

TEL2813/IS2820 Security Management

Legal & Ethical Issues
Lecture 12
April 7, 2005



Laws and Security

- Federal and state laws affect privacy and secrecy
 - Rights of individuals to keep information private
- Laws regulate the use, development and ownership of data and programs
 - Patent laws, trade secrets
- Laws affect actions that can be taken to protect secrecy, integrity and availability



Copyrights

- Designed to protect expression of ideas
- Gives an author exclusive rights to make copies of the expression and sell them to public
- Intellectual property (copyright law of 1978)
 - Copyright must apply to an original work
 - It must be done in a tangible medium of expression
- Originality of work
 - Ideas may be public domain
- Copyrighted object is subjected to fair use



Copyright infringement

- Involves copying
- Not independent work
 - Two people can have copyright for identically the same thing
- Copyrights for computer programs
 - Copyright law was amended in 1980 to include explicit definition of software
 - Program code is protected not the algorithm
 - Controls rights to copy and distribute



Patent

- Protects innovations
 - Applies to results of science, technology and engineering
 - Protects new innovations
 - Device or process to carry out an idea, not idea itself
 - Excludes newly discovered laws of nature
 - $2+2 = 4$



Patent


- Requirements of novelty
 - If two build the same innovations, patent is granted to the first inventor, regardless of who filed first
 - Invention should be truly novel and unique
 - Object patented must be non-obvious
- Patent Office registers patents
 - Even if someone independently invents the same thing, without knowledge of the existing patent
- Patent on computer objects
 - PO has not encouraged patents for software – as they are seen as representation of an algorithm

Trade Secret

- Information must be kept secret
 - If someone discovers the secret independently, then there is no infringement – trade secret rights are gone
 - Reverse-engineering can be used to attack trade secrets
- Computer trade secret
 - Design idea kept secret
 - Executable distributed but program design remain hidden


Comparison

	Copyright	Patent	Trade secret
Protects	Expression of idea	Invention	Secret information
Object made public	Yes: intention is to promote	Design filed at patent office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Life of human originator or 75 years of company	19 years	Indefinite
Legal protection	Sue if copy sold	Sue if invention copied	Sue if secret improperly obtained
Examples	Object code, documentation	Hardware	Source code




Employee and Employer Rights

- Employees generate idea and products
- Ownership is an issue in computer security
 - Rights of employer to protect the works of employees
- Ownership of products
 - Eve writes programs at night and sells it herself
 - If Eve is a programmer in a company and the program remotely corresponds to her job,
 - Employer may claim it!
- If Eve is self-employed but an earlier version was developed for a company
 - Company may show that it had paid for the program and then claim ownership



Employee and Employer Rights

- Ownership of patents
 - If employee lets employer file the patent employer is deemed to own the patent and therefore the rights to the innovation
 - Employer has right to patent if the employee's job function includes inventing the product
- Similar issues for ownership of copyright
 - A special issue is work-for-hire
 - Employer is the author of the work



Employee and Employer Rights

- Work-for-hire situations
 - The employer has a supervisory relationship overseeing the manner in which the creative work is done
 - The employer has right to fire the employee
 - The employer arranges work to be done before the work was created
 - A written statement that states the employer has hired the employee to do certain work
- Alternate to work-for-hire is License
 - Programmer owns the product- sells license to company
 - Beneficial for the programmer



Computer crime

- Hard to predict for the following reason
 - Low computer literacy among lawyers, police agents, jurors, etc.
 - Tangible evidence like fingerprints and physical clues may not exist
 - Forms of asset different
 - Is computer time an asset?
 - Juveniles
 - Many involve juveniles




The Legal Environment

- Information security professionals and managers must possess a rudimentary grasp of the legal framework within which their organizations operate
- This legal environment can influence the organization to a greater or lesser extent depending on the nature of the organization and the scale on which it operates



Types Of Law

- Civil law: pertains to relationships between and among individuals and organizations
- Criminal law: addresses violations harmful to society and actively enforced/prosecuted by the state
- Tort law: subset of civil law which allows individuals to seek recourse against others in the event of personal, physical, or financial injury
- Private law: regulates relationships among individuals and among individuals and organizations
 - Encompasses family law, commercial law, and labor law
- Public law: regulates structure and administration of government agencies and their relationships with citizens, employees, and other governments
 - Includes criminal, administrative, and constitutional law



Computer Fraud and Abuse Act of 1986

- Computer Fraud and Abuse Act of 1986 (CFA Act)
 - cornerstone of many computer-related federal laws and enforcement efforts
 - Amended October 1996 by National Information Infrastructure Protection Act of 1996
 - to increase penalties for selected crimes
 - further modified by the USA Patriot Act of providing law enforcement with broader latitude to combat terrorism-related activities



Communication Act of 1934

- Communication Act of 1934 was revised by the Telecommunications Deregulation and Competition Act of 1996,
 - which attempts to modernize archaic terminology of older act
 - Provides penalties for misuse of telecommunications devices, specifically telephones



Computer Security Act of 1987

- Computer Security Act of 1987
 - was one of first attempts to protect federal computer systems by establishing minimum acceptable security practices
- Act charged National Bureau of Standards and National Security Agency with the following tasks:
 - Developing standards, guidelines, and associated methods and techniques for computer systems
 - Developing uniform standards and guidelines for most federal computer systems



Computer Security Act of 1987 (Continued)

- Developing technical, management, physical, and administrative standards and guidelines for cost-effective security and privacy of sensitive information in federal computer systems
- Developing guidelines for use by operators of federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice
- Developing validation procedures for, and evaluate the effectiveness of, standards and guidelines through research and liaison with other government and private agencies



Computer Security Act of 1987 (Continued)

- Established Computer System Security and Privacy Advisory Board within Department of Commerce
- Amended Federal Property and Administrative Services Act of 1949,
 - requiring National Bureau of Standards to distribute standards and guidelines pertaining to federal computer systems,
 - making such standards compulsory and binding
- Requires
 - mandatory periodic training in computer security awareness and accepted computer security practice for all users of federal computer systems



Privacy Laws

- Many organizations collect, trade, and sell personal information as a commodity
 - Many individuals are becoming aware of these practices and looking to governments to protect their privacy
- In the past, not possible to create databases that contained personal information collected from multiple sources
 - Today, aggregation of data from multiple sources permits some to build databases with alarming quantities of personal information



Privacy Laws

- Privacy of Customer Information Section of the section of regulations covering common carriers specifies that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes



Privacy Laws (Continued)

- Federal Privacy Act of 1974
 - regulates the government's use of private information
 - Created to ensure that
 - government agencies protect privacy of individuals' and businesses' information, and
 - hold them responsible if this information is released without permission
- Electronic Communications Privacy Act of 1986
 - is a collection of statutes that regulates the interception of wire, electronic, and oral communications
 - Works in cooperation with the Fourth Amendment of the U.S. Constitution which prohibits search and seizure without a warrant



HIPAA

- Health Insurance Portability & Accountability Act Of 1996 (HIPAA),
 - also known as the Kennedy-Kassebaum Act
 - Protects confidentiality and security of health care data by establishing and enforcing standards and standardizing electronic data interchange
 - Requires organizations that retain health care information to use information security mechanisms to protect this information, as well as policies and procedures to maintain them
 - Requires comprehensive assessment of organization's information security systems, policies, and procedures



HIPAA (Continued)

- HIPAA provides guidelines for
 - the use of electronic signatures based on security standards ensuring message integrity, user authentication, and non-repudiation
- Five fundamental privacy principles:
 - Consumer control of medical information
 - Boundaries on the use of medical information
 - Accountability for the privacy of private information
 - Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
 - Security of health information



Gramm-Leach-Bliley Act

- Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999
 - Applies to banks, securities firms, and insurance companies
 - Requires all financial institutions
 - to disclose privacy policies and
 - To describe how they share nonpublic personal information and
 - To describe how customers can request that their information not be shared with third parties
 - Ensures that
 - privacy policies are fully disclosed when a customer initiates a business relationship, and
 - distributed at least annually for the duration of the professional association




Export and Espionage Laws

- Congress passed the Economic Espionage Act (EEA) in 1996
 - In an attempt to protect intellectual property and competitive advantage,
 - it attempts to protect trade secrets
- Security and Freedom through Encryption Act of 1997
 - Provides guidance on use of encryption
 - Institutes measures of public protection from government intervention
 - Reinforces individual's right to use or sell encryption algorithms without concern for the impact of other regulations requiring some form of key registration
 - Prohibits federal government from requiring use of encryption for contracts, grants, and other official documents and correspondence



U.S. Copyright Law

- U.S. copyright law
 - extends protection to intellectual property, which includes words published in electronic formats
- 'Fair use' allows
 - material to be quoted so long as the purpose is educational and not for profit, and the usage is not excessive
- Proper acknowledgement
 - must be provided to author and/or copyright holder of such works, including a description of the location of source materials by using a recognized form of citation



Freedom of Information Act of 1966 (FOIA)

- All federal agencies are required under the Freedom of Information Act (FOIA) to
 - disclose records requested in writing by any person
- FOIA applies
 - only to federal agencies and
 - does not create a right of access to records held by Congress, the courts, or by state or local government agencies



Sarbanes-Oxley Act of 2002

- Sarbanes-Oxley Act of 2002
 - enforces accountability for financial record keeping and reporting at publicly traded corporations
 - Requires that CEO and chief financial officer (CFO) assume direct and personal accountability for completeness and accuracy of a publicly traded organization's financial reporting and record-keeping systems
- As these executives attempt to ensure that the systems used to record and report are sound—often relying upon the expertise of CIOs and CISOs to do so—the related areas of availability and confidentiality are also emphasized




International Laws And Legal Bodies

- Many domestic laws and customs
 - do not apply to international trade which is governed by international treaties and trade agreements
- Because of cultural differences and political complexities of the relationships among nations,
 - there are currently few international laws relating to privacy and information security



European Council Cyber-Crime Convention

- European Council Cyber-Crime Convention
 - Empowers an international task force to
 - oversee a range of Internet security functions and
 - to standardize technology laws internationally
 - Attempts
 - to improve effectiveness of international investigations into breaches of technology law
 - Overall goal:
 - simplify acquisition of information for law enforcement agents in certain types of international crimes, as well as the extradition process



Digital Millennium Copyright Act (DMCA) and other IP protection

- Digital Millennium Copyright Act (DMCA)
 - U.S.-based international effort
 - to reduce impact of copyright, trademark, and privacy infringement especially via the removal of technological copyright protection measures
- European Union created Directive 95/46/EC
 - that increases individual rights to process and freely move personal data
 - United Kingdom has already implemented a version of this directive called the Database Right




State and Local Regulations

- Georgia Computer Systems Protection Act
 - Has various computer security provisions
 - Establishes specific penalties for use of information technology to attack or exploit information systems in organizations
- Georgia Identity Theft Law
 - Requires that a business may not discard a record containing personal information unless it, shreds, erases, modifies or otherwise makes the information irretrievable



Policy versus Law

- Key difference between policy and law is that ignorance of policy is an acceptable defense; therefore policies must be:
 - Distributed to all individuals who are expected to comply with them
 - Readily available for employee reference
 - Easily understood, with multilingual translations and translations for visually impaired or low-literacy employees
 - Acknowledged by the employee, usually by means of a signed consent form



Ethical Concepts In Information Security

- Information security student is not expected
 - to study the topic of ethics in a vacuum, but within a larger ethical framework
- However, those employed in the area of information security may be
 - expected to be more articulate about the topic than others in the organization
 - Often must withstand a higher degree of scrutiny



Ethics

- An objectively defined standard of right and wrong
- Often idealistic principles
- In a given situation several ethical issues may be present
- Different from law



Law and Ethics in Information Security

- Laws are rules adopted and enforced by governments to codify expected behavior in modern society
- Key difference between law and ethics is that
 - law carries the sanction of a governing authority and ethics do not
- Ethics are based on cultural mores:
 - relatively fixed moral attitudes or customs of a societal group



Law vs. Ethics

Law

- Described by formal written documents
- Interpreted by courts
- Established by legislatures representing all people
- Applicable to everyone
- Priority determined by laws if two laws conflict
- Court is final arbiter for right
- Enforceable by police and courts

Ethics

- Described by unwritten principles
- Interpreted by each individual
- Presented by philosophers, religions, professional groups
- Personal choice
- Priority determined by an individual if two principles conflict
- No external arbiter
- Limited enforcement


Ethical reasoning

- Consequence-based
 - Based on the good that results from an action
- Rule-based
 - Based on the certain prima facie duties of people

	Consequence-based	Rule-based
Individual	Based on consequences to individual	Based on rules acquired by the individual from religion, experience, analysis
Universal	Based on consequences to all of society	Based on universal rules, evident to everyone


Ethics Example

- Privacy of electronic data
 - “gentlemen do not read others’ mail” - but not everyone is a gentleman!
 - Ethical question: when is it justifiable to access data not belonging to you
 - One approach: Protection is user’s responsibility
 - Another: supervisors have access to those supervised
 - Another: justifiably compelling situation



Codes of ethics

- IEEE professional codes of ethic
 - To avoid real or perceived conflict of interest whenever possible, and to disclose them to affected parties when they do exist
 - To be honest and realistic in stating claims or estimates based on available data
- ACM professional codes of ethics
 - Be honest and trustworthy
 - Give proper credit for intellectual property



The Ten Commandments of Computer Ethics (from The Computer Ethics Institute)

- Thou shalt not use a computer to harm other people
- Thou shalt not interfere with other people's computer work
- Thou shalt not snoop around in other people's computer files
- Thou shalt not use a computer to steal
- Thou shalt not use a computer to bear false witness
- Thou shalt not copy or use proprietary software for which you have not paid
- Thou shalt not use other people's computer resources without authorization or proper compensation
- Thou shalt not appropriate other people's intellectual output
- Thou shalt think about the social consequences of the program you are writing or the system you are designing
- Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans



Differences In Ethical Concepts

- Studies reveal that individuals of different nationalities have different perspectives on the ethics of computer use
- Difficulties arise when one nationality's ethical behavior does not correspond to that of another national group
 - Categories
 - Software licensing
 - Illicit use
 - Misuse of Corporate resources



Ethics And Education

- Differences in computer use ethics are not exclusively cultural
 - Found among individuals within the same country, same social class, same company
- Key studies reveal that overriding factor in leveling ethical perceptions within a small population is education
- Employees must be trained and kept up to date on information security topics, including the expected behaviors of an ethical employee



Deterring Unethical and Illegal Behavior

- Responsibility of information security personnel to do everything in their power
 - to deter unethical and illegal acts,
 - using policy, education, training, and technology as controls or safeguards to protect the information and systems
- Many security professionals understand technological means of protection
 - Many underestimate the value of policy



Deterring Unethical and Illegal Behavior (Continued)

- Three general categories of unethical behavior that organizations and society should seek to eliminate:
 - Ignorance
 - Accident
 - Intent
- Deterrence is the best method for preventing an illegal or unethical activity
 - Example: laws, policies, and technical controls



Deterring Unethical and Illegal Behavior (Continued)

- Generally agreed that laws, policies and their associated penalties only deter if three conditions are present:
 - Fear of penalty
 - Probability of being caught
 - Probability of penalty being administered



Organizational Liability And The Need For Counsel

- What if an organization does not support or even encourage strong ethical conduct on the part of its employees?
- What if an organization does not behave ethically?
 - If an employee, acting with or without authorization, performs an illegal or unethical act causing some degree of harm, organization can be held financially liable
 - Organization increases its liability if it refuses to take measures—due care—to make sure that every employee knows what is acceptable and what is not, and the consequences of illegal or unethical actions
 - Due diligence requires that an organization make a valid and ongoing effort to protect others




Certifications And Professional Organizations

- A number of professional organizations have established codes of conduct and/or codes of ethics that members are expected to follow
- Codes of ethics can have a positive effect on an individual's judgment regarding computer use
- Remains individual responsibility of security professionals to act ethically and according to the policies and procedures of their employers, professional organizations, and laws of society




Association of Computing Machinery

- ACM is a respected professional society, originally established in 1947 as "the world's first educational and scientific computing society"
 - One of few organizations that strongly promotes education and provides discounted membership for students
- ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional




International Information Systems Security Certification Consortium, Inc.

- (ISC)2
 - Manages a body of knowledge on information security
 - Administers and evaluates examinations for information security certifications
 - Code of ethics is primarily designed for information security professionals who have earned one of their certifications



International Information Systems Security Certification Consortium, Inc. (Continued)

- (ISC)2 code of ethics includes four mandatory canons:
 - Protect society, commonwealth, and infrastructure
 - Act honorably, honestly, justly, responsibly, and legally
 - Provide diligent and competent service to principals
 - Advance and protect the profession



System Administration, Networking, and Security Institute (SANS)

- Founded in 1989, SANS is a professional research and education cooperative organization with over 156,000 security professionals, auditors, system and network administrators
- SANS certifications can be pursued independently or combined to earn the comprehensive certification called the GIAC Security Engineer
- GIAC Information Security Officer is an overview certification that combines basic technical knowledge with understanding of threats, risks, and best practices




Information Systems Audit and Control Association (ISACA)

- Information Systems Audit and Control Association is a professional association with a focus on auditing, control, and security
 - Membership comprises both technical and managerial professionals
 - Has a code of ethics for its professionals
 - Requires many of the same high standards for ethical performance as other organizations and certifications



CSI - Computer Security Institute (CSI)

- Computer Security Institute
 - Provides information and certification to support the computer, networking, and information security professional
 - Publishes newsletter and threat advisory
 - Is well known for its annual computer crime survey of threats developed in cooperation with the FBI



Information Systems Security Association

- Information Systems Security Association (ISSA) (www.issa.org)
 - Nonprofit society of information security professionals
 - Primary mission: bring together qualified practitioners of information security for information exchange and educational development
 - Provides conferences, meetings, publications, and information resources to promote information security awareness and education
 - Promotes code of ethics, similar to those of (ISC)2, ISACA, and ACM, "promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources"



Other Security Organizations

- Internet Society or ISOC
 - Nonprofit, nongovernmental, international professional organization
 - Promotes development and implementation of education, standards, policy, and training to promote the Internet
- Internet Engineering Task Force (IETF)
 - Consists of individuals from computing, networking, and telecommunications industries
 - Responsible for developing Internet's technical foundations
 - Standards reviewed by Internet Engineering Steering Group (IESG), with appeal to the Internet Architecture Board, and promulgated by the Internet Society as international standards



Other Security Organizations (Continued)

- Computer Security Division (CSD) of the National Institute for Standards and Technology (NIST) runs the Computer Security Resource Center (CSRC)—an essential resource for any current or aspiring information security professional
- CSD involved in five major research areas related to information security:
 - Cryptographic standards and applications
 - Security testing
 - Security research and emerging technologies
 - Security management and guidance
 - Outreach, awareness, and education



Other Security Organizations (Continued)

- CERT Coordination Center, or CERT/CC is a center of Internet security expertise part of Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University
 - Studies security issues
 - Provides publications and alerts to help educate public to the threats facing information security
 - Provides training and expertise in handling of computer incidents
 - Acts both as a research center and outside consultant in the areas of incident response, security practices, and programs development




Other Security Organizations (Continued)

- Computer Professionals for Social Responsibility (CPSR)
 - Public organization for technologists and anyone with a general concern about impact of computer technology on society
 - Promotes ethical and responsible development and use of computing
 - Seeks to inform public, private policy and lawmakers on this subject
 - Acts as ethical watchdog for development of ethical computing




Key U.S. Federal Agencies

- Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC)
 - U.S. government's focal point for threat assessment and the warning, investigation, and response to threats or attacks against critical U.S. infrastructures
- National InfraGard Program
 - A key part of the NIPC's efforts to educate, train, inform, and involve the business and public sector in information security
 - Every FBI field office has established a chapter and collaborates with public and private organizations and academic community to share information about attacks, vulnerabilities, and threats
 - Free exchange of information to and from private sector about threats and attacks on information resources



Key U.S. Federal Agencies (Continued)

- National Security Agency (NSA)
 - Cryptologic organization
 - Coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information
 - Responsible for signal intelligence and information system security
 - Information Assurance Directorate (IAD) provides information security "solutions including the technologies, specifications and criteria, products, product configurations, tools, standards, operational doctrine and support activities needed to implement the protect, detect and report, and respond elements of cyber defense"



Key U.S. Federal Agencies (Continued)

- U.S. Secret Service
 - Department within Department of the Treasury
 - Protects key members of U.S. government
 - Detection and arrest of any person committing U.S. federal offense relating to computer fraud and false identification crimes
 - Patriot Act (Public Law 107-56) increased Secret Service's role in investigating fraud and related activity in connection with computers
- Department of Homeland Security
 - Established with passage of Public Law 107-296 which in part, transferred United States Secret Service from Department of the Treasury to the new department effective March 1, 2003