Question 1: Two of the key areas in security are data classification and security education. With the help of examples, explain why these particular areas are critical for security and describe at least two problems, for each area, that may arise if the security set-up does not take them into account.

Data classification is the process of organising data into categories that makes it easy to retrieve, sort and store for future use. There are five types of data that can be classified, specifically, Public Data, Private Data, Internal Data, Confidential Data and Restricted Data. Data classification helps to protect the integrity of the data in a company. Data classification is important as it determines which parties are allowed access to the information. If a security set-up does not take data classification seriously, an important document may be accidentally modified by an employee if it is not on a shared drive. Another problem that may arise is the chance that a disgruntled employee will have access to top secret information and may sell the information to the company’s competitors. Both issues compromise the integrity of data.

Security education should be enforced as this ensures that all employees are aware of the data policies that are in place. Without proper security education, employees will not be well trained to spot a phishing attack. The security of the data would be compromised as employees may click on phishing links, causing their computers to be prone to hacks. Staff members will also be unaware of how to report a phishing incident if it occurs and thus, the incident will be prolonged. The organisation will be better able to respond to the incident efficiently and accurately with appropriate reports.

Question 2 Explain why the current distributed nature of today’s systems poses new security challenges.

Communication is not secure, companies and individuals are prone to cyber attacks (eg. websites are not using https). There will also be more opportunities for hackers to access more information. Today’s systems are more complex and hackers will be able to find new ways to conceal themselves. This will make it more difficult to track hackers.

Question 3 Most organizations are putting a lot of effort into having an Internet presence as it offers the potential to reach a very large number of potential customers with minimal cost. Describe in detail at least two major drawbacks of having an Internet presence from a security perspective.

Having an internet presence will cause companies to be prone to social engineering attacks. This allows hackers to access information on the company. Hackers will be able to get emails and names of employees working in the company on the websites and send phishing emails to the company. Companies may also unintentionally show their vulnerabilities on the website. Hackers can then tap into these vulnerabilities and hack their system.

(Employees that deal with cyber security constantly try to hack into their company’s system and look for vulnerabilities to better patch the system.)

Question 4 The introduction of mobile devices such as iPhones and Android tablets has changed the way in which organizations deal with security. Explain two ways in which such mobile devices compound the problem of keeping a system secure.

Mobile devices adds to the vulnerability as information are now easily copied and recorded via the camera and microphone function.

Furthermore, phishing emails can extract information on mobile phones, access one’s photo gallery for personal information and steal credit card details from mobile banking applications. Viruses such as trojan horse connects devices back to the hackers and hackers will be able to access and control the devices remotely.

Question 5 Explain with the help of an example why old equipment can pose a major security problem for an organization.

Firstly, old equipments usually have servers that are end of life. End of life servers do not contain patches that are recently released by the vendors. Hackers can then make use and exploit the vulnerabilities that are present in the old servers.

Secondly, the older the hardware, the more likely it is to fail. This affects the availability of the hardware and customers as well as employees will not be able to access certain services.

Question 6 Consider the statement ‘‘The availability of information has made system security a much more difficult task than in the past.” Argue for and against the statement.

(\*For and against - present both sides)

(FOR) The availability of information has made system security a much more difficult task than in the past as operating systems and applications will be more vulnerable to security breaches and this compromises the confidentiality and integrity of the information available.

(AGAINST) However, the availability of information allows organisations to have access to knowledge on how to better secure operating systems more accurately. More testing tools will also be available on the web for professionals to test the security of their system and improve their current systems.

Question 7 What is the problem with an approach in which an organization is focused only on the business end and considers that information technology is solely the domain of the computer operators and system administrators?

Security is the responsibility of all members in an organisation. For a company that considers information technology to be solely the domain of the computer operators and system administrators, it will be more likely that security programs are developed without getting proper management support and direction. Such measures will be ad-hoc and only focuses on short-term issues instead of the long-term goals of the company. Such measures will be difficult in large organisations and will be like;y ineffective.

With unreserved backing of the management, computer operators and system administrators will be receive direction coming from the top management and implement measures that will be more aligned with the organisation’s long-term strategic goals. Such measures will also be more effective as directions would be from the management.

Question 8 List six (6) components of an information system. For each component, give an example of a data security issue associated with it. Your answer must cover two (2) availability issues, two (2) integrity issues, and two (2) confidentiality issues and you must clearly indicate the type of issue.

AVAILABILITY

One availability issue pertaining to hardware includes the uninterrupted power supply that may not be reliable. Unreliable power supply may then lead to downtime

Another availability issue pertains to software. A software may contain bugs and lagging would occur, servers will thus hang very regularly and the availability of the software would be affected.

INTEGRITY

An issue pertaining to software comes from the lack of proper data classification. Unauthorised people will be able to access information that are private or top secret. The integrity of the data would thus be jeopardised

Another issue pertaining to integrity stems from employees not being properly trained and educated. There will then be a higher chance for employees to make improper and unauthorised changes to the information.

CONFIDENTIALITY

One issue pertaining to the confidentiality of the information includes insecure wifi network and webpages. Hackers will be able to sniff and intercept the traffic of internet usage.

Another issue stems from the lack of security policies. If an employee uses computers in public spaces to access a shared organisation internet, trade secrets will be prone to leakage as information will be made public when other users access the same public computer. Confidential information will then also be prone to be released to the public.