***Activity 1***

**Main Cloud Security Issues and Threats in 2021**

* Misconfiguration. Misconfigurations of cloud security settings are a leading cause of cloud data breaches.
* Unauthorized Access.
* Insecure Interfaces/APIs.
* Hijacking of Accounts.
* Lack of Visibility.
* External Sharing of Data.
* Malicious Insiders.
* Cyberattacks.

**Benefits of Cloud Computing**

* Faster time to market. You can spin up new instances or retire them in seconds, allowing developers to accelerate development with quick deployments.
* Scalability and flexibility.
* Cost savings.
* Better collaboration.
* Advanced security.
* Data loss prevention.

***Argument in favor of cloud storage***

**Disaster Recovery**

When you use cloud storage, data is at a reduced risk of system failure since all data is stored and backed-up on an external devise often thousands of miles away from your own location. This means you avoid expensive data retrieval that follows an all-too-common hard-drive malfunctioning. Cloud providers automate the backup process for you. Therefore, there is no need to back-up your data on an external devise yourself. You save time and stress as a result.

**Access your data anywhere**

Since your data is stored remotely you can access it whether you are in Manchester or Madrid. This is especially helpful if your work requires frequent travel or if your team is located in different time-zones. Cloud-storage also helps the collaborative process when your team is spread out across the globe. Cloud storage makes it easy for employees to login and access other team members’ work regardless of location and distance that separates team members. When you use cloud storage you’re not restricted by place or medium and your employees are able to work from home or abroad as a result.

**Low cost**

Cloud storage eliminates the need to pay for software licenses and updates since all this is included in one global monthly price. Cloud storage also avoids the need to invest in expensive server infrastructure since the cloud company provides this off-site for you. You eliminate the need to pay a dedicated storage professional in-house since you are effectively outsourcing this to the cloud storage company. Unlike in-house employees, you do not need to pay the cloud storage company sick-pay or holiday pay.

**Scalability**

You only pay for the amount of storage you need. If your business experiences growth, the cloud operator is able to accommodate your corresponding growth in data storage needs. You simply extend the amount of available storage by varying how much you pay. Likewise, if your business shrinks, you can then opt for less storage space at a reduced rate. Scalable payment plans such as 'pay as you go' are commonly available. Thus, cloud storage caters for all business sizes and needs.

**Security**

Professional cloud storage firms typically offer far better data security than is otherwise available to small businesses through efforts of their own. Cloud storage companies offer password protected data storage. Data is then sent over the internet using encryption technology. This ensures the highest standards of security are upheld.

***What are the security risks involved in the cloud vs local store?***

* **In local**

Local storage shares many of the same characteristics as a cookie, including the same security risks. One of those is susceptibility to cross-site scripting, which steals cookies to let hackers masquerade as a user with their login session for a site

* **In cloud**
* Employees Using Unapproved File Sharing Systems
* Lack of Data Control
* Lack of Data Privacy
* Weak or Nonexistent Governance/Compliance Tools
* Lack of Employee Training

***Solutions***

Today's businesses are embracing digital deployment efforts that require robust, flexible, scalable, and high-availability IT environments for superior user experiences. As your business grows, your application needs to run with the same outstanding performance and security every day.

Any business looking to regain control over cloud security should seek help from trusted security companies. You can protect yourself by implementing a security plan to identify potential security risks and protect the company from the damaging consequences of a cybersecurity incident.

***Activity 2***

There are several precautions and safeguards that could have been in place to avert the WannaCry attack:

Keep all software and operating systems up to date with the latest patches and security updates. This would have prevented the WannaCry attack from exploiting a known vulnerability in older versions of Windows.

Use a firewall to block external access to your computer. This can help prevent malicious actors from remotely accessing your system.

Enable Network Level Authentication (NLA) for Remote Desktop Protocol (RDP) connections. This would have required an attacker to authenticate before they could gain access to the system.

Enable User Account Control (UAC) to prompt for confirmation before running programs with administrative privileges. This would have made it more difficult for the ransomware to execute.

Regularly back up important data and store the backups offline. This would have allowed organizations to recover their data in the event of an attack.

To safeguard your computer against attacks caused by legacy software without updates, the following security measures can be taken:

Uninstall any unnecessary software, especially those that are no longer supported or receive security updates.

Use a reputable antivirus software to detect and prevent malware from infecting your system.

Enable automatic updates for your operating system and other software to ensure that you are always running the latest version.

Use a firewall to block external access to your computer.

Enable NLA for RDP connections and UAC to prompt for confirmation before running programs with administrative privileges.

Regularly back up important data and store the backups offline.

Without the option for a software update, it is especially important to follow the other best practices listed above to ensure the security of your computer. It may also be necessary to consider replacing the legacy software with a newer, more secure version if it is critical for your operations.

***Activity 3***

Having a backup system in place is important because it helps to ensure that important data is not lost due to hardware failures, malware attacks, or other unforeseen events. This is especially important for businesses and organizations that rely on their data to operate and serve their customers.

A good backup system should be an integral part of a broader cyber security framework, as it helps to protect against data loss resulting from cyber threats such as ransomware attacks. Additionally, having a reliable backup system in place can also help to minimize the impact of a data breach by allowing organizations to quickly restore their systems to a known good state.

To create a backup system for my personal computer, I would follow these steps:

Identify the data that needs to be backed up. This might include documents, photos, music, and other personal files.

Choose a backup destination. This could be an external hard drive, a cloud storage service, or another type of storage media.

Set up a schedule for backing up the data. This could be done daily, weekly, or at some other interval depending on the needs of the user and the amount of data that needs to be backed up.

Use backup software to automate the backup process. This could be a built-in utility like Time Machine on a Mac, or a third-party application like Acronis True Image.

Test the backup system to ensure that it is working as intended and that all of the necessary data is being backed up.

Store the backup media in a secure location to protect against physical damage or theft.

Regularly review and update the backup system to ensure that it is still meeting the needs of the user and the organization.

***References***

* <https://cloud.google.com/learn/advantages-of-cloud-computing>
* <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/>