP addresses
- Source and destination TCP and UDP port numbers

The law still prohibits the collection of:

- E-mail subject lines
- Contents of e-mail
- Contents of downloaded files

One other change that will make it easier for law enforcement to investigate a crime is that trap and trace orders can now be obtained locally for devices that exist in another district. For example, an investigation in New York could obtain an order in New York that would be valid for information collection in California. The only restriction is that the court issuing the order must have jurisdiction over the offense.

Computer Trespass Exception

In the past, law enforcement was hampered in its ability to monitor the activities of an intruder. In order to help a victim monitor such activities, law enforcement would have to obtain a wiretap order even if the victim gave consent. The Patriot Act modifies both 18 US Code 2511 and 18 US Code 2701. The modifications to 18 US Code 2511 note that a person who is not authorized to access a system will have no **expectation of privacy**. In addition, the new law states that an interception requires the following:

- Consent of the owner must be given.
- It must be relevant to an investigation.
- The interception cannot acquire communications other than to/from the trespasser.

The Cable Act Fix

Since cable companies are now providing Internet access, there was a perceived conflict between the needs of law enforcement when investigating computer crimes and the law regarding disclosure of what cable customers are watching and/or doing online. The Patriot Act addresses this conflict by allowing the disclosure of wiretap and trap and trace evidence to law enforcement under the same statutes identified above (18 US Code 3127).

Homeland Security Act

The **Homeland Security Act** of 2002 (specifically the **Cyber Security Enhancement Act** of 2002 found in the document at section 225) describes issues regarding information security. The majority of the act is directed at the creation of the Department of Homeland Security; however, Section 225 does modify 18 US Code 1030 by increasing penalties for criminal acts. It also directs the United States Sentencing Commission to take into account the severity of the computer crime when determining sentencing guidelines.

CRITICAL SKILL

5.2

Understand State Laws

In addition to federal computer crime statutes, every state has also developed computer crime laws. These laws differ from the federal laws with regard to what constitutes a crime (many do not have any minimum damage amount) and how the crime may be punished. Depending on where the crime occurred, local law enforcement may have more interest in the case than the federal authorities. Be sure to speak with your local law enforcement organization to understand their interest in and their capabilities to investigate computer crime.

Remember that state laws may change frequently and computer crime is an area of continued research and development. If you have specific questions about a particular statute, consult your organization's general counsel or local law enforcement.

The concept of what constitutes a crime varies from state to state. Some states require that there must be an intent to permanently deprive the owner of access to information for computer theft to occur. Other states require that the owner of the information must actually be deprived of the information, so a backup of the information might negate the violation of the law.

There is also a big difference when it comes to accessing systems. Some states require that the system must actually be accessed for the crime to occur. Other states make the unauthorized attempt to be the crime. On the other hand, Utah allows organizations to attack back at the computer system that is attempting to breach their security.

Finally, some states consider modifying or forging of e-mail headers to be a crime. This type of statute is directed at bulk e-mail or spam.

No matter what state your organization is in, check with local law enforcement and with your organization's general counsel so that you understand the ramifications of the local laws. This will directly affect when you choose to notify law enforcement of a computer incident.



Progress Check

1. What is the title of the primary computer crime law in the United States?
 2. What part of the United States computer crime statutes did the Patriot Act modify that will make it easier to prosecute computer crimes in federal court?
-

CRITICAL SKILL**5.3**

Understand Laws of Other Countries

Computer crime laws in the United States vary from state to state. Internationally, laws vary from country to country. Many countries have no computer crime laws at all. For example, when the ILOVEYOU virus was traced to an individual who lived in the Philippines, he could not be prosecuted because the Philippines did not have a law that made it a crime to write and distribute a computer virus (since then, a computer crime law has been enacted).

Computer crime laws in other countries may have an effect on computer crime investigations in the United States as well. If an investigation shows that the attack came from a computer system in another country, the FBI will attempt to get assistance from the law enforcement organizations in that country (through the legal liaison at the U.S. embassy in that country). If the other country has no computer crime laws, it is unlikely that they will assist in the investigation.

The following sections provide brief discussions of computer crime laws in other countries. More specific information can be found by asking representatives of the foreign government (at an embassy or consulate) or by contacting the FBI.

Australia

Australian federal law specifies that unauthorized access to data in computers is a crime punishable by six months in jail (see Commonwealth Laws, Crimes Act 1914, Part VIA—Offences Relating to Computers). The punishment goes up to two years if the intent was to defraud or if the information was government-sensitive, financial, or trade secrets. It is also against the law for someone to gain unauthorized access to computers across facilities provided by the Commonwealth or by a carrier. No minimum damage amounts are specified. The punishment is based on the type of information that is accessed.

1. Computer Fraud and Abuse, 18 US Code 1030

2. The Patriot Act modified the way damage was assessed in computer crimes, thus making it easier to reach the \$5,000 damage minimum required for a violation of federal law.

Brazil

Brazil has identified two crimes: entry of false data into information systems and the unauthorized modification or alteration of an information system. Both are directed at employees of organizations who misuse their access to commit a crime. Punishments range from three months to twelve years of confinement and may include fines.

India

Hacking with a computer system is defined as a crime in India. To be guilty of this crime, an individual must be involved with destroying, deleting, or altering information on a computer system so that it diminishes its value. The individual must also have the intent to cause damage or must know that he is likely to cause the damage. If convicted, the penalty is up to three years confinement, a fine, or both.

The punishment does not change with the damage caused to the system or the type of information that is accessed.

The People's Republic of China

Decree No. 147 of the State Council of the People's Republic of China, February 18, 1994 defines two computer crimes. The first is for deliberately inputting a computer virus into a computer system. The second is for selling special safety protection products for computers without permission. In either case, the penalty is a fine and possible confiscation of the illegal income.

Hong Kong has a different set of computer crime laws. Telecommunication Ordinance: Section 27A defines unauthorized access to a computer via a telecommunication system as a crime. If a person accesses a computer without authorization over a telecommunications system, they are guilty of this crime. A conviction will incur a large fine. It is also a crime to access a computer with criminal or dishonest intent. This intent may be for dishonest gain or to cause loss. Upon conviction for this offense, the individual may be imprisoned for up to five years.



The People's Republic of China has preserved many laws in Hong Kong as they were before it was returned to China. However, the laws in force in Hong Kong may change over time.

United Kingdom

Computer crime statutes for the United Kingdom can be found in the Computer Misuse Act 1990, Chapter 18. The law defines unauthorized access to computer material as a crime. This access

has to have intent, and the individual who performs the act must know that the access is unauthorized. It is also a crime to cause unauthorized modifications or to cause a denial-of-service condition. The penalties for any modification or denial of service do not change based on whether the attack is temporary or permanent.

For a summary conviction, the penalties are up to six months in prison or a fine. If the individual is convicted on an indictment, the prison term may not exceed five years and there may also be a fine.

CRITICAL SKILL**5.4**

Understand Issues with Prosecution

If your organization is the victim of computer crime, your organization might choose to contact law enforcement in order to prosecute the offenders. This choice should not be made in the heat of the incident. Rather, detailed discussion of the options and how the organization may choose to proceed should be discussed during the development of the organization's incident response procedure (see Chapter 6). During the development of this procedure, your organization should involve legal counsel and also seek advice from local law enforcement. Your discussion with local law enforcement will provide information on their capabilities, their interest in computer crimes, and the type of damage that must be done before a crime actually occurs.

**NOTE**

When an incident occurs, your organization's general counsel should be consulted before law enforcement is contacted.

Evidence Collection

Whether your organization chooses to prosecute or not, there are a number of things that can be done while the incident is investigated and the systems are returned to operation, including **evidence collection**. First, we should dispel one myth that is prevalent in the security industry. The myth is that special precautions must be taken to preserve evidence if the perpetrator is to be prosecuted and if any of the information from the victim can be used in the prosecution.

There are actually two parts to the correct information regarding this situation. First, if normal business procedures are followed, any information can be used to prosecute the perpetrator. This means that if you normally make backups of your systems and those backups contain information that shows where the attack came from or what was done, this information can be used. In this case, no special precautions need to be taken to safeguard the information as evidence. That is not to say that making extra copies before system administrators do anything to fix the system is not a good idea. However, it is not necessary.

**NOTE**

Technically, information is not evidence until a law enforcement officer takes possession of it. Therefore, what you may be doing is safeguarding the integrity of the information rather than protecting evidence.

The second point is a little trickier. If your organization takes actions such as calling an outside consultant to perform a forensic examination of the system, you are now taking actions that are not part of normal business practices. In this case, your organization should take appropriate precautions. These may include any of the following:

- Making at least two image copies of the computer's hard drives
- Limiting access to one of the copies and bagging it so that any attempts to tamper with it can be identified
- Making secure checksums of the information on the disks so that changes to the information can be identified

In any case, the procedure to be followed should be developed prior to the event and should be created with the advice of organization counsel and law enforcement.

One other point to consider is that information on the victim computer system may not be the only location for information about the attack. Log files from network equipment or network monitoring systems may also provide information about the attack.

**NOTE**

While it may be possible to use information gathered from normal processes as evidence in court, the information must still be gathered through good procedures. For example, if you don't have good backup procedures, the backups may not help you at all. If there is any doubt about the information that you will collect, calling in a forensics expert or law enforcement is always a good idea.

Contacting Law Enforcement

You should get your organization's general counsel involved before law enforcement is contacted. The general counsel should be available to speak with law enforcement when they come on-site.

Once law enforcement is contacted and comes on-site to investigate, the rules change. Law enforcement will be acting as officers of the court and as such are bound by rules that must be followed in order to allow information that is gathered to be used as evidence. When law enforcement takes possession of backup copies or information from a system, they will control access to it and protect it as evidence according to their procedures.

Ask the Expert

Q: If I am monitoring my network, am I in violation of the wiretap laws?

A: Since the organization is the owner and operator of the computer network, this information can be gathered without violating the wiretap laws (18 US Code 2511 and 2701). In fact, this situation is a specific exemption under both of these statutes.

Likewise, if further information is to be gathered from the network, law enforcement will have to get a subpoena or a warrant to gather more information. This document will either allow them to request logs from a service provider or to install monitoring equipment of their own. Without the warrant they will not be able to gather information off the network. Here again, they will follow their own procedures.



Law enforcement does not require a warrant if the information is provided willingly (by the organization, for example). However, if law enforcement wants information from your site, it may be more appropriate for your organization to require a subpoena as this may protect you from some liability. This may be necessary if you are an ISP and law enforcement requires your logs of an activity that traversed your network. In any case, a request for tapes or logs from law enforcement should be run through your organization's legal office.

CRITICAL SKILL

5.5 Understand Civil Issues

Anyone can file a civil lawsuit against anyone for anything. There is the potential for civil lawsuits when it comes to computers and the information they store. In this section, I will identify some of the potential exposures that organizations may encounter. However, none of the following is intended to provide legal advice. For all legal advice, you should see your own attorney or the organization's general counsel.

Employee Issues

Computers and computer networks are provided by an organization for the business use of employees. This simple concept should be spelled out to all employees (see Chapter 6 for a discussion of computer use policies). This means that the organization owns the systems and

the network, and any information on the systems may be accessed by the organization at any time. Therefore, employees should have no expectation of privacy. To make sure that your policy on this matter complies with applicable laws, make sure the organization's general counsel is involved in the drafting of the policy. Privacy laws differ from state to state.

Internal Monitoring

As the provider of the network and computer services, the organization is permitted to monitor information on the network and how the network is used (as stated before, this is an exception to the wiretap laws). Employees should be informed that **internal monitoring** may occur, and this should be communicated to them in a policy and when they login through a login banner. A banner such as this may be appropriate:

This system is owned by <organization name> and provided for the use of authorized individuals. All actions on this computer or network may be monitored. Anyone using this system consents to this monitoring. There is no expectation of privacy on this system. All information on this or any organization computer system is the property of <organization name>. Evidence of illegal activities may be turned over to the proper law enforcement authorities.

Policy Issues

Organization policy defines the appropriate operation of systems and behavior of employees. If employees violate organization policy, they may be disciplined or terminated. To alleviate some potential legal issues, all employees should be provided copies of organization policies (including information and security policies) and asked to sign that they have received and understood the policies. This procedure should reoccur periodically (such as every year) so the employees are reminded of the existing policies. These policies should restate the information in the login banner (no expectation of privacy, monitoring will happen, and so on).

Some employees may be reluctant to sign such documents. This activity should be coordinated with the Human Resources department and with the organization's general counsel.

Downstream Liability

A risk that should be taken into account when performing a risk assessment of an organization is the potential for **downstream liability**. The concept is that if an organization (Organization A) does not perform appropriate security measures and one of their systems is successfully penetrated, this system might then be used to attack another organization (Organization B). In this case, Organization A might be held liable by Organization B (see Figure 5-1). The question will be whether Organization A took reasonable care and appropriate measures to prevent this from occurring.

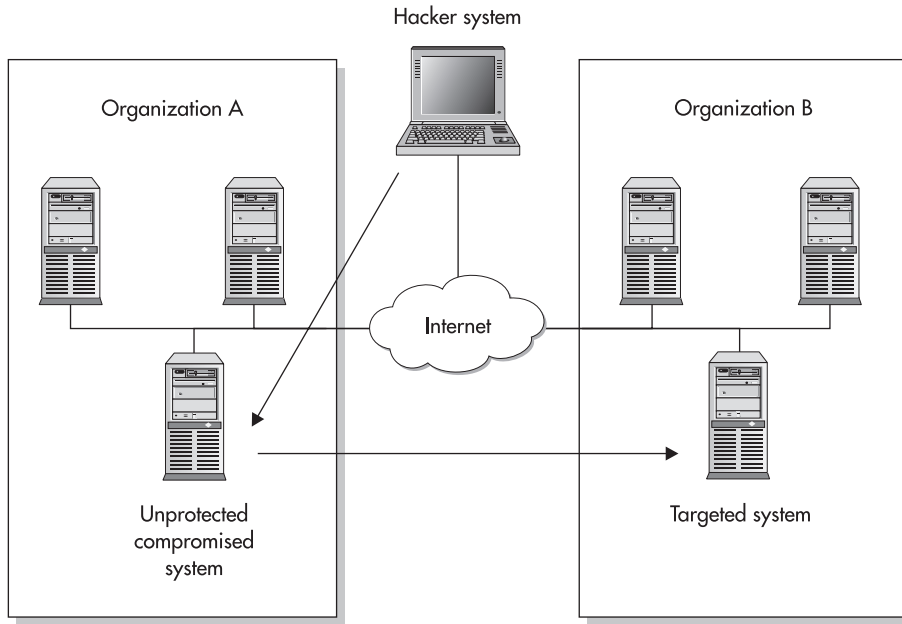


Figure 5-1 Downstream liability

Reasonable care and appropriate measures will be determined by existing standards (such as ISO 17799) and best business practices (see Chapter 9). Once again, the information security staff of the organization should discuss this issue with the organization's general counsel.

CRITICAL SKILL

5.6

Understand Privacy Issues

Privacy issues on the Internet are becoming a hot topic. We have already touched on the privacy issues when dealing with employees. This is not the only privacy issue that needs to be examined and handled properly. In the past few years, the federal government has enacted privacy legislation for banking and financial services as well as healthcare.

Customer Information

Customer information does not belong to you or your organization. Customer information belongs to the customer. Therefore, the organization should take appropriate steps to safeguard customer information from unauthorized disclosure. This is not to say that customer information cannot

be used, but care must be taken to make sure that customer information is used appropriately. This is one reason why many Internet sites notify the customer that some information may be used in mailing lists. Customers may also be given the option to keep their information from being used in this manner.

The issue that I wish to raise here is customer information being disclosed if the security of an organization is compromised. How can an organization decide if they have taken appropriate steps to prevent this type of disclosure? As with liability, the information security staff must work with the organization's general counsel to understand the issues involved and to identify the appropriate measures to take.

Health Insurance Portability and Accountability Act

On August 21, 1996, the **Health Insurance Portability and Accountability Act (HIPAA)** became law. This law places the responsibility for creating and enforcing the standards for the protection of health information under the Department of Health and Human Services. The act calls for the standardization of patient health information, unique identifiers for individuals, and most importantly, security standards for protecting the confidentiality and integrity of patient health information.

On February 20, 2003, the Department of Health and Human Services published the final HIPAA security regulations. The rules go into effect 60 days after publication (April 20, 2003). The compliance dates for various types of organizations are as follows:

- Health plans: April 20, 2005
- Small health plans (plans with annual receipts of \$5 million or less): April 20, 2006
- Health care clearinghouses: April 20, 2005
- Health care providers: April 20, 2005

Addressable vs. Required Components

The final security rule introduces the concept of “addressable” components. While many of the regulations in the rule are required (that is, they must be implemented by the organization), some of the regulations are listed as addressable by the organization.

If part of the regulation includes addressable items, the organization must assess whether the regulation is a reasonable and appropriate safeguard based on the organization's environment. If the regulation is determined to be reasonable and appropriate, the organization must implement the regulation. If not, the organization must document why the regulation is not reasonable or appropriate and implement an alternative mechanism.

Requirements of the Security Rule

The security rule sets out several general regulations and then provides detailed regulations in five specific areas:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational requirements
- Policies, procedures, and documentation requirements

The overall goal of these regulations is to ensure that the confidentiality, integrity, and availability of protected health information (PHI) is maintained. The regulations also encourage the organization to use a good risk management approach when determining the specific mechanisms to meet the requirements of the regulation.

Any organization that handles health care information should examine the regulations in detail to learn what must be done to be in compliance with the regulations. It is expected that health care organizations will expend significant resources in bringing their systems and procedures up to the regulations. The information security staff will need to work with the HIPAA compliance officer and the organization's general counsel to make sure the organization meets the requirements.

Administrative Safeguards

The HIPAA rule requires that each organization have the following administrative safeguards:

- **Security management process** The following components are required: a regular risk analysis, appropriate security measures to manage risk, a sanction policy for enforcement, and the regular review of security log and activity information.
- **Assigned security responsibility** It is required that an individual must be assigned the responsibility for security.
- **Workforce security** The following components are addressable by the organization: procedures for authorization, workforce clearance procedures, and termination procedures.
- **Information access management** The following component is required: isolating the health care clearinghouse function. The following components are addressable by the organization: access authorization procedures and access establishment and modification procedures.
- **Security awareness and training** The following components are addressable by the organization: periodic security updates, protection from malicious software, log-in monitoring, and password management.

- **Security incident procedures** Policies and procedures to address security incidents are required.
- **Contingency plans** The following components are required: a data backup plan, a disaster recovery plan, and an emergency mode operation plan. The following components are addressable by the organization: periodic testing and revisions of the contingency plans and the assessment of the relative criticality of specific applications.
- **Evaluation** Each organization is required to perform periodic evaluations of the security in place in response to changes in operations or environmental changes.
- **Business associate contracts and other arrangements** It is required that contracts requiring appropriate security must be in place with any organization that shares PHI.

Physical Safeguards

The HIPAA security rule shows an understanding that computer and network security are affected by the overall physical security safeguards that are used within the organization. The rule, therefore, includes significant requirements for physical security. These include

- **Facility access controls** The following components are addressable by the organization: procedures for contingency plans, facility security plan, access control and validation procedures, and procedures for recording repairs and modifications to the physical security of the facility.
- **Workstation use** Policies are required that specify the physical attributes of workstations that can access PHI.
- **Workstation security** Physical security safeguards are required for all workstations that can access PHI.
- **Device and media controls** The following components are required: procedures for the disposal of PHI and the media on which it was stored and for the removal of PHI before media can be reused. The following components are addressable by the organization: records of the movement of hardware and media and the backing up of PHI before equipment is moved.

Technical Safeguards

The HIPAA security rule includes five technical areas. The specific security mechanism that an organization chooses to meet a requirement may vary depending on the risk assessments that the organization performs (as well as other factors). The five areas are

- **Access control** The following components are required: each user must be assigned a unique identifier and emergency access procedures must be implemented. The following components are addressable by the organization: automatic logoff and encryption/decryption of PHI.

- **Audit controls** Mechanisms are required to be implemented that record and examine activity on any system that contains PHI.
- **Integrity** Each organization must address the need for a mechanism to authenticate electronic PHI.
- **Person or entity authentication** It is required that mechanisms be put in place to authenticate the identity of individuals who seek access to PHI.
- **Transmission security** The following components are addressable by the organization: mechanisms to detect unauthorized modifications of PHI while in transit and mechanisms to encrypt PHI whenever appropriate.

Organizational Requirements

The HIPAA security rule has organizational requirements that will force organizations to make changes to partner and sponsor contracts. Any contracts with organizations that will be able to access PHI must include provisions for security as outlined in this rule. In addition, health plan documents must provide for the sponsor to take appropriate security measures to protect PHI.

Policies, Procedures, and Documentation Requirements

Each organization is required to maintain the proper policies, procedures, and documentation. It is required that all documentation be kept for six years from the date of creation. It is also required that all policies and procedures be made available to those individuals who will be implementing the mechanisms. The policies and procedures of the organization are required to be updated as needed in response to changes in environmental or operational requirements.

The Graham-Leach-Bliley Financial Services Modernization Act

The **Graham-Leach-Bliley Financial Services Modernization Act (GLBA)** was signed into law on November 12, 1999. One of the key aspects of this act is related to the privacy of customer information. To address this issue, the act (in Subtitle A of Title V) imposes an affirmative duty to protect the private information of customers. Specifically, Section 502 of the act prohibits the financial organization from disclosing a customer's private information unless the organization has disclosed that this may occur and given the customer a chance to opt out of the disclosure.

In addition to the privacy issue, financial institutions are also required to protect customer records from unauthorized disclosure. This has led the financial oversight agencies (Office of Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision) to publish a joint rule on what exactly is required. This document is called "Interagency Guidelines Establishing Standards for Safeguarding

Customer Information” and is available at http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf.

Security Program Requirements

The guidelines impose requirements on the financial organization’s security program as a whole. These include

- **Information security program** Each organization must implement a comprehensive written information security program. This program must include administrative, technical, and physical safeguards.
- **Board involvement** The board of the organization must approve the written program and oversee development, implementation, and continued maintenance.
- **Assessing risk** Each organization must conduct periodic risk assessments that identify threats and vulnerabilities.

Managing and Controlling Risk

With the security program in place, the organization must continue to manage and control risk through the implementation of security mechanisms. The following mechanisms are specifically identified:

- Access controls on information
- Physical access restrictions on systems and records
- Encryption of sensitive information in transit
- System change procedures so system modifications do not adversely affect security
- Dual control procedures, segregation of duties, and background checks
- Intrusion detection systems to monitor attacks
- Incident response procedures to identify actions if an attack occurs
- Environmental protection to protect against the destruction of records

The guidelines also require that the organization’s staff be trained to implement the program and that regular tests be conducted to determine the program’s effectiveness.



The testing of the program should be conducted by independent parties. This does not mean that the organization cannot conduct its own tests, however.

Overseeing Service Provider Arrangements

GLBA takes into consideration the security issues involved with outside third parties who perform various services for financial organizations. Depending on the organization, the outside third parties may have significant access to sensitive information and thus must be examined in a similar manner to the organization itself. The guidelines identify the following requirements:

- **Due diligence in selecting service providers** The organization must exercise appropriate **due diligence** when selecting outside third parties to provide services.
- **Requiring service providers to implement security** The organization must require its service providers to implement appropriate security measures. This is to be done via contract.
- **Monitoring service providers** The organization is to monitor the outside third parties to determine that they have met their obligations under the contract.
- **Adjusting the program** The organization must make adjustments to its information security program to take into account changes in technology, threats, and business arrangements.
- **Reporting to the board** The organization must make periodic reports to its board regarding the state of its security program.

Project 5 Prosecute the Offender

This project is intended to show how the computer crime laws can be applied to an attack. We will use the work done on Project 2 as a starting point.

Step by Step

1. Locate the attack strategy that you created for Project 2.
2. Assuming that the attack was successful, identify which federal computer crime statutes would be violated by the attack. Don't forget to estimate the total damage suffered by your organization.
3. Now identify which systems would be used to develop evidence of the attack. What evidence would exist?
4. Identify how this evidence would be protected.
5. Determine if you would be able to identify the source of the attack.

Project Summary

The most obvious statute to be violated will be 18 US Code 1030. However, this statute requires a \$5,000 minimum damage amount so your organization will need to figure out how much the attack would cost. When you are looking at the systems that are attacked, don't forget the issues related to credit card or copyright information. Compromising such information might invoke other crime statutes.

Chapter 5 Review

Chapter Summary

After reading this chapter, you should understand the following facts about legal issues in information security.

Understand U.S. Criminal Law

- United States criminal law forms the basis for computer crime investigations by federal authorities (mainly the FBI and Secret Service).
- 18 US Code 1030 covers the primary crimes that apply to computer systems (computer fraud and abuse) for crimes that cause a minimum damage of \$5,000.
- An attacker who steals 15 or more credit card numbers can be charged under 18 US Code 1029.
- 18 US Code 2319 covers the punishments of copyright law. If a compromised computer is used as a distribution point for the copyrighted software, the person providing the distribution software is likely in violation of this statute.
- The wiretap statute (18 US Code 2511) prohibits the interception of telephone calls and electronic communications, with an exception of providers of the communication service monitoring the service for protection.
- Policies and procedures should identify which employees are authorized to perform monitoring and inform all employees that monitoring will take place.
- 18 US Code 2701 prohibits unlawful access to electronic information and prohibits preventing authorized users from accessing systems that store electronic communications.
- In addition to computer crime laws, other laws such as mail and wire fraud can be used to charge perpetrators who commit crimes through the use of computers.

- The USA-Patriot Act was passed in response to the terrorist attacks of September 11, 2001, and made changes or additions to several federal crime statutes.
- The Patriot Act increased penalties and modified wording of 18 US Code 1030; changed 18 US Code 3127 to allow law enforcement to gain information from devices in addition to telephones and obtain trap and trace orders for devices in other districts; modified 18 US Code 2511 and 18 US Code 2701 to allow for computer trespass exception, and provided the Cable Act Fix to address the issue of cable companies providing Internet access.
- The Homeland Security Act of 2002 established the creation of the Department of Homeland Security and also toughened the penalties for criminal acts and directed that the severity of the computer crime be taken into consideration during sentencing.

Understand State Laws

- Every state has computer crime laws, which change frequently as computer crime evolves.
- State laws differ from state to state.
- You should always consult with your company's general counsel and local law enforcement in determining local policies and procedures.

Understand Laws of Other Countries

- International laws vary from country to country.
- Many countries do not have computer crime laws.
- If a crime is committed in the United States by a perpetrator in another country, the FBI will attempt to get assistance from law enforcement organizations in that country, but prosecuting the crime may be difficult.
- Australia laws specify that unauthorized access to data in computers is a crime.
- Brazil has laws that are directed at employees who misuse their access to commit a crime.
- India defines hacking with a computer system as a crime.
- The People's Republic of China defines two computer crimes: inputting a virus into a computer system and selling safety protection software without permission. Hong Kong has a different set of computer laws that punish unauthorized access to computers.
- United Kingdom laws define unauthorized access to computer material with an intent, causing unauthorized modifications, and causing denial of service as crimes.

Understand Issues with Prosecution

- If your organization is the victim of a computer crime, always consult your organization's general counsel before contacting law enforcement.
- Any information collected during normal business procedures can be used to prosecute a perpetrator (for example, system backups).

- Develop a procedure with the advice of your organization's counsel and law enforcement before taking action beyond normal business practices, such as calling in an outside forensics consultant. You may need to take precautions such as making copies of a computer's hard drive and limiting access to one of the copies or making checksums of the information to ensure that information is not modified.
- Information on the attack and about the intruder can be found in many locations, including log files for network equipment or network monitoring systems.
- Once law enforcement comes on-site to investigate, they will gather information according to their procedures as officers of the court.
- Law enforcement will have to get a subpoena or warrant to gather more information if necessary.
- Law enforcement does not require a warrant if an organization agrees to provide information willingly, but it may be appropriate to require a subpoena as protection from some liability.

Understand Civil Issues

- The organization owns the equipment used by employees, and the organization may access that information at any time. Therefore, the employee should have no expectation of privacy.
- As the provider of computer and network services, the organization is permitted to monitor the information on the network and how the network is used.
- Employees of an organization should be informed through written policy and notification banners that they may be monitored.
- Organization policy should outline what appropriate activities are for computers and networks under their control, and employees should be oriented to the policy.
- For an organization to protect itself from downstream liability, it must take reasonable care and measures to prevent its systems from being used as a platform for attack.

Understand Privacy Issues

- Customer information does not belong to an organization, it belongs to the customer. Organizations must take appropriate steps to protect customer information.
- The Health Insurance Portability and Accountability Act (HIPAA) established standards for the security of patient health information.
- HIPAA uses administrative, physical, and technical safeguards as well as policies, procedures, and documentation requirements to protect patient information.
- The Graham-Leach-Bliley Financial Services Modernization Act (GLBA) specifies how financial organizations will protect the customer's private information.
- Financial organizations must implement a written information security program, have board involvement, and conduct risk assessments.

Key Terms

- 18 US Code 1029 (Credit Card Fraud)** (117)
- 18 US Code 1030 (Computer Fraud and Abuse)** (116)
- 18 US Code 2319 (Copyrights)** (117)
- 18 US Code 2511 (Interception)** (118)
- 18 US Code 2701 (Access to Electronic Information)** (118)
- downstream liability** (127)
- due diligence** (134)
- evidence collection** (124)
- expectation of privacy** (120)
- Graham-Leach-Bliley Financial Services Modernization Act (GLBA)** (132)
- Health Insurance Portability and Accountability Act (HIPAA)** (129)
- Homeland Security Act (Cyber Security Enhancement Act)** (121)
- internal monitoring** (127)
- protected computers** (117)
- USA-Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)** (119)

Key Term Quiz

Use terms from the Key Terms list to complete the sentences that follow. Don't use the same term more than once. Not all terms will be used.

1. _____ establishes the basis for federal intervention for computer-related crimes.
2. You work for an organization and have taken measures to ensure all patches have been applied to the computer systems to make them secure and to ensure that an attacker will have difficulty compromising your systems to use as a platform for attacking other computer systems. This is known in legal terms as _____.
3. The organization you work for has detected a break-in. There is concern that the intruder may have gained access to the customer database. Customers may feel that their _____ was violated.
4. If a hacker accesses your organization via a weakness in your network and then launches an attack against several other organizations, your organization may be sued by one of the other companies due to _____.
5. You have detected a break-in, and the administration and legal department have decided to contact authorities to prosecute the intruder. After the investigators arrive, they conduct _____ by tagging the affected computer system and taking it with them for analysis.

6. The _____ was implemented to enhance information security for the United States, increase the penalties for criminal acts, and direct the United States Sentencing Commission to consider the severity of the computer crime when determining sentencing guidelines.
7. _____ is the process where an employer checks on the activities of their employees to ensure that the organization cannot be held liable.
8. The _____ was created to protect patients from having their medical information released to unauthorized persons.
9. _____ makes it illegal to collect electronic communications.
10. The _____ was created to protect the financial information of the customer.

Multiple Choice Quiz

1. _____ forms the basis for federal intervention in computer crimes.
 - a. 18 US Code 1212
 - b. 18 US Code 1030
 - c. 18 US Code 1029
 - d. 18 US Code 2319
2. 18 US Code 2511 addresses _____.
 - a. Credit card fraud
 - b. Unlawful access to stored communications
 - c. The interception of electronic communications
 - d. The creation of the Department of Homeland Security
3. Monitoring policies should _____.
 - a. Require employees to go out of their way to monitor activities
 - b. Identify who will conduct the monitoring
 - c. Hide the fact from employees that monitoring is being conducted
 - d. Be enforced for all employees except the executive team
4. The collection of e-mail headers, source, and destination IP addresses when necessary by law enforcement is covered under _____.
 - a. The Patriot Act
 - b. State law

- c. The HIPAA
 - d. The Computer Fraud and Abuse Act
5. The Patriot Act changed or amended which of the following statutes?
- a. 18 US Code 2700
 - b. 18 US Code 3127
 - c. 18 US Code 2511
 - d. 18 US Code 0001
6. Which statement is true concerning what constitutes a crime?
- a. All states must be consistent in determining what constitutes a crime.
 - b. The federal government will tell states what a crime is in their state.
 - c. It is illegal for states to enact codes concerning computer crimes.
 - d. Some states consider modifying e-mail headers a crime.
7. If your organization is penetrated by an attacker, you should _____.
- a. Immediately contact law enforcement
 - b. Retaliate with a counter-attack
 - c. Discuss options with your organization's general counsel
 - d. Restore the system back to normal and delete any tampered logs
8. Once law enforcement has been contacted, they _____.
- a. Are acting as your representatives in the best interest of your organization
 - b. Can act on any information they find in your organization's system
 - c. Do not require a subpoena or warrant to investigate for additional information
 - d. Will gather and protect information according to their own procedures
9. Under 18 US Code 1030, the minimum amount of damage that must occur before the federal statute will apply is _____.
- a. \$1,000
 - b. \$5,000
 - c. \$10,000
 - d. \$15,000

10. As an employee of an organization, when using the information systems of the organization to conduct business, you _____.
- Should have a reasonable expectation of privacy
 - Should have no expectation of privacy
 - May take the organization to court for privacy violations
 - Do not have to be made aware of monitoring policies
11. Which of the following is an appropriate precaution to safeguard information after an attack before contacting law enforcement?
- Allow system administrators to fix the system before making copies of system backups.
 - Make copies of the involved computer's hard drive for analysis by system administrators.
 - Make at least two copies of the involved computer's hard drive and bag one so that it cannot be tampered with.
 - Collect affected hardware to give to law enforcement as evidence.
12. Which of the following is true concerning customer information?
- Customer information, once collected, belongs to the organization.
 - Customer information must be safeguarded from unauthorized disclosure.
 - Customer information may be used by the business in any way it chooses.
 - Customer information belongs to the government where the business is located.
13. 18 US Code 1029 makes it a crime to _____.
- Reproduce or distribute copyrighted material where at least 10 copies have been made
 - Reproduce or distribute copyrighted material where at least 1,000 copies have been made
 - Possess a counterfeit credit card
 - Possess 15 or more counterfeit credit cards
14. When managing and controlling the risk of financial data, organizations must _____.
- Require training for the customer
 - Use regular tests to determine program efficiency
 - Use technical security systems that need no other safeguards
 - Make all financial data public

15. The GLBA establishes guidelines for service providers who may have significant access to financial data. Which of the following is a guideline for those requirements?
 - a. The organization must demonstrate due diligence in selecting providers.
 - b. Service providers are not required to implement security.
 - c. Service providers cannot be monitored for compliance.
 - d. Once the program is in place, adjustments will never have to be made.

Essay Questions

1. Explain why and how the Patriot Act modified trap and trace laws.
2. Explain the steps a company should take to ensure that users understand policies and to alleviate any potential legal issues.
3. Why is it important to notify employees of the monitoring policies of the organization?
4. 18 US Code 2511 specifies that since the organization is the service provider, any employee of the organization can monitor communication in the normal course of his or her job for the “protection of the rights or property of the provider of that service.” What is meant by the “normal course of his or her job”?
5. Why would it be harder for a business in the United States to prosecute an attacker who is outside the country rather than inside the United States?

Lab Projects

1. Using the Internet, visit the FBI (<http://www.fbi.gov>), Department of Justice (<http://www.usdoj.gov>), and Secret Service (<http://www.ustras.gov/uss>) Web sites. What information is available on procedures for reporting computer crimes, and what types of incidents will they investigate?
2. Research computer crimes or computer scams. How are these types of attack likely to impact a business?
3. In two groups, research and discuss the Patriot Act. One group should take the pro stance, defending the reasoning for the act and its specific measures. The other group should take the con stance, raising any concerns with the act. Debate the privacy issues this act raises and whether the act is a sufficient measure to provide tools to obstruct terrorism.
4. In groups, visit the First Government Web site (<http://firstgov.gov>). Each group should select a state and research the computer crimes and penalties for that state. Present your findings to the rest of the class. As a class discussion, compare the states that are presented and how their laws differ.