Chapter 3: Law and 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 controversial 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

# Law and Ethics in Information Security

In general, people elect to trade some aspects of personal freedom for social order. **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/behaviours: 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

## 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 readingimpaired 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.
* 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 Kenyan Laws**

See Budapest convention for cybercrime and Kenya Cyber Crime Bill

# 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.

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 (violation). 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 endorsed 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 introduced

## *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

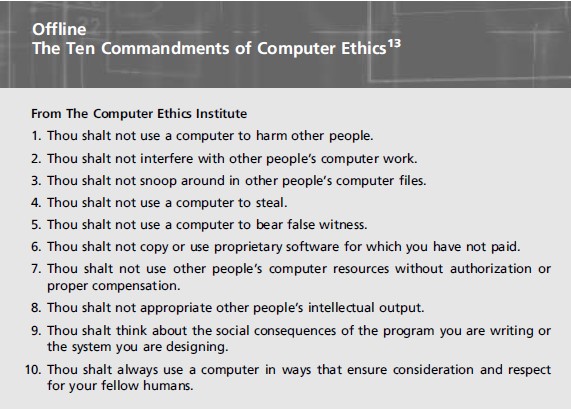
Prohibits the altering of information attached or imbedded into copyrighted material



Excludes Internet service providers from certain forms of related 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 (outstandingly bad or shocking)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 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



## 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. 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.

### Case Study

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. 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

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 a 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

# 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

# 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. 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 below provides an overview of these organizations. Many of these organizations offer certification programs that require the applicants to subscribe formally to the ethical codes.

**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 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) (**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) is primarily designed for information security professionals who have earned an (ISC) 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. “This code enables (ISC) 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)](http://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), ISACA, and the ACM, whose focus is “promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources.”

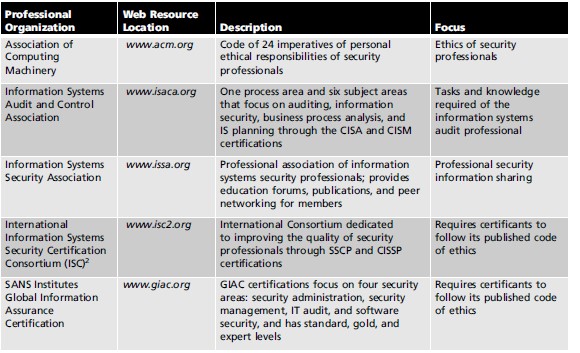


Table 1: Professional Organization of Interest to Information Security Professionals