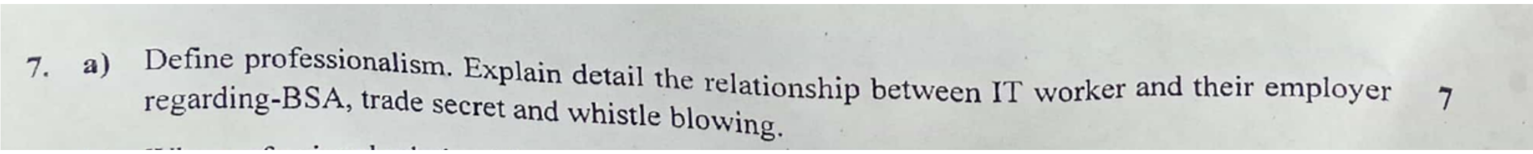
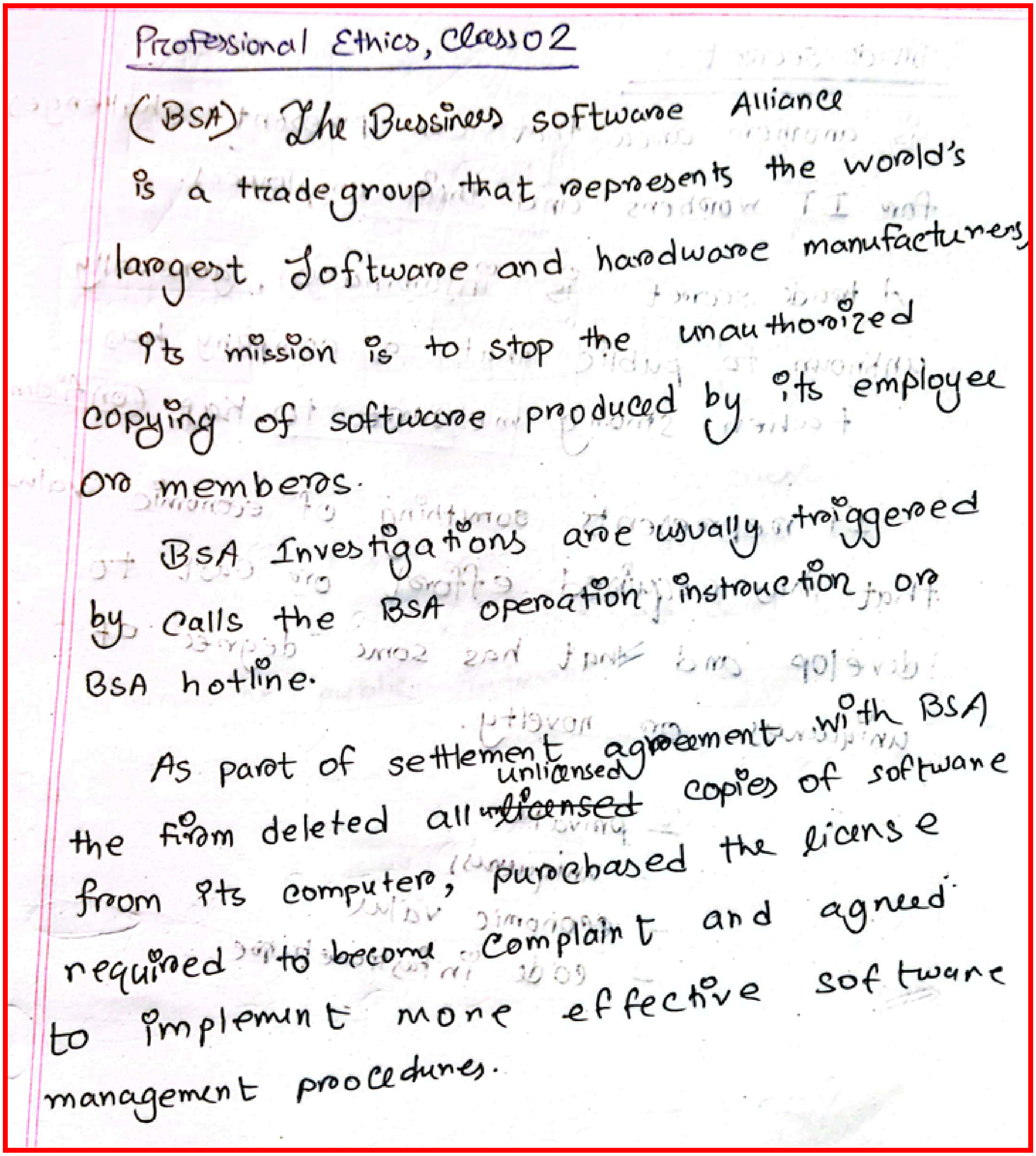


7. a) Define professionalism. Explain detail the relationship between IT worker and their employer regarding-BSA, trade secret and whistle blowing. 7

Professionalism refers to the set of behaviors, skills, and ethical principles that define a person's conduct in their profession. It includes expertise in a specific field, a commitment to continuous learning, and adherence to ethical principles. In the field of Information Technology (IT), professionalism involves integrity, accountability, and respect for confidentiality while maintaining technical competence. IT professionals are expected to follow industry standards, legal regulations, and ethical codes that guide their decision-making and interactions in the workplace.

The relationship between IT workers and their employers is governed by several ethical and legal considerations, particularly concerning software compliance, confidentiality, and ethical decision-making. IT professionals handle crucial aspects of software licensing, data security, and system management, making their role vital in protecting an organization's legal and ethical standing. Three major areas where this relationship is particularly significant are compliance with the **Business Software Alliance (BSA)** regulations, protection of **trade secrets**, and ethical concerns related to **whistleblowing**.

Business Software Alliance (BSA) and Software Compliance



Professional Ethics, Class02

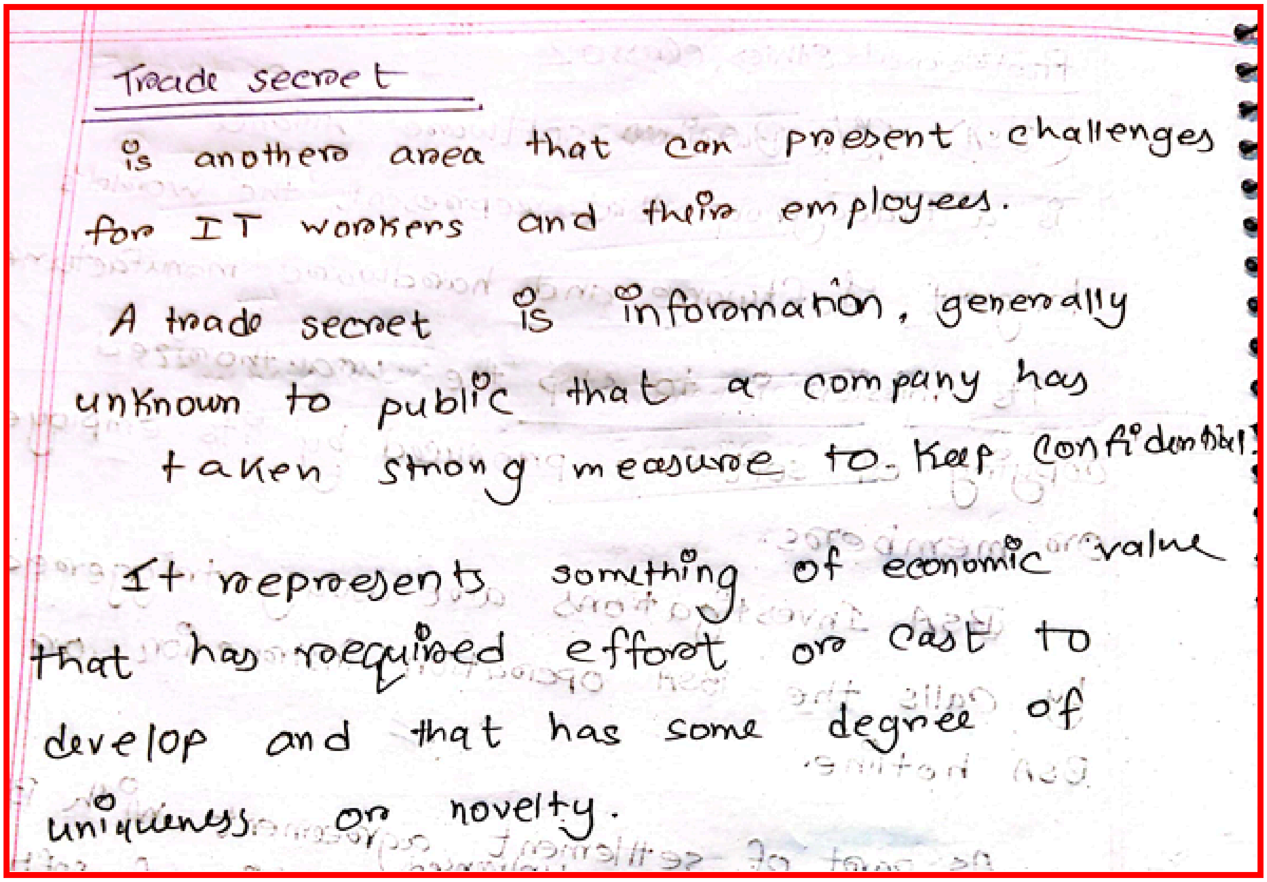
(BSA) The Bussiness software Alliance is a trade group that represents the world's largest Software and hardware manufacturers.

Its mission is to stop the unauthorized copying of software produced by its employee or members.

BSA Investigations are usually triggered by calls the BSA operation instruction or BSA hotline.

As part of settlement agreement with BSA the firm deleted all ~~ulicensed~~ unlicensed copies of software from its computer, purchased the license required to become Complaint and agreed to implement more effective software management procedures.

Trade Secrets and Confidentiality



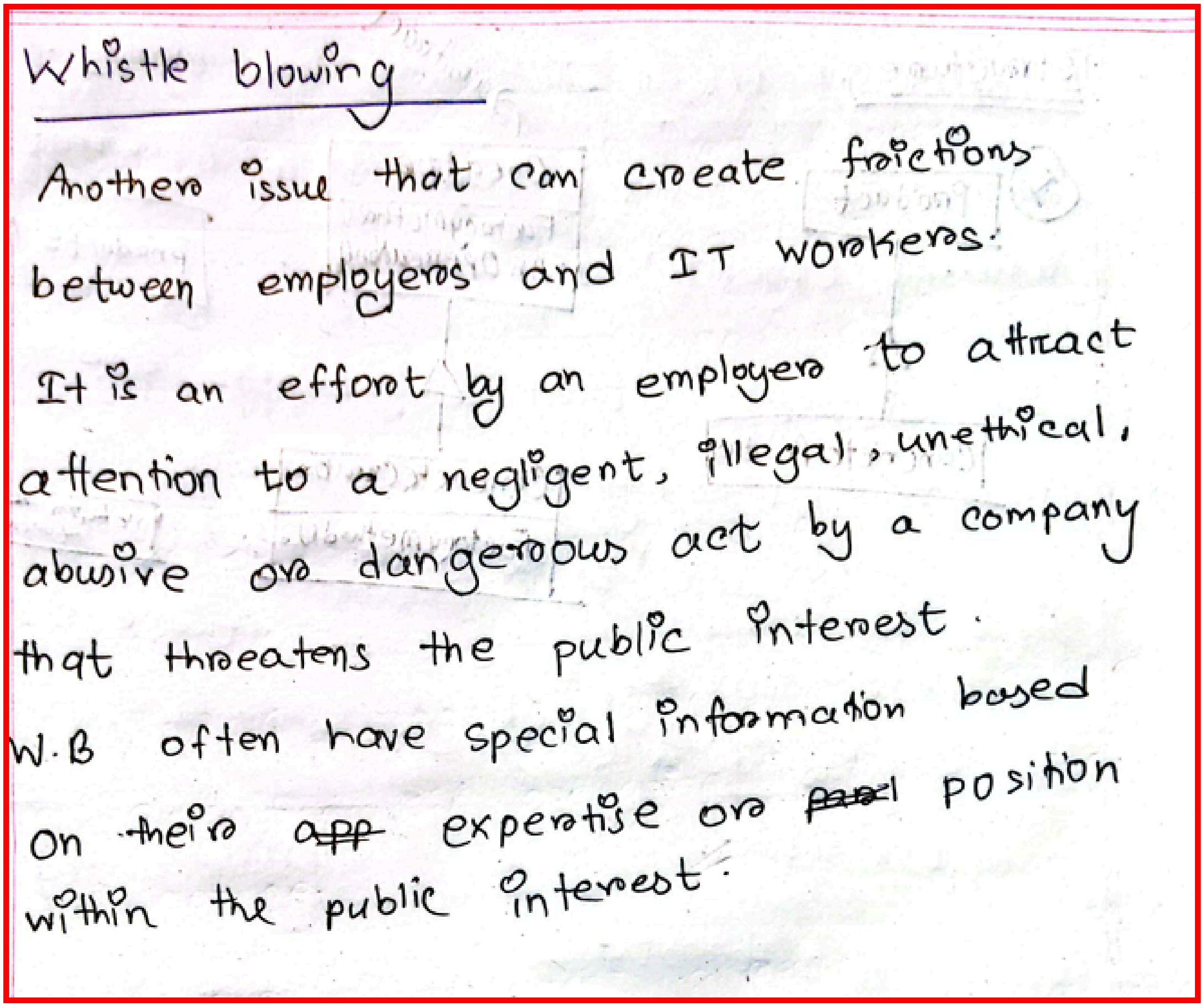
Trade secret

is another area that can present challenges for IT workers and their employees.

A trade secret is information, generally unknown to public that a company has taken strong measure to keep confidential

It represents something of economic value that has required effort or cast to develop and that has some degree of uniqueness or novelty.

Whistleblowing and Ethical Dilemmas

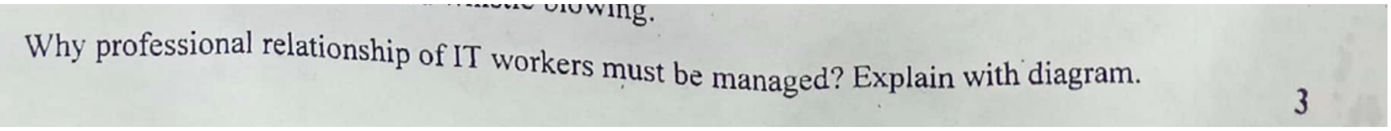


Whistle blowing

Another issue that can create frictions between employers and IT workers.

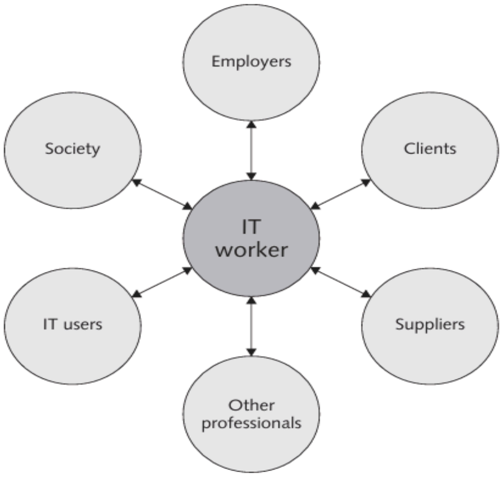
It is an effort by an employer to attract attention to a negligent, illegal, unethical, abusive or dangerous act by a company that threatens the public interest.

W.B often have special information based on their ~~app~~ expertise or ~~pa~~l position within the public interest.



whistle blowing.

Why professional relationship of IT workers must be managed? Explain with diagram. 3



IT workers typically become involved in many different relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed in the following sections.

Relationships Between IT Workers and Employers

IT workers and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong. An IT worker and an employer typically agree on fundamental aspects of this relationship before the worker accepts an employment offer. These issues may include job title, general performance expectations, specific work responsibilities, drug-testing requirements, dress code, location of employment, salary, work hours, and company benefits. Many other aspects of this relationship may be addressed in a company's policy and procedures manual or in the company's code of conduct, if one exists. These issues may include protection of company secrets; vacation policy; time off for a funeral or an illness in the family; tuition reimbursement; and use of company resources, including computers and networks.

Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those "clients" are coworkers who are part of the same organization as the IT worker. In other cases, the client is part of a different organization. In relationships between IT workers and clients, each party agrees to provide something of value to the other. Generally speaking, the IT worker provides hardware, software, or services at a certain cost and within a given time frame. For example, an IT worker might agree to implement a new accounts payable software package that meets a client's requirements. The client provides compensation, access to key contacts, and perhaps a work space. This relationship is usually documented in contractual terms— who does what, when the work begins, how long it will take, how much the client pays, and so on. Although there is often a vast disparity in technical expertise between IT workers and their clients, the two parties must work together to be successful.

Relationships Between IT Workers and Suppliers

IT workers deal with many different hardware, software, and service providers. Most IT workers understand that building a good working relationship with suppliers encourages the flow of useful communication as well as the sharing of ideas. Such information can lead to innovative and cost-effective ways of using the supplier’s products and services that the IT worker may never have considered.

Relationships Between IT Workers and Other Professionals

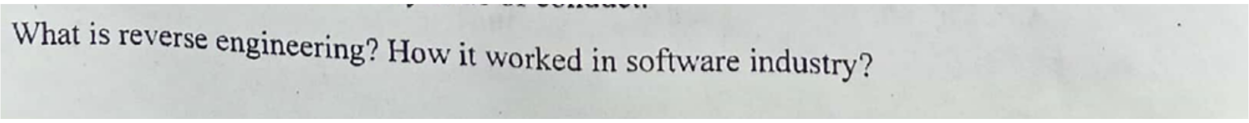
Professionals often feel a degree of loyalty to the other members of their profession. As a result, they are often quick to help each other obtain new positions but slow to criticize each other in public. Professionals also have an interest in their profession as a whole, because how it is perceived affects how individual members are viewed and treated. (For example, politicians are not generally thought to be very trustworthy, but teachers are.) Hence, professionals owe each other an adherence to the profession’s code of conduct. Experienced professionals can also serve as mentors and help develop new members of the profession.

Relationships Between IT Workers and IT Users

The term IT user refers to a person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity.

Relationships Between IT Workers and Society

Regulatory laws establish safety standards for products and services to protect the public. However, these laws are less than perfect, and they cannot safeguard against all negative side effects of a product or process. Often, professionals can clearly see the effect their work will have and can take action to eliminate potential public risks. Thus, society expects members of a profession to provide significant benefits and to not cause harm through their actions. One approach to meeting this expectation is to establish and main tain professional standards that protect the public.

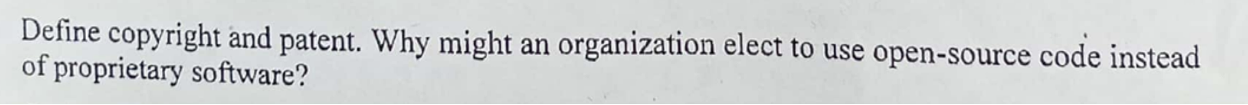


What is reverse engineering? How it worked in software industry?

Reverse engineering is the process of taking something apart in order to understand it, build a copy of it, or improve it. Reverse engineering was originally applied to computer hardware but is now commonly applied to software as well. Reverse engineering of soft ware involves analyzing it to create a new representation of the system in a different form or at a higher level of abstraction. Often, reverse engineering begins by extracting design stage details from program code. Design-stage details about an information system are more conceptual and less defined than the program code of the same system. Microsoft has been accused repeatedly of reverse engineering products—ranging from the Apple Macintosh user interface, to many Apple operating system utility features that were incor porated into DOS (and later Windows), to early word-processing and spreadsheet programs that set the design for Word and Excel, to Google's methods for improving search results for its Bing search engine.

One frequent use of reverse engineering for software is to modify an application that ran on one vendor's database so that it can run on another's (for example, from Access to Oracle). Database management systems use their own programming language for applica tion development. As a result, organizations that want to change database vendors are faced with rewriting existing applications using the new vendor's database programming language. The cost and length of time required for this redevelopment can deter an orga nization from changing vendors and deprive it of the possible benefits of converting to an improved database technology. Using reverse engineering, a developer can use the code of the current database pro gramming language to recover the design of the information system application. Next, code-generation tools can be used to take the design and produce code (forward engineer) in the new database programming language. This reverse-engineering and code-generating process greatly reduces the time and cost needed to migrate the organization's applica tions to the new database management system. No one challenges the right to use this process to convert applications developed in-house. After all, those applications were developed and are owned by the companies using them. Other reverse-engineering issues involve tools called compilers and decompilers. A compiler is a language translator that converts computer program statements expressed in a source language (such as Java, C, C++, and COBOL) into machine language (a series of binary codes of 0s and 1s) that the computer can execute. When a software manufacturer provides a customer with its software, it usually provides the software in machine-language form. Tools called reverse-engineering compilers, or decompilers, can read the machine language and produce the source code. For example, REC (Reverse Engineering Compiler) is a decompiler that reads an executable, machine-language file and produces a C-like representation of the code used to build the program.

The ethics of using reverse engineering are debated. Some argue that its use is fair if it enables a company to create software that interoperates with another company's software or hardware and provides a useful function. This is especially true if the software's creator refuses to cooperate by providing documentation to help create interoperable software. From the consumer's standpoint, such stifling of competition increases costs and reduces business options. Reverse engineering can also be a useful tool in detecting software bugs and security holes.



Define copyright and patent. Why might an organization elect to use open-source code instead of proprietary software?

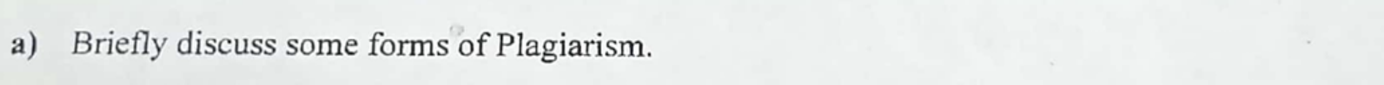
A copyright is the exclusive right to distribute, display, perform, or reproduce an original work in copies or to prepare derivative works based on the work. Copyright protection is granted to the creators of "original works of authorship in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." The author may grant this exclusive right to others. As new forms of expression develop, they can be awarded copyright protection. For example, in the Copyright Act of 1976, audiovisual works were given protection, and computer programs were assigned to the literary works category.

A patent is a grant of a property right issued by the United States Patent and Trademark Office (USPTO) to an inventor. A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators. Unlike a copyright, a patent prevents independent creation as well as copying. Even if someone else invents the same item independently and with no prior knowledge of the patent holder’s invention, the second inventor is excluded from using the patented device without permission of the original patent holder. The rights of the patent are valid only in the United States and its territories and possessions.

Organizations often prefer open-source software over proprietary solutions for several reasons:

1. **Cost Savings:** Open-source software is usually free or significantly less expensive than proprietary alternatives, helping businesses reduce software licensing costs.
2. **Customization & Flexibility:** Open-source code allows organizations to modify and adapt the software to meet their specific needs, which is often not possible with proprietary software.
3. **Security & Reliability:** Since open-source software is reviewed and tested by a large community of developers, vulnerabilities can be quickly identified and patched, making it more secure and reliable.
4. **Interoperability:** Open-source software facilitates seamless integration with other systems, helping businesses efficiently transfer data and enhance compatibility between applications.
5. **Community Support & Continuous Improvement:** Open-source projects are often supported by large developer communities, ensuring regular updates, bug fixes, and feature enhancements.
6. **Avoiding Vendor Lock-in:** Proprietary software locks organizations into using a specific vendor’s ecosystem, which can be restrictive. Open-source solutions provide more freedom and control over the software.
7. **Encouraging Innovation:** Open-source projects encourage collaboration and knowledge sharing, allowing businesses to benefit from the latest technological advancements without waiting for a commercial release.
8. **Legal & Compliance Advantages:** Many industries and government agencies prefer open-source software due to its transparency, ensuring compliance with regulations and avoiding hidden licensing fees.

By choosing open-source software, organizations can reduce costs, improve security, and retain control over their technology infrastructure, making it a strategic choice for many businesses and developers.

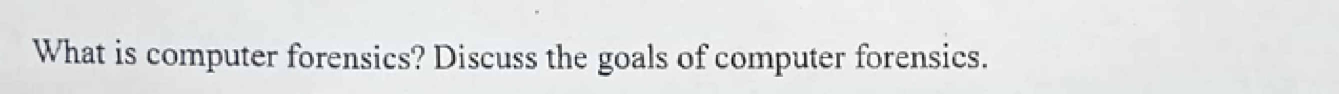


a) Briefly discuss some forms of Plagiarism.

Plagiarism is the act of using someone else's ideas, words, or work without proper acknowledgment. The widespread availability of electronic content and online "paper mills" has made it easier for students and professionals to commit plagiarism. Below are some common forms:

1. **Direct Plagiarism** – Copying someone else's work word-for-word without quotation marks or citations. This is the most blatant form of plagiarism.
2. **Self-Plagiarism** – Submitting one's previous work as new without proper disclosure. For example, a student submitting the same paper for multiple courses.
3. **Mosaic Plagiarism** – Patching together phrases from multiple sources without proper citations while maintaining the original structure of the text.
4. **Accidental Plagiarism** – Failing to properly cite a source due to a misunderstanding of citation rules, often because students assume online content is in the public domain.
5. **Paraphrasing Plagiarism** – Rewriting someone else's ideas in different words while keeping the original meaning without proper citation.
6. **Source-Based Plagiarism** – Citing incorrect or nonexistent sources or using a source that does not contain the referenced information.

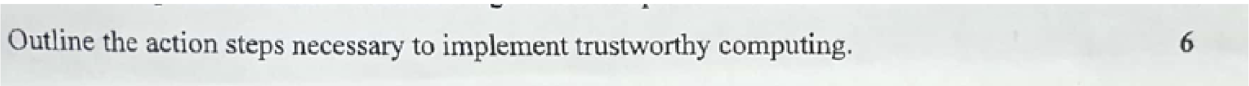
Beyond academia, plagiarism is prevalent in journalism, music, literature, and even software development. Institutions combat plagiarism using detection tools like **Turnitin, SafeAssign, and iThenticate** to identify copied content. Many universities also take preventive measures, such as educating students on proper citation and breaking assignments into stages to discourage last-minute copying.



What is computer forensics? Discuss the goals of computer forensics.

Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and stor age devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation. It may also be launched for a variety of other reasons, for example, to retrace steps taken when data has been lost, to assess damage following a computer incident, to investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.

Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law. In addition, extensive training and certification increases the stature of a computer forensics investigator in a court of law. There are numerous certifications related to computer forensics, including the CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst). The EnCE Certified Examiner program certifies professionals who have mastered computer investigation methods as well as the use of Guidance Software's EnCase computer forensics software. Numerous universities (both online and traditional) offer degrees specializing in computer forensics. Such degree programs should include training in accounting, particularly auditing, as this is very useful in the investigation of cases involving fraud.



Outline the action steps necessary to implement trustworthy computing. 6

Trustworthy computing is a method of computing that delivers secure, private, and reliable computing experiences based on sound business practices—which is what organizations worldwide are demanding today. Software and hardware manufacturers, consultants, and programmers all understand that this is a priority for their customers.

For example, Microsoft has pledged to deliver on a trustworthy computing initiative designed to improve trust in its software products, as summarized in Figure 3-4 and Table 3-7. The security of any system or network is a combination of technology, policy, and people and requires a wide range of activities to be effective. As the Committee on Improving Cybersecurity Research in the United States wrote in a report for the National Academy of Sciences, “Society ultimately expects computer systems to be trustworthy— that is, that they do what is required and expected of them despite environmental disruption, human user and operator errors, and attacks by hostile parties, and that they not do other things.”

A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating end users about the risks involved and the actions they must take to prevent a security incident.

An organization's IT security group must lead the effort to prevent security breaches by implementing security policies and procedures, as well as effectively employing available hardware and software tools. However, no security system is perfect, so systems and procedures must be monitored to detect a possible intrusion.

If an intrusion occurs, there must be a clear reaction plan that addresses notification, evidence protection, activity log maintenance, containment, eradication, and recovery.

The following sections discuss these activities.

TABLE 3-7 Actions taken by Microsoft to support trustworthy computing

Pillar	Actions taken by Microsoft
Security	Invest in the expertise and technology required to create a trustworthy environment.
	Work with law enforcement agencies, industry experts, academia, and private sectors to create and enforce secure computing.
	Develop trust by educating consumers on secure computing.
Privacy	Make privacy a priority in the design, development, and testing of products.
	Contribute to standards and policies created by industry organizations and government.
	Provide users with a sense of control over their personal information.
Reliability	Build systems so that (1) they continue to provide service in the face of internal or external disruptions; (2) they can be easily restored to a previously known state with no data loss in the event of a disruption; (3) they provide accurate and timely service whenever needed; (4) required changes and upgrades do not disrupt them; (5) they contain minimal software bugs on release; and (6) they work as expected or promised.
Business integrity	Be responsive—take responsibility for problems and take action to correct them. Be transparent—be open in dealings with customers, keep motives clear, keep promises, and make sure customers know where they stand in dealing with the company.

Source Line: Course Technology/Cengage Learning.

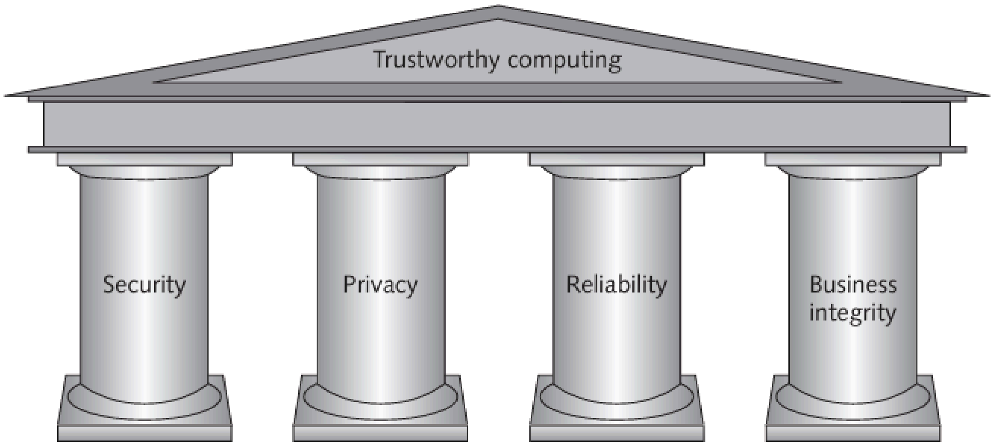
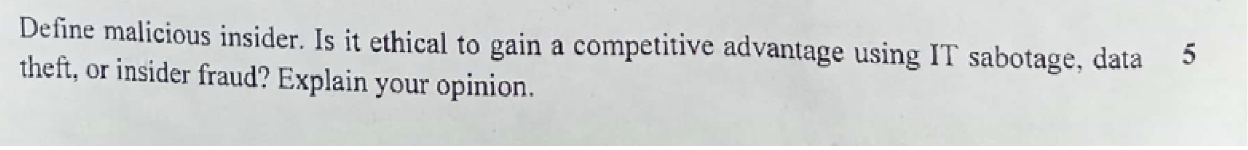


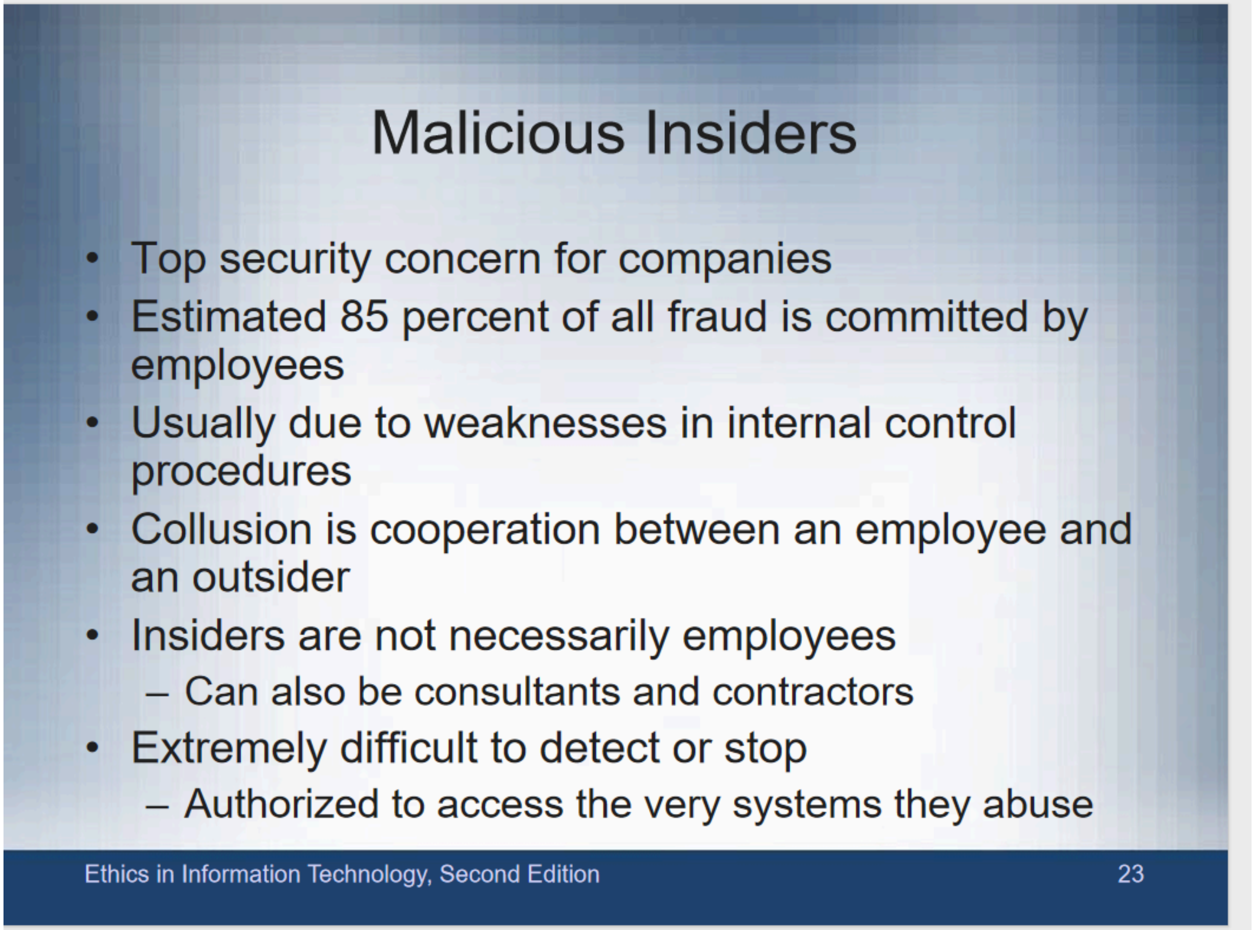
FIGURE 3-4 Microsoft's four pillars of trustworthy computing

Source Line: Course Technology/Cengage Learning.



Define malicious insider. Is it ethical to gain a competitive advantage using IT sabotage, data theft, or insider fraud? Explain your opinion. 5

Malicious insiders are individuals within an organization (employees, consultants, contractors) who intentionally abuse their access for harmful purposes. They pose a significant security risk due to their authorized access and knowledge of internal systems. They can be motivated by financial gain, revenge, or publicity.



Malicious Insiders

- Top security concern for companies
- Estimated 85 percent of all fraud is committed by employees
- Usually due to weaknesses in internal control procedures
- Collusion is cooperation between an employee and an outsider
- Insiders are not necessarily employees
  - Can also be consultants and contractors
- Extremely difficult to detect or stop
  - Authorized to access the very systems they abuse

Ethics in Information Technology, Second Edition 23