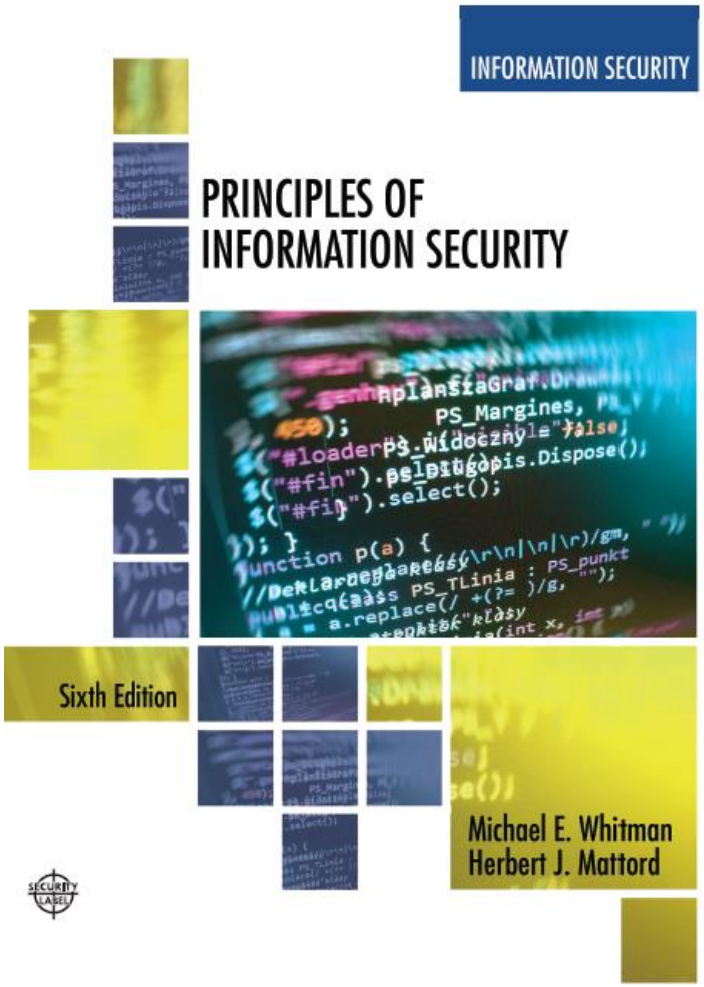
Principles of Information Security

Sixth Edition



Legal, Ethical, and Professional Issues in Information Security

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

- You 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

Law and Ethics in Information Security

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

Organizational Liability and the Need for Counsel (1 of 2)

- **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

Organizational Liability and the Need for Counsel (2 of 2)

- **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

Policy Versus Law (1 of 2)

- Policies: managerial directives that specify acceptable and unacceptable employee behavior in the workplace
- Policies function as organizational laws; must be crafted and implemented with care to ensure they are complete, appropriate, and fairly applied to everyone
- Difference between policy and law: Ignorance of a policy is an acceptable defense.

Policy Versus Law (2 of 2)

- Criteria for policy enforcement:
  - Dissemination (distribution)
  - Review (reading)
  - Comprehension (understanding)
  - Compliance (agreement)
  - Uniform enforcement

Types of Law

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

Cyber Laws in Pakistan

- Electronic Transaction Ordinance 2002
  - First IT-related legislation
  - Meant for protection of eCommerce business
  - Focused more on legal recognition of electronic documents
- Electronic Crimes Bill 2007
  - Defined several new offences, like electronic forgery, cyberstalking, data damage etc.
- Prevention of Electronic Crimes Act 2016
  - Revised form of 2007 bill

PECA 2016

- Defines several offenses and punishments
- Applies to
  - All over Pakistan
  - Pakistanis abroad
  - Persons outside Pakistan if they commits an offence affecting Pakistani persons or data

PECA 2016 full text

- https://pakistancode.gov.pk/pdffiles/administrator6a061efe0ed5bd153fa8b79b8eb4cba7.pdf

Some Offenses & Punishments

Action	Information/Data	Critical Infrastructure
Unauthorized Access	up to 3 months imprisonment and/or fine of up to Rs 50,000	3 years Rs 1 million
Unauthorized Copy	6 months Rs 1 lac	5 years Rs 5 million
Unauthorized Interference	2 years Rs 5 lac	7 years Rs 10 million

More offences

- Electronic forgery or fraud
- Using another person's identity
- Distributing and transmitting malicious code (malware)
- Cyber stalking / cyber bullying
  - Intimidating or harassing a person over electronic media
  - Includes blackmailing with inappropriate photo/video
- Spamming
  - Sending unsolicited information without permission from recipient (marketing emails/SMS)

Cognizable Offenses

Following offenses are cognizable, i.e. law enforcement can start arrests and investigation without judicial warrant.

- Cyber terrorism
  - Creating fear/panic in Government or public
  - Penalty of up to 14 year imprisonment and up to 50 million fine
- Offence against dignity of a person
  - e.g. spreading deepfake videos
- Child Pornography

Investigating Agency

- The act gives exclusive powers to Federal Investigative Agency (FIA) to investigate and charge cases against such crimes
  - Cybercrime wing of FIA is the only agency currently authorized.
  - Provincial police organizations are not authorized

PECA 2022 Amendment

- The section “Offence against dignity of a person” is amended to include online “defamation” of military authorities and judiciary.

Criticism

- https://www.amnesty.org/en/latest/news/2022/02/pakistan-repeal-draconian-cyber-crime-law/
- https://www.nchr.gov.pk/press_release/statement-against-the-prevention-of-electronic-crimes-amendment-ordinance-2022/

International Laws and Legal Bodies

- When 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.
- Because of the political complexities of relationships among nations and differences in culture, few international laws cover privacy and information security.
- These international laws are important but are limited in their enforceability.

WTO and the Agreement on Trade-Related Aspects of Intellectual Property Rights

- Created by the World Trade Organization (WTO)
- 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.
- Agreement covers five issues:
  - Application of basic principles of trading system and international intellectual property agreements
  - Giving adequate protection to intellectual property rights
  - Enforcement of those rights by countries within their borders
  - Settling intellectual property disputes between WTO members
  - Transitional arrangements while new system is being introduced

Digital Millennium Copyright Act (DMCA)

- U.S. contribution to international effort to reduce impact of copyright, trademark, and privacy infringement
- A response to European Union Directive 95/46/EC
- Prohibits
  - Circumvention of protections and countermeasures
  - Manufacture and trafficking of devices used to circumvent such protections
  - Altering information attached or imbedded in copyrighted material
- Excludes Internet Service Providers (ISPs) from some copyright infringement

Ethics and Information Security

- Many professional disciplines have explicit rules governing the ethical behavior of members.
- IT and InfoSec do not have binding codes of ethics.
- Professional associations and certification agencies work to maintain ethical codes of conduct.
  - Can prescribe ethical conduct
  - Do not always have the ability to ban violators from practice in field

Ten Commandments

The Ten Commandments of Computer Ethics from the Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.

Ten Commandments

7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

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.
- Scenarios are grouped into:
  - Software license infringement
  - Illicit use
  - Misuse of corporate resources
- Cultures have different views on the scenarios.

Table 3.2 Rates and Commercial Values of Unlicensed PC Software Installations Biennially from 2009 to 2015

Worldwide by Region

	Rates of Unlicensed Software Installations in 2015	Rates of Unlicensed Software Installations in 2013	Rates of Unlicensed Software Installations in 2011	Rates of Unlicensed Software Installations in 2009	Commercial Value of Unlicensed Software ($M) in 2015	Commercial Value of Unlicensed Software ($M) in 2013	Commercial Value of Unlicensed Software ($M) in 2011	Commercial Value of Unlicensed Software ($M) in 2009
Asia Pacific	61%	62%	60%	59%	$19,064	$21,041	$20,998	$16,544
Central & Eastern Europe	58%	61%	62%	64%	$3,136	$5,318	$6,133	$4,673
Latin America	55%	59%	61%	63%	$5,787	$8,422	$7,459	$6,210
Middle East & Africa	57%	59%	58%	59%	$3,696	$4,309	$4,159	$2,887
North America	17%	19%	19%	21%	$10,016	$10,853	$10,958	$9,379
Western Europe	28%	29%	32%	34%	$10,543	$12,766	$13,749	$11,750
Total Worldwide	39%	43%	42%	43%	$52,242	$62,709	$63,456	$51,443

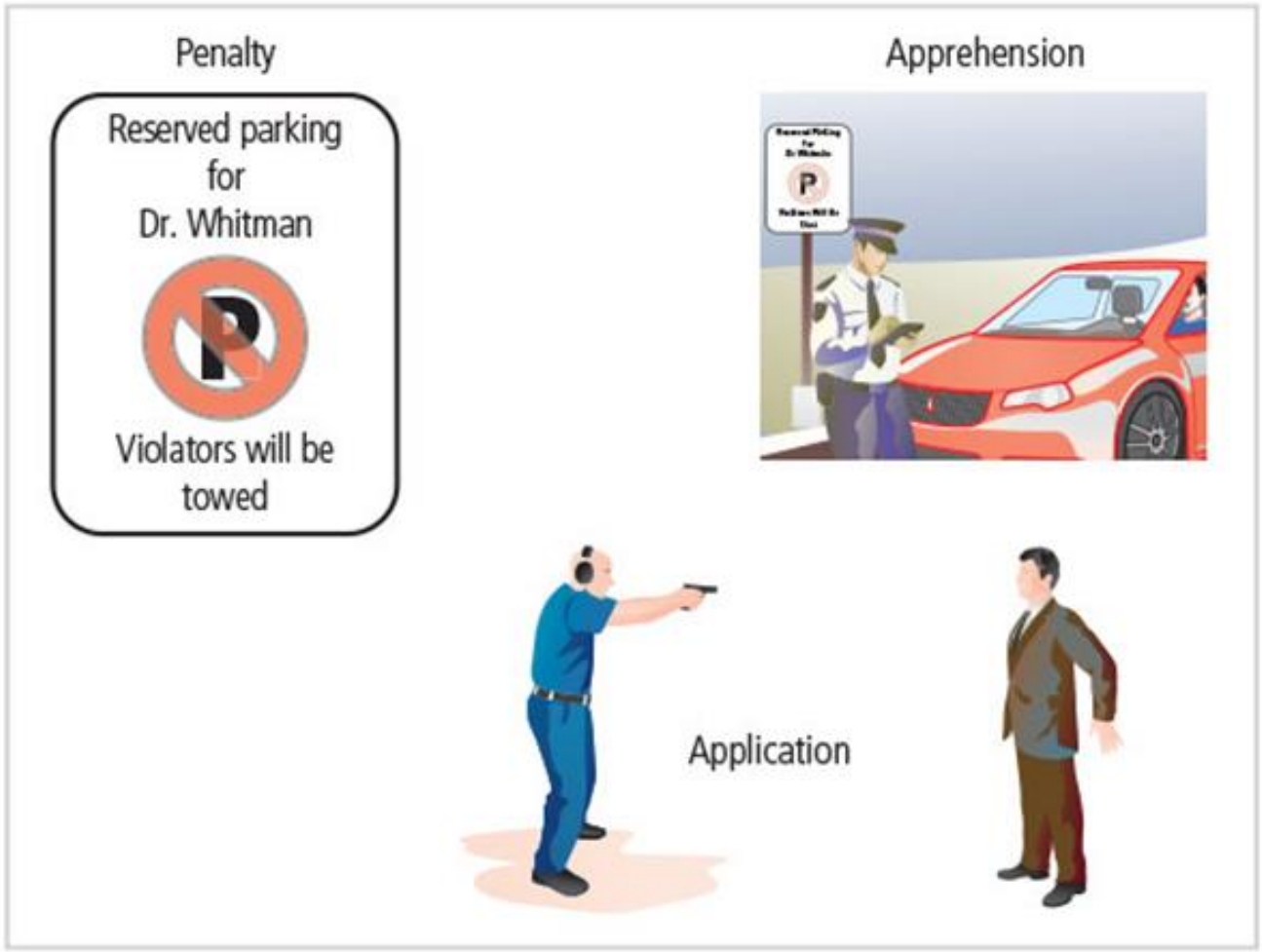
Ethics and Education

- Education is the overriding factor in leveling ethical perceptions within a small population.
- Employees must be trained and kept aware of the expected behavior of an ethical employee, as well as many other information security topics.
- Proper ethical training is vital to creating informed and a well-prepared system user.

Deterring Unethical and Illegal Behavior

- Three general causes of unethical and illegal behavior: ignorance, accident, intent
- Deterrence: best method for preventing an illegal or unethical activity; for example, 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

Figure 3-6 Deterrents to illegal or unethical behavior



Codes of Ethics of 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.

Table 3-3 Professional Organizations of Interest to Information Security Professionals (1 of 2)

Professional Organization	Web Resource Location	Description	Focus
Association of Computing Machinery	*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	*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	*www.issa.org*	Professional association of information systems security professionals; provides education forum, publications, and peer networking for members	Professional security information sharing

Table 3-3 Professional Organizations of Interest to Information Security Professionals (2 of 2)

Professional Organization	Web Resource Location	Description	Focus
International Information Systems Security Certification Consortium (ISQ^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	*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

Major IT and InfoSec Professional Organizations (1 of 5)

- Association of Computing Machinery (ACM)
  - Established in 1947 as “the world’s first educational and scientific computing society.”
  - Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others’ privacy, and respecting others’ intellectual property and copyrights.

Major IT and InfoSec Professional Organizations (2 of 5)

- International Information Systems Security Certification Consortium, Inc. $(ISC)^2$
  - Nonprofit organization focusing on the development and implementation of information security certifications and credentials.
  - Code is primarily designed for the information security professionals who have certification from $(ISC)^2$.
  - Code of ethics focuses on four mandatory canons.

Major IT and InfoSec Professional Organizations (3 of 5)

- SANS (originally System Administration, Networking, and Security Institute)
  - Professional organization with a large membership dedicated to the protection of information and systems.
  - SANS offers a set of certifications called Global Information Assurance Certification (GIAC).

Major IT and InfoSec Professional Organizations (4 of 5)

- ISACA (originally Information Systems Audit and Control Association)
  - Professional association with focus on auditing, control, and security
  - Concentrates on providing IT control practices and standards
  - ISACA has a code of ethics for its professionals

Major IT and InfoSec Professional Organizations (5 of 5)

- Information Systems Security Association (ISSA)
  - Nonprofit society of InfoSec professionals
  - Primary mission to bring together qualified IS practitioners for information exchange and educational development
  - Promotes code of ethics similar to $(ISC)^2$, ISACA, and ACM

Summary (1 of 3)

- Laws: rules that mandate or prohibit certain behavior in society; drawn from ethics
- Ethics: define socially acceptable behaviors, based on cultural mores (fixed moral attitudes or customs of a particular group)
- Types of law: civil, criminal, private, and public

Summary (2 of 3)

- 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.