1. **How many virtual processors and how much RAM do you require and why?**

Windows 7 will require more than 1 GB. Windows 8 and 10 will require more than 2 GB. So, it would be better if you could get a system with 8 GB RAM to use 2-3 VM. It depends on the OS as well. Some Linux requires 1 GB and others may require 2-4. So, it depends on what you want to run and where you hold the VMs. Intel i3, Intel i5, Intel i7, Intel i9 can all handle more than the number of VMs but with only a small processing function. Otherwise, the servers exist. Get at least 8 GB if you are looking for a smooth job.

1. **The exact disk layout you wish to have - For each:**

Disk type – SSD

Scenario - IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.

Max disk size - 65,536 gibibyte (GiB)

Max throughput - 2,000 MB/s

Max IOPS - 160,000

* 1. **What is the purpose of the given LUN or Volume?**

The sensible unit number (LUN), when introduced on the host, shows as a mounting volume of the same volume as the 'fraction' made by the controller, which hides any remaining volume in that RAID group. Any remaining volume can be 'cut' to an additional reasonable number (LUN) as required. Ultra-disks bring high throughput, high IOPS, and low disk storage capacity of Azure IaaS VMs. Other additional benefits of ultra-disks include the ability to dramatically change disk performance, as well as your operating loads, without the need to restart your virtual machine (VM). Ultra-discs are suitable for data performance uploads such as SAP HANA, high data, and heavy workloads. Ultra-disks can only be used as data disks. We recommend using premium SSDs as OS disks.

* 1. **How large will the LUN or Volume be? Why did you choose this size?**

There is a certain combination of FlexVol volume and file or LUN configuration that you can use, depending on your application and administrative requirements. Understanding the benefits and costs of these combinations can help you determine the right volume and combination for your LUN configuration.

The following combination of volume suspension and LUN is recommended:

Specified files or LUNs have a larger volume offer

Non-storage files or LUNs have a limited volume offer

Specified files or LUNs have a thick volume provision

You can apply a small SCSI supply to your LUN by combining any of these configuration combinations.

Specified files or LUNs have a larger volume offer

**Benefits:**

* + - All writing functions within space-reserved files are guaranteed; they will not fail because of insufficient space.
    - There are no limits to the efficiency of storage and data protection technology in volume.
    - Less space is reserved ahead of a given volume, and a good writing guarantee is still provided.
    - There are no limits to the efficiency of storage and data protection technology in volume.
    - Space is only shared as it is used.

**Costs and Limitations:**

* + - Adequate space should be set aside for pre-assembled to support a given maximum volume.
    - A space equal to twice the size of LUN is allocated from volume during LUN creation.
    - Non-storage files or LUNs have a limited volume offer
    - Writing tasks are not guaranteed; may fail if the volume runs out of free space.
    - You must manage the free space of the component successfully to prevent the merger expiring the free space.
    - Specified files or LUNs have a thick volume provision
    - Writing tasks may fail with this option.
    - You can reduce this risk by properly measuring the free space in volume by comparing data fluctuations.
    - You cannot rely on data storage protection such as Snapshot copies and FlexClone and LUN files.
    - You cannot use the ONTAP storage capacity that cannot be automatically removed, including extraction, compression, and ODX / Copy Offload.
  1. **What kind of storage would you like the LUN or Volume to be stored on?**

Volumes contain file systems in the NAS environment and LUNs in the SAN area. LUN (sensible unit number) is the identifier of a device called the intelligent unit referred to in the SAN law. LUNs are the ultimate basic unit in SAN configuration. The Windows host detects LUNs on your storage system as virtual disks.

* 1. **What RAID Level would you like the LUN or Volume to be stored on?**

RAID 5 is the most common RAID configuration for enterprise servers and enterprise NAS devices. This level of RAID provides better performance than mirror installation and error tolerance. With RAID 5, data and unity (which is additional data used for retrieval) has lines on three or more disks.

1. **How does this differ from your setup and why is your setup better than this setup?**

When providing an ultra-disk, you can independently adjust the volume and performance of the disk. Ultra-discs come in a limited number of sizes, ranging from 4 GiB to 64 TiB, and include a flexible performance model that allows you to independently configure IOPS and pass.

Some key skills for ultra-disks are:

* Disk Capacity: Ultra disk capacity ranges from 4 GiB to 64 TiB.
* Disk IOPS: Ultra Disks support 300 IOPS limits IOPS / GiB, up to 160 K IOPS per disk. To fulfill the IOPS you have provided, make sure that the selected Disk IOPS is below the VM IOPS limit. The guaranteed minimum of IOPS per disk is 1 IOPS / GiB, with a basic value of 100 IOPS. For example, if you had a 4 GiB disk, you would have 100 IOPS, instead of 8 IOPS.
* Disc Disk: For ultra-disks, the single disk access limit is 256 KiB / s for each given IOPS, up to 2000 MBps per disk (where MBps = 10 ^ 6 Bytes per second). The minimum guaranteed per disk is 4KiB / s for each given IOPS, with a minimum basic 1 MBps.
* Ultra-disks support optimizing disk signal performance (IOPS and login) during bootback without removing the disk from the virtual machine. Once the disk size enhancement function is removed from the disk, it can take up to an hour for the change to take effect. There is a performance limit to increase the working size within a 24-hour window. The performance-enhancing function may fail due to a lack of performance bandwidth.

1. **What are some of the dangers of using this setup as opposed to yours?**

Standard SSDs offer disk explosions. Disk explosion provides better tolerance to unexpected changes in IO patterns. You can make better use of OS disk boot and applications with spiky traffic.

1. **Use the answers from above to craft an email to the IT Manager where you professionally explain why this configuration may not work well for the database you are creating.**

The SQL Server Database Engine runs on the Windows operating system, which also uses the underlying program resources. These resources have a significant impact on the performance of the app and the data system. The functionality of any database system depends on four system resources:

Central processing unit (CPU)

Memory

Disk I / O

Network

CPU, as well as memory, is a key factor in marking computer speed. It is also the key to program performance, as it manages other system resources and performs all applications. Perform user processes and interact with other applications in your system. CPU problems can occur when an application and user applications make too many applications on it. In general, the more CPU power available to your computer, the better the overall system may work.

Database Engine is powerful and gets memory as needed. Performance problems related to memory can only occur if they are not sufficient to perform the required task. When this happens, most memory pages are written to the page file. (The page file view is explained in more detail later in this chapter.) If the process of writing a page file occurs more often, the operation of the system may slow down. Therefore, like the CPU rule, the more memory available on your computer, the better the system will perform.

There are two problems with disk I / O: disk speed and disk transfer rate. Disk speed determines how fast read and write tasks are performed on disk. Disk transfer rate determines how much data can be written to disk during a unit of time (usually measured in seconds). Obviously, the faster the disk, the more data is processed. Also, multiple disks are usually better than a single disk where multiple users use the data system at the same time. (In this case, data availability tends to spread to multiple disks, thus improving the performance of the entire system.)

With customer / server configuration, the database system sometimes works poorly when there is a lot of customer communication. In that case, the amount of data that needs to be transferred to a network may exceed the network capacity. To avoid such restrictions, the following general recommendations should be noted:

If the data server sends any lines to the app, only the required lines by the app should be sent.

If a long-lasting user application works firmly on the client side, move it to the server side (using it as a saved process, for example).

All these program resources depend on each other. This means that performance issues on one device may cause performance problems on other resources. Similarly, improvements related to a single source can significantly increase the performance of other (or all) resources.

For example:

If you increase the number of CPUs, each CPU can share the load evenly so it can adjust the disk I / O bottleneck. On the other hand, improper use of the CPU is often the result of heavy already existing disk I / O and / or memory.

The more memory is available, the more likely it is to find the required page with the app (rather than reading the page to disk), which leads to getting the functionality. In contrast, reading from a disk drive instead of drawing from very fast memory slows the system down a lot, especially when there are many similar processes.

The following sections describe detailed I / O and memory.

Disk I / O

One purpose of a database is to store, retrieve, and modify data. Therefore, Database Engine, like any other database system, has to do a lot of disk work. In contrast to other system resources, the disk system has two moving parts: the disk itself and the disk head. Disk rotation and disk head movement require a lot of time; therefore, disk read and write two of the most expensive functions performed by a database system. (For example, disk access is slower than memory access.)

Database Engine stores data on 8KB pages. The RAM cache is also separated by 8KB pages. The system reads data by page units. Readings occur not only in data recovery, but also in any conversion operations such as UPDATE and DELETE because the database system must read data before it can be converted.

If the required page is in cache, it will be read by memory. This I / O function is called logical I / O or logical reading. When not in memory, the page is read from disk to disk storage. This I / O function is called physical I / O or physical reading. Cache has been stolen because Web Engine uses a single-memory memory format. Therefore, more users can access the same page. Logical writing occurs when data is converted to temporary cache. Similarly, physical writing occurs when a page is written from a cache to a disk. Therefore, logical writing tasks can be performed on a single page before being written to disk.

Web Engine has a few things that have a big impact on performance because they make the most of I / O resources:

Read in advance

Test site

1. **What conclusions can you draw from the first page shown here?**

**Motherboard**

Why is it important to know about motherboards? If the CPU is the brain of your server, the motherboard is the computer board of your computer and acts as the heart and soul of your system. Contains the basic components of your computer architecture, including your RAM (L1, L2, L3 cache), your external connectors (PCIe), input / output ports, socket, and other important components.

Every computer, whether desktop or business has a motherboard, and its role is to facilitate communication between the various elements that reside within its domain; store and retrieve data, and perform the calculations needed to support software applications. Among the elements is the CPU.

**Parts**

Throughout this document, you will learn the references to the various critical elements that make up your server, and one of the most important is Clock Speed.

Clock speed is measured in gigahertz (GHz) and the measurement method is very simple, if the value goes up, the unit is faster. Your processor will calculate statistics continuously and will process billions of bits of data per second. If you use powerful apps, you can expect the best response with high clock speed.

**Cores**

A multi-core processor is a computer processor in a single integrated circuit with two or more different processing units called cores, each reading and executing system instructions. Having the speed of multiple cores will increase your processing power. You may already be using the Intel core on your home computer.

Previous generation cores are embedded in the same core before large tech companies like Intel replicate dual-core (Core i3), then quad-core (Core i5), and then six to eight (Core i7) and now we have a multi-threaded core (Core i9 - eighteen characters, with 35 threads). In a multimedia application, the threads share one or more window resources, including computer units, CPU caches, and lookaside buffer (TLB).

That is why in the past, we at the end of the century (2000) can remember when the system crashed, the whole computer crashed. One of the reasons was that the applications were not very stable, but the CPU was also flawed, lacking sufficient data processing resources. Since the processor has only one theme it means you can run one program at a time. With multiple cores, you can process multiple applications at a time.

**Threads**

If the basic calculation is the visible number of cores on the chip itself, the cable calculation is the number of single application threads that can be simultaneously performed on the CPU itself. Fibers correspond to the number of cores.

System cache is used by the processor to increase the speed of access to commands and data between processor and RAM.

1. **How many CPUs are attached to this machine?**

4

1. **What can you tell about the overall CPU usage on this machine?**

**Causes of high processor usage**

The Task Manager and “top” command not only provide numerical values and data curves to ensure that CPU usage is maximum. Usually, you will be able to identify the cause.

Within the Task Manager, under the “Processes” tab on the first row of the table, you can check how much CPU you are currently using. Separation of all operating systems and background processes can also be viewed. By clicking on the “CPU” column header, you can adjust the CPU according to usage power. If you see a program that you are not using but that takes up more CPU, you can cut it by right-clicking on the drop-down menu. This will reduce CPU usage.

The "top" command indicates CPU usage in all operating processes. This can be stopped immediately using the "kill" command.

Excessive use of the processor may be due to one of the following reasons:

Programs with high CPU requirements: Video and image editing programs, high-resolution video games, DVD burning programs and applications that convert film and image formats, require high processing power and are therefore known for high CPU usage. If, for this reason, the computer cannot work, you should run these programs simultaneously and close all other applications.

Autostart Programs: Applications presented by running an operating system and running in the background can affect CPU usage. That often happens in software required to connect hardware components such as cameras, MP3 players or printers. These programs will automatically start boot-up once installed. You can prevent this from happening by disabling the Task Manager with the "Autostart" tab.

Viruses: If you detect excessive use of CPU by about 100 percent but do not find the cause, a virus or some other form of malware may be the cause. Viruses often do not appear on popular monitoring tools. If you suspect a virus, you should immediately check your computer with an anti-virus program or malware scanner.

Browser: Under certain circumstances, a browser (e.g., with countless open tabs) can use a lot of CPU processing power. Plug-ins and extras that are not available in the background are some of the reasons for high CPU. By regularly checking your browser settings, you can double check if you need all the extensions listed and turn off unused or underused plug-ins.

1. **How much RAM is attached to this machine?**

4 GB

1. **Do you feel that adding more RAM will fix the performance challenges? Why or why not?**

In general, RAM is faster, processing speed is faster. With faster RAM, you increase the speed at which memory transfers information to other objects. That is, your faster processor now has the same faster way of communicating with other things, making your computer more efficient

1. **What can be said about the disk performance on this machine?**

**RAM Memory Lack**

RAM memory is a temporary, "flexible" memory on your PC. Unlike archived memory, RAM only works when the PC is turned on. The app relies heavily on RAM for efficient operations. Not having enough RAM for the processes, you are trying to perform can cause your computer to slow down.

Today's computer needs, especially memory-hungry browsers like Chrome, require a healthy supply of RAM memory for PCs. In the early 2000's, computers needed only about 2GB of RAM. Today, a 64-bit system requires at least 4 GB of RAM, preferably 8 GB of systems used for anything more than basic office work.

RAM upgrade is a great way to improve the performance of your entire PC. But first, make sure that the lack of RAM leads to failure.

You can easily change the current RAM sticks on your PC. These sticks are straight to remove and replace with new rods.

**Hard Disk Drive is old**

A slow computer is one of the hallmarks of an old hard disk. The normal life cycle of a hard drive is between three to five years. While there are stories of hard disks that last for ten years, don’t rely on them.

In addition to the backlog, other signs may indicate that your PC's hard disk is worn out. Are there any strange sounds from a computer with lag? If your slow computer has a normal operating system freeze, then the hard disk may be too old.

You can replace the old hard drive. In fact, it is recommended before remaining in place of the green screen of death. A new hard disk drive will not cost much. It can be very expensive to upgrade RAM.

1. **How many disks are on this system?**

1 physical disk, 4 virtual disks

1. **What is the maximum number of disks that can be lost before you are unable to repair the array?**

RAID configuration comes in a few different forms, each with its own advantages and disadvantages. Some provide increased speed while others provide tolerance for errors. Let’s focus on tolerating errors and how many drives can fail in each configuration without damaging your system.

RAID 0: This setting is built for speed and allows you to use all of your available space. RAID 0 does not provide tolerance for errors. Any drive failure will cause data loss, so do not use this sensitive machine server.

RAID 1: RAID 1 configuration is best used in situations where power is not a requirement but data protection. This sets the mirrors on two disks so that you fail to dial 1 and can access your data.

RAID 5: This RAID setting offers the best value for money. RAID 5 gives you access to more disk space and higher read speed. Writing speed suffers a bit from this setup but you can withstand one driving failure and get it right.

RAID 6: Due to the unity, RAID 6 can withstand two disk failures simultaneously. This could be a failure simultaneously or during rebuilding another drive may fail and the system will still work.

RAID 10: This RAID can survive a single drive failure with the same members. It is a very fast setup with built-in redundancy and requires a minimum of 4 drivers to operate.

1. **Why would you not want to use RAID 6 for heavy IO use cases**

RAID 5 requires the use of at least 3 drives (RAID 6 requires at least four drives). It takes the concept of RAID 0, and then removes data from multiple drives to increase performance. However, it also adds a demolition feature by distributing unity information across all disks. There are many technical tools out there on the Internet that can go into details of how this happened. But in short, with RAID 5 you can lose one disk, and with RAID 6 you can lose two disks, and keep working with your data. RAID 5 and 6 will improve your learning performance. However, write functionality is highly dependent on the RAID controller used. For RAID 5 or 6, you will need a dedicated hardware controller. This is due to the need to calculate the unity data and write it to all disks. RAID 5 and RAID 6 are often good options for standard web servers, file servers, and other common purpose programs where most transactions are read and have earned you a lot of money. This is because you only need to purchase one additional RAID 5 drive (or two RAID 6 drivers) to increase speed and recovery. RAID 5 or RAID 6 is not the best option for a hard disk space, such as a database server, as it may damage your overall performance. It is fair to say that in the case of RAID 5 or RAID 6, if you lose the drive, you will offer to work smarter to keep your environment running. Once you have replaced the failed drive, the data will need to be rebuilt without any further information. This will take a significant amount of total performance of the same members. These reconstruction times continue to grow year by year, as the drive gets bigger and bigger.

1. **What does RPO mean and how would you explain RPO to your management?**

An RPO is a measure of time from a failure, disaster or event that causes the same loss. RPOs measure back when your data is stored in usable formats, usually going to the most recent backup. Renewal updates usually keep any data changes made prior to a disaster or failure. RPOs can also look at how much data can be lost before your business suffers significant damage, also known as tolerance for your business losses.

**RPOs can be used to measure:**

* How far it must go, go back in time from disaster to end when data is in usable format
* How often do you need to back up your data, even if the RPO does not represent additional IT requirements?
* How much data is lost following a disaster or event that causes a loss

**RPOs and automatic data backup**

If your business backs up its data every 24 hours, there is a risk of data loss within the last 24 hours. The same danger is true with data supporting every 12 hours, 8 hours and 4 hours of nauseum ad. If you intend to automatically set up your data backups, then the right times may be all that is needed to meet your RPO goals. Fortunately, data backups are automated, so most automated RPO strategies are easily implemented.

**RPO implementation and quantity**

Because data usage is less consistent and has fewer variations, RPOs are generally easier to use than RTOs. However, because recovery times are calculated based on all your performance and not just your data, the opposite is true. The time of day or day of the week when a disaster occurs can also affect your recovery time.

The most important applications often require multiple RPOs. For four-hour RPOs, the IT department needs to use scheduled summary duplication and near-zero hour backups require continuous repetition. When RPO and RTO are close to zero, continuous duplication will be integrated with failover services, creating a close 100% application and data availability.

It is noteworthy that having a consistent RPO, like every 12 hours, does not mean that you will lose 12 hours of data during the event that causes the loss. For example, if there is an application failure at 3 AM and IT restores jobs by 6 AM, you may not have lost data for 3 hours. This low risk of data loss can be caused by the fact that 3 AM to 6 AM is a very busy time for your app.

Similarly, say you have an RPO every 10 hours, there is a disaster at 1 PM and at 1:15 PM your jobs are restored. You will not need to retrieve all data from the last 10 hours, only data from 15 minutes ago.

1. **What is the RPO of this solution?**

**Disaster Recovery and RPO**

One of the problems with disasters is that people do not always prepare for them. In a perfect world, disasters can be seen far and wide, allowing enough time for everyone to prepare and respond. In that country, when a disaster strikes your business, your data protection infrastructure will recover immediately, and your data and applications will return to normal before time and point of failure.

In the real world, you may have to discard an application and duplicate the data for near-term loss, but the functionality of this recovery requires a lot of resources. Your IT department should establish a separate RPO depending on the importance of the application, as well as the budget and resources allocated to them. IT needs to create an RPO for your business.

**What is an RTO and how are RPOs different?**

RPOs and RTOs are key concepts for keeping the business going as function as business metrics to calculate how often your business needs to back up data. RPOs related to recovery time objectives (RTOs), represent the time it takes for a system to go from loss to recovery, and what needs to be done to restore the application and its data to its pre-disaster state.

1. **What kind of cluster is this - and how would you describe this kind of cluster to your management?**

At the highest level, a set of computers is a group of two or more computers, or nodes, running parallel to achieve the same purpose. This allows for workloads that contain a higher number of individuals, comparable tasks that should be distributed between collections. As a result, these functions can increase the combined memory and processing power of each computer to maximize overall performance.

To create a set of computers, individual nodes must be connected to a network to enable internode communication. Computer software can be used to connect nodes together and create a collection. There may be shared storage device and / or local storage on each node. Normally, at least one node is set as the leader node, and it serves as a group entry point. A leader node may be responsible for transferring incoming work to other nodes and, if necessary, consolidating results and returning feedback to the user.

Ideally, the collection works like a single system. The user accessing the collection does not need to know whether the system is a collection or individual machine. In addition, the collection should be designed to minimize delays and prevent nodes in node connections.

Types of Cluster Computing

Computer collections can generally be divided into three categories:

* + Very common or failed
  + Load balancing
  + High computer performance

As you will see in the next section, the three types of collections are very much in line with the potential benefits offered by the collections. If applicable, I will refer to the type of related collection after defining a particular benefit and how the collection provides it. It is also important to note that the collection may be more than one of the three types. For example, a collection that hosts a web server will likely be a very limited and loading rating group.

1. **What does RTO mean and how would you explain RTO to your management?**

RTOs represent a time when the application is low and does not cause significant damage to the business and the time it takes for the system to go from loss to recovery. This recovery process includes steps that IT must take to restore the application and its data to its pre-disaster state. By applying advanced quality applications, the RTO can be displayed securely in seconds, as long as the IT department has invested in failover services. RTOs require your IT department to first process applications based on their importance and risk of business loss. IT then allocates to these systems the right number of resources for your business, namely time, money and IT infrastructure.

**Determining the RTO**

RTOs are used to measure the time after a disaster in the IT department for information. Based on their research framework, RTOs represent the overall needs of your business and determine how long your business can survive without IT infrastructure and services. RTOs first need to be aligned with the potential of your IT department. IT managers need a strong understanding of the different types of recovery speeds to calculate an RTO that meets business needs. For example, a one-hour RTO cannot be met if a minimum recovery time can be two hours.

Because the process involves retrieving all IT services, RTOs are often complex. Your IT department can streamline another recovery process by doing as automated as possible. An RTO can cost more than a gross RPO, and the required RTO includes your entire business infrastructure and not just data. The cost of obtaining an RTO or RPO is in line with your IT department's priorities for applications and data. IT prioritizes applications and data in terms of revenue and risk. If application data is controlled, loss of data from that application may result in significant fines regardless of how often the application is used.

**Finding an RTO near zero or RPO**

While RTOs and RPOs vary in terms of system and data prioritization, it is incredibly expensive for any business to bring an RTO or RPO near zero to all of their operating systems. 100% downtime RTO and RPO lost data can only be obtained by investing in continuous data replication and in visible areas.

**Example of RTO**

The return of the granular object is one example of the RTO. In this example, a busy company user deletes an important email and empties the trash folder. The company uses Microsoft Exchange as a critical business plan and the IT department regularly sponsors delta-level changes in Exchange and a backup application that includes backup and recovery. This feature allows the IT department to quickly retrieve important email in about five minutes instead of retrieving a full-featured machine for only one email.

1. **What is the RTO of this solution?**

**Disaster Recovery and RTO**

Electricity. Theft. Damaged servers and hard drives. Cyberattacks and pebbles. Tornados, earthquakes and hurricanes. There are many types of disasters that can cause damage to your business if you are not prepared. Because these disasters are often inevitable, having a strong IT infrastructure and setting regular recovery times and targeting goals are essential to strengthening your recovery. Your IT department may not reject the application and duplicate your data with minimal losses, but doing so requires significant resources. Your IT department needs to establish an RTO based on the value of your application and the budget and resources allocated to it.

**What is an RPO and how are RTOs different?**

RTOs are subject to the point of recovery (RPOs), the amount of time that results from a failure, disaster or similar event that causes a loss. RPOs count back to the time when your data was last used, perhaps the most recent backup. RPOs and RTOs are important concepts for business continuity and are the business metrics required to determine how often your business should arrange its data backups.

**Strengthening resilience and disaster recovery**

There are many challenges to disaster recovery strategy, especially IT disaster recovery. These challenges include, but are not limited to, the following:

Workloads are still distributed in various locations the interdependence between IT infrastructure and use Restore all devices, components, and applications to the RPO and restore the business to full functionality System restore may also be delayed by receiving incorrect systems and applications.

What can be done to improve and bring about a successful disaster recovery plan in spite of all obstacles? Getting a few critical applications in a few hours is traditionally possible with the right IT team, but it requires a lot of valuable resources. The current needs of major RTOs and RPOs as well as system restoration where many critical equipment applications are quickly restored. It is now possible to reduce the impact of the disturbance and perform a recovery within minutes of exit. Automation is important, allowing disaster recovery programs to automatically increase workflow between a variety of applications quickly and reliably across switch to hybrid locations.

Today's robust orchestration technology helps you effectively use your disaster recovery strategy and reduces the downtime requirements of production time and business exposure due to expiration. In terms of preparation, resilience helps organizations successfully conduct disaster recovery tests with fewer employees. Strengthening resilience helps these organizations produce significant reductions in disaster risk management and reassurance. One of the legal benefits of orchestration technology is its ability to work in all areas of the body, visible and cloud while maintaining application awareness. As the limits of the self-employment agreement and lower level of services remain the expectations of end-users of cloud services, robust-oriented-based strategies are becoming increasingly important for today's businesses seeking cloud hosting.

1. **How could this disaster have been prevented?**

**Train users to discover the software**

User training greatly reduces the risk of infection. Ransom attacks often start with malicious email. Users can be trained to detect cyber threats including fraud, cybercrime, and social engineering. Users who are trained to identify harmful messages are less likely to open a viral attachment. Hackers sometimes use social engineering in their attacks. Social engineering is when an attacker attacks certain users on the network with high rights. Attackers bet that these users have sensitive information on local storage or have access to sensitive business plans and infrastructure. This increases the chances of the business paying a ransom.

**Keep the software separate and updated**

Make sure firmware, anti-malware applications, operating systems, and third-party software have the latest patch installed. Newer types of software are constantly evolving, and software updates ensure that your anti-malware detects new threats.

WannaCry is an example of an app risk. It included EternalBlue, a malicious attack by the United States National Security Agency (NSA). Used vulnerabilities in Windows Server Block Server (SMB) protocols. Microsoft has announced spots to stop WannaCry 30 days before infection. Except for patches, Windows operating systems are at risk. We recently saw ZeroLogon used in ransomware attacks.

**Always have backups**

The best way to recover from a backup is to retrieve data from the backup. Backups exceed the ransom requirement by retrieving data from a source other than encrypted files. Your hackers know this, so they upgrade the network that scans the network for backup files. After retrieving from the backup, you still need to remove the ransom from the network. An effective way to stop malware encryption backup files to keep a backup copy of your backups. Cloud backups are a common business option that requires a backup solution without it. Using cloud backups, you keep a copy of your files safe from ransomware and other cyber security threats.

**Discovering Ransomware**

A ransomware attacks often appear in a usable file or text that downloads a usable file and executes it. Not all hacking attacks occur quickly. Some dolphins remain silent for a day. For example, a ransomware version called Locker, CryptoLocker copycat, was silent until midnight on May 25, 2015, when it made its payment.

Network administrators receive freeware with applications that monitor suspicious network traffic. Apps send notifications when malware renames many files. Anti-malware software protects against thousands of types of malwares. Contains digital signatures that identify the ransomware before downloading. It doesn’t always catch zero-day attacks - those that point to weak engineers they don’t know yet.

Current anti-malware solutions include artificial intelligence (AI), machine learning and performance monitoring. These solutions measure the current file status against changes to file access requests. They warn managers of suspicious activity so attacks can be resolved early and prevent file encryption and data destruction.

**Early detection helps prevent it**

Effective freeware blocking requires a combination of good monitoring applications, common file backups, anti-malware software, and user training. While there are no cyber defenses that completely reduce the risk, you can greatly limit the chances of successful attackers.

1. **Can the backups be used - why or why not?**

A backup server is a type of server that simplifies data, file, application, and / or data backup. It has both hardware and software capabilities so you can manage and retrieve your backups - either based on location or remote backup server. With the use of a backup solution, a backup server is installed on the local network. When it comes to cloud deployment, a remote backup server is used. This means that the backup solution is sent off-site, for example to a data center. When it comes to using a remote backup server, a backup agent is installed on each machine that needs to be backed up - or selected equipment, in the case of wireless VM storage; with a local server, sometimes you do not need agents.

1. **Assuming a full backup was found - what does this change about your answer?**

Backing up the data is a good practice, if there’s a complete backup is found, its like a boon at the time disastrous attacks.

1. **What would you suggest to mitigate issues in the future?**

Importance of backup and restore data

The purpose of the backup is to create copies of data that you can retrieve if your primary data fails. Basic data failures can result from many problems including software or hardware failures, man-made event, data corruption, malicious attacks, and accidental deletion of data. Ergo, backup copies allow you to restore your data from the past to help your business recover faster from an unplanned event.

Storing a copy of your data in a separate location is required to prevent corruption or loss. An additional device can be as simple as a USB stick or an external drive, or even larger, such as a tape drive, disk storage medium, or cloud storage. You can set another route to the same location as your primary data or keep it remotely. If you are in an area with a lot of opportunities for weather-related events using a remote location is ideal.

For best results, make backup copies regularly and consistently to minimize the amount of data lost between backups. This means that the more time you spend between your backup copies, the more likely you are to lose data when you recover from a failure. So don’t wait months to make your backup copies. Also, keeping multiple copies of your data gives you flexibility and insurance to restore your systems to a location that has not been affected by malicious attacks or data corruption.

In IT, Disaster Recovery (DR) is part of a security plan, and it is done with a business continuity plan. It means policies and procedures that focus on protecting the organization or business from any significant consequences in the event of an adverse event, which may include equipment failure or construction, computer attacks or natural disasters.

Disaster Recovery is important in developing strategies that can help your business quickly recover Hardware, application, and business continuity data. It is sometimes regarded as the basis for business continuity. Designing an appropriate disaster recovery plan requires the preparation of a comprehensive business impact and risk assessment analysis. These steps help to identify specific IT services that can support the important business activities of your organization. They also help to set recovery time targets and rescue point targets.

Disaster recovery measures can fall into the following three categories:

* Preventive Measures: Strive to prevent the occurrence of an event.
* Corrective Measures: They are designed to repair the system in the event of a disaster or adverse event.
* Investigative Measures: This focuses on detecting and detecting adverse events.

Any sound disaster recovery plan helps you to achieve business continuity or in the worst of circumstances. It is also wise to keep checks and checks regularly to ensure that you have effective disaster risk management measures in place for all your departments and the organization.

**The Importance of Disaster Recovery (DR)**

Disaster recovery allows your organization to quickly recover or restart critical mechanical operations following a disaster. Today's businesses are more confident and tend to have higher availability while tolerance for leisure time is much lower. Ergo, a disaster can have serious consequences for your business, especially in today's highly competitive market. As businesses may fail after experiencing significant data loss, disaster recovery has become an integral part of operations.

The purpose of the recovery time (RTO) and the purpose of the recovery point (RPO) are the two measurements used in the DR and the rest period.

RTO: Refers to the maximum time after your organization's disaster to recover its files from storage and return to normal operation. In other words, an RTO is the maximum amount of rest that your organization can use. If your organization's RTO is two hours, it can't sit still longer.

RPO: Refers to the maximum file age your organization must recover from its backup storage to resume normal post-disaster operations. The RPO will determine your minimum backup frequency. For example, if your organization's RPO is five hours, your system should back up data at least every five hours.

Therefore, the RTO and RPO are very helpful in helping you choose the right processes, strategies and technologies for your organization. Strong integration with RTO windows will require you to position your secondary data in a way that makes it easily accessible when needed.

Restoration is another effective way to recover data quickly. It includes the use of technology that can allow you to move your backup data files to live status in your backup application, eliminating the need to move data over the network. This protects server failures and system maintenance.

Disaster preparedness requires you to take a comprehensive approach that includes software and hardware, power, communication equipment, communications, and testing to ensure that DR can be found within your RTO and RPO objectives. While implementing a comprehensive disaster recovery plan is no small task, its potential benefits are significant.

Without sensible data backup and DR system, your business is at risk of permanent data loss, unnecessary costs, and large downtime. Here are five compelling reasons to back up data with the DR program:

All information is Target: Whether you are an attorney, dentist, running a pet store, or a company with $ 500, your information is always at risk of threats. Accidents, viruses, malware, and hackers are not selective. They will attack your business for any number of reasons such as filling a vendetta, obtaining sensitive data, or just because they can.

Easy Data Loss: Many data losses occur as a result of hardware malfunction or human error in contrast to natural disasters. This means that your data is much easier to dispose of. Some data is very important: Some of your business data cannot be recovered if lost.

Rest time is not fun: Losing results on a rest date because without it, it becomes very difficult for your employees to work. It is difficult to manage clients without their account status and contact details or working without your sensitive business requests. In addition to the audio recovery solution in your area, your auto-recovery efforts are rebuilt.

Your reputation is important: The downtime and the loss of your personal information will affect how other stakeholders view your business and their relationship with you. Damaged reputation can seriously damage your business, especially when stakeholders cannot trust you with their information.

**Backup and restore software**

Database Management System (DBMS) refers to a software package that helps you manage data easily and efficiently, allowing you to organize your data efficiently. DBMS has many advantages, for example, it allows you to store, use, and retrieve data from information. It also gives you the ability to create transactions and provides protection for your data. You may also need audio backup and recovery software such as Veritas NetBackup.