Legal, Ethical, and Professional Issues in Information Security

Learning Objectives

Upon completion of this topic, 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 laws (related to the US) that affect the practice of information security.
- Discuss the role of privacy as it applies to law and ethics in information security.

Introduction

- The **information security professional** must understand the scope/structure of an organization’s legal and ethical responsibilities.
- To minimize liabilities/reduce risks from electronic and physical threats, the information security professional must:
  1. Understand the current legal environment.
  2. Stay current with laws and regulations.
  3. Watch for new issues that emerge.
- In this topic, we will learn about the **laws** and **regulations** that affect the management of information in an organization.
- Finally, we will learn about the ethical issues related to information security.

Law and Ethics in Information Security

Basic Definitions of cultural mores, ethics, and laws:

- **Cultural mores** are the fixed moral attitudes or customs of a particular group.
- **Ethics** define socially acceptable behavior.
- **Laws** are rules that mandate or prohibit certain behavior and are enforced by the state.
- **Laws** carry sanctions of a governing authority; **ethics** do not.

Organizational Liability and the Need for Counsel

An **organization** should ensure that every employee knows what is acceptable and what is not, to meet the obligations imposed by laws or regulations. **Why?**

- To maintain the reputation of the company and its employees.
- To preserve the rights of the company, employees, and customers for example.
- Finally, because an **employee** can perform an **illegal** or **unethical** that causes some degree of harm, the employer can be held financially liable for the action. This entails/requires legal liability and sometimes compensation.

Policy and Law

- **Policy** is **defined** as the list of expectations that describe acceptable and unacceptable employee behavior in the workplace.
- **Policy** guidelines dictate certain behavior within the organization.
- Within an organization, information security professionals **help maintain security** via the establishment and enforcement of the policy.

Policy - Continue

For a policy to be **enforceable**, it must meet the following **five criteria**:

1. **Dissemination (distribution):** The organization must be able to prove that the policy has been made easily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
2. **Review (reading):** The organization must be able to prove that it disseminated the document (policies) in an understandable form, including versions for employees who are illiterate, and reading-impaired. Common techniques include recording the policy in many languages.

Policy - Continue

3. **Comprehension (understanding):** The organization must be able to prove that the employee understands the requirements and content of the policy. Common techniques include quizzes and other assessments.
4. **Compliance (agreement):** The organization must be able to improve that the employee agreed 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 indicating the employee has read, understood, and agreed to comply with the policy.

Policy - Continue

5. **Uniform enforcement:** The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employment status or assignment.

- **Note:** Only when all these five conditions are met can an organization penalize employees who violate a policy without fear of legal retribution.

Types of Law

There are several types of laws, the most common **four laws** are:

1. **Civil law.**
2. **Criminal law.**
3. **Private law.**
4. **Public law.**

Types of Law

1. **Civil Law:**

- Civil law includes a wide variety of laws about relationships between and among individuals and organizations.
- Civil law includes contract law, employment law, family law, and tort law.
- Tort law is the subset of civil law that allows individuals to demand redress (العدل) in the event of personal, physical, or financial injury.

Types of Law - Continue

2. **Criminal Law**

- Criminal law addresses violations harmful to society.
- Criminal law addresses rules associated with traffic law, public order, property damage, and personal damage.

Types of Law - Continue

3. **Private Law**

- Private law is considered a subset of civil law and regulates the relationships among individuals as well as relationships between individuals and organizations; it encompasses family law, commercial law, and labor law.

Types of Law - Continue

4. **Public Law**

- Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments.
- Public law includes criminal law, administrative law, and constitutional law.

Types of Law - Continue

- Regardless of how the laws are categorized, it is important to understand which laws and regulations are relevant to your organization and what the organization needs to do to comply.
- There are a lot of international laws related to information security.
- The USA has been a leader in the development and implementation of security legislation.
- Specially, we are trading globally, and we have more business at the international level.
- So, we need to have these kinds of laws established to be able to communicate with each other.

Table 1: Summary of information security – Related to U.S. laws.

Area	Act	Date	Description
Online commerce and information protection.	Federal Trade Commission Act (FTCA).	1914	Recently used to challenge organizations with deceptive claims regarding the privacy and security of customers’ personal information.
Protection of credit information.	Fair Credit Reporting Act (FCRA).	1970	Regulates the collection and use of consumer credit information.

Table 1: Summary of information security – Related to U.S. laws.

Area	Act	Date	Description
Privacy.	Federal privacy Act	1974	Governs federal agency use of personal information.
Copyright.	Copyright Act (update to U.S. Copyright Law (17 USC)).	1976	Protects intellectual property, including publications and software.

Table 1: Summary of information security – Related to U.S. laws.

Area	Act	Date	Description
Cryptography	Electronic Communications Privacy Act (update to 18 USC.)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act.
Threats of computers	Computer Fraud and Abuse (CFA) 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).

Table 1: Summary of information security – Related to U.S. laws.

Area	Act	Date	Description
Encryption and digital signatures	Security and freedom Through Encryption Act.	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.
Spam	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act (15 USC 7701 et seq.).	2003	Sets the first national standards for regulating the distribution of commercial e-mail, including mobile phone spam.

Privacy

- **Privacy** in the context of information security is the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality.
- **Privacy violation**: A person may experience a violation of privacy in different forms, such as:
  - Many organizations collect, swap, and sell “**Personal Information”** such as name, location, address, Tel. Number, etc. as a commodity (goods), and as a result, many people are looking to governments to protect their privacy from such organizations by enforcing the laws and considering it a crime punishable by law.
  - Eavesdropping on phone calls, private messages, etc. “**Private Communication**”**.**

References

1. Richard A. Spinello. CYBERETHICS – Morality and Law in Cyberspace, Sixth Edition, Jones & Bartlett Learning, 2017.
2. David Kim and Michael G. Solomon. Fundamentals of Information Security, Third Edition, Jones & Bartlett Learning, 2018.