Unit 7 Assignment 1: Preparation Task

Task 1

Find the definition, explain and give an example of the following malicious threats to a system:

Term	Definition
Trojan Horse	A virus or piece of malware that is disguised as an innocuous program or website. Examples include DarkComet, Gh0st and MEMZ.
Virus Attacks	A malicious computer that causes damage or annoyance to a system. Recent examples include CryptoLocker, Tiny Banker and Petya.
Worms	A piece of virus or malware that can self-replicate and spread itself to multiple computers. Examples include NGRBot, Daqu and Stuxnet.
Phishing	Grazing personal information by creating legitimate looking websites and convincing users to enter their information into them. An example is text messages claiming to be from delivery companies, asking victims to pay a small fee for a redelivery attempt; This is to harvest their banking information.
ID theft	Stealing someone's personal information and using it for malicious purposes, such as applying for credit cards in their name.
Piggybacking	Gaining access to a network or site by 'piggybacking' on an authorised party, for example someone holding a door open or someone unintentionally being invited to a meeting. Gives third-parties access to company information.
Tunnels	A tunnel is a method of transferring data securely between networks. An example of this is a VPN that allows access to a company network when not physically on-site.
Hacking	Hacking refers to gaining unauthorised access to a computer system, network and etc.
Key Logging	Saving what is typed on a keyboard using a covert program. Data such as passwords and financial information can be captured and sent to malicious parties.
Magic Disk tactics	Used to boot into alternative operating systems and can be used to gain access to and subsequently modify important user/system data.
Man in the Middle Attacks	Performed by a malicious party eavesdropping communication. Often done on networks that have little or no encryption or security, such as open WLANs.

Task 2

Explain the following threats relating to E-Commerce:

- **Website Defacement**
  Is when a website or product receives a flood of negative, incorrect reviews which lowers its reputation. Can also be performed by gaining access to the underlying website and modifying it to contain defamatory, inflammatory or derogatory information.
- **Control of Access to Data- how have eBay resolved this?**
  eBay have resolved the issue of third-party sellers requiring payment information by taking payments themselves and then passing on the monies to the seller themselves.
- **Denial of Service Attack**
  A "Volumetric" DDOS attack when a service is flooded with network traffic that overwhelms the network or web server, rendering the site usable or slow.
  Alternatively, a Protocol or Application Attack means that the application server or network itself is targeted. If either are taken down, access to the service is lost.
- **Counterfeit Goods**
  This refers primarily to piracy where paid software or games are obtained without the permission of the copyright holder. It can also refer to purchasing a product from an E-Commerce website and receiving an illegitimate or aftermarket version.

Task 3

If some of the above, in Task 1 and 2, occurred, what could be the organisational damage?

- Company information such as trade secrets could be leaked, payroll and employee information and other important documents could be irrecoverably lost.
- The company's reputation could be irreparably damaged and the public's trust in the company severely eroded.
- Both of these have the potential to cost the organisation a large amount of money, potentially taking them out of business entirely.

Unit 7, Assignment 1, Tasks 2–6 — Security Trade Show

Thomas Robinson

SOLIHULL COLLEGE

Task Two – Physical Security Measures (P2)

Locks

Door Locks

To prevent unauthorized access, locks can be fitted to doors. Traditional solutions employ physical keys or PINs whereas modern solutions make use of biometrics, cards and passes. A benefit of using standard key locks is that most everyone will be aware of how they work, and there is no need for additional training or guidance.

Biometrics

Rather than using physical keys or passes to unlock doors, it is possible to use biometric data of individuals instead. This can include iris scans, fingerprint scans and voice recognition. The benefit to using biometric access control is that no one can lose or give away a device, prohibiting their access or giving access to a rouge party.

Device Locks

Devices such as computers, monitors, etc. can often be secured in place with a Kensington Lock. This is a way to deter theft of equipment, however they are inconvenient when used with portable devices, such as laptops since they will need to be constantly locked and unlocked.

Visitor Passes

Visitor passes allow guests and visitors into an area that are usually reserved for employees or authorized people only. A visitor pass may not allow access into all areas of a building or may require the visitor to be accompanied when roaming. This requires more trained staff, however, ensures visitors do not perform activities or access areas they are not supposed to.

Sign in/out Systems

To control access to a site, one is required to know who is present at what time. This is especially important when it comes to visitors. A method of doing this is to have them sign in and out at reception so their presence and purpose is known. A downside of this system is the necessity of a log of visitors be kept. This would need to be stored securely.

Security Guards & CCTV

Employing security guards to check ID on entry can help unauthorized parties from gaining access.

CCTV systems allow suspicious behavior to be monitored remotely and can provide evidence of theft or malpractice if recorded. A downside of this method is the significant cost – installing the system and potentially employing someone to monitor the cameras throughout the day.

Cable Shielding

Cable shielding refers to the process of reducing electromagnetic interference with data travelling along a wire. This has the benefit of increasing the potential data throughput of the cable—as well as data integrity—although the security benefit of this is preventing a third party from wiretapping. If a cable is poorly shielding and is transferring an unencrypted signal, it may be possible to decode the data being transferred. This is more relevant to analogue communication cables, such as those used for telephones. A downside of this method is making cables thicker and harder to route.

Task Three – Software & Network Security (P3)

Encryption

Encryption is scrambling data such that it is unreadable by one without the decryption key. This protects information by ensuring it can only be read by the recipients it is intended for. If a computer's storage medium is encrypted, then the data will be irrecoverable even if stolen.

Handshaking

A handshake is the process of verifying the authenticity of the sending/receiving party. This makes sure that the information is being is not being sent to a malicious party.

Diskless Networks

A diskless network is one where end-user computers are forbidden from accessing portable external storage mediums, such as USB flash drives or optical media like CDs and DVDs. This means that company data cannot be stolen without being monitored.

Data Backup

Backing up data means creating a copy of it to protect against hardware failure, software failure, a malicious attack, or a careless employee. If a regular backup is kept, then data is shielded from drive failures, ransomware, or accidental deletions.

Password Changing

This process is advised against by the National Cyber Security Centre, since it is extremely likely that when forced to change passwords on a regular basis, users will create a system whereby each password is simply a modification of the previous one, thus negating any security benefit. It is also extremely likely that users will choose weaker passwords that are easier to remember since they know they will have to change it again.

Network Access Levels

Configuring ACLs (Access Control Lists) for networks and files allows users to only access what they are required to. This ensures that, for example, a rouge employee could not modify another person's data or access data they do not need access to. Use of VLANs also allows access control by segregating networks that do not need to communicate, such as security systems, guest wireless access, and employee PCs.

IDS & IPS

Intrusion Detection Systems are designed to detect potentially malicious traffic and alert the appropriate administrator who can take appropriate action. These help secure a network by deciding the threat level of inbound and outbound packets and flagging potential threats.

Intrusion Prevention Systems are similar; however, they carry out actions such as firewall reconfiguration, IP blocking and geo-blocking automatically.

Task Four – Information Security Discussion Notes (M1)

Confidential Data & the Data Protection Act (2018)

- Companies storing personally identifiable information must register with the Information Commissioner's Office, whom they must also report any mishandling to.

Data Protection Act Principles

They ensure that data is:

- used fairly, lawfully, and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant, and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

There is stronger protection for sensitive, protected information:
Race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics (where used for identification), health, sex life or orientation.

Access to Data & the Freedom of Information Act

The Data Protection act gives people the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

These cover all companies.

The Freedom of Information Act only covers public bodies, such as local authorities and governmental departments. It is designed to allow anyone to request information that has been recorded by these organisations.

Data Integrity

- **What is it?**
  Data integrity is how complete, accurate, and consistent data is. Things that compromise data integrity include computer malfunctions corrupting data, errors during file transfers, accidental modification or deletion of data and malicious means such as viruses.

- **Why is it important?**
  Ensures data complies with GDPR and other legislation relating to accuracy and completeness of data

Data Completeness

- **What is it?**
  Data completeness is ensuring how comprehensive a set of data is and whether it includes all the information that is required or not.

- **Why is it important?**
  Missing data can lead to incorrect reports, inability to contact people and other anomalies. As an example, a users' first and last name may be required information, whereas a middle name may be optional. This would mean the data is wholly complete even if some users are missing middle names.

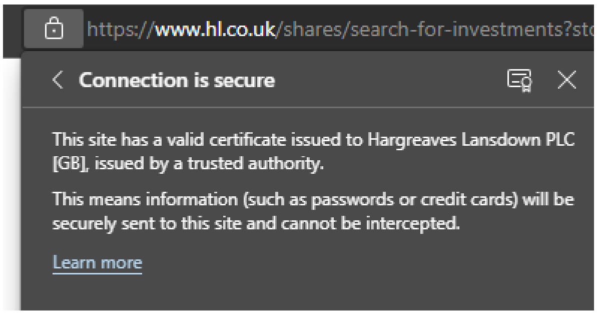
Task Five – Encryption Techniques & Usage (M2)

What is Encryption?

Encryption is the process of scrambling a message to make it harder or near impossible to decipher without the appropriate description key or cipher.

Use of Encryption

- Every webpage that uses SSL (shown as https and a padlock in browsers) makes us of encryption. This ensures that data transmitted cannot be read, intercepted, or modified while it is in transit. This allows sensitive information such as passwords, banking information and medical information to be kept secure.



https://www.hl.co.uk/shares/search-for-investments?st

Connection is secure

This site has a valid certificate issued to Hargreaves Lansdown PLC [GB], issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Learn more

- Many messaging apps such as Telegram, WhatsApp, iMessage and more make use of end-to-end encryption which ensures that messages can only be read by the intended recipients(s). This increases user privacy and enables secure communication between journalists and whistle-blowers as well as contact with human rights activists in draconian countries.
- Confidential information such as medical records, financial information and governmental data can be held and transmitted securely.

Disadvantages

- On slower devices, many forms of encryption can be very taxing on CPU resources. This makes it unfeasible to use.
- As newer, safer encryption methods start being used older devices may not support them. This is especially true for old versions of web browsers on older operating systems.
- Encryption is only as safe as the decryption key; people can still be compelled to hand over access to encrypted content.
- Some encryption methods

Methods of Encryption

Caesar Cipher

The Caesar Cipher is a weak method of encryption. Each letter or character in a string is shifted a specified number of places along.

With shift 4, the alphabet would look like this:

a b c d e f g h I j k l m n o p q r s t u v w x y z

e f g h I j k l m n o p q r s t u v w x y z a b c d

The message *"this is a test of encryption"* would become *"xlmw mw e xiwx sj irgvctxmsr".*

Decoding a message without the shift number simply involves trial-and-error; trying each of the twenty-six different combinations a recognisable sentence or word is formed. This means it is not secure, since brute-forcing the solution is trivial, even for a novice.

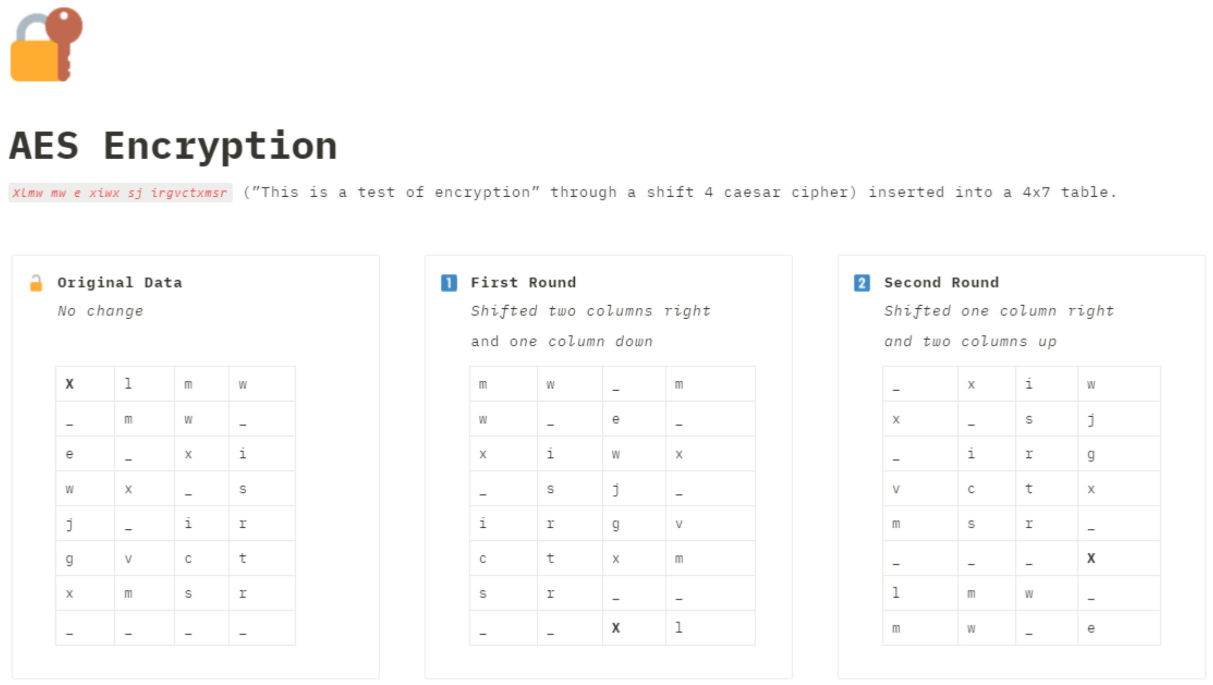
The message *"lipps, asvph"* uses shift 7 and is decoded to *"hello, world".* Below is the shift 7 cipher.

a b c d e f g h I j k l m n o p q r s t u v w x y z

t u v w x y z a b c d e f g h I j k l m n o p q r s

AES

AES—Advanced Encryption System—is a more recent invention that is still used today. It works by shifting data around in columns and rows many, many times. The key for a piece of AES encrypted data is the instructions used to shuffle the data.



AES Encryption

Xlmw mw e xiwx sj irgvctxmsr ("This is a test of encryption" through a shift 4 caesar cipher) inserted into a 4x7 table.

🔓 **Original Data**

No change

X	l	m	w
_	m	w	_
e	_	x	i
w	x	_	s
j	_	i	r
g	v	c	t
x	m	s	r
_	_	_	_

1 **First Round**

Shifted two columns right

and one column down

m	w	_	m
w	_	e	_
x	i	w	x
_	s	j	_
i	r	g	v
c	t	x	m
s	r	_	_
_	_	**X**	l

2 **Second Round**

Shifted one column right

and two columns up

_	x	i	w
x	_	s	j
_	i	r	g
v	c	t	x
m	s	r	_
_	_	_	**X**
l	m	w	_
m	w	_	e

Each "round," the data is shuffled in a different way. In a real implementation, this would be completed hundreds of thousands of times. The instructions for how the data is shuffled can be followed in reverse to decrypt the data.

Task Six – Disaster Recovery (D1)

Reasons for Data Loss & Recovering from Them

Data can be lost in many ways, ranging from accidental to malicious.

- **Natural disasters**, such as storms, tornados, earthquakes, and tsunamis can destroy office spaces and the equipment within them. It is not possible to completely protect against them physically, though the use of off-site backups can protect important data. Dark-sites and mirrored offices can allow a workforce to get back up to speed in a new location at pace.
- **Accidental deletion or modification** of files can be overcome through the use of document version control and recycle bins.
- **Malicious attacks** such as malware or ransomware irrecoverably modifying or removing data can be overcome using segregated backup options.
- **Hardware failure** of data storage devices can cause loss of data. This can be mitigated through the use of replicated storage solutions as well as backups.

Backups

Regular scheduled backups are essential to the smooth operation of an organisation. There are many methods of backing up data and locations in which the data can be backed up.

Locations

- **On-Site**
  Backups taken on-site are the quickest to perform and will offer protection against hardware failure and file deletion.

  External hard disk drives and data cassette tape are common ways of taking backups on-premises. External hard drives are quicker and more easily accessible; however, they are fragile and could be damaged easily. Data cassettes are slower and more expensive, though they can store significantly more data and are more robust for data archival.

- **Off-Site**
  Backups taken off-site are protected against damage caused by a natural disaster or a rouge employee.

Companies such as Backblaze offer cloud-based backup solutions where data is stored securely in the cloud. This provides incredible peace-of-mind; however, the uploading of data can be extremely slow depending on the speed of the connection and cloud services are often pricey. Additionally, the restoration of data can take a significant amount of time, with many providers simply emailing hard disk drives to restore your data from.

- **Mirroring & Redundancy**
  A mirror is an exact copy of a set of data or a device that can provide redundancy in the event of hardware failure.

  Redundancy within servers is common – hard disk arrays can be placed in RAID configurations, which stripes and mirrors data across a group of disks, allowing some to fail with no data loss. Many servers also have dual power supplies, allowing multiple power sources to be provided.

  A fully mirrored server solution would be having two identical servers that are identical in specification and configuration. The data from the primary server would be immediately copied to the secondary server as soon as possible. This allows the primary server to fail without any loss of productivity, since work can be moved onto the secondary server whilst the primary is being fixed.

  Mirroring entire servers is costly and often unnecessary for most companies since it requires twice the hardware to be procured. However, for businesses who cannot afford any downtime (such as financial institutions), cost is likely to be overlooked.

Frequency

Backups should ideally be taken as often as data is changed. It is common for workplaces to take regular daily on-site backups and then push data to an off-site provider on a less regular basis. This provides an adequate compromise between security and convenience.

Preventative Measures

- **Training staff** to manage files correctly and reliably can help prevent accidental deletions and modifications. Training staff how to make use of version control systems (that are built into many programs and operating systems) can also speed up the recovery of data that may have been considered lost.

- A **Disaster recovery plan** should be written that outlines how data is stored and what has been put in place in the event of significant data loss. This will provide confidence and clarity in the event that something does go wrong.
- **Maintenance of hardware** during regular time windows can mitigate disruption. Replacing devices that are nearing end-of-life, such as hard drives, can prevent them from failing during use causing downtime.
- The provision of a **mirrored office** can afford protection against physical damage caused by natural disasters or otherwise. This is an office facility that employees can be temporarily moved to if anything happens. The company may manage this in-house or make use of dedicated third-party providers.
- **Logging** of file creation, modification and deletion can provide accountability for any major issues which can foster learning opportunities. Additionally, the correct **documentation** of problems and previous data recovery events and how they were overcome can provide important insight and knowledge to IT.

Whole System Replacement

A whole system replacement is necessary if all possible recovery solutions have failed and involves the replacement and reconfiguration of an entire system or solution. This incurs and significant cost: both monetary and in lost productivity.

Data Recovery Tiers

Zero

Tier 0 refers to having no system in place for data recovery in the event of a disaster.

One

Tier 1 refers to the most traditional solution. Local backups are taken on a regular, scheduled basis which are then replicated to an off-site location.

Two

Tier 2 implementations have a failover hot site that can be switched to in the event of the primary solution failing.

Three

Tier 3 adds constant replication of mission-critical data to an off-site provider.

Four

At Tier 4, point-in-time copies are kept on faster storage devices, which allows data to be covered from a specified time at greater speed.

Five

Tier 5 introduces transaction integrity to file modification and backups.

Six

Tier 6 additionally requires all data to be replicated to an off-site location as it is modified.

Seven

Tier 7 is the implementation of all previous tiers but with integrated, automated solutions that require no human-input to recover from most disasters.

Recommendation

The recommendation given to a business will depend wholly on how the importance of the data they are creating and the amount of downtime that can be tolerated. A financial services company, for example, should have sophisticated solutions that replicate data off-site as it is created, with hot sites for employees ready in the event of a physical disaster.