****** Please grab current information for this semester as many things may have changed. This pdf is based on Spring-2022 lecture topics *****

Other resources:

https://drive.google.com/drive/folders/19BqDBp88IDOSM3JOlNTXBv2K1XNhsikS?usp=share_link

ETHICS

Final exam Topics

Tasnim Samin
C191267

Table of Contents

Syllabus:

Course Code : CSE-4805
Course Title : Social, Professional and Ethical Issues in Computing
Credit Hours: 2 **Contact Hours: 2 per week**
Section-B (Final Exam: 50 Marks)

Group-A (20 Marks)

4. Computer & Software Reliability: How liability is determined when computer hardware and software fails? Responsibility vs. Liability vs. Accountability; Some historical examples of software risks (such as the Therac-25 case)
5. Intellectual Property: What is intellectual property" Copyrights, patents, and trade secrets; Software piracy; Software patents; Free software, what is fair use?

Group-B (30 Marks)

6. Computer Crime: History and examples of computer crime; "Cracking" ("hacking") and its effects; Viruses, worms, and Trojan horses; Online scams, Identity theft; moral issues related to these crimes.
7. Computer and Work: Impact of employment, work environment, Employee monitoring, Health issues
8. Professional Ethics and responsibilities: What is Ethics? What is Computer ethics, Some ethical guidelines for computer professionals, Examine and discuss professional codes of ethics, conduct, and practice (IEEE, ACM, SE, AITP, and so forth).

Segment- 4 (Chapter 8)

1. How accountability should be maintained in order to preserve software reliability?

Answers:

To maintain accountability for preserve software reliability, we have to approaches some of this technique which are written below.

- Technical preservation (techno-centric) - **Preserve** original hardware and software in same state.
- Emulation (data-centric) - **Emulate** original hardware and operating environment, keeping software in same state.
- Migration (functionality-centric) - **Update** software as required to maintain same functionality, porting/transferring before platform obsolescence.
- Cultivation (process-centric) - Keep software '**alive**' by moving to more open development model bringing on board additional contributors and spreading knowledge of process.
- Hibernation (knowledge-centric) - Preserve the knowledge of **how to** resuscitate/**recreate** the exact functionality of the software at a later date.
- Deprecation - Formally retire the software without leaving the option of resuscitation/recreation.

2. Define liability. How Liability is determined when computer hardware and software is failed?

Answers

Liability means the state of being responsible for something, especially by law.

Software and hardware developers must realize that they will be amongst the first parties to be involved in the case of system failures. The strength of their defense may ultimately rest on their contractual documentation and/or their documented methodologies of testing. Some may not wish to take the chance and prefer to insure.

Possible parties to be sued/accused include the software developer, the hardware or software supplier, the hardware manufacturer, the systems integrator, the maintenance company and the user. Employees of the various parties may in certain circumstance be included personally in the litigation. In fact, all parties who remain standing at the end of an information technology disaster will be considered potential parties.

System crashes or security breaches/break can result in:

- Loss of data
- Loss of time (consider the cost of having one operator's terminal down for a day, let alone a whole system)
- Business interruption and economic loss (both expectation and reliance loss)
- Physical destruction of equipment
- Personal injury
- Reputation loss
- Privacy/Confidential Information loss and damage

Terms which are of such importance in Information Technology projects may include (depending on degree):

- **failure** to get the software or hardware up and **running** (implementation or integration problems or simply bad design)
- **failure** of **performance** or functional requirements (hopefully, but not necessarily, as set out in annexures or schedules to the contract).
- the **ability** to change or modify the software or hardware
- **failure** of essential support obligations.
- excessive down time
- Intellectual Property rights infringement

If the term is a warranty only then a claim only arises for damages or for rectification of the problem. **Typical warranty breaches may include** (depending on degree):

- **reduction** in hours of support.
- **inability** to correct minor faults.
- **delays** in providing support.
- **inability** to supply certain types of support.
- **failure** to provide minor functionality or performance requirements.

Our ever-increasing reliance on computer hardware and software is bound to be associated with a surge in litigation arising from “computer down time”. It is important for parties to clearly define who is responsible for which problems arising from system crashes and breaches and for the respective parties to have adequate insurance which will protect them from “down time liability”.

3. Define software risk to maintain reliability?

Answers

Reliability defined as the **probability** of a system or system **element** performing its intended function under **stated conditions** without failure for a given period of time. A precise definition must include a detailed description of the function, the environment, the time scale, and what constitutes a failure. Each can be surprisingly difficult to define as precisely as one might wish.

Software risk is defined here as the cost of failure weighted by the probability of failure. This definition differs significantly from current definitions of software reliability.

Software risk measurement can be used in developing and maintaining high quality software in several ways. **First**, it may be used to guide software testing. Generally, it is not possible to test a software system until perfection is assured. Trade-offs must be made concerning allocation of test resources: although all portions will be tested, some may be tested more intensively than others. It is reasonable to consider allocating test resources based upon software risk since consequences of failures differ among modules.

Since the consequences of s**oftware failure can be catastrophic/great damage**, it is reasonable for producers and, perhaps, users to **want to have some insurance against their losses.**

Software reliability models have not considered the cost of failure. They have been adapted from hardware reliability assessment, which models failure as producing a single, known consequence, generally total system failure. However, the consequences of software failure are more varied. Furthermore, the causes of failure differ: hardware may fail after use as components fatigue or wear out; software may fail as new use encounters old errors. We may therefore expect different. statistical properties for hardware and software failures. Thus, software risk assessment differs from hardware reliability assessment, and it is not surprising that traditional software methods, grounded in the hardware tradition, should prove less than wholly satisfactory.

4. The Therac-25 radiation machine involved errors in software overall design and management or operations. Describe one error of each type

Answers

The **Therac-25** was a radiation therapy machine produced by Atomic Energy of **Canada** Limited (AECL) in 1982 after the Therac-6 and Therac-20 units (the earlier units had been produced in partnership with CGR of France).

The accidents occurred when the **high-power electron beam was activated instead of the intended low power beam**, and **without the beam spreader plate rotated into place**.

Previous models had **hardware interlocks** in place to **prevent** this, but Therac-25 had removed them, depending **instead** on **software interlocks** for safety. The software interlock could **fail** due to a **race condition**.

[A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence to be done correctly.]

The defect was as follows: a **one-byte counter** in a testing routine frequently **overflowed**; if an operator provided manual input to the machine at the precise moment that this counter overflowed, the interlock would fail.

The Therac-25 malfunctioned frequently. One facility said there were sometimes 40 **dose rate** malfunctions in a day, generally underdoses. Thus, operators became used to error messages appearing often, with no indication that there might be safety hazards.

[Dose rate refers to the quantity of radiation absorbed per unit of time.]

There were a number of **weaknesses** in the design of the operator **interface**. The error messages that appeared on the display were simply **error numbers** or **obscure messages** ("Malfunction 54" or "H-tilt"). This was not **unusual** for early computer programs when computers had much less memory and mass storage than they have now. One had to look up each error number in a **manual** for more explanation. The operator's manual for the Therac25, however, **did not include an explanation of the error messages.** The maintenance manual did not explain them either.

Investigators were able to trace some of the **overdoses** to two specific software errors. After the operator entered treatment parameters at a control console, a software procedure called **Set-Up Test** performed a variety of checks to be sure the machine was in the correct position, and so on. If anything was not ready, this procedure scheduled itself to rerun the checks. (The system might simply have to wait for the turntable to move into place.) The Set-Up Test procedure can run several hundred times while setting up for one treatment. A flag variable indicated whether a specific device on the machine was in the correct position. A zero value meant the device was ready; a nonzero value meant it must be checked. To ensure that the

device was checked, each time the Set-Up Test procedure ran, it incremented the variable to make it nonzero. The problem was that the flag variable was stored in one byte. After the **256th** call to the routine, the flag overflowed and showed a value of zero.
Other bugs caused the machine to ignore changes or corrections made by the operator at the console. When the operator typed in all the necessary information for a treatment, the program began moving various devices into place. This process could take several seconds. The software checked for editing of the input by the operator during this time and restarted the set-up if it detected editing. However, because of bugs in this section of the program, some parts of the program learned of the edited information while others did not. This led to machine settings that were **incorrect** and **inconsistent** with safe treatment.

5. Define reliability of computer software

Answers

Software Reliability is the **probability** of **failure-free** software operation for a **specified period of time** in a **specified environment**. Software Reliability is also an important **factor** affecting **system reliability**.
Software Reliability is not a **direct function of time.** Electronic and mechanical parts may become "**old**" and wear out with time and usage, but software will not rust or wear-out during its life cycle. Software **will not change** over time unless intentionally changed or upgraded.
Software Reliability is an important to attribute of software quality, together with functionality, usability, performance, serviceability, capability, installability, maintainability, and documentation. Software Reliability is hard to achieve, because the complexity of software tends to be high. While any system with a high degree of complexity, including software, will be hard to reach a certain level of reliability, system developers tend to push complexity into the software layer, with the rapid growth of system size and ease of doing so by upgrading the software. For example, large next-generation **aircraft** will have over **one million source** lines of software on-board; next-generation **air traffic control systems** will contain between **one and two million lines;** the upcoming **international Space Station** will have over **two million lines** on-board and over **ten million lines of ground support software**; several major **life-critical defense systems** will have over **five million source lines** of software.

Segment-5 (Chapter-4)

1. Discuss the difference between copyright and patent

Answers

Differences between copyright and patent:

Copyright	Patent
A bundle of rights granted to the creator of work, which excludes others from performing, selling or producing the work, known as Copyright.	A legal grant given by the government to original work, the inventor which excludes others from making, utilizing or trading the invention known as Copyright for a set period, is called a patent.
Covers artistic and literary/writers works	Covers inventions
Copyright protection is automatic	Patent protection requires registration formality
Excludes Others from copying or trading the product	Excludes others from manufacturing or using the product
Copyright, in general, is granted for 60 years.	Patent is granted for 20 years
Subject matter is expression.	Subject matter is ideas.

2. Describe the benefits of copyright

Answers

Benefits of Copyright Protection:

1. Copyright protection provides a vital incentive/**security** for the creation of many intellectual works.

2. **Without** copyright protection, it would be easy for others to exploit/**use** these works without paying any royalties or remuneration to the owner of the work.

3. Copyright **encourages enterprise** and creates a favorable climate to **stimulate economic** activity.

4. Copyright protection provides benefits in the form of economic rights which entitle the creators to control use of their **literary** and **artistic material** and to obtain an appropriate **economic reward**.

5. Creators can therefore be **rewarded** for their **creativity** and **investment**.

6. Copyright also gives **moral** rights to the **creator**. An author's **right to object** to the **modification** of his or her work is known as an integrity right.

3. Write short note on trademark and trade secrets.

Answers

Trademark: A **trademark** is a word, phrase, symbol, and/or design that **identifies** and **distinguishes** the **source** of the **goods** of **one party from those of others.** A trademark is commonly used to refer to both marks associated with **services** and **goods**. The purpose behind trademarks is to allow companies and individuals to **indicate** the **source** of their **goods** or **services** and to distinguish them from others in the industry.

A trademark not only gives the trademark owner the **exclusive** right to use **the mark**, but also allows the owner to **prevent others** from **using** a **similar mark** that can be **confusing** for the **general public**. A trademark **cannot**, however, **prevent** another **person** or **company** from **making** or **selling** the **same** goods or **service** under a **clearly** different **mark**.

Trade Secret: Broadly speaking, any **confidential business information** which provides an enterprise a **competitive edge/special power**, which may be considered a trade secret. Trade secrets cover **manufacturing** or **industrial secrets** and **commercial secrets**. The **unauthorized** use of such information by **persons other** than the **holder** is regarded/considered as an **unfair practice** and a **violation** of the trade secret. Depending on the legal system, the protection of trade secrets forms part of the general concept of protection against unfair competition.

The subject matter of trade secrets is usually defined in broad terms and includes sales methods, distribution methods, consumer profiles, advertising strategies, lists of suppliers and clients, and manufacturing processes. Clearly unfair practices in respect of secret information include industrial or commercial espionage, breach of contract and breach of confidence.

4. How does new technology threaten the protection of copyrighted materials?

Answers

New technologies as a threat to copyright protection:

- The emergence of digital technologies towards the concluding decades of the twentieth century raised a whole **new set of challenges** to copyright regimes.
- All works can now be **digitalized** whether they comprise **texts**, **images**, **sound** or **diagrams**.
- Once digitalized the various elements such as images are all '**equal**' and can be **merged**, **transformed**, **manipulated** or **mixed** to create an endless variety of new works.
- With the advent of the digital environment, the **access**, **use**, **duplication** or **modification** of the **original** work has become **really easy.**

- Digital environment has created a platform for people for widespread cost effective distribution of the original works, posing serious threats to the interest of the creator.
- With the emergence of the **Internet** and increasing **use** of the **world wide web** possibilities of infringement of copyright have become mind boggling free and easy
- **Taking content** from **one site**, **modifying** it or just **reproducing** it on **another site** has been made possible by **digital technology**
- **Piracy** occurs when **copyrighted software** is made available to users to download without the express permission of the copyright owner. Such illegal software is offered over online sources
- Piracy hampers **creativity**, hinders/decrease the development of new software and local software industry and ultimately effects e-commerce

5. Define Software piracy and Intellectual property

Answers

Software Piracy:

The term "**piracy**" describes the act of **reproducing copyrighted** works without permission from the copyright owner.

Software piracy is a term that is frequently used to describe the **illegal copying**, **distribution** or **use of computer software** in **violation** of its **license** (commonly referred to as an end user licensing agreement or EULA).

Most software programs purchased are **licensed** for use by just **one user** or at just one **computer** site. Moreover, when someone **buys software**, he or she is known as a "**licensed user**" rather than as an **owner of the software**.

Intellectual Property:

Intellectual property (IP) refers to creations of the artistic works; designs; and symbols, names and images used in commerce.

Intellectual property rights (IPRs) are the rights granted to the creators of Intellectual property, and include trademarks, copyright, patents, industrial design rights, and in some jurisdictions trade secrets.

Artistic works including music and literature, as well as discoveries, inventions, software, words, phrases, symbols, and designs can all be protected as intellectual property.

The key to understanding intellectual property protection is to understand that the thing protected is the intangible creative work—not its particular physical form.

6. What is free software? Discuss briefly some benefits of free software

Answers

Free software is an **idea**, an **ethic**, **supported** by a large **loose-knit** group of **computer programmers** who allow people to **copy**, **use**, and **modify their software**.
The free in free software means **freedom**, not necessarily **lack of cost**, though **often**

there is **no charge**.

Free software enthusiasts advocate allowing **unrestricted copying** of programs and making the **source code** (the human-readable form of a program) **available** to everyone.

Software **distributed** or made **public** in **source code** is **open source**, and the open source movement is closely related to the free software movement. (Commercial software, often called **proprietary software**, is normally sold in object code, the code run by the computer, but not intelligible to people. The source code is kept secret.) **Benefits of Free Software:**

1) Available at **minimal cost**
2) Provides **full freedom**
3) No imposed upgrades
4) No **spying** on users
5) Auditability
6) Provides **better security**
7) No monopolies
8) **Truly user-oriented**
9) No lock-in standards
10) **Part of social movement**

7. What is fair use? How is it determined whether a particular use of a copyrighted use or not?

Answers

Fair Use:

Fair use is a doctrine/ideology that allows **uses** of **copyrighted material** which contribute to the creation of new work (such as quoting part of a work in a review) and uses **that are not likely to deprive authors or publishers of income for their work.**
Fair uses do not **require** the **permission** of the **copyright holder**. The notion of fair use (for literary and artistic works) grew from **judicial** decisions.
A law identifies possible fair uses, such as "criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research."
It lists four factors to consider in determining whether a particular use is a "fair use":

1. The purpose and nature of the use, including whether it is for **commercial** purposes or nonprofit **educational** purposes. (Commercial use is less likely to be fair use.)
2. The **nature** of the copyrighted work. (Use of creative work, such as a novel, is less likely than use of factual work to be fair use.)

3. The amount and **significance** of the portion used.

4. The effect of the use on the **potential market** for or value of the copyrighted work. (Uses that reduce sales of the original work are less likely to be considered fair.)

No single factor alone determines whether a particular use is a fair use, but the last one generally gets more weight than the others.

8. How intellectual Property be preserved?

Answers

Intellectual property rights include patents, copyright, industrial design rights, trademarks, plant variety rights, trade dress, geographical indications, and in some jurisdictions trade secrets.

Patents

A patent is a form of **right granted** by the **government** to an **inventor**, giving the owner the right to **exclude others** from making, using, selling, offering to sell, and importing an invention for a **limited period** of **time**, in exchange for the public disclosure of the invention. An invention is a **solution** to a specific **technological problem**, which may be a **product** or a **process** and generally has to fulfill three main requirements: it has to be new, not obvious and there needs to be an industrial applicability.

Copyright

A copyright gives the **creator** of an original work **exclusive rights** to it, usually for a **limited time**. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or "works". Copyright does not cover ideas and information themselves, only the form or manner in which they are expressed

Trademarks

A trademark is a **recognizable sign**, **design** or **expression** which distinguishes **products** or **services** of a particular trader from the similar products or services of other traders. Industrial design rights

An industrial design right (sometimes called "design right" or *design patent*) protects the **visual design** of objects that are not purely utilitarian. An industrial design consists of the creation of a shape, configuration or composition of pattern or color, or combination of pattern and color in three-dimensional form containing aesthetic value. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft.

9. Describe two technical means of protecting copyright of intellectual property on the web

Answers

Ways to Protect Web Content Copyright:

Preventative Measures:

There are certain measures that can be taken to discourage **plagiarism** of your content by illustrating that you are **aware** of your **rights** as the content's creator.

1. Register your website with the "**DMCA**" and add one of their **badges** to your website to let potential copyright infringers know that you are protecting your content
2. Include a **copyright notice** on your website. This will show that you are **aware** of your legal standing as the content's creator.
3. Save **drafts** of **everything** you **post** online in case you need to prove later that you are the original author.

Use Duplicate Content Detection and Monitoring Tools:

1. Use **Google Search** to scan the Internet for unique parts of your text.
2. Monitor your content to search for plagiarism. There are various tools that allow you to search certain text and inform you if parts of it have been used elsewhere. **Plagium** and **Plagiarisma** are two such tools.
3. You can also add your blog to the **Copygator** service, which monitors your blog for free and contacts you when it finds duplicate content on the internet.

10. What do you think the impact would be on creative industries, such as music, movies and fiction novels, if copyright laws did not protect their intellectual property?

Answers

discouraging plagiarism is important to all of us who consider **creative work** and **creative ideas** to be essential to the growth and health or our culture. Here are some reasons:

First, stealing the intellectual property of others **decreases** motivation to **produce original** material across the board in two ways. Even if **you have great writing potential and great ideas**. To share, your motivation to take the time and energy to do so is diminished

Second, failing to **cite** or **reference** the sources of ideas or words **decreases accountability/answarability**. It allows potentially **false information** to be **circulated** and re-circulated without any way of finding out where the **false** information **originated**. This decreases our ability to police and deal with unsubstantiated material that's presented as factual.

Third, it is your **legal right** to protect **your work**. Imagine writing a **poem**, putting it on your blog, with **no copyright**, and a few months later you find that **someone** has **published** your **poem** under **their own** name and received a tremendous **financial** gain for your work. There is virtually nothing you could do about it, there is no proof as to sole ownership that however could have been avoided entirely if you had taken preliminary action in gaining a copyright on your poem… and this sort of thing happens all the time. **In all of these ways, rampant plagiarism will contribute to the "dumbing down" of our culture rather than the rise of a Golden Age, which I believe our technology is making possible for us.**

11. How is intellectual property like physical property? And how is intellectual property different than physical property?

Answers

Intellectual property is intangible. **ideas**; It's something someone **conceive**/**innovate**/**create** of in their **mind**. The idea of making an **invention**, the idea of how a book should be written, the idea of how a painting should be painted. Yes, these ideas can be, and sometimes have to be, reduced to a physical embodiment book written on computer disk or paper.

-In contrast, physical property such as real estate doesn't require conception; ideas. Real estate just is. Sometimes you have to measure it (survey it) to have rights to it; or stake it out and do certain acts to own it (like homesteading), or discover it (like an uncharted, uninhabited island outside the existing national territory claims of a country (not likely here on Earth anymore), but you don't have to "conceive of it.

-Sometimes physical property is the result of Intellectual Property. the physical piece of artwork produced by an artist; but rarely does the mere possession of a piece of physical property carry all the intellectual property rights that are associated with the physical item.

Buying an automobile doesn't give you the right to make use of the inventions that are incorporated into the automobile -until the patent rights expire.

-You can negotiate the purchase of intellectual property rights along with a physical property, such as buying an original oil painting, and buying the rights to copy it and publish/sell reproductions of the painting. But you are really buying two things. the physical property and the intellectual property.

12. Write short note on Digital Rights Management.

Answers

Digital rights management technologies (DRM) are a **collection of techniques** that control access to and uses of **intellectual property** in digital formats. DRM includes **hardware** and **Software** schemes using **encryption** and other tools. DRM implementations **embedded** in text files, music, movies, eBook's, and so on, can prevent saving, printing, making more than a specified number of copies, distributing a file, extracting excerpts, or fast-forwarding over commercials.

Segment- 6 (Chapter 5)

1. Define Hacking & Cracking. Write down the differences between Hacking & Cracking.

Answers

The term "**Hacker**," to many people, means an irresponsible, destructive criminal. Hackers **break** into computer systems.
They **intentionally release** computer viruses.
They **steal sensitive** personal, business, and government information.
They **steal** money, crash websites, destroy files, and disrupt businesses.
In this way **Hacking** is done by hackers.
Or, **Hacking is identifying weakness/flaws in computer systems or networks to exploit its weaknesses to gain access.**

A "**Cracker"** is someone who breaks into someone else's **computer system**, often on a network; bypasses passwords or licenses in **computer programs**; or in other ways intentionally breaches **computer security**. Thus the Process is known as **Cracking.** Or, **Cracking** means gaining unauthorized access to computer systems to commit a crime, such as digging into the code to make a copy-protected program run and flooding Internet sites, thus denying service to legitimate users.
During a cracking exploit, important information can be erased or corrupted. Websites can be deliberately defaced.

\

The Differences Between Hacking & Cracking are given below,

Hacking	Cracking
1. **Hacking** is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.	1. **Cracking** means gaining unauthorized access to computer systems to commit a crime.
2. **Hacking**, is the act of stealing personal or private data, without the owner's knowledge or consent.	2. **Cracking** is where a cracker edit a program's source code, or you could create a program, like a key generator (more commonly known as a 'keygen'), patch, or some sort of application that tricks an application in to thinking that a particular process has occurred.
3. **Hacking** is for good purposes and improving security of individual's data and work.	3. **Cracking** is done mainly for evil purposes.
4. **Hacker** attacks systems and probing security vulnerabilities for fun, exploration, fame, proving that they can discover weaknesses which can assist owners etc.	4. **Cracking** is pretty much looking for a back door in software, and exploiting it for malicious use or for a copyright breaching act.
5. **Hacker** Building Things.	5. **Cracke**r break things.

2. Write the History of Hacking & Cracking?

Answers

To organize the discussion, we describe three phases of hacking:
Phase 1—the early years (1960s and 1970s), when hacking was a positive term.
Phase 2—from the 1970s to the 1990s, when hacking took on its more negative meanings.
Phase 3—beginning in the mid-1990s, with the growth of the Web and of e-commerce and the participation of a large portion of the general public online.

- Hacking begins in the 60s, mostly at MIT.
  These early hacks are simply shortcuts developed to bypass or improve the operation of systems.
- In 1971 John Draper (Captain Crunch) invents the 'blue box' – a method of making free long distance calls, with the help of a toy whistle given away with Cap'n Crunch cereal.
- In 1972 Steve Wozniak and Steve Jobs learn the art of phreaking, taking the names 'Berkeley Blue'(Wozniak) and 'Oaf Tobar'(Jobs).

- The Chaos Computer Club, Europe's largest association of hackers, is formed in 1981.
- In 1984, The first edition of 2600: The Hacker Quarterly is published.
- In 1986, The Computer Fraud and Abuse Act is passed in the US.
- In 1988, Kevin Poulsen (Dark Dante) hacks a federal computer network, is pursued by the police, and goes into hiding.
- Same year Robert Morris develops the 'Morris Worm', the first computer worm on the internet.
- In 1994, Vladimir Levin accesses the accounts of Citibank's customers through their dial-up wire transfer service, and steals around $10milion.
- In 1997, AOHELL, a hacking program, brings the AOL network to its knees, disrupting chat rooms and inboxes.
- In 2000, The "ILOVEYOU" computer worm is released. It rapidly spreads through email accounts, causing $10billion damage before it is finally stopped.
- In 2000, Michael Calce (MafiaBoy) launches a series of Distributed Denial of Service (DDoS) attacks, bringing down Yahoo!, eBay, CNN, Amazon and Dell.com in the space of a week.
- In 2001, Gary Mckinnon (Solo) hacks into 97 US military and NASA computers, allegedly disrupting operations, deleting files, and posting messages.
- In 2002, Adrian Lamo (the homeless hacker) hacks the website of The New York Times.
- In 2007, George Hotz becomes the first person ever to carrier unlock the iPhone.
- In 2010, George Hotz hacks the PlayStation 3.
- In 2011, Hacker group LulzSec hacks Sony repeatedly, stealing information from 70milion user accounts.
- In 2012, MasterCard and Visa are hacked. More than 1.5 million customers have their credit card numbers stolen.
- In 2013, Hacking group Anonymous hack the Twitter and Flickr accounts of the North Korean governments, posting insulting pictures and inflammatory comments.

3. What are the differences between Virus, Worms and Trojan Horse?

The differences between Virus, Worms and Trojan Horse are given below,

VIRUS	WORMS	TROJAN HORSE
1. A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program.	1. Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage.	1. Trojan horses are impostors--files that claim to be something desirable but, in fact, are malicious. It is a harmful piece of software that looks legitimate.
2. Viruses, which require the spreading of an infected host file	2. Worms are standalone software and do not require a host program or human help to propagate.	2. Users are typically tricked into loading and executing it on their systems.
3. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program.	3. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them.	3. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses).
4. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.	4. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.	4. Trojans are also known to create back doors to give malicious users access to the system.
5. some viruses overwrite other programs with copies of themselves, which destroys the host program altogether.	5. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from	5. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.
	computer to computer, so the entire document should be considered the worm.	

4. Define Identity theft. What are the types of Identity theft? Give Examples.

Answers

Identity theft is the deliberate **use** of **someone else's identity**, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name.

The types of Identity theft are given below,

- Criminal identity theft (posing as another person when apprehended for a crime)
- Financial identity theft (using another's identity to obtain credit, goods and services)
- Identity cloning (using another's information to assume his or her identity in daily life)

- Medical identity theft (using another's identity to obtain medical care or drugs)

Criminal identity theft

When a criminal fraudulently identifies himself to police as another individual at the point of **arrest**, it is sometimes referred to as "Criminal Identity Theft." In some cases criminals have previously obtained state-issued identity documents using credentials stolen from others, or have simply presented fake ID.

Financial identity theft

The most common type is financial identity theft, where someone wants to gain economical benefits in someone else's name. This includes getting credits, loans, goods and services, claiming to be someone else.
Stolen Checks, ATM Cards theft etc. are the types of financial identity theft.

Identity cloning

Identity cloning just may be the scariest variation of all identity theft.
Instead of stealing your personal information for financial gain or committing crimes in your name, identity clones comprise your life by actually living and working as you. They may even pay bills as you - get engaged and married as you - start a family as you. To sum things up, identity cloning is the act of an **imposter** literally assuming your life in a different location.

Medical identity theft medical identity theft occurs when someone seeks medical care under the identity of

another person. Insurance theft is also very common, if a thief has your insurance information and or your insurance card, they can seek medical attention posing as yourself. Child identity theft.

5. What is Online Scamming? Describe with some Examples.

Answers

A **fraudulent scheme** performed by a **dishonest individual**, group, or company in an attempt to obtain money or something else of value is known as scam. When this kind of schemes are performed online i.e. it makes use of the internet, it is called online scamming

Online scams are constantly evolving. Some of the common ones are described below.

Phishing Scams: Phishing emails try to trick the intended victim into visiting a fraudulent website disguised to look like a valid eCommerce or banking site.

Greeting Card Scams: Greeting card scams arrive in email pretending to be from a friend or family member. Clicking the link to view the card typically leads to a booby-trapped web page that downloads Trojans and other malicious software onto the systems of the unsuspecting.

Lottery Winning Scams: Lottery winner scams attempt to trick recipients into believing they have won large sums of cash and to claim this prize the recipient has to pay a fee.

Killer Email – Hitman threat Scams: Imagine opening your email inbox and reading a message from an alleged assassin - claiming you're the target. The gist of the email - pay the hitman thousands of dollars, or die.

Scareware Scams: Scareware claims the system is infected and instructs the user to purchase a 'full version' in order to clean the bogus infections.

6. What do you know about hacking by government?

Answers

Government **agents** may **infiltrate**, **copy**, **delete**, or **damage** data during digital **investigations**. The government may even actively **create** and disseminate/**spread malware** that can damage computers. The government will **design** and **deploy malicious code** that infects computers. All of these falls under hacking by government.

7. What do you mean by Phishing and Smishing?

Answers

Phishing : Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information in disguise of a reputable entity or person in email, IM or other communication channels. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Smishing: Smishing is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.
Smishing is short for "SMS phishing.

8. What are the potential solution for Hacking & Cracking?

Answers

Potential Solutions or Preventive actions for Hacking and Cracking:

Step 1: Tough passwords

You need to have a **separate password** for **each account**, so that if one account gets hacked, all of your vital information is not vulnerable. It's tough to remember dozens of passwords. The answer: a **password manager**. There are a variety of third-party software programs that will create and store passwords for you.

Step 2: Two-Step Authentication

When you log on to many different computers — especially **shared** computers — to access your email account, you are especially vulnerable to hackers. Many websites are moving toward two-step verification.

Step 3: Change Your Behavior

Over-sharing may not be just embarrassing, it may **cause harm**. Things like birth dates and graduation years can be used to access your information. That doesn't mean you need to shut down your online presence, but be careful what details you put out there.

Step 4: Consolidation

Sit down and think about the last 10 years of your online life. And then delete the accounts for the services you signed up for and **no longer use**.

Step 5: Back It Up

Back up all **data** is a must. You can either use an external hard drive or an online service. As more of the things we care about get stored electronically, the more vulnerable they are to get lost.

9.What are the potential solution for Trojan Horse, Viruses and Warms?

Answers

General precautions

- Be suspicious of email attachments from unknown sources.
- Verify that attachments have been sent by the author of the email. Threats can send email messages that appear to be from people you know.
- Do not set your email program to "auto-run" attachments.
- Obtain all Microsoft security updates.
- Back up your data frequently. Keep the (write protected) media in a safe place-preferably in a different location than your computer.

Specific to Anti-Virus Protection

Make sure that you have the most recent virus and spyware definitions. Response to new virus threats daily. By default, checks for updates regularly, the managed client updates Protection Manager as soon as new content is available. Other content, such as Intrusion Prevention signatures need to be updated when needed. Always keep Auto-Protect running. Scan all files, not just program files.

Scan all new software before installing it.

Scan all media that someone else has given you. Use caution when opening email attachments. Email attachments are a major source of virus infections. Microsoft Office attachments for Word, Excel, and Access can be infected by Macro viruses. Other attachments can contain file infector viruses. File system Auto Protect must scan these attachments for viruses as you open or detach them, as do the client email scanners.

10. What are the Problems of Normal identification and Biometric identification?

Answers

Problems of Biometric identification:

Biometric-enabled security creates profound threats to commonly accepted notions of **privacy** and **security**. It makes possible **privacy** violations.

In addition, once someone's **face**, **iris** or **DNA** profile becomes a digital file, that file will be difficult to protect. As the recent NSA revelations have made clear, the boundary between commercial and government data is porous at best.

Biometric identifiers could also be **stolen**.

Current law is not even remotely prepared to handle these developments. The legal status of most types of biometric data is unclear. No court has addressed whether law enforcement can collect biometric data without a person's knowledge, and case law says nothing about facial recognition.

11.Describe one method in financial websites used to convince a consumer that the site is authentic.

Answers

- One is by having a **copyright** mark.
- One is by having an **SSL** (https) certificate, indicating that communication between user's browser and web server will be through secure socket layer.
- By using third party websites like: Trustkeeper, Trustwave will validate the current financial activities of the website.

Steps for SSL:

Step 1: Host with a dedicated IP address.

In order to provide the best security, SSL certificates require your website to have its own dedicated IP address. With a dedicated IP, you ensure that the traffic going to that IP address is only going to your website and no one else's.

Step 2: Buy a Certificate.

A certificate is simply a paragraph of letters and numbers that only your site knows, like a really long password. When people visit your site via HTTPS that password is checked, and if it matches, it automatically verifies that your website is who you say it is – and it encrypts everything flowing to and from it.

Step 3: Activate the certificate.

Step 4: Install the certificate.

Step 5: Update the site to use HTTPS. once it's done then route people to use HTTPS instead of HTTP.

12.Define- Click Fraud, Stock Fraud, Digital Forgery.

Answers

Click Fraud:

Click fraud is the practice of repeatedly clicking on an advertisement hosted on a website with the intention of generating revenue for the host site or draining revenue from the advertiser.

Companies also analyze historical query information to detect and protect against click fraud.

Click fraud is a type of fraud that occurs on the internet in **pay-per-click (PPC)** online advertising.

Fraud occurs when a person, **automated script** or **computer program** imitates a legitimate user of a web browser, clicking on such an ad without having actual interest in the target of the ad's link.

Stock Fraud:

Securities **fraud**, also known as **stock fraud** and investment **fraud**, is a deceptive practice in the **stock** or commodities markets that induces investors to **make purchase** or **sale decisions** on the basis of **false information**, frequently resulting in losses, in violation of securities laws.

According to enforcement officials of the Securities and Exchange Commission, criminals disseminate false and/or fraudulent information's in chat rooms, forums, internet boards and via email (spamming), with the purpose of causing a dramatic price increase in thinly traded stocks or stocks of shell companies.

When the price reaches a certain level, criminals immediately sell off their holdings of those stocks, realizing substantial profits before the stock price falls back to its usual low level.
Any buyers of the stock who are unaware of the fraud become victims once the price falls.

Digital Forgery:

Digital artifacts are subject to forgery as much as any others. Documents, images, sound recordings, can all be manipulated. Detecting digital forgeries is a sophisticated skill.

Digital Forgery is defined as the criminal act that includes the purposeful defrauding, misleading, deception, and misrepresentation of a product, service, or item with the intent to deceive by help of digital tools.

Technology can deceive like Video-manipulation tools provide the opportunity for "forging" people.

13. What step can you take to protect yourself from Identity theft and Credit card theft?

Answers

Tactics and counter tactics in credit card and debit card fraud

Procedural changes helped protect against theft of new cards from the mail.

To verify that the legitimate owner received the card, credit card issuers require the customer to call in and provide identifying information to activate a card. This procedure is only as good as the security of the identifying information. Several Social Security Administration employees provided the Social Security numbers and mothers' maiden names of thousands of people to a credit card fraud ring so that they could activate stolen card**. Now credit card companies use caller ID to verify that the authorization call comes from the customer's telephone.** Similarly, if you send a

change of-address notification to your credit card company, **the company will probably send a confirmation to both your old and new addresses.** they send a change-of-address notice (using a fake address for the new one). A confirmation letter sent to the old address alerts the real card owner. **Encryption and secure servers solved much of that problem;** without such security, e-commerce could not have thrived. **Large stores and banks began printing only the last four digits on the receipts**.. Thieves surreptitiously install recording devices, called skimmers, inside the card readers in stores, gas stations, and restaurants. They collect debit card numbers and PINs, make counterfeit cards, and raid people's bank accounts through ATM machines. **Credit card companies run sophisticated artificial intelligence software to detect unusual spending activity .** When the system finds something suspicious, a merchant can ask a customer for additional identification or the credit card company can call a cardholder to verify purchases.

And to prevent identity theft use the techniques below:

- **Authenticating websites**
- **Authenticating customers and preventing use of stolen numbers Biometrics**

14. How can you discriminate between an email that is a Phishing attempt and an email from legitimate business?

Answers

Tip 1: Don't trust the display name

A favorite phishing tactic among cybercriminals is to spoof the display name of an email. Return Path analyzed more than 760,000 email threats targeting 40 of the world's largest brands and found that nearly half of all email threats spoofed the brand in the display name.

Tip 2: Look but don't click

Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it. If you want to test the link, open a new window and type in website address directly rather than clicking on the link from unsolicited emails.

Tip 3: Check for spelling mistakes

Brands are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.

Tip 4: Analyze the salutation

Is the email addressed to a vague "Valued Customer?" If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.

Tip 5: Don't give up personal information

Legitimate banks and most other companies will never ask for personal credentials via email.

Don’t give them up.

Tip 6: Beware of urgent or threatening language in the subject line

Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your “account has been suspended” or your account had an “unauthorized login attempt.”

Tip 7: Review the signature

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details.

Tip 8: Don’t click on attachments

Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don’t open any email attachments you weren’t expecting.

Tip 9: Don’t trust the header from email address

Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address. Return Path found that nearly 30% of more than 760,000 email threats spoofed brands somewhere in the header from email address with more than two thirds spoofing the brand in the email domain alone.

Tip 10: Don’t believe everything you see

Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it’s legitimate. Be skeptical when it comes to your email messages—if it looks even remotely suspicious, don’t open it.

15. Do you think hiring formal hacker to ensure security is a good idea or a bad idea?

Answers

I think it is a good Idea. Protecting your company from your own "hired gun “If you do make the decision to hire a former hacker, take steps to protect your company from the possible consequences:

- Do a thorough **background check**. Don't assume that what the hacker tells you is true. Believe it or not, some people will claim to be criminals when they really aren't, if they think it will get them a high paying job that makes them look "cool" to their friends.
- Have the hacker sign an employment **contract** (or independent contractor agreement) that very explicitly sets boundaries and prohibits any access not specifically authorized, prohibits any use or sharing with others of information

gathered in penetration testing or other parts of the job, and specifies the penalties for violation.

- Consider having the hacker covered by an employee dishonesty/fidelity bond, or if the hacker is a contractor, require that he provide proof of **insurance** that will reimburse you if he steals from you, defrauds you or otherwise deliberately causes a loss to your business.
- Don't give the hacker access to any more than he needs to do the job for which you've hired him. Never give him administrative passwords. If he can obtain those credentials on his own, you know you have a security problem, but you should not provide him with them.
- If the hacker leaves or when his contract work is over, change passwords (even if you *think* he didn't have them) and make sure strong intrusion detection/prevention controls are in place.
- Monitor network access while and after the hacker works for you and be on the lookout for any suspicious activity. Remember that the hacker may use some other user's account, not necessarily one that you've given him for his own use.

Segment-7 (Chapter 6)

1. List some job categories where the number of jobs declined drastically as a result of computerization.

Answer

Measuring the effects of computers alone is difficult, because other factors influence employment trends, but we can look at some overall numbers.

- As the use of ATMs grew, the number of bank tellers dropped by about 37% between 1983 and 1993.
- The number of telephone switchboard operators dropped from 421,000 in 1970 to 164,000 in 1996.
- The jobs of building, selling, and repairing typewriters have disappeared.
- Railroads computerized their dispatch operations and eliminated hundreds of employees.
- The jobs of electric meter readers disappeared as utility companies installed devices that send meter readings to company computers.
- Similar technology monitors vending machines and oil wells, reducing the number of people needed to check on them in person.
- Shopping on the Internet and self-service checkout systems in stores reduced the need for sales clerks.
- Hundreds of music stores closed and jobs in the printing industry declined as music, magazines, newspapers, and books went digital.

2. List some job categories where the number of jobs increased drastically with increasing use of computers.

Answer

A successful technology eliminates some jobs, but creates others.

- Countless new products and services based on computer technology create jobs: iPods, medical devices, 3-D printers, navigation systems, smartphones and apps for them, and so on and on.
- The Facebook app industry alone accounted for between 180,000 and 235,000 fulltime jobs in the United States in 2011.
- New technologies and products create jobs in design, marketing, manufacture, sales, customer service, repair, and maintenance.
- Computer and Internet technology generated all the jobs at Google, Apple, eBay, Hulu, Amazon, Microsoft, Twitter, Zappos—and thousands more companies.
- The projected growth in employment of computer programmers is attributable to increased demand for new and updated software. By writing computer code, they turn the designs created by software developers into instructions a computer can follow.
- Computer systems analysts workers serve as a link between IT departments and management. They analyze an organization’s computer systems and recommend ways

to make the business run more efficiently. Computer systems analysts employed in this industry often serve as consultants.

- Computer support specialists provide help and advice to consumers or organizations that are using computer software or equipment. Some assist customers who call the company to speak to a specialist when they are having trouble with a software program or networking device.
- Other computer support specialists work in a company's IT department and provide support for other company employees who are having computer problems.

3. Define telecommuting. What are advantages and disadvantages of telecommuting?

Answer

Telecommuting is working from a remote location outside of a traditional office. The remote location can be from home, a coffee shop, or hotel room. The Internet, faxes, phones, webcams, and instant messaging are some of the technological advances that enable this type of work arrangement. Most telecommuters work in the financial, high-tech, and communications industries.

Advantages of Telecommuting:

- **No Commuting.** Depending on your current commute, this can save you anywhere from minutes to hours every day, which you can spend doing things you enjoy, like sleeping, spending more time with your kids or spouse, going to the dog park, or any other activity you'd like to have more time for.
- **Increased Independence.** Working from home puts the onus on you to complete your work without constant reminders, which some people absolutely love. No office politics, no boss breathing down your neck, no distracting coworkers.
- **Increased Savings.** Most people who work from home have very little need for professional clothing, which not having to buy can save lots of money every year. Other things you'll find less need for: gas or public transit passes for commuting, lunches out, dry cleaning, and child care (depending on your situation).
- **More Flexibility.** Again, this depends on the type of job you'll have at home, but many work-from-home jobs allow for a flexible schedule, so if you need to go grocery shopping or do a load of laundry in the middle of the day, it's simple: you can. Or, if you're a morning person or a night owl, you can adjust your work schedule accordingly.
- **Fewer sick days.** Working in a traditional office exposes you to many people's germs, but if you work from home, you have less exposure to people, and therefore, to their germs. Also, if you're feeling under the weather, it's much easier to pamper yourself and still get some work done when you're at home, meaning you'll probably take fewer sick days.

Disadvantages of Telecommuting

- **Decreased human interaction.** If you're the sort of person who thrives on interactions with other people, working from home can feel isolating. It's possible to remedy this feeling with e-mail, phone calls, instant messaging, and video conferencing, but it's no substitute for face-to-face interaction.
- **Blurring Work and Personal Life.** When you work from home, you can't always shut out your personal life while you're working, or turn off your work life while you're "off the clock."
- **Difficulty Demonstrating Workload.** If you're a telecommuter working for a company with a traditional office, your office-bound coworkers might perceive you as doing less work simply because you're at home.

4.Write the reasons for monitoring employee communications.

Answer

Purposes of monitoring employee communications include training, measuring or increasing productivity, checking compliance with rules for communications, and detecting behavior that threatens the employer in some way. The below list a variety of purposes:

- Protect security of proprietary information and data
- Prevent or investigate possible criminal activities by employees. (This can be work related, such as embezzlement, or not work related, such as selling illegal drugs.)
- Check for violations of company policy against sending offensive or pornographic messages.
- Investigate complaints of harassment.
- Comply with legal requirements in heavily regulated industries.
- Prevent personal use of employer facilities (if prohibited by company policy).
- Locate employees.
- Find needed business information when the employee is not available.

5. What is offshoring? Write impact of offshoring in a country.

Answer Offshoring:

Offshoring is obtaining services or products from another country. It can simply refer to relocating certain aspects of a business to another country. It is primarily a geographical activity.
For example, a car manufacturer in the U.S. opens a factory in Thailand to make certain parts they are offshoring and everything still happens within the same company.

Impact of Offshoring:

When companies choose to save on labor costs by sending jobs overseas, it impacts how their human resources departments operate. Offshoring requires HR departments to communicate across cultures and often across time zones, perhaps requiring technological upgrades or management changes. Their role also includes making sure the overseas workers have the skills and training they need to succeed.

With the advent of the Internet came digital document processing, virtual-meeting technologies and other telecommunication advances. Companies no longer need onsite workers to perform every task, so they can shift some responsibilities to lower-paid employees overseas. This economic shift threatens many jobs in the service sector of our economy: Human resources is one of 160 occupation areas susceptible to offshoring, according to a December 2008 report by the U.S. Bureau of Labor Statistics.

6. Write advantage and disadvantage of offshoring.

Advantages of Offshoring:

1. *Business Growth:* Offshoring allows you to reduce one of the most expensive parts of your business, the labor costs. Freeing this up will allow you to reinvest funds in to your business and give you the opportunity to expand your offerings and service.
2. *Access to Staff:* This model gives you access to a young and vast pool of talent. In particular, to English speaking foreign countries, for people who are highly skilled and university educated, implementing offshore teams will complement the existing staff. The wide skill availability through offshoring becomes an advantage for any business looking to fulfill specific requirements.
3. *Greater Availability:* Having a different time zone and a workforce ready for 24×7 operation, gives you an outstanding opportunity to support your clients when they need it and fulfill their ever-changing needs. This results in a better level of service and higher level of customer experience with quicker and direct contact to your business.
4. *Reduced Risk:* To have multiple teams in different countries helps to reduce your risk, provide a greater marketing opportunity and allows you to support your clients when they need it.
5. *Control:* Many businesses may not want to relinquish control of part of their operations and production to an external party. Offshoring allows you to have dedicated staff to work for your company only. You provide the direction, train the staff and everything is done the way you want it to.
6. *Favorable Government Policies:* There are some governments that grant special exemptions and incentives to companies that invest in their economy. These include tax exemptions and access to cheap credit which could improve the bottom- line of the business.

Disadvantages of offshoring

1. Increase Unemployment

- The biggest criticism versus companies that offshore is that it increases the level of unemployment of the local economy.
- The aforementioned companies Caterpillar and Nike have been accused of taking away jobs from Americans and displacing their existing work force in favor of other nationalities.
- These companies argue that by offshoring they are able to improve profitability by lowering costs and increasing revenue. Thus, the increased profits can be used to improve facilities and programs of the principal company.

2. Cultural and Social Differences

- The client will be immersed in the culture and social practices of the host country. This may have an effect on productivity and communication.
- Unlike outsourcing, time zone differentials may work against the offshoring company because production could end up being delayed due to changes in manpower availability.

3. Security Issues

- Whenever you are sharing, transmitting data to another party, you are always at risk of security breach and compromised data integrity.
- There will always be transfer issues when it comes to data even when there is shared space collaboration.
- The decision on whether you should outsource or offshore will depend on the size and complexity of your operations, the scope of work that you need transferred and of course, your resources.
- Generally, you will benefit in terms of cost and depending on how operations are managed, you can realize great productivity on either business model. One thing is for sure both outsourcing and offshoring will be popular strategies for business development in the years to come.

7. **Write the advantages and disadvantages of Outsourcing.**

Answer

Advantages of outsourcing

1. Reduces Cost of Operations

The cost of hiring an external agency or a third-party service provider is lower than setting up in-house operations for a number of reasons:

- An external agency is a separate entity; it is an enterprise that is responsible for its own cost of operations.

- An external agency has the experience to get the job done according to expectation. If you create an in-house department, you will have to invest in the infrastructure and hire the right talent.
- An external agency does not need additional training expenses. An orientation or overview of the project may be required. But if you put up an in-house agency, you will have to invest in training, research and development.

2. Improves Productivity

- By outsourcing select business processes you can improve productivity because your company can focus its resources on its core functions.
- The cost savings from outsourcing can be repurposed to fund revenue- generating programs of the company. For example, the cost savings can be used to improve business infrastructure or enhance its marketing and promotional program.

3. Increases Flexibility

- A company can increase its flexibility with outsourcing by taking advantage of time zone differentials. By simply adjusting work shifts, it is possible to have your business managed for 16 hours by an external agency.

Disadvantages of outsourcing

1. Cultural and Social Differences

- There will be a period of adjustment needed for your company to accommodate certain cultural and social practices of the third party service provider.
- For example, if you contract an agency from the Philippines or India you will have to develop an understanding of their deeply rooted spiritual beliefs the dates of which may conflict with your work schedule.

2. Communication Problems

- Hand- in- hand with cultural and social differences are communication problems. There arise because of differences in perspectives.
- For example, North American companies tend to do business in a straight- forward manner. On the other hand, service providers from the Philippines are more introverted. They tend not to say much and keep to themselves.
- For the North American client it may be taken as a sign of aloofness, uncertainty or incompetence. But in reality, it is just part of their nature as a soft- spoken people.

3. Security Issues

- Despite the promulgation of the Data Protection Act in several popular outsourcing destinations, security breach and data integrity will remain serious issues.
- Even with tight IT networking protocols and safety measures, concerns on security will always come up in the absence of close collaboration.

8. Write the impact of employee monitoring system in the organizations

***Employee Monitoring*:** Employee monitoring allows a business to track employee activities and monitor worker engagement with workplace related tasks. A business using employee monitoring on a computer can measure productivity, track attendance, ensure security and collect proof of hours worked.

Impact of Employee Monitoring System in an organization:

1. Entrepreneurs, executives, and team leaders can reap a lot of rewards from employee monitoring system.

2. Time will be less wasted and cash leak can be eliminated easily

3. Fewer errors as having better employee insight in this way can help one to catch mistakes before they spiral out of control.

4. Monitoring the employees doesn't just identify but also the highest performers which helps in promoting them.

5. Monitoring increases security by making sure that the field employees aren't in danger and the workplace is safer.

6. It has a huge impact in connecting with everyone.

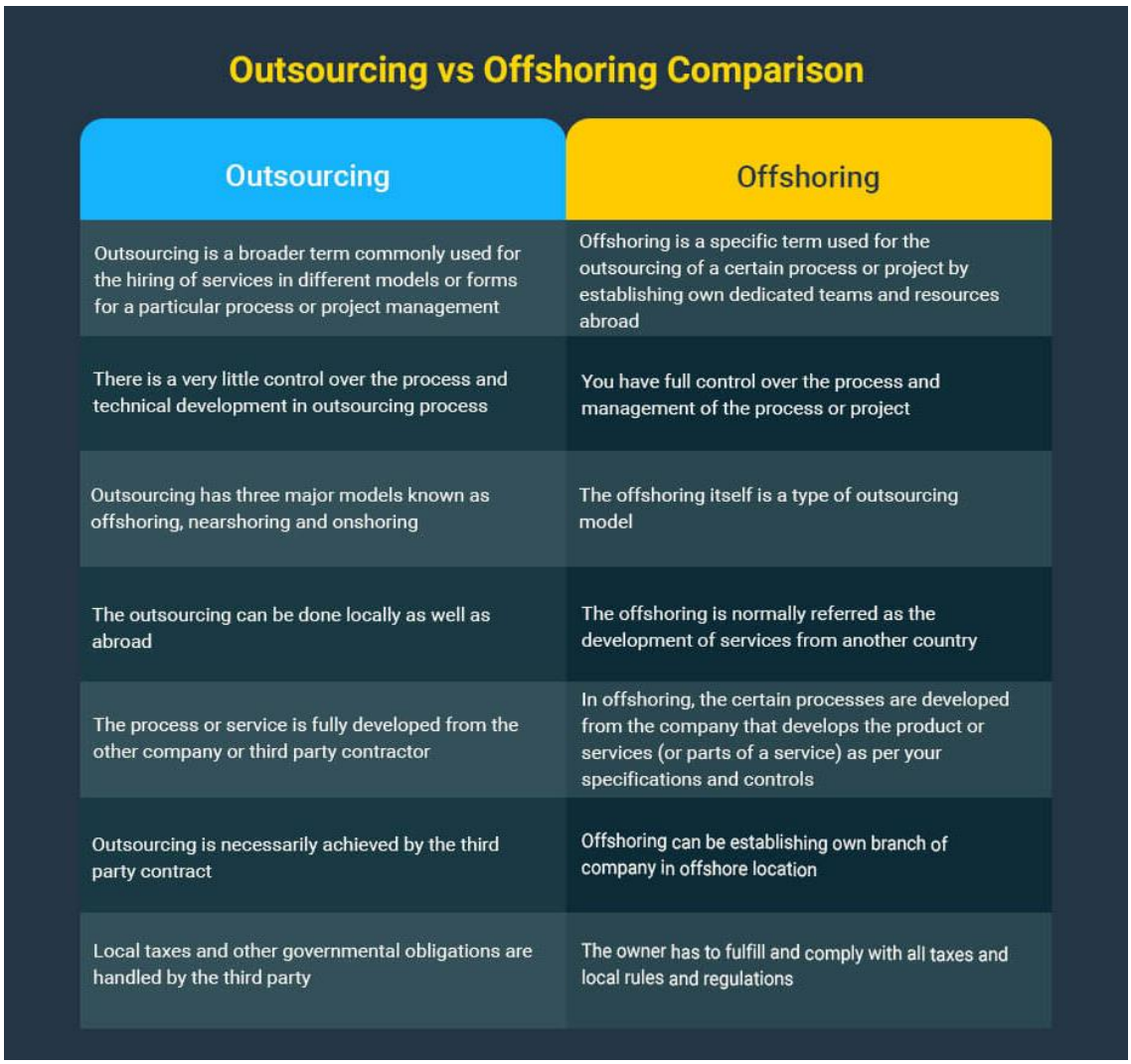
7. Because of access to data from each and every employee, one can get a high level view of what's happening any time he wants

8. Better understanding of employees' strengths and weaknesses leads to better delegation

9. With employee monitoring system a large portion of administrative work can be automated and thus less administrative work.

9. Write the differences between offshoring and outsourcing.

The differences between offshoring and outsourcing are given below,



Outsourcing vs Offshoring Comparison

Outsourcing	Offshoring
Outsourcing is a broader term commonly used for the hiring of services in different models or forms for a particular process or project management	Offshoring is a specific term used for the outsourcing of a certain process or project by establishing own dedicated teams and resources abroad
There is a very little control over the process and technical development in outsourcing process	You have full control over the process and management of the process or project
Outsourcing has three major models known as offshoring, nearshoring and onshoring	The offshoring itself is a type of outsourcing model
The outsourcing can be done locally as well as abroad	The offshoring is normally referred as the development of services from another country
The process or service is fully developed from the other company or third party contractor	In offshoring, the certain processes are developed from the company that develops the product or services (or parts of a service) as per your specifications and controls
Outsourcing is necessarily achieved by the third party contract	Offshoring can be establishing own branch of company in offshore location
Local taxes and other governmental obligations are handled by the third party	The owner has to fulfill and comply with all taxes and local rules and regulations

Segment-8 (Chapter 9)

1. What is "Professional Ethics"?

=> Professional ethics includes relationships with and **responsibilities** toward customers, clients, coworkers, employees, employers, people who use one's products and services, and others whom one's products affect.
We examine ethical dilemmas and guidelines related to actions and decisions of individuals who create and use computer systems. We look at situations where we must make critical decisions, situations where significant consequences for us and others could result. In numerous incidents, journalists at prominent news organizations plagiarized or invented stories. A famed and respected researcher published falsified stem cell research and claimed accomplishments he had not achieved. A writer invented dramatic events in what he promoted as a factual memoir of his experiences. These examples involve blatant dishonesty, which is almost always wrong.

2. What is "Computer Ethics"?

Computer ethics is a part of practical philosophy concerned with how computing professionals should make decisions regarding professional and social conduct. Margaret Anne Pierce, a professor in the Department of Mathematics and Computers at Georgia Southern University has categorized the ethical decisions related to computer technology and usage into three primary influences:
1.The individual's own personal code.
2.Any informal code of ethical conduct that exists in the work place.
3.Exposure to formal codes of ethics.

=> The scope of the term "computer ethics" varies considerably. It can include such social and political issues as the impact of computers on employment, the environmental impact of computers, whether or not to sell computers to totalitarian governments, use of computer systems by the military, and the impact of new applications on privacy.
It can include personal dilemmas about what to post on the Internet and what to download.

3. How Professional ethics differs from general ethics?

=> Professional ethics have several characteristics different from general ethics.

The role of the professional is special in several ways.
First, the professional is an **expert** in a **field**, be it **computer science** or **medicine**, that most customers know little about. Most of the people affected by the devices, systems, and services of professionals do not understand how they work and cannot easily judge their quality and safety. This creates responsibilities for the professional. Customers rely on the knowledge, expertise, and honesty of the professional.

Second, the products of many professionals (e.g., highway bridges, investment advice, surgery protocols, and computer systems) profoundly affect large numbers of people. A computer professional's work **can affect the life**, health, finances, freedom, and future of a client or members of the public. A professional can cause great harm through dishonesty, carelessness, or incompetence. Often, the victims have little ability to protect themselves; they are not the direct customers of the professional and have no direct control or decision making role in choosing the product or making decisions about its quality and safety.

Thus, computer professionals have special **responsibilities**, not only to their customers, but also to the general public, to the users of their products, regardless of whether they have a direct relationship with the users.
These responsibilities include thinking about potential risks to privacy and security of data, safety, reliability, and ease of use. They include taking action to diminish risks that are too high.

we observed that although people often associate courage with heroic acts, we have many opportunities to display courage in day-to-day life by making good decisions that might be unpopular.
Courage in a professional setting could mean admitting to a customer that your program is faulty, declining a job for which you are not qualified, or speaking out when you see someone else doing something wrong.

4. What are the Professional Codes of Ethics?

=> Many professional organizations have codes of professional conduct. They provide a general statement of ethical values and remind people in the profession that ethical behavior is an essential part of their job.
The codes provide reminders about specific professional responsibilities. They provide valuable guidance for new or young members of the profession who want to behave ethically but do not know what is expected of them, people whose limited experience has not prepared them to be alert to difficult Ethical situations and to handle them appropriately.
There are several organizations for the range of professions included in the general term "computer professional." The main ones are the ACM and the IEEE Computer Society (IEEE CS).
They developed the Software Engineering Code of Ethics and Professional Practice (adopted jointly by the ACM and IEEE CS) and the ACM Code Of Ethics and Professional Conduct. The Codes emphasize the basic ethical values of honesty and Fairness. They cover many aspects of professional behavior, including the responsibility to respect confidentiality, maintain professional competence, be aware of relevant laws, and honor contracts and agreements.

5. Write a guideline for Professional Responsibilities of computer user?

=> **Note: //Couldn't find the answer of this question too. //**

1.1 Contribute to **society** and human well-being.
1.2 Avoid **harm** to others.
1.3 Be **honest** and **trustworthy**.
1.4 Be fair and take action not to **discriminate**.
1.5 Honor property rights including copyrights and patent.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.

6. Write short note on Software Engineering Code of Ethics and ProfessionalPractice.

=> The short version of the code summarizes aspirations at a high level of the abstraction; the clauses that are included in the full version give examples and details of how these aspirations change the way we act as software engineering professionals. Without the aspirations, the details can become legalistic and tedious; without the details, the aspirations can become high sounding but empty; together, the aspirations and the details form a cohesive code.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1.PUBLIC – Software engineers shall act consistently with the public interest.

2.CLIENT AND EMPLOYER – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.

3.PRODUCT – Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

4.JUDGMENT – Software engineers shall maintain integrity and independence in their professional judgment.

5.MANAGEMENT – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

6.PROFESSION – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

7.COLLEAGUES – Software engineers shall be fair to and supportive of their colleagues.

8.SELF – Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

7. Write short note on ACM Code of Ethics and Professional Conduct

=> Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct.
Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

Lecture-5 Intellectual Property Right

I. What is Intellectual Property (IP)?

Intellectual Property:

Intellectual property is the legal right to ideas, inventions and creations in the industrial, scientific, literary and artistic fields. It also covers symbols, names, images, designs and models used in business.

2. What are intellectual property rights? Write its benefits or businesses. *Intellectual Property Rights:*

Intellectual property rights are like any other property right. They allow creators, or owners, of patents, trademarks or copyrighted works to benefit from their own work or investment in a creation. These rights are outlined in Article 27 of the Universal Declaration of Human Rights, which provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions.

Benefits for businesses:

Establishing intellectual property protection for our goods, services or brand names is important for a variety of reasons. Intellectual property can:

- Establish a right to, and ownership of, our intellectual creations so we can profit from them
- Prevent competitors from copying or closely imitating our products or services
- Protect the distinct identity, image, and reputation of our business
- Build customer trust and loyalty by establishing a unique brand name or image
- Local cultures also are at stake when works by local artists, authors and musicians are displaced by the illegal sale of pirated music, films and handicrafts.

3. Why do countries protect intellectual property?

Countries know that safeguarding intellectual property rights fosters economic growth, provides incentives for technological innovation, and attracts investment that will create jobs and opportunities for all their citizens.

4. Write the forms of intellectual property.

The forms of intellectual property are described

below: ***Copyright***

Copyrights offer essentially the only protection for music, films, written works of fiction, poems,
architectural designs and other works of cultural value. The owner of copyrighted material has
exclusive rights to reproduce the work, prepare derivative works, distribute copies of the work,

and perform or display the work. Intellectual property now includes such works as computer programs and sound recordings.

For works created after January 1, 1978, copyright protection generally lasts for the life of the author plus 70 years. Only an author or someone deriving their rights through the author, like a publisher, can claim copyright.

Patents

A patent gives the inventor the exclusive right to prevent others from making, using or selling a similar product for a fixed period of time 20 years in most countries.

Trade secrets

Any information that may be used in the operation of a business and is sufficiently valuable to give actual or potential economic advantage is considered a trade secret. Examples are recipes for popular food products, customer mailing lists, advertising strategies and distribution processes.

Trademarks

Trademarks are commercial source indicators, distinctive symbols, words or designs that identify certain goods or services produced or provided by a specific person or enterprise.

Geographical indications

Geographical indications identify a good as having a certain quality, reputation or other characteristic attributed to its location of origin. Geographic indications are treated as a subset of trademarks used to prevent consumer confusion.

5. What is intellectual property for software? Why intellectual property for software is important?

Intellectual property for software is inventive functions, methods, systems, and algorithms, including applied mathematical formulas. It also protects the graphical or ornamental aspects of a screen display by law under a copyright, trademark, trade secret, or software patent.

Software innovation is valuable to individuals, start-ups, and businesses. The law is the best way to protect material such as software. When you treat your software as intellectual property, you have more control over who gets to use it and how it gets to the public. Otherwise, people might use it without permission, and you'll lose the chance to get paid when people use your software. In extreme cases, you might lose the right to use software you created.

6. How to protect your software with intellectual property protection?

The U.S. Congress offers creators of computer software three direct types of intellectual property protection: patent protection, copyright protection and trade secret protection. Many products make use of two or even all three of these techniques.

L Patent Protection

A patent protects ideas and algorithms in a computer product rather than the particular set of code used to implement them.

Two basic types of patents are utility patents and design patents. Examples of utility patents include inventive functions, methods, systems, and algorithms, including applied mathematical formulas. Design patents, while not protecting the functional aspects of a screen display or a portion of computer code, protect the graphical or ornamental aspects of a screen display. Over 10,000 U.S. patents had been granted for software inventions by 1989.

ii. Copyright Protection

Copyright applies to virtually all computer software. It protects the form of expression, both source and object code, from duplication or close imitation. Beyond the program code itself, copyright may be applied to the program's structure, sequence and organization, and some elements of the user-interface (the "look and feel"). The copyright holder may prevent others from modifying or adapting the product for distribution in its modified form.

iii. Trade Secret Protection

Code, ideas, and concepts may be treated as trade secrets so long as they are not obtainable through other products by lawful means, including reverse engineering. However, it is essential that to take sufficient steps to develop a Trade Secret Protection Program for your software. A Software Developer must maintain the confidentiality of the source code to ensure trade secret protection. A proper Protection Program will include steps like requiring confidentially agreements, ensuring limited access to source code, having password protections, and limiting the number of people with access to sensitive information.

Imagine a clever software developer who writes a program that predicts the Stock Market with 99% accuracy. If he patents his software, in 20 years, everyone can create, use, and sell similar software. However, if he keeps the software a trade secret, he can control the source code indefinitely and no one will ever know how he achieved such accuracy.

7. What is a Patent? Why are patents necessary?

A patent is an exclusive right granted for an invention - a product or process that provides a new way of doing something, or that offers a new technical solution to a problem. A patent provides patent owners with protection for their inventions. Protection is granted for a limited period, generally 20 years.

Patents provide incentives to individuals by recognizing their creativity and offering the possibility of material reward for their marketable inventions. These incentives encourage innovation, which in turn enhances the quality of human life.

8. What kind of protection do patents offer?

Patent protection means an invention cannot be commercially made, used, distributed or sold without the patent owner's consent. Patent rights are usually enforced in courts that, in most systems, hold the authority to stop patent infringement. Conversely, a court can also declare a patent invalid upon a successful challenge by a third party.

9. What rights do patent owners have?

A patent owner has the right to decide who may — or may not — use the patented invention for the period during which it is protected. Patent owners may give permission to, or license, other parties to use their inventions on mutually agreed terms. Owners may also sell their invention rights to someone else, who then becomes the new owner of the patent. Once a patent expires, protection ends and the invention enters the public domain. This is also known as becoming off patent, meaning the owner no longer holds exclusive rights to the invention, and it becomes available for commercial exploitation by others.

10. What kinds of inventions can claim for patent?

Patents may be granted for inventions in any field of technology, from an everyday kitchen utensil to a nanotechnology chip. An invention can be a product such as a chemical compound, or a process, for example or a process for producing a specific chemical compound. Many products in fact contain a number of inventions. For example, a laptop computer can involve hundreds of inventions, working together.

Patents are divided up into three kinds: design, plant, and utility. They are given below:

a) ***Design Patents:*** A design patent is granted for protection of the "visual ornamental characteristics embodied in, or applied to, an article of manufacture." Design patents can apply to everything from a fashion designer's latest fabric design to an iPhone skin.

b) ***Plant Patents:*** A plant patent is granted to inventors who, "invent or discover and asexually reproduced a distinct and new variety of plant, other than a tuber propagated plant or a plant found in an uncultivated state." Plant patents are granted to inventors such as the inventors for the newest rose bowl parade rose and for those who create new forms of fruit trees.

c) ***Utility Patents:*** Utility patent protection covers the largest range of patent protection. Types of inventions in this category include useful processes, machines, articles of manufacture, and compositions of matter. For instance, in 2004 an inventor discovered a new way to bond color pigments with steel during the steel's initial curing phase. This useful process eliminated the need for spray painting during manufacture.

11. What is a trademark? Why it is important?

A trademark is any word, name, symbol, or device used to indicate the source of goods or services. Trademarks can be used to protect the company name or product name, domain names, images, symbols, logos, slogans, colors, product designs and product packaging. Registering of trademark will help to prevent others from using others mark in a way that might confuse customers or damage others business reputation.

Protecting the brand is especially important if the software is not entitled to other forms of protection. For example, an Internet browser may not be patentable, but a trademarked brand name can help ensure that the public perceives the browser as unique product associated solely with your company.

12. What are the benefits of protecting copyright?

The exclusive and assignable legal right, given to the originator for a fixed number of years, to print, publish, perform, film, or record literary, artistic, or musical material. Copyright is an essential component in fostering human creativity and innovation, Giving authors, artists and creators incentives in the form of recognition and fair economic reward increases their activity, output, and can also enhance the results. By ensuring the existence and enforceability of rights, individuals and companies can more easily invest in the creation, development and global dissemination of their works. This, in turn, helps to increase access to and enhance the enjoyment of culture, knowledge and entertainment the world over, and stimulates economic and social development.

13. What is the World Intellectual Property Organization? *World Intellectual Property Organization (WIP0):*

The World Intellectual Property Organization (WIPO), established in 1970, is an international organization dedicated to helping ensure that the rights of creators and owners of intellectual property are protected worldwide, and that inventors and authors are therefore recognized and rewarded for their ingenuity.

This international protection acts as a spur to human creativity, pushing back the limits of science and technology and enriching the world of literature and the arts. By providing a stable environment for marketing products protected by intellectual property, it also oils the wheels of international trade. WIPO works closely with its Member States and other constituents to ensure the intellectual property system remains a supple

and adaptable tool for prosperity and wellbeing, crafted to help realize the full potential of created works for present and future generations.

14. How does WIPO promote the protection of intellectual property?

As part of the United Nations system of specialized agencies, WIPO serves as a forum for its Member States to establish and harmonize rules and practices for the protection of intellectual property rights. WIPO also services global registration systems for trademarks, industrial designs and appellations of origin, and a global filing system for patents. These systems are under regular review by WIPO's Member States and other stakeholders to determine how they can be improved to better serve the needs of users and potential users.

In helping these systems to evolve through treaty negotiation; legal and technical assistance; and training in various forms, including in the area of enforcement.

WIPO works with its Member States to make available information on intellectual property and outreach tools for a range of audiences — from the grassroots level through to the business sector and policymakers — to ensure its benefits are well recognized, properly understood and accessible to all.

15. What is fair use, and why is it

important? ***Fair use:***

Fair use is an exemption within copyright law that potentially allows anyone to use copyrighted material without payment and without permission, subject to certain stipulations. In other words, every time you use a quotation in a paper. Every time you use an image in a PowerPoint presentation, and every time you rely on someone else's idea in order to enhance and create your own ideas, you are relying on the "fair use" exemption.

Why is Fair use important?

Fair use provides an important exception to copyright that helps to balance the interests of creators and the public good. Fair use provides an important safeguard against censorship via copyright.

Without fair use, universities, newspapers, TV programs, artists, and many others would have to ask permission for every time they have used another person's idea. Additionally, rightsholders can (and do!) refuse to grant permission for uses they see as undesirable or damaging, such as critical reviews. Without fair use, Google would have to pay someone every time a sentence from a website appears in search results. You would have to pay every time you quote someone's work. Musicians would have to pay every time they re-mix an album. In other words, creative and intellectual exercises would be next to impossible. Fair use is incredibly important for universities, and this ruling was a resounding victory for fair use on many fronts.

15. What is the fair use of doctrine?

Fair Use Doctrine

Fair use is a legal doctrine involving copyright. It is considered fair use to incorporate copyrighted material without permission when certain conditions apply. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:

a. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

b. the nature of the copyrighted work;

c. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

d. the effect of the use upon the potential market for or value of the copyrighted work.

17. Define Proprietary Software. Write the advantages and disadvantages of Proprietary Software.

Proprietary software is a piece of code that belongs to a single individual or organisation. In terms of online trading, you may have your own trading robot. And it will be your proprietary software, as it is a piece of code that is used to execute the trades.

Advantages: There are three advantages of opting out for a proprietary software.

- The first one - a competitive advantage. When a person develop a robot or a company develops a platform, they will have something unique. An individual is able to use this software to attract investors. A company may attract more clients.

✓ Secondly, a company gains quite some independence when it starts relying on its own software. What if a 3rd party platform developer goes out of business or decides to quadruple the price of the software? A company would have to suffer a lot, as it relies on this piece of software. This won't happen when a proprietary software is used.

- Finally, customisation is what really matters for many. With your own software it is possible

to tweak anything you want.

Disadvantages: There are quite many weak points too, but the main one is the resources needed for development.

V' Costly your own trading software is quite costly and not always needed.

V· Imagine you have to write an article. Would you fire up MS Word or any other text editor and just do the job or would you rather ask someone to code a word-processing software for you and then write the article?

Besides that, a company still needs to maintain the software, update it and so on.

18. Define Open-Source Software. Write the advantages and disadvantages of Open-Source Software.

Open Source software, like its name suggests, provides users with an open code that can be freely used, modified, and shared by everyone. Open source licenses can grant you the right to copy and redistribute the software to everyone you want. There are no set boundaries or any limitations.

Advantages: There are four advantages of opting out for an Open-Source Software.

1. It's generally free — it has been estimated that open source software collectively saves businesses $60 billion a year. These days for virtually every paid for proprietary software system you will find an open source version.
2. It's continually evolving in real time as developers add to it and modify it, which means it can be better quality and more secure and less prone to bugs than proprietary systems, because it has so many users poring over it and weeding out problems.
3. Using open source software also means you are not locked into using a particular vendor's system that only work with their other systems.
4. You can modify and adapt open source software for your own business requirements, something that is not possible with proprietary systems.

Disadvantages: There are quite many weak points too:

1. Because there is no requirement to create a commercial product that will sell and generate money, open source software can tend to evolve more in line with developers' wishes than the needs of the end user.
2. For the same reason, they can be less "user-friendly" and not as easy to use because less attention is paid to developing the user interface.
3. There may also be less support available for when things go wrong — open source software tends to rely on its community of users to respond to and fix problems.
4. Although the open source software itself is mostly free, there may still be some indirect costs involved, such as paying for external support.
5. Although having an open system means that there are many people identifying bugs and fixing them, it also means that malicious users can potentially view it and exploit any vulnerabilities.

19. Open-source versus proprietary software: Is one more reliable and secure than the other?

There are significant differences between these two variations of software, and each has benefits and drawbacks of their own.

While proprietary software has its advantages in maintaining developers' rights (something pretty important considering there are plenty of impersonating software out there looking to copy popular ones), we personally tend to lean in the direction of open-source software.

Sure, proprietary software is popular among developer studios looking to protect their assets and provide security for their intellectual property, however open-source programs are bigger with developers who decide to crowdfund their ideas.

Because open-source software is open to a community of contributors, it really just gets everyone involved and feeling like they are investing into the project, from a

non-monetary perspective. Essentially, it is what they say "by the people, for the people".

Not to mention, open-source programs will put a lot less stress on the developing team to develop every single part of the program, when the program can be self-reliant on contributors.

Is open source more secure than proprietary software?

The answer is probably yes, open source software is more secure than proprietary software in most cases.

More eyes will lead to better software. In open source particularly, those eyes are "fresh" and did not code on the project for months, therefore the possibility for finding security issues is greater. However, there's still a problem with the way most open source projects are maintained. For example — did you know that OpenSSL was maintained by two guys named Steve? Linus's law

doesn't always apply since the majority of users just plug & play. They do not actually go over the code.

Although I work for a company which alerts on security vulnerabilities and bugs, and we have seen many security vulnerabilities in open source in the past 2 years, it still doesn't mean open source is not safe. Can you imagine what would have happened if tens of thousands of people went over your proprietary code. Would they have found something you missed?

Yet I must add that nowadays, when it comes to software development, it's not a question
whether to choose open source or proprietary code, they do not compete with each other, or at
least don't aim to. Companies should use open source as complementary software in their

Lecture 6 Cyber Crime and Cyber Law

Information and Communication Technology Act (ICT) Act 2006

In order to facilitate e-commerce and promote the growth of information technology, the Information and Communication Technology Act (ICT) of 2006 of Bangladesh established provisions with a maximum penalty of up to 10 years imprisonment or a fine of up to 10 million taka or both. The ICT Act, 2006 as amended in 2013 is obviously quite a brilliant feat in the cyber law field of Bangladesh.

The ICT law was formulated to promote the development of Bangladesh's information and communication technologies. The aim is to facilitate the use of ICTs to build the information society.

The purpose of this Act is to guarantee the legal security of documentary communications between persons, partnerships and the State, irrespective of the medium used; the consistency of legal rules and their application to documentary communications using information technology- based media, whether electronic, magnetic, optical, wireless or otherwise, or based on technology combinations.

The ICT Act promotes the Public Key Technology Trust Chain. The law allows digital certificate infrastructure to be developed and managed by the Controller of Certifying Authorities (CCA), including audits to be carried out. Some Cyber Crimes which are to be dealt through this act are follows:

- Hacking or unauthorized entry into information systems
- Introduction of viruses
- Publishing or distributing obscene content in electronic form
- Tampering with electronic documents required by law
- Fraud using electronic documents
- Violation of privacy rights such as STALKING
- Violation of copyright, trademark or trademark rights

What are the main offences in Bangladesh in regards to ICT Act 2006?

Some of the main offences are pointed out below that may arise out of Online Law / Internet Law in Bangladesh ICT Rules, Regulations and Rights in Bangladesh (not in any specific order.)

1. Fake Electronic Publication

Anyone who commits the offense of electrically publishing false, obscene or defaming informati on shall be punished with imprisonment for a term of at least 7 years and a maximum of 14 year, and with a fine of up to 10 Taka lakes or both.

2. Hacking an electronic device (Hacking a Computer/Phone/Info):

Anyone who commits the offense (Hacking) of electrically publishing false, obscene or defaming information shall be punished with imprisonment for a term of at least 7 years and a maximum of 14 year, and with a fine of up to 10 Taka lakes or both.

3. Unauthorized access to protected systems in Bangladesh

Anyone who commits an offense of unauthorized access to protected systems shall be punished with imprisonment for a term which may extend to a minimum of 7 years and a maximum of 14 years or a fine which may extend to or with 10 lakes of Taka.

4. Disclosure of confidentiality and privacy in Bangladesh:

Any person committing disclosure of confidentiality and privacy shall be punished with imprisonment for a term of up to two years or with a fine of up to two Taka lakes or both.

5. Using a computer to help commit an offence in Bangladesh

Any person who assists in committing an offense as set out above shall be punished with the penalty for the core offence.

Findings on ICT Act 2006

1 Computer related crimes known as cybercrimes such as hacking, virus attack, online fraud, credit card fraud etc are increasing and it becomes a challenge to prevent and penalize.

2 Many cybercrimes or digital crimes did not fall under the purview of the law. For example, the law did not address any crime committed through using mobile phones. “Even the amendments did not address these issues.”

3 The law also considers e-mails as evidence, which conflicts with the country's Evidence Act which does not recognize e-mails as evidence, but the amendments did not address these issues.

4 By the amendment of ICT Act, 2006 in 2013, police have been given power to arrest

without warrant. Police can misuse this power. Making offences mentioned under ICT Act, 2006 cognizable may increase harassment to the general internet users and arbitrary arrest by police. As a result people can victim of arbitrary arrest. Terming the act a "black law" for the Article 57 provision for arrest without warrant

5 Without adopting any check and balance principle in respect of police power of arrest without warrant under ICT Act, 2006 is not justifiable. The number of person arrested under this Act is gradually increasing. But the process of arrest raises debate in the mind of the people.

6 Although the legitimate purpose of vesting police the power of arrest without warrant is to control and penalize cyber criminals, there exists an opportunity of using it as a political weapons. If it is used as so, the fundamental rights particularly the freedom of speech guaranteed in the constitution may be violated.

7 Police power of arrest has been legislated without any consideration for the nature of the internet. It is not the possible solution for stopping cybercrimes. For examples Geographical distances and borders are irrelevant to cybercrime. A cybercriminal sitting in one corner of the globe may hacked into the victim's bank's computer located in another corner and transfer funds online to yet another corner. Though the nature of cybercrime suggests that law enforcing agencies must empowered to use filter technology rather than using power of arrest without warrant, but the use of filter technology by law enforcing agencies has not been developed in our country.

Digital Security Act 2018

As per news reports, the Jatiya Sangsad (Parliament of Bangladesh) passed the Digital Security Act, 2018 on September 19, 2018. The Parliament passed the bill through a voice vote after the bill was presented by Mustafa Jabbar, the Minister of Post, Telecommunications, and IT. The Digital Security Act, 2018 has been ostensibly framed with the intention of ensuring national digital security in Bangladesh along with preventing and prosecuting digital offenses, but in practice, it poses significant threats to free expression.

Provisions under the Digital Security Act reportedly include imprisonment for multiple years and fines up to 10 million Taka (approximately USD 100,000) for use of digital media to intimidate people or cause damage to the state, or publishing information with the intent to defame someone. Additionally, the police are provided powers to search any person or place without a warrant, on suspicion of an offense being committed under the Digital Security Act.

Findings on Digital Security Act 2018

- The Digital Security Act establishes a Digital Security Agency as well as a National Digital Security Council, but the powers and functions of these entities are currently unclear. This law also establishes "digital offenses," penalties thereof, and authority for police to investigate such offenses.
- The law allows for up to 10 years imprisonment for spreading propaganda against

Bangladesh's Liberation War, the national anthem and national flag using digital devices. Repeated offences carry the maximum penalty of life imprisonment.

- The Editors Council of Bangladesh on 17 September 2018 rejected the draft Digital Security Act as it did not make the changes that were recommended in eight sections of the law. The law fails to uphold the guarantees of freedom of expression and freedom of the press in the Constitution of Bangladesh in Articles 39(2) A and B and international treaties ratified by the country.
- The newly enacted Digital Security Act 2018 in Bangladesh which has drawn serious concerns for press freedom and the right to freedom of expression - Amnesty International's South Asia Campaigner.

v' The new Digital Security Act under section 43 allows police in Bangladesh to arrest an individual if they believe that an offence under the law has been or is being committed or there is a possibility of committing crimes or destroying evidence.

1' Unfortunately, ARTICLE 19's analysis shows that not only does the 2018 Act expand existing restrictive provisions, it includes several provisions that are in breach of international human rights law. In particular, several definitions contained in the 2018 Act are too vague and overbroad.

Special Observation on article 19 of Digital Security Act 2018:

v' In this analysis, ARTICLE 19 reviews the compatibility of the Bangladesh Digital Security Act 2018 (the 2018 Act), adopted in October 2018, for its compliance with international standards on freedom of expression.

v' ARTICLE 19 concludes that the 2018 Act is deeply flawed and that it should be reviewed and its most problematic provisions repealed as a matter of urgency.

v' According to Article 19, the act violates human rights and threatens freedom of speech in Bangladesh. According to Amnesty International the act places *"dangerous restrictions on freedom of expression"*. It believed the act will be used against dissidents, similar to the way Information and Communication Technology Act was used to detains hundreds of people. The act has been criticized by the United States as something that could be used to suppress free speech. Bangladesh Nationalist Party has called for the act to be repealed.

Offences and Penalty of Digital Security Act 2018

- Section 3 of the new law includes a provision of the Right to Information Act 2009, which will be applicable in case of right to information-related matters.
- As per section 32 of the law, if a person commits any crime or assists anyone in committing crimes under Official Secrets Act, 1923, through computer, digital device, computer network, digital network or any other electronic medium, he or she may face a maximum 14 years in jail or a fine of Tk 25 lakh or both.

- The law also includes a definition of the "Spirit of the Liberation War" in section 21,

which says, “The high ideals of nationalism, socialism, democracy and secularism, which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle.”

- According to section 29 of the law, a person may face up to three years in jail or a fine of Tk 5 lakh or both if he or she commits the offences stipulated in section 499 of the Penal Code through a website or in electronic form.
- Section 31 of the act says a person may face up to seven years in prison or Tk 5 lakh in fine or both if he or she is found to have deliberately published or broadcast something on a website or in electronic form which can spread hatred and create enmity among different groups and communities, and can cause deterioration in law and order.

History of the Intellectual Property (IP) system in Bangladesh

The earliest legislation found to protect IP in Bangladesh was the Patents, Designs, and Trademarks Act of 1883. However, it was repealed, and the new Patents and Designs Act of 1911 and the Trademarks Act of 1940 were enacted respectively. Then, in 2003, both these Acts were amended, and the Departments of Patents, Designs, and Trademarks (DPDT) was created by merging two independently operational offices – the Patent Office and the Trademark Registry Office. The Trademarks Act 2009 was enacted after the Trademarks Ordinance was promulgated in 2008.

The copyright system in Bangladesh has resulted from the British Copyright System and the Copyright Ordinance that was promulgated by the amalgamation of different Copyright Laws in 1962. After the administration of this Ordinance up to 1999, the Copyright Act was enacted in 2000 and amended in 2005.

Present Scenario of IP system in Bangladesh

Because of the impact of globalization in the commercial environment, Intellectual Property Law in Bangladesh has now become an international concern. Bangladesh participated in the convention founding the World Intellectual Property Organization (WIPO) on May 11, 1985. It became a legal member of the Paris Convention for the Protection of Industrial Property and of the Berne Convention for the Protection of Literary and Artistic Works in 1991 and 1999 respectively. It is also a signatory of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement of the World Trade Organization (WTO).

IP Law in Bangladesh is administered by two offices empowered under two ministries: The DPDT under the Ministry of Industries (MOI) and the Copyright Office under the Ministry of Cultural Affairs (MOCA).

At present it is thought that eight subjects fall within the scope of Intellectual Property Rights. These are 1) Copyright, 2) Patents, 3) Industrial Designs, 4) Trade Marks and Merchandise Marks 5) Geographical Indications, 6) Layout Designs of Integrated Circuits, 7) Plant Variety Protection and 8) Electronic

Transactions or in other words Information Technology. Out of these eight

subjects Bangladesh has legislation on Patents and Designs since 1911, on Trade Marks since 1940 and on Copyright since 1962. In most of the countries of the World Patents and Industrial Designs are two different subjects and they have two different legislations on the same.

Out of aforesaid eight subjects of intellectual property rights the Law Commission prepared the draft law on 5 subjects of which on four updating was done while fifth one, viz. Information Technology in other words Law on Electronic Transactions is completely a new enactment in the context of Bangladesh. Bangladesh does not have any law on 3 subjects of Intellectual property rights, namely, 1) Geographical Indications, 2) Layout Designs of Integrated Circuits and 3) Plant Variety Protection.

To respect intellectual property rights (IPR), Bangladesh has enacted intellectual property laws. It has incorporated the relevant provisions from international standards in this regard.

Bangladesh has enacted the following laws on IPR:

1. Patent and Design Act, 1911
2. Trademarks Act, 2009
3. Copyright Act, 2000 (amended in 2005)

The Patents and Designs Act, 1911: Under this act, the Department of Patents, Design and Trademark (DPDT) provides patent protection (registration) to the patent holders for 16 years on payment of prescribed fees. Duration of protection may be renewed for a further period. A patent confers on the patentee the exclusive privilege of making, selling and using the invention throughout Bangladesh and of authorizing others to do so. For details and updated information on protection of patents and design,visit www.dpdt.gov.bd

Trade Marks: Under the Trade Marks Act, 2009, protection is granted for seven (7) years and it can be renewed after every expiry for further ten (10) years on payment of renewal fees. For details and updated information on Trademarks, visit www.dpdt.gov.bd

Copyright: The Copyrights Act, 2000 (amended in 2005) provides protection to authors, artists or dramatists. Copyright law protects only the form of expression of ideas, not the ideas themselves. In order to get a copyright, the owner has to show that the work is original. For details on Copyright protection in Bangladesh, visit www.copyrightoffice.gov.bd

Industrial Design/ Design: Under the Patents and Designs Act, 1911, any person claiming to be the proprietor of any new or original design not previously published in Bangladesh may register the design. The registered proprietor of the design shall have copyright in the design for five (5) years from the date of registration. For details and updated information on Patents and Designs, visit www.dpdt.gov.bd

Copyright Law in Bangladesh What is

Copyright?

 Copyright is a legal means of protecting an author's work. It is a type of intellectual property

that provides exclusive publication, distribution, and usage rights for the author. This means whatever content the author created cannot be used or published by anyone else without the consent of the author.

What copyright does not protect?

Copyright does not protect facts, ideas, systems, or methods of operation, although it may protect the way these things are expressed.

How is a copyright different from a patent or a trademark?

Copyright protects original works of authorship, while a patent protects inventions or discoveries. Ideas and discoveries are not protected by the copyright law, although the way in which they are expressed may be. A trademark protects words, phrases, symbols, or designs identifying the source of the goods or services of one party and distinguishing them from those of others.

Copyright Law of Bangladesh: An Overview

In Bangladesh, the copyright protection is governed by the Copyright Act 2000 (amended in 2005) and Copyright Rules 2010. As per the governing acts, the Copyright in literary, musical, dramatic, or artistic work continues for the lifetime of the author and until 60 years from the following death year. Nonetheless, the copyright for cinematographic film, a computer program, a photograph, or a sound recording, exists for 60 years from the publication of the work.

Copyright law protects only the form of expression of ideas, not the ideas themselves. It protects the owner of property rights against those who copy or otherwise take and use the form in which the original work was expressed by the author.

Definition of copyright

According to section 15 copyright subsists in

- literary works
- dramatic works
- musical works
- artistic works (*i.e.* painting, sculpture, drawing, engraving or a photograph, a work of architecture and any other work of artistic craftsmanship)
- cinematographic films
- sound recordings

and includes computer programmes (cf. s. 14 sub-s. 2) as well as addresses and speeches (cf. s. 17 cl. d).

Foreign works are covered by section 69 read with the *International Copyright Order, 2005*.

Owner of copyright

- The first owner of copyright in general is **author** (exceptions: works for hire, Government works; s. 17).
- The owner of copyright may **assign** the copyright (s. 18) or grant any interest in the copyright by **license** (s. 48). Licenses may also be granted by the Copyright Board (ss. 50– 54).
- Registration of copyright with the Copyright Office is not obligatory, but if registration has taken place the Register of Copyrights gives *prima facie* evidence of the particulars entered therein (s. 60).

Term of copyright

In Bangladesh, copyright terms are as follows:

a. In cases of literary, artistic, musical, dramatic works, the terms is 60 years from the beginning of the calendar years next following the year in which the author dies (Life + 60 years);

b. In cases of photograph, the term is 60 years from the beginning of calendar year next following the year in which the photograph is published (60 years from publication),

c. In cases of cinematographic film, the term is 60 years following the year in which the film is published (60 years from publication),

d. In cases of Govt. works, it is 60 years from publication (60 years from publication,),

e. In cases of local authority, the term is 60 years from first publication (60 years from first publication);

f. In cases of sound recordings, it is 60 years from publication (60 years from publications)

g. In cases of works of international organizations, the term is 60 years from 1st publication (60 years from first publication)

h. In cases of broadcasting, the term is 25 years from the beginning of the calendar year next following the year in which the broadcasting is made (25 years from broadcasting);

i In cases of performance, it is 50 years from the beginning of the year next following the year in which the performance is made (50 years from the first performance is made);

j. In cases of published edition (typographical arrangement), the term is 25 years from the beginning of the calendar year next following the year in which the edition is first published (25 years from the first publication);

k. In cases of joint authorship of a work, the term will be 60 years from the

 death of last surviving author (60 years from death of the last surviving author).

Meaning of copyright

Copyright means *inter alia* the exclusive right

- to reproduce the work
- to issue copies of the work to the public
- to perform or broadcast the work
- to make any translation or adaption of the work (for details see s. 14).

In addition, special moral rights lie with the author (s. 78) as well as a *droit de suite* (s. 23).

Copyright infringement

When copyright is infringed (s. 71), the owner of copyright (as well as the exclusive licensee) is entitled to certain **civil remedies** (injunction, damages, accounts; s. 76). Jurisdiction lies with

the court of District Judge of the place where the person instituting the proceeding resides or carries on business (s. 81).

Infringing copies are deemed to be the property of the owner of the copyright, who accordingly may take proceedings for the recovery of possession thereof or in respect of the conversion thereof (s. 79). Infringing copies may be seized by the police (s. 93) and can be forbidden to be imported (s. 74).

Copyright infringement may also lead to **criminal charges** (ss. 82 to 91) to be tried by no court inferior to that of a Court of Sessions (s. 92).

Some Findings on Academic Copyright issue:

1. Copyright Violation is a very regular affair in Bangladesh and copyright violation in academic activities increasing day by day.
2. A large number of people, especially students are using pirated books to save their money and huge number of people has misconception of fair use.
3. Copyright provisions are not clearly understood by massive segment of the academic and library related personalities. However, the present copyright law of Bangladesh is not formulated to protect the best interests of libraries and archives.
4. Lack of academic resources, such as; books, articles, journals and other internet related resources in educational institution.
5. Teachers and students have inadequate knowledge on “Plagiarism”. On the other hand, lack of skilled people in academic libraries in Bangladesh.
6. Ineffective activities of copyright board and department of copyright in Bangladesh.
7. Law enforcing agencies and law officials have poor knowledge and training on copyright issues.

Trademark Law in Bangladesh Definition

of Trademark

Trademark is a symbol or sign which indicates the source of goods; it distinguishes the goods or services of one entrepreneur from another. Under the Trade Mark Act, 2009, "Trademark" means a registered trade mark or a mark used in relation to goods or service or a mark used or proposed to be used in relation to any service or goods indicating a connection in the course of trade between the goods and the person having the right, either as proprietor or as registered user, to use the mark (Section 2(8)). In Bangladesh, the term „trademark" includes service mark too (section 2(8) (a) (ii)

C191267(Tasnim)

A trademark, trade mark, or trade-mark is a distinctive sign or indicator used by an individual, business organization, or other legal entity to help consumers identify that its products or services with which the trademark appears originate from a unique source, and to help distinguish its products or services from those of other entities.

Trademarks in Bangladesh may be designated by the following symbols:

~ TM (for an unregistered trademark, but for which application has been filed) . ® (for a registered trademark)

A trademark is typically a name, word, phrase, logo, symbol, design, image, or a combination of these elements. There is also a range of non-conventional trademarks comprising marks which do not fall into these standard categories, such as those based on color, smell, or sound.

In Bangladesh, a registered trademark is valid for seven years from the date of application and renewable for successive periods of ten years. The trademark applications, registrations, refusals, etc., are processed according to the Trademark Act 2009 and Trademark Rules 2015.

The owner of a registered trademark may initiate legal proceedings for trademark infringement to prevent unauthorized use of that trademark. However, registration is not required. The owner of a common law trademark may also file suit, but an unregistered mark may be protectable only in the geographical area within which it has been used or in geographical areas into which it may be reasonably expected to expand.

The term trademark is also used informally to refer to any distinguishing attribute by which an individual is readily identified, such as the well-known characteristics of celebrities. When a trademark is used in relation to services rather than products, it may sometimes be called a service mark, as in the United States.

Offences and Penalty of Trademark Law in Bangladesh:

Section 71 firstly discloses the meaning of applying trademarks and trade descriptions, and secondly Section 72 mentions the circumstances when the Trade Marks are falsified or falsely applied. The penalties under the Act are as under:

- Section 73: Penalty for falsifying or falsely applying Trademark: Imprisonment may extend to 2 years, but not less than 6 months, and/or fine which may extend to 2 lac taka, but not less than 50 thousand taka. For a second or subsequent conviction, the imprisonment would range from a minimum of 1 year to 3 years, and/or fine extendable up to 3 lac taka, but not less than 1 lac taka.
- Section 74: Penalty for selling goods to which a false trademark or trade description is applied: Imprisonment for a term up to 2 years, and/or fine. For a second or subsequent conviction, imprisonment for a term up to 3 years, and/or fine.
- Section 76: Penalty for falsely representing a trademark as registered: Imprisonment for a term up to 1 year, but not less than 6 months, and/or fine up to 1 lac, but not less than 50 thousand taka.
- Section 77: Penalty of improperly describing a place of business as connected with the Trademarks office: Imprisonment for a term which may extend to 1 year but not less than

WORKPLACE MONITORING AND ETHICAL ISSUES

For some companies, an important reason to monitor the workplace is to focus on protecting the business from potential legal problems that could arise if an employee were to use a company computer for improper, or even illegal, activities online. Other business owners may have legitimate concerns about employee productivity. The challenge with Internet monitoring and other workplace surveillance tools is to not only protect your interests as an employer and business owner, but in so doing, to retain the trust of your employees by protecting their privacy. Society is still struggling to define the extent to which employers should be able to monitor the work-related activities of employees.

On the other hand, workplace monitoring protects employee privacy. For example, an employee may sue his or her employer for creating an environment conducive to sexual harassment if other employees are viewing pornography online while at work and the organization takes no measures to stop such viewing. Email containing crude jokes and cartoons or messages that discriminate against others based on gender, race, sexual orientation, religion, or national origin can also spawn lawsuits.

Researchers highlight four broad trends in employee monitoring and surveillance technologies:

- **Prediction and flagging tools** that aim to predict characteristics or behaviors of employees or that are designed to identify or deter perceived rule-breaking or fraud.
- **Biometric and health data** of workers collected through tools like wearables, fitness tracking apps, and biometric timekeeping systems as a part of employer provided health care programs, workplace wellness, and digital tracking work shifts tools. Health data may challenge the boundaries of worker privacy, open avenues for discrimination, and raise questions about consent and workers' ability to opt out of tracking.
- **Remote monitoring and time-tracking** used to manage workers and measure performance remotely. More advanced time-tracking can generate

itemized records of on-the-job activities, which can be used to facilitate wage theft or allow employers to trim what counts as paid work time.

- **Gamification and algorithmic management** of work activities through continuous data collection. Technology can take on management functions, such as sending workers automated "nudges" or adjusting performance benchmarks based on a worker's real-time progress, while gamification renders work activities into competitive, game-like dynamics driven by performance metrics. However, these practices can create punitive work environments that place pressures on workers to meet demanding and shifting efficiency benchmarks.

VIDEO MONITORING/SURVEILLANCE

Video surveillance is a common technique employers use to monitor employee activities in the workplace. Many employers use video surveillance to minimize employee misconduct. Video monitoring can also provide evidence of a crime if one were to occur at the worksite. Employers

must consider the state laws for the state in which the surveillance occurs, whether the surveillance area is a public or private area, whether sound is captured in addition to the visual monitoring, and whether the camera is in open view or hidden. Employers should not use video surveillance in areas where employees have an expectation of privacy.

Some suggestions to avoid legal challenges in employee monitoring from *Employer's Guide to Workplace Privacy* (Aspen Publishing, 2004) by Amy L. Greenspan include:

- Use video surveillance only when justified by a legitimate business purpose (e.g., preventing theft or workplace violence, investigating illegal or improper conduct, monitoring employee performance).
- Limit video surveillance to the least unpleasant time, place and method that will serve the business purpose.
- Use only visible cameras or inform employees in writing that hidden cameras may be used.
- Obtain written employee consent to video surveillance for legitimate business purposes.
- Do not use video surveillance in areas where employees have a reasonable expectation of privacy (e.g., bathrooms, locker rooms, dressing rooms, lounges, employees' homes, or other places outside the workplace where employees are not in public view).
- Do not select employees for video surveillance in a manner that might be considered discriminatory under federal or state discrimination laws (e.g., do not videotape only women or only Muslims or only people with disabilities).
- Understand and comply with state or local laws dealing with video surveillance.
- Train supervisors in the legal issues involved in video surveillance.
- Treat information obtained through video surveillance as confidential, and limit access to

video recordings to security personnel or management personnel with a need to know.

- Adopt procedural safeguards to avoid unintended or improper use of work-related video recordings.

IS EMPLOYEE MONITORING ETHICAL? HOW?

It is important to understand why you seek to monitor employees as it sets the ethical foundation when you work with stakeholders to carry out your plan. One ethical question starts to become at which point does employee monitoring impose on their personal privacy? It depends of course on the means of how you apply the employee monitoring. The primary questions to ask here are: who are you monitoring? what are you monitoring? Where are you monitoring? When are you monitoring?

Whether employees should have the right to privacy in the workplace is the ethical challenge that companies face. There are many ethical considerations encouraging employee monitoring, including the need to avoid leaks of sensitive information, stop violation of company policies, recover lost crucial communications and limit legal liability, to name a few.

Provide guidelines through a company manual or handbook best practices when using company equipment, especially when conducting personal business at work. Some steps for ethical compliance:

Set written policies. Enact a code of ethics that ensures both employer and employee understand how to conduct themselves in the workplace and know exactly what is expected of each other.

- ***Inform employees.*** Make full disclosure about the stealth monitoring systems you are

implementing so that workers are not monitored without their knowledge.

- ***Uphold ethical standards.*** Ensure the monitoring exercise remains moral. Recognize that an employee does not give up all of his or her privacy when they are at work.
- ***Encourage participation.*** Involving employees in the decision to create surveillance will
allow for common ground in developing principles that are acceptable to both sides.

When it comes to workplace monitoring, it is usually the information technology personnel that are tasked with being the watchdogs and the gatekeepers of the organization. Whatever techniques are employed in these operations should be above board, ethical and within the law.

IS EMPLOYEE MONITORING LEGAL?

Employee monitoring is legal, however there are some stipulations that must be followed in some states. In some countries, employers must inform employees that they are being monitored electronically. Additionally there is federal legislation in effect which may impact your ability to monitor to the scale you want. However, like any regulation, there are exceptions and for businesses they allow to monitor employees as long as there is a "legitimate business purpose," which means a dragnet style of employee monitoring would violate the law if there was no sound cause for it.

WHAT IS ERGONOMICS?

Ergonomics comes from the Greek words `ergon' meaning work and 'nomos' meaning laws.

Ergonomics is the equipment and tools designed for workers to increase productivity and efficiency while reducing discomfort and fatigue. Ergonomics can make a workplace safer and reduce costs.

An ergonomic workspace can include adjustable workstations and computers, ergonomic chairs and a footrest under the desk. It allows workers to remain comfortable with temperature control, air conditioning, adjustable lighting and easy to access storage solutions. Everything is at a comfortable distance to reduce stress and strain and minimise the need for workers to twist, bend and reach.

C191267(Tasnim)

WHY DOES ERGONOMICS MATTER?

Organisations should take ergonomics seriously. Not only are staff at risk of experiencing an injury, but also the cost of lost productivity every year is significant.

Health of Workers

An employer is responsible for the physical and mental well-being of employees while they are at work. When workplaces are poorly designed, staff are at risk, particularly of musculoskeletal injuries. Making simple small changes can make a significant reduction in risk to workers.

Productivity Improvements with Ergonomic Workplaces

An ergonomically designed workplace takes into account the tasks staff need to do on a regular basis. If a staff member needs to walk to a storage area and reach for files on a daily basis, then it's likely no one has considered the wasted time in leaving her workstation every day not to mention the risk factors involved in reaching well above her head for heavy items.

Ergonomics improve staff output and increase profits. Staff can't work at their ultimate speed and efficiency if they are uncomfortable or fatigued and productivity ceases if they sustain an injury.

Ergonomics can Improve Staff Morale

A well-designed, aesthetically pleasing work environment can do wonders for staff satisfaction levels and morale. Staff members that feel appreciated are more likely to stay with their employer longer than a worker that doesn't. Even a slight reduction in turnover can have a significant impact on an organisation's costs.

Staff appreciate when their employer considers their individual needs. Examples of buying custom equipment can be as simple as an extra high sit-stand desk for a tall worker, a heavy-duty chair for heavier employees over 145 kg, or a vertical mouse for a worker with a sore wrist.

C191267(Tasnim)

The Cost of Workplace Injuries

Without even considering the human toll an injury can have on a worker, their friends and family, injuries are expensive. According to Safe Work Australia, the cost of workplace injury and disease in 2013 was $61.8 billion including direct costs like workers' compensation and indirect costs such as lost productivity. The most common injuries related to traumatic joint, ligament and muscle, and tendon injuries which accounted for almost 44% of all serious injuries in the workplace. An ergonomically-designed workplace could have prevented a large number of these injuries.

When an employee is injured, and off work, the organisation needs to find a replacement temporary staff member, train them in the role and wait weeks for them to improve their

productivity while they learn on the job. The injured worker makes a compensation claim which increases premiums. If the injury is serious, they may need to be redeployed to another role which incurs training costs. This US government calculator gives you an estimate of the impact an occupational injury or illness has on a company's profitability.

DIGITAL DIVIDE

Digital divide is a term that refers to the gap between demographics and regions that have access to modern information and communications technology, and those that don't or have restricted access. This technology can include the telephone, television, personal computers and the Internet.

The digital divide typically exists between those in cities and those in rural areas; between the educated and the uneducated; between socioeconomic groups; and, globally, between the more and less industrially developed nations. Even among populations with some access to technology, the digital divide can be evident in the form of lower-performance computers, lower-speed wireless connections, lower-priced connections such as dial-up, and limited access to subscription-based content.

Inequality in access to the Internet and ICT is known as the digital divide and affects 52 % of women and 42 % of men worldwide. This gap becomes even wider when we talk about regions: according to data taken from the Internet portal World Stats as of May 2020, in Africa only 39.3 % of its inhabitants had Internet access, compared to 87.2 % of Europeans and 94.6 % of Americans.

The data shows the technological gap that separates some countries from others, despite the fact that 3G and 4G networks, while awaiting the massive

Widening levels of education seem to magnify the digital divide; households with higher levels of education are increasingly more likely to use computers and the Internet. It has been observed

expansion of 5G, are already reaching almost every corner of the planet. Here, it is important to distinguish between access to the Internet and digital literacy,

that is, the learning process that enables a person to acquire the skills to understand and benefit from the educational, economic and social potential of the new technologies.

FACTORS ATTRIBUTING TO THE DIGITAL DIVIDE

According to a study conducted by the National Telecommunications and Information Administration (NTIA), entitled Falling Through the Net: Defining the Digital Divide, the gap is widening along already strained economic and racial lines.

Education

that those with college degrees or higher are 10 times more likely to have internet access at work as than those with only a high school education.

Income

The levels of household income also play a significant role in the widening gap. Due to lower income levels, poor neighborhoods lack the infrastructure available in affluent areas. Telecommunication facilities are more readily available for wealthier communities and are more attractive for developing companies to establish themselves. As a result, poverty in less fortunate neighborhoods make it less appealing for investments by outside companies, further aggravating the divide.

Race

At the same time, the digital divide continues to widen along very specific racial lines. Hispanic households are nearly 2.5 times less likely to use the internet than White households. The NTIA study also demonstrated the racial disparities in Internet access exist irrespective of income. In the Hispanic community, it was observed that computers were a luxury, not a need; computer activities isolated individuals and took away valuable time from family activities. In the African-American community, it was observed that African-Americans, historically, have had negative encounters with technological innovations. Asian-Americans, on the other hand, generally emphasize education, resulting in a larger number embracing rising technological advances.

TYPES OF DIGITAL DIVIDE

The digital divide was initially attributed to underdevelopment and was perceived as something temporary that would disappear with the popularisation of technology. Instead, **the divide persists today despite the mass marketing of electronic devices with Internet access.** The causes can range from the high price of the above-mentioned devices to the lack of knowledge about their use or the lack of infrastructure for their access. In this regard, we review the types of digital divide:

- **Access divide.** It refers to the possibilities that people have to access this resource. This is where socio-economic differences between people and

between countries come into play, since digitisation requires very costly investments and infrastructure for less developed regions and for rural areas.

- **Use divide. It** refers to the lack of digital skills, which impedes the handling of technology. In this regard, and to give an example, the ITU points out that there are 40 countries in which more than half of their inhabitants do not know how to attach a file to an email.
- **Quality of use gap.** Sometimes they have the digital skills to find their way around the Internet, but not the knowledge to make good use of and get the most out of it. For example, with regard to access to quality information.

CONSEQUENCES OF THE DIGITAL DIVIDE

Technological discrimination is a form of poverty and social exclusion, depriving some citizens of essential resources for development and wealth generation. We have seen this a lot during the COVID-19 pandemic, as many students and workers found it difficult to work from home and follow classes online. We review the main effects of the digital divide below:

- Lack of communication and isolation

People in remote areas who do not have access to the Internet are disconnected. Something similar happens to urban residents who are disconnected which causes social isolation.

- Barrier to studies and knowledge

The coronavirus crisis has shown the effects of the digital divide in education: teachers and students out of the loop because they lack sufficient technology and digital skills. It also increases lack of knowledge by limiting access to knowledge.

Accentuates social differences

Digital illiteracy reduces the chances of finding a job and accessing quality employment, which has a negative impact on the workers' economy.

- Gender di scrim i n ati o n

As we saw at the beginning, the digital divide negatively affects women more than men, which violates the principles of gender equality.

STRATEGIES ON BRIDGING THE DIGITAL DIVIDE

The digital divide, as a whole, remains an enormous and complicated issue - heavily interwoven with the issues of race, education, and poverty. The obstacle, however, is by no means insurmountable if broken down into specific tasks that

must be accomplished. Aside from the obvious financial barriers, the following would help narrow the gap:

Universal Access

As the use of computers and the Internet increases, so does the necessity for access. In the public sector, policy makers and community members must recognize the importance of such resources and take measures to ensure access for all. While increased competition among PC manufacturers and Internet Service Providers has substantially reduced the costs associated with owning a computer and maintaining a home connection, for many households the costs remain prohibitive. Like basic phone service, the government should subsidize Internet access for low-income households. At the same time, the private sector must commit to providing equal service and networks to rural and underserved communities so that all individuals can participate.

More Community Access Centers, Continued Support of Those Already Existing

Community access centers (CACs) are a critical resource for those without access to computers and the Internet at school or work. Community access centers, therefore, are clearly worthwhile investments. So, government should establish more community access centers, Also should continue support of those already existing.

Additional, Well-Trained Technical Staff

Computers and other technologies alone are not enough. Communities and schools must train and preserve additional, and more qualified staff, alongside new technologies to promote the best application of resources. In addition to understanding the new technologies, the staff must be able to teach others.

Change of Public Attitude Regarding Technology

At the same time, much of society needs to change its attitude concerning technology. Rather than perceiving computers and the Internet as a superfluous luxury, the public should view them as crucial necessities. The public must come to realize the incredible power of new technologies and embrace them as tools for their future and the future of their children.

Lecture 8 CODES OF ETHICS

FOR KEY TECHNICAL SOCIETIES

These codes are guides to personal conduct. They show great similarities, but were created by different organizations. A violation of the Code of Ethics of any of the societies (C1 to C8) may result in admonition, suspension, or expulsion from the society, depending on the society's constitution. By contrast, Canadian law enforces penalties under the Codes of Ethics of the provincial and territorial engineering and geoscience Associations (summarized in Appendix B).

Technical Societies

- **APPENDIX C-1: ACM / IEEE**
  Software Engineering – Code of Ethics and Professional Practice
- **APPENDIX C-2: ASCE**
  American Society of Civil Engineers – Code of Ethics
- **APPENDIX C-3: ASME**
  American Society of Mechanical Engineers – Code of Ethics
- **APPENDIX C-4: IEEE**
  Institute of Electrical and Electronics Engineers – Code of Ethics
- **APPENDIX C-5: NSPE**
  National Society of Professional Engineers – Code of

Ethics Societies of Corporations

- **APPENDIX C-6: FIDIC**
  International Federation of Consulting Engineers – Code of Ethics
- **APPENDIX C-7: CERES**
  Coalition for Environmentally Responsible Economies –

Principles International Mobility

- **APPENDIX C-8: NAFTA**

NAFTA – Conduct and Ethics in Engineering Practice

APPENDIX C-1

ACM / IEEE

Software Engineering

Code of Ethics and Professional Practice

The ACM / IEEE Code of Ethics is a comprehensive guide to conduct for software engineers
and was developed by the

Association for Computing Machinery, Inc.
www.acm.org
and the
Institute for Electrical and Electronics Engineers, Inc.
www.ieee.org

The ACM / IEEE Code of Ethics is of interest to other engineers and geoscientists, because computers are essential to every aspect of professional work. The short version of the code summarizes the key ideas; the full version includes examples of how the code should influence the work of software engineers. Both versions follow:

Software Engineering Code of Ethics and Professional Practice (Version 5.2)
as recommended by the ACM/IEEE-CS
Joint Task Force on Software Engineering Ethics and Professional Practices
and jointly approved by the ACM and the IEEE-CS as the
standard for teaching and practising software engineering.

ACM / IEEE Code of Ethics – Short Version

PREAMBLE

The short version of the code summarizes aspirations at a high level of the abstraction; the clauses that are included in the full version give examples and details of how these aspirations change the way we act as software engineering professionals. Without the aspirations, the details can become legalistic and tedious; without the details, the aspirations can become high sounding but empty; together, the aspirations and the details form a cohesive code.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected

profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1. **PUBLIC –** Software engineers shall act consistently with the public interest.

2. **CLIENT AND EMPLOYER** – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.

3. **PRODUCT** – Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

4. **JUDGMENT** – Software engineers shall maintain integrity and independence in their professional judgment.

5. **MANAGEMENT** – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

6. **PROFESSION** – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

7. **COLLEAGUES** – Software engineers shall be fair to and supportive of their colleagues.

8. **SELF** – Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

by the Association for Computing Machinery, Inc. and the Institute for Electrical and Electronics Engineers, Inc.]

ACM / IEEE Code of Ethics – Full Version

PREAMBLE

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those

who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because

of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making

software engineering a beneficial and respected profession. In accordance with that

commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policy makers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer's humanity, in special care owed to people affected by the work of software engineers, and the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission. The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should

influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings

with due respect; to consider how the public, if reasonably well informed, would view their decisions; to analyze how the least empowered will be affected by their decisions; and to consider

whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for the health, safety and welfare of the public is primary; that is, the “Public Interest” is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are

ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

PRINCIPLES

Principle 1: PUBLIC

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.01. Accept full responsibility for their own work.

1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.

1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.

1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

2.03. Use the property of a client or employer only in ways properly authorized, and with the clients or employers knowledge and consent.

1.07. Consider issues of physical disabilities, allocation of resources, economic

disadvantage and other factors that can diminish access to the benefits of software.

1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

Principle 2: CLIENT AND EMPLOYER

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

2.01. Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02. Not knowingly use software that is obtained or retained either illegally or unethically.

2.04. Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.

2.05. Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06. Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.

2.08. Accept no outside work detrimental to the work they perform for their primary employer.

2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

Principle 3: PRODUCT

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01. Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.

3.02. Ensure proper and achievable goals and objectives for any project on which they work or propose.

3.03. Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

3.04. Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.

3.05. Ensure an appropriate method is used for any project on which they work or propose to work.

3.06. Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.

3.07. Strive to fully understand the specifications for software on which they work.

3.08. Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.

3.09. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.

3.10. Ensure adequate testing, debugging, and review of software and related documents on which they work.

3.11. Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software.

3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.

3.14. Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

3.15 Treat all forms of software maintenance with the same professionalism as new development.

Principle 4: JUDGMENT

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

4.01. Temper all technical judgments by the need to support and maintain human values.

4.02. Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.

4.03. Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.

4.04. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06. Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

Principle 5: MANAGEMENT

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance. In particular, those managing or leading software engineers shall, as appropriate:

5.01. Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.

5.02. Ensure that software engineers are informed of standards before being held to them.

5.03. Ensure that software engineers know the employer's policies and procedures for

protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04. Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06. Attract potential software engineers only by full and accurate description of the conditions of employment.

5.07. Offer fair and just remuneration.

5.08. Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09. Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.

5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11. Not ask a software engineer to do anything inconsistent with

this Code. 5.12. Not punish anyone for expressing ethical concerns

about a project.

Principle 6: PROFESSION

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01. Help develop an organizational environment favorable to acting ethically.

6.02. Promote public knowledge of software engineering.

6.03. Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04. Support, as members of a profession, other software engineers striving to follow this Code.

6.05. Not promote their own interest at the expense of the profession, client or employer.

6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07. Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08. Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09. Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10. Avoid associations with businesses and organizations which are in conflict with this code.

6.11. Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12. Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13. Report significant violations of this Code to appropriate authorities when it is clear

that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

Principle 7: COLLEAGUES

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01. Encourage colleagues to adhere to this Code.

7.02. Assist colleagues in professional development.

7.03. Credit fully the work of others and refrain from taking undue credit.

7.04. Review the work of others in an objective, candid, and properly-

documented way. 7.05. Give a fair hearing to the opinions, concerns, or

complaints of a colleague.

7.06. Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07. Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08. In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

Principle 8: SELF

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03. Improve their ability to produce accurate, informative, and well-written documentation.

8.04. Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05. Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06. Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07. Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08. Not influence others to undertake any action that involves a breach of this Code.

8.09. Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

Previous Solve:

Autumn 2021

Group-A

1.

a) Assume that the family of one of the victims of the Therac-25 has filed three lawsuits. They are suing a hospital that used the machine, the company that made the machine (AECL), and the programmer who wrote the Therac-25 software. As a programmer what you will do?

OR

Write the consequences and remedies of three recent cases like Therac-25 case.

5

a) What are the four factors to consider in deciding whether a use of copyrighted material is a fair use? Describe any one with example.

b) Debate whether software should be copyrightable or should be freely 5 C01 E available for copying in context of Bangladesh.

OR

A website hosts written works posted by authors. Some people post copyrighted work by other authors without permission. When an author asks the site to remove such material, the site complies and adds the work to its filter database to prevent reposting without permission. An author sues the site claiming the site infringes her copyright by storing her work. Argue the author's case. Argue the site's defense. Evaluate the arguments and decide the case.

Group-B

3.

a) What did the word "hacker" mean in the early days of computing? Is it legal to release a computer virus that puts a funny message on people's screens but does not damage files?

b) What is Ethical hacking? What do you mean by it? Should we learn it? Justify your answer. 5

OR

The terms of use of the website for a rail ticket seller prohibit automated purchases. Should a person who used a software program to purchase a large number of tickets be prosecuted for exceeding authorized access to the site? Why or why not?

4.

4. a) What do you think about staff monitoring system? Is it legal? Justify your answer. 5

b) Consider an automated system that large companies can use to process job applications. For jobs such as truck drivers, cleaning staff, and cafeteria workers, the system selects people to hire without interviews or other involvement of human staffers. Describe advantages and disadvantages of such a system.

5. a) What is one important policy decision a company should consider when designing a system to target ads based on email content? 5

b) Some people fear that development of intelligent robots could have devastating consequences for the human race. Is it ethical to do research aimed at improving artificial intelligence? 5

OR

Suppose you are a programmer, and you think there is a serious flaw in software your company is developing. Who should you talk to about it first?

Spring 2019

[GROUP A: Answer any 2 (two) of the following questions]

1 a) What is Software Reliability? How should accountability be maintained in order to preserve 3

software reliability? b) What are the Software Reliability Improvement Techniques?

c) The Therac-25 radiation machine involved errors in software overall design and management or 5 operations. Describe each types of error with possible remedy.

2 a) What is intellectual property? Why do countries protect intellectual property?

4

b) What is patent? What kind of protection do patent offer? c) How to protect your software with intellectual property protection?

3 3

3 a) Open-source versus proprietary software: Is one more reliable and secure than the other? b) Compare and contrast the following: Software Responsibility vs. Software Liability

Software Liability vs. Software Accountability

4 6

2

[GROUP B: Answer any 3 (three) of the following questions]

4 a) Define identity theft. What are the types of identity theft?

b) Write short notes on: Data Diddling and Logic Bomb. c) How can you discriminate between an email that is a phishing attempt and an email from legitimate business?

5 a) Write the impact of employee monitoring in a workplace. b) What are the health related issues for a computer professional?

c) What are employer obligations with regard to healthy computing environment?

3

3

4

6 a) What is professional ethics? Write the importance of CSE graduates to know and follow the 4 professional ethics.

b) List and discuss guidelines for software professionals for producing good systems. What was the 4

main reason for the failure of the handwriting-recognition system developed by the team of

Microsoft programmers? c) Describe some guidelines for computer professionals to make ethical decision.

7 a) Do you think hiring formal hacker to ensure security is a good idea or a bad idea?

b) What do you know about hacking by Government? c) How can you protect your organization from cyber-criminal?

C191267(Tasnim)

Autumn-2018

1 a) Discuss the importance of software reliability. Why insufficient testing was a factor in a program error 4 or system failure?

b) Assume you are a professional working in your chosen field. Describe specific things you can do to reduce the software error and system failure.

3

e) Suppose you are responsible for design and development of a computer system to control an 3 amusement park ride. Sensors in the seats will determine which seats are occupied, so the software can consider weight and balance. The system will control the speed and duration of the ride. The amusement park wants a system where, once the ride starts. a person is not needed to operate it. List some important things that you can or should do to ensure the safety of the system. Consider all aspects of development, technical issues, operating instructions, and so on.

3

4

2 a) What are the factors to consider in deciding whether a use of copyrighted material is a fair use? b) Give examples in which plagiarism is also copyright violation and in which it is not. c) Some people argue that digital rights management violates the public's right to fair uses.

i) Should a person or company that creates intellectual property have an ethical and/or legal right to

offer it for sale in a form protected by their choice of digital rights management technology? Give

reasons.

ii) Should people have an ethical and/or legal right to develop. sell, buy and use devices and software to remove digital rights management restrictions for fair uses? Give reasons. 3 a) What do you think the impact would be on creative industries such as music. movies and fiction 3

novels. if copyright laws did not protect their intellectual property?

b) How accountability should be maintained in order to preserve software reliability?

c) What is fair use? How is it determined whether a particular use of a copyrighted use or not?

3

4

[GROUP B: Answer any 3 (three) of the following questions] 4 a) Define Identity theft. What are the types of Identity theft?

4

b) What are the potential solutions for Hacking & Cracking? c) How can you discriminate between an email that is a phishing attempt and an email from legitimate 3 business?

3

3

5 a) Write the impact of employee monitoring in a workplace. b) What are the health related issues for a computer professional?

c) Write the ideal way to monitor your employees.

6

3 3

a) What is professional ethics? Write the importance of CSE graduates to know and follow the 4

professional ethics.

b) List and discuss guidelines for software professionals for producing good systems. What was the main 4 reason for the failure of the handwriting-recognition system developed by the team of Microsoft programmers?

c) Describe some guidelines for computer professionals to make ethical decision. 7a) Do you think hiring formal hacker to ensure security is a good idea or a bad idea!

b) What do you know about hacking by Government? c) Write short note on code of professional ethics based on Islamic teaching

Spring -2018

Group-A

La) How does computer technology effect privacy? b) Write the religious views on pornography.

2233

c) Can censorship be justified in the context of free speech? d) How is right to free expression protected? Where do we draw the line?

2.a) Define cyber crime. Why is cyber crime increasing?

3

b) What is identity theft? Write types of iden y theft.

c) Define cyber warfare. What are the motivations for cyber warfare.

3 4

3.a) What are copyright and patent? Should software owners be given copyright or patent and 4 why? b) How does new technology threaten the protection of copyrighted materials?

3

3

c) Suppose the movie industry asks a court to order a Web site to remove links to other sites that have pirated DivX movie files. Give arguments for each side. What do you think the decision should be? Why?

Group-B

4.a) What is privacy? Distinguish between privacy and security. b) What is Hacktivism? What are the arguments to support or oppose it?

c) What is biometrics? Suppose thumbprint readers are a standard feature of personal computers and an ISP requires a thumbprin. match to log in. Would requiring a password in addition to thumbprint be redundant and pointless, or is there a good security reason to require both? Explain.

3

d) What is online scams? Give example of one scams.

5.a) How professional ethics differs from general ethics?

b) Describe ACM code of ethics and relate Islamic ethics to ACM code c) Suppose you are a programmer, and you think there is a serious flaw in software your company is developing. Who should you talk to about it first?

6.a) What are the ethical issues that have arisen as a result of using computers in the workplace? b) What are the effects of monitoring workplace computer? c) What are employer obligations with regard to healthy computing environment?

2 6

2

C191267(Tasnim)

4

3

7.a) What is the digital divide? What are the short term and long term effect of digital divide? How it can be resolved?

include? c) Your company has about 30 licenses for a computer program, but you discover that it has 2 been copied onto 50 computers. What will you do in such a situation?