

Legal, Ethical, and Professional Issues in Information Security

In civilized life, law floats in a sea of ethics.

EARL WARREN, CHIEF JUSTICE OF
THE UNITED STATES, 12 NOVEMBER 1962

Henry Magruder made a mistake—he left a CD at the coffee station. Later, when Iris Majwubu was topping off her mug with fresh tea, hoping to wrap up her work on the current SQL code module before it was time to go home, she saw the unlabeled CD on the counter. Being the helpful sort, she picked it up, intending to return it to the person who'd left it behind.

Expecting to find perhaps the latest device drivers, or someone's work from the development team's office, Iris slipped the disk into the drive of her computer and ran a virus scan on its contents before opening the file explorer program. She had been correct in assuming the CD contained data files, and lots of them. She opened a file at random: names, addresses, and Social Security numbers appeared on her screen. These were not the test records she expected; they looked more like critical payroll data. Concerned, she found a readme.txt file and opened it. It read:

Jill, see files on this disc. Hope they meet your expectations. Wire money to account as arranged. Rest of data sent on payment.

Iris realized that someone was selling sensitive company data to an outside information broker. She looked back at the directory listing and saw that the files spanned the range of

Not For Sale

Not For Sale

every department at Sequential Label and Supply—everything from customer lists to shipping invoices. She saw one file that appeared to contain the credit card numbers of every Web customer the company supplied. She opened another file and saw that it only contained about half of the relevant data. Whoever did this had split the data into two parts. That made sense: payment on delivery of the first half.

Now, who did this belong to? She opened up the file properties option on the readme.txt file. The file owner was listed as “hmagruder.” That must be Henry Magruder, the developer two cubes over in the next aisle. Iris pondered her next action.

LEARNING OBJECTIVES:

Upon completion of this material, you should be able to:

- Describe the functions of and relationships among laws, regulations, and professional organizations in information security
- Differentiate between laws and ethics
- Identify major national laws that affect the practice of information security
- Explain the role of culture as it applies to ethics in information security

Introduction

As a future information security professional, you must understand the scope of an organization’s legal and ethical responsibilities. The information security professional plays an important role in an organization’s approach to managing liability for privacy and security risks. In the modern litigious societies of the world, sometimes laws are enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations. Sometimes these damages are punitive—assessed as a deterrent. To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information security practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new and emerging issues. By educating the management and employees of an organization on their legal and ethical obligations and the proper use of information technology and information security, security professionals can help keep an organization focused on its primary objectives.

In the first part of this chapter, you learn about the legislation and regulations that affect the management of information in an organization. In the second part, you learn about the ethical issues related to information security, and about several professional organizations with established codes of ethics. Use this chapter as both a reference to the legal aspects of information security and as an aide in planning your professional career.

Law and Ethics in Information Security

In general, people elect to trade some aspects of personal freedom for social order. As Jean-Jacques Rousseau explains in *The Social Contract, or Principles of Political Right*¹, the rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called *laws*. **Laws** are rules that mandate or prohibit

certain behavior; they are drawn from **ethics**, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not. Ethics in turn are based on **cultural mores**: the fixed moral attitudes or customs of a particular group. Some ethical standards are universal. For example, murder, theft, assault, and arson are actions that deviate from ethical and legal codes throughout the world.

Organizational Liability and the Need for Counsel



What if an organization does not demand or even encourage strong ethical behavior from its employees? What if an organization does not behave ethically? Even if there is no breach of criminal law, there can still be liability. **Liability** is the legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make **restitution**, or to compensate for wrongs committed. The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action. An organization increases its liability if it refuses to take measures known as due care. **Due care** standards are met when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. **Due diligence** requires that an organization make a valid effort to protect others and continually maintains this level of effort. Given the Internet's global reach, those who could be injured or wronged by an organization's employees could be anywhere in the world. Under the U.S. legal system, any court can assert its authority over an individual or organization if it can establish **jurisdiction**—that is, the court's right to hear a case if a wrong is committed in its territory or involves its citizenry. This is sometimes referred to as **long arm jurisdiction**—the long arm of the law extending across the country or around the world to draw an accused individual into its court systems. Trying a case in the injured party's home area is usually favorable to the injured party.²

Policy Versus Law

Within an organization, information security professionals help maintain security via the establishment and enforcement of policies. These **policies**—guidelines that describe acceptable and unacceptable employee behaviors in the workplace—function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Because these policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace. The difference between a policy and a law, however, is that ignorance of a policy is an acceptable defense. Thus, for a policy to become enforceable, it must meet the following five criteria:

- **Dissemination (distribution)**—The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
- **Review (reading)**—The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.
- **Comprehension (understanding)**—The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.

Not For Sale

- **Compliance (agreement)**—The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation. Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
- **Uniform enforcement**—The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Only when all of these conditions are met can an organization penalize employees who violate the policy without fear of legal retribution.

Types of Law

Civil law comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people. **Criminal law** addresses activities and conduct harmful to society, and is actively enforced by the state. Law can also be categorized as private or public. **Private law** encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations. **Public law** regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

Relevant U.S. Laws

Historically, the United States has been a leader in the development and implementation of information security legislation to prevent misuse and exploitation of information and information technology. The implementation of information security legislation contributes to a more reliable business environment, which in turn, enables a stable economy. In its global leadership capacity, the United States has demonstrated a clear understanding of the importance of securing information and has specified penalties for people and organizations that breach U.S. civil statutes. The sections that follow present the most important U.S. laws that apply to information security.

General Computer Crime Laws

There are several key laws relevant to the field of information security and of particular interest to those who live or work in the United States. The **Computer Fraud and Abuse Act of 1986 (CFA Act)** is the cornerstone of many computer-related federal laws and enforcement efforts. It was amended in October 1996 by the **National Information Infrastructure Protection Act of 1996**, which modified several sections of the previous act and increased the penalties for selected crimes. The punishment for offenses prosecuted under this statute varies from fines to imprisonment up to 20 years, or both. The severity of the penalty depends on the value of the information obtained and whether the offense is judged to have been committed:

1. For purposes of commercial advantage
2. For private financial gain
3. In furtherance of a criminal act

The previous law, along with many others, was further modified by the **USA PATRIOT Act of 2001**, which provides law enforcement agencies with broader latitude in order to combat terrorism-related activities. In 2006, this act was amended by the **USA PATRIOT Improvement and Reauthorization Act**, which made permanent fourteen of the sixteen expanded powers of the Department of Homeland Security and the FBI in investigating terrorist activity. The act also reset the date of expiration written into the law as a so-called *sunset clause* for certain wiretaps under the Foreign Intelligence Surveillance Act of 1978 (FISA), and revised many of the criminal penalties and procedures associated with criminal and terrorist activities.³

Another key law is the **Computer Security Act of 1987**. It was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices. The National Bureau of Standards, in cooperation with the National Security Agency, is responsible for developing these security standards and guidelines.

Privacy

Privacy has become one of the hottest topics in information security at the beginning of the 21st century. Many organizations are collecting, swapping, and selling personal information as a commodity, and many people are looking to governments for protection of their privacy. The ability to collect information, combine facts from separate sources, and merge it all with other information has resulted in databases of information that were previously impossible to set up. One technology that was proposed in the past was intended to monitor or track private communications. Known as the Clipper Chip, it used an algorithm with a two-part key that was to be managed by two separate government agencies, and it was reportedly designed to protect individual communications while allowing the government to decrypt suspect transmissions.⁴ This technology was the focus of discussion between advocates for personal privacy and those seeking to enable more effective law enforcement. Consequently, this technology was never implemented by the U.S. government.

In response to the pressure for privacy protection, the number of statutes addressing an individual's right to privacy has grown. It must be understood, however, that **privacy** in this context is not absolute freedom from observation, but rather is a more precise "state of being free from unsanctioned intrusion."⁵ To help you better understand this rapidly evolving issue, some of the more relevant privacy laws are presented here.

Privacy of Customer Information Some regulations in the U.S. legal code stipulate the responsibilities of common carriers (organizations that process or move data for hire) to protect the confidentiality of customer information, including that of other carriers. The **Privacy of Customer Information Section** of the common carrier regulation states that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes, and that carriers cannot disclose this information except when necessary to provide their services. The only other exception is when a customer requests the disclosure of information, and then the disclosure is restricted to that customer's information only. This law does allow for the use of aggregate information, as long as the same information is provided to all common carriers and all carriers possessing the information engage in fair competitive business practices. **Aggregate information** is created by combining pieces of non-private data—often collected during software updates and via cookies—that when combined may violate privacy.

While common carrier regulation regulates public carriers in order to protect individual privacy, the **Federal Privacy Act of 1974** regulates government agencies and holds them



Not For Sale

accountable if they release private information about individuals or businesses without permission. The following agencies, regulated businesses, and individuals are exempt from some of the regulations so that they can perform their duties:

- Bureau of the Census
- National Archives and Records Administration
- Congress
- Comptroller General
- Federal courts with regard to specific issues using appropriate court orders
- Credit reporting agencies
- Individuals or organizations that demonstrate that information is necessary to protect the health or safety of that individual

The **Electronic Communications Privacy Act of 1986** is a collection of statutes that regulates the interception of wire, electronic, and oral communications. These statutes work in conjunction with the **Fourth Amendment of the U.S. Constitution**, which protects individuals from unlawful search and seizure.

The **Health Insurance Portability and Accountability Act Of 1996 (HIPAA)**, also known as the **Kennedy-Kassebaum Act**, protects the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange. HIPAA affects all health care organizations, including doctors' practices, health clinics, life insurers, and universities, as well as some organizations that have self-insured employee health programs. HIPAA specifies stiff penalties for organizations that fail to comply with the law, with fines up to \$250,000 and/or 10 years imprisonment for knowingly misusing client information. Organizations were required to comply with the act by April 14, 2003.⁶

How does HIPAA affect the field of information security? Beyond the basic privacy guidelines, the act requires organizations to use information security mechanisms, as well as policies and procedures, to protect health care information. It also requires a comprehensive assessment of information security systems, policies, and procedures where health care information is handled or maintained. Electronic signatures have become more common, and HIPAA provides guidelines for the use of these signatures based on security standards that ensure message integrity, user authentication, and nonrepudiation. There is no specification of particular security technologies for each of the security requirements, only that security must be implemented to ensure the privacy of the health care information.

The privacy standards of HIPAA severely restrict the dissemination and distribution of private health information without documented consent. The standards provide patients with the right to know who has access to their information and who has accessed it. The standards also restrict the use of health information to the minimum necessary for the health care services required.

HIPAA has five fundamental principles:

1. Consumer control of medical information
2. Boundaries on the use of medical information
3. Accountability for the privacy of private information

4. Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
5. Security of health information

Best known for its allocation of \$787 million to stimulate the U.S. economy, the American Recovery and Reinvestment Act of 2009 (ARRA) includes new legislation that broadens the scope of HIPAA and gives HIPAA investigators direct, monetary incentives to pursue violators. The HIPAA-specific parts of ARRA are found in the Health Information Technology for Economic and Clinical Health Act (HITECH), which Congress included in the overall ARRA legislation. HITECH broadens the scope of HIPAA to cover all business associates of Health Care Organizations (HCOs). This means that any accounting firm, legal firm, IT consultancy, or other business partner of an HCO must comply with HIPAA security mandates to protect PHI.

Effective February 2010, organizations face the same civil and legal penalties that doctors, hospitals, and insurance companies face for violating the HIPAA Privacy Rule. HITECH not only changes how fines will be levied, it also raises the upper limit on the fines that can be imposed. An HCO or business partner who violates HIPAA may have to pay fines reaching as high as \$1.5 million per calendar year. In addition, private citizens and lawyers can now sue to collect fines for security breaches. Overall, HITECH considerably increases the potential financial liability of any organization that mishandles the PHI that passes through its IT infrastructure.

The HITECH Act also includes new data breach notification rules that apply to HCOs and business partners. If an employee discovers a PHI security breach, the employee's organization has only 60 days in which to notify each individual whose privacy has been compromised. If the organization is unable to contact ten or more of the affected individuals, it must either report the security breach on its Web site or issue a press release about the breach to broadcast and print media. If the breach affects 500 or more individuals, the organization must additionally notify the Security of the HHS, along with major media outlets. The HHS will then report the breach on its own Web site.⁷

The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999 contains a number of provisions focusing on facilitating affiliation among banks, securities firms, and insurance companies. Specifically, this act requires all financial institutions to disclose their privacy policies on the sharing of nonpublic personal information. It also requires due notice to customers, so that they can request that their information not be shared with third parties. In addition, the act ensures that the privacy policies in effect in an organization are both fully disclosed when a customer initiates a business relationship, and distributed at least annually for the duration of the professional association.

See Table 3-1 for a summary of information security-related laws.

Identity Theft Related to the legislation on privacy is the growing body of law on identity theft. The Federal Trade Commission (FTC) describes identity theft as “occurring when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.”⁸ The FTC estimates that perhaps as many as nine million Americans are faced with identity



Not For Sale

Area	Act	Date	Description
Telecommunications	Telecommunications Deregulation and Competition Act of 1996—Update to Communications Act of 1934 (47 USC 151 et seq.)	1996	Regulates interstate and foreign telecommunications (amended 1996 and 2001)
Freedom of information	Freedom of Information Act (FOIA)	1966	Allows for the disclosure of previously unreleased information and documents controlled by the U.S. government
Privacy	Federal Privacy Act of 1974	1974	Governs federal agency use of personal information
Copyright	Copyright Act of 1976—Update to U.S. Copyright Law (17 USC)	1976	Protects intellectual property, including publications and software
Cryptography	Electronic Communications Privacy Act of 1986 (Update to 18 USC)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act
Access to stored communications	Unlawful Access to Stored Communications (18 USC 2701)	1986	Provides penalties for illegally accessing stored communications (such as e-mail and voicemail) stored by a service provider
Threats to computers	Computer Fraud and Abuse Act (also known as Fraud and Related Activity in Connection with Computers) (18 USC 1030)	1986	Defines and formalizes laws to counter threats from computer-related acts and offenses (amended 1996, 2001, and 2006)
Federal agency information security	Computer Security Act of 1987	1987	Requires all federal computer systems that contain classified information to have security plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems
Trap and trace restrictions	General prohibition on pen register and trap and trace device use; exception (18 USC 3121 et seq.)	1993	Prohibits the use of electronic "pen registers" and trap and trace devices without a court order
Criminal intent	National Information Infrastructure Protection Act of 1996 (update to 18 USC 1030)	1996	Categorizes crimes based on defendant's authority to access a protected computer system and criminal intent
Trade secrets	Economic Espionage Act of 1996	1996	Prevents abuse of information gained while employed elsewhere
Personal health information protection	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	1996	Requires medical practices to ensure the privacy of personal medical information
Encryption and digital signatures	Security and Freedom through Encryption Act of 1997	1997	Affirms the rights of persons in the United States to use and sell products that include encryption and to relax export controls on such products
Intellectual property	No Electronic Theft Act Amends 17 USC 506(a)—copyright infringement, and 18 USC 2319—criminal infringement of copyright (Public Law 105-147)	1997	Amends copyright and criminal statutes to provide greater copyright protection and penalties for electronic copyright infringement

Table 3-1 Key U.S. Laws of Interest to Information Security Professionals



Area	Act	Date	Description
Copy protection	Digital Millennium Copyright Act (update to 17 USC 101)	1998	Provides specific penalties for removing copyright protection from media
Identity theft	Identity Theft and Assumption Deterrence Act of 1998 (18 USC 1028)	1998	Attempts to instigate specific penalties for identity theft by identifying the individual who loses their identity as the true victim, not just those commercial and financial credit entities who suffered losses
Banking	Gramm-Leach-Bliley Act of 1999 (GLB) or the Financial Services Modernization Act	1999	Repeals the restrictions on banks affiliating with insurance and securities firms; has significant impact on the privacy of personal information used by these industries
Terrorism	USA PATRIOT Act of 2001 (update to 18 USC 1030)	2001	Defines stiffer penalties for prosecution of terrorist crimes
Accountability	Sarbanes-Oxley Act of 2002 (SOX) or Public Company Accounting Reform and Investor Protection Act	2002	Enforces accountability for executives at publicly traded companies; this law is having ripple effects throughout the accounting, IT, and related units of many organizations
Spam	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 CAN-SPAM Act (15 USC 7701 et seq.)	2003	Sets the first national standards for regulating the distribution of commercial email; the act includes mobile phone spam as well
Fraud with access devices	Fraud and Related Activity in Connection with Access Devices (18 USC 1029)	2004	Defines and formalizes law to counter threats from counterfeit access devices like ID cards, credit cards, telecom equipment, mobile or electronic serial numbers, and the equipment that creates them
Terrorism and extreme drug trafficking	USA PATRIOT Improvement and Reauthorization Act of 2005 (update to 18 USC 1030)	2006	Renews critical sections of the USA PATRIOT Act

Table 3-1 Key U.S. Laws of Interest to Information Security Professionals (continued)

theft each year. Many people, among them perhaps you or someone you know have been affected by some form of identity theft.⁹ Organizations can also be victims of identity theft by means of URL manipulation or DNS redirection, as described in Chapter 2. In May of 2006, President Bush signed an executive order creating the Identity Theft Task Force, which on April 27, 2007 issued a strategic plan to improve efforts of the government and private organizations and individuals in combating identity theft. The U.S. FTC now oversees efforts to foster coordination among groups, more effective prosecution of criminals engaged in these activities, and methods to increase restitution made to victims.¹⁰

While numerous states have passed identity theft laws, at the federal level the primary legislation is the **Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information** (Title 18, U.S.C. § 1028), which criminalizes creation, reproduction, transfer, possession, or use of unauthorized or false identification documents or document-making equipment. The penalties for such offenses range from 1 to 25 years in prison, and fines as determined by the courts.

Not For Sale

The FTC recommends that people take the following four steps when they suspect they are victims of identity theft:

1. Report to the three dominant consumer reporting companies that your identity is threatened so that they may place a fraud alert on your record. This informs current and potential creditors to follow certain procedures before taking credit-related actions.
2. If you know which accounts have been compromised, close them. If new accounts are opened using your identity without your permission, you can obtain a document template online that may be used to dispute these new accounts. The FTC offers a comprehensive identity theft site to provide guidance, tools, and forms you might need at www.ftc.gov/bcp/edu/microsites/idtheft.
3. Register your concern with the FTC. There is a form to register a complaint at the FTC's identity theft site.
4. Report the incident to either your local police or police in the location where the identity theft occurred. Use your copy of the FTC ID Theft complaint form to make the report. Once your police report has been filed, be sure to get a copy or acquire the police report number.¹¹

Export and Espionage Laws

To meet national security needs and to protect trade secrets and other state and private assets, several laws restrict which information and information management and security resources may be exported from the United States. These laws attempt to stem the theft of information by establishing strong penalties for these crimes.

To protect American ingenuity, intellectual property, and competitive advantage, Congress passed the **Economic Espionage Act** in 1996. This law attempts to prevent trade secrets from being illegally shared.

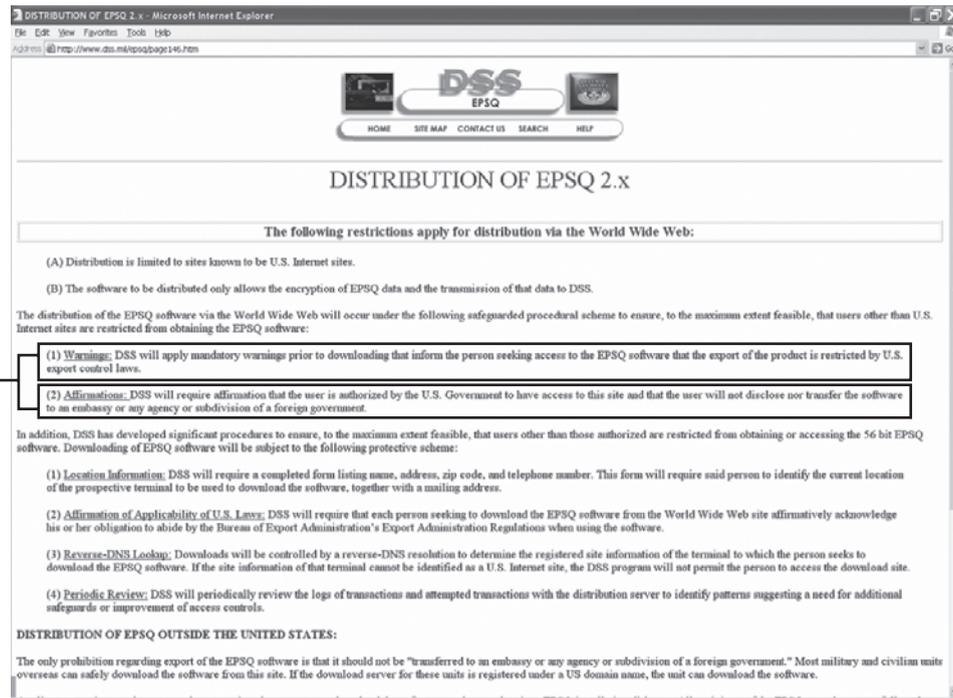
The **Security and Freedom through Encryption Act of 1999** provides guidance on the use of encryption and provides protection from government intervention. The acts include provisions that:

- Reinforce an individual's right to use or sell encryption algorithms, without concern for regulations requiring some form of key registration. Key registration is the storage of a cryptographic key (or its text equivalent) with another party to be used to break the encryption of data. This is often called "key escrow."
- Prohibit the federal government from requiring the use of encryption for contracts, grants, and other official documents and correspondence.
- State that the use of encryption is not probable cause to suspect criminal activity.
- Relax export restrictions by amending the Export Administration Act of 1979.
- Provide additional penalties for the use of encryption in the commission of a criminal act.

As illustrated in Figure 3-1, the distribution of many software packages is restricted to approved organizations, governments, and countries.

U.S. Copyright Law

Intellectual property is a protected asset in the United States. The U.S. copyright laws extend this privilege to the published word, including electronic formats. Fair use allows copyrighted materials to be used to support news reporting, teaching, scholarship, and a number of



For distribution in the U.S. and Canada only.

Figure 3-1 Export and Espionage

Source: Course Technology/Cengage Learning

similar activities, as long as the use is for educational or library purposes, is not for profit, and is not excessive. As long as proper acknowledgement is provided to the original author of such works, including a proper description of the location of source materials (citation), and the work is not represented as one's own, it is entirely permissible to include portions of someone else's work as reference. For more detailed information on copyright regulations, visit the U.S. Copyright Office Web site at www.copyright.gov.

Financial Reporting

The **Sarbanes-Oxley Act of 2002** is a critical piece of legislation that affects the executive management of publicly traded corporations and public accounting firms. This law seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies. Penalties for non-compliance range from fines to jail terms. Executives working in firms covered by this law seek assurance on the reliability and quality of information systems from senior information technology managers. In turn, IT managers are likely to ask information security managers to verify the confidentiality and integrity of those information systems in a process known in the industry as sub-certification.

Freedom of Information Act of 1966 (FOIA)

The **Freedom of Information Act** allows any person to request access to federal agency records or information not determined to be a matter of national security. Agencies of the federal government are required to disclose any requested information on receipt of a written request. This requirement is enforceable in court. Some information is, however, protected from disclosure, and the act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA.



State and Local Regulations

In addition to the national and international restrictions placed on organizational use of computer technology, each state or locality may have a number of its own applicable laws and regulations. Information security professionals must therefore understand state laws and regulations and ensure that the organization's security policies and procedures comply with those laws and regulations.

For example, in 1991 the state of Georgia passed the **Georgia Computer Systems Protection Act**, which seeks to protect information, and which establishes penalties for the use of information technology to attack or exploit information systems.

International Laws and Legal Bodies

It is important for IT professionals and information security practitioners to realize that when their organizations do business on the Internet, they do business globally. As a result, these professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries. While it may be impossible to please all of the people all of the time, dealing with the laws of other states and nations is one area where it is certainly *not* easier to ask for forgiveness than for permission.

A number of different security bodies and laws are described in this section. Because of the political complexities of the relationships among nations and the differences in culture, there are currently few international laws relating to privacy and information security. The laws discussed below are important, but are limited in their enforceability. The American Society of International Law is one example of an American institution that deals in international law (see www.asil.org).

Council of Europe Convention on Cybercrime

The Council of Europe adopted the **Convention on Cybercrime** in 2001. It created an international task force to oversee a range of security functions associated with Internet activities for standardized technology laws across international borders. It also attempts to improve the effectiveness of international investigations into breaches of technology law. This convention has been well received by advocates of intellectual property rights because it emphasizes prosecution for copyright infringement. However, many supporters of individual rights oppose the convention because they think it unduly infringes on freedom of speech and threatens the civil liberties of U.S. residents.

While thirty-four countries attended the signing in November 2001, only twenty-nine nations, including the United States, have ratified the Convention as of April 2010. The United States is technically not a “member state of the council of Europe” but does participate in the Convention.

As is true with much complex international legislation, the Convention on Cybercrime lacks any realistic provisions for enforcement. The overall goal of the convention is to simplify the acquisition of information for law enforcement agencies in certain types of international crimes. It also simplifies the extradition process. The convention has more than its share of skeptics, who see it as an overly simplistic attempt to control a complex problem.

Agreement on Trade-Related Aspects of Intellectual Property Rights

The **Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)**, created by the World Trade Organization (WTO) and negotiated over the years 1986–1994, introduced intellectual property rules into the multilateral trade system. It is the first significant international effort to protect intellectual property rights. It outlines requirements for governmental oversight and legislation of WTO member countries to provide minimum levels of protection for intellectual property. The WTO TRIPS agreement covers five issues:

- How basic principles of the trading system and other international intellectual property agreements should be applied
- How to give adequate protection to intellectual property rights
- How countries should enforce those rights adequately in their own territories
- How to settle disputes on intellectual property between members of the WTO
- Special transitional arrangements during the period when the new system is being introduced¹²

Digital Millennium Copyright Act (DMCA)

The **Digital Millennium Copyright Act (DMCA)** is the American contribution to an international effort by the World Intellectual Properties Organization (WIPO) to reduce the impact of copyright, trademark, and privacy infringement, especially when accomplished via the removal of technological copyright protection measures. This law was created in response to the 1995 adoption of **Directive 95/46/EC** by the European Union, which added protection for individuals with regard to the processing of personal data and the use and movement of such data. The United Kingdom has implemented a version of this law called the **Database Right**, in order to comply with Directive 95/46/EC.

The DMCA includes the following provisions:

- Prohibits the circumvention protections and countermeasures implemented by copyright owners to control access to protected content
- Prohibits the manufacture of devices to circumvent protections and countermeasures that control access to protected content
- Bans trafficking in devices manufactured to circumvent protections and countermeasures that control access to protected content
- Prohibits the altering of information attached or imbedded into copyrighted material
- Excludes Internet service providers from certain forms of contributory copyright infringement

Ethics and Information Security

Many Professional groups have explicit rules governing ethical behavior in the workplace. For example, doctors and lawyers who commit egregious violations of their professions' canons of conduct can be removed from practice. Unlike the medical and legal fields, however, the information technology field in general, and the information security field in particular, do not



Offline The Ten Commandments of Computer Ethics¹³

From The Computer Ethics Institute

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.

have a binding code of ethics. Instead, professional associations—such as the Association for Computing Machinery (ACM) and the Information Systems Security Association—and certification agencies—such as the International Information Systems Security Certification Consortium, Inc., or (ISC)²—work to establish the profession's ethical codes of conduct. While these professional organizations can prescribe ethical conduct, they do not always have the authority to banish violators from practicing their trade. To begin exploring some of the ethical issues particular to information security, take a look at the Ten Commandments of Computer Ethics in the nearby Offline.

Ethical Differences Across Cultures

Cultural differences can make it difficult to determine what is and is not ethical—especially when it comes to the use of computers. Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group. For example, to Western cultures, many of the ways in which Asian cultures use computer technology is software piracy.¹⁴ This ethical conflict arises out of Asian traditions of collective ownership, which clash with the protection of intellectual property. Approximately 90 percent of all software is created in the United States. Some countries are more relaxed with intellectual property copy restrictions than others.

A study published in 1999 examined computer use ethics of eight nations: Singapore, Hong Kong, the United States, England, Australia, Sweden, Wales, and the Netherlands.¹⁵ This

study selected a number of computer-use vignettes (see the Offline titled The Use of Scenarios in Computer Ethics Studies) and presented them to students in universities in these eight nations. This study did not categorize or classify the responses as ethical or unethical. Instead, the responses only indicated a degree of ethical sensitivity or knowledge about the performance of the individuals in the short case studies. The scenarios were grouped into three categories of ethical computer use: software license infringement, illicit use, and misuse of corporate resources.



Software License Infringement The topic of software license infringement, or piracy, is routinely covered by the popular press. Among study participants, attitudes toward piracy were generally similar; however, participants from the United States and the Netherlands showed statistically significant differences in attitudes from the overall group. Participants from the United States were significantly less tolerant of piracy, while those from the Netherlands were significantly more permissive. Although other studies have reported that the Pacific Rim countries of Singapore and Hong Kong are hotbeds of software piracy, this study found tolerance for copyright infringement in those countries to be moderate, as were attitudes in England, Wales, Australia, and Sweden. This could mean that the individuals surveyed *understood* what software license infringement was, but felt either that their use was not piracy, or that their society permitted this piracy in some way. Peer pressure, the lack of legal disincentives, the lack of punitive measures, and number of other reasons could explain why users in these alleged piracy centers disregarded intellectual property laws despite their professed attitudes toward them. Even though participants from the Netherlands displayed a more permissive attitude toward piracy, that country only ranked third in piracy rates of the nations surveyed in this study.

Illicit Use The study respondents unilaterally condemned viruses, hacking, and other forms of system abuse. There were, however, different degrees of tolerance for such activities among the groups. Students from Singapore and Hong Kong proved to be significantly more tolerant than those from the United States, Wales, England, and Australia. Students from Sweden and the Netherlands were also significantly more tolerant than those from Wales and Australia, but significantly less tolerant than those from Hong Kong. The low overall degree of tolerance for illicit system use may be a function of the easy correspondence between the common crimes of breaking and entering, trespassing, theft, and destruction of property and their computer-related counterparts.

Misuse of Corporate Resources The scenarios used to examine the levels of tolerance for misuse of corporate resources each presented a different degree of noncompany use of corporate assets without specifying the company's policy on personal use of company resources. In general, individuals displayed a rather lenient view of personal use of company equipment. Only students from Singapore and Hong Kong view personal use of company equipment as unethical. There were several substantial differences in this category, with students from the Netherlands revealing the most lenient views. With the exceptions of those from Singapore and Hong Kong, it is apparent that many people, regardless of cultural background, believe that unless an organization explicitly forbids personal use of its computing resources, such use is acceptable. It is interesting to note that only participants among the two Asian samples, Singapore and Hong Kong, reported generally intolerant attitudes toward personal use of organizational computing resources. The reasons behind this are unknown.¹⁶

Offline

The Use of Scenarios in Computer Ethics Studies

Adapted from “Cross-National Differences in Computer-Use Ethics”:

By Michael E. Whitman, Anthony M. Townsend, and Anthony R. Hendrickson,
The Journal of International Business Studies.

The following vignettes can be used in an open and frank discussion of computer ethics. Review each scenario carefully and respond to each question using the following statement, choosing the description you feel most appropriate: *I feel the actions of this individual were (very ethical / ethical / neither ethical nor unethical / unethical / very unethical)*. Then, justify your response.

Ethical Decision Evaluation

Note: These scenarios are based on published works by Professor Whitman and Professor Paradise.

1. A scientist developed a theory that required proof through the construction of a computer model. He hired a computer programmer to build the model, and the theory was shown to be correct. The scientist won several awards for the development of the theory, but he never acknowledged the contribution of the computer programmer.

The scientist’s failure to acknowledge the computer programmer was:

2. The owner of a small business needed a computer-based accounting system. One day, he identified the various inputs and outputs he felt were required to satisfy his needs. Then he showed his design to a computer programmer and asked the programmer if she could implement such a system. The programmer knew she could implement the system because she had developed much more sophisticated systems in the past. In fact, she thought this design was rather crude and would soon need several major revisions. But she didn’t say anything about her thoughts, because the business owner didn’t ask, and she hoped she might be hired to implement the needed revisions.

The programmer’s decision not to point out the design flaws was:

3. A student found a loophole in the university computer’s security system that allowed him access to other students’ records. He told the system administrator about the loophole, but continued to access others’ records until the problem was corrected two weeks later.

The student’s action in searching for the loophole was:

The student’s action in continuing to access others’ records for two weeks was:

The system administrator’s failure to correct the problem sooner was:

4. A computer user called a mail-order software company to order a particular accounting system. When he received his order, he found that the store had accidentally sent him a very expensive word-processing program as well as the accounting package that he had ordered. The invoice listed only the accounting package. The user decided to keep the word-processing package.

The user's decision to keep the word-processing package was:

5. A programmer at a bank realized that he had accidentally overdrawn his checking account. He made a small adjustment in the bank's accounting system so that his account would not have the additional service charge assessed. As soon as he deposited funds that made his balance positive again, he corrected the bank's accounting system.

The programmer's modification of the accounting system was:

6. A computer programmer enjoyed building small computer applications (programs) to give his friends. He would frequently go to his office on Saturday when no one was working and use his employer's computer to develop applications. He did not hide the fact that he was going into the building; he had to sign a register at a security desk each time he entered.

The programmer's use of the company computer was:

7. A computer programmer built small computer applications (programs) in order to sell them. This was not his main source of income. He worked for a moderately sized computer vendor. He would frequently go to his office on Saturday when no one was working and use his employer's computer to develop applications. He did not hide the fact that he was going into the building; he had to sign a register at a security desk each time he entered.

The programmer's use of the company computer was:

8. A student enrolled in a computer class was also employed at a local business part-time. Frequently her homework in the class involved using popular word-processing and spreadsheet packages. Occasionally she worked on her homework on the office computer at her part-time job, on her coffee or meal breaks.

The student's use of the company computer was:

If the student had worked on her homework during "company time" (not during a break), the student's use of the company computer would have been:

9. A student at a university learned to use an expensive spreadsheet program in her accounting class. The student would go to the university microcomputer lab and use the software to complete her assignment. Signs were posted in the lab indicating that copying software was forbidden. One day, she decided to copy the software anyway to complete her work assignments at home.

If the student destroyed her copy of the software at the end of the term, her action in copying the software was:

(continued)

Not For Sale

If the student forgot to destroy her copy of the software at the end of the term, her action in copying the software was:

If the student never intended to destroy her copy of the software at the end of the term, her action in copying the software was:

10. A student at a university found out that one of the local computer bulletin boards contained a "pirate" section (a section containing a collection of illegally copied software programs). He subscribed to the board, and proceeded to download several games and professional programs, which he then distributed to several of his friends.

The student's actions in downloading the games were:

The student's actions in downloading the programs were:

The student's actions in sharing the programs and games with his friends were:

11. State College charges its departments for computer time usage on the campus mainframe. A student had access to the university computer system because a class she was taking required extensive computer usage. The student enjoyed playing games on the computer, and frequently had to request extra computer funds from her professor in order to complete her assignments.

The student's use of the computer to play games was:

12. An engineer needed a program to perform a series of complicated calculations. He found a computer programmer capable of writing the program, but would only hire the programmer if he agreed to share any liability that may result from an error in the engineer's calculations. The programmer said he would be willing to assume any liability due to a malfunction of the program, but was unwilling to share any liability due to an error in the engineer's calculations.

The programmer's position in this situation is:

The engineer's position in this situation is:

13. A manager of a company that sells computer-processing services bought similar services from a competitor. She used her access to the competitor's computer to try to break the security system, identify other customers, and cause the system to "crash" (cause loss of service to others). She used the service for over a year and always paid her bills promptly.

The manager's actions were:

14. One day, a student programmer decided to write a virus program. Virus programs usually make copies of themselves on other disks automatically, so the virus can spread to unsuspecting users. The student wrote a program that caused the microcomputer to ignore every fifth command entered by a user. The student took his program to the university computing lab and installed it on one of the microcomputers. Before long, the virus spread to hundreds of users.

The student's action of infecting hundreds of users' disks was:

If the virus program output the message "Have a nice day," then the student's action of infecting hundreds of users' disks would have been:

If the virus erased files, then the student's action of infecting hundreds of users' files would have been:

Ethics and Education

Attitudes toward the ethics of computer use are affected by many factors other than nationality. Differences are found among individuals within the same country, within the same social class, and within the same company. Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education. Employees must be trained and kept aware of a number of topics related to information security, not the least of which are the expected behaviors of an ethical employee. This is especially important in information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal. Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user.



Deterring Unethical and Illegal Behavior

There are three general causes of unethical and illegal behavior:

- **Ignorance**—Ignorance of the law is no excuse; however, ignorance of policy and procedures is. The first method of deterrence is education. This is accomplished by means of designing, publishing, and disseminating organization policies and relevant laws, and also obtaining agreement to comply with these policies and laws from all members of the organization. Reminders, training, and awareness programs keep the policy information in front of the individual and thus better support retention and compliance.
- **Accident**—Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control helps prevent accidental modification to systems and data.
- **Intent**—Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Whatever the cause of illegal, immoral, or unethical behavior, one thing is certain: it is the responsibility of information security personnel to do everything in their power to deter these acts and to use policy, education and training, and technology to protect information and systems. Many security professionals understand the technology aspect of protection but underestimate the value of policy. However, laws and policies and their associated penalties only deter if three conditions are present:

- **Fear of penalty**—Potential offenders must fear the penalty. Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.
- **Probability of being caught**—Potential offenders must believe there is a strong possibility of being caught. Penalties will not deter illegal or unethical behavior unless there is reasonable fear of being caught.
- **Probability of penalty being administered**—Potential offenders must believe that the penalty will in fact be administered.

Not For Sale

Codes of Ethics and Professional Organizations

A number of professional organizations have established codes of conduct or codes of ethics that members are expected to follow. Codes of ethics can have a positive effect on people's judgment regarding computer use.¹⁷ Unfortunately, many employers do not encourage their employees to join these professional organizations. But employees who have earned some level of certification or professional accreditation can be deterred from ethical lapses by the threat of loss of accreditation or certification due to a violation of a code of conduct. Loss of certification or accreditation can dramatically reduce marketability and earning power.

It is the responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. It is likewise the organization's responsibility to develop, disseminate, and enforce its policies. Following is a discussion of professional organizations and where they fit into the ethical landscape. Table 3-2 provides an overview of these organizations. Many of these organizations offer certification programs that require the applicants to subscribe formally to the ethical codes. Professional certification is discussed in Chapter 11.

Major IT Professional Organizations

Many of the major IT professional organizations maintain their own codes of ethics.

The **Association of Computing Machinery (ACM)** (www.acm.org) is a respected professional society that was established in 1947 as "the world's first educational and scientific computing society." It is one of the few organizations that strongly promotes education and provides

Professional Organization	Web Resource Location	Description	Focus
Association of Computing Machinery	www.acm.org	Code of 24 imperatives of personal ethical responsibilities of security professionals	Ethics of security professionals
Information Systems Audit and Control Association	www.isaca.org	One process area and six subject areas that focus on auditing, information security, business process analysis, and IS planning through the CISA and CISM certifications	Tasks and knowledge required of the information systems audit professional
Information Systems Security Association	www.issa.org	Professional association of information systems security professionals; provides education forums, publications, and peer networking for members	Professional security information sharing
International Information Systems Security Certification Consortium (ISC) ²	www.isc2.org	International Consortium dedicated to improving the quality of security professionals through SSCP and CISSP certifications	Requires certificants to follow its published code of ethics
SANS Institutes Global Information Assurance Certification	www.giac.org	GIAC certifications focus on four security areas: security administration, security management, IT audit, and software security, and has standard, gold, and expert levels	Requires certificants to follow its published code of ethics

Table 3-2 Professional Organizations of Interest to Information Security Professionals

discounts for student members. The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm (with specific references to viruses), protecting the privacy of others, and respecting the intellectual property and copyrights of others. The ACM also publishes a wide variety of professional computing publications, including the highly regarded *Communications of the ACM*.

The **International Information Systems Security Certification Consortium, Inc. (ISC)²** (www.isc2.org) is a nonprofit organization that focuses on the development and implementation of information security certifications and credentials. The (ISC)² manages a body of knowledge on information security and administers and evaluates examinations for information security certifications. The code of ethics put forth by (ISC)² is primarily designed for information security professionals who have earned an (ISC)² certification, and has four mandatory canons: “Protect society, the commonwealth, and the infrastructure; act honorably, honestly, justly, responsibly, and legally; provide diligent and competent service to principals; and advance and protect the profession.”¹⁸ This code enables (ISC)² to promote reliance on the ethicality and trustworthiness of the information security professional as the guardian of information and systems.

The **System Administration, Networking, and Security Institute (SANS)** (www.sans.org), which was founded in 1989, is a professional research and education cooperative organization with a current membership of more than 156,000 security professionals, auditors, system administrators, and network administrators. SANS offers a set of certifications called the Global Information Assurance Certification, or GIAC. All GIAC-certified professionals are required to acknowledge that certification and the privileges that come from it carry a corresponding obligation to uphold the GIAC Code of Ethics. Those certificate holders that do not conform to this code face punishment, and may lose GIAC certification.

The **Information Systems Audit and Control Association (ISACA)** (www.isaca.org) is a professional association that focuses on auditing, control, and security. The membership comprises both technical and managerial professionals. ISACA provides IT control practices and standards, and although it does not focus exclusively on information security, it does include many information security components within its areas of concentration. ISACA also has a code of ethics for its professionals, and it requires many of the same high standards for ethical performance as the other organizations and certifications.

The **Information Systems Security Association (ISSA)** (www.issa.org) is a nonprofit society of information security professionals. As a professional association, its primary mission is to bring together qualified information security practitioners for information exchange and educational development. ISSA provides a number of scheduled conferences, meetings, publications, and information resources to promote information security awareness and education. ISSA also promotes a code of ethics, similar in content to those of (ISC)², ISACA, and the ACM, whose focus is “promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources.”¹⁹



Key U.S. Federal Agencies

A number of key U.S. federal agencies are charged with the protection of American information resources and the investigation of threats to, or attacks on, these resources. These include the Department of Homeland Security (DHS) and the Federal Bureau of Investigation

Not For Sale

Not For Sale

(see Figure 3-2), the National Security Administration, the FBI's Infragard program (see Figure 3-3), and the U.S. Secret Service (see Figure 3-4).

The **Department of Homeland Security (DHS)** was created in 2003 by the Homeland Security Act of 2002, which was passed in response to the events of September 11, 2001. DHS is made up of five directorates, or divisions, through which it carries out its mission of protecting the people as well as the physical and informational assets of the United States. The Directorate of Information and Infrastructure creates and enhances resources used to discover and respond to attacks on national information systems and critical infrastructure. The Science and Technology Directorate is responsible for research and development activities in support of homeland defense. This effort is guided by an ongoing examination of vulnerabilities throughout the national infrastructure, and this directorate sponsors the emerging best practices developed to counter the threats and weaknesses in the system.

Established in January 2001, the **National InfraGard Program** began as a cooperative effort between the FBI's Cleveland Field Office and local technology professionals. The FBI sought assistance in determining a more effective method of protecting critical national information



Figure 3-2 DHS and FBI Home Pages

Source: Course Technology/Cengage Learning

© Cengage Learning. All rights reserved. No distribution allowed without express authorization.



Figure 3-3 Infragard and NSA Home Pages

Source: Course Technology/Cengage Learning

resources. The resulting cooperative, the first InfraGard chapter, was a formal effort to combat both cyber and physical threats. Since then, every FBI field office has established an InfraGard chapter and collaborates with public and private organizations and the academic community to share information about attacks, vulnerabilities, and threats. The National InfraGard Program serves its members in four basic ways:

- Maintains an intrusion alert network using encrypted e-mail
- Maintains a secure Web site for communication about suspicious activity or intrusions
- Sponsors local chapter activities
- Operates a help desk for questions

InfraGard’s dominant contribution is the free exchange of information to and from the private sector in the areas of threats and attacks on information resources.

Not For Sale

Not For Sale

United States Secret Service
WWW.SECRETSERVICE.GOV

U.S. Department of Homeland Security News

Haiti Earthquake Relief
Washington, D.C. - The U.S. Government has mobilized resources and manpower to aid in the Haiti earthquake relief effort. Here are some ways that you can get involved: donate, get information about friends or family, find out how federal departments are responding, and view the video of President Obama's remarks on recovery efforts.
www.whitehouse.gov/haitiearthquake

Posted January 14, 2010 at the [White House](#)

Fraudulent Spam E-Mails Claiming to be from the U.S. Secret Service
[Read more](#)

Search
» [Search the website](#)
Powered by [USA.gov](#)

About
» [Home](#)
» [Who We Are](#)
- [Director](#)
- [Deputy Director](#)
- [Special Agents](#)
- [Uniformed Division](#)
- [Support Personnel](#)
» [Our Dual Mission](#)
» [Bowling Training Center](#)
» [History](#)
» [Frequently Asked Questions](#)
» [Student Q&A](#)

Contact Us
» [Contact Information](#)
» [Field Offices](#)

Investigations
» [Investigative Mission](#)
» [Criminal Investigations](#)
» [Forensic Services](#)
» [Investigative Support](#)
» [Know Your Money](#)
» [Electronic Crimes Task Force](#)
» [Law Enforcement Resources](#)

Protection
» [Protective Mission](#)
» [How Protection Works](#)
» [National Special Security Events](#)
» [National Threat Assessment Center](#)

Press Room
» [Most Wanted](#)
» [Photo Gallery](#)
» [Press Releases](#)
» [Annual Report](#)
» [FOIA](#)
» [Downloads](#)
» [Information Quality](#)

Business Opportunities
» [Procurement Division \(For Vendors\)](#)

Employment
» [Upcoming Career Fairs](#)
» [Current Vacancies](#)
» [Frequently Asked Employment Questions](#)

JOIN OUR TEAM
United States Secret Service
Special Agent and Uniformed Division Officer Vacancy Announcement on Nov 09/10
Local Open House at U.S. Customs and Border Protection
14 March - 16 April 2010
Headquarters of the United States Secret Service
1600 Constitution Avenue, NW
Washington, DC 20535

Employment Language Bonus
The Secret Service is looking for special agent applicants with a foreign language skill. A Foreign Language Recruitment Bonus of 25 percent of basic annual pay will be paid to newly hired special agents, who test at the skill level required.
[Read More](#)

Features

Protection
Learn about protecting the President & Vice President, former U.S. Presidents, visiting foreign dignitaries and other protectees.
[Learn more...](#)

Investigations
Our investigative mission is to safeguard the payment and financial systems of the United States.
[Learn more...](#)

History
The Secret Service was created in 1865 to suppress counterfeit currency.
[Learn more...](#)

Most Wanted Fugitives
Help the Secret Service locate Most Wanted Fugitives and those wanted for questioning.
[Learn more...](#)

Opportunities
A premier law enforcement organization is looking for highly qualified men and women from diverse backgrounds who desire a fast paced, exciting and challenging career.
[Learn more...](#)

Know Your Money
Every year the public is victimized by the counterfeiting of the United States currency and other U.S. obligations.
[Learn more...](#)

Pistol Match

Figure 3-4 The Secret Service Home Page

Source: Course Technology/Cengage Learning

Another key federal agency is the **National Security Agency (NSA)**. The NSA is:

*the Nation's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information ... It is also one of the most important centers of foreign language analysis and research within the Government.*²⁰

The NSA is responsible for signal intelligence and information system security. The NSA's Information Assurance Directorate (IAD) provides information security "solutions including the technologies, specifications and criteria, products, product configurations, tools, standards, operational doctrine, and support activities needed to implement the protect, detect and report, and respond elements of cyber defense."²¹ The IAD also develops and promotes an Information Assurance Framework Forum in cooperation with commercial organizations and academic researchers. This framework provides strategic guidance as well as technical specifications for security solutions. IAD's Common Criteria is a set of standards designed to promote understanding of information security.

Prominent among the NSA's efforts and activities in the information security arena are the Information Security Outreach programs. The NSA recognizes universities that not only offer information security education, but that have also integrated information security philosophies and efforts into the internal operations of the schools. These recognized "Centers of Excellence in Information Assurance Education" receive the honor of displaying the recognition as well as being acknowledged on the NSA's Web site. Additionally, the NSA has a program to certify curricula in information security. The Information Assurance Courseware Evaluation process examines institutional information security courses and provides a three-year accreditation. Graduates of these programs receive certificates that indicate this accreditation.

The U.S. Secret Service is an agency within the Department of the Treasury. In addition to its well-known mission of providing protective services for key members of the U.S. government, the Secret Service is also charged with the detection and arrest of any person committing a United States federal offense relating to computer fraud and false identification crimes. This is an extension of the agency's original mission to protect U.S. currency—a logical extension, given that the communications networks of the United States carry more funds than all of the armored cars in the world combined. Protect the networks and protect the data, and you protect money, stocks, and other financial transactions. For more information on the Secret Service, see its Web site (the home page is shown in Figure 3-4).



Selected Readings

- *The Digital Person: Technology and Privacy in the Information Age*, by Daniel Solove. 2004. New York University Press.
- *The Practical Guide to HIPAA Privacy and Security Compliance*, by Kevin Beaver and Rebecca Herold. 2003. Auerbach.
- *When Good Companies Do Bad Things*, by Peter Schwartz. 1999. John Wiley and Sons.

Chapter Summary

- Laws are formally adopted rules for acceptable behavior in modern society. Ethics are socially acceptable behaviors. The key difference between laws and ethics is that laws carry the authority of a governing body and ethics do not.
- Organizations formalize desired behaviors in documents called policies. Policies must be read and agreed to before they are binding.
- Civil law comprises a wide variety of laws that are used to govern a nation or state. Criminal law addresses violations that harm society and are enforced by agents of the state or nation.
- Private law focuses on individual relationships, and public law governs regulatory agencies.
- Key U.S. laws protecting privacy include the Federal Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, and the Health Insurance Portability and Accountability Act of 1996.
- The desire to protect national security, trade secrets, and a variety of other state and private assets has led to several laws restricting what information and information management and security resources may be exported from the United States.

- Intellectual property is recognized as a protected asset in this country. U.S. copyright law extends this privilege to the published word, including electronic media.
- Studies have determined that individuals of differing nationalities have differing perspectives on ethical practices regarding the use of computer technology.
- Deterrence can prevent an illegal or unethical activity from occurring. Deterrence requires significant penalties, a high probability of apprehension, and an expectation of enforcement of penalties.
- As part of an effort to encourage ethical behavior, a number of professional organizations have established codes of conduct or codes of ethics that their members are expected to follow.
- There are a number of U.S. federal agencies responsible for protecting American information resources and investigating threats to, or attacks on, these resources.

Review Questions

1. What is the difference between law and ethics?
2. What is civil law, and what does it accomplish?
3. What are the primary examples of public law?
4. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?
5. Which law was specifically created to deal with encryption policy in the United States?
6. What is privacy in an information security context?
7. What is another name for the Kennedy-Kassebaum Act (1996), and why is it important to organizations that are not in the health care industry?
8. If you work for a financial service organization such as a bank or credit union, which 1999 law affects your use of customer data? What other affects does it have?
9. What is the primary purpose of the USA PATRIOT Act?
10. Which 1997 law provides guidance on the use of encryption?
11. What is intellectual property (IP)? Is it afforded the same protection in every country of the world? What laws currently protect it in the United States and Europe?
12. How does the Sarbanes-Oxley Act of 2002 affect information security managers?
13. What is due care? Why should an organization make sure to exercise due care in its usual course of operations?
14. How is due diligence different from due care? Why are both important?
15. What is a policy? How is it different from a law?
16. What are the three general categories of unethical and illegal behavior?
17. What is the best method for preventing an illegal or unethical activity?
18. Of the information security organizations listed that have codes of ethics, which has been established for the longest time? When was it founded?

19. Of the organizations listed that have codes of ethics, which is focused on auditing and control?
20. What can be done to deter someone from committing a crime?

Exercises



1. What does CISSP stand for? Use the Internet to identify the ethical rules CISSP holders have agreed to follow.
2. For what kind of information security jobs does the NSA recruit? Use the Internet to visit its Web page and find out.
3. Using the resources available in your library, find out what laws your state has passed to prosecute computer crime.
4. Using a Web browser go to *www.eff.org*. What are the current top concerns of this organization?
5. Using the ethical scenarios presented in the chapter, finish each of the incomplete statements, and bring your answers to class to compare them with those of your peers.

Case Exercises

Iris called the company security hotline. The hotline was an anonymous way to report any suspicious activity or abuse of company policy, although Iris chose to identify herself. The next morning, she was called to a meeting with an investigator from corporate security, which led to more meetings with others in corporate security, and then finally a meeting with the director of human resources and Gladys Williams, the CIO of SLS.

Questions:

1. Why was Iris justified in determining who the owner of the CD was?
2. Should Iris have approached Henry directly, or was the hotline the most effective way to take action? Why do you think so?
3. Should Iris have placed the CD back at the coffee station and forgotten the whole thing? Explain why that action would have been ethical or unethical.

Endnotes

1. Noone, John B. *Rousseau's Social Contract: A Conceptual Analysis*. Athens: University of Georgia Press, 1981.
2. Alberts, Robert J., Townsend, Anthony M., and Whitman, Michael E. "The Threat of Long-arm Jurisdiction to Electronic Commerce." *Communications of the ACM* 41, no. 12 (December 1998): 15–20.
3. Yeh, B., and Doyle, C. "USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis" CRS Report for Congress. Accessed 22 February 2007 from www.fas.org/sgp/crs/intel/RL33332.pdf.

Not For Sale

4. EPIC. "The Clipper Chip." Accessed 6 March 2004 from www.epic.org/crypto/clipper/.
5. American Heritage Dictionary. "Privacy." *The American Heritage Dictionary of the English Language Online*. Accessed 22 February 2007 from www.bartleby.com/61/87/P0568700.html.
6. HIPAAAdvisory. "HIPAA Primer." *HIPAAAdvisory Online*. Accessed 31 January 2007 from www.hipaadvisory.com/REGS/HIPAAprimer.htm.
7. Proofpoint, HIPAA and Beyond: An Update on Healthcare Security Regulations for Email. WWW Document viewed 6/10/2010 from www.findwhitepapers.com/force-download.php?id=8558.
8. FTC. "About Identity Theft." Accessed 22 February 2007 from www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.
9. Ibid.
10. FTC. "The President's Identity Theft Task Force Releases Comprehensive Strategic Plan to Combat Identity Theft." Accessed 25 April 2010 from www.ftc.gov/opa/2007/04/idtheft.shtm.
11. FTC. "If You Think Your Identity Has Been Stolen, Here's What To Do." Accessed 22 February 2007 from www.ftc.gov/bcp/edu/microsites/idtheft/.
12. WTO. "Understanding the TRIPS Agreement." Accessed 22 February 2007 from www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm.
13. The Computer Ethics Institute. "The 10 Commandments of Computer Ethics." *CEI Online*. 1992. Accessed 14 April 2007 from www.brook.edu/lits/cei/overview/Ten_Commandments_of_Computer_Ethics.htm.
14. Inquirer. "Software Piracy in Asia Exposed." *The Inquirer Online*. 27 January 2002. Accessed 14 April 2007 from www.theinquirer.net/piracy1.htm.
15. Whitman, Michael E., Townsend, Anthony M., and Hendrickson, Anthony R. "Cross-National Differences in Computer-Use Ethics: A Nine Country Study." *The Journal of International Business Studies* 30, no. 4 (1999): 673–687.
16. Ibid.
17. Harrington, Susan J. "The Effects of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgment and Intentions." *MIS Quarterly* 20, no. 3 (September 1996): 257–278.
18. International Information Systems Security Certification Consortium, Inc. "(ISC)² Code of Ethics." *(ISC)² Online*. Accessed 14 April 2007 from www.isc2.org/cgi/content.cgi?category=12.
19. ISSA. "ISSA Code of Ethics." *ISSA Online*. Accessed 14 April 2007 from www.issa.org/codeofethics.html.
20. National Security Agency. *Introduction to NSA/CSS*. Accessed 14 April 2007 from www.nsa.gov/about/index.cfm.
21. National Security Agency. *Information Assurance*. Accessed 14 April 2007 from www.nsa.gov/ial/.