**CH4 Ethical and Social Issues in Information Systems**

學習目標 :

* 1. 資訊系統引發了哪些倫理，社會和政治問題？
  2. 哪些特定的行為原則可以用來引導道德決策？
  3. 為什麼現代資訊系統技術和網際網路對保護個人隱私和智慧產

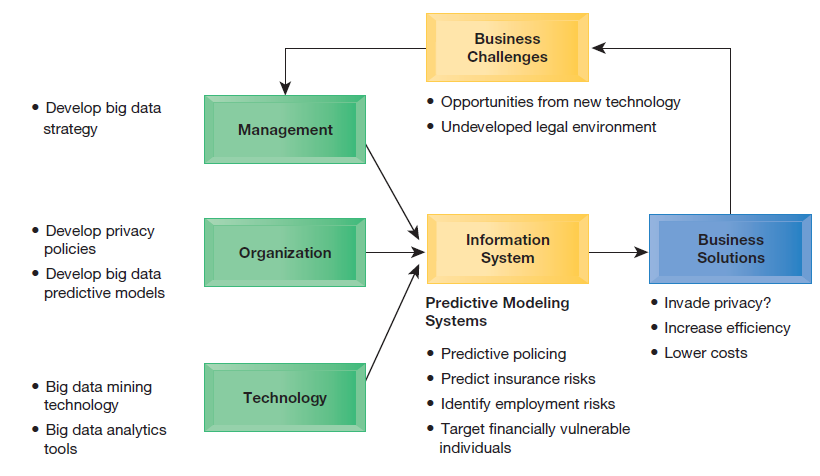
權(intellectual property)構成挑戰？

* 1. How have information systems affected laws for establishing

Accountability(個人) and liability(法律) and the quality of everyday

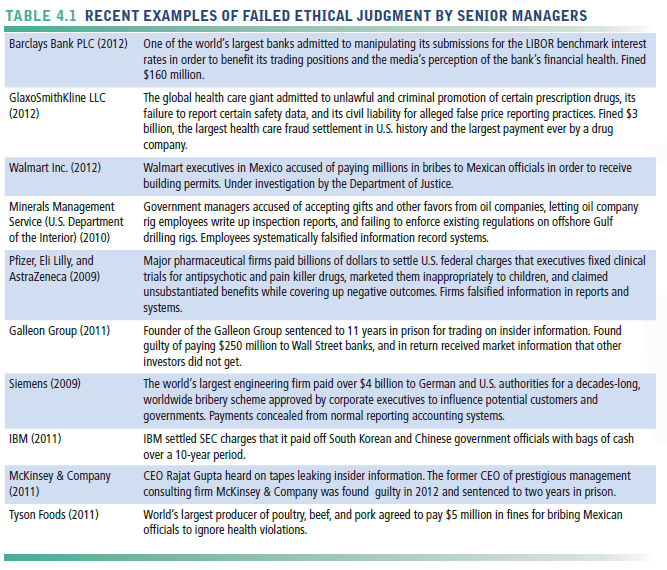
life?

* The Dark Side of Big Data
* Does analyzing big data about people create an ethical dilemma? Why or why not? Should there be new privacy laws to protect individuals from being targeted by companies analyzing big data? Why or why not?

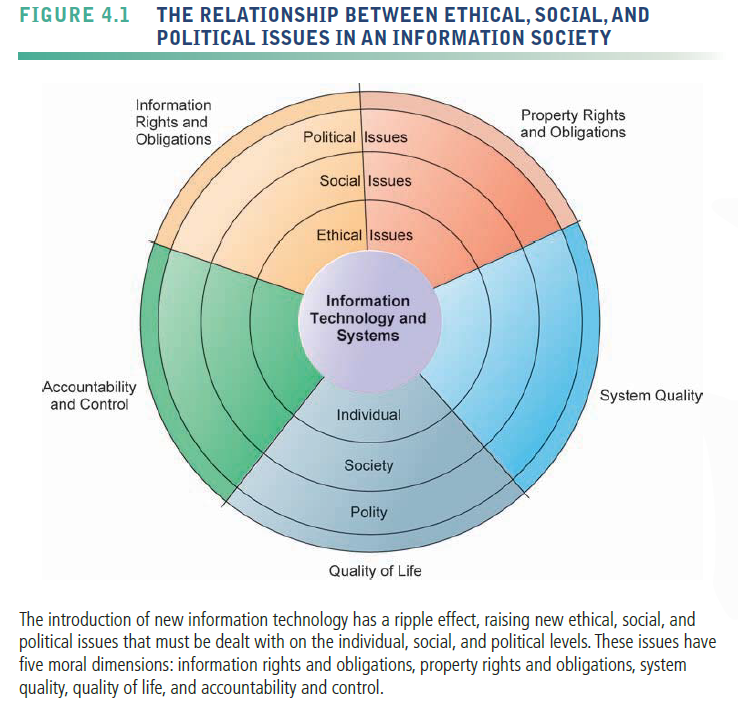


1. UNDERSTANDING ETHICAL AND SOCIAL ISSUES RELATED TO SYSTEMS
   * Preface

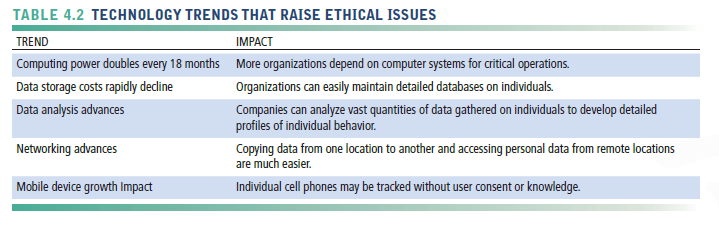
* Small sample of recent cases demonstrating failed ethical judgment by senior and middle managers.



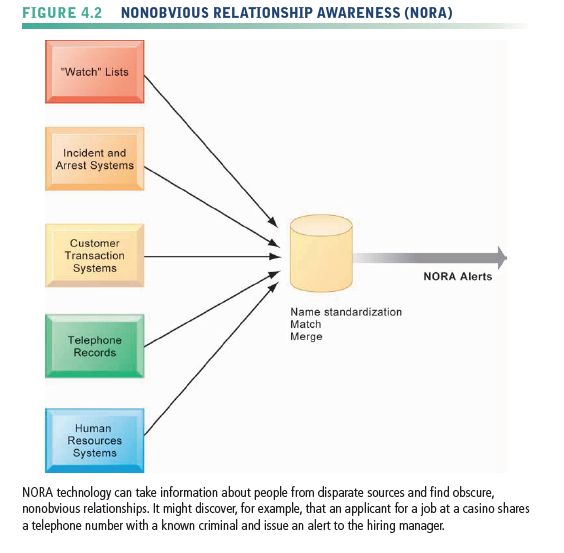
* Ethics
* refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors.
* Information systems raise new ethical questions because they create opportunities for:
* Intense social change, threatening existing distributions of power, money, rights, and obligations
* New kinds of crime
* When using information systems, it is essential to ask, “What is the ethical and socially responsible course of action?”
  + A Model for Thinking About Ethical, Social, and Political Issues
* society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions.
* IT as rock dropped in pond, creating ripples of new situations not covered by old rules
* Social and political institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, laws
* Requires understanding of ethics to make choices in legally gray areas
* This model is also useful for identifying the main moral dimensions of the information society, which cut across various levels of action—individual, social, and political.



* + Five Moral Dimensions of the Information Age
    - 1. Information rights and obligations
* What information rights do individuals and organizations possess with respect to themselves?
* What can they protect?
  + - 1. Property rights and obligations
* How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy?
  + - 1. Accountability and control
* Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?
  + - 1. System quality
* What standards of data and system quality should we demand to protect individual rights and the safety of society?
  + - 1. Quality of life
* What values should be preserved in an information- and knowledge based society?
* Which institutions should we protect from violation?
* Which cultural values and practices are supported by the new information technology?
  + Key Technology Trends that Raise Ethical Issues



* Computing power doubles every 18 months
* our dependence on systems and our vulnerability to system errors and poor data quality have increased
* Social rules and laws have not yet adjusted to this dependence
* Data storage costs rapidly decline
* These advances in data storage have made the routine violation of individual privacy both cheap and effective.
* Data analysis advances
* Profiling
  + - The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals
* Nonobvious relationship awareness (NORA)
  + - given both the government and the private sector even more powerful profiling capabilities.
    - take information about people
    - from many disparate sources, such as employment applications, telephone records, customer listings, and “wanted” lists, and correlate relationships to find obscure hidden connections that might help identify criminals or terrorists
    - scans data and extracts information as the data are being generated
    - a valuable tool for homeland security



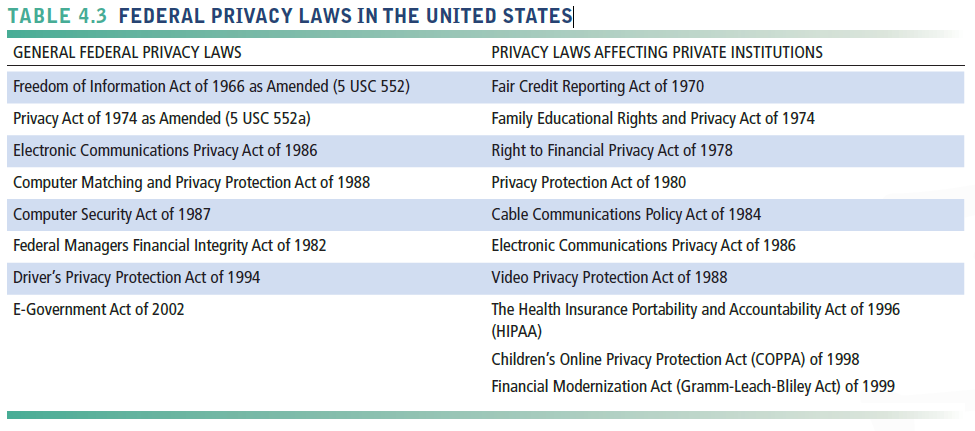
* Networking advances
* reduce the costs of moving and accessing large quantities of data and open the possibility of mining large pools of data remotely using small desktop machines, permitting an invasion of privacy on a scale
* Mobile device growth Impact
* Tracking of individual cell phones

1. ETHICS IN AN INFORMATION SOCIETY
   * Basic Concepts; Responsibility, Accountability, Liability

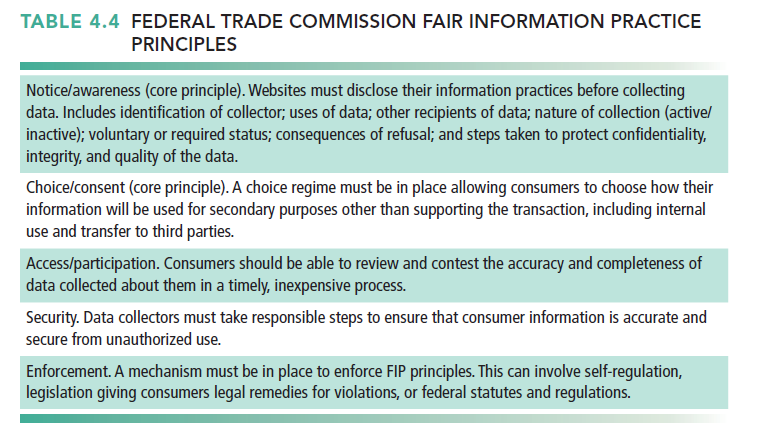
* These basic concepts form the underpinning of an ethical analysis of information systems and those who manage them.
* Responsibility
* you accept the potential costs, duties, and obligations for the decisions you make
* Accountability
* mechanisms are in place to determine who took responsible action, and who is responsible.
* Liability
* a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations.
* Due process
* a related feature of law-governed societies and is a process in which laws are known and understood, and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.
  + Ethical Analysis
    - 1. Identify and clearly describe the facts.
      2. Define the conflict or dilemma and identify the higher-order values involved.
      3. Identify the stakeholders.
      4. Identify the options that you can reasonably take.
      5. Identify the potential consequences of your options.
  + Candidate Ethical Principles
* Golden Rule
* Do unto others as you would have them do unto you
* Immanuel Kant’s Categorical Imperative
* If an action is not right for everyone to take, it is not right for anyone
* Descartes’ Rule of Change
* If an action cannot be taken repeatedly, it is not right to take at all
* Utilitarian Principle
* Take the action that achieves the higher or greater value
* Risk Aversion Principle
* Take the action that produces the least harm or the least potential cost
* Ethical “No Free Lunch” Rule
* Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise.
  + Professional Codes of Conduct
* When groups of people claim to be professionals, they take on special rights and obligations because of their special claims to knowledge, wisdom, and respect
* Professional codes of conduct are promulgated by associations of professionals
* American Medical Association (AMA), the American Bar Association (ABA)
* Codes of ethics are promises by professions to regulate themselves in the general interest of society
  + Some Real-World Ethical Dilemmas
* Information systems have created new ethical dilemmas in which one set of interests is pitted against another
* Facebook monitors its subscribers and then sells the information to advertisers and app developers
* Example: right of company to maximize productivity of workers versus workers right to use Internet for short personal tasks
* A close analysis of the facts can sometimes produce compromised solutions that give each side “half a loaf.”

1. THE MORAL DIMENSIONS OF INFORMATION SYSTEMS
   * Information Rights: Privacy and Freedom in the Internet Age

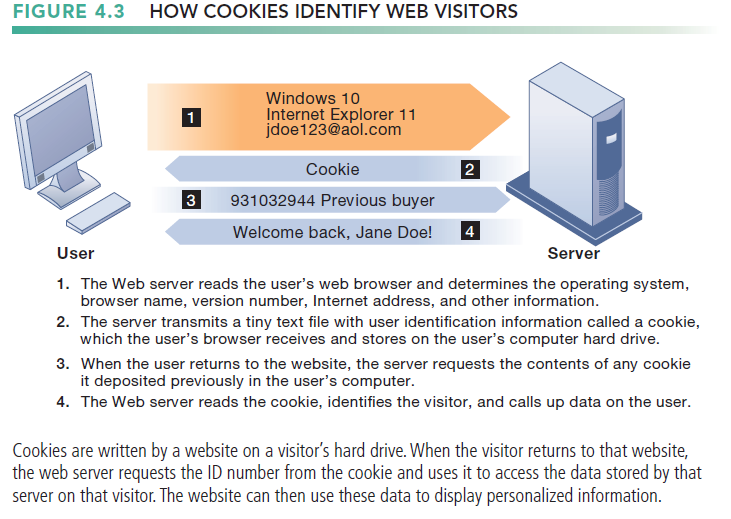
* Privacy
* the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state.
* FEDERAL PRIVACY LAWS IN THE UNITED STATES



* Fair information practices(FIP)
* a set of principles governing the collection and use of information about individuals
* Basis of most U.S. and European privacy laws
* updated most recently in 2010 to take into account new privacy-invading technology
* based on the notion of a mutuality of interest between the record holder and the individual.
* In 1998, the FTC (Federal Trade Commission) restated and extended the original FIP to provide guidelines for protecting online privacy.
* FIP principles are being used as guidelines to drive changes in privacy legislation
* FTC FIP principles
* Notice/awareness (core principle)
  + - Web sites must disclose practices before collecting data.
* Choice/consent (core principle)
  + - Consumers must be able to choose how information is used for secondary purposes.
* Access/participation
  + - Consumers must be able to review and contest accuracy of personal data.
* Security
  + - Data collectors must take steps to ensure accuracy, security of personal data
* Enforcement
  + - Must be mechanism to enforce FIP principles



* Used to drive changes in privacy legislation
* COPPA(Children’s Online Privacy Protection Act)
  + - requiring websites to obtain parental permission before collecting information on children under the age of 13.
* In 2010, the FTC added three practices to its framework for privacy
  + - Adopt privacy by design, building products and services that protect privacy
    - increase the transparency of their data practices
    - require consumer consent and provide clear options to opt out of data collection schemes
* Other proposed Internet privacy legislation focuses on protecting the online use of personal identification numbers
  + - Social security numbers
* Opt-in policy
  + - Privacy advocates want both an opt in policy at all sites and a national Do Not Track list.
    - The industry opposes these moves and continues to insist on an opt-out capability being the only way to avoid tracking.
* National Do-Not-Track lists
  + - Rockefeller supports the Do-Not-Track Online Act of 2011, which requires firms to notify consumers they are being tracked and allows consumers to opt out of the tracking (U.S. Senate, 2011).
* Gramm-Leach-Bliley Act(1999)
  + - required to disclose their policies and practices for protecting the privacy of nonpublic personal information and to allow customers to opt out of information-sharing arrangements with nonaffiliated third parties.
* HIPAA(1996)
  + - took effect on April 14, 2003, includes privacy protection for medical records
* The European Directive on Data Protection(已被GDRP取代)
* European countries do not allow businesses to use personally identifiable information without consumers’ prior consent.
* The directive requires companies to inform people when they collect information about them and disclose how it will be stored and used.
* Customers must provide their informed consent before any company can legally use data about them, and they have the right to access that information, correct it, and request that no further data be collected.
* In 2009, the European Parliament passed new rules governing the use of third-party cookies for behavioral tracking purposes, and required website visitors to give explicit consent to be tracked by cookies
* In 2015 Europe’s highest court struck down the safe harbor agreement, in large part because of revelations that U.S. intelligence agencies had gained access to EU personal data stored in the U.S
* The European Council subsequently approved the EU General Data Protection Regulation (GDPR) to replace the existing Data Protection Directive
  + - The concept of safe harbor was replaced by a policy now called Privacy Shield
* The GDPR will apply to any firm operating in any EU country
  + - require unambiguous consent to use personal data for purposes , limit the ability to use data for purposes other than those for which it was collected (tertiary uses, such as constructing user profiles), and strengthen the right to be forgotten, specifically, by allowing individuals to remove personal data from social platforms and prevent them from collecting any new information.
* Internet Challenges to Privacy
* Cookies
  + - small text files deposited on a computer hard drive when a user visits Web sites.
    - Identify visitor’s browser and track visits to site



* Super cookies (Flash cookies)
  + - cannot be easily deleted and can be installed whenever a person clicks on a Flash video.
    - “Local Shared Object” files are used by Flash to play videos and are put on the user’s computer without their consent.
* Web beacons (Web bugs)
  + - Tiny graphics embedded in e-mail messages and Web pages, Monitor who is reading e-mail message or visiting site
    - tiny software programs that keep a record of users’ online clickstream and report this data back to whomever owns the tracking file invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending e-mail.
    - Web beacons are placed on popular Web sites by third-party firms who pay the Web sites a fee for access to their audience.
* Spyware
  + - Surreptitiously installed on user’s computer
    - It calls out to Web sites to send banner ads and other unsolicited material to the user, and it can report the user’s movements on the Internet to other computers
* Google services and behavioral targeting
* The United States has allowed businesses to gather transaction information generated in the marketplace and then use that information for other marketing purposes
  + - without obtaining the informed consent of the individual whose information is being used.
* An opt-out model of informed consent
  + - permits the collection of personal information until the consumer specifically requests that the data not be collected
* Online industry promotes self-regulation over privacy legislation
  + - TRUSTe
* Members of the advertising network industry, including Google’s DoubleClick, have created an additional industry association called the Network Advertising Initiative (NAI)
  + - develop its own privacy policies to help consumers opt out of advertising network programs and provide consumers redress from abuses.
* extent of responsibility taken varies
  + - Statements of information use
    - AOL established an opt-out policy
    - Online “seals” of privacy principles
    - Most privacy policies are difficult to understand
* Technical Solutions
* few technologies that can protect user privacy during interactions with Web sites
  + - E-mail encryption
    - Anonymity tools
    - Anti-spyware tools
    - Browser features -“Private” browsing ,“Do not track” options
* For the most part, technical solutions have failed to protect users from being tracked as they move from one site to another
  + Property Rights: Intellectual Property
* Preface
* Intellectual property
  + - intangible property created by individuals or corporations.
* Information technology has made it difficult to protect intellectual property
  + - computerized information can be so easily copied or distributed on networks.
* trade secrets
* Any intellectual work product—a formula, device, pattern, or compilation of data—used for a business purpose can be classified as a trade secret, provided it is not based on information in the public domain.
* grant a monopoly on the ideas behind a work product, but it can be a very tenuous monopoly.
* Software that contains novel or unique elements, procedures, or compilations can be included as a trade secret.
* Trade secret law protects the actual ideas in a work product, not only their manifestation.
* take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain
* copyright
* Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author’s death
* For corporate-owned works, copyright protection lasts for 95 years after their initial creation.
* The intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work.
* Copyright protects against copying of entire programs or their parts.
* The drawback to copyright protection is that the underlying ideas behind a work are not protected, only their manifestation in a work.
* patent law
* A patent grants the owner an exclusive monopoly on the ideas behind an invention for 20 years.
* The key concepts in patent law are originality, novelty, and invention.
* The strength of patent protection is that it grants a monopoly on the underlying concepts and ideas of software.
* Challenges to Intellectual Property Rights
* Digital media different from physical media (e.g., books)
  + - Ease of replication
    - Ease of transmission (networks, Internet)
    - Ease of alteration
    - Difficulty in classifying software
    - Compactness
    - Difficulties in establishing uniqueness
* Closed environments
  + - iTunes Store, Kindle, Netflix, Spotify
* Digital Millennium Copyright Act (DMCA)
  + - implemented a World Intellectual Property Organization Treaty that makes it illegal to circumvent technology based protections of copyrighted materials.

1. How have information systems affected laws for establishing accountability and liability and the quality of everyday life?
   * Accountability, Liability, and Control

* Preface
* Along with privacy and property laws, new information technologies are challenging existing liability laws and social practices for holding individuals and institutions accountable.
  + - If a person is injured by a machine controlled, in part, by software, who should be held accountable and, therefore, held liable?
* Computer-related liability problems
* If software fails, who is responsible?
  + - If seen as part of machine that injures or harms, software producer and operator may be liable.
    - If seen as similar to book, difficult to hold author/publisher responsible.
    - What should liability be if software seen as service? Would this be similar to telephone systems not being liable for transmitted messages?
  + System Quality: Data Quality and System Errors
* What is an acceptable, technologically feasible level of system quality?
* Flawless software is economically unfeasible.
* Three principal sources of poor system performance
* software bugs and errors
* hardware or facility failures caused by natural or other causes
* poor input data quality
  + - The software industry has not yet arrived at testing

standards for producing software of acceptable but imperfect performance.

* By far the most common source of business system failure is data quality
* individual organizations report data error rates ranging from 0.5 to 30 percent.
  + Quality of Life; Equity, Access, and Boundaries
* Preface
* The negative social costs of introducing information technologies and systems are beginning to mount along with the power of the technology
* Balancing Power: Center Versus Periphery
* The shift toward highly decentralized computing, coupled with an ideology of empowerment of thousands of workers, and the decentralization of decision making to lower organizational levels, have reduced the fears of power centralization in government institutions
* At the same time, corporate Internet behemoths like Google, Apple, Yahoo, Amazon, and Microsoft have come to dominate the collection and analysis of personal private information of all citizens
  + - although computing power decentralizing, key decision making remains centralized
* Rapidity of Change: Reduced Response Time to Competition
* Time-based competition has an ugly side
  + - The business you work for may not have enough time to respond to global competitors and may be wiped out in a year, along with your job
* Maintaining Boundaries: Family, Work, and Leisure
* computing, Internet use lengthens work-day, infringes on family, personal time
* The traditional boundaries that separate work from family and just plain leisure have been weakened.
* The work umbrella now extends far beyond the eight-hour day into commuting time, vacation time, and leisure time.
* Extensive Internet use, even for entertainment or recreational purposes, takes people away from their family and friends.
* Among middle school and teenage children, it can lead to harmful antisocial behavior, such as the recent upsurge in cyberbullying
* Dependence and Vulnerability
* our businesses, governments, schools, and private associations, are incredibly dependent on information systems and are, therefore, highly vulnerable if these systems fail
* The absence of standards and the criticality of some system applications will probably call forth demands for national standards and perhaps regulatory oversight.
* Computer Crime and Abuse
* Computer crime
  + - the commission of illegal acts through the use of a computer or against a computer system
* The most common type of attack
  + - malware infection (67%)
    - phishing fraud (39%)
    - laptop and mobile hardware theft (34%)
    - attacks by botnets (29%)
    - insider abuse (25%)
* Computer abuse
  + - the commission of acts involving a computer that may not be illegal but that are considered unethical
* Spam
  + - junk e-mail sent by an organization or individual to a mass audience of Internet users who have expressed no interest in the product or service being marketed.
    - Spammers tend to market pornography, fraudulent deals and services, outright scams, and other products not widely approved in most civilized societies.
    - Most spam originates from bot networks, which consist of thousands of captured PCs that can initiate and relay spam messages.
* Employment: Trickle-Down Technology and Reengineering Job Loss
* redesigning business processes has caused millions of mid-level managers and clerical workers to lose their jobs.
* Careful planning and sensitivity to employee needs can help companies redesign work to minimize job losses.
* Equity and Access: Increasing Racial and Social Class Cleavages
* digital divide
  + - A similar digital divide exists in U.S. schools, with schools in high poverty areas less likely to have computers, high-quality educational technology programs, or Internet access availability for their students.
* Health Risks: RSI, CVS, and Technostress
* Repetitive stress injury (RSI)
  + - when muscle groups are forced through repetitive actions often with high-impact loads (such as tennis) or tens of thousands of repetitions under low impact loads (such as working at a computer keyboard).
    - Designing workstations for a neutral wrist position (using a wrist rest to support the wrist), proper monitor stands, and footrests all contribute to proper posture and reduced RSI.
    - Ergonomically correct keyboards are also an option
* carpal tunnel syndrome (CTS)
* Computer vision syndrome (CVS)
  + - refers to any eyestrain condition related to display screen use in desktop computers, laptops, e readers, smartphones, and handheld video games.
* Technostress
  + - Aggravation, impatience, fatigue