Md Khorshed Alom
CSE 066 07731
66 (C)

Question No 1:

Storage services: Storage Services means the provision by Us of storage of Precious Metal manufactured by Us, or at Our sole discretion, Precious Metal from other manufacturers.

Storage service is a business model in which a company leases or rents its storage infrastructure to another company or individuals to store data. Small companies and individuals often find this to be a convenient methodology for managing backups, and providing cost savings in personnel, hardware and physical space.

Different types of storage services:

1. ***File servers*** **:** A file server is a computer responsible for the storage and management of data files so that other computers on the same network can access the files. It enables users to share information over a network without having to physically transfer files.

   The file server takes on the computer or server role to store and make available data blobs to clients, serving as a central location to store and share files for a network. They can be limited to a single local area network (LAN) or can be open to the internet.

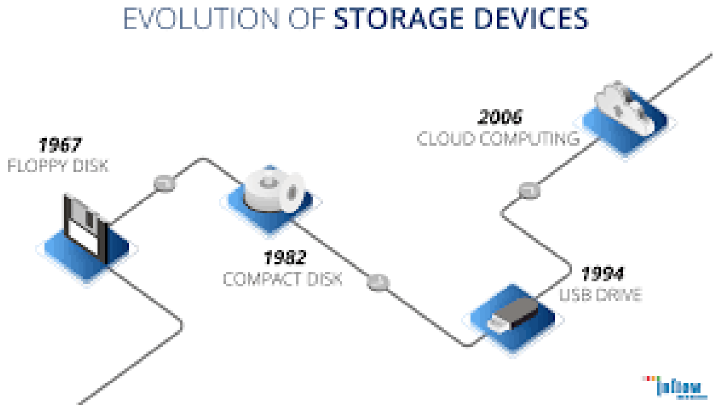
   File servers make storing, securing and sharing files in an organization simpler. File servers are a common target for hackers and ransomware, so particular attention must be given to securing them against attacks.

2. ***Database servers*** **:** Database servers are high-powered computers that store and manage data stored on a server for a network of users and devices. The terms database servers, database management systems (DBMS), and relational DBMS (RDBMS) get used interchangeably, but RDMBS is the most often implemented type of database management. Collectively, database server solutions offer central data management, security, controls for access and permissions, and an interactive repository for a network of users.
3. ***Data warehouses*** **:** A Data Warehousing (DW) is process for collecting and managing data from varied sources to provide meaningful business insights. A Data warehouse is typically used to connect and analyze business data from heterogeneous sources. The data warehouse is the core of the BI system which is built for data analysis and reporting.

   It is a blend of technologies and components which aids the strategic use of data. It is electronic storage of a large amount of information by a business which is designed for query and analysis instead of transaction processing. It is a process of transforming data into information and making it available to users in a timely manner to make a difference.

4. ***Data centers*** **:** Modern data centers are very different than they were just a short time ago. Infrastructure has shifted from traditional on-premises physical servers to virtual networks that support applications and workloads across pools of physical infrastructure and into a multicloud environment.

   In this era, data exists and is connected across multiple data centers, the edge, and public and private clouds. The data center must be able to communicate across these multiple sites, both on-premises and in the cloud. Even the public cloud is a collection of data centers. When applications are hosted in the cloud, they are using data center resources from the cloud provider.



The evolution of storage services :

Software-Defined Storage will ship more storage in 2018 than any other architecture

Software-defined storage adoption has continued to grow rapidly, due to its flexibility and agile architecture. 2018 will be the first year in which software-defined storage capacity shipped will exceed all of the traditional storage appliances combined (time to sell that Dell-EMC, IBM and Netapp stock).

Multi-Cloud data storage will gain traction into the largest Enterprise IT organizations

Cloud is a reality in the Enterprise IT world. IT organizations need to be in control of their data and will want a degree of cloud independence. The leading enterprises will become multi-cloud service organizations, using private and public cloud to transform and accelerate their business.

Md Khorshed Alom
CSE 066 07731
66 (C)

The Rise of Metadata

As the volume of data grows, metadata is critical. Metadata is king, and we're seeing a rise in storage systems that will store both the data itself and relevant metadata about that data. Traditional storage approaches like NAS, and even worse SAN storage, had no context knowledge of the data that they stored.

Convergence of object storage and analytics

Somewhat tied to the above point, storage systems must change to understand the data they are storing. That will apply to the metadata tagging and also to the data itself.

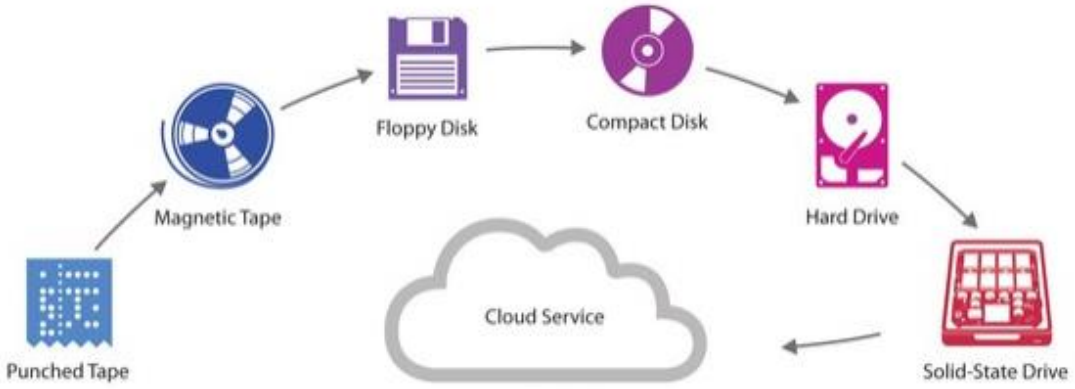
Last days for the Storage Administrator – application-driven DevOps takes over

DevOps is now commonplace, and as companies build applications, they design into those applications the ability to control the infrastructure. This will mean that the traditional role of storage administrator will start to disappear.

Privacy regulations like GDPR require data to be always-on and available

Lastly, but certainly not the least, in 2018, data controls and privacy management got teeth. New regulations like the European Community's General Data Privacy Regulations (GDPR), require data to be always available and indexed.

The decline of tape won't be driven by cost; it will be driven by the need for continuous, always-on access. So long tape; you've had a good run.



EVOLUTION OF STORAGE

Md Khorshed Alom
CSE 066 07731
66 (C)

Question No 2:

Different types of information theft methods :

1. ***Physical Theft****:* examples of this would be dumpster diving, mail theft, skimming, change of address, reshipping, government records, identity consolidation.
2. ***Technology-Based***: examples of this are phishing, pharming, DNS Cache Poisoning, wardriving, spyware, malware and viruses.
3. ***Social engineering:*** examples of this are pre-texting, contests and surveys, obtaining credit reports, bogus employment schemes.
4. ***Financial crimes***. We've all heard the classic story of somebody checking their credit card statement, only to find transactions they didn't make. These false transactions are often the result of computer hackers stealing your credit card numbers, checking account info or gaining access to other financial data.

5. ***Vandalism****.* Hacking has its own subculture, so some hackers may want to vandalize certain websites just to show off to other hackers. Does it sound ridiculous? Don't make the mistake of not taking this motivation seriously; it's fairly common, according to Malwarebytes.

6. ***Hacktivism****.* This portmanteau describes a form of hacking somewhat like vandalism. Some hackers may want to alter or destroy certain websites for politically motivated reasons.

7. ***Corporate espionage***. Spying existed long before the internet era, and hacking has only made espionage more accessible to the everyday person. With much of the world constantly connected to the internet, one company can hack into other companies' devices to steal their information and use it to build an unfair competitive advantage.

Anti-measurements that help us to secure your information storage:

1. *Use a firewall.*

Windows and macOS have built-in firewalls – software designed to create a barrier between your information and the outside world. Firewalls prevent unauthorized access to your business network and alert you to any intrusion attempts.

2*. Install antivirus software.*

Computer viruses and malware are everywhere. Antivirus programs such as Bitdefender, Panda Free Antivirus, Malwarebytes and Avast protect your computer against unauthorized code or software that may threaten your operating system. Viruses may have easy-to-spot effects – for example, they might slow your computer or delete key files – or they may be less conspicuous.

3. ***Install an anti-spyware package.***

Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove and tends to deliver unwanted ads or search results that are intended to direct you to certain (often malicious) websites.

4. ***Use complex passwords.***

Using secure passwords is the most important way to prevent network intrusions. The more secure your passwords are, the harder it is for a hacker to invade your system.

More secure often means longer and more complex. Use a password that has at least eight characters and a combination of numbers, uppercase and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes.

5. ***Keep your OS, apps and browser up-to-date.***

Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. The same goes for apps. Today's web browsers are increasingly sophisticated, especially in privacy and security. Be sure to review your browser security settings in addition to installing all new updates. For example, you can use your browser to prevent websites from tracking your movements, which increases your online privacy. Or, use one of these private web browsers.

6. ***Ignore spam.***

Beware of email messages from unknown parties, and never click on links or open attachments that accompany them. Inbox spam filters have gotten pretty good at catching the most conspicuous spam. But more sophisticated phishing emails that mimic your friends, associates and trusted businesses (like your bank) have become common, so keep your eyes open for anything that looks or sounds suspicious.

7. ***Use virtualization.***

Not everyone needs to take this route, but if you visit sketchy websites, expect to be bombarded with spyware and viruses. While the best way to avoid browser-derived intrusions is to steer clear of unsafe sites, virtualization allows you to run your browser in a virtual environment, like Parallels or VMware Fusion, that sidesteps your operating system to keep it safer.

8. ***Secure your network.***

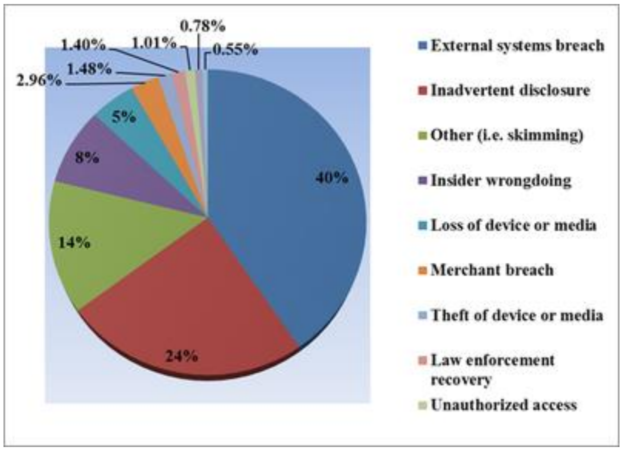
Routers don't usually come with the highest security settings enabled. When setting up your network, log in to the router, and set a password using a secure, encrypted setup. This prevents intruders from infiltrating your network and messing with your settings.

9. ***Use two-factor authentication.***

Passwords are the first line of defense against computer hackers, but a second layer boosts protection. Many sites let you enable two-factor authentication, which boosts security because it requires you to type in a numerical code – sent to your phone or email address – in addition to your password when logging in.

10. ***Use encryption*.**

Even if cybercriminals gain access to your network and files, encryption can prevent them from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker (Windows) or FileVault (Mac), encrypt any USB flash drive that contains sensitive information and use a VPN to encrypt web traffic. Only shop at encrypted websites; you can spot them immediately by the "https" in the address bar, accompanied by a closed-padlock icon.


External systems breach
Inadvertent disclosure
Other (i.e. skimming)
Insider wrongdoing
Loss of device or media
Merchant breach
Theft of device or media
Law enforcement recovery
Unauthorized access