IT AND ETHICS: 1

Overview

The assigned reading material and lecture notes for this week introduce the concepts of ethics and morality. Creating an ethical business environment is discussed and various approaches to making ethical decisions are presented. Finally, the reading material and lecture notes highlight some issues specific to information technology.

Learning Objectives

After reviewing the assigned reading material and lecture notes students should be able to:

1. Define ethics, and explain why it is important to act according to a code of ethics.
2. Outline why business ethics is becoming increasingly important.
3. Articulate what organizations are doing to improve their business ethics.
4. Describe corporate social responsibility.
5. Explore why organizations are interested in fostering corporate social responsibility and good business ethics.
6. Identify what approach you can take to ensure ethical decision making.
7. Recognize trends that have increased the risk of using information technology in an unethical manner.

Lecture Notes

I. What is ethics?

1. Every society forms a set of rules that establishes the boundaries of generally accepted behavior. These rules are often expressed in statements about how people should behave, and the individual rules fit together to form the moral code by which a society lives.
2. A moral code is a set of rules that establishes the boundaries of generally accepted behavior.
3. The term morality refers to social conventions about right and wrong that are so widely shared that they become the basis for an established consensus.

A. Definition of Ethics

1. Ethics is a set of beliefs about right and wrong behavior within a society.
   a. Ethical behavior conforms to generally accepted norms—many of which are almost universal. Behaviors that are considered ethical in one culture may be unethical in another. For example, software piracy —a form of copyright

infringement that involves making copies of software or enabling others to access software to which they are not entitled, may be acceptable in some cultures and yet considered very unethical in others. To learn more about software piracy, visit Adobe's Anti-Piracy site (http://www.adobe.com/aboutadobe/antipiracy/piracy.html).

b. People generally develop habits that make it easier for them to choose between what society considers good or bad. A virtue is a habit that inclines people to do what is acceptable, for example, fairness, kindness, and honesty. A vice is a habit of unacceptable behavior, such as greed, lying, and cheating.

B. The Importance of Integrity

1. A person who acts with integrity acts in accordance with a personal code of principles. One approach to acting with integrity—one of the cornerstones of ethical behavior—is to extend to all people the same respect and consideration that one expects to receive from others.
2. If people are consistent and act with integrity, they apply the same moral standards in all situations. However, there are situations in which it might be difficult to be consistent in applying moral standards because many ethical dilemmas are not as simple as right versus wrong but involve choices between right versus right.

C. The Difference between Morals, Ethics, and Laws

1. Morals refer to one's personal beliefs about right and wrong, while the term *ethics* describes standards or codes of behavior expected of an individual by a group (nation, organization, profession) to which an individual belongs.
2. Law is a system of rules that tells what can and cannot be done. Laws are enforced by a set of institutions (the police, courts, law-making bodies) and legal acts are acts that conform to the law.
3. Moral acts conform to what an individual believes to be the right thing to do.

II. Ethics in the Business World

1. Ethics has risen to the top of the business agenda because the risks associated with inappropriate behavior have increased, both in their likelihood and their potential negative impact.
2. Several trends have increased the likelihood of unethical behavior. For example, greater globalization has created a much more complex work environment that spans diverse cultures and societies, making it more difficult to apply principles and codes of ethics consistently.
3. Employees, shareholders, and regulatory agencies are increasingly sensitive to violations of accounting standards, failures to disclose substantial changes in business

conditions, nonconformance with required health and safety practices, and production of unsafe or substandard products. Such heightened vigilance raises the risk of financial loss for businesses that do not foster ethical practices or that run afoul of required standards.

A. Corporate Social Responsibility

1. Corporate social responsibility (CSR) is the concept that an organization should act ethically by taking responsibility for the impact of its actions on the environment, the community, and the welfare of its employees.
2. Supply chain sustainability is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs. For example, supply chain sustainability considers fair labor practices, human rights, and natural resource conservation.

B. Fostering Corporate Social Responsibility and Good Business Ethics

1. Reasons for pursuing CSR goals and promoting a work environment in which employees are encouraged to act ethically when making business decisions include:
    a. Gaining the Goodwill of the Community.
    b. Creating an Organization That Operates Consistently.
    c. Fostering Good Business Practices.
    d. Protecting the Organization and Its Employees from Legal Actions.
    e. Avoiding Unfavorable Publicity.

Gaining the Goodwill of the Community

1. Although organizations exist primarily to earn profits or provide services to customers, they also have some fundamental responsibilities to society. Organizations often declare these responsibilities in specific CSR goals including issuing a formal statement of the organization's values, principles, or beliefs.
2. Philanthropy is one way an organization can make a positive connection with associated communities. The goodwill that CSR activities generate can make it easier for organizations to conduct business. Organizations that are viewed as harmful to their community suffer disadvantages such as reduced sales.
3. To learn more about CSR activities, review Is Corporate Social Responsibility Responsible? (http://www.forbes.com/2006/11/16/leadership-philanthropy-charity-lead-citizen-cx_ba_1128directorship.html).

Creating an Organization That Operates Consistently

1. Organizations develop and abide by values to create an organizational culture and to define a consistent approach for dealing with the needs of their stakeholders.

2. Such consistency ensures that employees know what is expected of them and can employ the organization’s values to help them in their decision making.
3. Consistency also ensures that stakeholders know what to expect of the organization and that it will behave in the future much as it has behaved in the past.

Fostering Good Business Practices

1. In many cases, good ethics can mean good business and improved profits. Companies that produce safe and effective products avoid costly recalls and lawsuits.
2. To the contrary, bad ethics can have a negative impact on employees, many of whom may develop negative attitudes if they perceive a difference between their own values and those stated or implied by an organization’s actions.
3. When a discrepancy between employee and organizational ethics occurs, it destroys employee commitment to organizational goals and objectives, creates low morale, fosters poor performance, erodes employee involvement in organizational improvement initiatives, and builds indifference to the organization’s needs.

Protecting the Organization and Its Employees from Legal Actions

1. Current law states that organizations are liable for the acts of employees. In a 1909 ruling (*United States v. New York Central & Hudson River Railroad Co*.), the Supreme Court of the United States (SCOTUS) established that an employer can be held responsible for the acts of its employees even if the employees act in a manner contrary to corporate policy and their employer’s directions. The principle established is called *respondeat superior*, or “let the master answer.”
2. However, a coalition of several legal organizations argues that organizations should “be able to escape criminal liability if they have acted as responsible corporate citizens, making strong efforts to prevent and detect misconduct in the workplace.” One way to do this is to establish effective ethics and compliance programs.

Avoiding Unfavorable Publicity

1. The public reputation of a company strongly influences the value of its stock, how consumers regard its products and services, the degree of oversights it receives from government agencies, and the amount of support and cooperation it receives from its business partners.
2. Therefore, many organizations are motivated to build a strong ethics program to avoid negative publicity.

C. Improving Corporate Ethics

1. The Ethics Resource Center (ERC) has defined a set of characteristics of a successful ethics program. The characteristics include environments where:

a. Employees are willing to seek advice about ethics issues.
b. Employees feel prepared to handle situations that could lead to misconduct.
c. Employees are rewarded for ethical behavior.
d. Employees are not rewarded for success obtained through questionable means.
e. Employees feel positively about their company.

2. To improve business ethics, organizations should consider appointing a corporate ethics officer, ensuring that board of directors set ethical standards of behavior, establishing a corporate code of ethics, conducting social audits, requiring employees to take ethics training and including ethical criteria in employee appraisals.

Appointing a Corporate Ethics Officer

1. A corporate ethics officer (also called a corporate compliance officer) provides an organization with vision and leadership in the area of business conduct. The corporate ethics office is responsible for aligning the practices of the organization with the stated ethics and beliefs of the organization, holding people accountable to ethical standards.
2. Ideally, the corporate ethics officer should be a well-respected, senior-level manager who reports directly to the CEO.

Ethical Standards Set by Board of Directors

1. The board of director’s primary objective is to oversee the organization’s business activities and management for the benefit of all stakeholders.
2. Board members are expected to conduct themselves according to the highest standards for personal and professional integrity, while setting the standard for company-wide ethical conduct and ensuring compliance with laws and regulations.

Establishing a Corporate Code of Ethics

1. A code of ethics is a statement that highlights an organization’s key ethical issues and identifies the overarching values and principles that are important to an organization and its decision making. An effective code of ethics helps ensure that employees abide by the law, follow necessary regulations, and behave in an ethical manner.
2. The Sarbanes–Oxley Act of 2002 was passed in response to public outrage over several major accounting scandals, including those at Enron, WorldCom, Tyco, Adelphia, Global Crossing, and Qwest—plus numerous restatements of financial reports by other companies, which demonstrated a lack of oversight within corporate America.
3. Section 404 of the Sarbanes-Oxley Act states that annual reports must contain a statement signed by the CEO and CFO attesting that the information contained in all of the firm’s Securities and Exchange Commission (SEC) filings is accurate.

4. Section 406 of the Sarbanes-Oxley Act requires public companies to disclose whether they have a code of ethics and to disclose any waiver of the code for certain members of senior management.
5. To learn more about the Sarbanes-Oxley Act, visit Bill Text, 107th Congress (92001-2002), H.R.3763.ENR (http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:)

Conducting Social Audits

1. In a social audit, an organization reviews how well it is meeting its ethical and social responsibility goals, and communicates its new goals for the upcoming year.

Requiring Employees to Take Ethics Training

1. Lawrence Kohlberg found that many factors stimulate a person's moral development, but one of the most crucial is education.
2. An organization's code of ethics must be promoted and continually communicated within the organization, from top to bottom. Organizations can do this by showing employees examples of how to apply the code of ethics in real life. One approach is through a comprehensive ethics education program that encourages employees to act responsibly and ethically.
3. Formal ethics training not only makes employees more aware of a company's code of ethics and how to apply it, but also demonstrates that the company intends to operate in an ethical manner.
4. The existence of formal training programs can also reduce a company's liability in the event of legal action.

Including Ethical Criteria in Employee Appraisals

1. Managers can help employees to meet performance expectations by monitoring employee behavior and providing feedback.
2. Managers are increasingly including ethical conduct as part of an employee's performance appraisal.

III. Including Ethical Considerations in Decision Making

Most people have developed a decision-making process that they execute automatically, without thinking about the steps they go through. The process generally consists of (a) developing a problem statement, (b) identifying alternatives, (c) evaluate and choosing an alternative, (d) implementing a decision, and (e) evaluating results.

A. Develop a Problem Statement

1. A good problem statement answers the following questions:
   a. What do people observe that causes them to think there is a problem?
   b. Who is directly affected by the problem?

   c. Is anyone else affected?
   d. How often does the problem occur?
   e. What is the impact of the problem?
   f. How serious is the problem?
2. Part of developing a good problem statement involves identifying the stakeholders and their positions on the issue.
3. The textbook provides examples of good and bad problem statements on page 21.

B. Identify Alternatives

1. It is ideal to enlist the help of others, including stakeholders, to identify several alternative solutions to the problem. Brainstorming with others will increase a person's chances of identifying a broad range of alternatives and determining the best solution.
2. During any brainstorming process, one should try not to be critical of ideas, as any negative criticism will tend to shut down the discussion, and the flow of ideas will dry up. Instead, one should simply write down the ideas as they are suggested.

C. Evaluate and Choose an Alternative

1. Once a set of alternatives has been identified, they should be evaluated based on numerous criteria, such as effectiveness at addressing the issue, the extent of risk associated with each alternative, cost, and time to implement.
2. The alternative selected should be ethically and legally defensible; be consistent with the organization's policies and code of ethics; take into account the impact on others; and provide a good solution to the problem.
3. Philosophers have developed many approaches to aid in ethical decision making. Four of the most common approaches are discussed next.

Virtue Ethics Approach

1. The virtue ethics approach to decision making focuses on how people should behave and think about relationships if they are concerned with their daily life in a community. It does not define a formula for ethical decision making, but suggests that when faced with a complex ethical dilemma, people do either what they are most comfortable doing or what they think a person they admire would do.
2. A problem with the virtue ethics approach is that it doesn't provide much of a guide for action.

Utilitarian Approach

1. The utilitarian approach to ethical decision making states that one should choose the action or policy that has the best overall consequences for all stakeholders.
2. A complication of this approach is that measuring and comparing the values of certain benefits and costs is often difficult, if not impossible.

Fairness Approach

1. The fairness approach focuses on how fairly actions and policies distribute benefits and burdens among people affected by the decision.
2. Decisions made with this approach can be influenced by personal bias, without the decision makers even being aware of their bias.

Common Good Approach

1. The common good approach to decision making is based on a vision of society as a community whose members work together to achieve a common set of values and goals.
2. The potential complication of this approach is that consensus is difficult because people clearly have different ideas about what constitutes the common good.

D. Implement the Decision

1. Once an alternative is selected, it should be implemented in an efficient, effective, and timely manner.
2. Communication is crucial to implementing a decision because people tend to resist change unless the change is well communicated.

E. Evaluate the Results

1. Post-implementation, the results must be monitored to see if the desired effect was achieved, and its impact on the organization and the various stakeholders must be observed.
2. If further refinements are needed, managers should return to develop a problem statement step, refine the problem statement as necessary, and work through the process again.

IV. Ethics in Information Technology

1. The ability to capture and store vast amounts of personal data, and greater reliance on information systems in all aspects of life has increased the risk that information technology will be used unethically.

2. Examples of Information technology ethics challenges include:
    a. Employers monitoring email and Internet usage by employees.
    b. Illegal downloading of music and movies.
    c. Hackers breaking into financial and retail institutions such as the recent data breaches reported by Target and Home Depot.
    d. Use of big data to track people’s online purchases and activities.

IT and Ethics: 2

Overview

The assigned reading material and lecture notes for this week provides an overview of security, starting with reasons why attacks on computer systems are on the rise. The material presents different types of perpetrators of attacks, and the methods used by attackers. Finally, the material ends with a discussion of how to prevent attacks and an overview of the components of an effective security policy.

Objectives

After reviewing the assigned reading material and lecture notes students should be able to:

1. Identify key trade-offs and ethical issues associated with the safeguarding of data and information systems.
2. Explain why there has been a dramatic increase in the number of computer-related security incidents in recent years.
3. Outline the most common types of computer security attacks.
4. Classify the primary perpetrators of computer crime, and list their objectives.
5. Describe the key elements of a multilayer process for managing security vulnerabilities based on the concept of reasonable assurance.

Lecture Notes

I. IT Security Incidents: A Major Concern

1. The security of information technology used in business is critical, but it must often be balanced against other business needs.
2. Business managers, IT professionals, and IT users often face various IT Security ethical decisions including:
    a. Pursuing prosecution of criminals at all costs102 or maintaining a low profile to avoid negative publicity.
    b. What actions to take if recommended computer security safeguards make conducting business more difficult for customers and employees, resulting in lost sales and increased costs.

A. Why Computer Incidents Are So Prevalent

1. The rise in computer incidents may be attributed to factors that include the following:
    a. Increases in complexity coupled with increases in vulnerabilities.
    b. Higher computer user expectations.
    c. Expanding and changing systems introducing new risks.

d. Adoption of bring your own device (BYOD) policy by businesses.
e. Increased reliance on commercial software with known vulnerabilities.

Increasing Complexity Increases Vulnerability

1. Today's computing environment has become increasingly complex. The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches.
2. Today's computing environment is also further complicated by the growing use of cloud computing services. Cloud computing is an environment in which software and data storage are services provided via the Internet (the cloud); the services are run on another organization's computer hardware and are accessed predominantly via a Web browser.
3. Virtualization also introduces further complications into today's computing environment. Virtualization software is a software program that emulates computer hardware by enabling multiple operating systems to run on a single computer host.

Higher Computer User Expectations

1. Today, time means money, and the faster computer users can solve a problem, the sooner they can be productive.
2. As a result, computer help desks personnel are under intense pressure to respond very quickly to users' questions and sometimes forget to verify users' identities.

Expanding and Changing Systems Introduce New Risks

1. The growing adoption of computer use cases such as e-commerce, mobile computing, and collaborative work groups coupled with ever changing technology has introduced new security challenges for IT professionals.
2. It is increasingly difficult to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them.

Bring Your Own Device

1. **Bring your own device (BYOD)** is a business policy that permits, and in some cases encourages, employees to use their own mobile devices (smartphones, tablets, or laptops) to access company computing resources and applications, including email, corporate databases, the corporate intranet, and the Internet.
2. A **BYOD** policy raises potential security issues as such devices are also used for personal activities that expose the devices to malware (malicious software) much more frequently than devices used strictly for business purposes**.**

Increased Reliance on Commercial Software with Known Vulnerabilities

1. An exploit is an attack on an information system that takes advantage of particular system vulnerabilities. Once the system vulnerability is discovered software developers create and issue a patch to eliminate the problem. Any delay in installing a patch exposes computer systems to a potential security breach.

2. IT professionals often face the ethical dilemma of balancing the need to patch systems as soon as a patch is available and avoiding unnecessary interruptions to critical business workflows when systems are patched and restarted.
3. Zero-day attacks are attacks that take place before the security community or appropriate software developers know about the vulnerability or are able to repair it. To learn more about zero-day attacks, review 7 Lessons: Surviving A Zero-Day Attack (http://www.informationweek.com/news/security/attacks/231601692).

B. Types of Exploits

1. Common types of computer attacks include viruses, worms, Trojan horses, spam, distributed denial-of-service (DDoS), rootkits, phishing, spear-phishing, smishing, and vishing.

Viruses

1. The term computer virus has become synonymous with many types of malicious code. But, a **virus** is a piece of programming code usually disguised as something else, which causes a computer to behave in an unexpected and usually undesirable manner.
2. A true virus does not spread itself from one computer to another. A virus is spread to other machines when a computer user opens an infected email attachment, downloads an infected program, or visits infected Web sites. In other words, viruses spread by the action of the "infected" computer user.

Worms

1. **A worm** is a harmful program that resides in the active memory of a computer and duplicates itself. Unlike a computer virus, a worm does not require users to spread infected files to other users.
2. The negative impact of a worm attack on an organization's computers can be considerable—lost data and programs, lost productivity due to workers being unable to use their computers, additional lost productivity as workers attempt to recover data and programs, and lots of effort for IT workers to clean up the mess and restore everything to as close to normal as possible.

Trojan Horses

1. A **Trojan horse** is a program that a hacker secretly installs on a computer by hiding malicious code inside a seemingly harmless program.
2. A **Trojan horse** can be delivered as an email attachment, downloaded from a Web site, or contracted via a removable media device such as a CD/DVD or USB memory stick. Once an unsuspecting user executes the program that hosts the Trojan horse, the malicious payload is automatically launched as well—with no telltale signs. Common host programs include screen savers, greeting card systems, and games.

3. A **logic bomb** is a type of Trojan horse that executes under specific conditions, such as a change in a particular file, or a particular combination of keystrokes.

Spam

1. The term **spam** describes the abuse of email systems to send unsolicited email to large numbers of people.
2. The cost of creating an email campaign for a product or service is several hundred to a few thousand dollars, compared with tens of thousands of dollars for direct-mail campaigns.
3. Spam forces unwanted and often objectionable material into email boxes, detracts from the ability of recipients to communicate effectively due to full mailboxes and relevant emails being hidden among many unsolicited messages, and costs Internet users and service providers millions of dollars annually.
4. The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** which went into effect in January 2004. The act legalizes spamming, provided the messages meet a few basic requirements—spammers cannot disguise their identity by using a false return address, the email must include a label specifying that it is an ad or a solicitation, and the email must include a way for recipients to indicate that they do not want future mass mailings.

Distributed Denial-of-Service (DDoS) Attacks

1. A **distributed denial-of-service (DDoS) attack** does not involve infiltration of the targeted system. Instead, it keeps the target so busy responding to a stream of automated requests that legitimate users cannot get in—the Internet equivalent of dialing a telephone number repeatedly so that all other callers hear a busy signal.
2. The term botnet refers to a large group of computers controlled from one or more remote locations by hackers, without the knowledge or consent of their owners. Hackers often take advantage of the collective processing capacity of botnets when launching a distributed denial-of-service attack.
3. Based on a command by the attacker or at a preset time, the botnet computers called **zombies** go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
4. The target computers are so overwhelmed by requests for service that legitimate users are unable to "get through" to the target computer.

Rootkits

1. **A rootkit** is a set of programs that enables its user to gain administrator level access to a computer without the end user's consent or knowledge.
2. Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
3. Some symptoms of a rootkit infection include:
    a. Computer locking up or failing to respond to input from the keyboard or mouse.
    b. Screen saver changes without any user action.

    c. Computer taskbar disappearing without user action.
    d. Network based activities functioning extremely slowly.
3. When it is determined that a computer has been infected with a rootkit, there is little to do but reformat the disk; reinstall the operating system and all applications; and reconfigure the user's settings, such as mapped drives.

Phishing

1. **Phishing** is the act of fraudulently using email to try to get the recipient to reveal personal data.
2. **Spear-phishing** is variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees. The phony emails are designed to look like they came from high-level executives within the organization.

Smishing and Vishing

1. **Smishing** is a variation of phishing in which victims receive a legitimate-looking SMS text message on their phone telling them to call a specific phone number or to log on to a Web site.
2. **Vishing** is a variation of phishing in which victims receive a voicemail telling them to call a specific phone number or log on to access a specific Web site.

C. Types of Perpetrators

1. People who launch these kinds of computer attacks include thrill seekers wanting a challenge, common criminals looking for financial gain, industrial spies trying to gain a competitive advantage, and terrorists seeking to cause destruction to further their cause.
2. Each type of perpetrator has different objectives and access to varying resources. Each type of perpetrator has a different level of risk appetite for accomplishing his or her objective.
3. Common profiles of likely attackers include hackers, crackers, malicious insiders, industrial spies, cybercriminals, hacktivists, and cyberterrorists.

Hackers and Crackers

1. **Hackers** test the limitations of information systems out of intellectual curiosity—to see whether they can gain access and how far they can go.
2. Although a hacker might be motivated by curiosity, their actions are not harmless and even unskilled hackers can damage a system.
3. Some hackers a smart and talented, but many are technically inept. Hackers with better skills refer to the technically inept hackers as **lamers** or **script kiddies**.

Malicious Insiders

1. **Malicious insiders** are an ever-present and extremely dangerous adversary.
2. The fraud that occurs within an organization is usually due to weaknesses in its internal control procedures. As a result, many frauds are discovered by chance and by outsiders—via tips, through resolving payment issues with contractors or

suppliers, or during a change of management—rather than through control procedures.

3. Such frauds usually involve some form of **collusion** or cooperation, between an employee and a person outside of the organization.
4. Insiders are not necessarily employees; they can also be consultants and contractors. The risk tolerance of insiders depends on whether they are motivated by financial gain, revenge on their employers, or publicity.
5. Although malicious insiders may be difficult to detect, unlike hackers, once they are detected they can be held accountable, whereas with outside hackers it can be difficult to trace the attack back to the hacker.

Industrial Spies

1. **Industrial spies** use illegal means to obtain trade secrets from competitors. In the United States, trade secrets are protected by the Economic Espionage Act of 1996, which makes it a federal crime to use a trade secret for one's own benefit or another's benefit. Trade secrets are often stolen by insiders, such as disgruntled employees and former employees.
2. Competitive intelligence is legally obtained information gathered using sources available to the public; used to help a company gain an advantage over its rivals.
3. Industrial espionage involves using illegal means to obtain information that is not available to the public.

Cybercriminals

1. Cybercriminals are motivated by the potential for monetary gain and hack into computers to steal, often by transferring money from one account to another to another—leaving a hopelessly complicated trail for law enforcement officers to follow. The use of stolen credit card information is a favorite ploy of computer criminals.
2. The term **data breach** refers to the unintended release of sensitive data or the access of sensitive data by unauthorized individuals.
3. To reduce the potential for online credit card fraud, most e-commerce Web sites use some form of encryption technology to protect information as it comes in from the consumer.
4. Some debit or credit card issuers have adopted smart card technology to mitigate credit card fraud. A Smart card is a credit card that contains a memory chip that is updated with encrypted data every time the card is used.

Hacktivists and Cyberterrorists

1. The term **hacktivism**, a combination of the words *hacking* and *activism*, is used to describe hacking that achieves a political or social goal.
2. The term **cyberterrorist** is used to describe a hacker that intimidates or coerces a government or organization to advance a political or social objective by launching computer-based attacks against other computers.

D. Federal Laws for Prosecuting Computer Attacks

1. Over the years, several laws have been enacted to help prosecute those responsible for computer related crime.
    a. The USA Patriot Act defines cyberterrorism and associated penalties.
    b. The Identity Theft and Assumption Deterrence Act created a federal crime for identity theft, with penalties up to 15 years imprisonment and a maximum fine of $250,000.
    c. The Fraud and Related Activity in Connection with Access Devices Statutes addresses false claims regarding unauthorized use of credit cards.
    d. The Computer Fraud and Abuse Act address fraud and related activities in association with computers. Such activities include accessing a computer without permission or exceeding authorized access.
    e. The Stored Wire and Electronic Communications and Transactional Records Access Statutes proscribe unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage.

II. Implementing Trustworthy Computing

1. **Trustworthy computing** is a method of computing that delivers secure, private, and reliable computing experiences based on sound business practices—which is what organizations worldwide are demanding today.
2. The security of any system or network is a combination of technology, policy, and people and requires a wide range of activities to be effective. As the Committee on Improving Cybersecurity Research in the United States wrote in a report for the National Academy of Sciences, "Society ultimately expects computer systems to be trustworthy—that is, that they do what is required and expected of them despite environmental disruption, human user and operator errors, and attacks by hostile parties, and that they not do other things."
3. A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating end users about the risks involved and the actions they must take to prevent a security incident.

A. Risk Assessment

1. **Risk assessment** is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats. Such threats can prevent an organization from meeting its key business objectives.
2. The steps involved in a general security risk assessment process usually include:
    a. Identifying the set of IT assets about which the organization is most concerned.
    b. Identifying the risks or threats that could affect the identified assets.

c. Assessing the likelihood of each potential threat.
d. Determining the impact of each threat occurring.
e. Determining how each threat can be mitigated.
f. Assessing the feasibility of implementing the mitigation options.
g. Performing a cost-benefit analysis to ensure that mitigation efforts are cost effective. The concept of **reasonable assurance** 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.
h. Making the decision to implement or not implement a particular countermeasure.

3. A completed risk assessment identifies the most dangerous threats to a company and helps focus security efforts on the areas of highest payoff.

B. Establishing a Security Policy

1. A **security policy** defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements. A good security policy delineates responsibilities and the behavior expected of members of the organization.
2. The SANS (SysAdmin, Audit, Network, Security) Institute offers a number of security-related policy templates that can help an organization to quickly develop effective security policies. For more information on SANS institute's policy statements, review Information Security Policy Templates (http://www.sans.org/security-resources/policies).
3. The use of email attachments is a critical security issue that should be addressed in every organization's security policy. Sophisticated attackers may be able to penetrate a network via email attachments, regardless of the existence of a firewall and other security measures.

C. Educating Employees and Contract Workers

1. An ongoing security problem for companies is creating and enhancing user awareness of security policies.
2. Employees and contract workers must be educated about the importance of security so that they will be motivated to understand and follow the security policies.

D. Prevention

1. No organization can ever be completely secure from attack.
2. The key is to implement a layered security solution to make computer break-ins so difficult that an attacker eventually gives up. The layers of protective measures typically include the following:

Installing a Corporate Firewall

1. A firewall stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy.
2. The installation of a firewall can lead to another serious security issue—complacency. For example, a firewall cannot prevent a worm from entering the network as an email attachment. Most firewalls are configured to allow email and benign-looking attachments to reach their intended recipient.

Implementing Intrusion Detection Systems

1. **An intrusion detection system (IDS)** is software and/or hardware that monitors systems, network resources and activities, and notifies the proper authority when it identifies possible intrusions.
2. Examples included unusual traffic at off hours or traffic directed to unusual target hosts such as hosts in foreign countries.

Installing Antivirus Software on Personal Computers

1. Antivirus software should be installed on each user's personal computer and on all servers to scan the computer's memory and disk drives regularly for viruses.
2. Antivirus software scans for a virus signature. A virus signature is a specific sequence of bytes that is indicative of a virus.
3. Virus detection is based on a rule-based approach that looks for definitions of known viruses. As new viruses are written, the virus detection software must be updated with the new definitions in order to be effective.
4. The **United States Computer Emergency Readiness Team (US-CERT**) is a partnership between the Department of Homeland Security and the public and private sectors—established in 2003 to protect the nation's Internet infrastructure against cyberattacks.

Implementing Safeguards against Attacks by Malicious Insiders

1. User accounts that remain active after employees leave a company are a potential security risk.
2. The prompt deletion of computer accounts, login IDs, and passwords of departing employees and contractors reduces the threat of attacks.
3. An important safeguard is to create roles and user accounts so that users have the authority to perform their responsibilities and nothing more.

Defending Against Cyberterrorism

1. In the face of increasing risks of cyberterrorism, organizations need to be aware of the resources available to help them combat this serious threat. The **Department of Homeland Security (DHS)** leads the federal government's efforts in "securing civilian government computer systems, and works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems."
2. The Protected Critical Infrastructure Information Program encourages private industry to share confidential information about the nation's critical infrastructure

with the DHS under the assurance that the information will be protected from public disclosure.

Addressing the Most Critical Internet Security Threats

1. US-CERT regularly updates a summary of the most frequent, high-impact vulnerabilities being reported to them.
2. For more information, review US-CERT current summary (www.us-cert.gov/current)

Conducting Periodic IT Security Audits

1. A **security audit** evaluates whether an organization has a well-considered security policy in place and if it is being followed.
2. A thorough security audit should test system safeguards to ensure that they are operating as intended. Such tests might include trying the default system passwords that are active when software is first received from the vendor.
3. It's also good practice to perform a periodic penetration test throughout the network. This entails assigning individuals to try to break through the security measures and identify vulnerabilities that still need to be addressed.

E. Detection

1. Even when preventive measures are implemented, no organization is completely secure from a determined attack. Thus, organizations should implement detection systems to catch intruders in the act.

F. Response

1. Organizations should be prepared for the worst—a successful attack that defeats all or some of a system's defenses and damages data and information systems.
2. In a security incident, the primary goal must be to regain control and limit damage, not to attempt to monitor or catch an intruder.

Incident Notification

1. A key element of any response plan is to define who to notify and who not to notify. Questions to cover include the following:
   a. Within the company, who needs to be notified, and what information does each person need to have?
   b. Under what conditions should the company contact major customers and suppliers? How does the company inform them of a disruption in business without unnecessarily alarming them?
   c. When should local authorities or the FBI be contacted?

Protection of Evidence and Activity Logs

1. An organization should document all details of a security incident as it works to resolve the incident.
2. Documentation captures valuable evidence for a future prosecution and provides data to help during the incident eradication and follow-up phases.

Incident Containment

1. A security incident often requires acting quickly to contain an attack.
2. The security incident response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network.

Eradication

1. Before the IT security group begins the eradication effort, it must collect and log all possible criminal evidence from the system, and then verify that all backups are current, complete, and free of any virus.

Incident Follow-up

1. A review should be conducted after an incident to determine exactly what happened and to evaluate how the organization responded. One approach is to write a formal incident report that includes a detailed chronology of events and the impact of the incident.
2. Creating a detailed chronology of all events will also document the incident for later prosecution.
3. The potential for negative publicity must also be considered. Discussing security attacks through public trials and the associated publicity has not only enormous potential costs in public relations but real monetary costs as well.

Computer Forensics

1. **Computer forensics** is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.
2. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation.
3. Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law. In addition, extensive training and certification increases the stature of a computer forensics investigator in a court of law.
4. A computer forensics investigator must be knowledgeable about the various laws that apply to the gathering of criminal evidence, for example, the Fourth Amendment to the United States Constitution.

IT and Ethics: 3

Overview

The assigned reading material and lecture notes for this week help students understand the right to privacy, and presents an overview of developments in information technology that could impact this right. The material also addresses a number of ethical issues related to gathering data about people.

Objectives

After reviewing the assigned reading material and lecture notes students should be able to:

1. Describe the right of privacy, and articulate the basis for protecting personal privacy under the law.
2. List some of the laws that provide protection for the privacy of personal data, and identify any associated ethical issues.
3. Describe the various strategies for consumer profiling, and identify any associated ethical issues.
4. Describe the capabilities of advanced surveillance technologies, and identify any associated ethical issues.

Lecture Notes

I. Privacy Protection and the Law

1. Information about people is gathered, stored, analyzed, and reported because organizations can use it to make better decisions. Some of these decisions, including whether or not to hire a job candidate, approve a loan, or offer a scholarship, can profoundly affect people's lives. In addition, the global marketplace and intensified competition have increased the importance of knowing consumers' purchasing habits and financial condition.
2. After the United States Constitution went into effect in 1789, several amendments were proposed that would spell out additional rights of individuals; ten of these proposed amendments were ultimately ratified and became known as the **Bill of Rights**.
3. The concept of privacy is protected by the Bill of Rights. For example, the Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

4. In addition to protection from government intrusion, people want and need privacy protection from private industry. Few laws provide such protection, and most people assume that they have greater privacy rights than the law actually provides.

A. Information Privacy

1. A broad definition of the **right to privacy** is "the right to be left alone—the most comprehensive of rights, and the right most valued by a free people."
2. **Information privacy** is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).

B. Privacy Laws, Applications, and Court Rulings

1. A number of legislative acts have been implemented over time to address invasion of privacy by the government with little or no restrictions for private industry.
2. The next material addresses financial data, health information, children's personal data, electronic surveillance, fair information practices, and access to government records.

Financial Data

1. To access many of the financial products and services, individuals must use a personal logon name, password, account number, or PIN. The inadvertent loss or disclosure of this personal financial data carries a high risk of loss of privacy and potential financial loss.

2. The **Fair Credit Reporting Act** (1970) regulates the operations of credit-reporting bureaus, including how they collect, store, and use credit information.

3. The **Right to Financial Privacy Act** (1978) protects the records of financial institution customers from unauthorized scrutiny by the federal government.
   a. Prior to passage of this act, financial institution customers were not informed if their personal records were being turned over for review by a government authority, nor could customers challenge government access to their records.
   b. However, the Right to Financial Privacy Act only governs disclosures to the federal government; it does not cover disclosures to private businesses or state and local governments.

4. **The Gramm-Leach-Bliley Act (GLBA**), also known as the Financial Services Modernization Act of 1999, was a bank deregulation law that repealed a Depression-era law known as Glass-Steagall.
   a. Glass–Steagall prohibited any one institution from offering investment, commercial banking, and insurance services; individual companies were only

allowed to offer one of those types of financial service products. GLBA enabled such entities to merge.

5. The **Fair and Accurate Credit Transactions Act** was passed in 2003 as an amendment to the Fair Credit Reporting Act, and it allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies (Equifax, Experian, and TransUnion).

Health Information

1. The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread. Individuals are rightly concerned about the erosion of privacy of data concerning their health. The primary law addressing these issues is the Health Insurance Portability and Accountability Act (HIPAA).

2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was designed to improve the portability and continuity of health insurance coverage; to reduce fraud, waste, and abuse in health insurance and healthcare delivery; and to simplify the administration of health insurance.

3. Under the HIPAA provisions, healthcare providers must obtain written consent from patients prior to disclosing any information in their medical records.

4. The **American Recovery and Reinvestment Act**, passed in 2009, is a wide-ranging act that authorized $787 billion in spending and tax cuts over a 10-year period. Title XIII, Subtitle D of this act—also known as the Health Information Technology for Economic and Clinical Health Act, or **HITECH**—included strong privacy provisions for electronic health records, including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients.

Children's Personal Data

1. Only a few laws have been implemented to protect children online, and most of these have been ruled unconstitutional under the First Amendment and its protection of freedom of expression.

2. The **Family Educational Rights and Privacy Act (FERPA)** is a federal law that assigns certain rights to parents regarding their children's educational records. These rights transfer to the student once the student reaches the age of 18 or if he or she attends a school beyond the high school level.

3. The **Children's Online Privacy Protection Act (COPPA)** requires Web sites that cater to children to offer comprehensive privacy policies, notify parents or guardians about its data collection practices, and receive parental consent before collecting any personal information from children under 13 years of age.

Electronic Surveillance

1. The **Communications Act** of 1934 established the Federal Communications Commission and gave it responsibility for regulating all non-federal-government use of radio and television broadcasting and all interstate telecommunications as well as all international communications that originate or terminate in the United States.

2. The **Foreign Intelligence Surveillance Act (FISA)** (1978) describes procedures for the electronic surveillance and collection of foreign intelligence information in communications between foreign powers and the agents of foreign powers.
   a. **Foreign intelligence** is information relating to the capabilities, intentions, or activities of foreign governments or agents of foreign governments or foreign organizations.
   b. The act also created the **Foreign Intelligence Surveillance Act (FISA) court**, which meets in secret to hear applications for orders approving electronic surveillance anywhere within the United States.

3. **Title III of the Omnibus Crime Control and Safe Streets Act**, also known as the **Wiretap Act,** regulates the interception of wire (telephone) and oral communications. The Act allows state and federal law enforcement officials to use wiretapping and electronic eavesdropping, but only under strict limitations.

4. The **Electronic Communications Privacy Act (ECPA)** protects communications while in transfer from sender to receiver; protects communications held in electronic storage; and prohibits devices from recording dialing, routing, addressing, and signaling information without a search warrant.
   a. Under Title II of ECPA (also called the Stored Communications Act), the FBI director or someone acting on his behalf may issue a **National Security Letter (NSL)** to an Internet service provider to provide various data and records about a service subscriber.
   b. A National Security Letter compels holders of personal records to turn them over to the government; NSLs are not subject to judicial review or oversight.
   c. The ECPA also establishes a requirement for court-approved law enforcement uses of pen registers or a trap and trace devices.
      i. A pen register is a device that records electronic impulses to identify the numbers dialed for outgoing calls.
      ii. A trap and trace is a device that records the originating number of incoming calls for a particular phone number.

5. The **Communications Assistance for Law Enforcement Act** (CALEA) (1994) amended both the Wiretap Act and ECPA; it required the telecommunications industry to build tools into its products that federal investigators could use to eavesdrop on conversations and intercept electronic communications.
   a. CALEA covered emerging technologies such as wireless modems, radio-based electronic mail and cellular data networks.

6. The **USA PATRIOT Act** gave sweeping new powers both to domestic law enforcement and U.S. international intelligence agencies, including increasing the ability of law enforcement agencies to search telephone, email, medical, financial, and other records.

Fair Information Practices

1. The term **"fair information practices"** refers to a set of guidelines that govern the collection and use of personal data. The overall goal of such guidelines is to stop the unlawful storage of personal data, eliminate the storage of inaccurate personal data, and prevent the abuse or unauthorized disclosure of such data.
    a. For some organizations and countries, a key issue is the flow of personal data across national boundaries (**transborder data flow)**.
    b. The Organisation for Economic Co-operation and Development (OECD), an international organization established its fair information practices in 1980. The OECD's guidelines are often used as a model of ethical treatment of consumer data.

2. The **European Union Data Protection Directive** (officially known as Directive 95/46/EC) requires any company doing business within the borders of the countries comprising the European Union to implement a set of privacy directives on the fair and appropriate use of information.
    a. Directive95/46/EC simply outlined recommendations and had no real enforcement requirements.
    b. In 2012, the European Commission proposed a new **European Data Protection Regulation** to replace the 1995 Data Protection Directive.

Access to Government Records

1. The **Freedom of Information Act (FOIA)**, passed in 1966 and amended in 1974, grants citizens the right to access certain information and records of federal, state, and local governments upon request.
    a. FOIA is a powerful tool that enables journalists and the public to acquire information that the government is reluctant to release.
    b. There are two basic requirements for filing a FOIA request: (1) the request must not require wide-ranging, unreasonable, or burdensome searches for records, and (2) the request must be made according to agency procedural regulations published in the Federal Register.
    c. Exemptions to the FOIA bar disclosure of information that could compromise national security or interfere with an active law enforcement investigation.
    d. Another exemption prevents disclosure of records if it would invade someone's privacy.

2. The **Privacy Act** of 1974 establishes a code of fair information practices that sets rules for the collection, maintenance, use, and dissemination of personal data that is kept in systems of records by federal agencies. It also prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system.

   a. Under the Privacy Act, any agency that maintains such a system must publicly describe both the kinds of information in it and the manner in which the information will be used.

II. Key Privacy and Anonymity Issues

1. The next material discusses current and important privacy issues, including data breaches, electronic discovery, consumer profiling, workplace monitoring, and advanced surveillance technology.

A. Data Breaches

1. An alarming number of identity theft incidents can be traced back to data breaches involving large databases of personal information.

2. The cost to an organization that suffers a data breach can be quite high—by some estimates nearly $200 for each record lost.

B. Electronic Discovery

1. Discovery is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents.

2. **Electronic discovery (e-discovery)** is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings.

3. **Electronically stored information (ESI)** includes any form of digital information, including emails, drawings, graphs, Web pages, photographs, word-processing files, sound recordings, and databases stored on any form of electronic storage device, including hard drives, CDs, and flash drives.

4. Traditional software development firms as well as legal organizations have recognized the growing need for improved processes to speed up and reduce the costs associated with e-discovery. As a result, dozens of companies offer e-discovery software.

5. E-discovery raises many ethical issues:
   a. Should an organization ever attempt to destroy or conceal incriminating evidence that could otherwise be revealed during discovery?
   b. To what degree must an organization be proactive and thorough in providing evidence sought through the discovery process?

c. Should an organization attempt to bury incriminating evidence in a mountain of trivial, routine ESI?

C. Consumer Profiling

1. Many organizations obtain information about Web surfers through the use of cookies. Cookies are text files that can be downloaded to the hard drives of users who visit a Web site, so that the Web site is able to identify visitors on subsequent visits.

2. Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data, and then provide this data to companies to tailor their products and services to individual consumer preferences.

3. Concerns about how this data is used may prevent potential online shoppers from making purchases.

D. Workplace Monitoring

1. Many organizations have developed policies on the use of IT in the workplace in order to protect against employee abuses that reduce worker productivity or that expose the employer to harassment lawsuits.

2. Some organizations find it necessary to record and review employee communications and activities on the job, including phone calls, email, and Web surfing. Some are even videotaping employees on the job. In addition, some companies employ random drug testing and psychological testing.

3. As the laws governing employee privacy and monitoring continue to evolve, business managers must stay informed in order to avoid enforcing outdated usage policies.

4. Organizations with global operations face an even greater challenge because the legislative bodies of other countries also debate these issues.

E. Advanced Surveillance Technology

1. Advances in information technology such as surveillance cameras and satellite-based systems that can pinpoint a person’s physical location have provided new data-gathering capabilities.

2. However, these capabilities can also diminish individual privacy and complicate the issue of how much information should be captured about people’s private lives.

3. Advocates of advanced surveillance technology argue that people have no legitimate expectation of privacy in public places and thus Fourth Amendment privacy rights do not apply, while critics argue that this technology creates new possibilities for abuse and that it does not identify people accurately.

4. The next material provides an overview of common surveillance technologies.

Camera Surveillance

1. Camera surveillance is used extensively in the United Kingdom, and a number of U.S. cities plan to expand their surveillance systems.
2. At issue is whether people have an expectation of anonymity in public places and whether anonymity is protected under the law.

Vehicle Event Data Recorders

1. A **vehicle event data recorder (EDR)** is a device that records vehicle and occupant data for a few seconds before, during, and after any vehicle crash that is severe enough to deploy the vehicle’s air bags.
2. The EDR cannot capture any data that could identify the driver of the vehicle nor can it tell if the driver was operating the vehicle under the influence of drugs or alcohol.
3. The U.S. government does not require EDRs in passenger vehicles, but most new vehicles come equipped with EDRs.

Stalking Apps

1. A stalking app can be loaded onto someone’s cell phone or smartphone within minutes, making it possible for the user to perform location tracking, record calls, view every text message or picture sent or received, and record the URLs of any Web site visited on the phone.
2. There is no law that prohibits a business from making an app whose primary purpose is to help one person track another, and anyone can purchase this software online.
3. However, it is illegal to install the software on a phone without the phone owner’s permission.

III. Strategies for Avoiding Security Breaches

1. Protecting client collected personally identifiable information remains a top priority for any Information Manager. But, technology adoption for personal and business use has presented new challenges in protecting personally identifiable information. Moreover, ensuring compliance with data privacy laws is no easy task.

2. For a summary of security breaches from 2014, please read (http://www.networkworld.com/article/2861023/security0/worst-security-breaches-of-the-year-2014-sony-tops-the-list.html).

A. Implement Technical and Administrative Controls

1. Organizations rely on Information managers to prevent data breaches and protect confidential information.

2. To prevent data breaches, information managers should ensure that:
    a. At least one person is designated as the security and privacy official for the organization.
    b. Written security policies and procedures for proper handling of confidential information are established.
    c. Staff is properly trained on security policies and procedures.
    d. All computers and mobile devices that have the potential to access confidential information are encrypted.
    e. Access to confidential information is limited only to people with a need to access the information.
    f. An intrusion detection and prevention system (IDS/IPS) is implemented.
    g. Web filtering tools are deployed to prevent access to malicious or compromised sites.
    h. Scheduled vulnerability assessments are regularly conducted.
    i. All systems and operating systems are promptly patched.
    j. Data loss prevention (DLP) system is setup to block confidential data from leaving the organization's network.
    k. A written and practiced breach response plan is established.
    l. A written backup, disaster recovery, and business continuity plan is established.

B. Establish Strategic Contracts with Forensic Experts

1. Computer forensics enables forensics analysts to extract information pertinent to an investigation in cases where there is reason to suspect unauthorized disclosure of confidential information through malicious code or human error.

2. The wealth of information that can be gleaned from computer forensics is also valuable in conducting a breach analysis.

3. Forensic analysis also enables analysts to determine:
    a. If any external entity is illicitly connecting and communicating with the organization's computers.
    b. If there is unauthorized data egress from the organization's computer systems to an external command and control system managed by bad actors.

4. Considerations for engaging external forensic organizations include ensuring that:
    a. Forensics entities have local representatives that can get to the computer systems promptly when needed.

b. Forensics entities are experts at analyzing the type of systems in use at the organization, for example, mobile devices, windows-based systems, Macintosh systems, or database systems.
c. Forensics entities have experience analyzing malware, including the ability to reverse engineer different types of malware.
d. Forensics entities have a reasonable turnaround time for forensic investigations.

IT and Ethics: 4

Overview

The assigned reading material and lecture notes for this week provides an overview of intellectual property issues, including copyrights, patents and trade secret laws. The material discusses cross-licensing and software patents. The material also presents a discussion of plagiarism and plagiarism detection services. Ethical issues in reverse engineering are introduced, and the material ends with a discussion of competitive intelligence and cybersquatting.

Objectives

After reviewing the assigned reading material and lecture notes students should be able to:

- Describe intellectual property and identify why organizations are so concerned about protecting intellectual property.
- Review the strengths and limitations of using copyrights, patents, and trade secret laws to protect intellectual property?
- Define plagiarism, and articulate what can be done to combat it?
- Discuss reverse engineering, and identify issues associated with reverse-engineering a competitor's software program.
- Explore open source code, and articulate the fundamental premise behind its use.
- Differentiate competitive intelligence from industrial espionage, and identify how competitive intelligence is gathered.
- Define cybersquatting, and identify strategies used to protect organizations from cybersquatting.

Lecture Notes

I. What is Intellectual Property?

1. **Intellectual property** is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct and owned or created by a single person or group.

2. Intellectual property is protected through copyright, patent, and trade secret laws.
    a. Copyright law protects authored works, such as art, books, film, and music.
    b. Patent law protects inventions.
    c. Trade secret law helps safeguard information that is critical to an organization's success.

II. Copyrights

1. Copyright and patent protection was established through the U.S. Constitution, Article I, section 8, clause 8, which specifies that Congress shall have the power "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Rights to their respective Writings and Discoveries."

2. A **copyright** grants the creators of original works the exclusive right to distribute, display, perform, or reproduce the work in copies, or to prepare derivative work.

3. **Copyright infringement** is a violation of the rights secured by the owner of a copyright, which occurs when someone copies a substantial and material part of another's copyrighted work without permission.

A. Copyright Term

1. Copyright law guarantees developers the rights to their works for a certain amount of time. Since 1960, the term of copyright has been extended 11 times from its original limit of 28 years.
2. The current copyright term is life of the author plus 70 years.

B. Eligible Works

1. The types of work that can be copyrighted include architecture, art, audiovisual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works, as described in Title 17 of the U.S. Code.
2. To be eligible for copyright, a work must be fall within one of the identified categories, and it must be original.
3. An idea cannot be copyrighted but the expression of an idea can be copyrighted.

C. Fair Use Doctrine

1. The **fair use doctrine** allows portions of copyrighted materials to be used without permission under certain circumstances.
2. Courts consider the following four factors when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty:
   a. The purpose and character of the use (non-commercial versus commercial use).
   b. The nature of the copyrighted work.
   c. The portion of the copyrighted work used in relation to the work as a whole.
   d. The effect of the use on the value of the copyrighted work.

D. Software Copyright Protection

1. The use of copyrights to protect computer software raises many complicated issues of interpretation with regards to allegations of copyright infringement.
2. For example, to prove infringement, software copyright holders must show a striking resemblance between their software and another developer's new software that could be explained only by copying. This is often difficult because two developers can conceivably develop separate but nearly identical programs to perform simple tasks.

E. The Prioritizing Resources and Organization for Intellectual Property Act

1. The **Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008** increased trademark and copyright enforcement and substantially increased penalties for infringement.
2. The law also established the Office of the United States Intellectual Property Enforcement Representative within the U.S. Department of Justice.

F. General Agreement on Tariffs and Trade (GATT)

1. The GATT is a trade agreement between 117 countries and it created the World Trade Organization (WTO) to enforce its policies.
2. GATT includes a section covering copyrights called the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

G. The World Intellectual Property Organization (WIPO) Copyright Treaty

1. The WIPO Copyright Treaty, adopted in 1996, provides additional copyright protections to address electronic media.
2. The treaty ensures that computer programs are protected as literary works and that the arrangement and selection of material in databases is also protected.

H. The Digital Millennium Copyright Act (1998)

1. The **Digital Millennium Copyright Act (DMCA)** was signed into law in 1998 and implements two 1996 WIPO treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.
2. The act is divided into five sections, Titles I–V.
    a. Title II provides "safe harbors" for ISPs whose customers/subscribers might be breaking copyright laws by downloading, posting, storing, or sending copyrighted material via its services.

3. There are two competing views about the DMCA
    a. Some people view the DMCA as a boon to the growth of the Internet and its use as a conduit for innovation and freedom of expression. Without the safe harbors that the DMCA provides, the risk of copyright liability would be so great as to seriously discourage ISPs from hosting and transmitting user-generated content.
    b. Other people view the DMCA as extending too much power to copyright holders that it restricts the flow of information.

III. Patents

1. A **patent** is a grant of a property right issued by the United States Patent and Trademark Office (USPTO) to an inventor.
2. A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators.
3. Unlike a copyright, a patent prevents independent creation as well as copying.
4. To be a patentable, an invention has to be new (*not found in prior art*), useful, and not obvious to a person having ordinary skill in the art (PHOSITA). In addition the patent application must include a written description of the invention and the description must enable a PHOSITA to make and use the invention without undue experimentation.
5. An invention is new only if it cannot be found in prior art. **Prior art** is the existing body of knowledge that is available to a person of ordinary skill in the art.
6. Abstract ideas, laws of nature, and natural phenomena cannot be patented.
7. **Patent infringement** is a violation of the rights secured by the owner of a patent, which occurs when someone makes unauthorized use of another's patent. Patent infringement can be direct or indirect infringement.
8. To learn more about patents, review General Information Concerning Patents (http://www.uspto.gov/patents-getting-started/general-information-concerning-patents).

A. Leahy-Smith America Invents Act (2011)

1. The **Leahy-Smith America Invents Act of 2011** represents a major change in U.S. patent law.
2. Under this law, the U.S. patent system changed from a "first-to-invent" to a "first-inventor-to-file" system effective March 16, 2013.
3. The America Invents Act also expanded the definition of prior art used to determine the novelty of an invention and whether it can be patented.

B. Software Patents

1. Prior to 1981, courts regularly turned down requests to patent software, giving the impression that software could only be copyrighted but not patented.
2. However, in the 1981 *Diamond v. Diehr* case, the Supreme Court granted a patent

to Diehr, who had developed a process control computer and sensors to monitor the temperature inside a rubber mold. Based on this ruling, the courts have slowly broadened the scope of patent protection for software-related inventions.

3. Some experts believe that too many software patents are being granted, and that this inhibits new software development as evidenced by the number software patent infringement lawsuits between large software organizations such as Oracle, Google, and Apple.

C. Cross-Licensing Agreements

1. Many large software companies have cross-licensing agreements in which each party agrees not to sue the other over patent infringements.
2. Major IT firms usually have little interest in cross-licensing with smaller firms, so small businesses often have no choice but to license patents if they use them.

IV. Trade Secrets

1. A trade secret is defined as business information that represents something of economic value, has required effort or cost to develop, has some degree of uniqueness or novelty, is generally unknown to the public, and is kept confidential.
2. Trade secrets have the following key advantages over patents and copyrights:
    a. There is no time limitation on the protection of trade secrets.
    b. There is no need to file an application for trade secret protection.

A. Trade Secret Laws

1. Trade secret protection laws vary greatly from country to country. For example, there is no legal protection for trade secrets in the Philippines.
2. It is therefore important for information managers to understand the legal protections available especially when doing business in foreign countries.

Uniform Trade Secrets Act (UTSA)

1. The Uniform Trade Secrets Act (UTSA) was drafted in the 1970s to bring uniformity to all the United States in the area of trade secret law.
2. The first state to enact the UTSA was Minnesota in 1981, followed by 39 more states and the District of Columbia.

The Economic Espionage Act (EEA) (1996)

1. The **Economic Espionage Act (EEA) of 1996** imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets.
2. Before the EEA, there was no specific criminal statute to help pursue economic espionage; the FBI was investigating nearly 800 such cases in 23 countries when the EEA was enacted.

B. Employees and Trade Secrets

1. Employees are the greatest threat to the loss of company trade secrets—they might accidentally disclose trade secrets or steal them for monetary gain.
2. Organizations must educate employees about the importance of maintaining the secrecy of corporate information.
3. Organizations often try to prohibit departing employees from revealing secrets by adding nondisclosure clauses to employment contracts. A typical **nondisclosure clause** for software companies is a clause in an employment contract that states that an employee cannot take copies of computer programs or reveal the details of software owned by the firm, even when they leave.
4. Employers can also use noncompete agreements to protect intellectual property from being used by competitors when key employees leave. A **noncompete agreement** prohibits an employee from working for any competitor for a period of time, often one to two years.
5. Judicial treatment of noncompetent agreements varies from state to state. Thus, Information managers should be aware of how courts in their jurisdiction treat noncompete agreements.

V. Key Intellectual Property Issues

1. The next material discusses legal and ethics issues that apply to intellectual property and information technology, including plagiarism, reverse engineering, open source code, competitive intelligence, trademark infringement, and cybersquatting.

A. Plagiarism

1. **Plagiarism** is the act of stealing someone's ideas or words and passing them off as one's own.
2. The explosion of electronic content and the growth of the Internet have made it easy to cut and paste paragraphs into term papers and other documents without proper citation or quotation marks.
3. However, plagiarism detection services and software allow teachers, corporations, law firms, and publishers to check for matching text in different documents as a means of identifying potential plagiarism.
4. For an online resource for combating plagiarism, review, What is plagiarism? (http://www.plagiarism.org)

B. Reverse Engineering

1. **Reverse engineering** is the process of taking something apart in order to understand it, build a copy of it, or improve it.

2. **Reverse engineering** was originally applied to computer hardware but is now commonly applied to software as well.
3. A frequent use of reverse engineering for software is to modify an application that ran on one vendor's database so that it can run on another's (for example, from Access to Oracle).
4. Software license agreements increasingly forbid reverse engineering.
5. As a result of the increased legislation affecting reverse engineering, some software developers are moving their reverse-engineering projects offshore to avoid U.S. rules.
6. Reverse engineering introduces several ethical issues for consideration.
   a. Some argue that its use is fair if it enables a company to create software that interoperates with another company's software or hardware and provides a useful function.
   b. Others argue that it can uncover software designs that someone else developed at great research and development cost thereby robbing the creator of future earnings and consequently reducing the business incentive for software development.

C. Open Source Code

1. **Open source code** is any program whose source code is made available for use or modification, as users or other developers see fit.
2. The basic premise behind open source code is that when many programmers can read, redistribute, and modify a program's code, the software improves.
3. To learn more about open source code, review What is free software? (http://www.gnu.org/philosophy/free-sw.html).

D. Competitive Intelligence

1. Competitive intelligence is legally obtained information that is gathered to help a company gain an advantage over its rivals.
2. An effective competitive intelligence operation requires the continual gathering, analysis, and evaluation of data with controlled dissemination of useful information to decision makers.
3. Competitive intelligence is often integrated into a company's strategic plan and decision making.
4. **Industrial espionage** is the gathering of information not available to the public through illegal means.
5. In the United States, industrial espionage is a serious crime that carries heavy penalties.
6. Competitive intelligence analysts must avoid unethical or illegal actions, such as lying, misrepresentation, theft, bribery, or eavesdropping with illegal devices when gathering data for competitive intelligence.
7. For more information on competitive intelligence, review, Proprietary Information & Competitive Intelligence (http://www.lib.utexas.edu/engin/guides/proprietary.html).

E. Trademark Infringement

1. A **trademark** is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's.
2. Consumers often cannot examine goods or services to determine their quality or source, so instead they rely on the labels attached to the products. Thus, a **trademark** is anything that enables a consumer to differentiate one company's products from another's.
3. A trademark holder has the right to prevent others from using the same mark or a confusingly similar mark on a product's label.
4. Trademark infringement lawsuits often result from alleged uses of plaintiff's trademark in a Web site or a domain name.
5. However, nominative fair use is a defense often employed by the defendant in trademark infringement cases where the defendant uses a plaintiff's mark to identify the plaintiff's products or services in conjunction with its own product or services.

F. Cybersquatting

1. A **cybersquatter** is a person or company that registers domain names for famous trademarks or company names to which they have no connection, with the hope that the trademark's owner will buy the domain name for a large sum of money.
2. The Anticybersquatting Consumer Protection Act (ACPA), enacted in 1999, allows trademark owners to challenge foreign cybersquatters who might otherwise be beyond the jurisdiction of U.S. courts.
3. The ACPA also allows trademark owners to challenge the registration of their trademark as a domain name even if the trademark owner has not created an actual Web site.
4. To learn more about cybersquatting, explore Cybersquatters Rush To Claim Brands In The New GTLD Territories (http://www.forbes.com/sites/danielfisher/2014/02/27/cybersquatters-rush-to-claim-brands-in-the-new-gtld-territories/).
5. For a slate article on cybersquatting, visit, Is Cybersquatting Against the Law? (http://www.slate.com/id/2206596/).

Reference:

Reynolds, G. W. (2014). *Ethics in information technology* (5th ed.). Boston, MA: Cengage Learning.