



7. Security, Ethical, Privacy and Other Challenges

IT1106

Level I - Semester 1

7. Security, Ethical, Privacy and Other Challenges

7.1 Ethical Issues in Data Handling

7.2 Privacy Issues

7.3 Information System Security

7.3.1 Security Threats and Attacks

7.3.2 Information System Security Planning and Management

7.4 Ergonomics

7.1 Ethical Issues in Data Handling

Moral, Legal vs. Ethical

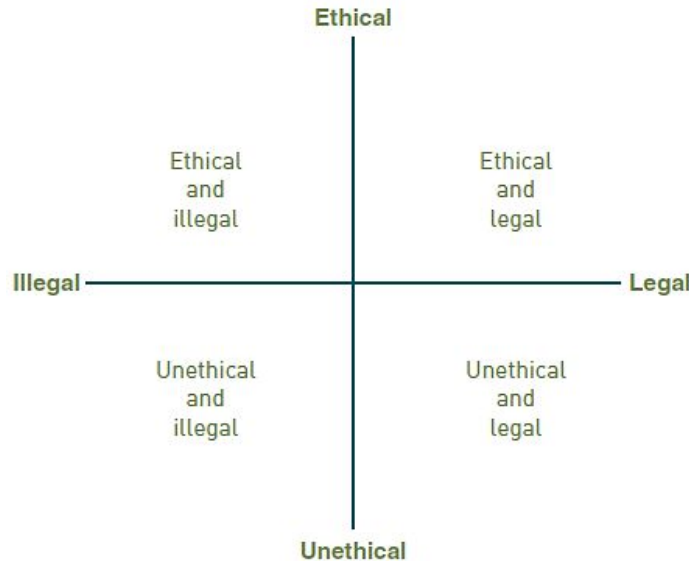
Morals: Personal beliefs about right and wrong behavior. Moral acts conform to what an individual believes to be the right thing to do.

Law: A system of rules that defines what we can do and cannot do. Laws are enforced by a set of institutions (the police, courts, law-making bodies). Legal acts are acts that conform to the law.

Ethics: Standards or codes of behavior expected of an individual by a group to which an individual belongs. Ethical behavior conforms to generally accepted social norms—many of which are almost universally accepted.

Legal vs. Ethical

- Laws do not provide a complete guide to ethical behavior. Just because an activity is defined as legal does not mean that it is ethical.



Code of Ethics

Code of Ethics: code of ethics states the principles and core values that are essential to their work and, therefore, govern their behavior. The code can become a reference point for weighing what is legal and what is ethical.

Business Ethics

- Business ethics is concerned with the numerous ethical questions that managers must confront as part of their daily business decision making.

Equity	Rights	Honesty	Exercise of Corporate Power
Executive salaries	Corporate due process	Employee conflicts of interest	Product safety
Comparable worth	Employee health screening	Security of company information	Environmental issues
Product pricing	Customer privacy	Inappropriate gifts	Disinvestment
Intellectual property rights	Employee privacy	Advertising content	Corporate contributions
Noncompetitive agreements	Sexual harassment	Government contract issues	Social issues raised by religious organizations
	Affirmative action	Financial and cash management procedures	Plant/facility closures and downsizing
	Equal employment opportunity	Questionable business practices in foreign countries	Political action committees
	Shareholder interests		Workplace safety
	Employment at will		
	Whistle-blowing		

Notice: The issues of *intellectual property rights*, *customer and employee privacy*, *security of company records*, and *workplace safety* are highlighted because they have been major areas of ethical controversy in information technology.

Ethical Use of Technology

- An important ethical dimension deals specifically with the ethics of the use of any form of technology.
- An example of technology ethics involves some of the health risks of using computer workstations for extended periods in high-volume data entry job positions.
 - Many organizations display ethical behavior by scheduling work breaks and limiting the time that data entry workers stare at a computer monitor to minimize their risk of developing a variety of work-related health disorders, such as eye-sight problems/back pain.

Four Principles of Technology Ethics

- These principles can serve as basic ethical requirements that companies should meet to help ensure the ethical implementation of information technologies and information systems in business.

Principles of Technology Ethics
<ul style="list-style-type: none">• Proportionality. The good achieved by the technology must outweigh the harm or risk. Moreover, there must be no alternative that achieves the same or comparable benefits with less harm or risk.
<ul style="list-style-type: none">• Informed Consent. Those affected by the technology should understand and accept the risks.
<ul style="list-style-type: none">• Justice. The benefits and burdens of the technology should be distributed fairly. Those who benefit should bear their fair share of the risks, and those who do not benefit should not suffer a significant increase in risk.
<ul style="list-style-type: none">• Minimized Risk. Even if judged acceptable by the other three guidelines, the technology must be implemented so as to avoid all unnecessary risk.

Ethical Guidelines

- Business and IS professionals can live up to their ethical responsibilities by following ethical guidelines which outlines the considerations inherent in the major responsibilities of an IS professional.
- For example:
you can be a responsible professional by;
 - (1) acting with integrity
 - (2) increasing your professional competence
 - (3) setting high standards of personal performance
 - (4) accepting responsibility for your work
 - (5) advancing the health, privacy, and general welfare of the public

Ethical Guidelines

- An example for a code of professional conduct:
 - code of professional conduct of the Association of Information Technology Professionals (AITP). Its code of conduct outlines the ethical considerations inherent in the major responsibilities of an IS professional.

AITP Standards of Professional Conduct

In recognition of my obligation to my employer I shall:

- Avoid conflicts of interest and ensure that my employer is aware of any potential conflicts.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Activity

Write down complete answers to the following questions.

- What is code of ethics and what is the intent of it?
- Distinguish between acting ethically and acting legally.
- Just because an activity is defined as legal does not mean that it is ethical. Discuss.
- Identify and briefly discuss a difficult decision you had to make that had some ethical considerations.

7.2 Privacy Issues

Information technology makes it technically and economically feasible to collect, store, integrate, interchange, and retrieve data and information. However, it can have a negative effect on the right to privacy of every individual.



Privacy Issues

- **Violation of privacy** - Accessing private e-mail and computer records to collect and sharing information about individuals gained from their visits to Internet Web sites and newsgroups
- **Computer monitoring** - Always knowing where a person is, especially as mobile and paging services become more closely associated with people rather than places.
- **Computer matching** - Using customer information gained from many sources to market additional business services
- **Unauthorized personal filing/ Identity Theft** - Collecting telephone numbers, e-mail addresses, credit card numbers, and other personal information to build individual customer profiles

Privacy and Fairness in Information Use

The opposite of the privacy is;

- freedom of information
- freedom of speech
- freedom of the press

Fairness Issues	Database Storage	Database Usage
The right to know	Knowledge	Notice
The ability to decide	Control	Consent
Knowledge. Should people know what data is stored about them? In some cases, people are informed that information about them is stored in a corporate database. In others, they are unaware that their personal information is being stored.		
Control. Should people be able to correct errors in corporate database systems? This ability is possible with most organizations, although it can be difficult in some cases.		
Notice. Should an organization that uses personal data for a purpose other than the original designated purpose be required to notify individuals in advance? Most companies don't do this.		
Consent. If information on people is to be used for other purposes, should these people be asked to give their consent before data on them is used? Many companies do not give people the ability to decide if such information will be sold or used for other purposes.		

Privacy Laws

- U.S. Electronic Communications Privacy Act & Computer Fraud and Abuse Act,
prohibit intercepting data communications messages, stealing or destroying data, or trespassing in federal-related computer systems.
- Children's Online Privacy Protection Act (COPPA),
 - requires websites that collect information about children under the age of 13 to post a privacy policy & adhere to certain information-sharing restrictions.
- U.S. Health Insurance Portability and Accountability Act (HIPAA),
intended to create safeguards against the unauthorized use, disclosure, or distribution of an individual's health-related information without their specific consent or authorization.

Individual Efforts to Protect Privacy

- Find out what is stored about you in existing databases.
- Be careful when you share information about yourself.
- Be proactive in protecting your privacy.
- Take extra care when purchasing anything from a Web site.

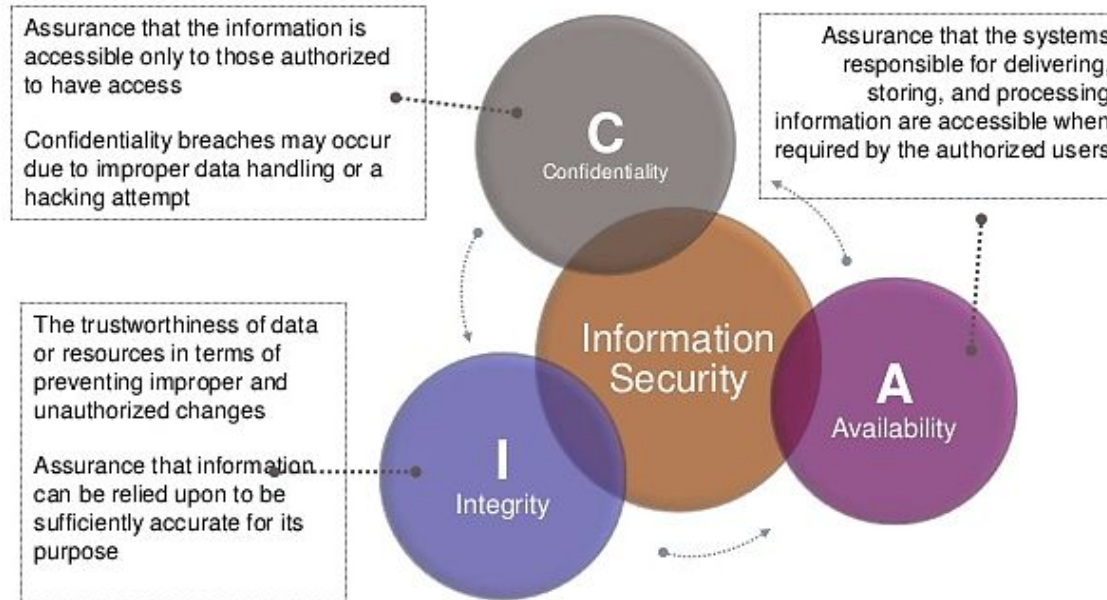
Activity

Write down complete answers to the following questions.

- Briefly discuss about one of the followings.
 1. Privacy at working environment
 2. Privacy and e-mail/messaging
 3. Privacy and Internet Libel Concerns
- What is the purpose and intent of a privacy policy?
- Compare and contrast Right to Privacy and Right to Know with examples.
- Should employers be able to monitor the email, text, and phone calls of employees?
Is there any degree of “monitoring” that you find acceptable/ unacceptable?

7.3 Information System Security

What is IT Security ?



7.3.1 Security Threats and Attacks

Why Computer Incidents Are So Prevalent:

- Increasing complexity increases vulnerability
- Higher computer user expectations
- Expanding and changing systems introduce new risks
- Increased prevalence of bring your own device (byod) policies
- Growing reliance on commercial software with known vulnerabilities
- Increasing sophistication of those who would do harm

Computer Crime

- Computer crime is defined by the Association of Information Technology Professionals (AITP) as including;
 - (1) The unauthorized use, access, modification, and destruction of hardware, software, data, or network resources
 - (2) The unauthorized release of information
 - (3) The unauthorized copying of software
 - (4) Denying an end user access to his or her own hardware, software, data, or network resources
 - (5) Using or conspiring to use computer or network resources to obtain information or tangible property illegally .

This definition was promoted by the AITP in a Model Computer Crime Act and is reflected in many computer crime laws.

Perpetrators of Computer Crime

Type of Perpetrator	Description
Black hat hacker	Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems)
Cracker	An individual who causes problems, steals data, and corrupts systems
Malicious insider	An employee or contractor who attempts to gain financially and/or disrupt a company's information systems and business operations
Industrial spy	An individual who captures trade secrets and attempts to gain an unfair competitive advantage
Cybercriminal	Someone who attacks a computer system or network for financial gain
Hactivist	An individual who hacks computers or Web sites in an attempt to promote a political ideology
Cyberterrorist	Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units

Common Hacking Tactics & Security Exploits

- Denial of Service
- Vulnerability Scan
- Packet Sniffer
- Spoofing (Phishing)
- Trojan Horse
- Back Doors
- Malicious Applets
- War Dialing
- Logic Bombs
- Buffer Overflow
- Password Crackers
- Social Engineering
- Dumpster Diving

Common Hacking Tactics and Security Exploits

Denial of Service. This is becoming a common networking prank. By hammering a Web site's equipment with too many requests for information, an attacker can effectively clog the system, slowing performance or even crashing the site. This method of overloading computers is sometimes used to cover up an attack.

Vulnerability Scans. Widespread probes of the Internet to determine types of computers, services, and connections. That way the bad guys can take advantage of weaknesses in a particular make of computer or software program.

Packet Sniffer. Programs that covertly search individual packets of data as they pass through the Internet, capturing passwords or the entire contents.

Spoofing (Phishing). Faking an e-mail address or Web page to trick users into passing along critical information like passwords or credit card numbers.

Trojan Horse. A program that, unknown to the user, contains instructions that exploit a known vulnerability in some software.

Back Doors. In case the original entry point has been detected, having a few hidden ways back makes reentry easy—and difficult to detect.

Malicious Applets. Tiny programs, sometimes written in the popular Java computer language, that misuse your computer's resources, modify files on the hard disk, send fake e-mail, or steal passwords.

War Dialing. Programs that automatically dial thousands of telephone numbers in search of a way in through a modem connection.

Logic Bombs. An instruction in a computer program that triggers a malicious act.

Buffer Overflow. A technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory.

Password Crackers. Software that can guess passwords.

Social Engineering. A tactic used to gain access to computer systems by talking unsuspecting company employees out of valuable information such as passwords.

Dumpster Diving. Sifting through a company's garbage to find information to help break into their computers. Sometimes the information is used to make a stab at social engineering more credible.

Types of Exploits

- Ransomware: Malware that stops you from using your computer or accessing your data until you meet certain demands such as paying a ransom or sending photos to the attacker.
- Virus: A piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.
- Worm: A harmful program that resides in the active memory of the computer and duplicates itself.
- Trojan Horse: A seemingly harmless program in which malicious code is hidden.
- Logic Bomb: A form of Trojan horse malware that executes when it is triggered by a specific event.

Types of Exploits

- Blended Threat: A sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload.
- Spam: The use of email systems to send unsolicited email to large numbers of people.
- Distributed Denial-of-Service (DDoS) Attack: An attack in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.
- Botnet: A term used to describe a large group of computers, that are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners.
 - Zombie: A computer that has been taken over by a hacker to be used as a part of a botnet.

Types of Exploits

- Rootkit: A set of programs that enables its user to gain administrator level access to a computer without the end user's consent or knowledge.
- Advanced Persistent Threat (APT): A network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time.
- Phishing: The act of fraudulently using email to try to get the recipient to reveal personal data.
- Identity Theft: The theft of personal information, which is then used without the owner's permission, often to commit fraud or other crimes.
- Data Breach: The unintended release of sensitive data or the access of sensitive data by unauthorized individuals.

Federal Laws for Prosecuting Computer Attacks

Federal Law	Subject Area
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Addresses fraud and related activities in association with computers, including the following: <ul style="list-style-type: none">• Accessing a computer without authorization or exceeding authorized access• Transmitting a program, code, or command that causes harm to a computer• Trafficking of computer passwords• Threatening to cause damage to a protected computer
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	Covers false claims regarding unauthorized use of credit cards
Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)	Makes identity theft a federal crime, with penalties of up to 15 years' of imprisonment and a maximum fine of \$250,000
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Focuses on unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage
USA Patriot Act	Defines cyberterrorism and associated penalties

Activity

Write down complete answers to the following questions.

- Distinguish between a black hat hacker, a white hat hacker and a cracker?
- What is a zero-day attack?
- Explain how a Distributed Denial-of-Service attack works.
- In which exploit the victims receive a voice mail message telling them to call a phone number or access a Web site?
- Briefly explain the differences of 'phishing' and 'spam'.

7.3.2 Information System Security Planning and Management

- The goal of security management is the accuracy, integrity, and safety of all information system processes and resources.
- Effective security management can minimize errors, fraud, and losses in the information systems.

Implementing Secure, & Reliable Computing

A strong security system begins by assessing threats to the networks, computers, identifying actions that addresses the most serious vulnerabilities, educating end users about the risks involved and the actions they must take to prevent a security incident. If an intrusion occurs, there must be a clear reaction plan that addresses until recovery.

- Risk Assessment
- Detection, Response & Prevention
- Establish Security Policy
- Educating Employees and Contract Workers

Risk Assessment

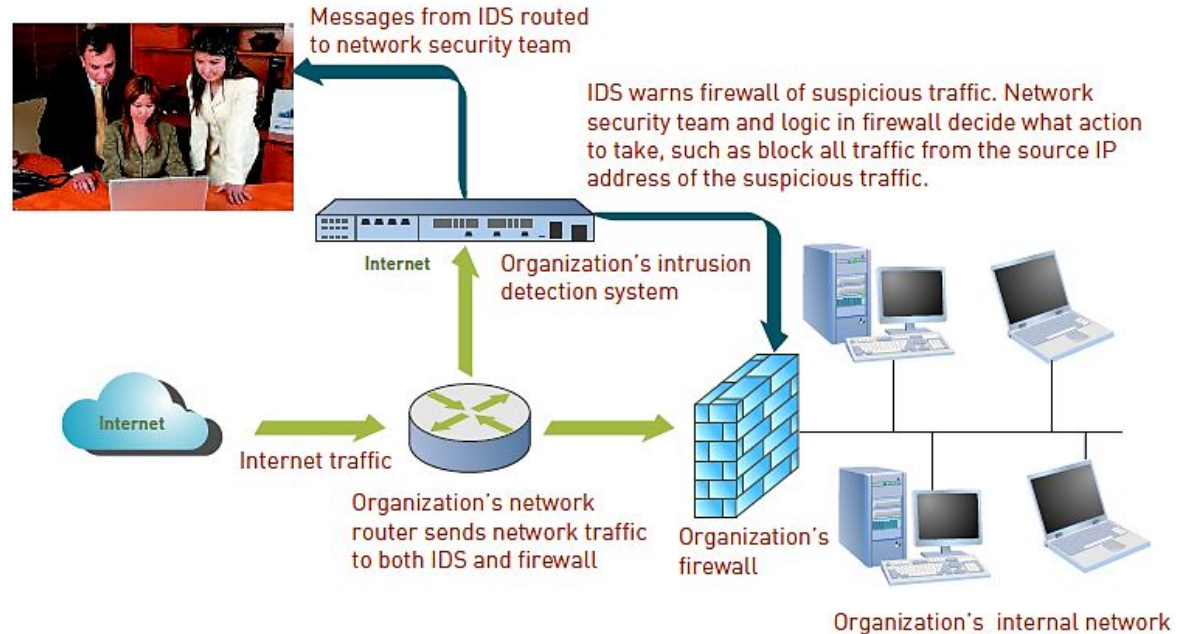
- The process of assessing security-related risks to an organization's computers and networks from both internal and external threats.
- **Step 1:** Identify the set of IS assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals.
- **Step 2:** Identify the loss events or the risks or threats that could occur, such as a distributed denial-of-service attack or insider fraud.
- **Step 3:** Assess the frequency of events or the likelihood of each potential threat; some threats, such as insider fraud, are more likely to occur than others.

Risk Assessment

- **Step 4:** Determine the impact of each threat occurring. Would the threat have a minor impact on the organization, or could it keep the organization from carrying out its mission for a lengthy period of time?
- **Step 5:** Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization.
- **Step 6:** Assess the feasibility of implementing the mitigation options.
- **Step 7:** Perform a cost-benefit analysis to ensure that your efforts will be cost effective.
- **Step 8:** Make the decision on whether or not to implement a particular countermeasure. If you decide against implementing a particular countermeasure, you need to reassess if the threat is truly serious and, if so, identify a less costly countermeasure.

Detection

Intrusion Detection System (IDS): Software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment.



Response

- Incident Notification
- Protection of Evidence and Activity Logs
- Incident Containment
- Eradication
- Incident Follow-Up

Prevention

- Implementing a Corporate Firewall
- Utilizing a Security Dashboard
- Installing Antivirus Software on Personal Computers
- Implementing Safeguards against Attacks by Malicious Insiders
- Addressing the Most Critical Internet Security Threats
- Conducting Periodic IT Security Audits

Establish a Security Policy

Security policy: A statement that defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements.

- Security policy delineates responsibilities and the behavior expected from employees of the organization.

Tools of Security Management

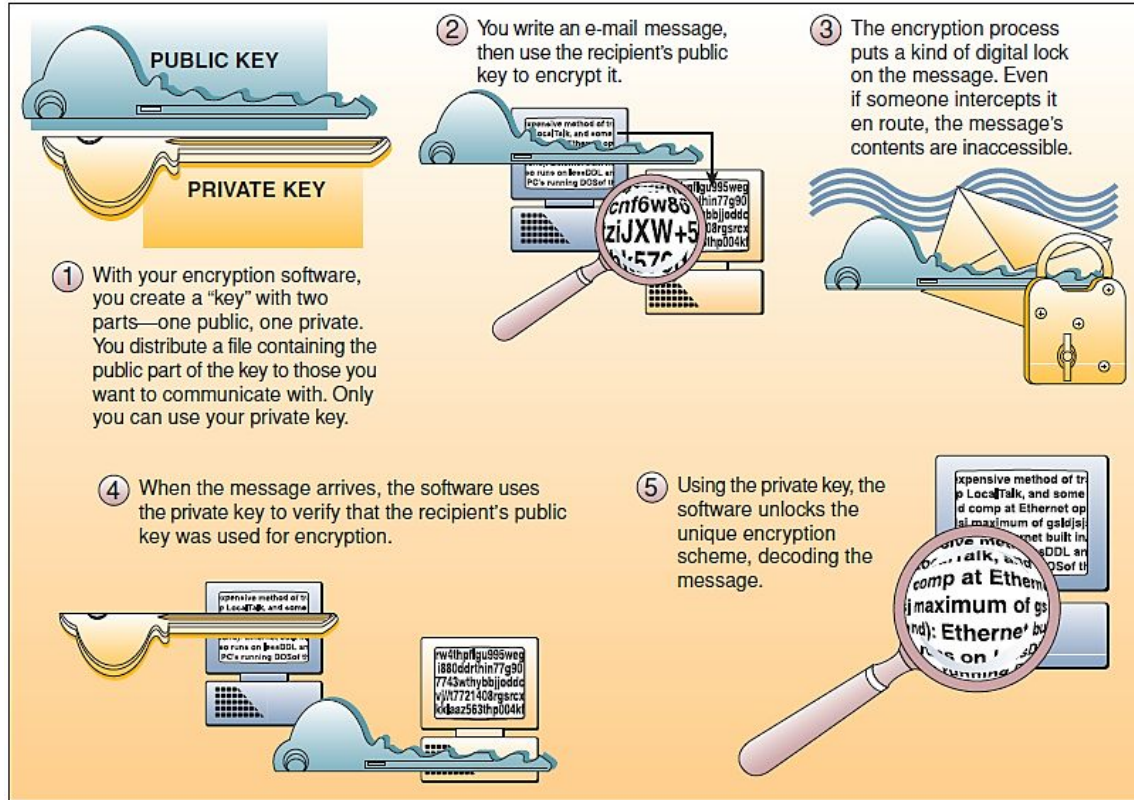


Inter-networked Security Defenses

Encryption

- Encryption of data has become an important way to protect data and other computer network resources, especially on the Internet, intranets, and extranets.
- Encryption involves using special mathematical algorithms, or keys, to transform digital data into an encoding before they are transmitted, and then to decode the data when they are received.

Encryption

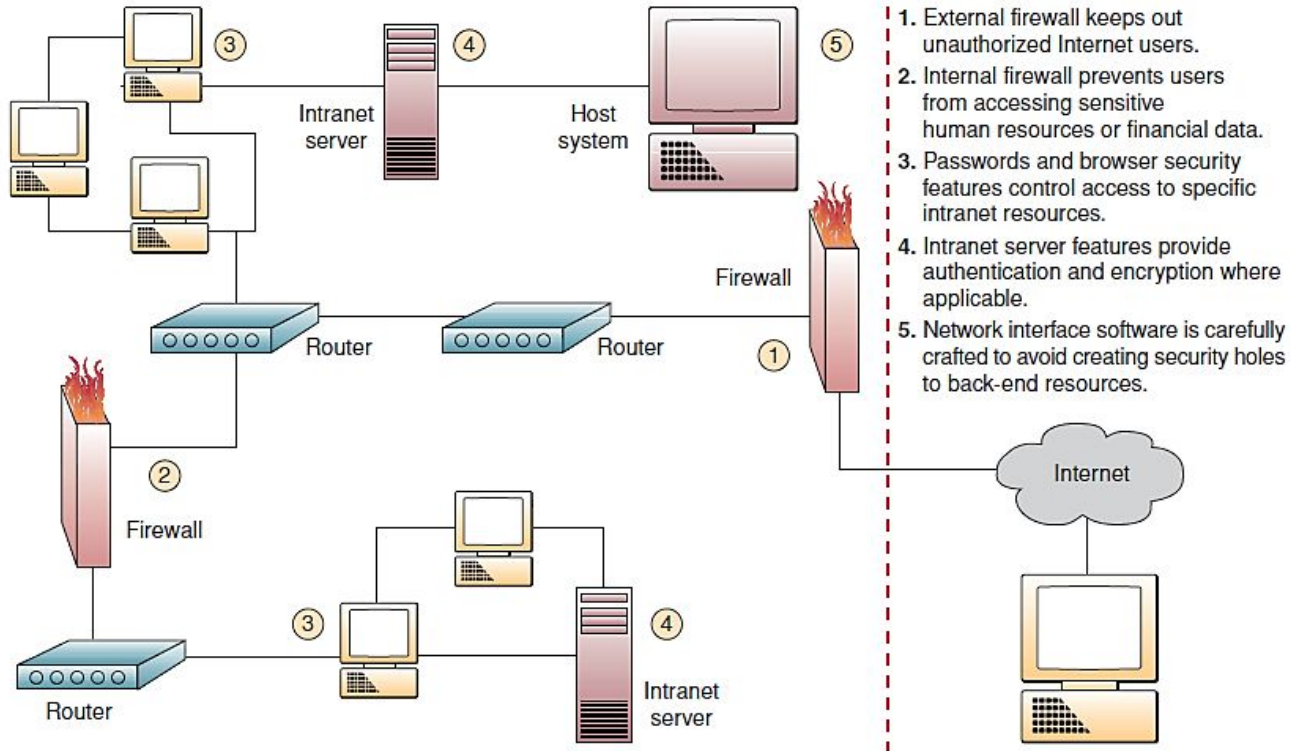


Inter-networked Security Defenses

Firewall

- A firewall serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks.


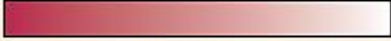


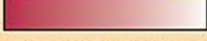


Firewalls



Other Security Measures

- Anti-virus Software
- Security Codes
- Backup Files
- Security Monitors
- Biometric Security
- Computer Failure Controls
- Fault-Tolerant Systems
- Disaster Recovery

Other Security Measures

Security Technologies Used	Security Management
<p>Antivirus 99%</p> 	<ul style="list-style-type: none">■ Security is about 6 to 8% of the IT budget in developed countries.
<p>Virtual private networks 91%</p> 	<ul style="list-style-type: none">■ 74% currently have or plan to establish in the next two years the position of chief security officer or chief information security officer.
<p>Intrusion-detection systems 88%</p> 	<ul style="list-style-type: none">■ 40% have a chief privacy officer, and another 6% intend to appoint one within the next two years.
<p>Data backup 82%</p> 	<ul style="list-style-type: none">■ 44% acknowledged that their systems had been compromised in some way within the past year.
<p>Annual security plan testing 48%</p> 	<ul style="list-style-type: none">■ 37% have cyber risk insurance, and another 5% intend to acquire such coverage.
<p>Security plan compliance audit 27%</p> 	
<p>Biometrics 19%</p> 	

Activity

Write down complete answers to the following questions.

- What is the intent of a security policy? What are some of the tags of a good security policy?
- Briefly explain the process of assessing security related risks to an organization's computers & networks from both internal and external threats.
- What is the difference between a risk assessment and an IT security audit?

7.4 Ergonomics

- Ergonomics (human factors engineering) is a solution to some health problems. The science of designing machines, products, and systems to maximize the safety, comfort, and efficiency of the people who use them.

The goal of ergonomics is to design a healthy working environment thus increasing employee morale and productivity.



Health Concerns

Common Discomforts Associated with Heavy Use of Computers	Preventative Action
Red, dry, itchy eyes	<p>Change your focus away from the screen every 20 or 30 minutes by looking into the distance and focusing on an object for 20 to 30 seconds.</p> <p>Make a conscious effort to blink more often.</p> <p>Consider the use of artificial tears.</p> <p>Use an LCD screen, which provides a better viewing experience for your eyes by eliminating most screen flicker while still being bright without harsh incandescence.</p>
Neck and shoulder pain	<p>Use proper posture when working at the computer.</p> <p>Stand up, stretch, and walk around for a few minutes every hour.</p> <p>Shrug and rotate your shoulders occasionally.</p>
Pain, numbness, or tingling sensation in hands	<p>Use proper posture when working at the computer.</p> <p>Do not rest your elbows on hard surfaces.</p> <p>Place a wrist rest between your computer keyboard and the edge of your desk.</p> <p>Take an occasional break and spread fingers apart while keeping your wrists straight. Taken an occasional break with your arms resting at your sides and gently shake your hands.</p>

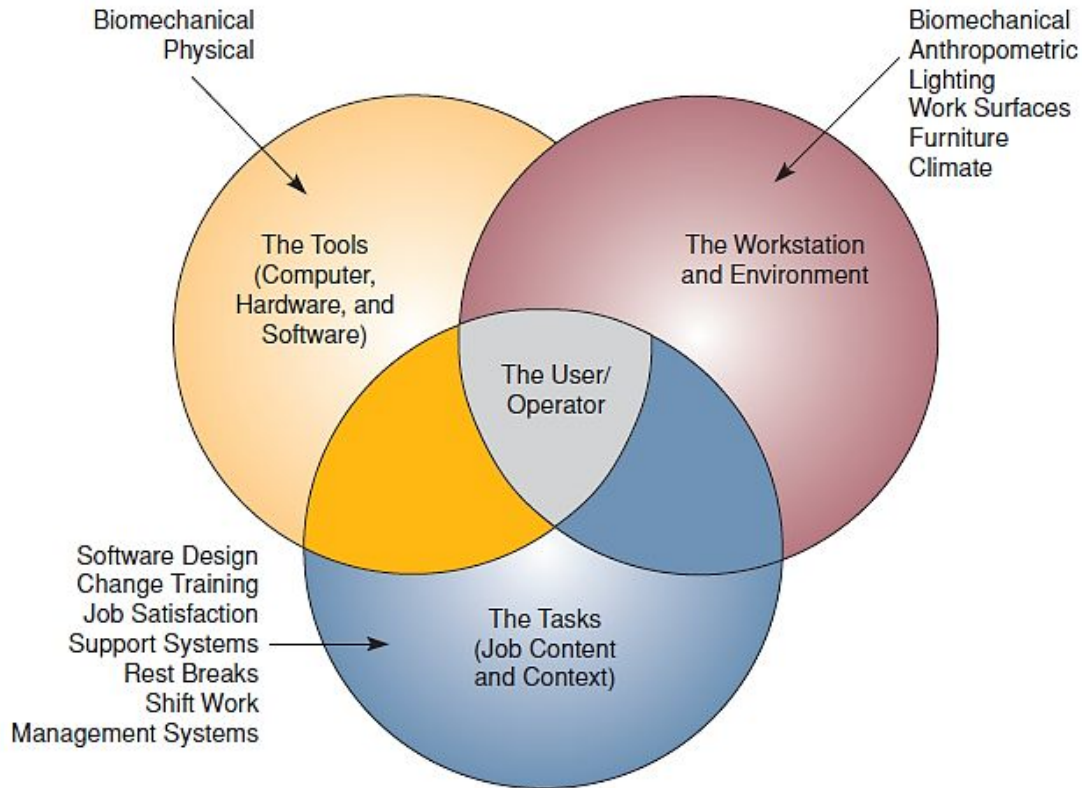
Avoiding Health and Environmental Problems

Example: Properly seating at a correctly positioned keyboard:

- Your elbows are near your body in an open angle to allow circulation to the lower arms and hands.
- Your arms are nearly perpendicular to the floor.
- Your wrists are nearly straight.
- The height of the surface holding your keyboard and mouse is 1 or 2 inches above your thighs.
- The keyboard is centered in front of your body.
- The monitor is about one arm's length (20 to 26 inches) away.
- The top of your monitor is at eye level.
- Your chair has a backrest that supports the curve of your lower (lumbar) back.



Ergonomics Factors



Activity

Write down complete answers to the following questions.

- Briefly explain two primary causes of computer-related health problems.
- What is ergonomics? How can it be applied to office workers?
- Heavy computer use can negatively affect one's physical health. Discuss.

Quiz

1. A(n) _____ is an attack on an information system that takes advantage of a particular system vulnerability.
 - a. virus
 - b. worm
 - c. Trojan horse
 - d. exploit
 - e. botnet

2. A _____ is someone who attacks a computer system or network for financial gain.
 - a. hacker
 - b. cracker
 - c. malicious insider
 - d. cybercriminal
 - e. hacktivist

Quiz

3. A _____ is a form of malware that fools its victims into thinking that it is useful software from a legitimate source.

- a. virus
- b. worm
- c. Trojan horse
- d. ransomware
- e. logic bomb

4. A _____ is a set of programs that enables a user to gain administrative access to the computer without the end user's consent or knowledge.

- a. zombie
- b. rootkit
- c. botnet
- d. blended threat
- e. phishing

Quiz

5. _____ involves the deployment of malware that secretly steals data in the computer systems of organizations.

- a. Cyberterrorism
- b. Cyberespionage
- c. Data breach
- d. Smishing
- e. spam

6. The concept of _____ recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

- a. risk assessment
- b. reasonable assurance
- c. security policy
- d. security versus privacy
- e. Detection, Response & Prevention

Quiz

7. A(n) _____ stands guard between an organization's internal network and the Internet and it limits network access based on the organization's access policy.

- a. router
- b. worm hole
- c. intrusion detection system
- d. firewall
- E. encryption

8. Which of the following is not a common computer-related mistake?

- a. Programming errors
- b. Shopping online while at work
- c. Data-entry or data-capture errors
- d. Errors in handling files
- e. download and upload data for personal use

Quiz

9. The Children's Online Privacy Protection Act (COPPA) was passed by Congress in October 1998. This act, directed at Web sites catering to children, requires site owners to post comprehensive privacy policies and to obtain parental consent before they collect any personal information from children under years of age.

- a. 10
- b. 13
- c. 15
- d. 11
- e. 17