<table>
<thead>
<tr>
<th>4.2 Network Issues and Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security issues regarding data transfer</td>
</tr>
<tr>
<td>• Network communication</td>
</tr>
</tbody>
</table>
4.2 Network Issues and Communication

Security Issues

How can hackers affect your network and data?

Introduce of viruses & spyware to the Network.

Threat to Data:
• Data could be deleted, edited, corrupted or be replicated.
• Data could be sold or passed on to other people.

Threat to Network:
• Network may have to be shut down to quarantine virus.
• This could stop production and cost an organisation a lot of money.

Should the internet be policed?

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To protect vulnerable users gaining access to undesirable websites.</td>
<td></td>
</tr>
<tr>
<td>• To prevent illegal material (software, videos) be openly posted and shared by web users.</td>
<td></td>
</tr>
<tr>
<td>• To bring to justice those users who continually misuse the internet for their personal gain.</td>
<td></td>
</tr>
<tr>
<td>• It would be extremely difficult and expensive to police the internet.</td>
<td></td>
</tr>
<tr>
<td>• Infrastructure including staff and offices would have to be required.</td>
<td></td>
</tr>
<tr>
<td>• Would be difficult to enforce different rules in different countries.</td>
<td></td>
</tr>
<tr>
<td>• Could go against freedom of speech.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.2 Network Issues and Communication

**User Name & Passwords:** Methods of Authentication (Network Security)

Authentication techniques are used to ensure only authorised users are able gain access to a Network via User Names/Passwords, Biometrics, Swipe Cards, TAN, Two Factor authentication etc.

<table>
<thead>
<tr>
<th>Passwords are a method of authentication.</th>
<th>Disadvantages</th>
<th>Avoiding password interception</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Password Image" /></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>• Passwords can be guessed especially if they are simple.</strong></td>
<td><strong>• Passwords may be seen by others.</strong></td>
<td><strong>• Set strong passwords which include multiple characters such letters and numbers.</strong></td>
</tr>
<tr>
<td><strong>• Passwords can be stolen and used by other people.</strong></td>
<td><strong>• Spyware could be used to logs key presses to get passwords.</strong></td>
<td><strong>• Ensure password is regularly changed.</strong></td>
</tr>
<tr>
<td><strong>• passwords can be hacked by using password generating software.</strong></td>
<td><strong>• Passwords can be hacked by using password generating software.</strong></td>
<td><strong>• Avoid using the same passwords for all of your accounts.</strong></td>
</tr>
<tr>
<td><img src="image" alt="Strong Password Image" /></td>
<td></td>
<td><strong>• Install spyware software which will block the installation of any key logging software.</strong></td>
</tr>
</tbody>
</table>
User Name & Passwords: Methods of Authentication (Network Security)

### Setting a strong Password:
- Use at least **8 characters**
- Includes **letters** and **numbers**
- Avoid using names or words which could be easily guessed.
- Use **upper** and **lower case** letters.

When users log onto their online accounts they may also be asked for additional information to verify their accounts.

### Security Question:
- Users may be asked to **answer security questions related to their account.**
- Typical questions includes **mothers maiden name.**

### Personal Image:
- QNB (Qatar National Bank) require users to identify **an image when they log in** on the website for online banking.
- Users will have to **confirm if the image shown** is one they selected as their **account image.**
### 4.2 Network Issues and Communication

#### Alternatives Methods of Authentication (Network Security)

<table>
<thead>
<tr>
<th>Device</th>
<th>Overview/Advantages</th>
</tr>
</thead>
</table>
| Biometrics                  | • Biometrics use unique data.  
• Only the person with the biometric features can access the network.  
• Can not copy/replicate biometric data |
| Magnetic Swipe Cards        | • Swipe cards are used to gain access to the system by swiping the card into the reader.  
• Swipe cards are quite easy to use and update.  
• Could also be used to gain entry into a room (hotel room). |
| Transaction authentication number (**TAN**) | • TAN is used by online banking services.  
• User will insert their bank card into the TAN reader which will then provide a code which will need to be entered to complete a transaction. |
| Two factor authentication   | • Two Factor Authentication involves the user typing in their password and then typing in a code.  
• The code is sent to the registered phone number of the account as a text.  
• If an unauthorised attempt is made to log into an account then the text message will alert the user. |
Chapter 4: Networks Issues and Communication

4.2 Network Issues and Communication

Security issues regarding data transfer: Viruses & Spyware

A computer virus is a piece of programming code/software which can install and replicate itself on to a computer system without the user’s permission. A computer virus can cause the following problems.

1. Causes the computer to crash – become slower
2. Sometimes files can be deleted – leads to computer malfunction.
3. Data files can be copied by the hacker or the files could be corrupted.
4. Could stop production until the virus has been quarantined.

Spyware gathers data from computers without the user knowing. Spyware could monitor key presses to gain personal information or passwords. This information would be sent back to the hacker.

Installing anti virus and spyware software and the use of a firewall is not enough to keep your computer safe. You also need to pay attention to the following points.

- Do not download any files from untrusted sources including email attachments.
- Do not install illegal software onto your computer.
- Do not click on links from unknown websites.
- Do not connect storage devices (e.g. USB) from unknown sources.
- Ensure virus software is up to date and virus definitions are regularly updated.
4.2 Network Issues and Communication

Security issues regarding data transfer: **Firewall**

- **Prevents computer accessing undesirable/unauthorised sites**
- **Monitors and controls incoming and outgoing data traffic.**
- Helps to prevent malware (viruses) getting into computer/from the internet
- Prevents unauthorised computers using the internet accessing the computer
- Keeps a list of undesirable sites/IP addresses
- Keeps a list of acceptable sites/IP addresses
- Warns you regarding threats/allows you to accept/reject downloaded programs
4.2 Network Issues and Communication

**Encryption**

Encryption is the process of converting information into a form that is meaningless to anyone except holders of a ‘key’.

1. Data is scrambled up (Data is Encrypted).
2. If the data is intercepted it then it prevents people from understanding and reading the data.
3. The person with the key is able to Decrypt and understand the data.

**Disadvantages**

- Data can still be deleted from system
- Criminals can use encryption to keep incriminating material secure
4.2 Network Issues and Communication

- Proxy Server

Can be used to **monitor** Internet usage

Can **block** certain sites

Server passes on **requests** to the Internet
PASSES THE REQUESTED WEB PAGES TO INDIVIDUAL COMPUTERS

Can **cache/store** the webpages

Can act as a **buffer** (between Internet and LAN)

Can act as a **web server**
4.2 Network Issues and Communication

Security issues regarding data transfer: Data Protection Act

Data protection Act applies to paper based or electronic forms of data stored on a computer. The data protection act is to protect rights of the individual who the data is obtained from.

Web based business such as Amazon or Ebay store sensitive data about customers including payment details. They would have to abide by the data protection act to keep the data secure.

Principles of the Data Protection Act

1. Data must be fairly and lawfully processed.
2. Data can only be processed for the stated purpose.
3. Data must be adequate, relevant and not excessive.
4. Data must be accurate.
5. Data must not be kept longer than necessary.
6. Data must be processed in accordance with the data subject rights.
7. Data must be kept secure.
8. Data must not be transferred to another country unless they have adequate protection.
### 4.2 Network Issues and Communication

#### Network communication

<table>
<thead>
<tr>
<th>Type of Communication</th>
<th>Overview/Advantages</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Faxing</strong></td>
<td>• Requires a fax machine and a telephone line.</td>
<td>• Anyone can access faxed documents.</td>
</tr>
<tr>
<td></td>
<td>• Number of the recipient dialled before the document is copied and sent.</td>
<td>• The fax may be out of paper or ink (toner).</td>
</tr>
<tr>
<td></td>
<td>• Physical documents are printed and can be signed.</td>
<td>• No notification of fax received.</td>
</tr>
<tr>
<td><strong>Email Communication</strong></td>
<td>• Can send multiple attachments.</td>
<td>• Email attachments may include viruses.</td>
</tr>
<tr>
<td></td>
<td>• Can send to multiple recipients in one message.</td>
<td>• May receive spam (unwanted mail).</td>
</tr>
<tr>
<td></td>
<td>• Emails can be received instantly and accessed on many platforms including tablets and phones.</td>
<td>• May receive phishing (scam) emails to obtain personal data.</td>
</tr>
<tr>
<td><strong>Electronic Faxing</strong></td>
<td>• Electronic Fax is sent via a internet connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No need to buy a fax machine, ink or paper.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Electronic Fax documents are sent to an email which will ensure the correct person will receive the fax – less chance of document being intercepted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Electronic Fax's can also be sent directly to a fax machine.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Send fax's from any location with an internet connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No additional cost to send fax over internet network.</td>
<td></td>
</tr>
</tbody>
</table>
## 4.2 Network Issues and Communication

### Network communication

#### Advantages and Disadvantages of using email compared with faxing

<table>
<thead>
<tr>
<th></th>
<th>Fax</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advantages</strong></td>
<td>• Documents can be signed which are legally accepted.</td>
<td>• Emails are password protected so less likely chance of data being intercepted.</td>
</tr>
<tr>
<td></td>
<td>• Physical copies of documents can be sent and automatically printed.</td>
<td>• Emails can be received instantly.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attachments can be edited and sent back.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Can send to many recipients at the same time.</td>
</tr>
<tr>
<td><strong>Disadvantages</strong></td>
<td>• Data is more likely to be intercepted once it is printed from the fax machine.</td>
<td>• Cant be used when documents need to be signed.</td>
</tr>
<tr>
<td></td>
<td>• There could be delays in receiving the fax due to a busy telephone line or lack of paper or ink.</td>
<td>• Viruses can be download from attachments.</td>
</tr>
<tr>
<td></td>
<td>• Fax can only be received during office hours.</td>
<td>• Unwanted emails could be received (Phishing/Spam).</td>
</tr>
<tr>
<td></td>
<td>• Not everyone has a fax machine.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.2 Network Issues and Communication

#### Network communication

<table>
<thead>
<tr>
<th>Type of Communication</th>
<th>Overview</th>
<th>Hardware</th>
</tr>
</thead>
</table>
| **Video Conferencing**  | • Video conferencing uses both **video** and **sound** using an **internet connection**.  
• It can be used to have business meeting when people are in different locations.                                                                                                                                   | • Web Camera      |
| **Advantages**          | • **No need to travel** to have meetings which would cut down on travelling costs (including flights and hotel) and travelling time.  
• Video conference can be **held at short notice**.  
• Facilitates **long distance learning** – students can access live lectures without travelling.                                                                                                                  | • Screen/Monitor  |
|                         | **Disadvantages**                                                                                                                                                                                                                                                                                                                      | • Speaker         |
|                         | • **Technical problems** with the internet or hardware could effect the quality of the video conference.  
• **Set up costs** to purchase hardware/software and to provide relevant training to staff.  
• **Lack of personal contact** you would have if it was a face to face meeting.  
• **Different time zones** could make it difficult to find to find a suitable time to have a meeting.  
• Not possible to **sign documents**.                                                                                                                                                                              | • Microphone      |
## 4.2 Network Issues and Communication

### Network communication

<table>
<thead>
<tr>
<th>Type of Communication</th>
<th>Overview</th>
<th>Hardware</th>
</tr>
</thead>
</table>
| Audio-Conferencing    | Audio conference can be done over the telephone network or using a computer making use of VOIP.  
1. The organiser of the phone conference is given a unique PIN which can be shared participants.  
2. For Participants to join they have to dial the conference phone number.  
3. Then they would have to enter a PIN.                                                                                                             | • Telephone  
- VOIP  
- Microphone  
- Speakers                                                                                                                                          |
| Web-Conferencing      | • Web conference can be done using internet connection.  
• It is very similar to video conference as participants can hear audio and see a live video stream.  
• Participants can join the web conference by clicking on the supplied link from the organiser.  
• Participants can join and leave the web conference at any time.  
• Instant messaging (IM) feature is available to communicate with other participants.  
• Participants can be given permission to speak and can share content such as images, video or presentations. | • Same as video conferencing.  
• Keyboard could be use for IM.                                                                                                                     |