

**Yussuf Seifudin 660411**

**Question 1**

What are some of the commonest causes of data loss in Small and Medium Sized Enterprises such as Lipscomb & Pitts Insurance LLC?

**Definition in Information Security**

Data loss occurs when valuable or sensitive information on a computer is compromised due to theft, human error, viruses, malware, or power failure. It may also occur due to physical damage or mechanical failure.

**Common causes of data loss in Small and Medium Sized Enterprises**

1. **Human error** – One of the biggest issues in terms of security threats that an organization can face. Human errors can occur in various ways which can be categorized into various ways:
2. **Skilled-based error** – This type of error can be encountered when an employee is completing a task that they are familiar with. An example can be an employee who is tasked with reviewing documents and shredding the documents that might not be needed. The error can come in terms of not properly disposing of the document and someone might end up picking it up and misusing the information.
3. **Decision-making** – this may occur when an employee compromises sensitive data because they don’t understand the risks involved. This could be because they don’t have the necessary information in question. An example can be that the employee has been tasked to configure a database containing customer records. The error can occur when the employee does not encrypt the customer’s sensitive data within the database.
4. **Natural Disasters** – This can cause data loss whereby the hardware that is responsible to store the company data is compromised. Such as Wildfires, hurricanes, tornadoes, extreme rainfalls, landslides, and among others. Natural disasters pose a huge threat to both the employees and office structures, especially to the IT infrastructure. An example would be when a fire or flooding would occur in an organization’s server room the organization’s key business data could be destroyed.
5. **Hardware Failure** - Hardware damage and system malfunction are among the top causes of data loss. It happens every day at businesses of all sizes, all over the world. There are several ways in which IT malfunction can cause data loss within an organization.
6. Hard drive failure
7. Operating system crashes
8. Software errors and crashes (more on this below)
9. Network hardware failure
10. Physical damage to hardware
11. **Viruses and Malware** – Malware is one of the most frustrating causes of data loss because it’s a threat that’s constantly evolving. Anti-malware systems are constantly blocking malicious viruses, bad websites, suspicious attachments, bad IP addresses, hijackers, worms, adware, and more. But tomorrow, those threats will be back. And there will be new ones too: new strains of malware that your anti-virus systems don’t even know about it.

**Question 2**

1. **How does a cloud network-attached storage (NAS) work?**

To understand how a NAS works, we must first understand what it is to get a gist of what could be its purpose.

***Definition***

A Network-Attached Storage according to AWS is a file storage that provides employees access to data over the network with the key element of having access always as long as a person is connected to the internet and collaboration of data. NAS devices are special servers configured to handle requests for storing and sharing files and they achieve this by providing fast, secure and reliable storage services via private networks.

***How they work***

NAS combines protocols used by hardware and software in file sharing over the network which allows computers to access files as if the files were stored locally

Some of the protocols include:

Data Transfer protocols are similar to the IP and TCP protocols used in most machines. The IP dictates where the Packet will be sent and TCP delivers the data packets over the network.

File formatting protocols – in the file formatting protocols, NAS implements some servicing systems to translate data into acceptable formats depending on the OS being used in the file sharing.

Network File System (NFS) – Linux and Unix systems

Server Message Block (SMB) Microsoft Windows-based machines

Apple Filing Protocol (AFP) – MacOS

1. **What are the advantages and disadvantages of a cloud network attached storage (NAS)?**

**Advantages**

1. Offsite storage and file collaboration – An organization can outsource the storage and file management to another individual leaving them with additional time to conduct other activities.
2. Available active data backups – implementation of NAS ensures that there are backups and in case of failure, the business is not at a complete loss since there are ‘save points that can be traced for the organization to pick up from.

**Disadvantages**

1. Management complexity – NAS increases the operational load of an organization and drains its funds in maintenance due to most services being charged periodically and not as a one-time purchase hence the organization must allocate time, staff, and money to use NAS.
2. Scaling quickly is difficult – Although it is network-based, NAS devices still use similar architecture to those of a normal computer such as HDD and SSD storage mediums that tend to get overloaded if many requests are sent to retrieve or save data at a go.
3. No warranty – Reliance on NAS devices cannot be guaranteed since drawbacks may still be experienced by the organization implementing it one being data loss which is the main purpose of its implementation.

**Importance of a disaster recovery plan**

****

* A Disaster Recovery Plan ensures that Small and Medium Sized Enterprises avoid large losses in the event that the IT infrastructure and data are damaged. It will minimize the operational and financial impact of unplanned business disruption at any level.
* A DRP plan that includes regular data backups in multiple locations avoids losing vital business data in a cyber-attack or a network outage.
* A Disaster Recovery Plan will also help an SME maintain its good reputation with its clients. These days, more and more customers are demanding evidence of an effective Disaster Recovery Plan before they do business with an organization. Organizations without a plan will risk a loss in sales because of their refusal to implement one.
* A Disaster Recovery Plan will ensure minimized downtime.