THOMSON
COURSE TECHNOLOGY

Ethics in Information Technology, Second Edition

Lecture 1

An Overview of Ethics in IT

Ethics in Information Technology

- Public concern about the ethical use of information technology includes:
  - E-mail and Internet access monitoring
  - Peer-to-peer networks violation of copyright
  - Unsolicited e-mail
  - Hackers and identify theft
  - Plagiarism
  - Cookies and spyware

Ethics in Information Technology (continued)

- The general public has not realized the critical importance of ethics as applied to IT
- Important technical decisions are often left to technical experts
- General business managers must assume greater responsibility for these decisions

IT Professionals

- Are IT Workers Professionals?
  - Generally, No!
- Partial list of IT specialists
  - Programmers
  - Systems analysts
  - Software engineers
  - Database administrators
  - Local area network (LAN) administrators
  - Chief information officers (CIOs)

Professional Organizations

- No universal code of ethics for IT professionals
- No single, formal organization of IT professionals has emerged as preeminent
- Most prominent organizations include:
  - Association for Computing Machinery (ACM)
  - Association of Information Technology Professionals (AITP)
  - Computer Society of the Institute of Electrical and Electronics Engineers (IEEE-CS)
  - Project Management Institute (PMI)

Certification

- Indicates a professional possesses a particular set of skills, knowledge, or abilities in the opinion of a certifying organization
- Can also apply to products
- Generally voluntary
- Carries no requirement to adhere to a code of ethics

Certification (continued)

- Vendor certifications
  - Some certifications substantially improve IT workers' salaries and career prospects
  - Relevant for narrowly defined roles
    - Or certain aspects of broader roles
  - Require passing a written exam
  - Workers are commonly recertified as newer technologies become available

Common Ethical Issues for IT Users

- Software piracy
- Inappropriate use of computing resources
- Inappropriate sharing of information
  - Private data
  - Confidential information

IT Security Incidents: A Worsening Problem

- Security of information technology is of utmost importance
  - Protect confidential data
    - Safeguard private customer and employee data
  - Protect against malicious acts of theft or disruption
  - Must be balanced against other business needs and issues
- Number of IT-related security incidents is increasing around the world

Classifying Perpetrators of Computer Crime

TABLE 3-2 Classifying perpetrators of computer crime

Type of perpetrator	Objectives	Resources available to perpetrator	Level of risk acceptable to perpetrator	Frequency of attack
Hacker	Test limits of system and gain publicity	Limited	Minimal	High
Cracker	Cause problems, steal data, and corrupt systems	Limited	Moderate	Medium
Insider	Make money and disrupt company's information systems	Knowledge of systems and passwords	Moderate	Low

TABLE 3-2 Classifying perpetrators of computer crime (continued)

Type of perpetrator	Objectives	Resources available to perpetrator	Level of risk acceptable to perpetrator	Frequency of attack
Industrial spy	Capture trade secrets and gain competitive advantage	Well funded and well trained	Minimal	Low
Cyber-criminal	Make money	Well funded and well trained	Moderate	Low
Cyber-terrorist	Destroy key infrastructure components	Not necessarily well funded or well trained	Very high	Low

Hackers and Crackers

- Hackers
  - Test limitations of systems out of intellectual curiosity
- Crackers
  - Cracking is a form of hacking
  - Clearly criminal activity

Malicious Insiders

- Top security concern for companies
- Estimated 85 percent of all fraud is committed by employees
- Usually due to weaknesses in internal control procedures
- Collusion is cooperation between an employee and an outsider
- Insiders are not necessarily employees
  - Can also be consultants and contractors
- Extremely difficult to detect or stop
  - Authorized to access the very systems they abuse

Industrial Spies

- Illegally obtain trade secrets from competitors
- Competitive intelligence
  - Uses legal techniques
  - Gathers information available to the public
- Industrial espionage
  - Uses illegal means
  - Obtains information not available to the public

What Topics will be covered?

- Chapter 4
  - Personal data privacy
  - Employee monitoring
- Chapter 6
  - Protection of intellectual property rights through patents, copyrights, and trade secrets
- Chapter 7
  - Software development process
  - Quality Assurance