Cyber Security

Unit R012 - Understanding tools, techniques, methods and processes for technological solutions

Introduction

- When a cyber security attack happens, there are certain vulnerabilities that can be exploited, these include:
  - **Environmental**
  - **Physical**
  - **System**

- Some organisations run **vulnerability testing** when a computer system is being created.

- The **vulnerability** that can affect computer devices and systems the most, however, is the **behaviour** of the **users** of the computer system.

Environmental

- With the increase in the use of mobile computer devices and the cloud, there are vulnerabilities that can affect data.

- E.g. if an **earthquake** occurred, it is probable that internet access would be lost. This would make the cloud inaccessible.

Environmental

- It is possible that computer devices could be destroyed during **tsunamis, earthquakes, floods**, etc. if buildings are destroyed, so would the computer systems, infrastructure and internet.

- If the **government stores data about a location**, including the number of people in remote villages (Census), rescuers may not know who or how many people they are looking for.

Environmental

- Even if you have **physical backups** were available on physical storage media such as flash drives, there is a chance that these would also be affected by the same natural disaster.

- If the backup was stored in the **cloud**, these would be inaccessible if there was **no internet access**.

Environmental

- One of the after-affects of a natural disaster may be **power failure**.
- One way to keep systems operating is by using **batteries or a power generator.**
- Another natural disaster is a **lightning strike** which can cause a surge or spike in the electricity supply.
- These surges can affect how hard drives and other storage devices operate.

Physical

- Some vulnerabilities relate to the **physical devices** that can be used to store and process data.
- Physical vulnerabilities can also be lead to the **theft of identity**.
- The most common vulnerability relating to computer devices and portable storage is **theft**.
- Another example could be that an authorised user may leave their belongings on a train and somebody else may pick it up.

System

- Some vulnerabilities relate to the running of the devices and the **computer system**.
- One vulnerability relates to the use of **weak passwords**.
- User IDs and passwords are provided by businesses to their computer users, but passwords can be changed by the user.
- A weak password is one that is easy to find or guess, the simpler the password, the easier it is to guess.

System

- It is important that **software is updated**.
- Most software vendors issue **updates** for their software following its release.
- These updates are called "**patches**". Patches attempt to resolve potential vulnerabilities that may have been identified by vendors or users.
- Many operating systems have the facility to **update automatically**, this happens as the computer system is going through the shutdown process.

System – Security Software Updates

- Security software will also **update automatically** and will constantly be checking for new updates.
- It means that any **vulnerabilities** are **identified** and solved **before** a cyber-security **attack** can take place.
- **Manually updating** operating systems and security software can be **dangerous** to the computer **system** and the **data** held on it.

System – Manually Updating Software Problems

- One problem is the **time taken to download** the patch. Some software will only update certain files, where some will send a new copy of the entire software package.
- Another problem is there may be a **delay** between the **patch** being **released** and the time taken for the vendor to **update** the software.
- Another problem with **manually scheduling updates** is that the computer system must be **switched on** and connected to the **internet**.
- If the patch has been scheduled for when the computer is turned off. This can leave the computer system open to attacks and threats.

System – Insecure Hardware

- **Insecure hardware** can also cause system **vulnerabilities**.
- **Wireless** internet **connections** are increasingly popular in both homes and offices.
- In different shops for example, they may offer Wi-Fi to their customers. Some of these **connections** are **unsecure**, meaning a user ID or password is not needed to join.

System – Insecure Hardware

- **Unsecured modems**, **hubs** and **routers** can mean that the internet access or the computer devices connected to the Wi-Fi are **vulnerable** to a cyber-security **attack**.

- This vulnerability can make a cyber-security **attack** easier to **carry out**.

Vulnerabilities

Type of Vulnerability	What is it?
Environmental	Vulnerabilities can occur when there is a natural disaster or environmental event. Due to the damage caused by a disaster, such as an earthquake, it is easier for a cyber-security attack to take place.
Physical	Vulnerabilities can occur due to physical devices being stolen or misplaced. When they fall into the wrong hands, the data can be used for a cyber-security attack.
System	Bugs are usuaully the result of human error when coding the software. They can usually be fixed by the creator issuing a fix or a patch. They can allow attackers to bypass security, override privledges or steal data.

Problems with manually updating

Problem #	Why is it a problem?
1	It takes a long time to manually update software – this is a problem because it means other day to day tasks cannot be completed as somebody is working on the updates
2	Another problem is there may be a delay between the patch being released and the time taken for the vendor to update the software. This is a problem because during the delay, the software is vulnerable to a cyber-security attack.
3	Another problem with manually scheduling updates is that the computer system must be switched on and connected to the internet. This is a problem because the update may be scheduled for when the computer is switched off and therefore will not update, leaving the system vulnerable to a cyber-security attack.

Impacts And Consequences Of A Cyber-security Attack

- If a cyber security **attack** takes **place** and is **successful**, this can have an **impact** on businesses and individuals.

- Sometimes a successful attack on a business can have an impact on both the businesses and its **customers**.

Denial of Service Attack - IMPACT

- A **denial of service** attack is when an attacker **blocks access** to a website for authorised users.

- **Authorised users** cannot access the website whilst it is under attack.

- E.g. if a bank was a victim of a DoS attack – users would not be able to access their bank accounts online, pay bills, transfer money or complete any other banking transaction.

Identify Theft - IMPACT

- **Identity theft** is one result of a cyber-security attack.
- **Identity theft** is when **personal details** are used to commit **fraud**, for example taking out a **loan** in someone else's name.
- If a person's **identity** is **stolen** then this could result in, for example, **big debts** being run up in their name or passports being issued and possibly used for **criminal activity**.

Impacts of a cyber-security attack

Type	Impact
Denial of Service Attack	During an attack, authorised users cannot access their data/website – this can have an impact as it slows down business and can affect customers trust
Identity Theft	The impact of identity theft is that a cyber-criminal can steal somebody's personal information and take out loans or credit cards in their name and rack up large bills.

IMPACT to Data

- During a cyber security attack, data could be destroyed, manipulated, modified or stolen.

- **Data Destruction** - data is destroyed by a cyber-security attacker and no longer exists.

- **Data Manipulation** - when data is edited, usually to meet the needs of cyber-security attackers. For example, the attackers could change the data in a news feed on Twitter or Facebook.

IMPACT to Data

- During a cyber security attack, data could be destroyed, manipulated, modified or stolen.

- **Data Modification** - changes data to meet the needs of the attacker, for example, changing the amount of money in a bank account. The attacker can then withdraw the increased amount of money, causing the bank to lose money.

- **Data Theft** - Data theft is when cyber-security attackers steal computer-based data from a person or business, with the intent of compromising privacy or obtaining confidential data. Data that can be stolen include passwords. Data theft can also be committed by stealing portable storage devices.

IMPACT to Data

Impact to Data	What happens to data?
Data Destruction	Data is destroyed by a cyber-security attacker and no longer exists.
Data Manipulation	When data is edited, usually to meet the needs of cyber-security attackers.
Data Modification	Changes data to meet the needs of the attacker, for example, changing the amount of money in a bank account.
Data Theft	Data theft is when cyber-security attackers steal computer-based data from a person or business, with the intent of compromising privacy or obtaining confidential data.

Consequences of a cyber-security attack

- Any cyber-security attack can have **consequences**, which can be related to **loss**, **disruption** or **safety**.

- Each of these can in turn have consequences on different areas.

Loss

- Many cyber-security attacks result in data and information being stolen or corrupted so it can no longer be used.
- If there is a **backup** then it is possible to **restore** the data and information, but most businesses back up only once a day.
- This means that at least one day's data and information will have been lost or corrupted.
- There are three main consequences resulting from the loss of data: **financial, data and reputation**.

Financial - Loss

- When data and information is **lost** or **corrupted**, a business can suffer **financially**.
- For example, accounts records may be lost and it is also possible that invoices **created on the day** of the attack may be **lost** or **corrupted**.
- This would mean that **records** of who **owes** the business **money** needs to be **recreated**.
- It is possible that all the data/invoices can not be recreated resulting in a **loss of income**.

Financial - Loss

- If personal data is targeted during a cyber-security attack then the company may have to pay **compensation** to repay the individuals.
- Another cost is that companies may have to **increase their security** so it doesn't happen again.
- This is **expensive** as the cost of installation, maintenance, hardware and software will need covering.
- If there is a cyber-security attack – **customers** may **lose trust** in the company and take their business elsewhere, which will make the company lose income.

Data - Loss

- The **timing** of **backups** can lead to **data loss**.
- Account data can be lost, as well as supplier and consumer data which can have **financial consequences**.
- There is a **time delay before** the most recent **backup** can be used.
- With many **transactions** happening **online**, e.g. e-commerce, **customer orders** may be **lost**. The loss of data can have consequences for customers as their orders or personal information may be lost.

Reputation - Loss

- If a business has been the target of a cyber-security attack and data has been lost, then its **reputation** will be **negatively affected**.
- It is very likely that the business will **no longer** be seen as **trustworthy** by its customers.
- This could result in **customers moving** their **custom** to a different business, which could lead to the business stopping trading.

Disruption

- A cyber-security attack will always cause some level of disruption, both when the attack is taking place and after it has happened.

- There are three main consequences resulting from the disruption caused by a cyber-security attack:
  - **Operational**
  - **Financial**
  - **Commercial**

Operational Disruption

- Cyber-security **attack** can **result** in **lost** or **corrupt data**.
- The business may have **backups**, but the **time** taken to **reinstall** the data can have an impact on its operations.
- A business **relies** on data to carry out its **day-to-day functions**, both internally and in the **interaction** between it and its **suppliers/customers**.

Financial Disruption

- A cyber-security attack can impact negatively on a business's finances.

- The financial consequences of a cyber-security attack can include:
  - **Loss of customers, leading to a loss of revenue**
  - **Possible payment of compensation**
  - **Increased costs to improve security and computer devices, including installation and maintenance**
  - **Loss of revenue, for example, if invoices are lost**

Commercial Disruption

- The commercial consequence of the cyber-security attack would depend on the **function** of the **business**.
- It would be **devastating** if a **nuclear power plant** were a victim of an **attack**.
- It would affect **day-to-day** business but could also have **safety consequences**.
- It would be **less catastrophic**, but **no** less **serious**, if a supermarket chain were the victim of an attack.
- Although **customer details** could be **stolen**, a **supermarket** would still be able to function with **limited** commercial **consequences**.

Safety

- A cyber-security attack can have **serious effects** on various aspects of **safety**.
- However, the systems that are linked with safety are very **well protected** against cyber-security **attacks**, with logical and physical protection measures.
- The safety of **individuals**, **equipment** and **finance** is at risk if targeted by a cyber-security attack.

Individual Safety

- A targeted cyber-security **attack** on a government **website** and the data held could have an **impact** on **national security**.
- E.g. **prisoners** could be **released early** if there was an **attack** on the **prison** service.
- The loss or **corruption** of personal **data** could result in personal **details** becoming **known** to the **attackers**.
- This could lead to **identity theft**.

Equipment Safety

- During a cyber-security attack, equipment such as computer devices, including internet access devices could be targeted.
- This could take the form of a **Distributed Denial of Service (DDoS).**
- If computer **devices** are **targeted**, businesses or individuals may **not** be able to **carry out tasks**.
- E.g. if an individuals hub has been targeted, they will not be able to carry out tasks such as online banking or shopping using e-commerce websites.

Finance Safety

- The impact of a cyber-security attack on finance can occur both **while** the **attack** is **taking place** and **after**.

- While a cyber-security attack is happening, **access** may be **denied** to **websites** such as **banking**. If a business **loses** personal **data** during the attack then this can have an **impact** on its **finances**.

- If an account is **wiped out**, any **direct debits** set up will **not** be able to be **transferred**, which would lead to **negative consequences**, such as a **low credit score**, and possible **legal action** if a debt is not paid.

- If the loss of personal data resulted in **identity theft** occurring, then there would be also a **financial impact** on the person whose identity has been stolen.