Management of Information Security, 4th Edition

Chapter 12

Law and Ethics

Acknowledgement: with very minor modification from the author's slides

Objectives

- Differentiate between law and ethics
- Describe the ethical foundations and approaches that underlie modern codes of ethics
- Identify major national and international laws that relate to the practice of InfoSec
- Describe the role of culture as it applies to ethics in InfoSec
- Discuss current laws, regulations, and relevant professional organizations

Law and Ethics in InfoSec

- **Laws** - rules adopted and enforced by governments to codify expected behavior in modern society
- **Ethics** - define socially acceptable behaviors that conform to the widely held principles of the members of that society
- **Cultural mores** - relatively fixed moral attitudes or customs of a societal group
- Some ethics are thought to be universal
  - Example: murder, theft, and assault are actions that deviate from ethical/legal codes in most cultures

Types of Law

- **Civil law** - laws pertaining to relationships between and among individuals and organizations
- **Criminal law** - addresses violations harmful to society and is enforced and prosecuted by the state
- **Tort law** - allows individuals to seek redress in the event of personal, physical, or financial injury
  - Subset of **Civil Law**
- Legislation affecting individuals in workplace
  - **Private law -** regulates relationships among individuals and organizations (family law, labor law, commercial law, etc.)
  - **Public law -** regulates the structure and administration of government agencies

Relevant U.S. Laws

- The United States has led the development and implementation of InfoSec legislation to prevent misuse and exploitation of information and information technology
  - This development promotes the general welfare and creates a stable environment for a solid economy
- Table 12-1 on pages 448-450:
  - Summarizes the U.S. federal laws relevant to InfoSec

General Computer Crime Laws

- **Computer Fraud and Abuse (CFA) Act** - the cornerstone of many computer-related federal laws and enforcement efforts
  - Was amended by the National Information Infrastructure Protection Act of 1996, which modified several sections of the previous act and increased penalties for selected crimes
- The CFA was further modified by the USA PATRIOT Act of 2001
  - Provides law enforcement agencies with broader latitude to combat terrorism-related activities

General Computer Crime Laws

- **Computer Security Act (CSA)** - was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices
- The CSA established a Computer System Security and Privacy Advisory Board
- The CSA also amended the Federal Property and Administrative Services Act of 1949
- CSA requires mandatory training in computer security awareness and accepted computer security practice for all federal employees

Privacy Laws

- Many organizations collect, trade, and sell personal information as a commodity
  - The number of statues addressing individual privacy rights has grown
- Privacy is defined as the “state of being free from unsanctioned intrusion”
  - It is possible to track this freedom from intrusion to the Fourth Amendment of the U.S. Constitution
- The Privacy of Customer Information –
  - specifies proprietary information shall be used for providing services, not for marketing

Privacy Laws

- The Federal Privacy Act of 1974 regulates the government's use of private information
- The following entities are exempt from some of the regulations so they can perform their duties:
  - Bureau of the Census
  - National Archives and Records Administration
  - U.S. Congress
  - Comptroller General
  - Certain court orders
  - Credit agencies

Privacy Laws

- **The Electronic Communications Privacy Act (ECPA)** of 1986 - a collection of statutes that regulates the interception of wire, electronic, and oral communications
- ECPA statutes address the following:
  - Interception and disclosure of wire, oral, and electronic communications
  - Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices
  - Confiscation of wire, oral, or electronic communication intercepting devices

Privacy Laws

- ECPA statutes address the following (cont'd):
  - Evidentiary use of intercepted wire or oral communications
  - Authorization for interception of wire, oral, or electronic communications
  - Authorization for disclosure and use of intercepted wire, oral, or electronic communications
  - Procedure for and reports concerning interception of wire, oral, or electronic communications
  - Injunction against illegal interception

Privacy Laws

- **Health Insurance Portability and Accountability Act (HIPAA)** of 1996 –
  - attempts to protect the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange
    - Also known as the Kennedy-Kassebaum Act
    - Affects all health care organizations
- Privacy standards of HIPAA
  - severely restrict the dissemination and distribution of private health information without documented consent
  - Known as the HIPAA Privacy Rule

Privacy Laws

- HIPAA has five fundamental privacy principles:
  - Consumer control of medical information
  - Boundaries on the use of medical information
  - Accountability for the privacy of private information
  - Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
  - Security of health information

ARRA and HITECH

- American Recovery and Reinvestment Act (ARRA)
  - was designed to provide a response to the economic crisis in the U.S.
  - Included another act called the Health Information Technology for Economic and Clinical Health (HITECH)
- HIPAA and HITECH require that covered entities notify information owners of breaches

Gramm-Leach Bliley (GLB) Act of 1999

- The Gramm-Leach Bliley (GLB) Act –
  - contains a number of provisions that affect banks, securities firms, and insurance companies
    - Requires all financial institutions to disclose their privacy policies
    - Also ensures that the privacy policies in effect in an organization are fully disclosed when a customer initiates a business relationship
      - Are distributed annually for the duration of the professional association
  - aka the Financial Modernization Act of 1999

Gramm-Leach-Bliley Act

- The Act consists of three sections:
  - The Financial Privacy Rule,
    - regulates the collection and disclosure of private financial information;
  - The Safeguards Rule,
    - stipulates that financial institutions must implement security programs to protect such information; and
  - The Pretexting provisions
    - prohibit the practice of pretexting (accessing private information using false pretenses).

Export and Espionage Laws

- Economic Espionage Act (EEA) –
  - attempts to protect trade secrets
  - Intended to protect intellectual property and competitive advantage
- Security and Freedom through Encryption Act –
  - provides guidance on the use of encryption and institutes measures of public protection from government intervention

Homeland Security Act

- Primary goal:
  - ‘to prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize damage and assist in recovery for terrorist attacks that occur in the United States’
- Created DHS which includes a privacy office whose objectives are:
  - Evaluating the department's legislative and regulatory proposals that involve the collection, use, and disclosure of personally identifiable information
  - Centralizing and providing program oversight and implementing all FOIA and Privacy Act operations
  - Operating a privacy incident response program that addresses incidents involving personally identifiable information
  - Responding to, investigating, and addressing complaints of privacy violations
  - Providing training, education, and outreach that build the foundation for privacy practices across the department and create transparency

FERPA

- The Family Educational Rights and Privacy Act
  - a Federal law that protects the privacy of student education records.
  - gives parents certain rights with respect to their children's education records.
  - prohibits the disclosure of a student's "protected information" to a third party
- It classifies protected info into three categories:
  1. educational information;
  2. personally identifiable information; and
  3. directory information. The limitations imposed by FERPA vary with respect to each category.

U.S. Copyright Law

- U.S. Copyright Law - extends protection to intellectual property
  - Which includes words published in electronic formats
  - The doctrine of fair use allows materials to be quoted for the purpose of news reporting, teaching, scholarship, and a number of other related activities

Freedom of Information Act (FOIA) of 1966

- Under FOIA, all federal agencies are required to disclose records requested in writing by any person
  - Agencies may withhold information
    - pursuant to nine exemptions and three exclusions contained in the statute
  - Applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies

Sarbanes-Oxley (SOX) Act of 2002

- Sarbanes-Oxley Act –
  - designed to enforce accountability for the financial reporting and record-keeping at publicly traded corporations
    - Requires that the CEO and CFO assume direct and personal accountability for the completeness and accuracy of a publicly traded organization's financial reporting and record-keeping systems
  - CIOs are responsible for the security, accuracy, and reliability of the systems that manage and report the financial data

Payment Card Industry Data Security Standard (PCI DSS)

- Payment Card Industry Data Security Standard (PCI DSS) –
  - a set of industry standards that are mandated for any organization that handles credit, debit, and specialty payment cards
  - Created in an effort to reduce credit card fraud
- PCI DSS includes three sub-standards:
  - *PCI Data Security Standard*
  - *PIN Transaction Security Requirements*
  - *Payment Application Data Security Standard*

Payment Card Industry Data Security Standard (PCI DSS)

- PCI Security Standards Council has identified six steps associated with PCI DSS:
  - *Build and Maintain a Secure Network*
  - *Protect Cardholder Data*
  - *Maintain a Vulnerability Management Program*
  - *Implement Strong Access Control Measures*
  - *Regularly Monitor and Test Networks*
  - *Maintain an Information Security Policy*

The Future of U.S. Information Security Laws

- Bills that are fighting their way through U.S. Congress, are designed to protect consumers by requiring reasonable security policies and procedures to protect personal information:
  - Data Security Act of 2010
  - Data Security and Breach Notification Act of 2010
  - Cybersecurity Act of 2012
- All of the above bills failed to pass
  - It is expected that similar legislation will inevitably make its way through Congress

International Laws and Legal Bodies

- Many domestic laws and customs do not apply to international trade
- Few international laws currently relate to privacy and InfoSec
- These international security bodies and regulations are sometimes limited in scope and enforceability

European Council Cybercrime Convention

- Drafted in 2001, the European Council Cybercrime Convention
  - empowers an international task force to oversee a range of Internet security functions
  - To standardize technology laws across international borders
- Goal:
  - simplify the acquisition of information for law enforcement agents in certain types of international crimes as well as during the extradition process

Digital Millennium Copyright Act (DMCA)

- Digital Millennium Copyright Act (DMCA) –
  - the U.S.-based international effort to reduce the impact of copyright, trademark, and privacy infringement
- The European Union equivalents to the DMCA are Directive 95/46/EC of the European Parliament
  - Which also increase individual rights to process and freely move personal data
  - The United Kingdom has implemented a version of this directive
    - Called the Database Right

Australian High Tech Crime

- Australia's Computer Offences of the Criminal Code Act 1995 specifically includes:
  - Data system intrusions (such as hacking)
  - Unauthorized destruction or modification of data
  - Actions intended to deny service of computer systems to intended users
    - Such as denial-of-service (DoS) attacks
  - The creation and distribution of malware

State and Local Regulations

- Each state and locality may have a number of laws and regulations related to IT
  - Example:
    - the state of Georgia passed the Georgia Computer Systems Protection Act in 1991
    - Georgia legislature also passed the Georgia Identity Theft Law in 1998
    - The law requires businesses to destroy or erase personal information before discarding a record

Policy versus Law

- The key difference between policy and law is that ignorance of policy is a viable defense, therefore policies must be:
  - Distributed to all individuals who are expected to comply with them
  - Readily available for employee reference
  - Easily understood, with multilingual translations and translations for visually impaired or low-literacy employees
  - Acknowledged by the employee
  - Uniformly enforced for all employees

Ethics in InfoSec

- The foundations and frameworks of ethics include:
  - *Normative ethics* - the study of what makes actions right or wrong
  - *Meta-ethics* - the study of the meaning of ethical judgments and properties
  - *Descriptive ethics* - study of the choices that have been made by individuals in the past
  - *Applied ethics* - applies moral codes to actions drawn from realistic situations
  - *Deontological ethics* - study of the rightness or wrongness of intentions and motives

Ethics in InfoSec

- From ethical frameworks come a series of ethical standards:
  - *Utilitarian approach* - emphasizes that an ethical action is one that results in the most good
  - *Rights approach* - the ethical action is the one that best protects and respects the moral rights of those affected by that action
  - *Fairness or justice approach* - defines ethical actions as those that have outcomes that regard all human beings equally

Ethics in InfoSec

- From ethical frameworks come a series of ethical standards (cont'd):
  - *Common good approach* - this approach tends to focus on the common welfare
  - *Virtue approach* - ethical actions ought to be consistent with so-called ideal virtues
- These ethical standards or approaches offer a set of tools for decision making in the era of computer technology

Ethics and Education

- Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education
- Employees must be trained and kept up to date on InfoSec topics
  - Including the expected behaviors of an ethical employee
- Proper ethical and legal training is vital to creating an informed, well-prepared, and low-risk system user

Deterring Unethical and Illegal Behavior

- Three general categories of unethical behavior that organizations and society should seek to eliminate:
  - Ignorance
  - Accident
  - Intent
- **Deterrence** - the best method for preventing an illegal or unethical activity
  - Laws, policies, and technical controls are all examples of deterrents

Deterring Unethical and Illegal Behavior

- Laws and policies and their associated penalties only deter if three conditions are present:
  - *Fear of penalty*
  - *Probability of being caught*
  - *Probability of penalty being administered*

Professional Organizations and Their Codes of Ethics

- A number of professional organizations have established codes of conduct and/or codes of ethics that members are expected to follow
  - Code of ethics can have a positive effect on an individual's judgment regarding computer use
- The following sections describe several of the relevant professional associations

Association for Computing Machinery (ACM)

- ACM - was established in 1947 as the world's first educational and scientific computing society
  - It is one of the few organizations that strongly promote education and provide discounted membership for students
- The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional
  - Contains specific references to protecting the confidentiality of information, causing no harm, protecting the privacy of others, and respecting intellectual property of others

International Information Systems Security Certification Consortium, Inc. $(ISC)^2$

- $(ISC)^2$ is a nonprofit organization that focuses on the development and implementation of InfoSec certifications and credentials
- The code of ethics put forth by $(ISC)^2$ includes four mandatory canons:
  - Protect society, the commonwealth, and the infrastructure
  - Act honorably, honestly, justly, responsibly, and legally
  - Provide diligent and competent service to principals
  - Advance and protect the profession

SANS

- Formerly known as the System Administration, Networking, and Security Institute
- SANS - a professional research and education cooperative organization
  - Dedicated to the protection of information and systems
- Individuals who seek one of SANS's many Global Information Assurance Certification (GIAC) credentials must agree to comply with the organization's code of ethics

Information Systems Audit and Control Association (ISACA)

- ISACA - a professional association with a focus on auditing, control, and security
  - Membership comprises both technical and managerial professionals
  - Focuses on providing IT control practices and standards
- ISACA offers the Certified Information Systems Auditor (CISA) certification
  - Which contains many InfoSec components

Information Systems Security Association (ISSA)

- The ISSA is a nonprofit society of InfoSec professionals
  - Its primary mission is to bring together qualified practitioners of InfoSec for information exchange and educational development
- ISSA supports a code of ethics similar to those of previously discussed organizations
  - Goal is to promote management practices that will ensure the confidentiality, integrity, and availability of organizational information resources

Organizational Liability and the Need for Counsel

- Liability for a wrongful act includes an obligation to make payment or restitution
  - Can be applied to conduct even when no law or contract has been breached
- An organization increases its liability if it refuses to take measures to make sure employees know what is acceptable and what is not
- **Jurisdiction** - a court's right to hear a case
  - Any court can impose its authority if the act was committed in its territory or involve its citizenry
  - Sometimes referred to as "**long-arm jurisdiction**"

Key Law Enforcement Agencies

- Local law enforcement is capable of handling physical security threats or employee problems
  - It is usually ill equipped to handle electronic crimes
- A number of key federal agencies are charged with the protection of U.S. information resources
  - FBI InfraGard organization
  - Department of Homeland Security (DHS) National Protection and Programs Directorate
  - The NSA
  - The U.S. Secret Service

Managing Investigations in the Organization

- **Digital forensics** - involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
- **Evidentiary material (EM)** - any information that could potentially support the organization's legal-based or policy-based case against a suspect
- **E-discovery** - the identification and preservation of EM related to a specific legal action

Managing Investigations in the Organization

- Digital forensics can be used for two key purposes:
  - *To investigate allegations of digital malfeasance*
    - Which is a crime against or using digital media, computer technology, or related components
  - *To perform root cause analysis*
- An organization must choose one of two approaches when employing digital forensics:
  - *Protect and forget*
  - *Apprehend and prosecute*

Digital Forensics Team

- Most organizations cannot sustain a permanent digital forensics team
  - May be better to collect the data and then outsource the analysis component to a regional expert
- There should be people in the InfoSec group trained to understand and manage the forensics process
  - Expertise can be obtained by sending staff members to a regional or national InfoSec conference with a digital forensics track

Affidavits and Search Warrants

- **Affidavit** - sworn testimony that certain facts are in the possession of the investigating officer
  - That the officer believes warrant the examination of specific items located at a specific place
- When an approving authority signs the affidavit or creates a synopsis form based on this document, it becomes a **search warrant**
  - Permission to search and seize items

Digital Forensics Methodology

- In digital forensics, investigations follow the same basic methodology:
  - Identify relevant items of evidentiary value (EM)
  - Acquire (seize) the evidence without alteration or damage
  - Take steps to assure that the evidence is verifiably authentic and is unchanged
  - Analyze the data without risking modification or unauthorized access
  - Report the findings to the proper authority

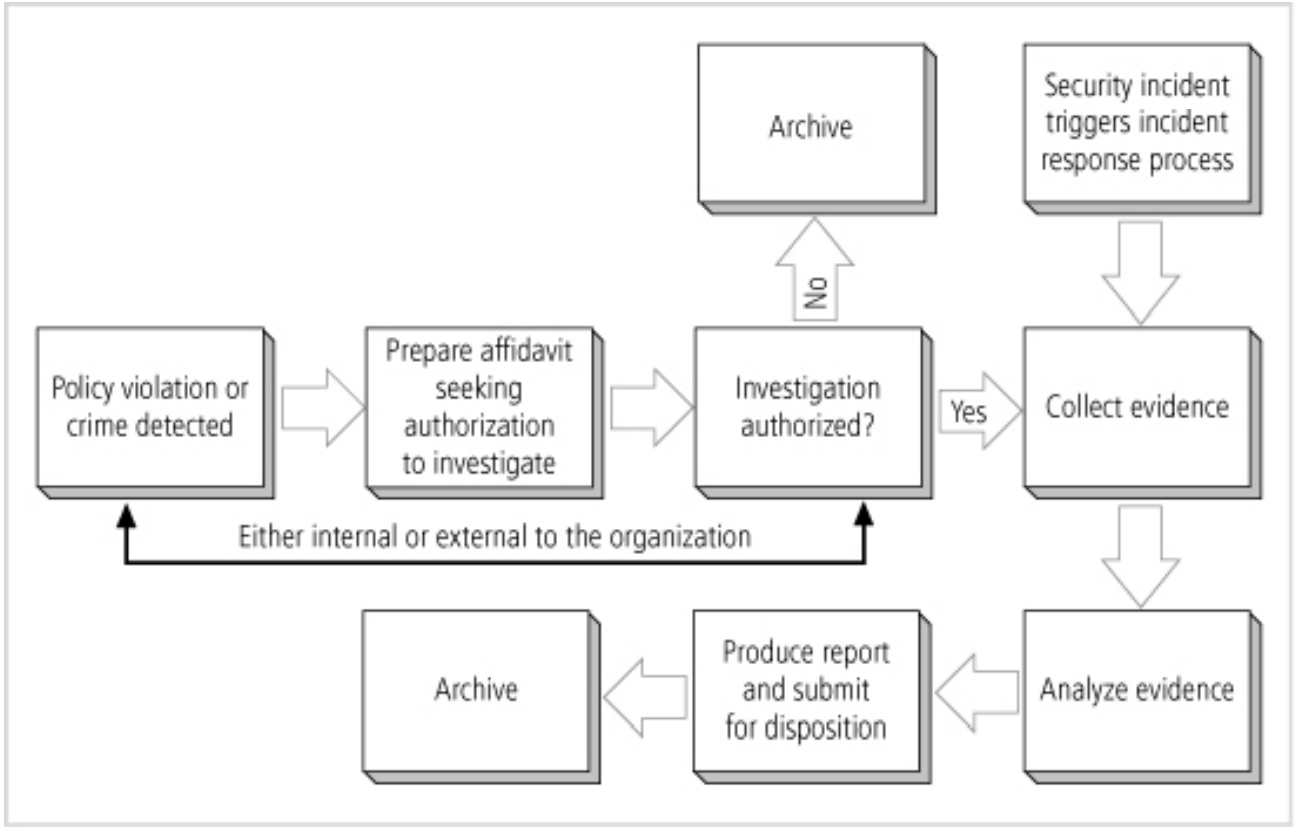

Figure 12-1 Digital forensics process

Evidentiary Procedures

- In digital forensics, the focus is on procedures
- Organizations should develop specific procedures, along with guidance on the use of these procedures
- The policy document should specify:
  - Who may conduct the investigation
  - Who may authorize an investigation
  - What affidavit-related documents are required
  - What search warrant-related documents are required

Evidentiary Procedures

- The policy document should specify (cont'd):
  - What digital media may be seized or taken offline
  - What methodology should be followed
  - What methods are required for chain of custody or chain of evidence
  - What format the final report should take and to whom it should be given
- By creating and using these policies and procedures, an organization can best protect itself from challenges by employees who have been subject to unfavorable action resulting from an investigation

Summary

- Laws are formally adopted rules for acceptable behavior in modern society
- Organizations formalize desired behaviors in documents called policies
- Civil law encompasses a wide variety of laws that regulate relationships between and among individuals and organizations
- The desire to protect national security, trade secrets, and a variety of other state and private assets has led to several laws affecting what information management and security resources may be exported from the U.S.

Summary

- U.S. copyright law extends intellectual property rights to the published word, including electronic publication
- Deterrence can prevent an illegal or unethical activity from occurring
- As part of an effort to sponsor positive ethics, a number of professional organizations have established codes of conduct and/or codes of ethics that their members are expected to follow
- A number of key U.S. federal agencies are charged with the protection of American information resources and the investigation of threats to these resources

Summary

- Digital forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
- Most organizations cannot sustain a permanent digital forensics team
- There should be people in the InfoSec group trained to understand and manage the forensics process