Higher Computing Science
Security risks and precautions
Legal implications and Environment, Economic and Social impact
Summary notes

Security risks

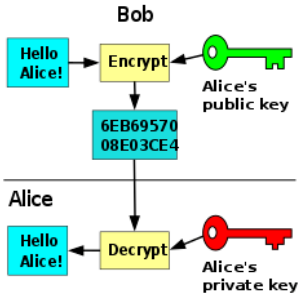
Some of the risks associated with using computers and the internet include:

Trojans	Any software that appears to be a useful program on the surface but actually performs a secondary function that is malicious in intent e.g. gathering information about a user's activities. Trojan cans be used to create a 'backdoor' which will allow unauthorised access to the user's computer without their knowledge. Users may download and install what they believe to be legitimate software without realising that a Trojan horse will also be installed. Examples of Trojans might be: • A free online game that you can download. These may be tracking your activity which can be recorded and sold to a third party. • Third party browser toolbars. These appear to add features to your web browser but in reality, are usually tracking your online browsing • The Trojan may be downloaded and installed as part of another piece of software such as trial versions of less well known anti-virus software.
Adware	Software that advertises a product or service and intends to generate revenue for the host company or developer. Often information will be gathered from the user which can be considered a security threat. When the adware becomes intrusive like this, then it is spyware. Adware installed with the ability to review browsing habits makes use of tracking cookies and may use data gather to advertise products and services that are more likely to appeal to the user.
Tracking cookies	Cookies are simply small text files that contain information that relates to use of websites and the World Wide Web. This can include login details, browsing information or session data (i.e. remembering the contents of a shopping basket). Tracking cookies are where the details recorded are a threat to either privacy or security (e.g. browser search history, saved passwords for websites etc.). This information can be sent to a third party who can use this maliciously.

Denial of Service (DOS/DDOS) attacks	A denial of service attack involves flooding a web server with a large number of access requests over a short period of time. The targeted domain is then unable to cope with the demand of the sudden increase and this results in significantly reduced performance. In many cases this can even result in webpages and services becoming unavailable to legitimate users. **Effects and cost** The effects of the attack can result in bandwidth consumption and starvation of resources. The disruption in service that can also effect the host financially through lost revenue (missed sales) as well as the costs involved in resolving the issue. **Reasons** There can be a variety of motivations behind the attack: **Financial** – the main intention may be to harm the host company's finances. At times this may be combined with another form of attack (e.g. hacking, remote access) in a bid to access personal or sensitive information that can be used for monetary gain. **Political** – others attacks are the result of the instigator holding political, ethical or idealistic views opposing that of the target. For example an animal rights group may target the servers of an organisation that harms animals for sport or food. **Personal** – sometimes the motivation be for personal reasons that relate to the individual. In some cases, this could be revenge against what could be considered maltreatment or as punishment for previous actions. Another alternative is where the attack itself can be considered a challenge and used as a means of proving a point or improving the status of the individual.

Security precautions

There are a variety of procedures that are used to reduce the risk of security breaches.

Encryption	Encoding data before it is stored or transmitted. The data must then be decrypted using the correct key before it can be understood. If data is intercepted it cannot be easily deciphered. One method is achieved with the use of a public and private key (public key/asymmetric encryption) system.  By using a key pair (public and private key) the data can be protected against interception and unauthorised access. The **public key** is shared by the sender and recipient and is used to **encrypt** the data. The **private key** is known only to the recipient and this is used to **decrypt** and reveal the message. This system ensures that only the intended recipient can decipher the message. It also can be used as a means of verifying the identity of the other party.
Digital signatures	Uses encryption methods as a way of authenticating data so that the recipient can be sure it has not been altered or tampered with.
Digital certificate	An electronic document used to prove that the person sending data is who they claim to be.  A padlock icon in the address bar of your browser shows that the website has a digital certificate so you can be sure that you're dealing with a genuine website.
Server-side validation of online form data	Online forms allow you to enter data into a website, such as a username and password. Server-side validation means that your login details are stored on the web server. The username and password you input will be compared to the details held on the server and, if they match, the server will send your account data to your computer.
Biometrics in industry	Biometrics (using unique characteristics as identification, such as fingerprint, iris or voice) is increasingly popular in industry. E.g. banks using fingerprint recognition, facial recognition at airports, etc.

Legal implications

Regulation of Investigatory Powers Act (RIPA)

Commonly referred to as the RIPA, the Regulation of Investigatory Powers Act is an act of parliament that applies in the UK. Introduced in 2000 the RIPA was designed to give certain groups the legal right to carry out electronic surveillance and access the details of electronic communication by a person or organisation.

The act allows certain organisations and government bodies (e.g. the police, local councils, MI5) to intercept data, access password protected data and carry out surveillance for the purposes of crime prevention.

- Protects individuals' rights to privacy.
- ISPs must be prepared to provide data to authorised bodies if request to do so.
- Refusing to provide keys to access encrypted data can lead to a jail sentence.

Other responsibilities of the act include:

- A requirement for companies to inform employees of access to electronic communications and that data is subject to the act.
- The provision of access or encryption keys to authorised authorities, bodies or personnel.
- The fitting or maintenance of equipment or facilities to support surveillance operations and store electronic communications.
- Providing access or allowing payment for facilities/software to monitor electronic communications.

Environmental implications

Some of the environmental factors to consider when using computer systems include:

Environmental benefits of computers

- Reduction of paper used in offices/places of work
- A reduced need for manufacturing or transportation of physical goods (e.g. books, music, videos) due to electronic distribution (i.e. downloading, cloud services).
- Global climate analysis, forecasting and modelling.
- Easy communication across the globe which can provide the ability to work from home, reducing the need for travel.

Lifetime carbon footprint

A measure of how much carbon dioxide is produced over the lifecycle of a product. In terms of computer systems this includes:

- the manufacture of devices and peripherals relating to computer systems.
- the electricity consumed through use of computer systems that has been produced using fossil fuels.
- the disposal or recycling of equipment that contains dangerous elements or toxic materials.

The above factors have a negative impact on the environment and can contribute to global warming.

Intelligent control of heating systems

One of positive impacts of computer systems on the environment is the use of intelligent control for heating systems that leads to increased efficiency and less energy wastage. The benefits of this can be achieved through the following:

- Remote access that allows heating system to be controlled when away from home.
- Use of geolocation data that automatically turn heating off or on according to distance.
- System that accounts for external weather forecast with the ability to make adjustments to temperature accordingly.
- Real time monitoring of temperature through mobile devices which can reduce unnecessary gas/fuel use.
- Data from system can be analysed to determine how quickly a home heats and how slowly it loses heat which can allow the boiler to be used more efficiently.
- The use of multi room control systems that prevent rooms being overheated when not in use.

Economic impact

Some of the economic factors to consider when using computer systems include:

Competitive advantage	Dynamic websites and social networking can allow businesses to gather information about the market which can give them an advantage over their competitors.
Global marketplace	Businesses now have access to, and can cater for, customers across the globe. Location is less of limiting factor.
Business costs	Costs involved in setting up a business have changed – no need for expensive premises, it is cheap to set up an e-commerce site. Specific factors include: **Training** – requirement to train employees on the use of computer systems and this must be factored into the overall cost. **Hardware/software**– purchasing both hardware and suitable software that can support the use of computer systems. This can be a significant upfront investment but will also be an ongoing cost as both will need to be maintained (repairing, upgrading, updating etc.). **Storage** – companies must decide on an approach to store data required for their business to operate. Solutions may include either local or cloud storage, or in some cases a combination. Both will cost the business so they must decide what system is best to maintain and how it can adapt to changes in the business itself.

	Connectivity -companies must be aware of costs involved in connecting to the market place and their customers. Communication is important for businesses to operate effectively so a model appropriate to the business needs should be implemented.
Maintainability	Quickly updatable, database-driven websites, make it easy to upgrade prices, put on special offers or change branding to suit business needs. This reduces the time and costs required to maintain the business.
Scalability	It can be easy for businesses to adjust according to a changing customer base, high street premises are not a requirement. Businesses can adapt to a changing market more easily.

Social impact

Censorship and freedom of speech	Anybody can make their views heard online but some governments may try to impose censorship on content which is acceptable elsewhere. This can take the form of a locked down internet where access to certain websites is restricted.
Privacy and encryption	Huge amounts of data about individuals are stored and shared readily, leading to concerns about invasion of privacy and the need for encryption by all data users. Many companies take active steps to ensure the privacy of their users is maintained.
Global citizenship	Online communities and a breaking down of international barriers has led to the idea of the global citizen, somebody who is aware of their responsibilities and impact upon the planet as a whole.
Online communities	Online communities allow people from anywhere in the world to interact and collaborate. Physical location may longer not be a barrier.