**Module Code UFCHJ-15-M**

**Module Title: Information Security**

**STUDENT ID: 21071999**

QUESTION 1

(a)

Before we differentiate between privacy and security, we need to understand both terms and the concept guiding each and everyone.

**Privacy**

The word privacy does not have a general definition. It depends on the aspect of human life and what activities are attached.

According to (John bonga , 2021) Privacy refers to the control that you have over your personal information and how that information is used .Personal information is any information that can be used to determine ones identity.

And **Security**refers to how the personal information are protected. Security has to deal with the confidentiality, integrity and availability of that personal data and information.

Let us take this example; when we go the General Practitioners (GP) for medical registration, we will be asked some personal data like your name, mobile number, your address, your previous health related records, Whether or not we choose to share certain details with our GP system is a matter of personal privacy, this data are processed by the GP system to process into a meaningful information which gives the identity of the user, our consent will be asked if this information should be shared with the NHS system , giving our consent to the information sharing is also our privacy. How well the NHS protects the information that it requires us to provide so we can use the platform is a matter of security.  If [a data breach](https://www.howtogeek.com/devops/how-data-breaches-and-leaks-can-affect-your-employees/) occurs and cyber attackers get a hold of your information, both your security and privacy are compromised.

**Differences between personal privacy and security.**

* Personal privacy sometimes has to deal with confidentiality

**while;** Security has to do with confidentiality, integrity and availability of personal information.

* Privacy refers to the ability to protect personally identifiable information

**while;** The word “Security” refers to the ability to prevent unauthorized access into the information.

* Privacy procedures are related to personal data such as names, addresses, security numbers, login details, and financial information

**while;** security procedures are related to various information assets generated by enterprises.

* When it comes to processing personal data, privacy comes first

**while;** security relates to preventing unauthorized access to information assets. Personal data includes names, personal addresses, bank account information, credit card numbers, and other information about an individual.

1B

**Ways We can protect Software Infringement**

Software are lines of codes, programs or instructions given to the computer to perform a given task. (David, 2011).These programs are said to be intangible (Intellectual property) created by mind to give functions to some specific tasks.

According to Justine 2021, intellectual property is an asset the company owns that gives it the edge and a competitive advantage in the marketplace. So software infringement are the reproduction, reuse copying of someone’s original work without their consent in an unauthorized manner. Infringing on our software protects will destroy the uniqueness and originality of our software and we need to protect them in some ways which are analysed below:

**COPYRIGHT**

Copyright is a legal right, which protects the creator of a work most especially the author of a book, publications, novels or stories. Copyright gives the owner control over their work and how it is used, this law is a balancing act between intellectual promotion and property rights.

**PATENTS**

 This simply means having a legal right to one’s software which then restrict others from manufacturing or marketing the software. This patent usually last for twenty years(20) years.

**TRADEMARK**

A trademark refers to a recognizable sign, design or expression which identifies products or services of a particular source from those of others. This refers to names, phrases, symbols, even sounds used with services or products. That is essential for any brand with a level of quality on which companies build a reputation. This last for ten years(10) years.

1C

The fear of adversary is what led to identification and authentication.

**IDENTIFICATION**

Identification is the disclosure of one’s personality. This means who we claim to be.  A username, school id , smart card, or anything else that may uniquely or person can be used for identification. Security systems use this method of identification to determine whether an individual has permission to access an object. Identification is just a declaration of identity. The crucial factor to realise is that when working with identification, an unsubstantiated claim of identify is not reliable information on its own. Unfortunately some of the supposedly unique methods of identification, such as the fingerprint, can be duplicated or spoofed in many cases. In this case of security challenge, we can verify and validate identity. Who we claim to be can in many cases, be an item of information that is subject to change. Identification is not a genuine security measure because we can have a false identity, for instance if I misplaced my credit card and found by a bad guy, this bad guy uses my card to purchase items from the mall, the system recognizes the bad guy as myself because he claims to be me.

**AUTHENTICATION**

Authentication puts processes in place for a user to prove that they are still that person they claim to be. The process of authentication in the context of computer security means assurance and confirmation of a user's identity. Authentication employs different combinations of data, passcodes, QR codes, passwords, pass cards, digital signatures, fingerprint, retinal, face and voice scans to verify a users' identity before they can access a network. Proper authentication is often provided through a solution like a secure web gateway and deployment of multiple, cohesive security protections and solutions, like next-generation firewall and endpoint protection.

**DIFFERENCES BETWEEN IDENTITY AND AUTHENTICATION**

Identification and authentication are commonly used as a two-step process, but they are distinct activities.

* **Identification** is the first step in accessing a gated system

**while;** authentication is proving the identity is right and correct.

* A username, process ID, smart card, or anything else that may uniquely [identify a subject](https://imageware.io/imageware-identify/) or person can be used for identification

**while;** Authentication takes place when subjects present suitable credentials to prove themselves.

* Identification is the claiming of an identity. This only needs to occur once per authentication or access process. Any one of the three common authentication factors can be employed for identification. Once identification has been performed, the authentication process must take place. Authentication is the act of verifying or proving the claimed identity. The issue is both checking that such identity actually exists within the known accounts of the secured environment and also ensuring that the human claiming the identity is the correct, valid.

2a

Physical and environmental control is a security measure put in place to protect the who have access to the organization data why they must have access, when they have access.

1. Electronic monitoring
2. Guards and dogs
3. ID card and badges
4. Locks and keys
5. Alarms and alarm system.

**Electronic monitoring:** are used for incident capturing and future refence. Some systems collect constant video feeds, while others rotate input from a number of cameras, sampling each in turn. This will help the organisation track a security breach or invasion of the companies of privacy.

**Guards and dogs:** these are another security measure put in place to secure our physical environment. Guards are physical security control(mostly uniform human)which have standard operating procedures that help them to act decisively in unfamiliar situations. Also for an organisation protecting valuable resources, or with specific risks, **dogs** can form an important part of physical security, providing they are well trained into the plan and managed properly. There’s no denying a dog’s ability to react quickly which can prove particularly useful if they are working dogs in the security field, especially if you chose the right kind of dog. Whilst all dogs are known to have quick reactions of barking or snooping to see who’s around, there are certain breeds that are infamous for their protective qualities.

**ID CARDS AND BADGES:**

ID cards can have a magnetic strip or radio chip that can be read by automated control devices to allow an organisation to restrict access to sensitive areas. And badges can have pictures or serial numbers declaring the authorization of a staff in the organization. A key weakness of cards and badges is the human factor.

**ALARMS AND ALARM SYSTEM:**

[Alarm systems](https://en.wikipedia.org/wiki/Alarm_systems) can be installed to alert security personnel or the guards when unauthorized access is attempted. Alarm systems work in line with physical barriers, mechanical systems, and security guards, serving to trigger a response when these other forms of security have been breached. They consist of sensors including [perimeter sensors](https://en.wikipedia.org/wiki/Perimeter_intrusion_detection_system), [motion sensors](https://en.wikipedia.org/wiki/Motion_sensors), contact sensors, and [glass break detectors](https://en.wikipedia.org/wiki/Glass_break_detector)

Physical attacks could be breaking into a secure data centre, sneaking into restricted areas of a building, or using terminals they have no business accessing. Attackers could steal or damage important IT assets such as servers or storage media, gain access to important terminals for mission critical applications, steal information via USB, or upload malware onto your systems.

Rigorous controls at the outermost perimeter should be able to keep out external threats, while internal measures around access should be able to reduce the likelihood of internal attackers (or at least flag unusual behaviour) physical security is equally important as cybersecurity, and it keeps you protected from theft, vandalism, burglary, fire, flood, and other natural disasters.

2b

ways in which a firewall keeps the network safe are;

* The firewall physically cut off all access to the local network except via firewall.

• Only authorized traffic which is delineated by the local security policy will be allowed to proceed.

• The firewall itself is resistant to penetration inclusive in a solid trustworthy system with a protected operating system.

2c

Distributed Denial of Service or DDoS attacks are cyberattacking no network administrator wants to deal with. The goal of an attack like this is to render a network or service inoperable. Luckily, network redundancy can help to mitigate the impact of DDoS attacks, because it improves [network security](https://www.auvik.com/features/network-privacy-and-security/). You can prevent these attacks by implementing redundant networks. These networks will ensure that you can use [backup systems](https://bleuwire.com/why-businesses-choose-cloud-based-backup/) in case of an attack. You can use diverse traffic routing technology for bypassing DDoS attacks without worrying about bandwidth. Also, you can increase network latency by using traffic routing options. These services will help you in increasing your network uptime. They will help you in creating an incident response plan which will help you in protecting your business from various cyberattacks.

3a

Computer Security: This refers to the protection and defence against vulnerable attacks and unauthorized use of the computer system which includes network programs and data. This component include data, hardware, software and firmware.

Computer security has some characteristics:

Confidentiality: making sure that information is available only to the intended audience. Confidentiality includes privacy of information that may be personal or sensitive. Confidentiality can be achieved by physical isolation, cryptography, background checks on people.

Integrity: Making sure people cannot change information they should not. There by causing inaccurate of data because of unintended changes. Data integrity can be achieved by redundancy, backups, checksums and digital signatures.

**Availability**: Making sure people cannot stop the computer from doing its job when necessary. This can be achieved by hardening, redundancy, reference check on people.

Control: this has to do with the controls that limit access to the computer, the controls come from physical or technical and procedural choices that limit access the computer components. This can be achieved by access control list and physical security.

**Audit** : this has to do with monitoring of log files and typically have regular audits to ensure the smooth working of the systems, to easily identify any threat or vulnerability.. this can be achieved by log files and human auditors and expert systems.

A scenario example, Tom is an audit manager in his company, he discovered that the computer (PC) in the organization is faulty and decide to give his brother after deleting all possible information’s, Tom’s brother took the PC to a repair shop and bad guys were able to gain access to the company’s information thereby causing exploit and using the computer for crime like making false identity documents.

**INFORMATION SECURITY**: This refers to protecting information and information systems

from unauthorized access, use, disclosure, disruption, modification, or destruction,”

according to US law. it means we want to protect our data (wherever it is) and systems assets from those who would seek to misuse it. this is simply the security of information. The characteristics of information security are

Information security strategies target three key metrics: the integrity, confidentiality, and availability of information systems. Protecting the integrity of information entails guarding against unauthorized alteration or destruction of data. Preserving confidentiality of information involves restricting access to private personal or proprietary information. Finally, maintaining the availability of information systems requires ensuring that information can be reliably accessed by authorized personnel. Each of these processes is covered in-depth through information security classes, allowing professionals to develop the ability to craft comprehensive cyber security strategies.

A scenario on information security: Tony, a data analyst for a major casino, is working after normal business hours to finish an important project. He realizes that he is missing data that had been sent to his co-worker Robert. Tony had inadvertently observed Robert typing his password several days ago and decides to log into Robert’s computer and resend the data to himself. Upon doing so, Tony sees an open email regarding gambling bets Robert placed over the last several days with a local sports book. All employees of the casino are forbidden to engage in gambling activities to avoid any hint of conflict of interest. Tony knows he should report this but would have to admit to violating the company’s information technology regulations by logging into Robert’s computer. If he warns Robert to stop his betting, he would also have to reveal the source of his information. Robert made his information vulnerable to Tony.

**INFORMATION ASSURANCE**: this is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. This includes the protection of the confidentiality, integrity, availabilities, non-repudiation, authenticity of users data. It uses physical, technical and administrative control to accomplish these tasks

A scenario

3b.

The relationship between information security and information assurance disciplines

Both information security and information deals more holistic approach of securing data and not just focusing on the technical aspect.

• Information Assurance is a discipline of wider scope which includes Information Security

Information Security refers to the technical and practical aspects of information protection – (SANS, n.d.) – Citing Wikipedia, ‘Info Sec is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take electronic, print, or other forms and Information Assurance is the management of Information Security.

3c.

I will sincerely advice my client to go for Information Assurance because it tries to determine what data is actually information and what value that information has which enable us to take proper risk assessment. An information assurance manager will not then waste resources protecting data that is not information, especially if it will detract from the protection of more valuable information. s. Examples can include security audits, network architecture, compliance audits, database management, and development, implementation, and enforcement of organizational information management policies.

4a.

**Injection vulnerability**: This is when a hacker supplies input into the software with the intention of getting the untrusted input processed by the interpreter of the software to data theft, data destruction and compromise the system.

Example of injection vulnerability, SQL Injection - Is a particularly widespread and dangerous form of injection. To exploit a SQL injection flaw, an attacker needs to find a parameter that the web application passes through to a database interaction. An attacker can then embed malicious SQL commands into the content of the parameter, to trick the web application to forward a malicious query to the database. SQL queries could be modified by adding additional ‘constraints’ to a where clause (e.g., OR 1=1) to gain access to or modify unauthorized data

**Security misconfigurations** are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. The application server’s configuration allows detailed error message.

Example of security misconfiguration :stack traces, to be returned to users. This potentially exposes sensitive information or underlying flaws such as component versions that are known to be vulnerable.

**Buffer overflow:** Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information.

Example of buffer overflow :Adobe Flash Player: In 2016, a buffer overflow vulnerability was found in Adobe Flash Player for Windows, macOS, Linux and Chrome OS. The vulnerability was due to an error in Adobe Flash Player while parsing a specially crafted SWF (Shockwave Flash) file. Malicious entities could exploit these vulnerabilities to bypass security restrictions, execute arbitrary code, and obtain sensitive information by enticing users to open the SWF files or Office documents with embedded malicious Flash Player content distributed via email. Adobe responded by releasing security updates that addressed and resolved the issues. (Amakiri,2020).

4b

Malware is any type of software created to harm or exploit another piece of software or hardware. Short for “malicious software,” malware is a collective term used to describe viruses, ransomware, spyware, Trojans, and any other type of code or software built with malicious intent. The type of malware I chose is RANSOMEWARE.

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom.

Attacks often start with a malicious phishing email intended to trick the recipient into disclosing login credentials then Using stolen credentials or other means, attackers hit your website and applications to access your business data. Finally With access to your data, the attackers encrypt your data so that you can’t access it. They then demand a ransom payment to unencrypt it and avoid exposing that data.

4c

Direct attack means that the adversary strikes against the target from the launch point, without intermediate or third-party hosts involved except in normal traffic routing.

Examples of attacks that often use the direct strategy are spam email, cache poisoning, and routing black-hole attacks. In the case of the non-profit, one attack of concern might be a volunteer making unauthorized changes to the financial information.

Reference

Barr, M. (2018). *Intellectual Property Protections for Software*. [online] barrgroup.com. Available at: <https://barrgroup.com/software-expert-witness/articles/intellectual-property-protections-embedded-software-primer> [Accessed 10 May 2022].

Cannell, J. (2013). *Tools of the Trade: Exploit Kits*. [online] Malwarebytes Labs. Available at: <https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/>.

Gov.UK (2012). *Redundancy: your rights*. [online] GOV.UK. Available at: <https://www.gov.uk/redundancy-your-rights>.

Imageware. (2021). *Identification, Authentication, Authorization - What’s The Difference -*. [online] Available at: <https://imageware.io/identification-authentication-authorization-difference/>.

Miller, S. (2021). *What GC should know about 4 types of intellectual property*. [online] legal.thomsonreuters.com. Available at: <https://legal.thomsonreuters.com/en/insights/articles/four-types-of-intellectual-property>.

Sharma, A. (2021). *How to Ensure Data Integrity in Your Organization*. [online] DATAVERSITY. Available at: [https://www.dataversity.net/how-to-ensure-data-integrity-in-your-organization/#](https://www.dataversity.net/how-to-ensure-data-integrity-in-your-organization/).

Thomas, J.P. and Essaaidi, M. (2006) *Information assurance and computer security* Amsterdam ; Washington, Dc, Ios Press.

Wikipedia. (2022). *Information security*. [online] Available at: <https://en.wikipedia.org/wiki/Information_security#:~:text=Information%20security%2C%20sometimes%20shortened%20to> [Accessed 10 May 2022].

‌