




Legal, Ethical, and Professional Issues in Information Security

Chapter 3



Law and Ethics in Information Security

- ▶ Laws
 - ▶ Rules that mandate or prohibit certain behavior
 - ▶ Drawn from ethics
- ▶ Ethics
 - ▶ Define socially acceptable behaviors
- ▶ Key difference
 - ▶ Laws carry the authority of a governing body
 - ▶ Ethics do not carry the authority of a governing body
 - ▶ Based on cultural mores
 - ▶ Fixed moral attitudes or customs
 - ▶ Some ethics standards are universal



Organizational Liability and the Need for Counsel

- ▶ Liability
 - ▶ Legal obligation of organization
 - ▶ Extends beyond criminal or contract law
 - ▶ Include legal obligation to restitution
 - ▶ Employee acting with or without the authorization performs and illegal or unethical act that causes some degree of harm
 - ▶ Employer can be held financially liable
- ▶ Due care
 - ▶ Organization makes sure that every employee knows what is acceptable or unacceptable
 - ▶ Knows the consequences of illegal or unethical actions



Organizational Liability and the Need for Counsel

- ▶ Due diligence
 - ▶ Requires
 - ▶ Make a valid effort to protect others
 - ▶ Maintains the effort
- ▶ Jurisdiction
 - ▶ Court's right to hear a case if a wrong is committed
 - ▶ Term – long arm
 - ▶ Extends across the country or around the world



Policy Versus law

- ▶ Policies
 - ▶ Guidelines that describe acceptable and unacceptable employee behaviors
 - ▶ Functions as organizational laws
 - ▶ Has penalties, judicial practices, and sanctions
- ▶ Difference between policy and law
 - ▶ Ignorance of policy is acceptable
 - ▶ Ignorance of law is unacceptable
- ▶ Keys for a policy to be enforceable
 - ▶ Dissemination
 - ▶ Review
 - ▶ Comprehension
 - ▶ Compliance
 - ▶ Uniform enforcement



Types of Law



- Civil – govern a nation or state
- Criminal – addresses activities and conduct harmful to public
- Private – encompasses family, commercial, labor, and regulates the relationship between individuals and organizations
- Public – regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments



International Laws and Legal Bodies

- Organizations do business on the Internet – they do business globally
- Professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries
- Few international laws relating to privacy and informational security
- International laws are limited in their enforceability



Council of Europe Convention on Cybercrime

- ▶ International task force
- ▶ Designed to oversee range of security functions
- ▶ Designed to standardized technology laws across international borders
- ▶ Attempts to improve the effectiveness of international investigations into breaches of technology law
- ▶ Concern raised by those concerned with freedom of speech and civil liberties
- ▶ Overall goal
 - ▶ Simplify the acquisition of information for law enforcement agencies in certain types of international crimes



Agreement on Trade-Related Aspects of Intellectual Property Rights

- Created by the World Trade Organization
- Introduced intellectual property rules into the multilateral trade system
- First significant international effort to protect intellectual property rights



Agreement on Trade-Related Aspects of Intellectual Property Rights

- ▶ 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


- ▶ American contribution to WTO
- ▶ Plan to reduce the impact of copyright, trademark, and privacy infringement
- ▶ United Kingdom has implemented a version
 - ▶ Database Right



DMCA 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




Major IT Professional Organizations

- ▶ Association of Computing Machinery
 - ▶ “World's first educational and scientific computing society”
 - ▶ Strongly promotes education
 - ▶ Provides discounts for student members
- ▶ International Information Systems Security Certification Consortium, Inc. (ISC)²
 - ▶ Nonprofit organization
 - ▶ Focuses on the development and implementation of information security certifications and credentials
 - ▶ Manages a body of knowledge on information security
 - ▶ Administers and evaluated examinations for information security certifications



Major IT Professional Organizations

- ▶ Information Systems Audit and Control Association
 - ▶ Focuses on auditing, control, and security
 - ▶ Membership includes technical and managerial professionals
 - ▶ Does not focus exclusively on information security
 - ▶ Has many information security components
- ▶ Information Systems Security Associations (ISSA)
 - ▶ Nonprofit society of information security professionals
 - ▶ Mission – bring together qualified information security practitioners
 - ▶ Information exchange
 - ▶ Education development
 - ▶ Focus – “promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources”



Major IT Professional Organizations

- ▶ Systems Administration, Networking, and Security Institute (SANS)
 - ▶ Professional research and education cooperative
 - ▶ Current membership > 156,000
 - ▶ Security professionals
 - ▶ Auditors
 - ▶ System administrators
 - ▶ Network administrators
 - ▶ Offers set of certifications



Federal Agencies

- ▶ Department of Homeland Security
 - ▶ Five directorates or divisions
 - ▶ Mission – protecting the people as well as the physical and informational assets of the United States
 - ▶ Directorate of Information and Infrastructure
 - ▶ Creates and enhances resources used to discover and responds to attacks on national information systems and critical infrastructure
 - ▶ Directorate of Science and Technology
 - ▶ Research and development activities in support of homeland defense
 - ▶ Examination of vulnerabilities
 - ▶ Sponsors emerging best practices



Federal Agencies

- ▶ National InfraGard Program
 - ▶ Each FBI office establishes a chapter
 - ▶ Collaborates with public and private organizations and academia
 - ▶ Serves members in 4 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
 - ▶ Contribution – free exchange of information to and from the private sector in the areas of threats and attacks on information resources



Federal Agencies



- National Security Agency (NSA)

“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.”

- U. S. Secret Service

- Located in Department of the Treasury

- Charged with the detection and arrest of any person committing a United States federal offense relating to computer fraud and false identification crimes.