D333 Study Guide

Section 1

This section overviews the course layout.

Pages 1-57 (Filled in Study Guide from Resources)
Pages 58-114 (Summary of the Chapters)
Pages 115-120 (Terms)

Some stuff from the study guide and summary of chapters repeats. Some stuff is a further explanation.

Section 2

In this section, three competencies are covered across three modules. This section of the course contains Modules 1, 2, and 3, as follows:

- **Module 1: An Overview of Ethics**
- **Module 2: Ethics for IT Workers and IT Users**
- **Module 3: Cyberattacks and Cybersecurity**

Module 1	**An Overview of Ethics**

Define the following terms. (p.4)

Ethics: is a code of behavior defined by a group an individual belongs to.

Morals: a person’s standards of behavior or beliefs concerning what is and is not acceptable for them to do.

Virtue: a form of ethics that centers on human character as the focus of moral activity and pays special attention to how we develop and exercise good qualities. Virtue ethics is an approach to ethics organized around the idea of human flourishing and human excellence. It's basic assumption is that all human beings share some basic qualities of character, though we vary widely and how much we excel at those qualities and how we express them, and each of us gets better (or worse) at them according to our experiences. It further assumes that human beings are concerned with how to live the good life and that ethics is a subset of what it means to live a full and happy life.

Vice: continence has much more in common with temperance and wholeheartedness then it does with various forms of bad living, such as vice (that is, the extreme states of being that virtues avoid) or being ruled by one's appetites.

Integrity: a person who acts with integrity acts in accordance with personal code of principles.

Complete the table by identifying the legal and ethical considerations for each example. (p.6)

Ethical?	Legal?	Example

1.N	Y	Sleeping on the clock.
2.N	N	Using a business donation for personal use.
3. Y	Y	Asking for a promotion at work.
4.N	N	Drinking wine while on call at work.

Explain the meaning of the term Bathsheba syndrome. (p.8): the inability to cope with and respond to the byproducts of success. Ethical failures and leaders are a product of success, not pressure to perform. Success may cause leaders to shift focus from those things that made them successful to less important issues. Success leads to access to privileged information that may be abused.

Identify the importance of Corporate Social Responsibility. (p.11): is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.

Why is fostering corporate social responsibility and good business ethics important?

It can help companies build a positive reputation, gain customer loyalty, and avoid legal issues:

Reputation: ethical behavior and CSR practices can help companies differentiate themselves from competitors and attract stakeholders who share their values. These practices can also lead to positive word-of-mouth referrals and higher sales and market share.

Customer loyalty: consumers are increasingly aware of a business′ social and environmental impact, and more than half of the US consumers say they won't buy from companies they consider unethical. Ethical companies can cultivate trust with customers, which can lead to increased loyalty and retention.

Legal compliance: good business ethics can help companies avoid legal and regulatory problems

What is one way an organization can improve their business ethics?

Organizations can improve their business ethics in many ways, including:

- Establishing a code of conduct: a code of conduct document can establish ethical standards for the company and its employees. It can be rooted in core values like trust and integrity and should be made available to all staff in their language.
- Training employees: ethics training can- be included in corporate training programs.

Identify one way you include ethical considerations in your own decision making.

- Consider multiple perspectives: involve stakeholders and decision-making processes and consider their perspectives. For example, in business leadership, this can help leaders make more informed and ethical choices.
- Evaluate information: gather relevant information and evaluated against ethical guidelines.

Why should a business appoint a corporate ethics officer? (p. 18)

The ethics officer serves as the organization's internal control point for ethics and improprieties, allegations, complaints, and conflicts of interest and provides corporate leadership and advice on corporate governance issues.

What might a company's code of ethics look like? (p.21)

Is a set of principles and values that guide employee behavior and decision making. It can include sections on a variety of topics, such as:

- mission and values: the company's purpose and core values
- ethical standards: principles like honesty, integrity, respect, and responsibility
- policies: guidelines for how employees should conduct themselves and make decisions
- Accountability: a commitment to ethical behavior in all actions, decisions, and relationships
- reporting concerns: ways employees can report concerns or incidents, such as talking to their manager, filing a report, or using an anonymous hotline

Identify two managerial behaviors that might encourage unethical behavior from employees.

- Misusing company time
- Taking credit for others hard work
- Abusive behavior
- Data breaching

Topic: Ethical Decision-Making Process

Complete the table of a Five Step Ethical Decision-Making Process.

Name of Step	Define or explain
1.	**Identify the ethical issues**
2.	**Get the facts**
3.	**Evaluate alternative actions**
4.	**Choose an option for action and test it**
5.	**Implement your decision and reflect on the outcome**

What trends have increased the likelihood of an unethical behavior?

Unethical behavior can be caused by a number of factors, including individual characteristics, organizational environments, and trends:

- Competition: both too much and too little competition can lead to unethical behavior. When there's no competition, companies may try to eliminate potential competitors, make excessive profits, or lie to avoid audits. When there is competition, employees may compete for recognition, bonuses, and promotions, which can lead to unethical behavior.
- Information technology: the growth of the Internet and the ability to store large amounts of information has increased the risk of unethical use of information technology,
- Work environment: employees may actually unethically, if they don't see their actions causing harm, such as when the victim is far away or the damage is delayed. They may also act unethically if they feel their peers won't condemn them for their actions, or if they are afraid to speak up. Other factors that can encourage unethical behavior include pressure to succeed, unrealistic expectations, lack of training, and manager setting bad examples.

Module 2	Ethics for IT Workers and IT Users

What is the Software & Information Industry Association (SIIA) and BSA responsible for (p.46)?

SIIA provides global services in government relations, business development, corporate education and intellectual property protection to leading companies that are setting the pace for the digital age. Business Software Alliance (BSA): the trade groups that represent the world’s largest software and hardware manufacturers

Define the following terms (pp. 47- 48).

Trade secret: Trade secrets are a type of intellectual property that includes formulas, practices, processes, designs, instruments, patterns, or compilations of information that have inherent economic value because they are not generally known or readily ascertainable by others, and which the owner takes reasonable measures to keep secret.

Conflict of Interest: Occurs when an individual's personal interests – family, friendships, financial, or social factors – could compromise his or her judgment, decisions, or actions in the workplace. Government agencies take conflicts of interest so seriously that they are regulated.

Misrepresentation: any statement by words or other conduct that, under the circumstances, amounts to an assertion that is false or erroneous, i.e., not in accordance with the facts.

Breach of contract: occurs when a party to a binding agreement fails to fulfill their obligations as outlined in the contract. This can happen in both written and oral contracts.

In order to prove fraud in the court of law, what must be demonstrated (p. 49)?

1. A representation of facts
2. Its falsity
3. Its materiality
4. the representer's knowledge of its falsity or ignorance of its truth
5. the representer's intent that it should be acted upon by the person in the manner reasonably contemplated
6. the injured party's ignorance of its falsity
7. the injured party party's reliance on its truth
8. the injured party's right to rely thereon
9. the injured party's consequent and proximate injury

Identify two types of bribery (p. 51).

Active Bribery: when a party offers or pays a bribe to another party in exchange for a favor. For example, paying a public official to get a contract, license, or avoid safety or planning regulations.

Passive Bribery: when a party asks for a bribe from another party in exchange for a favor.

An organization's internal control includes:

A combination of plans, policies, procedures, and activities that help an organization achieve its goals and objectives. Internal controls can include:

- Control activities: Such as authorization, documentation, reconciliation, security, and separation of duties
- Preventative controls: Designed to stop undesirable events from happening
- Corrective controls: Put in place when errors or irregularities are found
- Detective controls: Provide evidence that an error or irregularity has occurred
- Risk assessment: The organization's process for assessing risk
- Information and communication: How information is shared within the organization
- Monitoring activities: How the organization monitors its performance against its goals

Define the following terms (p. 52).

Policies: course or principle of action adopted or proposed by a government, party, business, or individual.
Process: a series of actions or steps taken in order to achieve a particular end.
Procedure: an established or official way of doing something.
Separation of Duties (SoD): also known as segregation of duties, is an administrative control that involves assigning different tasks of a process to more than one person. The goal is to prevent fraud, errors, and other security compromises by ensuring that no one person has sole control over a transaction or process.

Identify the act makes it a crime to bribe a foreign official, a foreign party official, or candidate for foreign political office. This act applies to all US citizens and companies listed on any US stock exchange.

The Foreign Corrupt Practices Act (FCPA) of 1977, as amended, makes it illegal for certain people and entities to offer, pay, or authorize payments to foreign government officials, political parties, party officials, or candidates for foreign public office.

Explain three common exaggerations on resumes (p. 54).

changing job titles, exaggerating employment dates, lying about former employers or embellishing the duties they performed in past roles.

What relationships must an IT worker manage, and what key ethical issues can arise in each?

IT professionals can have many different relationships, including with clients, employers, suppliers, other professionals, IT users, and society at large. Ethical issues can arise in each of these relationships, including:

- IT professionals and IT users: Issues such as software piracy, inappropriate use of IT resources, and inappropriate sharing of information can arise.
- IT professionals and clients: IT professionals and clients must work together to be successful, with the client trusting the IT professional's information, recommendations, and alternatives.
- IT professionals and employers: IT professionals should set an example.

What can be done to encourage the professionalism of IT workers?

- Set clear expectations: Define realistic standards for punctuality, dress code, quality of work, customer service, and conduct.
- Communicate effectively: Listen to colleagues, subordinates, and superiors to understand business goals. Provide constructive criticism to subordinates and use policies, procedures, training, and feedback to communicate.
- Lead by example: Demonstrate professionalism yourself so employees are encouraged to follow suit.
- Recognize and reward professionalism: Reinforce desired behaviors by recognizing and rewarding them.
- Mentoring: Mentoring can be an effective way to improve professionalism at any stage of a career.
- Empathize: Showing empathy when a co-worker needs to share issues can help create a culture of compassion.
- Maintain a positive attitude: A friendly and encouraging demeanor can help you bond with co-workers, build confidence, and get noticed.
- Avoid gossip: Keep conversations professional and appropriate to set a good example and help your team focus on work.
- Be honest: Honesty and transparency can reduce tensions and conflicts among colleagues.
- Be punctual: Punctuality shows your motivation and respect for your employer's requirements.

How is an IT certification different from an IT license (p. 60-61)?

IT certifications are voluntary and show that you have met certain standards, while IT licenses are legally required to work in a specific occupation:

- IT certifications: These are non-governmental processes that show that you have the skills and knowledge to work in a specific role or occupation. They can be useful for people entering the workforce or changing careers, and can help you get a better job title, pay grade, or status. Certifications can be earned by meeting predetermined criteria, such as passing an exam or having a degree. Some certifications may be required by employers in certain fields.
- IT licenses: These are state-granted documents that give you the legal authority to practice a profession. They are often required for careers in health, public education, law, and finance. Licenses must be renewed with continuing education.

The core body of knowledge for any profession outlines agreed-upon sets of skills and abilities that all licensed professional must possess.

Topic: Software Engineering Code of Ethics and Professional Practice

Complete the table of eight principles for software engineers. Fill in the blank to identify each domain outlined in (p. 61).

Principles	Guideline
1. Public	**Shall act consistently with the public interest.**
2. Client and Employer	**Shall act in a manner that is in the best interests of their client and employer consistent with the public interest.**
3. Product	**Shall ensure that their products and related modifications meet the highest professional standards.**
4. Judgement	**Shall maintain integrity and independence in their professional judgement.**
5. Management	**Shall subscribe to and promote an ethical approach to the management of software development and maintenance.**
6. Profession	**Shall advance the integrity and reputation of the profession consistence with public interest.**
7. Colleagues	**Shall be fair to and supportive of their colleagues**
8. Self	**Shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.**

The nonprofit organization National Council of Examiners for Engineering and Surveying (NCEES) develops, administers, and scores the examinations used for engineering and surveying licensure in the United States (p. 62).

What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

Ethical Issues

- Misuse of personal data
- Spread of misinformation
- Lack of Accountability
- Liability for autonomous technology
- AI bias and Accountability

Define the following terms (p. 63).

Negligence: Negligence is the failure to act with the same level of care as a reasonable person would in similar circumstances, resulting in injury or loss. It can also refer to an action that a reasonable person would not take. Negligence can be applied to both actions and omissions. For example, if someone turns left into oncoming traffic while you are driving through a green light, that would be considered negligent.

Duty of Care: Duty of care (DoC) is a legal concept that requires people to act with reasonable care to prevent foreseeable harm to others. In information security, DoC is the requirement that organizations establish reasonable security. This requirement is included in many privacy laws and proposed bills, and is cited in litigation.

Reasonable Professional Standard: is a dynamic concept that considers the circumstances of a case to determine if a professional's actions were reasonable. It's often used in civil cases involving negligence, such as personal injury lawsuits, insurance claims, or wrongful death lawsuits.

Professional Malpractice: also known as computer malpractice, is a type of professional negligence that occurs when an IT professional fails to meet the standards of care for their profession. This can include situations where the professional represents themselves as having above average skills and expertise, and the law holds them to a higher standard.

Module 3	**Cyber Attacks and Cybersecurity**

Topic: The Threat Landscape

Define a Zero-day exploit. is a cyberattack that takes advantage of a security flaw in software, hardware, or firmware before a vendor can release a patch or fix. The term "zero-day" refers to the fact that the vendor has zero days to fix the flaw before malicious actors can use it to access systems.

Explain several reasons why are computer incidents so prevalent (p. 86-87)?

Malware, application vulnerabilities, social engineering, human error, ransomware, hardware failure, and power outages

What are some common reasons mentioned for computer exploits?

Password vulnerabilities, OS and Endpoint application vulnerabilities, injection vulnerabilities, -Cross-site scripting (XXS) attacks, authentication issues, application authorization issues, application vulnerable components

Complete the perpetrator table.
Using the descriptions shared on the table, identify the types of computer perpetrators noted in the reading (p. 88).

Perpetrator Type	Description
Black Hat Hacker	**Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems).**
Malicious Insider	**An employee or contractor who attempts to gain financially or disrupt a company's information systems and business operations.**
Cybercriminal	**Someone who attacks a computer system or network for financial gain.**
Cyberterrorist	**Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations.**
Hacker	**An individual who causes problems, steals data, and corrupts systems.**

Topic: Types of Exploits

Define the following terms.

Ransomware: Is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen or deleted.

Virus: is a software program that infects a computer by inserting itself into programs that already reside in the machine.

Worm: is an autonomous program that forwards copies of itself to other machines in a network and could result in detriment of individuals machines or the operations of the network.

Trojan Horse: A Trojan horse is a type of malware that tricks users by appearing as a legitimate program or application. The term comes from the Ancient Greek story of the Trojan Horse that deceived the city of Troy.

What is it called when a threat combines various types of exploits and vulnerabilities in one payload?

A blended threat is an exploit that combines elements of multiple types of malware and usually employs various attack vectors to increase the severity of damage and the speed of contagion.

Answer the following questions about spam.

In states where it is legal to spam, what are the usual requirements?

Since spammers like to hide, CAN-SPAM requires businesses sending unsolicited commercial emails to have a valid physical mailing address in the message. You can usually find this address at the bottom of the email. It's often alongside other contact information like social media links.

How common is spam?

- Email: In 2023, some say that 45.6% of emails worldwide were spam, while others estimate that as much as 85% of emails are spam or malicious. Spam emails can include advertising, phishing, malware, or ransomware.
- Text: In 2022, Americans received 225 billion spam texts, which was a 157% increase from the previous year. In March 2024, Americans received 19.2 billion spam texts.
- Social media: Spam on social media can include fake followers, clickbait links, and deceptive advertising.
- Messaging apps: Spam in messaging apps can include unwanted messages with scams, malware, or unsolicited marketing.

Define the following attacks and terms (p.93-96).

DDos Attack: A distributed denial-of-service (DDoS) attack is a cybercrime that involves flooding a server with internet traffic to prevent users from accessing online services. DDoS attacks are a subcategory of denial-of-service (DoS) attacks, but are larger in scale and use thousands or millions of connected devices.

Botnet: A botnet attack is a cyberattack that uses malware to infect devices and turn them into bots that can be controlled remotely. Botnets can be used for a variety of reasons, including:

- Stealing money
- Extorting payments

- Mining for cryptocurrency
- Stealing confidential account data
- Overwhelming a target website with fake traffic
- Gaining illegal access to websites
- Bricking devices

Rootkit: A rootkit attack occurs when a malicious software program, or rootkit, is installed on a system and gives an attacker access to a computer's privileged software areas. Rootkits can be difficult to detect because they can block antivirus and malware scanner software and remain on a system for years.

APT: is a prolonged and targeted cyber-attack in which an intruder gains access to a network and remains undetected for extended period. APT attacks are initiated to steal highly sensitive data rather than cause damage to the target organization’s network.

Spear Phishing: Spear phishing is a type of cyberattack that uses personalized scams to target specific individuals, organizations, or roles within a company to steal sensitive information or infect devices with malware. Spear phishing attacks can be conducted through email, text messages, social media, instant messaging, and other platforms.

Smishing: is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals. The term “smishing” is a combination of “SMS”—or “short message service,” the technology behind text messages—and “phishing.”

Identify the large federal agency with a budget of almost $65 billion whose goal is to provide for a “safer, more secure America, which is resilient against terrorism and other potential threats.” (p. 98) : Department of Homeland Security (DHS)

Topic: Federal Laws for Prosecuting Computer Attacks

Complete the table of Federal Laws. These laws were enacted to address computer crimes (p. 100).

Law	Subject Area
The Computer Fraud and Abuse Act (CFAA) of 1984	**Address fraud and related activities in association with computers including access, transmission, password trafficking, and threats.**
The Fair and Accurate Credit Transactions Act	**Covers false claims regarding unauthorized use of credit cards.**

The Stored Communications Act (SCA), 18 U.S.C. § 2701	**Focuses on unlawful access to stored communications to obtain, alter, or prevent unauthorized access to electronic communication while it is in electronic storage.**
The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. **1030**	**Defines cyberterrorism and associated penalties.**

Topic: CIA Triad (p.100)

Identify are the three components of the CIA triad:

1. Confidentiality

2. Integrity

3. Availability

Describe a layered solution that can help prevent or minimize an attack.

- Firewall. ...
- Patch Management. ...
- Multi-Factor Authentication. ...
- Endpoint Protection. ...
- Web Content Filtering. ...
- Email Filtering. ...
- Security Awareness Training and Phishing Simulations. ...
- Sophisticated Password Policy.

How can an organization implement a CIA security strategy (p. 101)?

The CIA triad, which stands for confidentiality, integrity, and availability, is a framework for applying core cybersecurity principles to an organization. Here are some ways organizations can implement the CIA triad:

- Confidentiality-Restrict access to sensitive data through policies and security measures. This can include:
  - Using encryption and multi-factor authentication (MFA) systems
  - Classifying and labeling restricted data
  - Following the organization's data-handling security policies
  - Keeping access control lists and other file permissions up to date
- Integrity-Ensure data remains unaltered and consistent to avoid errors, fraud, and legal complications. This can include:
  - Reviewing all data processing, transfer, and storage mechanisms
  - Using version control, data logs, granular access control, and checksums
  - Using hash functions to prevent data corruption
  - Employing techniques such as data validation and error checking

    - Using backup and recovery software and services
- Availability- Ensure reliable access to data for those who need it. This can include:
    - Using preventive measures such as redundancy, failover, and Redundant Array of Independent Disks (RAID)
    - Ensuring systems and applications stay updated
    - Using network or server monitoring systems

Define the following terms (102-103).

Risk-Assessment: IT risk assessment is a process of analyzing potential threats and vulnerabilities to your IT systems to establish what loss you might expect to incur if certain events happen. Its objective is to help you achieve optimal security at a reasonable cost.

Reasonable Assurance: Reasonable assurance is a high level of assurance that there is a low probability that material misstatements will not be found or prevented in a timely manner. It is similar to absolute assurance, but with reasonable assurance, there is still a small chance that material misstatements exist.

Disaster Recovery Plan: A disaster recovery plan (DRP) is a guide that outlines the steps to take in the event of a disaster that could impact a business, such as a natural disaster, human error, or cyber-attack. A DRP can help a business get back on its feet faster and limit downtime, which can help maintain customer satisfaction and a competitive advantage.

Business Continuity Plan (BCP) is a document that outlines how an organization can continue operating during an unplanned event. It's a strategic playbook that helps organizations prevent or recover from disruptions, such as natural disasters, cyberattacks, or civic unrest. BCPs can help minimize downtime and other problems that could harm an organization's financial health.

What does a good security policy do (p. 104)?

A good security policy can help an organization in several ways, including:

- Protection: A security policy can protect an organization's critical information and intellectual property by clearly defining employee responsibilities. This can help employees act accordingly and be held accountable for their actions.
- Consistency: A security policy can help ensure consistency in monitoring and enforcing compliance. It can also help avoid duplication of effort by getting everyone on the same page.
- Compliance: A security policy can help an organization comply with data protection laws.

- Reputation: A security policy can help an organization maintain a positive reputation.

What should a good security audit do?

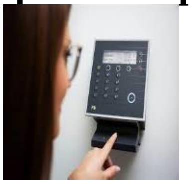
A good security audit should assess the strength of an organization's security controls and governance and identify areas for improvement. It should also help organizations comply with security standards and certifications.

Complete the table of Regulatory Standards Compliance. In addition to the requirement to comply with your own security program, you may also be required to comply with external security standards (p.106).

Act or Standard	Subject Matter
Under the Bank Secrecy Act (BSA)	**Requires financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering.**
The Foreign Corrupt Practices Act of 1977	**Makes certain payments to foreign officials and other foreign persons illegal and requires companies to maintain accurate records**
The Leach-Bliley Act (GLBA)	**Governs the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information**
HIPAA	**Regulates the use and disclosure of an individual's health information**
The Payment Card Industry Security Standards Council (PCI SSC) Document Library	**Provides a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information**
The Sarbanes-Oxley Act (SOX)	**Protects shareholders and the general public from accounting errors and fraudulent practices in the enterprise**

Topic: Implementing CIA at the Network Level (p.108)

Develop an example of one type of authentication method.

- 

  Biometric authentication

  Uses unique physical characteristics, like fingerprints, facial recognition, or voice, to verify a person's identity. The user's device stores digital templates of their biometric data, which are then compared to real-time readings to determine a match. Biometric authentication is considered secure because it's difficult to copy or steal a person's unique features.

-

  Multifactor authentication

  Combines multiple types of identity dimensions to grant a user access to a digital asset. This can include using a password, PIN, code word, or secret handshake in addition to something else, like a code sent via SMS. Multifactor authentication can make it harder for attackers to access a protected account because a password alone isn't enough.

-

  Passwordless authentication

  Doesn't require a user to enter a static password. Instead, it uses other methods to identify the user, such as biometrics, hardware tokens, or time-based one-time passwords (TOTP).

Explain how a next-generation firewall (NGFW) is different from a standard firewall.

Next-generation firewalls (NGFWs) are a third generation of firewall technology that combine traditional firewalls with other network device filtering functions. NGFWs have additional features that help block more threats and address a wider range of organizational needs than traditional firewalls

Explain the following two encryption terms (p. 109):

Encryption Key- An encryption key is a string of numbers or letters that's used to encode and decode data. It's a vital component of cryptography, as it's what allows data to be locked (encrypted) so that only those with the correct key can unlock (decrypt) it. Encryption keys are unique and difficult to replicate because they're specific to a particular encryption code and are generated using algorithms that ensure they're unpredictable. Longer keys are harder to break, but they also require more processing power to encrypt data. For example, 256-bit keys are stronger but less efficient than 128-bit and 192-bit keys.

Triple Layer Security (TLS)- Triple layer security is a method that uses multiple layers to protect data or information. If one layer fails, the others can step in to prevent a breach or loss of data. This type of security is also known as "defense in depth" (DID). Device, Document, Network. Every link in the chain is critical: every access point and every connection; every protocol, setting, and function; every print, copy, and scan.

How does an intrusion detection system work (p. 111)?

Is a software application that monitors network traffic and systems for malicious activity or policy violations. When it detects a threat, the IDS sends an alert to IT and security teams so they can evaluate the threat and take action.

Topic: Implementing CIA at the End-User Level (p.113)

Identify the several components of a good security education for employees.

All hands training (yearly), security tips (monthly), threat simulations (intermittently),

What does most antivirus software scan for?

Antivirus software scans for malicious software, or malware, by looking for patterns in files or a computer's memory. These patterns are based on the signatures or definitions of known malware, such as viruses, worms, Trojans, spyware, ransomware, and adware. Antivirus software scans by reading the code of files and folders and comparing it to a database of known threats. It can also identify suspicious code that doesn't match the database perfectly but may still be a threat.

Topic: Response to Cyberattack (p.115)

Why might a company try to conceal information about a data breach to its customers?

Companies may try to conceal information about a data breach to customers for a number of reasons, including:

- Reputational damage: Companies may be concerned about the damage to their reputation that could result from publicizing a breach. News of a breach can remain on the internet and social media for years, and companies may need to spend a lot of time and money on marketing and public relations to repair the damage.
- Customer and shareholder confidence: Companies may believe that disclosing a breach could negatively impact customer or shareholder confidence.
- Financial impact: Companies may be concerned about the impact on quarterly revenues and stock price.
- Avoiding panic: Companies may want to avoid creating undue panic by notifying everyone too soon.
- Avoiding fines: Companies may want to avoid heavy fines.

Explain the importance of activity logs surrounding a data breach or other security incident.

By using log files, you are able to determine the causes of a certain error or security breach. This is because the log files record data in concurrently with the activities of the information system. For instance, you are able to determine the last active user account prior to the error.

What must the IT security group do before it begins eradication efforts for a cyberattack?

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 necessary backups are current, complete, and free of any malware.

Identify at least 3 key elements that should be included in the formal incident following a cyberattack (p. 116):

a. A plan overview

b. A list of roles and responsibilities

c. The current state of network infrastructure and security controls

d. detection, investigation and containment procedures

e. eradication procedures

What is a MSSP and what does it do (p.117)?

MSSP stands for Managed Security Service Provider, which is an IT service provider that offers security services to businesses. MSSPs can help protect businesses from cyberthreats by providing software and services, building a network of security experts, and managing cybersecurity.

Explain the role of a computer forensics team-also known as digital forensics teams, help law enforcement, businesses, and individuals collect, preserve, and analyze digital evidence. Their work can help with criminal investigations, cybercrime, data breaches, intellectual property protection, and recovering lost data.

Section 3

In this section, one competency is covered across three modules. This section of the course contains Modules 4, 5, and 6, as follows:

- **Module 4: Privacy**
- **Module 5: Freedom of Expression**
- **Module 6: Intellectual Property**

Module 4	Privacy

Topic: Privacy Protection and the Law

What is the right of privacy, and what is the basis for protecting personal privacy under the law? (p.136)

The right to privacy is a basic law that protects an individual's right to be free from public interference and unwarranted publicity. It includes the right to be left alone, and to have private information free from public scrutiny. The right to privacy is based in the Constitution and is found in a "penumbra" cast by the First, Third, Fourth, Fifth, and Ninth Amendments. For example, the Fourth Amendment states 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.

Identify at least 3 systems that gather data about individuals? (p. 137)

1. Surveys and Questionnaires. Surveys and questionnaires, in their most foundational sense, are a means of obtaining data from targeted respondents with the goal of generalizing the results to a broader public. ...
2. Interviews. ...
3. Observations. ...
4. Records and Documents. ...
5. Focus Groups.

Define the following terms.

Right of Privacy: The right to privacy is a legal principle that aims to limit government and private actions that threaten an individual's privacy. It can be defined as the right to be free from interference or intrusion, or to be let alone. It can also include the right to control how personal information is collected and used.

Information Privacy also known as data privacy or data protection, is the right of individuals to control how their personal information is collected, used, and disclosed. It also involves the policies, procedures, and controls that determine how individuals are informed and involved in the process.

Topic: Privacy Laws, Applications, and Court Rulings

Complete the table below by identifying the applicable Law or Act (p. 139). Use this to review the patterns and changes in legislation relating to privacy. While you do not need to memorize these, you will want to be familiar with them and notice how they affect one another and change over time due to political and environmental circumstances.

Law or Act	Year	Impact
Financial Data		
The Fair Credit Reporting Act (FCRA)	**1970**	**Regulates the operations of credit reporting bureaus, including how they collect, store, and use credit information. This act is enforced by the U.S. Federal Trade Commission.**
The Right to Financial Privacy Act (RFPA)	**1978**	**Protects the records of financial institution customers from unauthorized scrutiny by the federal government.**
Gramm-Leach-Bliley Act (GLBA)	**1999**	**Also known as the Financial Services Modernization Act of 1999. Includes three key rules that affect personal privacy: Financial privacy (collection and disclosure guidelines), Safeguards (data security plan), and Pretexting rules.**
The Fair and Accurate Credit Transactions Act (FACTA)	**2003**	**Allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies. The act helped establish the National Fraud Alert system to help prevent identity theft.**
Health Data		
HIPAA (Public Law 104-191, also known as the Kennedy-Kassebaum Bill)	**1996**	**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.**
The American Recovery and Reinvestment Act (ARRA)	**2009**	**Included strong privacy provisions for electronic health records (EHRs), including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients. Individuals whose health information has been**

		exposed be notified within 60 days after discovery of a data breach.
Children’s Data		
The Family Educational Rights and Privacy Act (FERPA)	**1974**	**Assigns certain rights to parents regarding their children’s educational records. Includes rights to access, request, amend school records; along with file complaints for disclosure violations.**
Children's Online Privacy Protection Act (COPPA)	**1998**	**Any website that caters to children must 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.**
Surveillance		
The Electronic Communications Privacy Act (“ECPA”)	**1968**	**Allows state and federal law enforcement officials to use wiretapping and electronic eavesdropping, but only under strict limitations. Under this act, a warrant must be obtained from a judge to conduct a wiretap.**
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. Requires the government to obtain a court order before it can intentionally target a U.S. person.**
THE CIA	**1981**	**Identifies various U.S. governmental intelligence-gathering agencies and defines what information can be collected, retained, and disseminated by these agencies. These agencies are allowed to collect information, including messages, obtained**

		during lawful foreign investigations.
electronic communications privacy act	**1986**	**Deals with three main issues: the protection of communications while in transfer from sender to receiver; the protection of communications held in electronic storage; and the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant. Under this act, the FBI director may issue a National Security Letter (NSL) to an Internet service provider to provide various data and records about a service subscriber.**
The Communications Assistance for Law Enforcement Act (CALEA)	**1994**	**Required the telecommunications industry to build tools into its products that federal investigators could use, with a court order, to eavesdrop on conversations and intercept electronic communications.**
	(Terrorist attacks of September 11, 2001)	
USA PATRIOT Act	**2001**	**It gave sweeping new powers to both 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. It also eased restrictions on foreign intelligence gathering in the United States.**
The Foreign Intelligence Surveillance Act of 1978 (FISA)	**2004**	**Congress amended the FISA to authorize intelligence gathering on individuals not affiliated with any known terrorist organization (so-called lone wolves).**
USDOJ	**2008**	**Grants NSA expanded authority to collect, without court-approved**

		warrants, international communications as they flow through U.S. telecommunications network equipment and facilities. The targets of the warrantless eavesdropping had to be "reasonably believed" to be outside the United States.
	(Edward Snowden leaks NSA secrets)	
USA Freedom act	**2015**	**Act terminated the bulk collection of telephone metadata by the NSA. Instead, telecommunications providers are now required to hold the data and respond to NSA queries on the data. The act also restored authorization for roving wiretaps.**
Fair Information Practices		
OECD Privacy Principles	**1980**	**Often held up as the model for ethical treatment of consumer data. These guidelines are composed of the eight principles: collection limitation, data quality, purpose, use limitation, safeguards, openness, individual participation, and accountability.**
Communications Privacy Act	**1995**	**Requires any company doing business within the borders of the countries comprising the European Union (EU) to implement a set of privacy directives on the fair and appropriate use of information.**
The European Union's General Data Protection Regulation (GDPR)	**2018**	**Strengthens data protection for individuals within the EU by addressing the export of personal data outside the EU, enabling citizens to see and correct their personal data, and ensure data protection consistency across the EU.**
Access to Government Records		
	1966	**Grants citizens the right to access certain information and records of**

Freedom of Information Act		federal, state, and local governments upon request. Enables journalists and the public to acquire information that the government is reluctant to release.
The Privacy Act	1974	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 hiding any personal data keeping system.

Topic: Key Privacy and Anonymity Issues (p.158)

Identify and explain at least three common ways businesses may use a person's cookie information:

1. **Create personalized experiences by tracking behaviors and preferences**
2. **Gather analytics metrics such as pages visited, time spent on each page, and how frequently users return**
3. **Save login credentials or shopping-cart items**

About how much does a data breach cost a company per record? (p. 159)

$183 per record stolen in 2023.

What act makes identity theft illegal and punishable up to 15 years of imprisonment?

Identity Theft and Assumption Deterrence Act of 1998, As amended by Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998) Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled

Topic: Electronic Discovery (p.162)

Explain an electronic discovery and what types of information it might include.

Is a form of digital investigation that attempts to find evidence in email, business communications and other data that could be used in litigation or criminal proceedings. The traditional discovery process is standard during litigation, but e-discovery is specific to digital evidence.

What might a litigation hold prevent?

A litigation hold, also known as a legal hold or preservation order, prevents the destruction, alteration, or loss of evidence that may be relevant to a legal proceeding. This can include both physical and electronic evidence.

How might predictive coding assist in an e-discovery? What issues might arise from this?

Predictive coding, also known as technology-assisted review (TAR), is a machine learning tool that can help reduce the amount of content that needs to be reviewed in eDiscovery. It automates the document review process by teaching computers to learn from human input and make educated guesses about how to classify documents. This can help legal professionals identify relevant documents and data, such as responsive documents, privilege, and issue codes. Predictive coding can reduce document sets from millions to thousands of documents.

Topic: Workplace Monitoring (p.163)

What are some examples of cyber loafing?

Cyberloafing is when someone uses electronic devices during work or class hours for personal reasons. Some examples of cyberloafing include:

- In the workplace: Using work hours for non-work-related activities like browsing the internet, using social media, sending personal emails, or playing online games
- In the classroom: Using electronic devices during class for activities that aren't considered class-related, such as sending personal emails, watching videos, or playing online games

It is estimated that cyberloafing costs U.S. business as much as $85 billion a year.

Explain why a business may want to monitor its employees and if they are legally allowed to.

Basically, it is perfectly legal for an employer to monitor: Live telephone calls. In addition to having a legitimate business interest, the employer needs either to inform about monitoring or obtain consent from at least one party of real-time conversation. Private conversations must not be intercepted.

What type of employee information and data are frequently tracked?

Business performance management, attendance data, employment agreements, background checks, exit interviews, offer letters, benefits, demographic information, employment data, disciplinary actions and warnings, job descriptions, performance data, home address, PTO, time tracking, employment length, medical information, beneficiary information, leave records and balances, and personal data

Topic: Advanced Surveillance Technology (p.165)

Complete the following table. In the second column, describe the types of data collected by each of the following terms:

Type	What data do they capture?
Camera Surveillance	• Visual and auditory data: Video and audio recordings can be collected for a set amount of time. • Metadata: This can include timestamps, device locations, and network details. • Environmental data: Some cameras can collect information like ambient temperature and light conditions using embedded sensors. • Personal information: This can include images of people, which can be used to identify them directly or indirectly. • Social media posts: Homeowners may post videos of package thieves or attempted home entry to social media sites.
Vehicle Event Data Recorder (EDR)	Event Data Recorders (EDRs) can record a wide range of data about a vehicle's operation and performance before, during, and after a crash. The types of data collected can vary by vehicle model and manufacturer, but some common data points include: • Vehicle dynamics: Speed, acceleration, braking, steering, and engine performance • Occupant information: Seatbelt usage and airbag deployment • Crash signature: Collision severity and Delta-V, which is the change in velocity during the crash • Other events: Automatic collision notification (ACN) system activation and sudden speed changes

Stalking Apps	Permissions such as access to your location, contacts, camera, microphone, and other personal data can indicate that the app may be collecting information. Check how to review permissions on your Google/Android and Apple devices.

Module 5	**Freedom of Expression**

Topic: 1st Amendment Rights

What is the basis for the protection of freedom of expression?

The basis for the protection of freedom of expression can be found in the United States Constitution and the Universal Declaration of Human Rights:

- United States Constitution: The First Amendment to the U.S. Constitution protects freedom of expression from government interference. It states that Congress cannot make any law that abridges freedom of speech. The First Amendment also protects other rights, such as freedom of religion, freedom of the press, and the right to peacefully assemble. The Supreme Court interprets the extent of protection afforded to these rights.
- Universal Declaration of Human Rights: Article 19 of the Universal Declaration of Human Rights enshrines the right to freedom of expression. This right is later protected by international and regional treaties. Freedom of expression is considered vital for holding the powerful to account and for allowing other human rights, such as freedom of thought, conscience, and religion, to flourish.

The Supreme Court has held that the following types of speech are not protected by the First Amendment and may be forbidden by the government: (p. 188)

The Supreme Court has ruled that the First Amendment does not protect certain types of speech, including:

- True threats - Statements that indicate a serious intent to commit violence against a specific person or group, even if the speaker doesn't intend to carry it out
- Fighting words - The Supreme Court ruled in Chaplinsky v. New Hampshire (1942) that fighting words are not protected
- Obscenity - The Supreme Court upheld a ban on broadcasting vulgar words in FCC v. Pacifica Foundation (1978)

- Defamation - False statements of fact that harm someone's reputation and are communicated to a third party

Explain one of the three questions that can be used to determine if speech is considered obscene:

The Supreme Court's Miller v. California (1973) case established a three-part test to determine if speech is obscene:

- Prurient interest - Would the average person find the work appealing to prurient interests, applying contemporary community standards? Obscenity is defined as appealing to a shameful or morbid interest in sex, not normal, healthy sexual desires.
- Patently offensive - Does the work depict or describe sexual conduct in a way that goes beyond contemporary community standards and is patently offensive?
- Lack of value - Does the work lack serious literary, artistic, political, or scientific value, taken as a whole? A reasonable person would need to find value in the material for it not to be considered obscene.

Define the following terms.

Defamation: Online defamation, also known as cyber-libel or internet defamation, is the publication of false statements about a third party online that damage their reputation. It can occur on many platforms, including social media, blogs, and other websites.

Slander: Slander is a legal term that refers to the act of harming someone's reputation by making a false and damaging statement about them orally. It's a type of defamation, which is defined as a false statement that damages someone's reputation.

Libel: Libel in IT, also known as cyberlibel, is the act of publishing false information about a person, group, or organization online that could damage their reputation. Libel is a form of defamation, which is a legal term for certain types of false statements that harm someone's reputation. Libel can be communicated in writing, pictures, signs, or other physical forms.

Topic: Freedom of Expression- Key Issues

What important freedom of expression issues relate to the use of information technology?

You have the right to seek, receive and impart information and ideas of your choice without interference and regardless of frontiers. This means: You have the freedom to express yourself online and to access information and the opinions and expressions of others.

Complete the following access table by identifying the key legislation in column one (pp. 190-192).

Law or Ruling	Year	Description
RULING	**1996**	**Title V of the Telecommunications Act, aimed at protecting children from pornography. Penalties include fines and imprisonment.**
LAW	**1998**	**States that "whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor…" is subject to fines and/or imprisonment.**
RULING	**2004**	**Declared COPA was unconstitutional and could not be used to shelter children from pornographic materials.**

What then can be used by households to protect children from explicit websites while still allowing open access to media by adults? (p.192)

Parental controls are software and tools that allow parents to set controls on their children's internet use. They are a great way of helping prevent children from accessing unsuitable content online.

Explain at least two ways a government may censor a website (p.195).

1. Technical censorship: Governments can block or tamper with domain names, filter keywords, block IP addresses, or use packet filtering to terminate TCP packet transmissions when certain keywords are detected. They can also use URL filtering to scan URL strings for keywords, regardless of the domain name.
2. Forcing ISPs and search engines: Governments can force internet service providers (ISPs) to block websites or the entire internet, or require search engines to block certain queries or only return government-approved results.

3. Pressuring content providers: Governments can ask online content providers to remove content or search results.
4. Legislation: Governments can create legislation, extra-legal incentives, or policy to compel technological firms to carry out the blocking and surveillance for them.

Identify the top three countries with the largest populations of internet users (p.196):

China, India, and the US

What is a SLAPP? (p.197)

A SLAPP, or Strategic Lawsuit Against Public Participation, is a lawsuit that aims to silence or punish someone for speaking out on a matter of public interest. SLAPPs can be based on defamation law, but can also include issues surrounding privacy, confidentiality, and data protection. The goal of a SLAPP is to get a person to retract their criticism of the person or business, or to temporarily prevent critics from making public statements. SLAPPs can be costly and lengthy legal battles that make critics spend time and resources defending the lawsuit.

SLAPPs can arise when someone:

- Erect signs on their own property
- Speaks at public meetings
- Reports violations of environmental laws
- Testifies before Congress or state legislatures
- Protests publicly
- Posts a review on the Internet
- Writes a letter to the editor

Identify one court case where the US protected the right of anonymity. (p.198)

The US Supreme Court has ruled in many cases that the First Amendment protects the right to anonymous free speech, including:

- Talley v. California (1960)

  The court ruled that an ordinance requiring handbills to identify the publisher violated the First Amendment rights of speech and press. In this case, civil rights activist Mr. Talley was arrested for distributing a handbill calling for a boycott of businesses that didn't hire minorities. The court's ruling was a major victory for anonymous speech advocates and an example of how anonymity can help keep people safe.

- McIntyre v. Ohio Elections Commission (1995)

  The court ruled that anonymity protects people from retaliation by an intolerant society, and exemplifies the purpose of the First Amendment.

Define the following terms.

Doxing: is a cyberbullying tactic that involves releasing someone's personal information online without their consent, often with malicious intent. The term comes from "dropping dox," or "documents". Doxers may share this information to harass, intimidate, or seek revenge on their target.

Anonymous re-mailer service: hides the origin of an email by removing the return address and replacing it with a computer-generated code. The message is then resent from the remailer's server.

John Doe Lawsuit: A John Doe lawsuit is a legal action filed against an anonymous or unknown defendant, using the name "John Doe" as a placeholder. The term is used in many jurisdictions, including the United States and the United Kingdom.

Hate Speech: Hate speech is a form of expression that intends to humiliate, vilify, or incite hatred against a group or class of people based on their identity factors. These factors can include race, religion, ethnicity, nationality, gender, sexual orientation, disability, health status, language, economic or social origin, or age. Hate speech can be discriminatory, meaning it is biased, bigoted, or intolerant, or pejorative, meaning it is prejudiced, contemptuous, or demeaning. It can include epithets, slurs, statements that promote stereotypes, or nonverbal symbols. Some examples of hate speech include the Nazi swastika, the Confederate Battle Flag, and pornography.

Module 6	Intellectual Property

Topic: What is Intellectual Property

What does the term intellectual property encompass?

Intellectual property (IP) is a non-physical property that refers to creations of the human mind, such as original thoughts, inventions, designs, literary and artistic works, symbols, names, images, and computer code. IP rights protect the rights of creators over their creations.

What measures can organizations take to protect their intellectual property?

Copyrights, trademarks, patents, and trade secrets are the four primary types of intellectual property protection.

Define the following terms. (p. 225)

1. **Intellectual property:** a work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc.
2. **Copyright:** the exclusive legal right, given to an originator or an assignee to print, publish, perform, film, or record literary, artistic, or musical material, and to authorize others to do the same.

How long does the current copyright term protect authors?

In the United States, the length of copyright protection for a work depends on several factors, including when it was created and whether it was published:

- Works created after January 1, 1978 - Copyright protection lasts for the author's life plus 70 years after their death. For joint works by more than one author who weren't working for hire, the copyright lasts for 70 years after the death of the last surviving author.
- Anonymous, pseudonymous, or works made for hire - Copyright protection lasts for 95 years from the first publication date or 120 years from creation, whichever comes first. This also applies to works created by organizations like universities or journals.
- Works created before 1978 - The length of copyright protection varies depending on several factors. For example, the Orrin G. Hatch-Bob Goodlatte Music Modernization Act of 2018 changed the calculus for published sound recordings before 1972.

Explain the four factors that should be considered when determining whether a copyrighted work is prohibited by the fair use doctrine. (p. 226)

1. Purpose and character of the use
2. Nature of the copyrighted work
3. Amount and substantiality of the portion used
4. Effect of the use on the potential market for or value of the work

What must be proven to validate a software claim of copywrite infringement? (p. 227)

A copyright infringement action requires a plaintiff to prove (1) ownership of a valid copyright, and (2) actionable copying by the defendant of constituent elements of the work that are original.

What act created the position of Intellectual Property Enforcement Coordinator within the Executive Office of the President, while also increasing enforcement and penalties for infringement? (p. 228)

The Prioritizing Resources and Organization for Intellectual Property Act of 2008, Public Law 110–403 (Oct. 13, 2008) (also known as the “PRO IP Act") created, within the Executive Office of the President, the position of the Intellectual Property Enforcement Coordinator (IPEC).

International trade in counterfeit and pirated goods could have accounted for as much as $461 billion or 2.5 percent of world trade in 2013.

In WTO TRIPS Agreement table, the second column lists the key terms of the agreement. In the first column, enter the form of intellectual property that is protected. (p. 229)

Form of Intellectual Property	Key Term of Agreement
Copyright	**Computer programs are protected as literary works. Authors of computer programs and producers of sound recordings have the right to prohibit the commercial rental of their works to the public.**
Patents	**Patent protection is available for any invention—whether a product or process—in all fields of technology without discrimination, subject to the normal tests of novelty, inventiveness, and industrial applicability.**
Trade Secrets	**These have commercial value must be protected against breach of confidence and other acts that are contrary to honest commercial practices. Steps must have been taken to keep it secret.**

In the Digital Millennium Copyright Act (DMCA), enter the name of the title section in the second column to match the appropriate description. (p. 230)

Title	Name	Description
1	WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998	**This section implements the WIPO treaties by making certain technical amendments to the U.S. law to provide appropriate references and links to the treaties. It also creates two new prohibitions, one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information. Adds penalties for violation.**
2	Online Copyright Infringement Liability Limitation Act	**This section enables website operators that allow users to post content on their website (e.g., music, video, and pictures) to avoid copyright infringement liability if certain "safe harbor" provisions are followed.**
3	Computer Maintenance Competition Assurance Act	**This section permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer. The new copy cannot be used in any other manner and must be destroyed immediately after the maintenance or repair is completed.**
4	Miscellaneous provisions	**This section adds language to the Copyright Act confirming the Copyright Office's authority to continue to perform the policy and international functions that it has carried out for decades under its existing general authority.**
5	Vessel Hull Design Protection Act	**This section creates a new form of protection for the original design of vessel hulls**

Since DMCA does not directly govern copying, what does it do instead?

The DMCA was passed in the year 1998 in the US and is considered a copyright law. However, it does not focus on copying issues mainly but is actually focused on copyright infringements and distribution of tools and software.

Define the following terms. (p.232)

Utility Patent: A utility patent, also known as a "patent for invention", protects the functionality of a new or improved product, process, machine, or composition of matter. It gives the patent owner the exclusive right to make, use, or sell the invention for up to 20 years from the date of issue, unless maintenance fees are required.

Design Patent: A legal protection for the unique visual qualities of a manufactured item, such as its shape, configuration, or surface decoration. Design patents are different from utility patents, which protect an item's functionality or unique way of operating.

Prior Art: a concept in patent law used to determine the patentability of an invention, in particular whether an invention meets the novelty and the inventive step or non-obviousness criteria for patentability.

The U.S. Supreme Court has ruled that three classes of items cannot be patented (p. 233):

1. Laws of nature: Such as basic physical principles like Einstein's mass-energy equivalence (E=mc2) or the law of gravity
2. Natural phenomena: Such as human genes, which the Court ruled are not patentable because DNA is a "product of nature"
3. Abstract ideas: Such as only an idea or suggestion

If a court determines that the infringement is intentional, it can award up to 3 times the amount of the damages claimed by the patent holder.

Under the Leahy-Smith America Invents Act, the U.S. patent system changed from a "first-to-invent" to a "first inventor to file" system effective from March 16, 2013. (p.234)

Topic: Trade Secrets

Explain how trade secret laws protect more technology worldwide than patent laws do. (p. 236)

Trade secret laws can protect technology worldwide more than patent laws in a few ways:

- Protection duration: Trade secret protection can last indefinitely, while patents typically last up to 20 years.

- Application process: Trade secrets don't require an application or approval process, while patents can take several years to get approved.
- Cost: Trade secrets don't require registration fees, while patents can be costly.
- Disclosure: Trade secret protection doesn't require public disclosure, while the patent process may require inventors to disclose their invention.
- Other factors: Trade secrets can be a better option than patents if there are many alternative approaches to an invention, or if keeping the invention confidential is more cost-effective. For example, Coca-Cola's classic Coke recipe would have been in the public domain long ago if the company had filed for a patent when it started selling the drink.

In the Trade Secret Laws table, identify the law in column 1 that is described in column 2.

Act	Description
The Uniform Trade Secrets Act (UTSA)	**Defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, persons who can obtain economic value from its disclosure or use, and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."**
The Economic Espionage Act (EEA)	**An act passed in 1996 to help law enforcement agencies pursue economic espionage. It imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets.**
The Defend Trade Secrets Act (DTSA)	**An act passed in 2016 that amended the Economic Espionage Act to create a federal civil remedy for trade secret misappropriation.**

Define the following terms. (p. 238)

□ **Nondisclosure Clause:** A non-disclosure agreement (NDA), also known as a confidentiality agreement, is a legally binding contract that prevents one party from sharing confidential information with another party for a specified period of time. NDAs can be used in many situations, such as when hiring employees or contractors, negotiating business partnerships, or disclosing information to investors. They can help businesses protect their competitive edge, prevent intellectual property theft, and build trust with customers and partners.

- □ **Noncompete Agreement:** A non-compete agreement, also known as a restrictive covenant, is a legal contract that prevents an employee from competing with their employer after their employment ends. Non-competes can also prohibit employees from disclosing proprietary information. They are used in many industries, including information technology (IT), media, financial services, corporate management, and manufacturing. In IT, non-competes can last up to two years in high tech fields where employees have access to sensitive information about new technologies.

Topic: Current Intellectual Property Issues

Define the following terms. (p. 240-242))

Plagiarism: Plagiarism in IT is the act of using another person's ideas, computer code, algorithms, or other intellectual property without giving proper credit. This can include using a program from a textbook as the solution to a programming assignment without citing the original author. Other examples of plagiarism in IT include:

- Copying and pasting text from a website into a project
- Paraphrasing or editing a sentence without citing the original source
- Using data from a book, journal, lecture, thesis, or other student's essay without attribution

Reverse Engineering: also known as back engineering, is the process of breaking down a piece of software or hardware to understand how it works and what tools were used to create it. The knowledge gained from reverse engineering can be used to create new code, software, hardware, or network firewalls, or to improve existing products.

Identify one argument for and one argument against reverse engineering.

Pros: product improvement, innovation inspiration, design, cost-effective, update existing cad models, enhancing compatibility, maintaining quality, revamp an obsolete product

Cons:

- Legal concerns - Reverse engineering can violate intellectual property rights or software licenses, which can lead to legal challenges. It can also breach contracts, such as end-user license agreements (EULAs).
- Ethical considerations - Analyzing proprietary software or sensitive data can raise ethical concerns. Unintentional data exposure during the reverse engineering process can also lead to privacy issues.
- Resource-intensive - Reverse engineering requires specialized tools, expertise, and time, which can make it a resource-intensive process for organizations.
- Limited scope - Reverse engineering may not be effective in identifying all potential security vulnerabilities if it requires advanced skills and knowledge.

- Security risks - Reverse engineering may inadvertently expose vulnerabilities or sensitive data in systems or software, which could be exploited for malicious purposes.
- Equipment and software - You might not have the right equipment or software for the next object you need to scan. For example, after 3D scanning equipment creates a point cloud, the data needs to be converted to a usable digital format.
- Skills - You need people who are trained to use the scanning equipment and software to effectively reverse engineer an object.

Explain the reasoning behind why firms or individual developers create open source code, even though they do not receive money for it. (p. 244)

Whether small or large, every company wants to reduce expenses, and open source has made it more accessible. As open source reduces the time-to-market, the cost of developing any software or app is also reduced.

Contrast competitive espionage from industrial espionage. (p. 245)

Competitive espionage, also known as competitive intelligence (CI) or corporate intelligence, is the legal and ethical gathering of information about competitors and the market. Industrial espionage, also known as economic espionage or corporate spying, is the illegal gathering of confidential information about competitors.

Explain what is covered by a trademark and who it protects. (p.247)

A trademark is a word, phrase, symbol, or design that identifies a company's goods or services and distinguishes them from competitors. It gives the company the exclusive right to use the mark and prevents others from using a similar mark for related goods or services. Trademarks are a type of intellectual property (IP) that protects intangible assets from being used without consent.

When might nominal fair use apply?

Nominative fair use is a trademark law doctrine that allows a third party to use another party's trademark to identify the trademark owner or their goods and services. It's generally permitted if the following conditions are met:

- The product or service can't be easily identified without the trademark
- Only as much of the mark as is necessary is used
- The use doesn't imply sponsorship or endorsement by the trademark owner

Here are some examples of nominative fair use:

- A media outlet using a registered trademark name to report on an event
- An instructor using the name of a software program in advertising materials for a class on how to use it

- A real estate company listing mortgage companies' trademarks on their website to advertise their services
- An auto repair shop specializing in Volkswagens mentioning that fact in their advertising

Other situations where nominative fair use may apply include:

- Comparative advertising
- News reports, commentary, and academic works
- Parody, criticism, and commentary

What does a cybersquatter typically hope to gain? (P. 248)

"Cybersquatting" is registering, selling, or using a domain name with the intent of profiting from the goodwill of someone else's trademark.

Section 4

In this section, one competency is covered across three modules. This section of the course contains Modules 7, 8, and 9, as follows:

- **Module 7: Ethical Decisions in Software Development**
- **Module 8: The Impact of Information Technology on Society**
- **Module 9: Social Media**

Module 7	Ethical Decisions in Software Development

Topic: Software Quality and Why It Is Important

Explain quality management and state it's primary objective. (p. 266)

Quality management includes the determination of a quality policy, creating and implementing quality planning and assurance, and quality control and quality improvement. TQM requires that all stakeholders in a business work together to improve processes, products, services and the culture of the company itself.

The focus is to improve the quality of an organization's outputs, including goods and services, through the continual improvement of internal practices. Total quality management aims to hold all parties involved in the production process accountable for the overall quality of the final product or service.

Identify and explain at least three factors that can contribute to poor-quality software. (p.267)

1. Lack of Collaboration. ...
2. Lack of Code Coverage. ...
3. Poor Test Coverage. ...
4. Choosing a wrong Testing Framework. ...
5. Not having a proper Test Reporting System in place. ...
6. Lack of a proper Defect Management Process.

Fill in the blank. An INFORMATION SYSTEM is a set of interrelated components (including hardware, software, databases, networks, people, and procedures) that collects and processes data and disseminates the output. (p. 269)

Explain what a DSS is and how it may be used by a company. (p. 269)

is a software program that helps companies make better decisions by analyzing large amounts of data. DSSs can be used for a variety of purposes, including:

- Problem solving: Improving efficiency and streamlining operations
- Planning: Planning and company management
- Data understanding: Expanding data understanding, especially in the age of big data, AutoML, AI and machine learning

DSSs can use a combination of raw data, documents, personal knowledge, and/or business models to help users make decisions. They can produce reports that may project revenue, sales, or manage inventory. DSSs can also integrate multiple variables to produce different outcomes based on a company's previous data and current inputs. Some companies prefer a fully automated DSS that both analyzes information and makes a decision, while others decide to discuss the data and make a decision manually. Some professionals may also use a combination of both approaches.

Here are some examples of how DSSs can be used:

- GPS routing: Compares different routes, taking into account factors such as distance, driving time, and cost
- ERP dashboards: Visualizes changes in production and business processes, monitors current business performance against set goals, and identifies areas for improvement
- Crop planning: Helps farmers know the best time to plant, fertilize and harvest crops

Compare the terms product liability and strict liability. (p. 270)

Product liability is a type of strict liability that holds manufacturers or sellers responsible for injuries caused by defective products. Strict liability is a legal doctrine that holds parties liable for damages or injuries caused by their actions or products, regardless of fault.

What must be proven in a breach of warranty claim?

To win a breach of warranty claim, you must prove the following elements:

- Warranty: The seller made an express or implied warranty about the product's quality or title
- -Non-compliance: The product did not meet the seller's standards or description
- Injury: The failure to comply caused you quantifiable damages or injury

The burden of proof is on you, the buyer. Possible defenses to a breach of warranty claim include: Lack of privity, Lack of warranty, and Buyer misuse of the product.

Depending on the circumstances, damages for a breach of warranty can include: Repair costs, Loss of value, and Difference between the product's actual value and its value under warranty.

The UCC gives buyers the right to claim damages, product replacement, or repair for breach of warranty. However, parties can also agree on additional remedies.

Topic: Strategies for Developing Quality Software

Explain the two types of popular software development methodologies from the reading: (p.272-273)

1. Waterfall System: The waterfall model is a project management workflow that uses a linear, sequential approach to break down development activities into phases. Each phase depends on the deliverables of the previous phase, and the phases cascade down to the next, with little to no flexibility for changes. The term "waterfall" refers to this flow.

2. Agile: is a software development methodology that helps developers create and deliver applications more quickly and efficiently. It's based on principles like collaboration, customer feedback, and the "three C's" of card, conversation, and confirmation. Agile methods generally promote a disciplined project management process that encourages frequent inspection and adaptation.

In the Software Testing table, identify the type of testing in column 1 that is described in column 2. (p. 276)

Test Type	Description
White Box Testing	**A type of dynamic testing that involves viewing the software unit as a device that has expected input and output behaviors but whose internal workings are unknown (a black box).**
Black Box Testing	**A type of dynamic testing that treats the software unit as a device that has expected input and output behaviors but whose internal workings, unlike the unit in black-box testing, are known.**

Static testing	**A software-testing technique in which software is tested without actually executing the code. It consists of two steps—review and static analysis.**
Unit Test	**A software-testing technique that involves testing individual components of code (subroutines, modules, and programs) to verify that each unit performs as intended.**
Integration Testing	**Software testing done after successful unit testing, where the software units are combined into an integrated subsystem that undergoes rigorous testing to ensure that the linkages among the various subsystems work successfully.**
System Testing	**Software testing done after successful integration testing, where the various subsystems are combined to test the entire system as a complete entity.**
User Acceptance Testing UAT	**Software testing done independently by trained end users to ensure the system operates as expected.**

What are Capability Maturity Model Integration (CMMI) models? (p.277)

Capability Maturity Model Integration (CMMI) models are a set of best practices that help organizations build, improve, and measure their capabilities. CMMI models can be used to guide process improvement across a project, division, or entire organization. The goal of CMMI is to create reliable environments where products, services, and departments are proactive, efficient, and productive.

Describe the five levels of maturity described CMMI

1. Initial	**Unpredictable and reactive.** Work gets completed but is often delayed and over budget.
2. Managed	**Managed on the project level.** Projects are planned, performed, measured, and controlled.
3. Defined	**Proactive, rather than reactive.** Organization-wide standards provide guidance across projects, programs, and portfolios.
4. Quantitatively Managed	**Measured and controlled.** Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.
5. Optimizing	**Stable and flexible.** Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization's stability provides a platform for agility and innovation.

Define the following terms. (p. 279-280)

- □ **Safety-Critical System:** is a system that's designed to prevent or lessen the consequences of dangerous events. These systems are intended to function properly without any malfunctions to prevent worst-case scenarios like human injury or death, property damage, environmental damage, or financial loss

- □ **System Safety Engineer:** is an engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated.
- □ **Annualization Loss Expectancy (ALE):** is a calculation that estimates the expected monetary loss an asset may incur over a year due to a specific risk. It's a key part of quantitative risk assessments, which use hard numbers to evaluate the likelihood and impact of risks.
- □ **Risk Management:** is the application of risk management methods to manage IT threats. IT risk management involves procedures, policies, and tools to identify and assess potential threats and vulnerabilities in IT infrastructure.

Identify the five strategies for addressing a particular risk? (p.281)

1. **Avoidance**
2. **Retention**
3. **Transferring**
4. **Sharing**
5. **Loss Reduction**

Fill in the blank. Reliability and safety are two different system characteristics. Reliability has to do with the capability of the system to continue to perform; Safety has to do with the ability of the system to perform in a safe manner. (p.282)

Describe the ISO 9001 family of standards guide. (p. 283) - Is a globally recognized quality management system (QMS) that helps organizations meet customer needs and expectations. Is part of the ISO 9000 series of standards, which are developed and published by the International Organization for Standardization (ISO).

Explain Failure Mode and Effects Analysis (FMEA). Is a systematic method for identifying and addressing potential problems in a process or system before they occur. FMEA is a proactive tool that can be used to evaluate both new and existing processes, and can be applied to many different areas, including product design, production, and organizational issues.

During an FMEA, a team representing all areas of the process works together to:

1. Predict and record where, how, and to what extent the system might fail
2. Assess the relative impact of different failures

3. Identify the parts of the process that need the most change
4. Devise improvements to prevent those failures

The output of an FMEA is a Risk Priority Number (RPN), which is calculated by multiplying the severity, occurrence, and detection of each failure mode. The team can then use their experience and judgment to prioritize actions based on the RPN.
FMEA can help prevent costly manufacturing issues, improve product quality and service reliability, and increase customer satisfaction.

Module 8	**The Impact of Information Technology on Society**

Describe what might be included in a patient's electronic health record (EHR). (p. 300).

An electronic health record (EHR), also called an electronic medical record (EMR), is a digital version of a patient's medical history. EHRs can include a variety of information, such as:

- Demographics: Age, gender, and ethnicity
- Health history: Diagnoses, allergies, and treatment plans
- Medications: Prescriptions and other medications
- Vital signs: Blood pressure and other vital signs
- Immunizations: Immunization dates and status
- Laboratory data: Lab test results
- Radiology reports: Radiology images
- Billing information: Hospital discharge instructions and billing information
- Progress notes: SOAP notes (Subjective, Objective, Assessment and Plan) that can provide an overview of the patient at the time of consultation

What does the Health Information Technology for Economic and Clinical Health Act (HITECH) do?

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 was passed by Congress as part of the American Recovery and Reinvestment Act (ARRA) to promote the use of health information technology (HIT). The act's goals include:

- Improving health care

  HITECH gives the Department of Health and Human Services (HHS) the authority to create programs that improve the quality, safety, and efficiency of health care through HIT. This includes electronic health records (EHRs) and secure electronic exchange of health information.

- Encouraging EHR adoption

  HITECH encourages healthcare providers to adopt EHRs by offering financial incentives. For example, physicians who could show meaningful use of a certified EHR system between 2011 and 2015 could receive up to five years of bonus Medicare payments.

- Protecting privacy and security

  HITECH includes provisions to address privacy and security concerns related to electronic health information. These provisions include:

  - Strengthening the civil and criminal enforcement of the HIPAA Privacy and Security Rules
  - Establishing four categories of violations and corresponding penalty amounts
  - Holding more parties accountable

  HITECH increases protections and holds more parties accountable. Compliance with HIPAA now also means compliance with HITECH.

Explain labor productivity and key factors related to improving it. (p. 303)

Labor productivity is defined as output per worker or per hour worked. Factors that can affect labor productivity include workers' skills, technological change, management practices and changes in other inputs (such as capital).

Topic: IT and Workplace Automation (p.306)

According to the reading, about how much of human work could be automated using existing technology? (p.306)

However, automation is likely to have widespread effects. Researchers estimate that anywhere from 9% to 47% of jobs could be automated in the future.

Identify types of work activities lease suited for automation.

In the Artificial Intelligence table, identify the type of AI in column 1 that is described in column 2.(p. 307-309)

AI Type	Description
Reinforcement Learning	A type of artificial intelligence (AI), involves computer programs that can learn some tasks and improve their performance with experience.
Machine Learning	A branch of engineering that involves the development and manufacture of mechanical or computer devices that can perform tasks that require a high degree of precision or that are tedious or hazardous for human beings, such as painting cars or making precision welds.

Natural Language Processing (NLP)	**An aspect of artificial intelligence that involves technology that allows computers to understand, analyze, manipulate, and/or generate "natural" languages, such as English.**
Unit Test	**A software-testing technique that involves testing individual components of code (subroutines, modules, and programs) to verify that each unit performs as intended.**

What are the three major components of machine learning? (p. 307)

- Representation. Representation refers to formulating the problem as a machine learning problem typically one among these a classification problem, a regression problem or a clustering problem. ...
- Evaluation.
- Optimization

Identify some of the major improvements made by IT to the healthcare industry. (p.311)

- Artificial intelligence. ...
- Extended reality. ...
- Health trackers, wearables and sensors. ...
- Portable diagnostics devices. ...
- Direct-to-consumer genetic testing. ...
- Revolutionizing drug development. ...
- Digital therapeutics.

Contrast the how an electronic medical record is different from a personal health record. (p. 312)

Personal health records (PHRs) and electronic medical records (EMRs) differ in who controls the record, how it's accessed, and who can share it:

- Control: A PHR is controlled by the patient, while an EMR is controlled by the institution that operates it, like a hospital.
- Access: A patient can set up and access their PHR themselves, while authorized clinicians can access an EMR to provide care.
- Sharing: A patient can share their PHR with others, like family members, caregivers, and providers, while an EMR is designed to be shared with multiple healthcare providers and organizations.

Explain Health Information Exchange (HIE) and its benefits.

Health Information Exchange (HIE) is a system that allows patients and healthcare providers to securely share a patient's medical information electronically. HIE can improve the quality, speed, safety, and cost of patient care, and can lead to better healthcare outcomes, patient safety, and healthcare system effectiveness.

Define the following terms. (p. 312-314)

- □ **Clinical Decision Support (CDS):** Clinical decision support (CDS) is a health information technology (HIT) component that provides clinicians, staff, patients, and others with information to improve health care. CDS tools and systems can help clinical teams by taking over some routine tasks, warning of potential problems, or providing suggestions for the clinical team and patient to consider.
- □ **Computerized Provider Order Entry (CPOE):** is a system that allows healthcare providers to electronically enter and send medical treatment instructions to patients using a computer application. CPOE can replace traditional methods of entering orders, such as on paper, by fax, or over the phone.
- □ **Telehealth:** the provision of healthcare remotely by means of telecommunications technology.

Identify the three basic forms of telemedicine: (p.314)

The three main types of telemedicine are store-and-forward, remote monitoring, and real-time interactive services:

- Store-and-forward: Also known as asynchronous telemedicine, this type involves transmitting medical information, such as images or test results, from one healthcare provider to another. This can be done using specialized technology that stores the data in a secure cloud-based platform for later retrieval by another professional. Store-and-forward telemedicine is often used in specialties such as dermatology, radiology, and pathology.
- Remote monitoring: Also known as remote patient monitoring (RPM), this type involves collecting a patient's health data, such as blood pressure, glucose levels, weight, and sleep apnea, and electronically sending it to a healthcare professional for review. RPM can be especially helpful for seniors or in senior living areas to prevent falls and monitor residents' vitals. Patients may also like RPM because it can reduce the need for frequent follow-up appointments with their doctor.
- Real-time interactive services: This type allows patients and physicians to communicate in real-time, which can save patients time traveling to and from the doctor's office.

Module 9	**Social Media**

Explain the meaning of social media and what it includes. (p.330) What is Social Media? Social media refers to the means of interactions among people in which they create, share, and/or exchange information and ideas in virtual communities and networks. The Office of Communications and Marketing manages the main Facebook, X/Twitter, Instagram, LinkedIn, and YouTube accounts.

Topic: Social Networking Platforms (p.331)

How do individuals use social networks?

- Connecting with others: People can reconnect with friends and family, or connect with people who share similar interests, goals, or experiences. They can use groups, lists, and hashtags to find each other.
- Sharing content: People can share photos, status updates, videos, and other images. They can also share useful content, such as news stories, inspiration, or information.
- Communicating: People can communicate with each other one-on-one, or form forums for discussions. Popular communication platforms include WhatsApp and Snapchat.
- Entertainment: People can use social networks for entertainment, such as sharing multimedia content. Popular multimedia networking platforms include YouTube and Flickr.
- Driving traffic: People can use social media to drive traffic to real events and activities.

What are some practical business uses of social networking?

Social networking, or social media, can be used by businesses in many practical ways, including:

- Building brand recognition: social media can help businesses establish an online presence that reflects their values, mission, and offerings.
- Communicating with customers: social media can provide a direct line of communication with customers, allowing businesses to respond to inquiries, address concerns, and build stronger relationships.
- Promoting products and services: Businesses can use social media to advertise and sell their products or services, and to inform customers of new releases, delivery schedules, and price changes.
- Increasing traffic: social media can help businesses drive traffic to their website and improve their SEO.
- Gathering customer feedback: social media can encourage customers to provide timely feedback, which can be vital for businesses to offer services that meet their needs.
- Analyzing competitors: businesses can use social media to keep an eye on their competitors.
- Networking: Social media can help businesses connect with potential employers, industry professionals, and other entrepreneurs.

Topic: Business Applications of Social Media

Identify some business-oriented social networking platforms. (p.333)

Many social networking platforms can be used for business purposes, including:

- Facebook

  A well-known platform with over 2.37 billion users and 60 million business pages, Facebook allows businesses to create pages to promote themselves

- LinkedIn

  A business app and employment-oriented social network that allows workers and employers to connect and make business contacts

- Instagram

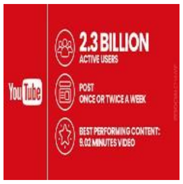
  A fast-growing platform with over 1 billion active users, 90% of whom follow at least one business page, making it a good fit for business promotion

- Twitter

  A popular platform with over 450 million monthly active users that can be used by B2B SaaS companies to connect with their audience, promote products and services, and provide customer service

- Pinterest

  A network that can be used for B2C or B2B marketing to connect with audiences, raise brand awareness, build communities, drive website traffic, and improve customer relationships

- 

  YouTube

A popular marketing channel for businesses and influencers, with 62% of businesses using it to post video content to promote their brand

TikTok

A fast-growing platform that offers potential for business, particularly given that social media marketing is highly competitive

- Snapchat

  A platform with high engagement rates that allows businesses to communicate with their audience in real time, which can be useful for local advertising and interactive stories

- WhatsApp

  A popular messaging app with over 50 million business users that can be used to drive sales, communicate with customers, and build relationships

Describe social media marketing. (p. 335)

Social media marketing (SMM) is the use of social media platforms to promote a company's products or services, build a brand, and connect with audiences. It can also help increase sales and drive website traffic.

Explain the following four types of social media marketing and it benefit to a business:

1. Organic Media Marketing: Organic media marketing, also known as organic marketing, is a long-term digital marketing strategy that uses non-paid tactics to increase brand awareness and build connections with audiences. The goal is to drive traffic to a business over time without using paid advertising.

2. Paid Media Marketing: is a marketing strategy that involves paying for ad space to promote a brand to a wider audience. It can be an important part of a brand's strategy to increase revenue, sales, and traffic through clicks. Paid media can also help with brand awareness.

3. Earned Media: also known as earned content or organic visibility, is any publicity or coverage a company receives from third-party sources without paying for it. It can include content and conversations about a brand or product that are created by others and published outside of a company's owned channels.

4. Viral Marketing: is a sales technique that uses word-of-mouth or organic information to spread about a product or service at an increasing rate. The term comes from the idea of consumers spreading information about a product to others, similar to how a virus spreads from person to person.

Topic: Social Networking Ethical Issues (p. 339)

Define the following types of cyber abuse:

Cyberharassment: Cyberharassment, also known as online bullying or cyberbullying, is a pattern of threatening or malicious behavior that happens online. It can include any kind of inappropriate, mean, or uncomfortable online behavior, such as:

- Harassing or threatening emails or instant messages
- Blog entries or websites that torment someone
- Unconsented conduct
- Outing and trickery, such as tricking someone into revealing personal information
- Targeted harassment, where multiple people work together to repeatedly harass someone online

Cyberstalking: The use of technology to stalk, sometimes called "cyberstalking," involves using the Internet, email, or other electronic communications to stalk someone. Stalking is against the law. Stalking and cyberstalking can lead to sleeping problems or problems at work or school.

Describe at least one way the law protects against cyberstalking.

Cyberstalking laws Combat Online Predators Act: A law that increased the maximum prison sentence for perpetrators who stalk minors online. Title 18 : An anti-stalking law prohibiting various forms of stalking, including using electronics to cause physical harm or emotional distress.

What does SORNA stand for?

Sex Offender Registration and Notification Act. It's Title I of the Adam Walsh Child Protection and Safety Act of 2006, and it establishes minimum standards for sex offender registration and notification in the United States.

Fill in the blank. The First Amendment of the U.S. Constitution protects the right of freedom of expression from government interference; however, it does not prohibit free speech interference by private individuals or businesses. **(p.344)**

SECTION 5

In this section, four competencies are covered across two modules. This section of the course contains Modules 10 and 11, as follows:

- **Module 10: Ethics of IT Organizations**
- **Module 11: AI Ethics and Appendix A: A Brief Introduction to Morality**

Module 10	**Ethics of IT Organizations**

Topic: Use of Contingent Workers (p. 360)

Define the following types of contingent working:

Temporary Staffing: Temporary staffing, also known as contingent work, is when a company hires someone to work in a specific role for a set period of time, usually on a contractual basis. Temporary employees can work part- or full-time, and their assignments can range from a few days to several months.

Employee Leasing: is a type of human resource outsourcing (HRO) where a staffing firm supplies workers to a business on a temporary or project-specific basis. The leasing agency handles all HR administration for the employees, including payroll, benefits, compensation, and reporting wages and taxes. The employees work for the client business, but are considered common law employees of the leasing organization.

Professional Employer Organization: is a human resources (HR) company that contracts with businesses to perform various administrative tasks. PEOs are also known as employee leasing companies.

In a gig economy, how might an individual make a profit? (p.361)

Gig economy jobs are often one-time or short-term contract jobs. These include driving for a ride-sharing service, painting someone's house, freelance work, coaching, fitness training, and tutoring. The job is exchanged for cash and there are no other benefits, such as health insurance.

Identify at least one benefit and one drawback to being employed as an independent contractor. (p. 362)

The advantages of being an independent contractor over being an employee include more control since you're your own boss. You might earn more as an independent contractor, and the tax benefits can include deducting your business expenses. The drawbacks to being an independent contractor include more responsibility.

Describe at least two benefits to a business when they hire contingent workers. (p.363)

Sourcing and hiring employees takes time, and sometimes the need for critical talent is immediate. By using contingent workers, employers can move quickly to fill their openings. Unique skills. Contingent workers may have hard-to-find skills that businesses need.

Describe at least one disadvantage to a business hiring contingent workers.

Drawbacks of Hiring Contingent Workers

- Less Control. You cannot manage the activities of a contingent worker. ...
- There Are Increased Tax Risks. ...
- It Comes With Security Risks. ...
- There's Reduced Learning.

Topic: H-1B Workers (p. 366)

Explain what an H-1B visa is.

The H-1B visa is a nonimmigrant visa that allows employers in the United States to temporarily hire foreign workers in specialty occupations. These occupations require a bachelor's degree or higher in a specific field, or its equivalent, and the ability to apply specialized knowledge in both theoretical and practical ways. Some examples of H-1B specialty occupations include:

- Architecture
- Engineering
- Mathematics
- Physical sciences
- Social sciences
- Medicine
- Health
- Education
- Business Specialties
- Accounting and
- Law

How long can an individual work in US as an H-1B employee?

The H-1B visa is a nonimmigrant visa that allows foreign professionals to work in specialty occupations in the United States for up to six years. The initial period of stay is usually three years, but can be extended for up to an additional three years. However, the six-year limit restarts if the beneficiary has been outside of the U.S. for more than one year. Employers can also request to "recapture" any time an employee has spent outside of the U.S. and add it back into the maximum period of stay.

In general, if an H-1B worker reaches the six-year limit and has not obtained a green card or other visa status, they are required to leave the U.S.. However, there are some exceptions and alternatives that may allow them to stay longer, such as:

- Filing an Application for Permanent Employment Certification (PERM) with the U.S. Department of Labor (DOL)
- Filing an I-140 Immigrant Petition with the USCIS
- Sections 104 and 106 of the American Competitiveness in the 21st Century Act (AC 21)

To extend an H-1B visa, the employer must complete and file Form I-129 again on behalf of the employee, along with any supporting documents, and pay the filing fee.

What would an individual need to do to transition from a temporary H-1B employee to full-time US resident?

To transition from an H-1B visa to a Green Card and become a full-time US resident, an individual can follow these steps:

1. Employer applies for Permanent Labor certification (PERM)
2. Employer submits Form I-140: This form determines the individual's priority date and preference level
3. Individual submits Form I-485: This is the Green Card application
4. Individual attends an interview
5. If approved, individual receives a passport stamp
6. Green Card arrives by mail

Identify at least one disadvantage to a business relying heavily on H-1B employees?

An H-1B visa holder can lose his or her job with no reason given. The H-1B holder will lose the right to remain in the USA if employment is terminated but sometimes the USCIS will grant a 10 day grace period. The U.S. employer has the right to displace an H-1B worker with a qualified U.S. worker.

Topic: Outsourcing

Explain the difference between outsourcing and offshore outsourcing. (p. 372)

Outsourcing is when a company contracts with a third party to perform a task or function, while offshoring is when a company moves some or all of its operations to another country. Offshoring can be considered a type of outsourcing when the third party is located in another country.

What is outsourcing so common in the IT field?

IT outsourcing is a growing business practice that allows companies to hire outside service providers to perform IT tasks. It's common in the IT field because it can help businesses achieve many goals, including:

- Cost savings

  Outsourcing can reduce operational costs and avoid full-time employment.

- Access to expertise

  Businesses can gain access to specialized skills and knowledge, such as subject matter experts and emerging IT talent.
- Focus on core business

  Outsourcing can free up resources for a company's core business operations, such as development.
- Improve efficiency

  Outsourcing can help businesses simplify processes and accelerate digital transformation efforts.
- Competitive edge
  Outsourcing can help businesses maintain their competitiveness in a rapidly changing technology environment and foster innovation.

Identify one pro and one con to offshoring. (p.373)

Offshoring has many advantages, including cost savings and access to a wider talent pool, but it also has some disadvantages, such as quality control issues.
Here are some pros and cons of offshoring:

Pros

- Lower costs Labor and facility rental costs are often cheaper overseas.
- Access to talent Companies can tap into a global talent pool with specialized skills that may not be available locally.
- Improved economies Offshoring can help improve other economies.
- Round-the-clock support Businesses can have support available around the clock.
- Frees up resources Offshoring can free up time and resources for a company's core competencies.

Cons

- Quality control Offshoring can lead to quality control issues.
- Communication Offshoring can pose communication challenges.
- Language barriers Language barriers can be an issue.
- Loss of control Companies may lose some control over their intellectual property or operations.
- Job losses Domestic workers may lose their jobs to offshoring.

What can improve the chances that offshoring will be successful? (p374)

By establishing robust quality assurance measures and effective communication channels, organizations can ensure that offshoring operations meet high-quality standards and customer expectations.

What does a successful Statement on Standards for Attestation Engagements (SSAR) demonstrate?

Is a Generally Accepted Auditing Standard produced and published by the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board.

Topic: Whistle-Blowing

Define the term whistle-blowing and explain who might be behind it. (p.375)

A Whistleblower is any individual who provides the right information to the right people. Stated differently, lawful whistleblowing occurs when an individual provides information that they reasonably believe evidences wrongdoing to an authorized recipient.

Explain two common legal provisions from the reading that are associated with whistle-blowing: (p.376)

1. **False Claims Act:** The False Claims Act (FCA) is a US law that protects the federal government from fraud and abuse. It was signed into law by President Abraham Lincoln in 1863 to prevent contracting fraud during the Civil War. The FCA has been amended several times, most recently in 2009 to clarify terms.
2. **Qui tam:** Qui tam is a Latin phrase that means "who sues in the name of the king as well as for himself". It's a type of whistleblower lawsuit that allows a private citizen to file a civil action on behalf of the government to recover damages and penalties for fraud. The term is a provision of the federal False Claims Act (FCA).

Identify the eight steps behind an effective whistle-blowing process:

1. Set Up and Name A Dedicated Team
2. Be Responsive
3. Internal vs External Whistleblowing Case Management
4. Establish A Whistleblowing Mechanism With Anonymity
5. Create A Policy That Matches Your Vision And Mission
6. Refer To Whistleblower Protection Rights And Laws
7. Ensure Your Worker’s Awareness
8. Keep the lines of investigation confidential

Explain what green computing refers to. (p.381)

Green computing, also known as sustainable IT or green IT, is the practice of using technology in a way that reduces its environmental impact. It involves a range of strategies and practices that aim to minimize the environmental impact of information technology use throughout a product's lifecycle.

What are the goals of green computing?

Green computing, also known as sustainable computing, aims to reduce the environmental impact of computer systems, software, and chips through their design and use. The goals of green computing include:

- Energy efficiency: Designing, manufacturing, and using IT systems to use less electricity
- Resource reduction: Using greener energy sources and reducing resource use
- Product lifecycle: Improving the reusability, maintainability, and repairability of products to extend their lifespan
- Recyclability and biodegradability: Improving the recyclability or biodegradability of products

What does EPEAT do?

EPEAT, or the Electronic Product Environmental Assessment Tool, is a global ecolabel that helps people evaluate the environmental impact of electronics and technology products. The Green Electronics Council (GEC) manages EPEAT, which was originally developed between 2002 and 2006 with a grant from the U.S. Environmental Protection Agency (EPA).

Module 11	**AI Ethics & Morality**

Topic: Understanding Bias & Fairness (Video)

(Go to Module 12 and go under AI Ethics and watch the video from Pluralsight.

Identify and explain the three core components of AI Trust:

1. Understanding- Define hazards and thresholds

2. Action - Guardrails to mitigate hazard likelihood & severity

3. Explanation - Communicate risk behaviors & events, i.e. compliance documentation & visualizations

List the five defined measurements of performance.

Data Quality, Accuracy, Robustness, Stability, and Speed

List the five defined measurements of operations

Monitoring, Compliance, Security, Humility, Business Rules

List the five defined measurements of ethics

Interpretability, Bias/Fairness, Governance, Social Impact Assessment

Explain the following common sources of bias

- □ **Skewed Sample** - Dataset is skewed towards certain group or may not reflect the real world
- □ **Limited Features** - Feature collection for certain groups may not be informative or reliable
- □ **Tainted Examples** - Unreliable labels, historical bias
- □ **Sample Size** - Do we have enough data?
- □ **Proxies** - Zip code or school can be proxies for race. School or sport activity can be proxies for gender

What are four suggestions are made for tackling AI bias?

1. Identify protected features in your dataset (i.e. race, color, age, religion, disability, sex, and etc.).

2. **Select** an appropriate "fairness metric" for your use
3. **Build** insights to identify & understand your model's potential bias
4. **Mitigate** bias uncovered in your data or model

Explain the following bias mitigation techniques

- □ **Pre-processing** - Transform your data such that the target would not be correlated to protected attributes
- □ **In-processing** - Modifying the loss function in your algorithm to have fairness to constraints
- □ **Post-processing** - Changing the model predictions to avoid discriminations

Topic: A Brief Introduction to Morality (Appendix A)

Complete the table by describing the following ethical theories.

Theory	Description
Deontology	Deontology is a normative ethical theory that judges the morality of an action based on whether it is right or wrong under a set of rules and principles, rather than on the consequences of the action. The word deontology comes from the Greek words deon (duty) and logos (science or study of).
Consequentialism/ Utilitarianism	Consequentialism is a moral philosophy theory that states that the consequences of an action are the basis for determining whether the action is right or wrong. It's a results-based ethics that judges whether something is good or bad based on its outcomes. Consequentialism is based on two principles: • The results of an action determine whether it's right or wrong • The more good consequences an action produces, the better or more right it is Utilitarianism is a moral philosophy and ethical theory that suggests actions that maximize happiness and well-being for the greatest number of people. It is a form of consequentialism, which means that the right action is determined by its consequences. Utilitarianism also values impartiality and agent-neutrality.
Virtue Ethics	Virtue ethics is a philosophical approach to morality that focuses on a person's character and virtue as the primary subjects of ethics. It's a person-centered theory that considers the whole of a person's life, rather than specific actions, and encourages people to develop virtuous habits to live a moral life.

Relativism	Relativism in IT ethics, also known as ethical relativism or moral relativism, is the idea that ethical or moral values and beliefs are relative to the individuals or societies that hold them. This means that there is no objective right or wrong, and what is right for one person or in one situation may not be right for another.

SECTION 6

Course summary and completion notice.

Collection of chapter summaries from *Ethics in Information Technology* (Reynolds, G. 6th edition, 2019)

Chapter 1 summary: An Overview of Ethics

What is ethics?

•Ethics is a code of behavior that is defined by the group to which an individual belongs.

•Morals are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong.

•A person who acts with integrity acts in accordance with a personal code of principles.

•Law is a system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (the police, courts, and law-making bodies).

•A code of ethics states the principles and core values that are essential to one's work.

•Just because an activity is defined as legal does not mean that it is ethical.

<u>What trends have increased the likelihood of an unethical behavior?</u>

•Globalization has created a much more complex work environment, making it more difficult to apply principles and codes of ethics consistently.

•Organizations may be tempted to resort to unethical behavior to maintain profits in today's more challenging and uncertain economic climate.

•It is not unusual for powerful, highly successful individuals to fail to act in morally appropriate ways as such people are often aggressive in striving for what they want and are used to having privileged access to information, people, and other resources. Furthermore, their success often inflates their belief that they have the ability and the right to manipulate the outcome of any situation.

<u>What is corporate social responsibility, and why is fostering good business ethics important?</u>

•Corporate social responsibility is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.

•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.

•Each organization must decide if CSR is a priority, and if so, what its specific CSR goals are.

•Organizations have five good reasons for pursuing CSR goals and promoting a work environment in which they encourage employees to act ethically: (1) to gain the goodwill of the community, (2) to create an organization that operates consistently, (3) to foster good business practices, (4) to protect the organization and its employees from legal action, and (5) to avoid unfavorable publicity.

<u>What measures can organizations take to improve their business ethics?</u>

•An organization can take several actions to improve its business ethics including: appointing a corporate ethics officer, requiring its board of directors to set and model high ethical standards, establish a corporate code of ethics, conduct social audits, require employees to take ethics training, include ethical criteria in employee appraisals, and create an ethical work environment.

<u>How can you include ethical considerations in your decision making?</u>

•Often, people employ a simple decision-making model that includes these steps: (1) define the problem, (2) identify alternatives, (3) choose an alternative, (4) implement the decision, and (5) monitor the results.

•You can incorporate ethical considerations into decision making by identifying and involving the stakeholders; weighing various laws, guidelines, and principles—including the organization's code of ethics—that may apply; and considering the impact of the decision on you, your organization, stakeholders, your customers and suppliers, and the environment.

What trends have increased the risk that information technology will be used in an unethical manner?

•The growth of the Internet and social networks; the ability to capture, store, and analyze vast amounts of personal data; and a greater reliance on information systems in all aspects of life have increased the risk that information technology will be used unethically.

•In the midst of the many IT breakthroughs in recent years, the importance of ethics and human values has been underemphasized—with a range of consequences.

Chapter 2 Summary: Ethics for IT Workers and IT Users

What relationships must an IT worker manage, and what key ethical issues can arise in each?

•An IT worker must maintain good working relationships with employers, clients, suppliers, other professionals, IT users, and society at large. Each relationship has its own set of ethical issues and potential problems.

•In relationships between IT workers and employers, important issues include setting and enforcing policies regarding the ethical use of IT, the potential for whistle-blowing, and the safeguarding of trade secrets.

•In relationships between IT workers and clients, key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project. The IT worker must remain objective and guard against any sort of conflict of interest, fraud, misrepresentation, or breach of contract.

•A major goal for IT workers and suppliers is to develop good working relationships in which no action can be perceived as unethical.

•Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.

- Internal control is the process established by an organization's board of directors, managers, and IT group to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.

- Policies are the guidelines, standards, and laws by which the organization must abide. Policies drive processes and procedures. Processes are a collection of tasks designed to accomplish a stated objective. A procedure defines the exact instructions for completing each task in a process.

- A fundamental concept of good internal control is the careful separation of duties associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people.

- The Foreign Corrupt Practices Act (FCPA) makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office. The act applies to any U.S. citizen or company and to any company with shares listed on any U.S. stock exchange.

- In relationships between IT workers and other professionals, the priority is to improve the profession through activities such as mentoring inexperienced colleagues, demonstrating professional loyalty, and avoiding résumé inflation and the inappropriate sharing of corporate information.

•In relationships between IT professionals and IT users, important issues include software piracy, inappropriate use of IT resources, and inappropriate sharing of information.

•When it comes to the relationship between IT workers and society at large, the main challenge for IT workers is to practice the profession in ways that cause no harm to society and provide significant benefits.

What can be done to encourage the professionalism of IT workers?

•A professional is one who possess the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well.

•A professional is expected to contribute to society, to participate in a lifelong training program, to keep abreast of developments in the field, and to help develop other professionals.

•IT workers of all types can improve their profession's reputation for professionalism by (1) subscribing to a professional code of ethics, (2) joining and participating in professional organizations, (3) obtaining appropriate certifications, and (4) supporting government licensing where available.

•A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group.

•Codes of ethics usually have two main parts—the first outlines what the organization aspires to become and the second typically lists rules and principles that members are expected to live by. The codes also typically include a commitment to continuing education for those who practice the profession.

•Adherence to a code of ethics can produce many benefits for the individual, the profession, and society as a whole, including ethical decision making, high standards of practice and ethical behavior, trust and respect with the general public, and access to an evaluation benchmark that can be used for self-assessment.

•Several IT-related professional organizations have developed a code of ethics, including ACM, IEEE-CS, AITP, and SANS.

•Many people believe that the licensing and certification of IT workers would increase the reliability and effectiveness of information systems.

•Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Numerous companies and professional organization offer certification.

•Most states support the licensing of software engineers, and the state licensing boards have ultimate responsibility over specific requirements for licensing in their jurisdiction.

<u>What ethical issues do IT users face, and what can be done to encourage their ethical behavior?</u>

•IT users face several common ethical issues, including software piracy, inappropriate use of computing resources, and inappropriate sharing of information.

•Actions that can be taken to encourage the ethical behavior of IT users include establishing guidelines for the use of company hardware and software; defining an AUP for the use of IT resources; structuring information systems to protect data and information; installing and maintaining a corporate firewall; and ensuring compliance with laws, policies, and standards.

•The information security (infosec) group is responsible for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information.

•The audit committee of a board of directors and members of the internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with organizational guidelines and policies as well as various legal and regulatory practices.

Chapter 3 summary: Cyberattacks and Cybersecurity

Why are computer incidents so prevalent, and what are their effects?

•Increasing computing complexity, expanding and changing systems, an increase in the prevalence of BYOD policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents.

•An exploit is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is due to poor system design or implementation.

•Many different types of people launch computer attacks, including the black hat hacker, cracker, malicious insider, industrial spy, cybercriminal, hacktivist, and cyberterrorist. Each type has a different motivation.

•A white hat hacker is someone who has been hired by an organization to test the security of its information systems allowing the organizations to improve its defenses.

•Ransomware, viruses, worms, Trojan horses, logic bombs, blended threats, spam, DDoS attacks, rootkits, advanced persistent threats, phishing, spear phishing, smishing, vishing, cyberespionage, and cyberterrorism are among the most common computer exploits.

- The DHS has the responsibility to provide for a “safer, more secure America, which is resilient against terrorism and other potential threats.” The agency's Office of Cybersecurity and Communications is responsible for enhancing the security, resilience, and reliability of U.S. cyber and communications infrastructure.

- The US-CERT is a partnership between DHS and the public and private sectors that was established to protect the nation's Internet infrastructure against cyberattacks by serving as a clearinghouse for information on new viruses, worms, and other computer security topics.

- Over the years, several laws have been enacted to prosecute those responsible for computer-related crime, including the Computer Fraud and Abuse Act, the Fraud and Related Activity in Connection with Access Devices Statute, the Stored Wire and Electronic Communications and Transactional Records Access Statutes, and the USA Patriot Act.

What can be done to implement a strong security program to prevent cyberattacks?

- The IT security practices of organizations worldwide must be focused on ensuring confidentiality, maintaining integrity, and guaranteeing the availability of their systems and data.

Confidentiality, integrity, and availability are referred to as the CIA security triad.

•An organization's security strategy must include security measures that are planned for, designed, implemented, tested, and maintained at the organization, network, application, and end-user levels.

•Every organization needs a risk-based strategy with an active governance process to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack. Key elements of such a strategy include a risk assessment to identify and prioritize the threats that the organization faces, a well-defined disaster recovery plan that ensures the availability of key data and information technology assets, definition of security policies needed to guide employees to follow recommended processes and practices to avoid security-related problems, periodic security audits to ensure that individuals are following established policies and to assess if the policies are still adequate even under changing conditions, compliance standards defined by external parties, and use of a security dashboard to help track the key performance indicators of their security strategy.

•The concept of reasonable assurance in connection with IT security 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.

- Authentication methods, a firewall, routers, encryption, proxy servers, VPN, and an IDS are key elements of the network security layer.
- Authentication methods, user roles and accounts, and data encryption are key elements of the application security layer.
- Security education, authentication methods, antivirus software, and data encryption are key elements of the end-user security layer.

What actions must be taken in the event of a successful security intrusion?

- No security system is perfect, so systems and procedures must be monitored to detect a possible intrusion. A response plan should be developed well in advance of any incident and be approved by both the organization's legal department and senior management. The response plan should address notification, evidence protection, activity log maintenance, containment, eradication, and follow-up.
- Organizations must implement fixes against well-known vulnerabilities and conduct periodic IT security audits.
- Many organizations outsource their network security operations to a MSSP, which is a company that monitors, manages, and maintains computer and network security for other organizations.

•Organizations must be knowledgeable of and have access to trained experts in computer forensics 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.

Chapter 4 summary: Privacy

What is the right of privacy, and what is the basis for protecting personal privacy under the law?

•The right of privacy is "the right to be left alone—the most comprehensive of rights, and the right most valued by a free people."

•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).

•The use of information technology in business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used. A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales.

•The Fourth Amendment reads, “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.” The courts have ruled that without a reasonable expectation of privacy, there is no privacy right to protect.

•Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. For many, the existing hodgepodge of privacy laws and practices fails to provide adequate protection and fuels a sense of distrust and skepticism, and concerns over identity theft.

What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?

•Few laws provide privacy protection from private industry and there is no single, overarching national data privacy policy for the United States.

•The Fair Credit Reporting Act regulates operations of credit reporting bureaus.

•The Right to Financial Privacy Act protects the financial records of financial institution customers from unauthorized scrutiny by the federal government.

•The GLBA established mandatory guidelines for the collection and disclosure of personal financial information by financial institutions; requires financial institutions to document their data security plans; and encourages institutions to implement safeguards against pretexting.

•The Fair and Accurate Credit Transaction Act allows consumers to request and obtain a free credit report each year from each of the three consumer credit reporting agencies.

•The HIPAA defined numerous standards to improve the portability and continuity of health insurance coverage; reduce fraud, waste, and abuse in health insurance care and healthcare delivery; and simplify the administration of health insurance.

•The American Recovery and Reinvestment Act included strong privacy provisions for EHRs, including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients. It also mandated that each individual whose health information has been exposed be notified within 60 days after discovery of a data breach.

•The FERPA provides students and their parents with specific rights regarding the release of student records.

•The COPPA requires websites that cater to children to offer comprehensive privacy policies, notify parents or guardians about their data collection practices, and receive parental consent before collecting any personal information from children under the age of 13.

•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 FISA describes procedures for the electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers.

•Executive Order 12333 identifies the various government intelligence-gathering agencies and defines what information can be collected, retained, and disseminated by the agencies. It allows for the tangential collection of U.S. citizen data—even when those citizens are not specifically targeted.

•The ECPA deals with the protection of communications while in transit from sender to receiver; the protection of communications held in electronic storage; and the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant.

•The CALEA requires the telecommunications industry to build tools into its products that federal investigators can use—after gaining a court order—to eavesdrop on conversations and intercept electronic communications.

•The USA PATRIOT Act modified 15 existing statutes and gave sweeping new powers both to domestic law enforcement and to international intelligence agencies, including increasing the ability of law enforcement agencies to eavesdrop on telephone communication, intercept email messages, and search medical, financial, and other records; the act also eased restrictions on foreign intelligence gathering in the United States.

•The Foreign Intelligence Surveillance Act Amendments Act of 2004 authorized intelligence gathering on individuals not affiliated with any known terrorist organization (so-called lone wolves).

•The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 granted the NSA expanded authority to collect, without court-approved warrants, international communications as they flow through the U.S. telecommunications equipment and facilities.

•The PATRIOT Sunsets Extension Act granted a four-year extension of provisions of the USA PATRIOT Act that allowed roving wiretaps and searches of business records. It also extended authorization intelligence gathering on "lone wolves."

•USA Freedom Act terminated the bulk collection of telephone metadata by the NSA instead requiring telecommunications carriers to hold the data and respond to NSA queries for data.

The act also restored authorization for roving wiretaps and the tracking of lone wolf terrorists.

•“Fair information practices” is a term for a set of guidelines that govern the collection and use of personal data. Various organizations as well as countries have developed their own set of such guidelines and call them by different names.

•The OECD for the Protection of Privacy and Transborder Data Flows of Personal Data created a set of fair information practices that are often held up as the model for organizations to adopt for the ethical treatment of consumer data.

•The European Union Data Protection Directive requires member countries to ensure that data transferred to non-EU countries is protected. It also bars the export of data to countries that do not have data privacy protection standards comparable to those of the EU. After the passage of this directive, the EU and the United States worked out an agreement that allowed U.S. companies that were certified as meeting certain “safe harbor” principles to process and store data of European consumers and companies.

•The European–United States Privacy Shield Data Transfer Program Guidelines is a stopgap measure that allows businesses to transfer personal data about European citizens to the United States. The guidelines were established after the European Court of Justice declared invalid the Safe Harbor agreement between the EU and the United States.

- The GDPR takes effect in May 2018 and addresses the export of personal data outside the EU enabling citizens to see and correct their personal data, standardizing data privacy regulations within the EU, and establishing substantial penalties for violation of its guidelines.
- The FOIA grants citizens the right to access certain information and records of the federal government upon request.
- The Privacy Act prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system.

<u>What are the various strategies for consumer profiling, and what are the associated ethical issues?</u>

- Companies use many different methods to collect personal data about visitors to their websites, including depositing cookies on visitors' hard drives.
- Consumer data privacy has become a major marketing issue—companies that cannot protect or do not respect customer information have lost business and have become defendants in class actions stemming from privacy violations.
- A data breach is the unintended release of sensitive data or the access of sensitive data (e.g., credit card numbers, health insurance member ids, and Social Security numbers) by unauthorized individuals. The increasing number of data breaches is alarming, as is the lack of initiative by some

companies in informing the people whose data are stolen. A number of states have passed data breach notifications laws that require companies to notify affected customers on a timely basis.

What is e-discovery, and how is it being used?

•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.

•E-discovery is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings.

•Predictive coding is a process that couples human intelligence with computer-driven concept searching in order to “train” document review software to recognize relevant documents within a document universe.

Why and how are employers increasingly using workplace monitoring?

•Many organizations have developed IT usage policies to protect against employee abuses that can reduce worker productivity and expose employers to harassment lawsuits.

- About 80 percent of U.S. firms record and review employee communications and activities on the job, including phone calls, email, web surfing, and computer files.
- The use of fitness trackers in the workplace has opened up potential new legal and ethical issues.

What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

- Surveillance cameras are used in major cities around the world to deter crime and terrorist activities. Critics believe that such security is a violation of civil liberties.
- An 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. The fact that most cars now come equipped with an EDR and that the data from this device may be used as evidence in a court of law is not broadly known by the public.
- Stalking apps can be downloaded onto a person's cell phone, making it possible to perform location tracking, record calls and conversations, view every text and photograph sent or received, and record the URLs of any website visited on that phone.

Chapter 5: Freedom of Expression

What is the basis for the protection of freedom of expression in the United States, and what types of expressions are not protected under the law?

•The First Amendment protects Americans' rights to freedom of religion, freedom of expression, and freedom to assemble peaceably. The Supreme Court has ruled that the First Amendment also protects the right to speak anonymously.

•Obscene speech, defamation, incitement of panic, incitement to crime, "fighting words," and sedition are not protected by the First Amendment and may be forbidden by the government.

What are some key federal laws that affect online freedom of expression, and how do they impact organizations?

•Although there are clear and convincing arguments to support freedom of speech on the Internet, the issue is complicated by the ease with which children can use the Internet to gain access to material that many parents and others feel is inappropriate for children. The conundrum is that it is difficult to restrict children's Internet access without also restricting adults' access.

•The U.S. government has passed several laws to attempt to address this issue, including the Communications Decency Act

(CDA), which is aimed at protecting children from online pornography, and the Child Online Protection Act (COPA), which prohibits making harmful material available to minors via the Internet. Both laws were ultimately ruled largely unconstitutional. However, Section 230 of the CDA, which was not ruled unconstitutional, provides immunity from defamation charges to ISPs that publish user-generated content, as long as they do not also serve as a content provider.

•Software manufacturers have developed Internet filters, which are designed to block access to objectionable material through a combination of URL, keyword, and dynamic content filtering.

•The Children's Internet Protection Act (CIPA) requires federally financed schools and libraries to use filters to block computer access to any material considered harmful to minors. In United States v. American Library Association, Inc., the American Library Association challenged CIPA. Ultimately in that case, the Supreme Court made it clear that the constitutionality of government-mandated filtering schemes depends on adult patrons' ability to request and receive unrestricted access to protected speech.

•The Digital Millennium Copyright Act (DMCA) addresses a number of copyright-related issues, with Title II of the act providing limitations on the liability of an ISP for copyright infringement.

<u>What important freedom of expression issues relate to the use of information technology?</u>

•Internet censorship is the control or suppression of the publishing or accessing of information on the Internet. There are many forms of Internet censorship. Many countries practice some form of Internet censorship.

•A SLAPP (strategic lawsuit against public participation) is a lawsuit filed by corporations, government officials, and others against citizens and community groups who oppose them on matters of concern. Anti-SLAPP laws are designed to reduce frivolous SLAPPs. As of 2015, 28 states and the District of Columbia have put into effect anti-SLAPP legislation to protect people who are the target of a SLAPP.

•Anonymous expression is the expression of opinions by people who do not reveal their identity. The freedom to express an opinion without fear of reprisal is an important right of a democratic society. Anonymity is even more important in countries that don’t allow free speech. Maintaining anonymity on the Internet is important to some computer users. Such users sometimes use an anonymous re-mailer service, which strips the originating header and/or IP address from the message and then forwards the message to its intended recipient.

•Doxing involves doing research on the Internet to obtain someone’s private personal information (such as home address, email address, phone numbers, and place of employment) and even private electronic documents (such as photographs), and then posting that information online without permission.

•Many businesses monitor the web for the public expression of opinions that might hurt their reputations. They also try to guard against the public sharing of company confidential information.

•Organizations may file a John Doe lawsuit to enable them to gain subpoena power in an effort to learn the identity of anonymous Internet users who they believe have caused some form of harm to the organization through their postings.

•In the United States, speech that is merely annoying, critical, demeaning, or offensive enjoys protection under the First Amendment. Legal recourse is possible only when hate speech turns into clear threats and intimidation against specific citizens.

•Some ISPs and social networking sites have voluntarily agreed to prohibit their subscribers and members from sending hate messages using their services. Because such prohibitions can be included in the service contracts between a private ISP and its subscribers or a social networking site and it members—and do not involve the federal government—they do not violate subscribers’ First Amendment rights.

•Many adults, including some free-speech advocates, believe there is nothing illegal or wrong about purchasing adult pornographic material made by and for consenting adults. However, organizations must be very careful when dealing with pornography in the workplace. As long as companies can show that they were taking reasonable steps to prevent pornography, they have a valid defense if they are subject to a sexual harassment lawsuit.

•Reasonable steps include establishing a computer usage policy that prohibits access to pornography sites, identifying those who violate the policy, and taking action against those users—regardless of how embarrassing it is for the users or how harmful it might be for the company.

•Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend that can lead to many problems for both senders and receivers.

•The Controlling the Assault of Non Solicited Pornography and Marketing (CAN-SPAM) Act specifies requirements that commercial emailers must follow when sending out messages that advertise a commercial product or service. The CAN-SPAM Act is also sometimes used in the fight against the dissemination of pornography.

•The proliferation of online sources of information and opinion means that the Internet is full of “news” accounts that are, in fact, highly opinionated, fictionalized, or satirical accounts of current events presented in journalistic style.

Chapter 6 summary: Intellectual property

What does the term intellectual property encompass, and what measures can organizations take to protect their intellectual property?

•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.

•Copyrights, patents, trademarks, and trade secrets form a complex body of law relating to the ownership of intellectual property, which represents a large and valuable asset to most companies. If these assets are not protected, other companies can copy or steal them, resulting in significant loss of revenue and competitive advantage.

•A copyright is the exclusive right to distribute, display, perform, or reproduce an original work in copies; to prepare derivative works based on the work; to and grant these exclusive rights to others.

•Copyright infringement is a violation of the rights secured by the owner of a copyright. Infringement occurs when someone copies a substantial and material part of another’s copyrighted work without permission.

•Copyright law has proven to be extremely flexible in covering new technologies, including software, video games, multimedia works, and web pages. However, evaluating the originality of a work can be difficult and disagreements over whether or not a work is original sometimes lead to litigation.

•Copyrights provide less protection for software than patents; software that produces the same result in a slightly different way may not infringe a copyright if no copying occurred.

•The fair use doctrine established four factors for courts to consider when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the portion of the copyrighted work used, and (4) the effect of the use on the value of the copyrighted work.

•The use of copyright to protect computer software raises many complicated issues of interpretation of what constitutes infringement.

•The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 increased trademark and copyright enforcement; it also substantially increased penalties for infringement.

•The original General Agreement on Tariffs and Trade (GATT), signed in 1993, created the World Trade Organization (WTO) in Geneva, Switzerland, to enforce compliance with the agreement. GATT includes a section covering copyrights called the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

•The WTO is a global organization that deals with rules of international trade based on WTO agreements that are negotiated and signed by representatives of the world’s trading nations The goal of the WTO is to help producers of goods and services, exporters, and importers conduct their business.

•The World Intellectual Property Organization (WIPO) is an agency of the United Nations dedicated to “the use of intellectual property as a means to stimulate innovation and creativity.”

•The Digital Millennium Copyright Act (DMCA), which was signed into law in 1998, implements two WIPO treaties in the United States. The DMCA also makes it illegal to circumvent a technical protection or develop and provide tools that allow others to access a technologically protected work. In addition, the DMCA limits the liability of Internet service providers for copyright infringement by their subscribers or customers.

•Some view the DMCA as a boom to the growth of the Internet and its use as a conduit for innovation and freedom of expression. Others believe that the DMCA has given excessive powers to copyright holders.

•A patent is a grant of property right issued by the U.S. Patent and Trademark Office (USPTO) to an inventor that permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators. A patent prevents copying as well as independent creation (which is allowable under copyright law).

•For an invention to be eligible for a patent, it must fall into one of three statutory classes of items that can be patented: (1) it must be useful, (2) it must be novel, and (3) it must not be obvious to a person having ordinary skill in the same field.

•A utility patent is "issued for the invention of a new and useful process, machine, manufacture, or composition of matter, or a new and useful improvement thereof." A design patent, which is "issued for a new, original, and ornamental design embodied in or applied to an article of manufacture," permits its owner to exclude others from making, using, or selling the design in question.

•Unlike copyright infringement, for which monetary penalties are limited to certain specified dollar amounts, if the court determines that a patent has been intentionally infringed, it can award up to triple the amount of the damages claimed by the patent holder.

•The Leahy-Smith America Invents Act changed the U.S. patent system from a "first-to-invent" to a "first-inventor-to file" system and expanded the definition of prior art, which is used to determine the novelty of an invention and whether it can be patented. The act made it more difficult to obtain a patent in the United States.

•The courts and the U.S. Patent and Trademark Office (USPTO) have changed their attitudes and opinions of the patenting of software over the years.

•To qualify as a trade secret, information must have economic value and must not be readily ascertainable. In addition, the trade secret's owner must have taken steps to maintain its secrecy. Trade secret laws do not prevent someone from using the same idea if it was developed independently or from analyzing an end product to figure out the trade secret behind it.

•Trade secrets are protected by the Uniform Trade Secrets Act, the Economic Espionage Act, and the Defend Trade Secrets Act, which amended the Economic Espionage Act to create a federal civil remedy for trade secret misappropriation.

•Trade secret law has three key advantages over the use of patents and copyrights in protecting companies from losing control of their intellectual property: (1) There are no time limitations on the protection of trade secrets, unlike patents and copyrights; (2) there is no need to file any application or otherwise disclose a trade secret to outsiders to gain protection; and (3) there is no risk that a trade secret might be found invalid in court.

•Because organizations can risk losing trade secrets when key employees leave, they often try to prohibit employees from revealing secrets by adding nondisclosure clauses to employment contracts. 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 competitors for a period of time, often one to two years.

What are some of the current issues associated with the protection of intellectual property?

•Plagiarism is the act of stealing someone’s ideas or words and passing them off as one’s own. Plagiarism detection systems enable people to check the originality of documents and manuscripts.

•Reverse engineering is the process of breaking something down in order to understand it, build a copy of it, or improve it. It was originally applied to computer hardware but is now commonly applied to software.

•In some situations, reverse engineering might be considered unethical because it enables access to information that another organization may have copyrighted or classified as a trade secret.

•Recent court rulings and software license agreements that forbid reverse engineering, as well as restrictions in the DMCA, have made reverse engineering a riskier proposition in the United States.

- Open source code is any program whose source code is made available for use or modification, as users or other developers see fit. The basic premise behind open source code is that when many programmers can read, redistribute, and modify it, the software improves. Open source code can be adapted to meet new needs, and bugs can be rapidly identified and fixed.

- Competitive intelligence is legally obtained information that is gathered to help a company gain an advantage over its rivals. It is not the same as industrial espionage, which is the use of illegal means to obtain business information that is not readily available to the general public. In the United States, industrial espionage is a serious crime that carries heavy penalties.

- Competitive intelligence analysts must take care to avoid unethical or illegal behavior, including lying, misrepresentation, theft, bribery, or eavesdropping with illegal devices.

- A trademark is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's. Website owners who sell trademarked goods or services must take care to ensure they are not sued for trademark infringement.

- Cybersquatters register domain names for famous trademarks or company names to which they have no connection, with the hope that the trademark's owner will eventually buy the domain name for a large sum of money.

•The main tactic organizations use to circumvent cybersquatting is to protect a trademark by registering numerous domain names and variations as soon as they know they want to develop a web presence.

Chapter 7 Summary: Ethical Decisions in Software Development

What is meant by software quality, why is it so important, and what potential ethical issues do software manufacturers face when making decisions that involve trade-offs between project schedules, project costs, and software quality?

•High-quality software systems are easy to learn and use. They perform quickly and efficiently to meet their users' needs, operate safely and reliably, and have a high degree of availability that keeps unexpected downtime to a minimum.

•High-quality software has long been required to support the fields of air traffic control, nuclear power, automobile safety, health care, military and defense, and space exploration.

•Computers and software are integral parts of almost every business, and the demand for high-quality software is increasing. End users cannot afford system crashes, lost work, or lower productivity. Nor can they tolerate security holes through which intruders can spread viruses, steal data, or shut down websites.

•A software defect is any error that, if not removed, could cause a software system to fail to meet its users' needs.

•Software quality is the degree to which a software product meets the needs of its users. Quality management focuses on defining, measuring, and refining the quality of the development process and the products developed during its various stages.

•Software developers are under extreme pressure to reduce the time to market of their products. They are driven by the need to beat the competition in delivering new functionality to users, to begin generating revenue to recover the cost of development, and to show a profit for shareholders.

•The resources and time needed to ensure quality are often cut under the intense pressure to ship a new software product. When forced to choose between adding more user features and doing more testing, many software companies decide in favor of more features.

•A business information system is a set of interrelated components—including hardware, software, databases, networks, people, and procedures—that collects and processes data and disseminates the output.

•Software product liability claims are typically based on strict liability, negligence, breach of warranty, or misrepresentation—sometimes in combination. Strict liability means that the defendant is held responsible for injuring another person regardless of negligence or intent.

•A warranty assures buyers or lessees that a product meets certain standards of quality and may be either expressly stated or implied by law. If the product fails to meet the terms of its warranty, the buyer or lessee can sue for breach of warranty.

<u>What are some effective strategies for developing quality systems?</u>

•A software development methodology is a standard, proven work process that enables systems analysts, programmers, project managers, and others to make controlled and orderly progress in developing high-quality software. Software methodologies define the activities in the software development process as well as the individual and group responsibilities for accomplishing objectives, recommend specific techniques for accomplishing the objectives, and offer guidelines for managing the quality of the products during the various stages of the development cycle.

•The waterfall system development model is a sequential, multistage system development process in which development of the next stage of the system cannot begin until the results of the current stage are approved or modified as necessary.

•Under the agile development methodology, a system is developed in iterations (often called sprints), lasting from one to four weeks. Agile development, which accepts the fact that system requirements are evolving and cannot be fully understood or defined at the start of the project, concentrates on maximizing the team’s ability to deliver quickly and respond to emerging requirements.

•Using an effective development methodology enables a manufacturer to produce high-quality software, forecast project-completion milestones, and reduce the overall cost to develop and support software. An effective development methodology can also help protect software manufacturers from legal liability for defective software in two ways: by reducing the number of software errors that could cause damage and by making negligence more difficult to prove.

•The cost to identify and remove a defect in the early stages of software development can be up to 100 times less than removing a defect in a piece of software that has been distributed to customers.

•Quality assurance (QA) refers to methods within the development process that are designed to guarantee reliable operation of a product. Ideally, these methods are applied at each stage of the development cycle.

- There are several tests employed in software development including black-box and white-box dynamic testing, static testing, unit testing, integration testing, system testing, and user acceptance testing.

- Capability Maturity Model Integration (CMMI) models are collections of best practices that help organizations improve their processes. A best practice is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark within a particular industry. CMMI-Development (CMMI-DEV)—is frequently used to assess and improve software development practices.

- CMMI defines five levels of software development maturity: initial, managed, defined, quantitatively managed, and optimizing. CMMI identifies the issues that are most critical to software quality and process improvement. Its use can improve an organization’s ability to predict and control quality, schedule, costs, and productivity when acquiring, building, or enhancing software systems. CMMI also helps software engineers analyze, predict, and control selected properties of software systems.

- A safety-critical system is one whose failure may cause human injury or death. In the development of safety-critical systems, a key assumption is that safety will not automatically result from following an organization’s standard software development methodology.

- Safety-critical software must go through a much more rigorous and time-consuming development and testing process than other kinds of software; the appointment of a project safety engineer and the use of a hazard log and risk analysis are common in the development of safety-critical software.
- Risk is the potential of gaining or losing something of value. Risk can be quantified by three elements: a risk event, the probability of the event happening, and the impact (positive or negative) on the business outcome if the risk does actually occur.
- The annualized rate of occurrence (ARO) is an estimate of the probability that an event will occur over the course of a year. The single loss expectancy (SLE) is the estimated loss that would be incurred if the event happens. The annualized loss expectancy (ALE) is the estimated loss from this risk over the course of a year.
- The following equation is used to calculate the annual loss expectancy: ARO × SLE = ALE.
- Risk management is the process of identifying, monitoring, and limiting risks to a level that an organization is willing to accept.
- Reliability is a measure of the rate of failure in a system that would render it unusable over its expected lifetime.
- The International Organization for Standardization (ISO) issued its 9000 series of business management standards in 1988.

These standards require organizations to develop formal quality management systems that focus on identifying and meeting the needs, desires, and expectations of their customers.

•The ISO 9001 family of standards serves as a guide to quality products, services, and management; it provides a set of standardized requirements for a quality management system. Many businesses and government agencies specify that a vendor must be ISO 9001 certified to win a contract from them.

•Failure mode and effects analysis (FMEA) is an important technique used to develop ISO 9001–compliant quality systems. FMEA is used to evaluate reliability and determine the effects of system and equipment failures.

Chapter 8 summary: The Impact of Information Technology on Society

What is the relationship between IT investment and productivity growth in the United States?

•The most widely used measurement of the material standard of living is gross domestic product (GDP) per capita.

•In the United States, as in most developed nations, the standard of living has been improving over time. However, its rate of change varies as a result of business cycles that affect prices, wages, employment levels, and the production of goods and services.

•Labor productivity is a measure of the economic performance that compares the amount of goods and services produced with the number of labor hours used in producing those goods and services.

•Most countries have been able to produce more goods and services over time—not through a proportional increase in labor but rather by making production more efficient. These gains in productivity have led to increases in the GDP-based standard of living because the average hour of labor produced more goods and services.

•Innovation is a key factor in productivity improvement, and IT has played an important role in enabling innovation. Organizations use IT, other new technology, and capital investment to implement innovations in products, processes, and services.

•It can be difficult to quantify the benefits of IT investments on worker productivity because there can be a considerable lag between the application of innovative IT solutions and the capture of significant productivity gains. In addition, many factors other than IT influence worker productivity rates.

How will artificial intelligence, machine learning, robotics, and natural language processing affect the future workforce?

•Advances in artificial intelligence, machine learning, robotics, and natural language processing are fundamentally changing the way work gets done and have the potential to affect the tasks, roles, and responsibilities of most workers.

•Almost every job has partial automation potential and research suggests that 45 percent of human work activities could be automated using existing technology.

•It is likely to take decades for automation to achieve anywhere near its full potential.

•Artificial intelligence systems can simulate human intelligence processes, including learning, reasoning, and self-correction.

•Machine learning, a type of artificial intelligence (AI), involves computer programs that can learn some task and improve their performance with experience.

•Robotics is a branch of engineering that involves the development and manufacture of mechanical or computer devices that can perform tasks that require a high degree of precision or that are tedious or hazardous for human beings.

•Natural language processing is an aspect of artificial intelligence that involves technology that allows computers to understand, analyze, manipulate, and/or generate “natural languages” such as English.

What impact has the application of IT had on health care?

- Healthcare costs in the United States are expected to increase an average of 5.6 percent per year from 2016 to 2025.
- Much of this increase is due to the continued aging of the population, government policy, and lifestyle changes, and to a lesser extent the development and use of new medical technology.
- In order for the United States to rein in healthcare spending, patient awareness must be raised and technology costs must be managed more carefully.
- An electronic medical record (EMR) is a collection of health-related information on an individual that is created, managed, and consulted by authorized clinicians and staff within a single healthcare organization. The information in an EMR is not easily shared with others outside of the healthcare organization where the data originated.
- An electronic health record (EHR) is a comprehensive view of the patient's complete medical history designed to be shared with authorized providers and staff from more than one organization.
- Health information exchange (HIE) is the process of sharing patient-level electronic health information between different organizations. HIE can result in more cost-effective and higher-quality care.
- A personal health record (PHR) includes those portions of the EHR that an individual patient "owns" and controls such as

personal identifiers, contact information, health provider information, problem list, medication history, allergies, immunizations, and lab and test results.

•Clinical decision support (C D S) is a process and a set of tools designed to enhance health-related decision making through the use of clinical knowledge and patient-specific information to improve healthcare delivery. Effective use of C D S systems increases the quality of patient care while at the same time cutting costs.

•A computerized provider order entry (CPOE) system enables physicians to place orders (for drugs, laboratory tests, radiology, physical therapy) electronically with the orders transmitted directly to the recipient. CPOE streamlines the ordering process.

•Telehealth employs modern telecommunications and information technologies to provide medical care to people who live or work far away from healthcare providers, provide professional and patient health related training, and support healthcare administration.

•Telemedicine is the component of telehealth that provides medical care to people at a location different from the healthcare providers. Telemedicine helps reduce the need for patients to travel for treatment and allows healthcare professionals to serve more patients in a broader geographic area.

•Store-and-forward telemedicine involves acquiring data, sound, images, and video from a patient and then transmitting everything to a medical specialist for later evaluation.

Chapter 9 summary: Social Media

How do individuals use social networks, and what are some practical business uses of social networking and other social media tools?

•Social media are web-based communication channels and tools that enable people to interact with each other by creating online communities where they can share information, ideas, messages, and other content, including images, audio, and video.

•A social networking platform creates an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences; such a site allows people to interact with others online by sharing opinions, insights, information, interests, and experiences.

•The number of Internet users worldwide is approaching 4 billion or roughly half the population.

- Many organizations employ social networking platforms to advertise, identify and access job candidates, improve customer service, and sell products and services.

- An increasing number of business-oriented social networking platforms are designed to encourage and support relationships with consumers, clients, potential employees, suppliers, and business partners around the world.

- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services.

- Two significant advantages of social media marketing over traditional marketing are that marketers can create a conversation with viewers of their ads and that ads can be targeted to reach people with the desired demographic characteristics.

- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services. The two primary objectives of social media marketers are raising brand awareness and driving traffic to a website to increase product sales.

- Organic media marketing employs tools provided by or tailored for a particular social media platform to build a social community and interact with it by sharing posts and responding to customer comments on the organization's blog and social media accounts.

•Paid media marketing involves paying a third party to broadcast an organization's display ads or sponsored messages to social network users. Two common methods of charging for paid media are cost per thousand impressions and cost per click.

•Earned media refers to media exposure an organization gets through press and social media mentions, positive online ratings and reviews, tweets and retweets, reposts (or "shares"), recommendations, and so on. Earned social media traffic enables an organization to reach more people without any additional cost.

•Viral marketing is an approach to social media marketing that encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence.

•Some 60 percent of employers used social media to research job candidates with half of those finding information that gave a negative impression of the candidate.

•Employers can legally reject a job applicant based on the contents of the individual's social networking profile as long as the company is not violating federal or state discrimination laws.

•Job seeking candidates should review their presence on social media and remove photos and postings that portray them in a potentially negative light. Many jobseekers delete their social media accounts altogether.

•Increasingly, consumers are using social networks to share their experiences, both good and bad, with others. Because of this, many organizations actively monitor social media networks as a means of improving customer service, retaining customers, and increasing sales.

•A social shopping platform brings shoppers and sellers together in a social networking environment in which members share information and make recommendations while shopping online.

What are some of the key ethical issues associated with the use of social networks and other social media?

•Cyberabuse is any form of mistreatment or lack of care, both physical and mental, based on the use of an electronic communications device that causes harm and distress to others.

•Nearly three-quarters of U.S. Internet users have witnessed online harassment or abuse and almost half have personally experienced it.

•Cyberharassment is a form of cyberabuse in which the abusive behavior, which involves the use of an electronic communications device, is degrading, humiliating, hurtful, insulting, intimidating, malicious, or otherwise offensive to an individual or group of individuals causing substantial emotional distress.

•Cyberstalking is also a form of Cyberabuse that consists of a long-term pattern of unwanted persistent pursuit and intrusive behavior (involving the use of an electronic communications device) that is directed by one person against another that causes fear and distress in the victim.

•The National Center for Victims of Crime offers tips on how to combat cyberstalking.

•The 1994 Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act set requirements for sex offender registration and notification in the United States. It also that states create websites that provide information on sex offenders within the state.

•The Sex Offender Registration and Notification Provisions (SORNA) of the Adam Walsh Child Protection and Safety Act of 2006 set national standards that govern which sex offenders must register and what data must be captured.

•Most social networking platforms have terms of use agreements, a privacy policy, or a content code of conduct that summarizes key legal aspects regarding use of the platform. Typically, the terms state that the platform has the right to delete material and terminate user accounts that violate its policies. These policies can be difficult to enforce.

•Inappropriate material posted online includes nonconsensual posts that include intimate photos or videos of people without their permission; such posts are often referred to as “revenge porn.” This type of content is often uploaded by ex-partners with an intention to shame, embarrass, and/or harass their former partner.

•The First Amendment of the U.S. Constitution protects the right of freedom of expression from government interference, however, it does not prohibit free speech interference by private employers.

•Organizations should put in place a social media policy to avoid legal issues and set clear guidelines and expectations for employees.

•The increased risk of accidents associated with social media interaction while driving, the tendency of many social media users to become narcissist in their postings, and the ability to perform self-image manipulation are additional social media issues.

Chapter 10 summary: Ethics of IT Organizations

What key legal and ethical issues are associated with the use of contingent workers, H-1B visa holders, and offshore outsourcing companies?

•Contingent work is a job situation in which an individual does not have an explicit or implicit contract for long-term employment.

•Organizations can obtain contingent workers through temporary staffing firms, employee leasing organizations, and professional employment organizations.

•Temporary staffing firms recruit, train, and test job seekers in a wide range of job categories and skill levels, and then assign them to clients as needed.

•In employee leasing, the subscribing firm transfers all or part of its workforce to the leasing firm, which handles all human-resource-related activities and costs such as payroll, training, and the administration of employee benefits. The subscribing firm leases these workers, but they remain employees of the leasing firm.

•A coemployment relationship is one in which two employers have actual or potential legal rights and duties with respect to the same employee or group of employees.

•A Professional Employer Organization (PEO) is a business entity that hires the employees of its clients and then assumes all responsibility for all human resource management functions, including administration of benefits. The client company remains responsible for directing and controlling the daily activities of the employees. The client maintains a long-term investment and commitment to the employees, but uses the PEO as a means to outsource the human resource activities.

•The gig economy refers to a work environment in which temporary positions are common and organizations contract with independent workers for short-term engagements.

•An independent contractor is an individual who provides services to another individual or organization according to terms defined in a written contract or within a verbal agreement.

•Organizations that use contingent workers must be extremely careful how they pay and treat these workers, or run the risk of getting dragged into a class action lawsuit over mis-classification of workers.

•When a firm employs a contingent worker, it does not usually have to provide benefits, can easily adjust the number of workers to meet its business needs, and does not incur training costs.

•Contingent workers may have a low level of commitment to the company and its projects. The skills and knowledge a contingent worker gains while working for a particular are lost when the worker departs at a project's completion.

•An H-1B is a temporary work visa granted by the U.S. Citizenship and Immigration Services (USCIS) for people who work in specialty occupations—jobs that require at least a four-year bachelor's degree in a specific field, or equivalent experience.

•Employers hire H-1B workers to meet critical business needs or to obtain essential technical skills or knowledge that cannot be readily found in the United States. H-1B workers may also be used when there are temporary shortages of needed skills.

•Congress sets an annual cap on the number of H-1B visas to be granted—although the number of visas issued often varies greatly from this cap due to various exceptions.

•Companies applying for H-1B visas must offer a wage that is at least 95 percent of the average salary for the occupation. Because wages in the IT field vary substantially, unethical companies can get around the average salary requirement.

•Companies that employ H-1B workers are required to declare that they will not displace American workers; however, they are exempt from that requirement if 15 percent of more of their workers are on H-1B visas and the H-1B workers are paid at least $60,000 a year.

•Many U.S. companies complain they have trouble finding enough qualified workers and urge that the cap on visas be raised. Unemployed and displaced IT workers challenge whether the United States needs to continue importing tens of thousands of H-1B workers each year.

•The number of degrees awarded in the field of computer and information sciences at post-secondary institutions in the United States reached 130,000 in 2015. The Bureau of Labor Statistics has projected an increase of 53,000 new U.S. tech jobs per year from 2014 to 2024.

•Opinions vary as to whether or not the hiring of H-1B workers affects job opportunities and wages.

•Outsourcing is a long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a specific function.

•Offshore outsourcing is a form of outsourcing in which the services are provided by an organization whose employees are in a foreign country.

•Outsourcing and offshore outsourcing are used to meet staffing needs while potentially reducing costs and speeding up project schedules.

•Many of the same ethical issues that arise when considering whether to hire H-1B and contingent workers apply to outsourcing and offshore outsourcing.

•Successful offshoring projects require day-to-day interaction between software development and business teams, so it is essential for the hiring company to take a hands-on approach to project management.

What is whistle-blowing, and what ethical issues are associated with it?

•Whistle-blowing is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.

•Whistle-blower protection laws allow employees to alert the proper authorities to employer actions that are unethical, illegal, or unsafe, or that violate specific public policies. Unfortunately, no comprehensive federal law protects all whistle-blowers from retaliatory acts.

•A potential whistle-blower must consider many ethical implications prior to going public with his or her allegations, including whether the high price of whistle-blowing is worth it;

whether all other means of dealing with the problem have been exhausted; whether whistle-blowing violates the obligation of loyalty that the employee owes to his or her employer; and whether public exposure of the problem will actually correct its underlying cause and protect others from harm.

•An effective whistle-blowing process includes the following steps: (1) assess the seriousness of the situation, (2) begin documentation, (3) attempt to address the situation internally, (4) consider escalating the situation within the company, (5) assess the implications of becoming a whistle-blower, (6) use experienced resources to develop an action plan, (7) execute the action plan, and (8) live with the consequences.

What is green computing, and what are organizations doing to support this initiative?

•Green computing is concerned with the efficient and environmentally responsible design, manufacture, operation, and disposal of IT-related products.

•Green computing has three goals: (1) reduce the use of hazardous material, (2) allow companies to lower their power-related costs, and (3) enable the safe disposal or recycling of computers and computer-related equipment.

•Electronic Product Environmental Assessment Tool (EPEAT) is a system that enables purchasers to evaluate, compare, and select electronic products based on 51 environmental criteria.

•The European Union passed the Restriction of Hazardous Substances Directive to restrict the use of many hazardous materials in computer manufacturing, require manufacturers to use at least 65 percent reusable or recyclable components, implement a plan to manage products at the end of their life cycle in an environmentally safe manner, and reduce or eliminate toxic material in their packaging.

Ethics in Technology
Acronym Glossary

ACPA (Anti-cybersquatting Consumer Protection Act): An act that allows trademark owners to challenge foreign cybersquatters otherwise beyond the jurisdiction of U.S. courts.

AI (Artificial Intelligence)

AIA (Leahy-Smith America Invents Act): An act that changed the U.S. patent system so that the first person to file with the U.S. Patent and Trademark Office will receive the patent, not necessarily the person who actually invented the item first.

APT (Advanced Persistent Threat): A network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time (weeks or even months).

AUP (Acceptable Use Policy): A document that stipulates restrictions and practices that a user must agree in order to use organizational computing and network resources.

BSA | The Software Alliance (Business Software Alliance): The trade groups that represent the world's largest software and hardware manufacturers.

BYOD (Bring Your Own Device): 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.

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart): Software that generates and grades tests that humans can pass and all but the most sophisticated computer programs cannot.

CDS (Clinical Decision Support): A process and a set of tools designed to enhance healthcare-related decision making through the use of clinical knowledge and patient-specific information to improve healthcare delivery.

CDA (Communications Decency Act): Title V of the Telecommunications Act, it aimed at protecting children from pornography, including imposing $250,000 fines and prison terms of up to two years for the transmission of "indecent" material over the internet.

COPA (Child Online Protection Act): An act signed into law in 1998 with the aim of prohibiting the making of harmful material available to minors via the internet; the law was ultimately ruled largely unconstitutional.

COPPA: (Children's Online Privacy Protection Act): An act that requires U.S.-based websites that collect personal information from people under the age of 13 to obtain permission from parents or guardians before asking for such data.

CIPA (Children's Internet Protection Act): An act passed in 2000; it required federally financed schools and libraries to use some form of technological protection (such as an internet filter) to block computer access to obscene material, pornography, and anything else considered harmful to minors.

CIA Security Triad (Confidentiality, Integrity, and Availability)

CPOE System (Computerized Provider Order Entry System): A system that enables physicians to place orders—for drugs, laboratory tests, radiology, or physical therapy—electronically, with the orders transmitted directly to the recipient.

CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act): A law specifying that it is legal to spam, 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.

CDS (Clinical Decision Support): A process and set of tools designed to enhance health-related decision making using clinical knowledge and patient-specific information

CSR (Corporate Social Responsibility): The concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.

CPC (Cost Per Click): One of the two common methods of charging for paid media in which ads are paid for only when someone actually clicks on them.

CPM (Post Per Thousand Impressions): One of the two common methods of charging for paid media in which ads are billed at a flat rate per 1,000 impressions, which is a measure of the number of times an ad is displayed whether it was actually clicked on or not.

DDS (Decision Support System): A business information system used to improve decision making in a variety of industries. A DSS can develop accurate forecasts of customer demand, recommend stocks and bonds, or schedule shift workers to minimize cost while meeting customer service goals.

DHS (Department of Homeland Security): A large federal agency with more than 240,000 employees and a budget of almost $65 billion whose goal is to provide for a "safer, more secure America, which is resilient against terrorism and other potential threats."

DMCA (Digital Millennium Copyright Act): Signed into law in 1998, the act addresses a number of copyright-related issues, with Title II of the act providing limitations on the liability of an Internet service provider for copyright infringement.

DDoS Attack (Distributed Denial-of-Service Attack): An attack in which a malicious hacker takes over computers via the internet and causes them to flood a target site with demands for data and other small tasks.

DTSA (Defend Trade Secrets Act): Amended the EEA (see below) to create a federal civil remedy for trade secret misappropriation.

EEA (Economic Espionage Act): An act passed in 1996 to help law enforcement agencies pursue economic espionage. It imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets.

EHR (Electronic Health Record): A comprehensive view of the patient's complete medical history designed to be shared with authorized providers and staff from more than one organization.

EMR (Electronic Medical Record): A collection of health-related information on an individual that is created, managed, and consulted by authorized clinicians and staff within a single healthcare organization.

EPEAT (Electronic Product Environmental Assessment Tool): A system that enables purchasers to evaluate, compare, and select electronic products based on a total of 51 environmental criteria.

FCPA (Foreign Corrupt Practices Act): An act that makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office.

FERPA (Family Educational Rights and Privacy Act): A federal law that assigns certain rights to parents regarding their children's educational records.

HIE (Health Information Exchange): The process of sharing patient-level electronic health information between different organizations.

HIPPA (Health Insurance Portability and Accountability Act): An act that required national standards to protect patients' health information from being disclosed without their consent.

HITECH Act (Health Information Technology for Economic and Clinical Health Act): A program to incentivize physicians and hospitals to implement such systems. Under this act, increased Medicaid and Medicare reimbursements are made to doctors and hospitals that demonstrate "meaningful use" of EHR (Electronic Health Record) technology.

ICANN (Internet Corporation for Assigned Names): a nonprofit corporation responsible for managing the internet's domain name system.

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

IPR (Intellectual Property Rights)

ISAE No. 3402 (International Standard on Assurance Engagements No. 3402): Developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.

ISO 9001 Family of Standards (International Organization for Standardization 9001 Family of Standards): A set of standards written to serve as a guide to quality products, services, and management. It provides a set of standardized requirements for a quality management system.

IT (Information Technology)

NGFW (Next-Generation Firewall): A hardware- or software-based network security system that detects and blocks attacks by filtering network traffic based on the packet contents.

PAPA (Privacy, Accuracy, Property, Access)

PHR (Personal Health Record): Information from the electronic health record (EHR) that are routinely shared with the patient—such as personal identifiers, contact information, health provider information, problem list, medication history, allergies, immunizations, and lab and test results.

PRO-IP Act (Prioritizing Resources and Organization for Intellectual Property Act): An act that created the position of Intellectual Property Enforcement Coordinator within the Executive Office of the President. It also increased trademark and copyright enforcement and substantially increased penalties for infringement.

PEO (Professional Employer Organization): A business entity that co-employs the employees of its clients and typically assumes responsibility for all human resource management functions.

RWB (Reporters without Borders): An NGO (nongovernmental organization) that promotes and defends freedom of information and freedom of the press around the world.

SIIA (Software & Information Industry Association): A trade group that represents the world's largest software and hardware manufacturers.

SSAE No. 16 Audit Report (Statement on Standards for Attestation Engagements No. 16 Audit Report): An auditing standard issued by the Auditing Standards Board of AICPA (the American Institute of Certified Public Accountants). It demonstrates that an outsourcing firm has effective internal controls in accordance with the Sarbanes Oxley Act of 2002.

SLAPP (Strategic Lawsuit Against Public Participation): A lawsuit filed by corporations, government officials, and others against citizens and community groups who oppose them on matters of concern. Such lawsuits typically are without merit and are used to intimidate critics.

TLS (Transport Layer Security): A communications protocol or system of rules that ensures privacy between communicating applications and their users on the internet.

US-CERT (U.S. Computer Emergency Readiness Team): Established in 2003 to protect the nation's internet infrastructure against cyberattacks and serves as a clearinghouse for information on new viruses, worms, and other computer security topics.

UTSA (Uniform Trade Secrets Act): An act drafted in the 1970s to bring uniformity to all the United States in the area of trade secret law.

WTO TRIPS Agreement (World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights): An agreement of the WTO that requires member governments to ensure that intellectual property rights can be enforced under their laws and that penalties for infringement are tough enough to deter further violations.