Simple Solutions

Data Security

Data Packets to/fro via Ports

- Data packets travel to and from numbered network ports associated with IP addresses and endpoints, using the TCP layer protocols.
- All ports are potentially at risk of attack. If a port is not configured properly, a hacker can gain access to a server that can contain valuable data.
- Any device and the associated user on that network is then at risk.
- There is 65,535 TCP ports; some of the more common ones are on the next page.

Port attacks

****** SIMPLE SOLUTION ******

- Be aware of port traffic
- Intrusion Detection Software
- Hardware Firewall
- Limiting / permissions for port traffic
- Guest network access control
- Software permissions
- Monitoring and reporting software

Port Number	Port Use
21	Connects FTP (File Transfer Protocol) servers to the internet
110	POP3 (Post Office Protocol version 3) - used for retrieving E-mails
80	HTTP traffic. Unencrypted web traffic
25	SMTP (Simple Mail Transport Protocol) - used for e-mail routing between mail servers
More…	Full List of TCP ports can be located here: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Passwords

Weak and stolen passwords:

- Weak passwords are often a source of a data breach.
- An opportunist hacker may guess a password to a system, or the user has left clues about their password in a security question that leads the hacker to the password.
- Sometimes a password is a simple word from the dictionary that a hacker can do a dictionary attack or a brute force attack and gain access to an account.

Password threats

****** SIMPLE SOLUTION ******

- Use a password manager
- Use complex passwords
- Never share passwords

Back door vulnerabilities

Back door and application vulnerabilities:

If a door is already open, there is no need to break it down.

Hackers love to exploit software that has been poorly written, or networks that are poorly designed and implemented.

Software that has not been updated may contain vulnerabilities that allow a hacker to exploit, thus giving them access to databases.

Back door threats

****** SIMPLE SOLUTION ******

Keep software up to date and fully patched.

Keep hardware up to date and fully patched.

Malware

Malware:

Malware is an umbrella term for viruses, Trojans and worms.

Malware is malicious software that can cause damage to a system and is loaded onto the system without intention; it can give a hacker access to the data.

If the system that contains the malware is connected to other networks, then that malware can spread allowing a hacker access to other areas of a network.

Malware threat

****** SIMPLE SOLUTION ******

Be aware that accessing websites that promote free movies and software may contain malware.

Use anti malware protection and scan the system regularly.

Do not open up e-mail attachments that look suspicious.

Malicious Insider

Malicious insider:

A rogue employee, a disgruntled contractor, someone who may have even been placed in an organisation with the intent on causing a data breach, or even someone in the organisation who just does not know any better.

What stops people who already have access to a system from copying, altering or stealing data?

Malicious Insider

****** SIMPLE SOLUTION ******

Know whom you are dealing with and act fast if there is any hint of a problem.

Have good procedures in place

Make sure all staff are trained

Unintended Disclosure

Unintended disclosure:

Human error can sometimes lead to a data breach.

Something as simple as sending an e-mail to the wrong person can be very serious if that e-mail contained sensitive data.

Posting too much information online can also lead to a data breach, if a hacker is able to use that information to gain access.

Examples of unintended disclosure on the next page …

Unintended Disclosure

****** SIMPLE SOLUTION ******

Know whom you are dealing with and act fast if there is any hint of a problem.

Have good procedures in place

Make sure all staff are trained

Reasons

A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation that holds it.

Many reasons

****** SIMPLE SOLUTIONS ******

- Loss or theft of data or equipment on which data is stored
- **** Control of devices, logging, monitoring (software), alarms (hardware) ****
- Inappropriate access controls allowing unauthorised use
- **** Limiting permissions (software), placement of equipment (hardware) ****
- Equipment failure
- **** Updated and maintained hardware, software maintenance ****
- Human error and blagging offences
- **** Training, Policy & Procedures, software restrictions, hardware safeguards ****
- Unforeseen circumstances such as a fire or flood
  **** Insurance, maintenance of equipment, cleaning, recovery plan****
- Hacking attack
- **** Security software and hardware, VPN, firewall and intrusion detection software ****

Task

- Now do Task 17