8 **(a)** Describe what is meant by identity theft.

.....

.....

.....

.....

.....

..... [2]

(b) Describe the impact of identity theft on individuals.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
8(a)	**Two from:** • Unauthorised use of personal information • So that perpetrator can pretend to be another person/use their identity • Using the information (in an unauthorised manner) for personal gain • Using the information to cause harm/loss/disadvantage to victim • Combining valid identity data with false/fabricated data to create a new/synthetic identity.	**2**
8(b)	**Six from e.g.:** • Use of victim's identity when committing a crime/being questioned about a crime can bring innocent victim under suspicion/investigation/prosecution for these crimes • Difficult to prove innocence of crime when victim of ID theft/may have crimes/incidents recorded against name on police records/may be repeatedly accused of other crimes and suffer continued distress • Victim may be refused credit/finance/credit cards on basis of incorrect data stored by financial institutions (due to (fraudulent) use of ID by others) • Victims find it difficult to correct false information held by government/credit/security institutions • Victims can be left financially liable for fraudulent transactions/debts/purchases/taxes of others (who have stolen/used their ID) • Innocent individuals can be confused (in eyes of law enforcement/government agencies) with synthetic identities • Innocent victims may have false medical data added to their records when the identity thief uses their ID to gain access to medical services/insurance resulting in incorrect medical diagnosis/treatments • Victims can be left psychologically harmed/mental health issues (by theft of ID) • Adults may discover that they were victims of identify theft as a child/children's ID stolen and used before victim's adulthood so when child comes of age/reaches legal adulthood they have debts/financial harm/criminal records that are not theirs.	**6**

4 **(a)** Describe what is meant by a botnet.

.....

.....

.....

.....

.....

.....

.....

..... [3]

(b) Malicious botnets are used to attack systems and can be a threat to the security of stored data.

Explain how these botnets can be used to gain unauthorised access to data.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
4(a)	**Three from:** • Collection/group/number of internet-connected devices/smartphones • (One or more) bot/malware is running on each/every (connected) device • Security of (each/every) device has been taken over by third party • Controlled by third party/controller/bot herder via internet links • Use of digital signatures to ensure that bot herder is only one able to direct/control bot/botnet • Connection uses standard/usual internet protocols.	**3**
4(b)	**Six from:** *Setup:* • Device(s) has/have malware/bot installed without knowledge of owner/user • Bots set up as clients on devices • Bots can be set up as peer-to-peer with controller device • Bots connect together using internet communication systems/protocols • Bot herder/controller at remote location directs/sends commands to bots using a device as a server/Command and Control (C&C) • Use of Internet Relay Chat (IRC)/websites/telnet/domain/social media platforms to communicate with remote server • Bots can automatically scan their computing environment to discover ways of propagating themselves to other devices *Use:* • Bot herder/controller directs bot(s) to gather keystrokes to discover login credentials • Bots can execute/run other malware to access files/gather data and send back to controller • Botnets can carry out Denial-of-Serve (DoS) attacks on servers preventing legitimate use of files/data/services • Botnets can send (spam/unwanted/fraudulent) disguised emails from infected devices/zombie computing devices with attached data/files/request for login credentials/financial details • Botnets can distribute/direct spyware to gather user credentials/details/data and send to controller • Botnets use computing resources without knowledge/permission of user ('scrumping') and can compromise legitimate file/data storage.	**6**

9 Data that is transmitted on networks or stored on servers needs to be protected.

Analyse the use of software methods to protect data.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [7]

Question	Answer	Marks
9	***Analyse: examine in detail to show meaning, identify elements and the relationship between them.*** ***Seven from e.g.:*** • Use of regularly updated/up-to-date anti-malware/anti-virus/anti-spyware software to protect against malware… • … provides real-time monitoring/alerts to continually protect data/isolate/delete/remove infections/compromised files/data • Use of encryption to make data unintelligible/not understood by unauthorised users/viewers… • … prevents theft/misuse of personal/financial/confidential information • Encryption of hard disks/USB devices/removable storage so that if lost the content of data is unusable/inaccessible … • … requires user to remember the password else data is lost • Biometrics used to compare existing/stored unique ID data with newly presented ID data for authentication of user ID… • …allowing access only to authorised users to areas/devices/laptops/tablets/smartphones storing data • Use of access rights/permissions on files/folders to control user access with Access Control Lists/ACLs … • … which have allow/deny entries • Use of passwords on individual files… • … to control user access • … encrypt documents • …control editing rights to prevent unauthorised viewing/reading/alteration of content • Use of steganography/hide data within other data/text in JPEG images/MP3 files requiring the use of secret key/public/private key encryption … • … that unauthorised users are unaware of the data/cannot access the information in the data • Use of automatic backup schedules to ensure that (copies of) data is regularly stored elsewhere… • … can restored/retrieved if original lost/damaged. • Use of regular software updates/updates to applications/apps … • … ensure that security issues are addressed/corrected as soon as possible. ***Max 5 marks if bullets/list of points/characteristics.***	7

10 The security of data can be threatened by unauthorised destruction or modification.

(a) Explain these terms. Give an example of each.

(i) data destruction

.....

.....

.....

.....

.....

..... [2]

(ii) data modification

.....

.....

.....

.....

.....

..... [2]

(b) Describe ways that data can be protected from unauthorised destruction and modification.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [4]

Question	Answer	Marks
10(a)(i)	**One from:** • (data destruction) is the deleting/removing of data ***One** example:* • Valid example of e.g. deleting a record from a database.	**2**
10(a)(ii)	**One from:** • (data modification) is changing data to a different value • Changed value is stored in the same location as the original/overwriting the original value ***One** example:* • Valid example of e.g. change value in cell/cell ref of spreadsheet from e.g. 100 to 101.	**2**
10(b)	**Four from:** • Security measures to detect/prevent unauthorised access to network/network connections • Segmenting/zoning network sections/servers to prevent/reduce access by intruders • Use of firewalls to prevent unauthorised access/intrusion to networks/network storage • Use of VPN/secure connections to cloud storage systems • Use of authorisation/authentication techniques for gaining access to data • Regular/automatic check on data integrity with automatic alters/alarms/notifications (if data change is not authorised) • Use of (high-level/256-bit) encryption techniques to restrict access/understanding or data so amendment of data is more difficult.	**4**

10 Data stored on a network can be subject to different types of threats.

Explain how these threats can be detected.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
10	**Six** from: Use of anti-malware software/anti-virus/anti-spyware to scan incoming data/packets/requests to network Use of anti-malware software/anti-virus/anti-spyware to scan existing on/new files added to network Use of anti-malware software/anti-virus/anti-spyware software to examine signature data from previous/known threats and comparing it to organisation's data to identify (known) threats Use of firewall to filter packets and block packets identified as containing malicious code Use of proxy servers to hold/use anti-malware software/anti-virus/anti-spyware on requests/incoming data Analyse user actions/behaviour to establish normal/baseline for detection of abnormal/outlier action/behaviour/check what a user normally does/accesses to be able to compare with abnormal accesses by user/check user access times against expected times of access to data Set up traps for intruders that trigger alerts when intruder accesses certain data/'honey trap' files that are tempting to intruders and then set off alerts for administrators Hunt for threats by examining network traffic/monitor network/user activity to reveal patterns/abnormal activity Analyse network traffic patterns to detect abnormal patterns Gather/analyse user access logs/authentication attempts to discover threats Collect detailed information of malicious events/attacks to provide basis of investigations.	**6**

1 Data can be at risk of being lost from computer systems.

(a) Describe the ways that data can be lost from computer systems.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

(b) Backups are used to minimise the risk of data loss. Backup strategies are created for technicians to ensure that data can be recovered in the event of a disaster occurring.

Describe **three** instructions to the technicians that should be included in a backup strategy.

1 .....

.....

.....

2 .....

.....

.....

3 .....

.....

.....

[3]

Question	Answer	Marks
1(a)	**Five** from: Accidental deletion of files which are not backed up/have no other copies available Malware/viruses can automatically delete/damage/amend data Mechanical failure of storage systems/hard disks so that data cannot be retrieved Magnetic/electromagnetic failure/interference with hard disk surfaces leading to loss of sectors Power failure/loss/switch off during use of file/unsaved file resulting in corruption of data/data lost from memory buffers Theft of storage devices/computing devices resulting in physical loss of data/files Physical damage of computing devices by user/dropping/liquid spillage onto device prevents access to data Loss/damage to devices through natural disaster/fire/flood/water damage prevents access to data.	**5**
1(b)	**Three** from: Make copies/backups of the data regularly Automate the backup making process Save the copies/backups on different media Have a rolling backup strategy where media is reused at intervals Implement an incremental/differential/full backup system Keep accurate records of backups Store the copies/backups in remote locations/away from the originals/other backups/copies Test the restore process periodically.	**3**

7 Airports and railway stations provide public WiFi access to the internet for their passengers. Using public WiFi may put the passengers' information at risk.

Explain how passengers can try to protect their information from security issues when using public WiFi.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
7	**Eight** from: Log out of accounts/services when finished using them to stop others (following/observing) using the account Disable file-sharing to prevent unauthorised copying/access to folders/files Turn off WiFi/Bluetooth when not using it so prevent unauthorised use of connections/pairings Only use websites that use HTTPS to ensure encryption of data exchanges Use a (secure) virtual private network/VPN to ensure public connections are private/encrypted to prevent unauthorised users understanding the data/transmitted data Do not allow WiFi to auto-connect to networks/make device 'forget' connection after use to prevent devices making unwanted connections/connections to potential fraudulent/fake WAPs/devices Do not log into accounts via apps that hold sensitive information but use website of service and verify use of secure connection to prevent unauthorised collection/access to stored data Do not access websites that hold sensitive information/financial/healthcare accounts to prevent exchange of the data over open/unencrypted connections Do not log into WiFi/networks that are not password protected as these are usually unencrypted/may be fraudulent/fake/can be accessed by anyone.	**8**

12 The directors of a company are trying to protect the company's data.

Explain the measures that could be taken by the company to help protect the network from a data breach.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
12	**Eight** from: Use/create/enforce access control policy to dictate use of passwords/type of passwords/change of passwords by staff/employees Use access control to restrict access to the data Ensure that all software is kept up to date to minimise security risks/vulnerabilities Use standardised software/all computers use same software across departments to minimise vulnerabilities from unexpected/unapproved software Ensure that users cannot install unauthorised/non-standard software Ensure that networks are protected by firewalls to control/inward/outward data flow Segment networks to restrict access to sensitive data Use VPNs for remote access to data by authorised users Ensure that all employees/staff are properly trained in network/data security Ensure that all employees/staff are properly trained in identifying threats Ensure that all employees/staff are properly trained in how to respond to security issues/data breaches Use antivirus software to scan company data and any external storage systems e.g. USB memory sticks.	**8**

3 Ferdinand shops online using his credit card. Ferdinand has noticed that fraudulent transactions have appeared on his credit card statement.

Describe how it is possible for Ferdinand to be subjected to fraud when using his credit card for online shopping.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
3	**Six** from: Loss of (credit card) data of/associated with account/account number/details/ name of card holder/card number/expiration date/verification/card verification value, CVV code Merchant could use card details fraudulently Cardholder/Ferdinand is unaware of loss/does not report loss to the bank/card issuer 'Cardholder not present' transactions can be made using the details Unexpected repeat billing/merchant makes repeated charges to card Charges made to check account validity are not cancelled by merchant when full payment is made Directed to fake websites resulting in loss of data/description of pharming Fraud as a result/consequence of pharming Fake requests for personal data/description of phishing Fraud as a result/consequence of phishing Bank Identification number (BIN) attack/auto generation of range of similar/ sequential card numbers may allow charges to valid account numbers Ferdinand has used his credit card while connected to an unencrypted WiFi network, and it has been accessed by an unauthorised third party Physical theft of (credit) card occurs/has occurred Credit card details are stored by merchants and could be stolen, resulting in financial loss (to holder).	**6**

4 Evaluate, by weighing up the advantages and disadvantages, the use of encryption to protect confidential data.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
4	*Evaluate: Discuss the importance of, weigh up the advantages and disadvantages, judge the effectiveness, weigh up your opinions.* **Six** from: *Advantages:* Encryption requires an encryption key so that stolen data cannot be understood by unauthorised persons/without encryption key so it stops data breaches Data can be sent via unsecured media as the data is itself secure/data is secure so it does not matter how it is stored/transmitted Data remains confidential because it can only be read by the intended recipient (who has the key to opening the data) and not by e.g. system administrators/other users Data security is separate/independent from the security of the device on which it is stored so it is not necessary to secure the device *Disadvantages:* Administration of encryption keys is time consuming for user so it may not always be done/used/may prevent other task If the encryption key is lost, then the data associated with it is lost because the data is not understandable/is unrecoverable Can be expensive in terms of systems to maintain encryption because systems must have the capacity and capability for tasks so need more processing power Requires more time/processing to exchange data because of the encryption/ decryption process Can be difficult to maintain compatibility with all applications/programs in use by company/user so requires more maintenance/updates IT departments may find encryption too complex to manage/administer so require specialised staff/training (Symmetric) encryption requires sharing of keys which can be insecure so needs time/effort/processing to carry out Symmetric keys have to distributed/generated every time so needs more processing power/increases time to prepare data. *Max 5 if all advantages or disadvantages.* *Must be a proper evaluation to obtain full marks.* *Max 4 marks if bullets/list of points.*	**6**

8 Biometric payment systems can be used to pay for school meals. Students do not need to carry or use a payment card to buy goods but can use their fingerprints at the Point-of-Sale terminal.

(a) Describe **three** components of a biometric payment system that might be used.

.....

.....

.....

.....

.....

.....

..... [3]

(b) Describe how the biometric payment system is used by students to pay for meals.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
8(a)	**Three** from: Reader/scanning device to record the biometric factor being authenticated Software for converting the scanned biometric data into a standardised digital format Software for comparing the match points of the observed data with stored data Database to securely store biometric data for comparison Database to store student account data A payment system to transfer funds/debit account/credit school.	**3**

Question	Answer	Marks
8(b)	**Six** from: Student registers/is registered for a biometric program at the school by presenting valid identification Student scans (index) finger/iris/face/biometric parameter (using (school's) appropriate scanner/reader). The school's (finger) scanner/reader encrypts multiple point-to-point measurements of the fingerprint/iris/face/biometric parameter Student's biometric data and account information is stored in a (centralised) database. Student scans finger at the checkout with the school's electronic reader Software/reader compares the data from the new scan to the encrypted data in the database System locates the student in the database Checks that there is sufficient funds available Transaction approves/declined If approved, the funds are electronically transferred from the student's account to the merchant/school Receipt issued to student (if requested)/amount displayed on screen (to show cost)/indicates how much (money) has been spent/is left in account If declined, student is informed and notice printed/asked to retry.	**6**

11 It is sometimes possible for people to gain unauthorised access to computer rooms. A school has a computer room with a number of standalone computers.

Evaluate, by weighing up the advantages and disadvantages, methods for protecting data stored on these computers.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
11	*Evaluate: Discuss the importance of, weigh up the advantages and disadvantages, judge the effectiveness, weigh up your opinions.* **Six** from e.g.: *Advantages:* Use of passwords/PINs/login details/biometrics restricts access to computer system/folders/files Use of dongles/tokens/USB devices that must be attached/inserted to create one-time-passwords (OTP) prevent anyone other than carrier/owner from accessing data/device Tokens do not need network connection/OTP cannot be intercepted Physical barriers e.g. tethers on the equipment/locks on doors are cheap to install/use to impede intruders Use of security cameras/recording can cover wide area and provide deterrence/evidence of unauthorised entry Encryption protects contents of data from being understood but does not protect the data from being read/stolen/deleted Backup can restore stolen/deleted/damaged data but does not protect the original data from being damaged/deleted *Disadvantages:* Passwords can be forgotten, resulting in no access to system/data Sharing of passwords can result in unwanted access/loss/damage to system folders/files Tokens have limited number of uses for access Tokens cannot be used on other systems so have limited use/are effective in restricting access to other data/systems Keys can be pre-installed on tokens so manufacturers/supplier knows the keys Battery life of tokens can be limited Physical barriers e.g. tethers can be broken/removed/require constant attention/circumvented to be secure Security cameras must be watched all the time/watchers may be distracted. Must be at least one of each for full marks. 1 mark available for valid opinion/conclusion.	**6**

2 Companies are concerned that their employee files may be viewed and used by unauthorised people. A company uses access rights (permissions) to protect files stored on its network.

Explain how different access rights can be used to control access to files.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
2	**Six** *from:* Different access rights/permissions given to different individuals/groups of individuals Set up as Access Control Lists Works on files/folders/directories Permissions on folder/directory may be cascaded down to files contained within Files within a folder/directory do not (necessarily) have same permissions as parent folder If a permission/access right is not explicitly set, the right is denied Read permission allows only viewing of file/directory/folder Write permission allows modification of files/deletion/creation/renaming of files (within folder/directory) Execute permission allows file to run/executed Permissions must be set/mandatory if OS is able to run/execute file for user.	**6**

3 IT crime (cybercrime) is crime committed using computers and networks.

Explain how encryption can be used to combat IT crime.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
3	**Six** *from:* Encryption protects information by scrambling it using an algorithm with an encryption key to create data Data cannot be understood/decrypted without the key (Asymmetric encryption) uses public keys which can be accessed by anyone so no need to send key to specific user Private key is known only to recipient so no risk of key interception by unauthorised persons Protects data transferred over the internet between web browser and servers reducing possibility of financial data being stolen Secures email/text messages to prevent confidential data being read by unauthorised persons Protects cloud storage from outside attacks to prevent confidential data/information being read/used by unauthorised persons Prevents the loss/theft of data on USB and external drives Used in VPNs for secure data transfer across public networks Prevents use of stolen passwords to protect personal data from use in e.g. identity theft.	**6**

5 An online financial services company uses biometrics as part of its security measures to control access to its services.

(a) Describe how fingerprints would be used to allow access to these services.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) Evaluate, by weighing up the advantages and disadvantages, the suitability of biometrics in controlling access to company services.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
5(a)	**Four** *from:* Fingerprints are scanned into the system Image is converted into a binary pattern Binary pattern is stored on the system/in database Pattern is compared with existing fingerprint patterns in database If match found access is allowed If no match found error message/access denied/prompts for retry.	**4**

Question	Answer	Marks
5(b)	**Eight** *from:* *Advantages:* Biometric data is unique to/possessed only by one individual so is very secure Biometric data is difficult/impossible to forge so is more secure More than one characteristic can be used to increase accuracy Staff always have biometric data with them/no forgetting passwords/ID cards Staff cannot share biometric data to allow others access so more secure Costs e.g. paperwork/administrative work/password reset costs are reduced *Disadvantages:* Cost of/time taken for enrolment of staff can be high Biometric data can have a high false match rate leading to access by authorised persons Biometric data can have a high error rate leading to entry failures by staff/staff inconvenience/annoyance Authorised sharing of access using biometric data is difficult (unlike user IDs/passwords) Characteristics may alter over time so have to be retaken/staff re-enrolled at intervals Staff may object to having their biometric data stored/used Staff may be identified when they do not need to/should not be/e.g. facial recognition in a crowd/rest area. *Must have at least one of each for full marks.* *One mark is available for a reasoned opinion/conclusion.*	**8**

4 A company is concerned that their personnel files may be viewed and used by unauthorised people. The company uses access rights (permissions) to protect their files when they are stored on their network and encryption when the files are sent to other companies by email.

(a) Explain how the use of different access rights (permissions) applied to files can be used to control access to files.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

(b) Describe the advantages of the different encryption methods for protecting files when sending them over public telecommunications systems.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
4(a)	*Six from:* Different access rights/permissions can be given to different individuals/groups of individuals. Set up as Access Control Lists. Works on files/folders/directories. Permissions on folder/directory may be cascaded down to files contained within. Files within a folder/directory do not (necessarily) have same permissions as folder/director. If a permission/access right is not explicitly set, the right is denied. Read permission allows only viewing of file/directory/folder. Write permission allows modification of files/deletion/creation/renaming of files (within folder/directory). Execute permission allows file to run/executed. Permissions must be set/mandatory if OS is able to run/execute file for user.	**6**
4(b)	*Six from:* *Advantages of symmetric:* Symmetric uses keys/same keys for encryption and decryption so that must be shared to access the data so sharing of keys (also) has to be secured. Symmetric can be less secure because keys have to be shared/confidentiality of shared keys cannot be guaranteed. Can be very/more secure as (can) use (fixed-size) block encryption rather than encryption of bits/multiple rounds of encryption (which encrypts the encrypted block over and over). Keys have no special properties so are simple to generate. *Advantages of asymmetric:* Asymmetric uses public keys which can be accessed by anyone so no need to send key to specific user. Asymmetric uses a private/confidential key (known only to owner) so is (very) secure/data can be transferred without danger of public access. Key size is large/1024 to 2048 bits so security is high. Keys are reusable saving time/cost for owner.	**6**

9 Describe the security issues that may arise when computers are networked.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
9	*Six from e.g.:* Data can be lost/stolen by unauthorised users/hackers using gaining access to storage devices. Data can be stolen by interception of network traffic/capturing of IP packets. Valid user accounts can be abused/accidently cause data loss/damage. Malicious attacks with viruses/trojans/malware that damages/deletes/alters data. Misuse of resources by (unauthorised) persons/devices. Eavesdropping on other users' activities can enable theft of data/ID. Failure of hardware/software may expose data to loss/theft/damage. No need to have physical proximity to computer to access/can access systems remotely.	**6**

12 List **five** principles that should be included in a data protection act.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

Question	Answer	Marks
12	*Five from:* Key contents of a Data Protection Act include: 1 Personal data should be collected and processed fairly and lawfully. Data subject should be informed about the data being collected. Data subject should be asked for permission to collect it. 2 Personal data can be held only for specified and lawful purposes. Data subject should know why data is collected/stored. Law is broken if data is used for other purposes. 3 Personal data should be adequate, relevant and not excessive for the required purpose. Only data that is needed can be stored. 4 Personal data should be accurate and kept up-to-date. Wrong/inaccurate data must not be stored. Wrong/inaccurate data should be corrected. 5 Personal data should not be kept for longer than is necessary. Data must not be kept forever/unreasonable lengths of time/must be destroyed when no longer needed. 6 Data should be processed in accordance with the rights of the data subject. Data subjects can inspect the data held about them. Data subjects can insist that incorrect data is amended.	**5**

7 **(a)** Describe the **benefits** of using back-ups to prevent loss of data from computer systems.

.....

.....

.....

.....

.....

.....

.....

.....

..... [3]

(b) Describe the **drawbacks** of using back-ups to prevent loss of data from computer systems.

.....

.....

.....

.....

.....

.....

.....

.....

..... [3]

Question	Answer	Marks
7(a)	***Three** from:* Rapid access to (lost/removed) data/files Protection of data/files against power loss/failure of main system Protects against failure of storage system/hard disk Protects against loss of data from viruses/malware Protects against failure of OS.	**3**
7(b)	***Three** from:* Backups will store malware as well as safe data Backups will not remove malware Backups will restore data to time before malware infection but latest data will be lost Backups may not store up to date data if run during office/use hours Backups take snapshot of data which may change soon after backup is run so some data may not be backed up Backups can be stolen in their entirety If not encrypted all data can be stolen/accessed Backup windows should use system downtime which may be limited to out of hours' time System performance is reduced when backups are being carried out Restoration of data after malware infection can be laborious and time consuming Cost of extra hardware/storage may be excessive.	**3**

8 A bank stores details of customer accounts on its computer system. Customers and staff can access the accounts by logging in to the bank's website.

(a) Describe the security methods that could be used to ensure that the person logging in is authorised to do so.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
8(a)	**Six** *from:* Use of user ID with password/PIN known only to user Request random selection of three of the digits of password/PIN Transaction authentication number sent to customer/generated by code machine held by customer or by number on screen/sent to cell phone of customer … ... OTP/TAN is entered after user ID/password/PIN as next level of authentication … ... OTP/TAN checked against list issued to/held by customer Use of one-time password generated by a security token Multi-factor authentication using tokens/sequence of characters Use of security questions/memorable words plus example Use of biometrics such as fingerprint/retinal scan Query use of different devices to log in.	**6**

9 Evaluate the use of physical security in combatting IT crime.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
9	**Command word: Evaluate: discuss the importance of, weigh up, the advantages and disadvantages, judge the overall effectiveness, weigh up your opinions.** *This question to be marked as a Level of Response.* **Level 3 (7–8 marks)** Candidates will evaluate, giving advantages and disadvantages, of at least three ways in which physical security can be used in combatting IT crime. The information will be relevant, clear, organised and presented in a structured and coherent format. There will be a reasoned conclusion / opinion. Subject specific terminology will be used accurately and appropriately. **Level 2 (4–6 marks)** Candidates will explain giving advantages and disadvantages of at least two ways in which physical security can be used in combatting IT crime. For the most part, the information will be relevant and presented in a structured and coherent format. There may be a reasoned conclusion / opinion. Subject specific terminology will be used appropriately and for the most part correctly. **Level 1 (1–3 marks)** Candidates will give advantages / disadvantages of using physical security in combatting IT crime. Answers may be in the form of a list. There will be little or no use of specialist terms. **Level 0 (0 marks):** Response with no valid content. *Answers may make reference to e.g.:* Physical barriers such as wall / doors / bars / use of floors other than ground floor which are cheap and easy to make use of / make use of existing resources which lowers costs Use of CCTV which can be placed overtly to deter unauthorised persons just by their presence or by a warning / notice that watching is occurring / can be cost effective as a deterrent Video surveillance can be used to watch large areas with few staff Physical presence of guards / security staff shows persons that a security system is in operation ... can deal with issues quickly / immediately Security lighting / automatic lights / sensor-controlled lights can illuminate when persons present to act as deterrent / highlight intruders / warn intruders that they have been seen and these have low cost if e.g. solar powered Computer devices can be easily / cheaply / quickly fixed / attached to large objects / shelving to deter theft Physical locks require keys that may be lost / key fobs etc may be lost or stolen / given to unauthorised persons Combinations to locks can be forgotten	8

Question	Answer	Marks
9	Locks can be left unlocked in error Physical keys can be copied / given to unauthorised person Physical combinations to locks can be compromised by watching as lock is accessed Security staff / guards may not be alert / honest / in place when required.	

11 Evaluate the use of anti-virus software and anti-spyware in combatting IT crime.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
11	This question to be marked as a Level of Response. **Level 3 (7–8 marks)** Candidates will evaluate, giving both advantages and disadvantages, of the use of anti-virus software in combatting IT crime. The information will be relevant, clear, organised and presented in a structured and coherent format. There will be a reasoned conclusion / opinion. Subject specific terminology will be used accurately and appropriately. **Level 2 (4–6 marks)** Candidates will explain both advantages and disadvantages, of the use of anti-virus software in combatting IT crime. For the most part, the information will be relevant and presented in a structured and coherent format. There may be a reasoned conclusion / opinion. Subject specific terminology will be used appropriately and for the most part correctly. **Level 1 (1–3 marks)** Candidates will describe the use of anti-virus software in combatting IT crime Candidates will explain advantages / disadvantages of the use of anti-virus software in combatting IT crime Answers may be in the form of a list. There will be little or no use of specialist terms. **Level 0 (0 marks):** Response with no valid content. *Answers may make reference to e.g.:* **Advantages** Removes virus / malicious software that could delete / edit / destroy data Protect against spyware to prevent theft of confidential / personal information thus preventing unauthorised access to bank accounts leading to financial loss Can help / may protect against spam / phishing emails thus preventing the divulgence of confidential / personal information Protect against identity theft that may be a result of stolen confidential / personal information Protect against redirection of automatic payments ('stealware' or 'chargeware / affiliate fraud') to help prevent 'click fraud' Can help protect / stop unwanted / unauthorised use of computer for crypto-currency mining	8

Question	Answer	Marks
11	**Disadvantages** Anti-virus software must be kept up to date in order to combat the most recent viruses / malicious software Anti-virus software must be running all the time so places a performance 'overhead' on a computer system that may make the system slow / sluggish / unresponsive Anti-virus software will not detect all / every instance / type of malicious software so perpetrators can find ways around it ...infected websites use malicious code which is often not picked up by anti-virus software.	

12 Explain how perpetrator analysis could be used when planning for disaster recovery.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
12	**Six** *from:* Perpetrators are the attackers and include e.g. script kiddies, crackers, hackers, terrorists, business competitors, (foreign) governments who carry out the crimes / intrusions Each type of perpetrator has different skills / aims that can be identified by an analysis .. the higher the skill, the higher the risk of crime being perpetrated Analysis of their actions is carried out by the company / victim agents / representatives who design / implement the plan for disaster recovery Allocation of resources to disaster recovery from cyber threats depends on likelihood of perpetrators succeeding / wishing to / probability of attack on the company Analysis will define / determine the type of resource allocated e.g. firewalls / antivirus / antispyware software Intrusion detection systems can be deployed to combat the type of perpetrator identified by the analysis Resources can be targeted at the type of intruder / risk identified by the analysis of who / what is likely to be of concern.	**6**

13 Many countries have enacted laws to govern the use of personal data.

Analyse the need for data protection laws.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
13	**Eight** *from e.g.:* *Data protection laws are needed to address these concerns e.g.:* Personal data is stored on computer systems / in databases which may not be secure Databases are easily edited / searched / accessed (remotely) so data can be seen / manipulated Data can be easily / quickly cross-referenced / correlated by computer systems Computer systems can be networked so data can be accessed from many different locations / shared more easily between users Control over shared data is more difficult to maintain Accuracy of the information may be compromised / difficult to maintain when shared Data can be easily copied to other media / stolen without any trace of the action Data about individuals can be stored without their knowledge so infringing their privacy Keeping records of who / what / when data is accessed are difficult to maintain unless enforced by law.	**8**

3 Evaluate the use of quantum cryptography when transmitting confidential data over public networks.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
3	*Command word: Evaluate: discuss the importance of, weigh up, the advantages and disadvantages, judge the overall effectiveness, weigh up your opinions.* This question to be marked as a Level of Response. **Level 3 (7–8 marks)** Candidates will evaluate/explain in detail the benefits and drawbacks of the use of quantum cryptography when transmitting confidential data over public networks. The information will be relevant, clear, organised and presented in a structured and coherent format. There will be a reasoned conclusion/opinion. Subject specific terminology will be used accurately and appropriately. **Level 2 (4–6 marks)** Candidates will explain the benefits and drawbacks of the use of quantum cryptography when transmitting confidential data over public networks. For the most part, the information will be relevant and presented in a structured and coherent format. There may be a reasoned conclusion/opinion. Subject specific terminology will be used appropriately and for the most part correctly. **Level 1 (1–3 marks)** Candidates will describe a benefit and/or drawback of the use of quantum cryptography when transmitting confidential data over public networks. Answers may be in the form of a list. There will be little or no use of specialist terms. **Level 0 (0 marks):** Response with no valid content. *Answers may make reference to e.g.:* Allows use of cryptographic tasks that would be deemed impossible without the use of quantum cryptography, e.g. the guarantee that any interception/viewing/eavesdropping on/disturbance of the data is detected Calculations can be carried out extremely rapidly so much higher bi-length for keys can be used so increasing security of data when encrypted Does not do away with conventional cryptographic keys i.e. a mathematical algorithm is still needed for the actual encryption of the data Uses photons to carry data in terms of their 'spin' which is difficult to control/generate consistently/precise filters to determine the spin are difficult to manufacture/deploy Requires extremely pure fibres to transmit photons intact/undisturbed over anything but short distances – maximum so far is about 60 km/far shorter distance than conventional fibre use can reach Requires a new type/generation of computers to become a viable reality In theory, quantum techniques can break any encryption in a usefully short time.	8

7 Evaluate ways of combatting spyware.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

Question	Answer	Marks
7	*Command word: Evaluate: discuss the importance of, weigh up, the advantages and disadvantages, judge the overall effectiveness, weigh up your opinions.* **Eight** *from:* Use of anti-spyware software will prevent spyware being installed May not detect spyware already installed May not detect spyware disguised as legitimate feature of another program/application Use of antivirus software – will detect and remove some spyware but not all, so has limited effectiveness when used on its own Real time scanning of incoming programs/applications/data can provide protection by blocking spyware from entering the system provided the spyware is recognised/in its database/can be analysed to be spyware Dedicated anti-spyware can detect and remove spyware provided all areas of system are regularly scanned Lists of spyware must be up to date Options may include option to manually delete files if anti-spyware is 'uncertain' of status of detected file/data Spyware may resist attempts to be deleted/uninstalled… May recreate another running process to reinstall itself once deleted by anti-spyware software Using alternative web browsers may prevent spyware being installed as some are more vulnerable than others… Web browsers are not designed to detect spyware Using reputable sources for download of software may help prevent spyware being installed Reputable sources can be 'infected' Use of combination of methods is most successful but takes awareness and time to implement Using a firewall to prevent spyware from returning data to the spyware source *One mark is available for a valid reasoned opinion/conclusion.*	**8**

8 A research and development (R&D) department of a company develops expensive goods. The development process has to be kept secret. The biometrics of all staff of the company are to be measured and used to restrict entry via the doors to the department.

A comparison of the suitability of various biometric methods that are available for use to identify staff has been compiled and is shown in Fig. 6. Each aspect of the biometric method has been rated High (H), Medium (M) or Low (L).

Biometric method used to identify a member of staff	How universal amongst staff members?	How unique is the measurement amongst staff members?	How permanent is the measurement to staff members?	How easy to collect at door from staff?	How acceptable to staff?	How resistant is the method to circumvent by staff?	Performance rating of the biometric method
Face	H	L	M	H	H	L	L
Fingerprint	M	H	H	M	M	H	H
Hand shape/ geometry	M	M	M	H	M	M	M
Veins in hand	M	M	M	H	H	H	M
Iris	H	H	H	H	H	H	H
Retina	H	H	M	L	L	H	H
Voice of staff member	M	L	L	M	H	L	L
Facial thermogram of staff member	H	H	L	H	H	H	H
DNA of staff member	H	H	H	L	L	H	H

Key: H = High M = Medium L = Low

Fig. 6

Use the information in Fig. 6 to choose, with reasons, the biometric measurements that would be most suitable for measurement at the door.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[8]

Question	Answer	Marks
8	**Eight** *from:* Face, hand geometry, and iris fit this parameter are easy to read quickly/highly collectable at the door Face, hand geometry, iris can be collected by machine/ computer system/ have a M/H Fingerprint, facial thermogram, retina and iris have a M/H /highly unique to individuals.... ...but can be found in every individual Iris, retina, voice and facial thermogram are acceptable to staff both in original collection and use at the door... ...must not be intrusive/embarrassing when collected/read parameter/have a M/H Face, voice and DNA fit this parameter are difficult/not easy to circumvent to prevent copying/use by several individuals Fingerprint, retina, iris, DNA do not change over time/be permanent so readings are repeatable ...facial thermogram is not permanent Voice is most acceptable, but not very unique Facial thermogram is unique, acceptable and easily collectable, but changes over time so would need to be re-measured often Fingerprint, Iris, Retina are most unique, collectable and accepted.	**8**

1 Credit card accounts are often required for payment when buying goods online.

(a) Describe how the use of a credit card for online purchases may subject credit card account holders to fraud.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[8]

(b) Explain how a merchant selling goods online can attempt to combat credit card fraud.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[5]

Question	Answer	Marks
1(a)	**Eight** *from:* (Unauthorised persons obtain credit card details by various methods): skimming/interception of details/theft of details from website/phishing Use of number generator to create card numbers close to known good one Last four numbers are usually in a sequential range with same expiry date Use of generated card numbers to make transactions Even if customer not present/if card stolen transactions can still be carried out using security numbers Security number obtained by theft/phishing/selling/smishing by unscrupulous merchants Thieves/hacker use credit card for small transaction to see if valid Once small transaction is successful then much larger transactions are made Subscriptions to web services are a common method to test card validity as nothing physical is purchased Repeat billing/invoicing/recurring charges for card holder An uncancelled 'membership' is charged monthly Use of spyware/keylogger software to capture credit card numbers/details as they are typed.	**8**
1(b)	**Five** *from:* Demand for extra security information/PIN or card security code/last three numbers Check location of card holder matches address given for delivery by use of IP lookup of purchaser for geolocation Compare delivery address with credit card billing address Use of third-party services/escrow services to take payment from card account and pass it to merchant Not displaying the full card number (Primary Account Number – PAN truncation) on receipts/email/website confirmations Not storing the whole number/credit card details on computer systems Encrypt stored credit card details so that they are not understood by unauthorised persons.	**5**

6 Describe how quantum cryptography can help to ensure that data is kept secure when being transferred electronically between users.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[6]

Question	Answer	Marks
6	**Six** *from:* Use of polarised light for encoding data In quantum states for transmission between two parties Initial polarisation/oscillation of first two photons determines 0 and 1 bit of the data Polarisation of subsequent bits is determined at random Recipient measures data using random polarisation until data is as sent Used to establish a shared key between sender/recipients No third party learns/sees the key Key then used to create other keys for use in encryption Called quantum key distribution (QKD) Data state is changed when viewing by others Impossible to copy/eavesdrop on data encoded in quantum state without alerting the sender/recipients.	**6**

10 Evaluate the use of asymmetric-key and symmetric-key cryptography when encrypting data for electronic transmission between two people.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[8]

Question	Answer	Marks
10	This question to be marked as a Level of Response. **Level 3 (7–8 marks)** Candidates will evaluate in detail, giving both advantages and disadvantages of, the use of asymmetric and symmetric cryptography when encrypting data for electronic transmission between two persons. The information will be relevant, clear, organised and presented in a structured and coherent format. There will be a reasoned conclusion/opinion. Subject specific terminology will be used accurately and appropriately. **Level 2 (4–6 marks)** Candidates will explain the use, giving both an advantage and disadvantage, of asymmetric and symmetric cryptography when encrypting data for electronic transmission between two persons. For the most part, the information will be relevant and presented in a structured and coherent format. There may be a reasoned conclusion/opinion. Subject specific terminology will be used appropriately and for the most part correctly. **Level 1 (1–3 marks)** Candidates will describe, with a least one advantage/disadvantage of, the use of asymmetric and symmetric cryptography when encrypting data for electronic transmission between two persons. Answers may be in the form of a list. There will be little or no use of specialist terms. **Level 0 (0 marks):** Response with no valid content. ***Answers may make reference to e.g.:*** ***symmetric-key*** cryptography: *Advantages:* shares the same/related key with sender and receiver... ...process is relatively fast ...used on solid state drives to encrypt/decrypt data as it is written/read to/from disk. *Disadvantages:* ...keys must be kept secret from others ...sharing keys between sender/ recipient is a security issue ...if key is compromised both sender and recipient are at risk.	**8**

Question	Answer	Marks
10	***asymmetric key*** cryptography (public key) *Advantages:* uses different keys to encrypt and decrypt ...public key is known to all, but private key is known only to recipient ...only private key must be kept secret …anyone can use public key to encrypt ...only recipient can decrypt ...keys are not shared ...so is very secure ...if private key compromised, only senders data is at risk as any other data sent to others is encrypted with a different public key. *Disadvantages:* ...process is relatively slow... ...so not suitable for e.g. hard disk encryption on-the-fly.	

4 A new online supermarket will have a very large amount of data about its customers, products and services that has to be kept safe. Complete back-ups of all its data are to be created at regular intervals. Jaswinder, the IT manager, is considering the options of using tape-based systems, hard disk-based systems or back-ups to the 'cloud' for storing the back-ups.

Evaluate the three options for storing the back-ups.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>4</td><td>
<table>
<tr><th>Answers/Indicative content</th><th>Level of Response</th></tr>
<tr><td>
This question to be marked as a Level of Response.

Evaluation requires that advantages and disadvantages be discussed and weighed up in importance.

Answers may make reference to e.g.:

Tape-based:
established technology
∞ huge storage capacity
∞ serial access
∞ cheap per GByte
∞ can be slow to create backup
∞ can be slow to recover files
∞ tapes can be fragile
∞ tapes may not work in different tape drives.

Hard disk-based:
∞ quick to produce backup
∞ quick to recover files
∞ direct access
∞ cost per GByte varies/can be expensive
∞ large capacities
∞ hard disk can fail losing large amounts of data.

'Cloud'-based:
∞ off-site technology used so not so vulnerable to on-site disasters
∞ hardware/maintenance/service costs borne by supplier
∞ security arranged by supplier
∞ security of data issues
∞ unlimited capacity available
∞ reliable internet connection required
∞ high bandwidth connection preferred.
</td><td>
Level 3 (7–8 marks)

Candidates will evaluate in detail the options for creating backups.
The information will be relevant, clear, organised and presented in a structured and coherent format.
There will be a reasoned conclusion/opinion.
Subject specific terminology will be used accurately and appropriately.

Level 2 (4–6 marks)

Candidates will evaluate the options for creating backups.
For the most part, the information will be relevant and presented in a structured and coherent format.
There may be a reasoned conclusion/opinion.
Subject specific terminology will be used appropriately and for the most part correctly.

Level 1 (1–3 marks)

Candidates will describe the options for creating backups.
Answers may be in the form of a list.
There will be little or no use of specialist terms.

Level 0 (0 marks)

Response with no valid content.
</td></tr>
</table>
</td><td>8</td></tr>
</table>

8 A data protection act can contain principles that create rights for those people who have their data stored and processed by companies.

(a) Describe the rights that could be created by a data protection act.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) Data controllers are appointed by companies to safeguard the rights of individuals whose data is stored.

Describe **two** criminal offences that may be committed by data controllers if they fail to abide by the principles of a data protection act.

1 .....

.....

.....

2 .....

.....

..... [2]

Question	Answer	Marks
8(a)	***Four** from:* *(Derived from section 7, sixth principle of Act:* *'personal data shall be processed in accordance with the rights of data subjects under this Act':)* A right of access to a copy of the information held in their personal data ...told whether personal data is being processed ...given a description of personal data ...given reason(s) for processing ...given details of source of data A right to object to processing that is likely to cause/is causing damage/distress A right to prevent processing for direct marketing A right to object to decisions being taken by automated means A right (in certain circumstances) to have inaccurate personal data rectified, blocked, erased or destroyed A right to claim compensation for damages caused by a breach of the Act.	**4**
8(b)	***Two** from:* Failure to register when required ...and to keep personal data if not registered ...failure to provide accurate information/providing false information when registering Failure to comply with provisions/stick to reasons for storing data supplied when registering Processing data if not registered To fail to provide Data Commissioner with updated address failure to comply with enforcement order ...prohibition notice e.g. not to send data overseas/supply data to third party ...information notice e.g. supplying false information/not all of information when ordered to do so.	**2**

1 A bank has strategies in place to safeguard its information technology (IT) services. You have been asked to check and update the strategies that are designed to try and prevent IT disasters from happening, the strategy for disaster recovery management and the strict password policy.

(a) Describe how you would use risk analysis to check the strategy for disaster recovery management.

.....

.....

.....

.....

.....

.....

.....

.....

.....[4]

(b) The bank's strict password policy has rejected these two passwords:

abc
1234AAA

Explain why they have been rejected.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[6]

(c) Explain the precautions that you would take to try and prevent a disaster happening to the data used by the IT services.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[6]

Question	Answer	Marks
1(a)	***Four** from:* Qualitative risk analysis to prioritise risks for analysis Quantitative risk analysis ...of likelihood of occurrence/probabilities ...of consequences of occurrence To identify effect/cost of risks caused by e.g. ...loss of access to premises ...loss of data ...loss of it function ...loss of skills Produce a computer simulation of the disaster Produce a report of the risks.	**4**
1(b)	***Six** from:* The abc password is too short and does not meet minimum length requirements/number of character requirements Does not meet requirement for different types of characters Passwords must not be easily guessed and this is a simple pattern 1234AAA password has a sequence of characters/numbers ...has repeating characters Neither have a combination of upper/lower case/number/special characters.	**6**
1(c)	***Six** from:* Backups made and sent off-site at regular intervals Backups made on-site and automatically copied to off-site disk Backups made directly to off-site/remote/'cloud' servers Local mirrors of systems and/or data and use of disk protection technology such as RAID Surge protectors to minimize the effect of power surges on computer systems Using uninterruptible power supply (UPS) and/or backup generator to protect against a power failure Use of fire prevention/mitigation systems such as alarms and fire extinguishers Use of anti-virus software to protect data against corruption/loss/deletion Use of firewalls to prevent unauthorised/control access Use of physical security measures to control access by personnel Important passwords/codes should be held by more than one person/in secure conditions, but accessible in an emergency.	**6**

2024

7 Many companies have access control strategies to protect their data.

Explain how the use of an access control strategy can minimise the risks to computer data.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
7	**Six** from: • Access control ensures that users are who they say they are/confirms the identity of the user/authenticates the user • Ensures users have the appropriate access to data • Provides selective access to data/company controls who has access to what data • distribution of data is controlled/known • (Company) managers/staff/IT staff/users know who has/can have/is allowed access and who is not allowed access • Can be adapted (automatically) in response to changing conditions/change of staff (1st) – so that new employees can have access (1) – employees/staff who leave can no longer access data (1) • Can be adapted (automatically) in response to data breaches/analysis of risks (1st) – so that relevant employees/staff/users are isolated from the data (1) • Access control can be based on attribute of user within company (1st) – so that they can only access data appropriate for their job/task/role (1) – so that they can only access data depending on the location/time of access (1).	**6**

9 Botnets are software applications that are connected together over the internet.

Describe how botnets attack computer systems.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Question	Answer	Marks
9	**Six** from: • (Bot/malware/software application) installed on system without knowledge of owner/user • Bots set up as clients on system to communicate with controller device (on another device/peer-to-peer) • Use internet to communicate with remote server • Can execute/run other malware to access files/gather data and send back to controller • Can carry out Denial-of-Service (DoS) attacks on servers/preventing legitimate use of files/data/services • Can send (spam/unwanted/fraudulent) disguised emails from infected devices/zombie computing devices with attached data/files/request for login credentials/financial details which can be used to gain access to system • Can distribute/direct spyware to gather user credentials/details/data and send to controller • Can use system resources and reduce its performance • Can compromise legitimate file/data storage systems so that data/files are damaged/lost.	**6**