Answer Sheet – Level 3 Principles of ICT Systems and Data Security

(7540-040/7630-345) Assignment A

Task A1**:** Identify and describe the consequences of **ten** common physical threats to ICT systems and data including hardware damage, loss and theft eg

* deliberate damage to hardware or equipment
* inadequate physical security
* loss or theft due to size or portability of devices
* accidental damage to hardware or equipment.

|  |
| --- |
| Poor physical security through no or bad locks on:   * Building doors * Server enclosures * Hardware not being tied down |
| Not signing in visitors |
| Power Cuts |
| Water damage from rain |
| Natural disasters (earthquakes, typhoons) |
| Hardware wearing out |
| Accidental Damage, such as impact dropping devices |
| Fire |
| Smoke |
| Act of Terror (such as a bombing) |
| Combined consequences of the above physical threats:   * Data loss can cause the business to lose money and face through them not being able to secure customer data. * Data used for malicious purposes could cause legal repercussions by customers for not protecting their data. * Replacing hardware can cost financial resources including manpower to repair/replace the equipment as well as the cost of the hardware itself. * If the threat of the IT Systems and Data could have been secured by the IT personal then the IT personal may lose their jobs for not working effectively. * Threat resolution may cause system downtime, which could affect company productivity. * Poor security can also cause vandalism, theft or destruction of hardware in the workplace. |

Task A2: Identify and describe the consequences of the following types of malicious code:

* Virus
* Malware
* Spyware
* Adware
* Trojan
* Logic bomb
* Worm
* Rootkits
* Keylogger.

|  |
| --- |
| Malware – a general umbrella term for a piece of software or program that is used to impede computer operation, gather information or gain access to computer systems. The consequences are varied and explained in each of the below forms of malicious code. |
| Virus – a program that replicates itself inside of another program causing program malfunction when initiated by a form of execution. The consequence of which include system or program failure, data theft, lost or failure. |
| Spyware – a specific malware used for gathering information on users data without the user knowing that they are being “spied” upon. The consequence of this is the user can have their personal information gathered and stolen, for instance a keylogger is a form of spy ware that can do this. |
| Adware – a program used to feed targeted ads to the user so the company behind it can receive revenue. The consequence of this is varied as Adware can be good and verified, such as Google Ads or malicious and infect user’s computer with ads that they haven’t given permission to see through unauthorised tracking. |
| Trojan – a non-replicating program that is usually hidden within a legitimate program or file and when executed runs. The consequence of this is usually loss, theft of data or system damage. |
| Logic bomb – malicious software that can be triggered when a certain condition is met. The consequences of this is that it can trigger other forms of malicious code, thus making it difficult to diagnose the root cause of viruses. |
| Worm – a self-propagating malicious program that replicates similar to a virus and can spread across computers via a network. The consequence of this is the large downtime necessary to solve a widespread virus. If the company has 100+ computers connected in a network, then each of them are susceptible to the worm virus. |
| Rootkits – a program that hides other programs or processes and give access to the user’s computer to outside influences (usually found in the registry). The consequence of this is that the user’s information can be tracked, stolen or manipulated without them knowing through it hiding other malicious programs. |
| Keylogger – a program used to track keyboard and mouse inputs. The consequence of this is that user’s passwords, links and personal data can be gathered in the background without them knowing they are being tracked. |

Task A3: Identify and describe the consequences of **seven** other common types of electronic threats to ICT systems and data.

|  |
| --- |
| Power Surge – a faulty PSU or usage too many components may cause a power surge which can break your motherboard and any attached components. This can cause a major monetary offset. |
| Electrostatic Discharge (EDS) – consequence would be any additional electronics which are not regulated and can interfere with WiFi signal or reduce operating capacity. |
| PSU failure – may result in a power surge, which would enact the power surge consequences above, in addition to needing to replace the power supply. |
| Weak passwords – the consequence being increased chance of hacker’s brute forcing themselves into a network or a visitor easily gathering the password through a glance, causing potential network vulnerability. |
| Hacking, e.g.   * DDOS (Distributed Denial of Service) attacks – consequence being network disruption and downtime through blocked traffic. * Drive-by-download attacks – consequence being a virus running on the system. * Phishing – user may trust the phishing attempt causing information loss that may cost the company business. |
| Incorrectly configured hardware – consequence being potential hardware failure or inability to start, which may cause financial loss for the company. |
| Data corruption – consequence being loss of company or customer data which may break legal rules or cause manpower to be reassigned so time can be focused on it. |

Task A4: Explain **five** security vulnerabilities associated with remote access technologies, including wireless.

|  |
| --- |
| **Remote Desktop Connection or TeamViewer**  Remote access technologies allow workers to access other computers either through a local area network or online. This has two main security vulnerabilities, the first being that one user is able to access all others user’s local data if they have an administrative account and the computer is turned on. Another one being that if a user connects via online then depending on the security credentials that they setup or use, then it is possible that their connection is being monitored and someone else can gather login credentials to login themselves, thus exposing data. |
| **Home-working**  Remote Access allows for homeworking to be accomplished as users will be able to login to their company network or work computer from home. However, in addition to the security concerns mentioned previously. There is the added concern that as the user can access and download files to their local system, then any sensitive company information is now accessible on the user’s network infrastructure. Therefore even if the company has good data protection, the user may not, causing data to be vulnerable. |
| **Wireless**  Open wireless connections are not secure. Whenever a user sends a request to a website, their data packets are able to be viewed by spyware or through legitimate network monitoring tools such as Wireshark. This would reveal user passwords, internet history, anything they use the internet for. It is also possible to access the user’s computer from the web using malicious programs sent to them anonymously. Most home networks use upgraded encryption, called WPA2, which provide a greater level of protection then open networks. As everyone can see wireless connections, it is possible to log into the users router using default connection if they haven’t changed them. |
| **Bluetooth**  Bluetooth versions 4.0 or prior have only basic security available on a consumer scale. Even newer versions of Bluetooth can be easily eavesdropped or undergo DDoS attacks because of the security vulnerabilities that it contains on an initial design level. This has caused Bluetooth to go out of fashion for managing secure connection of files, most often they are used for general voice calls or transferring music to portable speakers even though newer versions have better basic security such as 128 encryption. |
| **Webpages**  Webpages or websites typically run scripts can be run in the background or upon activation and can infect the user’s browser, which can then be used to gleam further details. For example, a script that installs a browser keylogger, which then logs user passwords and username, allowing the person behind the script to access the user’s details. |

Task B1: Describe the methods of providing physical access control and security for ICT systems including:

* locks (hardware locks and entry locks)
* biometric controls (fingerprint, voice and retina recognition)
* CCTV
* fire control systems
* shielding (cable screening)
* Faraday Cage
* Motion detector.

|  |
| --- |
| Hardware locks and entry locks are physical devices used to provide security against a physical entity gaining physical access to a building or room. These devices are often used as a deterrent by making it appear difficult to enter a room. Locks allow hardware to be not easily removed from a premises. |
| Biometric controls have the same intention of limiting access to the physical building or room that regular hardware locks and entry locks provide. However they have additional security controls built into it that are tied directly digitally to the person whom is accessing it. This makes it a lot harder for potential thieves to break or crack locks as they require the relevant biometric data of a person who has direct access. If a brake in does occur and the biometric controls get set off then it would be easy for the authorities to track down the person with the relevant access control. |
| CCTV (Closed-Circuit Television) is a common deterrent and method of limiting security breaches. The visual presence of security cameras often dissuades people from tampering with equipment and if they are do, they are recorded. This recording can then be reviewed in court as evidence against them. |
| Fire control systems are used to prevent and mitigate fire damage to various IT systems. Temperature logging is a very important competent in IT infrastructure because components may overheat if they are used at or beyond their typical operating limits. This logging allows fire prevention in case of a component blowout which may lead to a fire. Additional most IT rooms should contained Co2 Fire extinguishers so that if a fire does occur then it can be exterminated without affecting the components. All IT rooms should have a fire alarm connected to the local fire department also. |
| Cable shielding involves layer of metal, usually copper or aluminium that covers the wires through a piece of cabling. This covering acts as a protective jacket against electromagnetic interference of electronic components, which may corrupt data transfer and individuals entering the cabling themselves as they can be quite tough. These types of wire are called STP (Shielded-Twisted Pairs) and act as a faraday cage. |
| A faraday cage is a metallic conductive cage that transmits electronic discharge around the cage so that the components within the cage, typically servers or cabling, are protected. As there are a lot of electronic equipment within a server room or cabinet, faraday cages are an important data protection method to ensure if a fault or electronic discharge occurs, the data is protected. |
| Motion detectors are used to deter and catch any physical access to rooms or buildings. They are sensing devices linked to an alarm systems that when activated alerts the relavant persons to an unauthorised entry. |

Task B2: Describe methods of providing electronic protection and security controls for any **six** of the following:

* firewalls
* virtual networks
* secure connection/transfer protocols
* wireless connection security
* login and password protection
* access rights and permissions (including limiting data access)
* virus, malware and spyware protection
* secure remote access
* backup and restore systems
* monitoring systems (activity logging, access logs and audit logs).

|  |
| --- |
| Firewalls are both application level code and hardware orientated device (router) that manages access to a network. Network orientated firewalls are typically on a separate router device to prevent hackers from easily navigating to computers on a shared network. Each computer should have its own firewall built into it, which blocks unauthorised entry or exit of packet data from the computer. You can assign specific ports to specific reasons and track the usage of this. |
| It is important to encrypt the safe transfer of data across a network. This is achieved through using protocols to establish a secure connection. Internet access is a connection that needs to be secured especially in when shopping over the internet. This is done through SSL or Secure-Socket Layer, which encrypts data sent across a network so that the users information cannot be easily picked up on. |
| Wireless connections can provide encryption upon the data packets that are sent across. There have been a number of different encryption algorithms used in wireless connections including, WEP, WPA, with the latest consumer version being WPA2. WPA2 has 256 bit encryption, which provides a secured network from bruteforce attacks. Wireless networks need to have regular changed router passwords too as the default passwords for many routers are breakable. This interface is changeable within the router management console. |
| Login and password protection provides electronic protection for users on an account level. It is important that users generate a complex password and that it is regualry changed, every three months. Users need to look after their password and not advertise it to others. Having an account level password protection allows users to securely access a network infrastructure and protect data files on their computer. |
| Access rights allow users who login to be assigned a particular access level onto an Access Control List. The ACL manages what resources what the user can access including the software, peripherals, folders or files that they can use. The ACL is often used in addition to Windows UAC (User Account Control) to provide selected access to documents and software on a need by need bases. |
| Backups are an important form of electronic protection in IT security because regular backups provide a level of data redundancy in case files are lost. This is important both for working files and for customer data that need to be secured as part of the data protection act. Backing up data needs to be as automatic as a possible and data needs backed up in 3 locations. On the initial machine (such as a server), on a backup tape or drive stored in a data-safe on premises, and an offsite backup either in the cloud or in a secure location. Restoring a backup through following these three levels is usually a quick and simple process as you have the relevant data that you can access when necessary and run the restore process via restoration software either on windows or with the backup tapes. |

Task B3: Differentiate the following access control methods:

* mandatory
* discretionary
* role based.

|  |
| --- |
| Mandatory Access Control – Is an access control list setup by the system administrator, which provides users and folders/files certain levels of classification and categorisation. If both a user’s classification and categorisation matches the folders/files classification/categorisation then the user can access the file. If both forms of checks then the user will be blocked access. |
| Discretionary Access Control – Is the typical access control level setup by default on most desktops. This access control level gives the user complete control over their own system to determine the access level of their software and objects. This allows them to setup their own permission on folders and files, which other users will need the relevant access permissions to gain access to. Most administrators on the machine or domain can bypass this access control as they have full-control permissions typically. |
| Role based Access Control – Is the most business oriented and practical form of access control that assigns users to particular groups and then assigns access level permissions to the groups that the user belongs to. This recursively updates the users permissions, giving them only access to the role group that they are assigned. For example, the admin group could have access to everything, but a data entry clerk would only be able to access certain files and folders that pertain to their job role. |

Task B4: Describe the characteristics of strong passwords and the methods of attacking password protected systems relating to any **six** of the following:

* complexity
* length
* duration (mandatory changing)
* password history
* storing (electronic/non-electronic)
* dictionary attack
* brute force attack
* social engineering attack
* keyboard attack
* ‘man in the middle’ attack.

|  |
| --- |
| Passwords need to have a level of complexity to be determined a strong password. Complexity compresses of the different characters that are used when creating the password, the typical strong passwords needs to have the inclusion and combination of the following characters:   * Uppercase characters (A-Z) * Lowercase characters (a-z) * Numerical digits (0-9) * Non-alphanumeric characters (~!@#$%^&\*\_-+=`|\(){}[]:;"'<>,.?/) |
| Passwords need to be a certain length to be determined a strong password. Minimum recommended length of passwords are typically 8-15 characters, with no average upper limit, although no more than 20 is necessary to deter most brute force attacks. |
| Passwords need to be regularly changed to be determined a strong password. Typically often used passwords need to be changed every three months. This is to prevent passwords that are continually used from being picked up overtime from being regularly changed. |
| Dictionary Attacks are a form of attacking passwords to gain access to an account. Dictionary attacks utilise a dictionary or popular books/repositories of information to systematically try words or combination of words to “guess” the user password to gain access to their account. This process is typically automated by software as it is a long process. |
| Brute Force Attacks are a form of attacking passwords to gain access to an account. They try every possible combination of password possible on a character by character basis, eventually building up to full words and combination of words with numbers. A long and complex password is necessary to prevent brute force attacks as the longer and more complex it takes the more iterations it takes to compile an answer. For example, a bad password “bottle”, could be brute forced by the computer trying 26x26x26x26x26x26, combinations. |
| Man in the Middle Attacks are a form of listening to communication to gain access to a user’s password. When users communicate between each other, or a user to a server, then a man-in-the-middle could sit between the connections between two sources and simply rely the user’s connection to its destination. The user would think their connection is secure, but they are actually being monitored at the relay point. The man-in-the middle can then use any information that he user transmits (such as login details) to change the users account details. |

Task C1: Describe the following cryptographic algorithms:

* hashing
* symmetric
* asymmetric.

|  |
| --- |
|  |
|  |
|  |

Task C2: Describe how cryptography can be applied to ICT systems and data security in terms of:

* confidentiality
* integrity
* authentication
* non-repudiation
* access control.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

Task C3: Explain the operation of Public Key Infrastructure (PKI).

|  |
| --- |
|  |

Task C4: Explain the concepts of Key Management and Certificate lifecycles.

|  |
| --- |
|  |

This form can be handwritten or completed electronically.