One **internal** security threat that can affect the IT systems of an organisation is a weak password and lack of two-factor-authentication, this can make it easier for people to guess your password or just use a brute force tool to get your password which can lead to important company information being compromised. Another internal threat is employee misconduct where an employee goes against the company rules which can hurt the organisation, and unintentional disclosure of information where crucial data is leaked by accident. Also, unsafe practices such as using external flash storage and CD’s, visiting untrusted websites and downloading files from disreputable locations, this can unintentionally or secretly steal your data or give you malware, this is a breach of confidentiality and is against the law.

An **external threat** is data theft (it is also possible for theft to be an inside job) and withholding of digital information for either political purposes, such as defamation or exposing someone’s crimes, or financial gains (to gain money through blackmail or stealing it). The data that is obtained by the attacker maybe sold to a third party or they may encrypt the data and sell the decryption key to the organisation it was taken from using ransomware ( the purpose of this is to lock them out of their data and force them to pay to open it), this can be protected against by locking it in a secure area to protect it from people who have malicious intent towards the company such as rivals or thieves. This is usually classed as cybercrime and is when someone on the inside tries to get into the system and use it as ransom or to obtain data. These can be protected against by having a firewall / antivirus software.

A **physical threat** is theft or damage of equipment, damage by accidents such as floods, fires or any other disasters including terrorist actions. This usually targets servers or backups and can be prevented or at least safe guarded against by keeping them secluded in a secure area with locked doors and pass codes guarded by trusted employees.

Physical threats to computer systems are also sometimes caused by losing your secure credentials. This is not a physical threat in the sense of damaging your equipment, but it is the loss of a password and the related disclosure of sensitive data that puts your computer out of action. You can easily and safely reset a compromised password or even get a new one, but it's essential to keep a copy of the most recent password on hand to avoid a potential security breach in the future.

**Software Threats** can be caused, some software is harmless and actually quite helpful and others can be malicious and try to steal your data or downright delete it; there are some other malicious software that can hack your computer and install virus’, ransomware or spyware which can impact the security of a business. Malware like trojans can be installed secretly with other non-malicious software and make it much harder to see the root cause of the problem when you are trying to get rid of it. An example of trojans are keystroke loggers, used to steal passwords and can then be used to hack into accounts for ransomware or to steal money.

Software threats come from downloads off of the internet especially if the download is from untrusted websites with no reputation or even negative reputation. Preventative measures can be put in place by blocking the users access to certain websites, having a good firewall and antivirus or not allowing downloads to take place.

Privilege escalation is a threat where software exploits such as backdoors or bugs are used to gain more user privileges.

A logic bomb is a small piece of code that can be implemented into a piece of code in order to set off a malicious action like deleting or stealing files or even writing a rootkit to a server to have complete superiority over what happens in the server and always know the confidential data of the company.

Some examples of software threats are:

* Malware – any types of a malicious software.
* Virus - spreads from one computer to another, usually sent attached to emails or secretly downloaded from strange websites - they infect your computer and send spam, steal passwords, contacts details, bank details, keystrokes and other things such as erasing all of the data on your hard drive or SSD.
* Adware – software that keeps track of what you browse and shows you adverts and popups with your consent. If this is done without your consent it is called malicious adware which is against the law and classed as a malware.
* Spyware - installs on your computer without your knowledge, it spies on you and steals your data and keeps track of your activity like key strokes or passwords or internet history; it can even record videos through your webcam or sound from your microphone - which is why people usually cover their laptop cameras with tape.
* Trojans - tricks users into running it by hiding behind a legitimate program. One of the things that trojans can do is record your passwords by logging keystrokes, they usually spread by email. Unlike worms they cannot create copies of themselves.
* Phishing - a method of obtaining private data such as passwords and credit card details.
* Rootkit - enables remote control and admin access over a computer network or a single computer. When access is obtained the rootkit has keyloggers and antivirus disablers amongst other malicious things.
* DDOS - attackers flood a website with too much traffic (DOS). A DDOS is when this is sent from multiple computers or ‘nodes’ called a botnet (which are different computer stations which are also remotely activated in the ddos attack to flood the website with more traffic), it can be sent from anywhere from tens to hundreds of thousands.
* Computer worms – malware that replicates very fast and spreads from the infected computer to others, it sends the virus to the target’s contacts, then to their contacts and so on.
* Rogue security software - misleads users to believe there is a problem with their computer such as a virus. They then ask you to install their ‘security software’ from a link to remove the problem or pay for a tool that removes them for you. Both of these actions will lead to some form of malware being installed onto your computer.
* SQL injection - SQL injections, this injects malicious code into an entry field to be executed, this is done by exploiting invulnerabilities within an application. It can be used to spoof your identity, tamper with pre-existing data or destroy or steal data completely.
* Man-in-the-middle attacks - cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen to a communication which should be private.
* This can be spoofing your DNS or IP address or email hijacking in order to obtain private data.

A social engineering threat is similar to software threats but they include more deception like phishing and identity fraud. The above-mentioned phishing emails and rogue security software are included in this.

A **passive threat** to the security of the systems of the organisation is something that happens without the need for the attacker to constantly pay attention to it and it can collect information from the systems.

Examples of this are:

* Wiretapping, which is tapping into the telephone wires to intercept any calls or transmission used in phone calls and to eavesdrop on calls. This is used a lot in spy movies by the police but the way it works is by connecting a listening device to the circuit carrying information between the phones - when you talk into a phone the sound waves from your voice are transmitted across a copper wire, when this current goes to the phone network in is translated into digital information so that it can be sent as fast as possible to the receiver over a long distance. The listening device intercepts this digital information and allows you to hear it.
* Port scanning, which is used to check which ports on a network are active so that an attacker can know the best way to infiltrate a system. This is not always a malicious act as it can be used to check if a server is active and then join it such as a chat group or a game match, but it can be used as a precursor for an attack and be the setup for it. A port sweep is where you scan for every terminal that is connected to a certain port, it is used to search for a specific service.
* Idle scanning, this is where a computer sends a signal to probe a ‘zombie’ computer and find out which services are available, this is done by copying the zombie computers ID and copies it whilst spoofing its own ID to emulate it (to exploit the trusted relationships between IP’s of machines) and then impersonates the zombie and observing its behaviour. This is a very good attack because there is no interaction between the attacker and the defender ass the zombie is used to attack.
* Man-in-the-middle-attacks: IP spoofing where you trick the target into thinking you are interacting with a website when you are not, giving the attacker access to classified information. DNS spoofing where the user is forced to go to a fake website rather than a real website. The goal is usually to either divert traffic from the real site or to capture the user’s login credentials or pin codes. Email hijacking is where the attacker gains access to the Targets email address and can see their personal email such as bank statements or being able to monitor transactions between an organisation and its customers. The attacker can then spoof the banks email and send their own email to the customers and convince them to follow their orders, an example of this is pretending to be a bank and having the target send you money.

An **active threat** to the security of the systems of the organisation is something that happens with the attacker constantly inputting data to manually control the attack. Examples of this are:

* DDOS attacks, this is where attackers flood a website with too much traffic (DOS). A DDOS is when this is sent from multiple computers or ‘nodes’ called a botnet (which are different computer stations which are also remotely activated in the ddos attack to flood the website with more traffic), it can be sent from anywhere from tens to hundreds of thousands.
* Spoofing, this is where the attacker impersonates another user or device on a network in order to access classified information or to launch attacks against network hosts
* Smurf attacks, A DDOS attack which sends a lot of internet control message protocol packets with the intended victims spoofed IP to a computer network which will in return send a reply to the victims IP, the aim of this is to send so many replies to them so that their PC slow down and has trouble running properly and is almost impossible to use
* Buffer overflows, this occurs when there is too much data being written to a buffer and the data is written onto adjacent memory locations, this may cause undesirable effects when the code is run or the program may crash or return incorrect results. By causing a buffer overflow it is possible to write malicious code into areas where executable code is supposed to be, or to overwrite specific parts of the program to your will.
* SQL injections, this injects malicious code into an entry field to be executed, this is done by exploiting invulnerabilities within an application. It can be used to spoof your identity, tamper with pre-existing data or destroy or steal data completely.
* ARP Poisoning, also called ARP spoofing is where you spoof the ARP (address resolution protocol, this is a communication protocol used for discovering the link layer address which allows you to find the address of who to send messages to) messages to a LAN. The aim is usually to associate the attackers MAC address with another host’s IP address thereby intercepting their traffic – ARP spoofing can be used to modify the traffic, stop the traffic in its entirety or to intercept the data on a network, it is often used as an opening for other attacks such as man-in-the-middle, session hijacking or DDOS attacks. Under normal operation data is sent from the LAN user to a hub/switch, then to a LAN gateway and finally to the internet and information is retrieved in the opposite direction. A routing subject to ARP spoofing will have the malicious user connected to the hub/switch in order to intercept the incoming traffic. The downside to this however is that the attack can only be used on networks that use ARP and requires the attacker to already have access to the local network that is going to be attacked, such as an internet café.

Some risks with the **security** of **cloud computing** are, loss of property or data as a result of more companies using cloud servers from hackers. You have no control over how your data is handled as the employees can be doing pretty much anything to your data whilst staying undetected. There is also the risk of users losing trust in the organisation after a data has been lost, which could negatively affect the reputation and image of the company which in turn would cause less people to use their storage and instead go to other competitors in the same market.

The 3 principles of information security are confidentiality, integrity and availability.

Confidentiality – Keeping data secret and being trusted to do, so that the there is no risk of the data being used against the will of the original owner and so their security is not compromised.

Integrity – There are 3 goals for this: making sure that data cannot be modified by any unauthorised users, preventing unauthorised modifications and maintenance of data consistency and data accuracy.

Availability – to ensure that data is available in the case of any external influence. There are commonly 3 external threats to the availability of data: DDOS attacks or errors in the software that can cause flaws in it and cause breaches, malfunctions of the systems that store data due to f natural actions, human actions or failing equipment.

Unauthorised access/modification of data -This is when someone has access to information they shouldn’t either by hacking or being granted permission by someone with a higher security clearance.

Principle of minimal access to information or lowest required access permission to be able to maximise protection - only allows the employee the least amount of permissions that allows them to properly perform their work. So they can’t access and tamper with confidential data or data that is not suited for their job roles such as the CEO or HR managers data.

Deliberate or accidental loss of information – (deliberate data loss) when your data is maliciously stolen by an external force, or in some cases it may be an internal force such as a backstabbing employee or a spy. The stolen data can then be held hostage and used for a ransom. (accidental data loss) accidental deletion, human error or natural causes such as a fire, gas leaks, pipe leaks, flood or earthquake. Measures can be put in place to prevent this by not allowing most employees access to files that contain important data or in the case of physical threats like fire you can improve your security around the storage devices in real life and perform maintenance regularly.

The need to protect intellectual property from theft or malicious damage:

Personal information – if leaked can result in identify theft and misuse, it should be protected from people with malicious intents or not high enough security clearance to reduce the chance of the customers private details being deleted or tampered with. The data should be protected because if it is breached or leaked and gets into the wrong hands it would compromise the integrity of the data and will affect customer and employee trust in the company and may result in legal issues and punishments such as lawsuits.

Bank account details – need to be protected so customers dont need to create new bank accounts or freeze their current ones because of theft, as it could lead to exploitation such as money being stolen or used to open up more fake bank accounts in your name.

Employee details – the employee details need to be protected as if they are stolen it could lead to wages not being paid at all or incorrectly paid too much or too little which may cost a lot to fix and they may lose faith in the business as it can be seen as not secure with their private details.

**Data protection act:** This outlines the rules for organisations to follow when it comes to using personal data. This includes regulating the processing of personal data, protecting the rights of the data subject, allowing the ICO (the company that enforces the data protection act) to enforce the rules of the data protection act.

They must make sure that data is used fairly, lawfully, transparently and for specified purposes. It should be used in a way that is adequate, relevant and limited to what is needed. It should be accurate, have minimal discrepancies and be kept up to date if possible. It should be kept for no longer than is necessary and handled in a way that makes sure that there is appropriate security against unlawful or unauthorised processing, access, loss, destruction or damage of data.

Organisations ensure data is kept secure by having regular check-ups on data that is collected by ‘data cleansing and validation’, checking if they are of decent quality, they also make sure that the correct roles are set for the data management for a data protection officer.

**Computer misuse act:** This was put into action in 1990 and defined 3 offences to deal with the problems of hacking, virus’ and malware. These are, ‘unauthorised access to computer programs or data’, ‘unauthorised access with a further criminal intent’ and ‘unauthorised modification of computer material’ (data or programs).

The computer misuse act states that a person is guilty of ‘unauthorised access to computer material if they cause a computer to perform any function with the intent to secure access to any program or data help in any computer, the access they want is unauthorised or they are aware that they are taking part in an illegal act’.

**Copyright, designs and patent act:** This is a way of making sure that no one steals another person’s work or blatantly plagiarises it. I began in 1998 in the UK and was originally intended for books, sheet music and photographs among other things, it is the UK’s form of the IRP (intellectual property rights) which exist in other countries.

It’s areas of expertise are Copyright, design, licensing and royalty agreements, trademarks and trademark searches, confidential information including non-disclosure agreements and IP agreements, IP disputes including injunctions.

**Book:** protects the book’s content whether it be pictures or words regardless of the content. Others can write about the same or similar subjects as long as it doesn’t directly copied word for word or adapted and minimally changed, this also applies to work submitted online.

**Software:** protects the software and the code behind them so isn’t copied (stolen or plagiarised) and passed off as the thief’s own creation.

**Media:** protects movies, videos, images and music by copyrighting the characters and storylines from books and novels or comics. It protects music and soundtracks from movies too. Copyright always lasts 70 years for all types of media - This is done to protect media from being stolen and/or plagiarised.

**Telecommunications regulations:** These regulations began on the 24th October 2000, it states that ‘businesses in EU member states may legally record communications on private networks that occur as part of lawful business practice’, interception of communications is only lawful in the case that it allows the business to comply with other regulations, if it establishes the existence of facts, acts as a means of verification to ensure that the person being monitored is performing his or her work to standards and conducting themselves appropriately towards customers, if it helps maintain and bolster UK security and could prevent, or at the very least detect, criminal activity.

**Monitoring** can be done through gathering data from terminals, CCTV cameras, checking workers emails, using automated checking software, examining logs of visited websites to make sure that workers are not misusing their work time on unproductive things that are unrelated to work such as games or pornography, recording phone calls, checking the logs of telephone numbers, videoing workers outside of the workplace that claim to be sick to ensure that they are telling the truth, obtaining information through credit reference agencies to check that workers are not in any financial difficulties.

**Company email and phone monitoring:** This can be used to protect employees if they are taken to court by any customers for any work-related reasons. It is legal to monitor the employees if a reason is given as to why it is happening, and is long as it is not for malicious reasons. Meetings can be done only on company equipment such as tape recorders such as HR meetings that are to inform an employee if they are breaking any rules and to give them warnings. Certain websites can be blocked to ensure that employees aren’t being distracted during their work time and that malicious software cannot be unintentionally downloaded to the company network thereby not only jeopardising the company’s private data and the customers account details but also compromising the security of its data and potentially getting that employee fired.

**Fraud act:** the fraud act states that a person has committed fraud if a person has ‘represented something falsely in order to gain something and it is considered false in the case that it is intentionally untrue or misleading, failed to disclose information if dishonesty is used to fail to disclose another person information if gain is intended to be gained through misleading or loss to another is intended, or abusing the position they are in’. This can lead to up to 10 years in prison or 12 months in prison and a fine.

There are different kinds of fraud such as Botnet-related, slick fraud, hacking, rogue security software, software service fraud, domain name scams, facility takeovers, invoice scams, internet dialler scams, malware and computer viruses, phishing, proxy servers, tab napping and website domain name scams.

**Legal liability for contract obligations:** Organisations and/or individuals can be held accountable to a legal standard if they break the law. This includes disclosing confidential materials to aid any investigations that may take place do to legality issues or such as if the company is being sued by a former employee for any reasons such as mistreatment, this is so that they can protect themselves against false claims placed against them by employees.

Compensation claims can be made if data has been lost or leaked. If businesses have had their company data leaked, if your data has been sent to a third party or if your information was used for journalism, artistic or literary purposes without your permission.

P4 “**Explain** the principles and uses of **cryptography** to secure and protect data.”

**Cryptography principles:** This is used to improve data security when sending confidential data. The principle of encryption is to make data unreadable by making it disorderly and mixed up in to improve security so that no one can read it. The encrypted data can be decrypted if you are using a decryption key, it is meant to protect the data even if it is intercepted.

**Cryptography methods:**

* Digital rights management (DRM) – rights that allow you to use digital media or use any electronic devices. It protects digital products such as software and games from copyright.
* Password storing and salts – salts are added to hashed passwords to increase their security even further by adding random characters, numbers and symbols to make it harder to de-hash into their original form.
* Obfuscation – making something hard to understand and/or read and making its meaning less clear. This is done to data to improve the security. An example of this is mixing up the sequence of letters in a word.
* Steganography – where messages are hidden in plain sight such as in a picture or a tattoo. This is done by changing various aspects of the image such as colours, brightness, contrast or other visual settings, in tattoos they can be hidden beneath hair as hidden messages, this allows secret messages to be hidden and will be very hard for anyone else to find them.
* Secure transactions –increases security by encrypting and hashing data. It does this to restrict sight of card details in payment transactions to restrict what hackers can have access to.
* Two factor authentications – where a second layer of validation checking after the password is required to unlock something, such as another password, passcode or secret information / question.
* File, folder and disc encryption – encrypted files are only available if the user who encrypted the date is currently logged in to the computer.

**Cryptography applications/methods:**

* Encryption algorithms – different ways to use encryption.
* Shift cyphers – a cipher where the letters are moved along by a certain key, an example of this is a Caesar cipher.
* Block ciphers – a cipher that encrypts a block of text at a time instead of a stream of text, a predetermined number of bits at a time.
* Stream ciphers – a cipher that encrypts a stream of text at a time instead of a block of text, one bit at a time.
* One-time pads – a uncrackable encryption technique that uses a one-time pre-shared key that is longer or the same size than the message being sent, this key is combined with plain text to encrypt it.
* Hash functions – any function that is used to map any data whether it is fixed or changeable, the values returned by this are hashes, hash values, hash codes or digests. They can be put into a hash table.
* Cryptography primitives – low level cryptographic algorithms that can be used to make cryptographic protocols, an example of these are encryption functions and one-way hash functions.
* Cryptographic salts and their use in storing passwords – random data that is added to hashes to make them harder to decipher, they are used to protect passwords.

**Cryptography applications:**

* HTTPS protocol – this stands for hypertext transfer protocol secure, it is usually used for a website and is a protocol that dictates the secure communication on a network, the communication protocol is encrypted by TLS or transport layer security.
* Symmetric key encryption – a form of encryption where the same key is used to both encrypt and decrypt data.
* Public key encryption – allows you to send the key to the recipient on an open insecure channel, it is also known as asymmetric encryption.
* Virtual private networks (VPNs) – allows you to spoof your ip and location so that you can access websites that are blocked in your region.
* Key exchanges – where cryptographic keys are exchanged between 2 parties.
* Digital certificates – an electronic identity certificate.
* Generic routing encapsulation (GRE) tunnels – a tunnelling protocol that can express the features of a wide variety of network layer protocols over an IP network.

**M1** Assess the impact that IT security threats can have on organisations’ IT systems and business while taking account of the principles of information security and legal requirements – Organisations and/or individuals can be held accountable to a legal standard if they break the law. This includes disclosing confidential materials to aid any investigations that may take place do to legality issues or such as if the company is being sued by a former employee for any reasons such as mistreatment, this is so that they can protect themselves against false claims placed against them by employees.

Compensation claims can be made if data has been lost or leaked. If businesses have had their company data leaked, if your data has been sent to a third party or if your information was used for journalism, artistic or literary purposes without your permission.

Some examples of security breaches affecting companies are:

NHS (National Health Service): the openly funded healthcare system of the United Kingdom. The official NHS website says “The core function of the NHS is emphasised in this value – the NHS seeks to improve the health and wellbeing of patients, communities and its staff through professionalism, innovation and excellence in care.” Which means its primary purpose is to help people.

The Key Challenges: The Nuffield Trust surmises that the developing populace alone could mean we need another 17,000 clinic beds by 2022 and that is only the medical clinic beds. The quantity of specialists, medical caretakers, other staff and hardware all need to meet cases.

* A mature, growing population.
* Developing medicinal service’s needs, for example, the augmentation in instances of overweighting and diabetes or anti-infection opposition.
* Clinical enhancements spare loads of lives each year, however push up costs huge. It is speculated that advancement in clinical innovation costs the NHS at any rate an extra £10 Billion per year
* The Closure of nearby administrations planned to centralisation drives.
* An increase in reliance on privatized administrations.

The Issues: typical themes at clinical school meetings you will frequently be asked your assessment on current news influencing the NHS are:

* The Brexit’s impact on the NHS.
* The Current NHS mental health services.
* The Vaccinations.
* The weekly NHS.
* The Junior doctors’ contract.

The Approaches: The present Conservative government has concurred for an extra £8 Billion in financing by 2020, which is the base sum NHS England manager Simon Stevens says it will require so as to deal with its current issues (covid-19).

•To set aside cash by cutting a greater amount of the social consideration spending plan.

•But barely increase the funding for psychological wellness.

•To attempt to diminish the holding up times by guaranteeing section to a GP week after week and arrangements inside 48 hours for the more than 75-year olds.

•However, they won't decline the cap on the measure of pay NHS Trusts can make from private patients, which could negatively affect holding up times and the weight on administrations.

•BA (British Airways): It is the UK's national aircraft set up in London and at the London Heathrow Airport. It is one of the world's greatest aircrafts and an establishing individual from the oneworld navigation partnership.

Technical Issues and IT Glitches – A solitary mishap of a specialized issue is difficult to pardon. Be that as it may, some will result it in destroying the designs for a large number of travelers is over the assents. These flaws came about by and large in undoings and mass humiliation. The travelers money related and individual information additionally got hacked, which is illicit.

Imitation of Budget Airlines – It makes the clients troubled, which raises when they began to perceive British Airways is secretly transforming into a budget airline. The benefit of flying with them began to diminishing rapidly. The expression 'budget airline’ normally has some positive undertone, yet not when there are no points of interest involved. That is simply called being a cheapskate.

The Staff Strikes – The Passengers are not by any means the only ones demonstrating their despondency. Affirmation of the newspaper service 'The Guardian', the staff went on strikes in light of BA's low badge policies and general administration issues. Pilots feel slighted and frequently get the flights dropped. This influences the travellers, bringing about a dangerous cycle of consistent complaints.

Unforgivable Delays – The delays, brought about by strikes and specialized issues is accompanying long stretch flights, which got grounded for as long as 22 hours. Particularly those going for business surely passed up some significant occasions and obligations.

They Terminated Their Partnership with Financial Times – The BA are also minor. They halted given Financial Times to travellers in light of the fact that the paper ensures some unpleasant tales about BA, that they disagree with.

NatWest (National Westminster Bank): It is a British ‘major retail and commercial bank in the United Kingdom. It was established in 1968 by the merger of National Provincial Bank and Westminster Bank. Since 2000, it has been part of The Royal Bank of Scotland Group.’

* Payment risks – To trade this globally can appear to be trickier than trading in the UK. The Exporters need to get paid on schedule. The Importers need to get their hardware's on schedule. To understand your choices is to lead the managing and lessen the payment risk.
* Foreign exchange risks – To trade rate variation to give a risk to any organisations that exchanges internationally. Our FX risk management services could help cover you versus such vaporizing.
* Regulations that deal with risk – To understand your duty in international exchange and the global trade can be a threat. The industry-wide standards and norms and terms can be confounding. To popularise yourself and advance with the basics could assist your association with running more simple when exchange cross wide borders.
* Incoterms – An internationally notice methods for resolve obligation when equipment is moved overseas.
* Uniform customs & practice – These authorize rules as to control about the letters of wealth and the record assortments.
* Scottish Environment Protection Agency (SEPA) – An EU action that makes it easier to make any payments inside the Eurozone.
* Payment Services Directive – To make it easier and faster to cross-board the payments across Europe.

**M2** Analyse how the principles and uses of cryptography impact the security and protection of data.