Backup and Disaster Recovery in Schools

This white paper proposes backup strategies that could be employed by schools; the hardware and software that can be used; and the agreements within schools around data protection.

Contents

Introduction

Data on a school's network is ever increasing. With the extended use of the network throughout the school, larger numbers of people are storing more important data than ever before. The loss of data even for a short time can have a significant impact on the teaching and learning in your school. It is therefore essential that you always back up your important information and have a plan for recovering from a system failure.

With the rise in malware, viruses and ransomware attacks the need to ensure that your data is safely backed up becomes even more paramount. Should your school be attacked by ransomware, it will affect all your onsite systems and you will need to rebuild your network from scratch using uninfected data from a backup. As such a true test of backup success is the restore. Therefore, a 'backup' policy should be termed a 'restore' policy.

Before investigating the technology associated with backup, the most important thing is to understand the purpose of the backup and to whom it is important.

Understand your commitments

In a school, the owner of the backup process is usually the Network Manager; the owners of the data are typically the senior leadership team, the staff and the learners.

It is unusual for all parties to have the same expectations for the backup and possible disaster recovery of the network. The Network Manager is inevitably familiar with the day-to-day problems of managing large amounts of data across a complex network, whilst senior leadership may not be familiar with the practical limitations of the technology available.

Typically, a service level agreement (SLA) would define all aspects of the IT department's interaction with the school at large, allowing for both the IT team and its clients, be it the school's management team, the teaching staff or the learners, to understand and agree the levels of support available.

The SLA need not be long or complicated, but it should form the basis of agreed level of service and commitment. This will allow all parties to clearly understand each other's responsibilities and help to avoid conflict.

The generation of a complete SLA is out of the scope of this white paper. However, by way of an example, a SLA may well cover the following areas:

- **Scope of agreement** – this might state to whom the agreement will apply and the duration of the agreement (it might be limited to the duration of a school year to allow regular review and update of the terms of the SLA).
- **Scope of support** – this might define the systems and software for which the IT team are to be responsible.
- **Define support events** – establish an agreed definition of events, from routine maintenance events through to events that seriously disrupt system operation.
- **Response times** – this would establish the time taken to respond to different levels of event.
- **Definition of support available** – this could define the actual responsibilities of each of the parties in relation to the different elements of the IT infrastructure. For example, where a printer is located within a department, the replacement of toner cartridges and addition of paper may be designated as a customer responsibility, but the clearing of paper jams may be designated as an IT responsibility.
- **Regular system maintenance windows** – this would allow for the establishment of regular, mutually agreeable windows of system unavailability.
- **Procurement and testing of hardware & software** – this may well define the process for teachers and students to request the restoration of data.
- **Monitor and report on the performance against targets** – a key part of having a SLA is being able to measure performance against your declared targets and where necessary, review and make changes.

Understand the nature of your data

Rather than treat all your data as the 'same', it is good practice to categorise it. Good reasons for doing this include:

- As your data grows, you can ensure that the backups are completed in the most efficient way.
- When compiling a SLA, it will allow each category to have a level of service applied to it.
- When buying a backup solution, it will allow for accurate sizing and costing.
- When storing data, it will allow different levels of data security and retention to be applied.

You may want to consider limiting yourself to a small number of categories to enable easy management.

For each category that you decide upon you will need to decide:

The Recovery Point Objective (RPO) of the data

RPO is a term used in industry to mean how recent the backup of a file or data is. It is usually measured in hours - for instance, if the data has a five hour RPO, it means that a maximum of five hours of data is lost in the event or a file being deleted or a server recovery.

The standard nightly backup in a school allows for an RPO of 24 hours or one day. In the majority of the cases, this is acceptable to the data owners.

The Recovery Time Objective (RTO) of the data

RTO relates to the time taken to recover any lost data from your backup solution. Having a different RTO for different classifications of data will allow you concentrate on returning the most important data back into use as fast as possible, with the less important data following on behind.

How long you want to retain the data?

Understanding how long data is to be kept is important and will have a big impact on the sizing of your backup solution. Defining different retention periods for different types of data will allow the data owners to understand how long data is retained and allow you to optimise the use of backup resources. Some data may need to be kept for a longer period of time such as schools' financial data. The need for this level of retention might indicate that an archiving solution would be advisable.

It is important to note that the length of a given retention period is not directly related to how long a type of data may need to be kept. If a file is not being used it could be archived on the network for several years with a 1 month retention. A level of expectation will need to be set within your school of how long it is reasonable to expect a user to ask for a deleted file to be restored, and that length of time would be your retention.

Once you have your list of categories, you may decide, in the first instance, that the majority of these can be treated in the same manner. As time progresses you may choose to subsequently assign a lower level of backup service to different categories without the need to reengineer your SLA or your backup schedule.

Your categories could look like the following:

Category 1 Data – Information that changes on a regular basis.

- One day RPO – aim to restore data no older than 24 hours.
- Four hour RTO – aim to restore data in less than four hours.
- One month retention period.
- Data is unencrypted or encrypted.

This might include the following type of data:

- Network operating system and configuration data.

This would give you good 'granularity' of restore, allowing you to restore any file or data that has changed in the last month on a day-by-day basis.

Category 2 Data – Information that changes on a regular basis and has to be retained.

- One day RPO – aim to restore data no older than 24 hours.
- Four hour RTO – aim to restore data in less than four hours
- Two or three month retention period
- Data is encrypted.

This might include the following type of data:

- User data; shared areas, pupil / staff individual
- Your school management information.

This again would give you good 'granularity' of restore, allowing you to restore any file or data that has changed in the last month on a day-by-day basis and providing for the storage of data for up to three months. Also as user specific data is being stored, the data is encrypted to prevent unauthorised use.

Design and implement your backup solution

Once you understand the nature of your backup, you can design a solution to meet the commitments made as part of your SLA.

In any backup solution, you need to consider the backup software and backup storage. These are often considered as one and the same; however, it is important to ensure that the features of both are considered.

Backup software

When selecting backup software, it is important to look for the following features:

- **Flexible backup support** – the ability to support partial backups is important.
    - A full backup of a set of data is usually followed by either an incremental or a differential backup:
    - A differential backup backs up data added or changed since the last full backup.
- An incremental backup backs up data added or changed since the last full or incremental backup.
- **Flexible data selection** – the ability to select data based on your chosen criteria is important. This might mean the ability to select data based on:
    - Its location.
    - The type of data (video clip, document or spreadsheet).
    - The size of the data.
    - The age of the data.
- **Ability to span across media** – if you are planning to use removable media, the ability to span across media is important. Where the amount of data exceeds the individual tape or cartridge, the backup software must have the ability to seamlessly continue the backup on another tape or cartridge either utilising a media autoloader or through manual media swap.
- **Data encryption** – if your data is likely to contain learner specific information, the ability to encrypt data is important. For Cloud backup, onsite encryption is also key so un-encrypted data is not transferred over your broadband connection.
- **Centralised backup and management** – when backing up more than three servers it will be more cost-effective and allow for easier management to move to a centralised backup software suite. This allows the backup storage to be centralised and shared amongst multiple servers.

Backup storage

There are a variety of different storage media for your backup data, from traditional tape to cloud options. Whatever method you choose, it is important to consider the following principles when storing your backups:

- **Always ensure that your backup data is removable.** Backup destinations located on the network, whether disk staging or some form of network storage, are always at risk of hardware failure, disaster or theft. Ensuring that you can physically remove data from the network minimises the chance that it might be irretrievably lost.
- **Always locate your backup data away from the original source.**
  The safe and organised storage of your backup media is critical to the success of your strategy.
    - The backup media should be stored in a separate physical location to the backup solution and servers.
    - If your school has a separate building, then a secure room or cupboard with a purpose-built media storage safe would be ideal.
    - Backup data to an offsite datacentre, which is a low maintenance way of ensuring a copy of backup data is stored away from the original source in a secure way.

- **Always store media in accordance to the manufacturer's guidelines.**
  Some types of media can be susceptible to environmental factors, such as temperature and magnetic fields. Incorrect storage can lead to a total loss of data, usually discovered at the worst time.

Types of backup storage

- **RDX** – the RDX cartridge actually contains a hard disk, but is removable in the same way as a normal tape. The cartridge is shock resistant, withstanding a metre drop onto concrete.

The cartridges come with capacities of up to 4TB. The RDX drive can accommodate all sizes of cartridge, together with any future sizes without any requirement to change drive. It is expected that the cartridge capacity will increase in line with hard disk capacity.

The cartridge is designed to be used 5,000 times which typically equates to over ten years of use in an educational environment.

- **Disk staging solutions** – disk staging solutions utilise an array of hard disks as a backup destination. This increases the performance of the backup by utilising the speed of writing to disk and the ability to backup up multiple servers simultaneously. This is also known as Virtual Tape Library (VTL) technology, as the hard drives are often presented to the servers as 'virtual' tape drives. In some solutions, this maybe the only backup destination and, as such, might present a single point of failure in the event of a hardware problem.

- **Cloud storage** – Data is stored in large datacentres, where space is rented as and when it is used. This is the lowest maintenance and highest security way of storing data as the datacentres have high levels of redundancy and availability, with the data stored strongly encrypted and strict rules around who can see the data. This type of storage is often used to store 3rd copies of backed up data, and in conjunction with one of the above two onsite backup storage types.

- **Tape autoloader backup** – The traditional method of providing the 3rd copy of data. Tape autoloaders are used in conjunction with disk staging solutions. Although the autoloader does provide some automation to swapping tapes there still remains a manual element to managing the backup hardware.

It is recommended to follow the 3-2-1 rule of backing up data; 3 copies of data, 2 types of media, 1 different location. As such a combination of backup storage will need to be used to ensure an optimal backup solution is employed.

Maintain, monitor and test

Selecting and implementing your backup solution is only half the battle. The solution will need to stand the test of time. To enable this, you will need to consider implementing policies, processes and logs to ensure everything runs smoothly. These will:

- make it easier to measure the success of your backup in relation to your SLA commitments.
- make it easier to train new staff.
- help with managing the time of both yourself and any staff you may have.
- demonstrate a high level of competence to your Senior Leadership Team, LA and external inspection authorities.

A schedule for everything – knowing what to backup and when is critical to backup success. A clearly communicated schedule minimises the chances of missing a backup.

Roles and responsibilities – if there are multiple people responsible for the performance of your backups, you will need to clearly define each person's responsibilities. When deciding this, it is also a good idea to split some tasks to ensure that processes are double checked. This could help reduce the likelihood of human error.

A process for everything – the performance of backup can be a complex series of tasks. Develop a document that details all the steps required for each of the processes that are required. Example processes that might be considered:

- The daily maintenance process.
- The weekly maintenance process.
- The monthly maintenance process.
- A process for the recovery of deleted data.
- A process to test data recovery.
- A process for the adding or removing data from the backup schedule.
- A log of all backup activities to enable monitoring of backup success and failures.

Develop a disaster recovery plan

In the unlikely event that you have a complete disaster, you must ensure that you are in the best possible position to recover your network. A disaster recovery plan may not just be a sequence of technical tasks performed by IT staff to resolve a short-term problem, but it should also consider the following:

- communicating with the school at large, keeping people informed of progress and expected time for return to service. This might include the times for the different categories of data that you have to restore. For instance, this might mean the return of basic system functionality within four hours and the restoration of large multimedia files within two days.
- Long-term network unavailability. This is often termed 'business continuity', and concerns what happens to critical services if you cannot quickly return a system to full use.

Practical elements that should be considered as part of a disaster recovery plan are:

Hardware maintenance contacts – a full list of the various agents responsible for maintaining your equipment, together with any requirements they may have for logging a call. This might include serial numbers, for instance.

Operating system and server driver media – a full selection of the required operating installation system media and any required drivers for the server hardware should be duplicated.

Operating system installation process – the process required to install the servers operating system and backup software should be copied and stored.

Server information manifest – make a copy of the server configuration information. This should include:

- Server name.
- Server IP information.
- Server disk partition sizes.
- Server SAN connection information (if a SAN is installed).

All of the above should be duplicated at least twice and combined together in a 'kit'. This would minimise time required to locate the required information.

Reviewing your strategy

Having successfully implemented all of the above, a yearly review should be conducted. As part of the review, you may well consider:

- **Reviewing your agreed backup and recovery plan with your SMT. Does it need refining?**
- **Reviewing the service level agreement (SLA) with your teachers for recovery of lost/deleted files**
- **Testing the SLA has been met. If not, changes to the backup process or to the SLA should be agreed.**
- **Reviewing hardware and software maintenance required for your backup equipment.**
- **Reviewing that the processes are still relevant, and updating them if required.**
- **Formulating a purchasing plan for any new backup media requirements in the coming year.**
- **Reviewing any process problem or failures during the year and if any necessary action is required.**

Hopefully this white paper has helped stimulate thought and debate on the back up and disaster recovery strategies deployed in your school.

Find out more

RM.com/backup

Call us on **0800 046 9798** or email **networks@rm.com**

140 Eastern Avenue, Milton Park, Abingdon, Oxon OX14 4SB