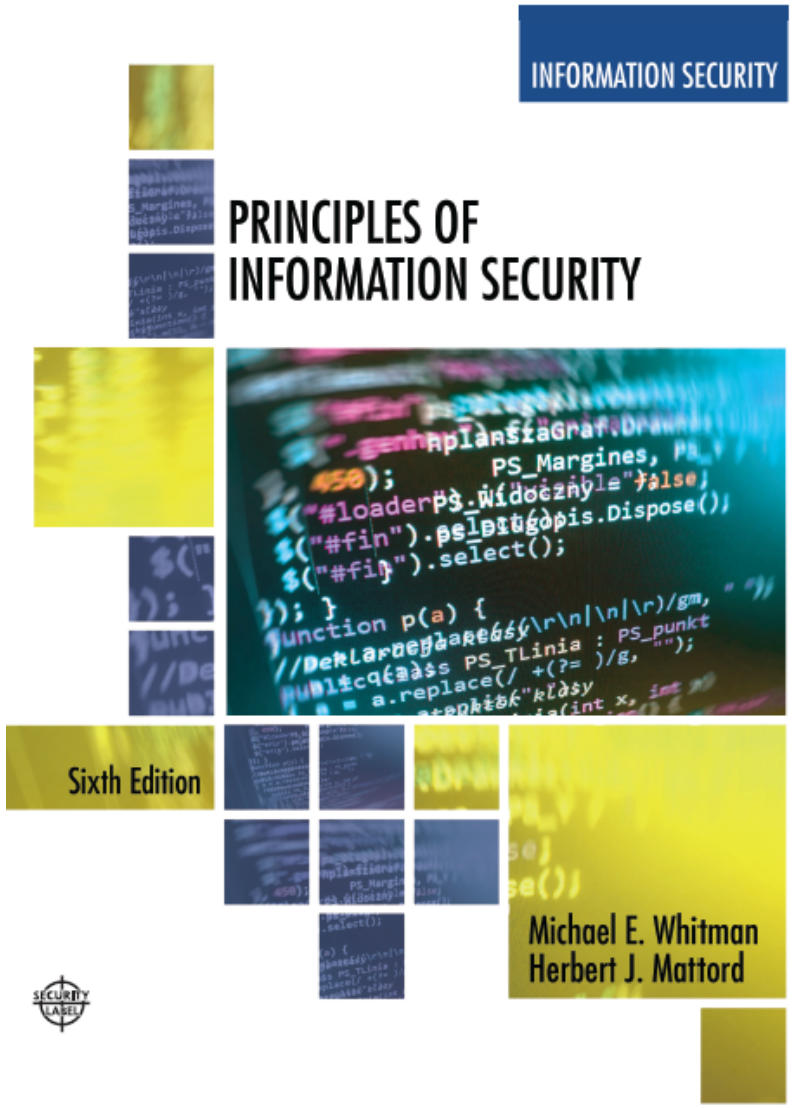

Source: Principles of Information Security

Chapter 3

Legal, Ethical, and Professional Issues in Information Security

Dr. Ibrahim Waziri Jr.

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
- Explain the differences between laws and ethics
- Identify major national laws that affect the practice of information security
- Discuss the role of privacy as it applies to law and ethics in information security

Introduction

Every Information Security professional must understand the scope of an organization's legal and ethical responsibilities.

To minimize liabilities/reduce risks, the information security practitioner must:

- Understand the current legal environment
- Stay current with laws and regulations
- Watch for new and emerging issues

Policy vs Law

Policies: managerial directives that specify acceptable and unacceptable employee behavior in the workplace.

Criteria for policy enforcement:

- Dissemination (distribution)
- Review (reading)
- Comprehension (understanding)
- Compliance (agreement)
- Uniform enforcement

Laws: rules that mandate or prohibit certain behavior and are enforced by the state

Types of Law:

- Constitutional
- Statutory
- Civil - Tort
- Criminal
- Regulatory or Administrative
- Common Case, and Precedent
- Private and Public

Difference between policy and law: Ignorance of a policy is an acceptable defense.

Ethics

Ethics: regulate and define socially acceptable behavior.
Cultural mores: fixed moral attitudes or customs of a particular group

Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical.
- Difficulties arise when one nationality's ethical behavior conflicts with the ethics of another national group.

Organization Liabilities in Info Sec

- **Liability:** the legal obligation of an entity extending beyond criminal or contract law; includes the legal obligation to make restitution
- **Restitution:** the legal obligation to compensate an injured party for wrongs committed
- **Due care:** the legal standard requiring a prudent organization to act legally and ethically and know the consequences of actions
- **Due diligence:** the legal standard requiring a prudent organization to maintain the standard of due care and ensure actions are effective
- **Jurisdiction:** court's right to hear a case if the wrong was committed in its territory or involved its citizenry
- **Long-arm jurisdiction:** application of laws to those residing outside a court's normal jurisdiction; usually granted when a person acts illegally within the jurisdiction and leaves

Laws carry the authority of a governing authority; ethics do not

Deterring Unethical and Illegal Behavior

- Three general causes of unethical and illegal behavior are: ignorance, accident, intent.

- Deterrence: best method for preventing an illegal or unethical activity are: laws, policies, technical controls

- Laws and policies only deter if three conditions are present:
  - Fear of penalty
  - Probability of being apprehended
  - Probability of penalty being applied

U.S Federal, States and Local Laws

Information security professionals are responsible for understanding federal, state and local laws and regulations, and also ensuring that organization is in compliance with regulations.

General Computer Crime Laws
- Computer Fraud and Abuse Act of 1986 (CFA Act)
- Computer Security Act of 1987
- National Information Infrastructure Protection Act of 1996
- USA PATRIOT Act of 2001
  - USA PATRIOT Improvement and Reauthorization Act
- USA FREEDOM Act - Inherited select USA PATRIOT functions as the PATRIOT act expired in 2015

Identity Theft
- Title 18, U.S.C. § 1028). - Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information Act

Export and Espionage Laws
- Economic Espionage Act of 1996
- Security and Freedom through Encryption Act of 1999

Privacy and Information Sharing
- Title 47, U.S.C § 222 **-** Privacy of Customer Information Section of the common carrier regulation
- Federal Privacy Act of 1974
- Electronic Communications Privacy Act of 1986
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), aka Kennedy-Kassebaum Act
- Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999
- Child Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Freedom of Information Act of 1966 (FOIA)

U.S Copyright Laws
- U.S. Copyright Office Web site: www.copyright.gov/.

Financial Reporting
- Sarbanes-Oxley Act of 2002

Key U.S. Federal Agencies

Department of Defense (DoD)

- National Security and Armed Forces

Central Intelligence Agency (CIA)

- National Security Intelligence Gathering and Processing

Department of Homeland Security (DHS)

- United States Computer Emergency Readiness Team (US-CERT)

U.S. Secret Service

- U.S financial infrastructure and payments system.

National Security Agency (NSA)

- Cryptography
- Signal Intelligence and Information Assurance Directorate (IAD)

Federal Bureau of Investigation (FBI)

- Investigates traditional crimes and cybercrimes
- U.S InfraGard Program: Maintains an intrusion alert, suspicious activities and secure web/network communications.

European Computer Security Laws

Computer Misuse Act 1990 (UK): Defined three "computer misuse offenses": Unauthorized access to computer material, Unauthorized access with intent to commit or facilitate commission of further offenses and Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

Privacy and Electronic Communications (EC Directive) Regulations 2003: Focuses on protection against unwanted or harassing phone, e-mail, and SMS messages.

Police and Justice Act 2006 (UK): Updated the Computer Misuse Act, modified the penalties, and created new crimes defined as the "unauthorized acts with intent to impair operation of computer, etc."

General Data Protection Regulation (GDPR): is a regulation in EU law on data protection and privacy for all individuals citizens of the European Union and the European Economic Area.

International Laws and Legal Bodies

Agreement on Trade-Related Aspect of Intellectual Property Rights - Created by the World Trade Organization (WTO) This is the first significant international effort to protect intellectual property rights; outlines requirements for governmental oversight and legislation providing minimum levels of protection for intellectual property.

Digital Millennium Copyright Act (DMCA) - U.S. contribution to international effort to reduce impact of copyright, trademark, and privacy infringement in response to European Union Directive 95/46/EC.

Council of Europe Convention on Cybercrime - Created international task force to oversee Internet security functions for standardized international technology laws.

Payment Card Industry Data Security Standards (PCI DSS) - PCI Security Standards Council offers a standard of performance to which organizations processing payment cards must comply.

Information Security Professional Organizations

- Many professional organizations have established codes of conduct/ethics.
- Codes of ethics can have a positive effect; unfortunately, many employers do not encourage joining these professional organizations.
- Responsibility of security professionals is to act ethically and according to the policies of the employer, the professional organization, and the laws of society.

Professional Organization	Web Resource Location	Description	Focus
Association of Computing Machinery (ACM)	www.acm.org	Code of 24 imperatives of personal and ethical responsibilities for security professionals	Ethics of security professionals
Information Systems Audit and Control Association (ISACA)	www.isaca.org	Focus on auditing, information security, business process analysis, and IS planning through the OSA and OSM certifications	Tasks and knowledge required of the information systems audit professional
Information Systems Security Association (ISSA)	www.issa.org	Professional association of information systems security professionals; provides education forum, 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 Institute's Global Information Assurance Certification (GIAC)	www.giac.org	GIAC certifications focus on four security areas: security administration, security management IT audits, and software security, these areas have standard, gold, and expert levels	Requires certificants to follow its published code of ethic

Summary

- Laws: rules that mandate or prohibit certain behavior in society; drawn from ethics
- Ethics: define socially acceptable behaviours, based on cultural mores (fixed moral attitudes or customs of a particular group)
- Types of law: civil, criminal, private, and public
- Relevant U.S. laws:
- Many organizations have codes of conduct and/or codes of ethics.
- Organization increases liability if it refuses to take measures known as due care.
- Due diligence requires that organizations make a valid effort to protect others and continually maintain that effort.