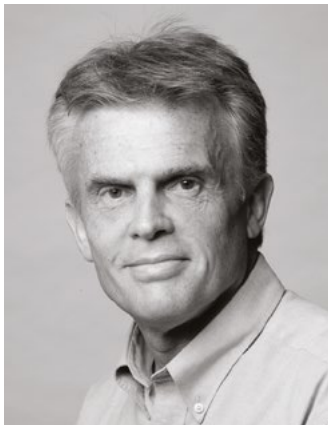
ICAEW INFORMATION TECHNOLOGY FACULTY

Data backup solutions

Ensuring the availability of your business data



Adequately protecting your IT systems is essential to survival. Knowing how to is also a potential source of consultancy fee income for your firm.

Chartered accountant and disaster recovery specialist Ian Cockburn offers **5 top tips** to help you choose the most effective solution:

1. Off-site backup of servers is a fundamental requirement. Cloud-based backup to remote data centres provides fully-automated protection that eliminates the problems associated with tape-based backup.
2. Ensure the service includes regular testing of the full server restore process so that reliability and timescales are fully understood.
3. Inspect the location to ensure it is a high-security Tier 3 (or in certain cases, Tier 4) private cloud data centre with suitably high-capacity bandwidth availability.
4. Make sure the backup maintains several data revisions, to allow restore of earlier versions in case of corruption, for example if a virus gets copied into the backup.
5. Assess the cost of backup and disaster recovery arrangements against the probability of any particular risk crystallising. The probability of data loss or corruption, or of hardware failure, is relatively high, so it is worth paying for a quality cloud-based solution.

For more top tips, visit www.rescueit.co.uk/toptips

To explore how you can protect your firm fully, increase your fee income and provide best advice to your clients, contact Ian Cockburn FCA, Managing Director of Rescue IT on **0870 60 90 999** or email **ian_cockburn@rescueit.co.uk**.

By Accountants for Accountants
www.RescueIT.co.uk

Rescue IT

Professional Online Back Up and Data Recovery

Contents

ICAEW's IT Faculty provides products and services to help its members make the best possible use of IT. It represents chartered accountants' IT-related interests and expertise, contributes to IT-related public affairs and helps those in business to keep up to date with IT issues and developments. The faculty also works to further the study of the application of IT to business and accountancy, including the development of thought leadership and research. As an independent body, the IT Faculty is able to take a truly objective view and get past the hype surrounding IT, leading and shaping debate, challenging common assumptions and clarifying arguments.
For more information about the IT Faculty please visit icaew.com/itfac

About the author

As a writer, consultant and researcher in the use of technology, Barnaby Page has worked over the last quarter century with firms including IBM, HP Europe, 3M, JCDecaux, Tesco, Target (US retailer), Planet Hollywood and Archant (one of Britain's biggest regional publishing groups). The author of a previous ICAEW guide on cloud computing, he has also contributed to numerous publications including eTrend, Display Monitor, the *Journal of Retail Analytics*, and *The Times*.

ISBN 978-1-78363-191-9

1 Introduction

Data is the lifeblood of most businesses – but many have no idea how long they could survive without it, or how much data they could actually afford to lose.

Those are the fundamental questions that need to be addressed at a high level of management in developing a business's approach to data backup. Which data is most important to a business, and which less so? What are the necessary objectives, in terms of recovery time and recovery point? In other words, how long can be allowed to elapse between losing data and getting it back, and how much can you live with losing permanently?

This guide considers the business benefits of backup, including the specific advantages it can deliver in terms of business continuity, disaster recovery, and other areas. It then looks at some of the major approaches to backup, at both the system and hardware levels, and at the factors beyond technology that must be considered, such as data protection.

Much of this relates to organisations managing their own data backup requirements, but we also provide an overview of special considerations raised by the use of third-party backup service providers. The growth of cloud computing means an entirely different approach to backup, in which it becomes essentially a contractual and service-level issue rather than a question of internal systems.

The guide also provides an overview of some of the many management issues involved, for example the role of backup as a part of broader business continuity and resilience strategies. These highlight the fact that backup is not merely a technology issue but one that can go to the heart of the business's survival.

2 What is backup and why is it important?

Key point

- Growing volumes of data and greater reliance on it, combined with increased cyber-security risks, all make backup more critical than ever.

A commonly-used definition for backup is 'copying and archiving of computer data so it may be used to restore the original after a data loss event'. But if this sounds like a routine technical process, we will see that it has implications much more profound for business.

Losing data in today's digitally dominated environment means losing information that is essential to the day-to-day, even minute-to-minute, conduct of the business. Backups are no longer just nice to have, they are critical.

Moreover, there may be greater risks than ever before. The direct linkage of business operations to IT systems means that much data is derived from recording conditions in the real world – the temperature in a refrigeration plant, for instance, or the fact that a parcel's recipient has signed for their delivery. And unless this is backed up, it could be lost forever when problems arise.

Data is also stored in a much more diverse group of locations than it once was: no more is it limited to the relatively secure data centre, but instead may be scattered across laptops, mobile phones and cloud-computing service providers. This diversity increases the risk of loss or data corruption, and means greater diligence is required to ensure all locations are backed up effectively. At the same time, hacking attacks are growing in sophistication and number.

So, four factors combine to make data backup an indispensable IT requirement on a larger-than-ever scale:

- reliance on IT that has increased to be almost total in many organisations;
- more data stored than ever before;
- data kept in more diverse locations; and
- greater risks.

2.1 CASE STUDIES

Having identified the reasons for putting an effective backup plan in place, it's also instructive to look at the potential pitfalls of failing to do so. The following case studies illustrate the possible consequences of not having a suitable backup plan.

Example 1:

The business had a website and a customer relationship management (CRM) system on a shared cloud platform. The cloud company they were using went out of business and consequently the platform went down. As a result they were unable to get access to the platform, and as they hadn't backed up their files, all of their client records were lost.

Example 2:

The business backed up data to an in-house central server which was also used to store other media. The server became infected with a ransomware virus that had inadvertently been downloaded in a file from the internet and subsequently saved on the server. As a result, all the backups became encrypted, as well as the other files held on the system. The outcome was that the business needed to pay the 'hacker' responsible for infecting the server a significant sum of money to decrypt the files.

Example 3:

The business paid a lot of money for an externally hosted, high-availability cloud platform. The platform was their own and was not shared with other users. It was not expected to ever go down and had built-in resilience and redundancy; as a consequence it was decided that no backups would be needed. Unfortunately the server was hacked via a vulnerability in some software and became a botnet that was

part of a larger malicious network. The server was found to have participated in various denial-of-service attacks and other illegitimate activities, and as a consequence it was seized by the National Cyber Crime Unit (NCCU). The service provider had no option but to comply with the request. As no backups had been taken, the whole system was offline and unavailable until a new platform could be recreated when the data was returned from the NCCU and the 'good' data could be transferred across. Subsequently the business was unable to continue trading.

Example 4:

The business scanned and stored all their working papers over time using a document-imaging software solution. The electronic copies were kept off-site on separate systems. A fire occurred in the business's offices, destroying all of the original papers. The business went to get the restored files, but discovered that they needed appropriate software in order to do so. Having searched online they found that the software company had been bought out by a larger one and the software no longer existed. All of their records were stored in proprietary format, so they were left with no option but to pay a specialist developer to write a tool that was able to re-convert the files and make them available in a modern, common format, which had significant cost and time implications.

3 Benefits of backup

3.1 DISASTER RECOVERY/BUSINESS CONTINUITY

Key points

- The main benefit of backup is avoiding the cost of not having it.
- Disaster recovery/business continuity in the case of serious IT problems or non-IT disasters is a major reason for backup.
- Without adequate backups, an organisation can suffer impaired productivity, lose business, encounter legal/compliance problems, and incur costs.

Backup has been compared to insurance: something you pay for and may never need, but may suffer greatly from missing. So its benefits are more the 'absence of negatives'; it is a way of mitigating the risk of data loss. In order to justify the level of investment that an adequate backup system requires, it is necessary to see the scale of the negatives that will be avoided.

The first and perhaps most obvious is permanent data loss. If data that is lost or damaged has not been backed up – or is not retrievable from the backup quickly, in a usable form, when it is needed – then in many cases it will be impossible, or at least highly impractical, to recreate this data. Every business has different data sets that are crucial to its survival, whether they are financial records, customer lists, work in progress, or something else. What would you do if they disappeared tomorrow?

The loss of data can also create compliance and liability issues, if the organisation is legally required to store the data. Equally it could compromise revenue-generating activities if the ability to fulfil a client order depends upon the availability of other data in a system.

In case of disaster, whether that is limited to IT systems or part of a broader occurrence (such as a fire at the company premises), properly-managed backups can help restore the business's data and systems close to the point at which they were before the disaster struck (recovery), and thus enable it to continue operating while keeping interruption to a minimum (continuity).

Of course, merely having a backup is not enough to achieve these things. It is just as important that the backup itself is insulated (for example, by being stored off-site) from suffering the same problems that afflict the main systems and also that there is a coherent plan for how data restored from the backup will – in practice – aid continuity and recovery.

This involves looking at the way data is used in the business, and indeed the way the business is conducted in general, just as much as focusing on the technical requirements of restoring the data.

For example, to avoid losing customers, it is important to decide which of the business's functions must resume most urgently, which data is most important to those functions, and which can wait.

An organisation's IT activity can often be split into 'core systems' which are needed for day-to-day operations – for example order-taking, or manufacturing automation – and 'supporting systems' that are no less necessary, but could, in a crisis, wait a short while to be updated, for instance HR or financial records.

Any assessment of backup plans and systems should take this into account, recognising that acceptable levels of loss and delay vary for different systems. Individual data sets can also be ranked in a similar way – some will be crucial to continuing operations, others much less vital. However, it should be noted that any loss or damage to personal data will be treated the same way by the relevant regulator, regardless of whether such personal data resides in 'core systems' or supporting systems.

The ranking does not have to be a simple 'core versus supporting' split – for example, systems and data sets could be ranked from one (most critical) to five (least critical).

There is a range of other considerations besides this important prioritisation. Will the backed-up data be easily available from substitute systems if the problem is of a scale that prevents use of the business's usual IT infrastructure? What will happen to those business functions that don't get their data immediately restored (the 'supporting systems') – will they be able to continue creating new data so that they can do at least some

work, and if so, will it be easily integrated with the old data once it is finally restored?

Where technology is concerned, one of the major demands of backup for business recovery and continuity is that it should be quickly usable – time really is of the essence, and the more critical a system is, the greater the urgency.

Even when it is possible to generate the data again, the business will suffer a considerable productivity hit from the time and effort required. It could, for example, mean re-entering information from hard copy, rebuilding complex spreadsheets or databases, or paying a specialist recovery company to rebuild damaged data.

The harm done to productivity can have a direct impact on revenue-generative business, for example by delaying the delivery of customer orders. This in turn can lead to loss of business and customer confidence, or liability costs.

In summary, the risks of inadequate backup can be described at a high level as comprising loss of revenue, compliance problems, impaired productivity and, inevitably, further cost to address the fall out from all of these.

3.2 OTHER BENEFITS

Key points

- Archiving can also have positive benefits to the business.
- Some backups may be required for compliance.

Archiving

Business continuity and recovery is for many of us what we first think of when we hear the word 'backup', in part because most of us have had the experience of a personal PC or laptop going wrong and our work being irretrievably and, infuriatingly, lost. But there are other strong reasons for backup which have nothing to do with IT problems.

One of these is archiving. There is frequently a desire to store all, or at least a lot, of the data an organisation generates over time. This might be in case there is a contract dispute, or an unexpected need to check engineering calculations when a problem arises, or more positively, a desire to always have the organisation's past on tap in case it can be learned from, for example through data mining. Many organisations are also adding at least some of their surviving hard copy records to their archives through digitisation.

As in a large library, the nature of this information is that most of it will rarely be wanted – perhaps never needed at all – but its completeness can make it valuable in itself.

It also tends not to be needed instantly, so the technology requirements differ from those for business continuity and recovery. The volumes of data may be extremely large, but they can be stored in a comparatively inaccessible way. On the other hand, because of the amount of data and the fact that you will want to recover very specific small parts of it, rather than getting a whole company IT system up and running again, the way in which it is organised and indexed can make all the difference to its practical value.

Effective archiving will not, however, just be a pleasant by-product of a more general backup strategy. Archiving has its own technologies and disciplines, which require planning and investment in their own right, for those businesses that can benefit.

Legal/compliance

In recovery/business continuity and archiving we have looked at types of backup which, essentially, the organisation makes because it needs or wants to. But there are other cases where it has to retain information by law, typically for a limited period of time. There are both general rules, for example those relating to the retention of accounting records (in the UK, HM Revenue & Customs requires each year's records to be kept for a further six years, or in a few circumstances even longer), and more specific rules for particular industries.

Some small businesses may find that the demands of this kind of backup are quite limited. But other businesses, especially those in tightly-regulated sectors such as gaming or pharmaceuticals, may find that retention of a huge amount of data is demanded by law.

Those more highly regulated businesses first need to get to grips with the technological and management challenges of ensuring that backups of the statutorily required data are actually made. But in addition they must ensure that these backups are robustly protected from tampering – especially important since they are among the data most likely to be involved in serious legal disputes.

It should also be remembered that not only may legislation require backups to be made, data protection rules also govern how long such data should be retained. This applies especially where personal data is involved. We discuss this in more detail in section 7.2.

4 Developing a backup strategy

4.1 SETTING RECOVERY POINT AND RECOVERY TIME OBJECTIVES

Key point

- A recovery point objective (RPO) and recovery time objective (RTO) for each data set are the essential goals of your backup strategy – everything else flows from these decisions.

We saw in the previous section that an organisation's data can be divided into 'core' systems, which are essential to its everyday operations and must be working again as soon as possible following problems, and 'supporting' systems, which are less of a priority.

Bearing this in mind, the business can start to develop its backup strategy by determining two key goals for each data set.

The **RPO**: this is the point in time to which data must always be backed up. For a particular data set, is it acceptable to lose a day's worth of data, or an hour's?

The **RTO**: this is the time that you can afford to wait for data to be restored. Again, this may be different for each data set.

The concepts of RPO and RTO are simple enough, but they are all-important in devising the backup strategy; it is therefore essential that they are determined for each data set with a very clear vision of exactly how the business would be affected in the event that data is lost temporarily or permanently. This is called a business impact analysis (BIA).

It is also crucial that the capabilities of backup technology are not allowed to influence the RPO and RTO – they should dictate the technology approach and not vice-versa.

4.2 MATCHING SOLUTIONS TO REQUIREMENTS

Key point

- Different backup solutions and approaches exist for different scales of business.

There are backup solutions for organisations of every size. At the very simplest single-user level, the 'solution' might be simply to copy important files to CD or a USB stick every so often and keep the installation disks (or online purchase details) for software. That very rudimentary system at least means that if the user's computer fails terminally they haven't lost everything. However, the tendency for people to forget to make manual backups is so well known that it's not an advisable route even for one-man bands, let alone larger organisations.

But that doesn't mean that every business requires a full-blown enterprise backup system, and certainly at the very smallest end of the scale, quite a simple approach can meet many needs. At this level, archiving needs are unlikely to be onerous (and occasional exceptions can probably be handled manually), while the volume of data required to be kept by law is also not likely to be great.

So it is possible that a single system will suffice for all three of the main backup objectives: recovery/continuity, archiving, and regulatory. Typically, this will take the form of a dedicated hard disk and software, attached to the company network, which periodically backs up data from the network's attached PCs and servers.

Some more cautious users may make further backups from this hard drive and store them off-site, although in practice many don't.

Cloud backups, where the data to be saved is sent over the internet to a remote backup service provider, are another option.

Irrespective of the solution, it is important to understand what is on the backup and how the data is structured, so that if it is necessary to restore data from the backup, you are not likely to exacerbate a problem by having to deal with unfamiliar technology.

Once an organisation is larger than a small handful of users, however, a more sophisticated system may be required, although the basic principles remain similar. As the business scales up, not only will there be more data to deal with, but it is also likely that the relative importance of central servers vs individual PCs will grow.

At this stage, a more powerful backup system capable of coping with those volumes of data becomes a requisite, and it will certainly operate at the level of the whole network rather than individual PCs. There is a wider choice of technologies; the growing scale – and importance – of the backup project also makes the choice of backup models more significant. (See section 5 for further details on both of these choices.)

A proactive approach to managing backup also becomes essential, rather than simply taking comfort in the knowledge that some backup is better than none (as the smallest users might). For example, decisions now need to be taken about future capacity requirements, about backup scheduling, and about the level of acceptable vulnerability. in other words, those windows of time when the most recent versions of data will not be backed up – how much can you realistically afford to lose?

5 Technology options

5.1 MODELS

Key points

- The backup model determines how data is backed up – for example, all of it, or just some of it.
- All models have pros and cons, affecting storage requirements, speed, IT-resource overhead, and the rapidity with which you can restore from a backup.

A range of backup models allows you to fine tune your backup system to the requirements of the business. Although the differences may seem technical, they can have an impact on the ease with which data can be restored, and the gaps of vulnerability. A basic understanding of the options can therefore help to inform your approach to backup and highlight some of the decisions that need to be made, even if implementing the technicalities will be left to a specialist.

It is important to note that choosing the backup model is distinct from choosing the backup medium, which we will look at in the next section, although the two are interconnected – for example, a model which requires constant copying of data from live systems to the backup will require faster storage media than one which only calls for backups to be conducted occasionally, such as overnight.

Disk versus file backups

A fundamental question is whether to backup individual files or complete disks.

Disk backup at its most basic makes a literal copy of a whole hard disk, byte by byte, including empty space, deleted files and the like. This is clearly a slow process, which is wasteful of resources, although modern systems do improve speed and efficiency through compression and by skipping some inessential data. However, this model has the advantage that you are assured your data is backed up exactly as it was held on the live system, and also that the backup system does not need to 'know' anything about the structure of the live system, thereby reducing compatibility issues – it simply copies everything that is there.

Types of disk backup include a **clone or disk image**, which saves not only your data but also all the other contents of the disk, such as the operating system's thousands of files, in a form that can quickly provide a fully working disk if the original one has problems. The idea here is that you go a step beyond backing up by creating an alternative, bootable disk which you can simply plug in and use. But this is potentially the most demanding kind of backup in terms of resources, which is unlikely to be necessary for anything other than the most business-critical systems, and not practical on a large scale.

File backup is a more common approach and is offered by a wider range of software. The concept here is that instead of backing up an entire volume regardless of contents, individual files are copied from the live system to the backup. This gives you more control over what is backed up and when – for example, you could specify more frequent backups for some data. Because there is less data involved, continuous backups are feasible, as well as backups to remote sites.

Full, differential and incremental backups

A further choice is among full, differential and incremental backups. The trade-offs here include the speed of backing up, the speed of restoring the backups when you need them, and the data storage requirement.

A **full backup** is exactly that – a complete copy is made of every file you have marked as needing to be backed up (which could be all files, or only a subset). Of course, this is slow to undertake and requires the most storage; however, because of its simplicity, it is the fastest to restore.

A **differential backup** is a twist on the full backup. A full backup is still conducted periodically, but in between the full backups differential backups take over, storing only those files which have changed (or been created anew) since the last full backup. Clearly this has advantages in terms of speed and data storage requirements.

An incremental backup is the fastest form of backup with the lowest storage requirements, although it is also the slowest to restore. Here, each backup just saves the changes since the last incremental backup – not the last full backup. This further reduces the amount of data that has to be stored each time, but, it also means that you need the complete set of backups (the initial full backup, then all subsequent incremental backups) to restore your data to its latest state. This makes it potentially less reliable.

Scheduling

It should be clear from the above that the scheduling of differential and incremental backups is a crucial factor in determining their usefulness. The more frequently they are made, the more current the backed-up data will be – but equally, the greater the overhead on all systems involved, on the network, and on backup storage.

A common approach would be one full backup weekly, and incremental or differential backups daily. The key question once again is how much data – or how many hours' work – you can afford to lose, although for any business, very infrequent backups are likely to be of little value.

Where a business is closed overnight, that is the natural time to perform backups without impacting system performance. For those that operate 24/7, scheduling can be a tougher challenge.

It is also important to establish how a proposed backup solution treats files that are in use at the time of the backup. If it skips them, it may not be providing as recent a backup as it appears.

Mirroring and replication

All the types of backup discussed above make copies of data and then essentially leave them alone until they are needed, other than deleting the oldest copies when newer ones are added. A mirror backup is a more dynamic form that frequently adjusts the actual backup so that it resembles – mirrors – the live data as closely as possible.

In a sense, it's a constantly-shifting full backup of a whole disk or selected parts of a disk (for example, a folder). The advantage of this is that the backup is up to date and ready to use as a substitute for the live data if the latter becomes damaged or unavailable. The downside is that mirroring by its nature only saves the latest version; previous states of the data are not available, and the mirror might even be backing up the sources of data problems such as viruses or corrupt files.

Mirroring on a large scale, for instance of an entire network rather than a single hard drive, can be termed 'replication'.

Then there is **continuous data protection** (CDP), which takes the mirroring principle to the extreme by saving every change to data, however minor, in real time. In theory, at least, nothing can be lost – but the bandwidth requirements can be considerable.

Some vendors address this by performing 'CDP' only at intervals, but then it is debatable whether it is really CDP at all.

5.2 MEDIA

Key points

- The choice of backup media is distinct from, but intertwined with, the choice of backup model.
- As with backup models, major considerations include cost and speed.
- Reliability is also a factor.
- Cloud backup is increasingly popular.

Most forms of backup involve copying data from hard drives (for example those on PCs or servers) to slower, but less expensive media. Slower is acceptable because a backup does not have to be constantly accessed in the course of day-to-day work; less expensive is desirable because the volumes of backed-up data can be sizeable compared with those in regular use. In this section, we look at some of the options.

Choosing a storage medium involves a trade-off among three factors: affordability, speed, and reliability. Any two of these can be achieved, but whichever you opt for, you will then have to compromise on the third.

At a more technical level, factors to consider when choosing storage media include the type of backup you have selected (as discussed in the previous section). This directly impacts both the amount of storage space needed and the speed of operation required. The volumes of data involved are also a consideration; for example, as we discussed earlier, some businesses bear a heavy regulatory burden which requires them to keep backups of vast amounts of data.

Moreover, in any kind of organisation, the volume of digital data is only likely to increase. Generous capacity planning is therefore essential to ensure that you don't run out. One rule of thumb suggests that businesses allow for 20–30% excess capacity – in other words, estimate how much capacity is needed over the next few years, then plan to invest in that amount plus 20–30%. This is likely to be cheaper and will certainly be less of a headache than having to bolt on extra storage in a hurry when your backup media suddenly cannot cope.

The various types of backup media and their associated advantages and disadvantages are listed below.

Magnetic tape

Magnetic tape has been the most common backup medium for long-term storage, but these days it is largely confined to older systems.

Pros: comparatively low cost, good longevity.

Cons: low speed of data access, requires dedicated tape drive hardware.

Optical media

Optical disks of various types (similar to CDs and DVDs) are another low-cost option and frequently used for small backups at the individual PC level. However, the use of jukeboxes (which, like their musical counterparts, automatically switch between one disk and another) can allow optical media to be employed on a larger scale.

Pros: data integrity – once a disk is written, the contents are fixed forever.

Cons: disks can become unreadable.

Hard disks

Pros: low and falling cost per megabyte.

Cons: complex structure compared to a tape or optical disk can also make them more prone to failure.

Cloud backup

As with all cloud services, cloud backup is purchased as a service on a pay-for-what-you-use basis. (Unsurprisingly, the term BaaS – for Backup as a Service – has already entered the IT jargon in a small way.) Data is sent over the internet to a cloud service provider, who stores it securely on their own systems.

Pros: as the customer, you are removed entirely from the details of storage media and other backup technology.

Cons: you are entrusting your data – and potentially the survival of your business – to another party.

5.3 SOFTWARE AND SYSTEMS

Key points

- There are innumerable backup software solutions on the market for every size of organisation, but they tend to share common features.
- Often they are sold as part of larger data or storage management systems.

Features

There are backup solutions for every size of business, ranging from simple utilities which schedule the copying of files from a PC to a local disk at set intervals, to enterprise-level tools. Increasingly, there are online options too.

Different packages support varying types of backup and scales of data. However, a number of core features are common, including:

- scheduling of backups;
- selection of different backup types (eg, full or incremental);
- selection of only certain volumes, folders or files to be backed up;
- compression of the backed-up data, to reduce storage requirements;
- verification of the backed-up data by comparing it to the live data to ensure integrity, and error reporting;
- file management, making information about backed-up data available, for example, when it was backed up and where the backup is held;
- encryption of backed-up data for security;
- restoration of the backed-up data; and
- deduplication of backed-up data to reduce storage requirements and network overhead.

Major vendors include CA Technologies, CommVault, EMC, HP, IBM and Symantec, but there are others too. Most vendors offer a full suite of options catering for different backup requirements.

5.4 LOCATIONS

Key point

- Choosing where to store your backups is a trade-off involving convenience, cost, and security.

Another choice that has to be made in developing a backup strategy is the location where your data is actually stored. This does not dictate the type of backup or the physical medium you choose, or generally the backup software either, although it certainly may be an influence – for example, a bandwidth-intensive approach to backup will be cheaper to implement locally than at a remote site.

The fundamental choices are local, where the backup is made and kept at the same location as the business, and off-site/remote, where the backup is at a different location. Online/cloud is a particular type of off-site backup where the precise location is often unknown, or at least of little relevance to you.

Local backup

The main advantages of local backup are that it may be simpler to implement and manage, especially for smaller single-site businesses, and that it can benefit from existing fast connections on the local network. The disadvantage is that if a non-IT-related disaster such as a fire affects the business premises, the backups could very well be destroyed along with the live systems – negating their purpose.

Off-site/remote backup

Backing up to a remote site, whether other premises owned by the organisation or a data centre where facilities are hired out by a third party, largely eliminates the risk that physical disasters will affect both the live systems and the backup simultaneously.

The downsides here are the opposite of local backup's advantages: long-distance network connections are likely to be slower and/or more expensive than local ones, while management may be more challenging. The involvement of a third party also incurs extra cost.

A halfway approach is to make backups locally, but store them off-site. In some smaller organisations this is as simple as the IT manager taking optical disks home each evening. It is clearly not an elegant or ideal solution, but does add a measure of protection.

At the other extreme, if you are transferring and storing data outside the EEA, there will be data protection implications – see section 7.2.

Online/cloud backup

As with storage media, location becomes a less relevant issue where cloud backup is concerned, but not entirely irrelevant. Many cloud providers offer services in other jurisdictions and there may be compliance implications (for example data protection – again see section 7.2) with storing your backed-up data in another country.

5.5 PHONES, TABLETS AND PERSONAL DEVICES

Key points

- New kinds of devices, especially personal ones, pose new backup challenges.
- They are best dealt with through usage policies, rather than technological fixes.

The ever-growing plethora of digital devices raises continual new challenges for backup – not just laptops but also mobile phones, tablets, and even the likes of Kindles or iPods.

One problem is that they are usually not permanently linked to the company network, so data may be added or changed but misses the next backup slot. Another is that personal portable devices, in particular, may well use idiosyncratic operating systems and file formats which a backup system developed for Windows, Linux or another mainstream IT platform won't recognise.

A third problem is quite simply that the number and variety of these devices is constantly growing and even if it is possible to tweak the backup system to handle them, making it compatible with every single device will be an enormous task, most likely far out of proportion to the benefit.

These issues are probably best addressed by policy rather than technology. An agreement on 'bring your own device' (BYOD) use with employees can mandate that they should perform their own backups, and that these devices should not be used to store the only copy of critical data.

But technology can help too. For example, a backup system may recognise when a laptop which has been absent from the company network for two weeks (eg, while its user was on a business trip) rejoins the network – and immediately start to back it up.

6 Backup for cloud users

Key points

- Backing up data already held in the cloud is a different proposition from backing up locally-held data to the cloud.
- The agreement with the cloud provider is of paramount importance.

We have already looked at some aspects of backing up to the cloud. But what if your IT is wholly or partly conducted in the cloud? For example, this applies to any organisation which uses software as a service (SaaS) applications such as Xero or Salesforce.

In this case, the major issues of backup lie not in technology but in management, and specifically in the relationship with the cloud provider.

Diligence must be performed on any cloud solution (as of course it should for all IT solutions). Specific points include the following questions.

- Where is the data held?
- What is the backup plan?
- What are the RTO and RPO?
- What guarantees does the cloud provider offer (in the form of a service level agreement (SLA))?
- What happens if data is lost and cannot be recovered – is the provider covered by insurance to compensate you?

The International Organization for Standardization is developing a new standard, ISO 27017, covering cloud-specific security measures and supplementing the existing ISO 27002 on broader information security issues. This is expected to be published in 2015 and should provide a framework for ensuring that cloud providers provide adequate data security.

You should also bear in mind that data protection issues gain even greater significance in the case of cloud computing – particularly those relating to the international transfer of personal data. Many cloud providers operate data centres around the world and if personal data is transferred to and from those data centres, potential issues could arise if such data centres are located outside the EEA (see section 7.2 for further comment on this issue).

7 Formulating the backup plan

Key points

- A backup plan calls for answers to all the questions discussed in the previous sections, along with many others.
- Cost is also a consideration, although it should not be the prime one.
- A backup plan needs to be integrated with wider-ranging disaster recovery and business continuity plans.

As we have seen, there is a wide range of technical solutions to the need for backup, but business imperatives still drive it. In defining the right backup approach, key questions to ask include the following.

- **What, where, when?** What data will be backed up, where will it be stored, and how often will backups be made? As we have seen, this involves identifying the different data sets held by the business, assessing the importance of each, and then deciding the appropriate recovery time objective (RTO) and recovery point objective (RPO).
- **Scale:** for example, how much data will be involved in each backup, and how much data in total will the backup storage media have to handle? How many devices, and how many different kinds, are involved? And how is this likely to change (realistically, to grow) in coming years?
- **The backup model:** as we have seen, choosing the right backup model is a trade-off between expense, fast and easy restoring of data, reliability, storage requirements, and other factors. Of course, more than one model may be chosen for different kinds of data within the business – again, the RTO and RPO for different data sets will dictate this.
- **Location:** many would say that an off-site backup is always preferable, for obvious reasons. How can it be achieved cost-effectively?
- **Long-term requirements:** can a proposed backup system cope with the likely development of your business and its data in the future?
- **Specific technical challenges:** some IT practices bring their own backup challenges. Older backup systems, for example, cannot cope easily with virtualisation. Unusual operating systems or file formats may pose challenges too.
- **Security:** most of the threats that can affect your live systems can affect your backups too, and it is easy to overlook them.
- **Transition:** once a technology solution has been chosen, how will it be rolled out and tested? Assuming some sort of existing backup system is already in place, how will the crossover period be handled? Will old backups need to be transferred to the new system?
- **What are the testing requirements?** A backup system must be tested regularly, not only to ensure that backups are being made, but also that data is actually recoverable from them – both in a usable form, and within the RTO for each data set.
- **What are the cost implications?** We suggested earlier that the main cost to consider when planning a backup strategy is the cost of not doing it, in terms of lost productivity and lost business. However, backup technology itself does of course incur costs – not only in hardware and software but also in human resource, although a well-implemented system should work without much active management most of the time. It is important here to figure in some of the less obvious costs, such as network bandwidth.

7.1 BACKUP AND DISASTER RECOVERY/CONTINUITY

Disaster recovery, resilience and business continuity as such are beyond the scope of this guide, but backup is clearly an essential part of them and therefore the backup strategy needs to be integrated with them.

How will backups be used in practice? In a given set of circumstances, which data will need to be restored, and where will it be restored to? (Note that this will very likely not be the devices or systems from which it was originally backed up.) How quickly will it be needed? Can a backup technology or service under consideration restore data accurately and rapidly enough, bearing in mind that there may be far more of it in the future than today?

Although again not a backup issue as such, it is also worth bearing in mind that backing up data does not make it magically compatible with future technology. If you need to restore today's data ten years down the line when the systems of 2015 are legacy technology, will it still be usable?

7.2 BACKUP AND DATA PROTECTION

Many organisations' backups will include large quantities of personal data, which fall under data protection rules designed to protect information about individuals from abuse.

While in the UK there is no specific limit on the time that a backup of personal data can be kept, the 'data protection principles', which underpin data protection regulation, state that you should 'retain personal data no longer than is necessary for the purpose you obtained it for'.

The Information Commissioner's Office (ICO) says you should:

- review the length of time you keep personal data;
- consider the purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for these purposes; and
- establish standard retention periods for different categories of information.

This clearly means that as well as classifying the different data sets you hold, according to their business value, and designing your backup strategy appropriately, it is also necessary to determine how long each type of personal data can reasonably be held and then establish a plan for securely deleting it once its time is up.

The ICO explicitly states that the requirements apply to backups as well as to live data. 'You should only archive a record (rather than delete it) if you still need to hold it,' the office says, and 'if it is appropriate to delete a record from a live system, it should also be deleted from any backup of the information on that system'.

More guidance can be found at ico.org.uk

The data protection picture becomes even more complicated when you consider backing up data overseas (or operating in the cloud).

Within the European Economic Area (EEA), you are free to move personal data around as you wish. The EEA comprises all EU countries except Croatia (which has applied to join), plus Iceland, Liechtenstein and Norway.

However, outside the EEA, the options are much more limited. As the ICO puts it, you cannot transfer personal data 'to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data', unless you are able to rely on any of the specific exemptions. These rules are not only applicable to your own IT operations, but also to those of a cloud provider who is holding data for you.

The EU Commission maintains a list of compliant countries.[1] There are currently only a dozen countries on the list, including the US.

Where the US is concerned, there is an agreement with the EU under which the US Department of Commerce operates the Safe Harbor Scheme. American companies registered in this scheme will, in theory, provide adequate data protection and can therefore store and process data on behalf of EU companies. However, the EU Commission has recently been critical of the system's enforcement, for instance questioning the provision that allows Safe Harbor members to pass data on to non-members by vouching for their reliability.[2]

It is also worth noting that many countries are giving their intelligence agencies widened powers to monitor and have access to digital data in response to the threat of terrorism. An example of this is the American legislation known as the USA PATRIOT Act, signed into law shortly after the terrorist attacks of 11 September 2001. This may weaken the compatibility of those countries' laws with European data protection rules.

More positively, there is a relatively new EU system known as 'binding corporate rules' (BCRs) which allows a company or group to transfer and process personal data outside the EEA if approved by data protection authorities within it. However, this is a costly and time-consuming exercise to implement.

This can be of benefit not only to companies with international operations, but also to those using service providers such as cloud computing firms. For their clients, the effect is that a cloud provider operating under appropriate BCRs will be compliant with EU data protection requirements even if it transfers data outside the EEA, thus addressing one potential headache induced by the move to the cloud. Another option to address this issue is to gain the express consent of the individual data subject to his or her personal data being transferred outside the EEA. You should be aware of any clauses in your contract with the cloud service provider which states that you have obtained the requisite consent from your clients or employees.

1 ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/
2 The list of Safe Harbor Scheme members is at safeharbor.export.gov/list.aspx

8 Conclusions

- Increasing volumes of data within businesses, greater reliance on it, and growing risks all combine to make backup more important than ever.
- Without adequate backups, an organisation can suffer impaired productivity, lose business, encounter legal/compliance problems, and incur costs.
- When developing a backup strategy, the most important decisions are setting RPOs and RTOs for each data set – everything else flows from these, including the technology choices. It is essential that these RPOs and RTOs are firmly based upon the business criticality of the processes that use/generate the data.
- Where technology and implementation are concerned, the RPOs and RTOs influence the choices of backup model, media, software and location.
- New technological practices, such as cloud computing and the use of personal devices for business, bring their own backup challenges.
- A backup plan needs to be driven by wider-ranging disaster recovery and business continuity plans.

9 Action checklist

All the questions in section 7 need to be studied, debated, and decided upon before a complete backup strategy can be formulated. The key action points required boil down to a few crucial issues, although other nuances (such as the cloud) may also prove important for individual businesses.

- Survey and list the current backup practices, formal and informal, within the organisation.
- Identify core and supporting systems by considering the impact on the business if any specific one was lost (section 3.1). A more granular ranking than a simple binary 'core' and 'supporting' can be used.
- Do the same with data sets (section 3.1).
- Identify regulatory/compliance requirements for backup – both general rules and any relating to your specific industry (section 3.2).
- Based on the above, establish RTOs and RPOs for each data set (section 4.1) and the other business requirements for backup.
- Ask: do your current backup practices satisfy all these requirements, and are they likely to continue to do so?
- If not: start considering the technology and deployment issues outlined in section 4.2 and onward.

Appendix A: Glossary

- **Business Impact Analysis (BIA):** an analysis of how business functions would be affected by disruption, such as damage to, or loss of, data.
- **CDP:** continuous data protection.
- **Clone:** a complete copy of a disk.
- **Cloud computing:** a broad term referring to an IT approach where, instead of a business owning and running all its own hardware and software, it uses the internet to access a service provider's IT systems and runs parts of its business on these.
- **Continuous data protection:** mirroring in real time.
- **De-duplication:** removing redundant duplicate copies of the same data from a backup, to reduce storage requirements.
- **Differential backup:** one where only changes made to data since the last full backup are copied.
- **Disk image:** a complete copy of a disk.
- **Encryption:** encoding stored data in a more secure form that cannot easily be deciphered by unauthorised parties.
- **Full backup:** one where all files are copied, regardless of whether or when they have been changed.
- **Incremental backup:** one where only changes made to data since the last incremental backup are copied.
- **ISO 27017:** an international standard, currently in development, covering cloud-specific security measures and supplementing the existing ISO 27002.
- **Jukebox:** a device for accessing data stored across multiple optical disks, automatically switching among them as necessary.
- **Live data:** the data in actual use by the business, as opposed to the backup.
- **Mirroring:** a dynamic form of backup that aims to ensure the backed-up data is always as close a copy as possible of the live data.
- **Recovery point objective (RPO):** in a backup strategy, this is the point in time to which data must always be backed up (eg, 'one hour ago' or 'one day ago').
- **Recovery time objective (RTO):** in a backup strategy, the acceptable time between losing data and having it restored.
- **Replication:** another term for mirroring, on a large scale (eg, a whole business rather than a single disk).
- **Restoration:** retrieving data from a backup so that it can be used as live data again.
- **Software as a service (SaaS):** a type of cloud computing where the service provider makes software applications available via the cloud.

Appendix B: Further information

- Introduction to Backup & Recovery
  youtube.com/watch?v=Zhz4d9xdPrI
- Introduction to data protection: backup to disk, tape and beyond
  snia.org/sites/default/education/tutorials/2012/spring/data/FrankHolliman_%20Introduction_to_Data_Protection.pdf
- Straight talk: Introduction to the cloud for data backup and disaster recovery
  itproportal.com/2014/09/19/straight-talk-introduction-to-the-cloud-for-data-backup-and-disaster-recovery
- The history of backup
  backuphistory.com

Big Data. Big Headaches. Simple Solutions.

Instant & Secure Access to your data

Cloud Backup from iomart delivers next generation intelligent data backup and recovery to protect your critical data in a simple unified solution. Using Tier 1 vendor technology solutions from our partners – EMC, Panzura & CTERA – we offer a choice of flexible, highly secure cloud storage and backup solutions which are centrally controlled and managed by you but protected by us. We own and manage – 24 x 7 - an estate of UK data centres in 8 locations, all accredited to ISO9001, ISO27001 and ISO20000 standards, guaranteeing that you data never leaves these shores.

FREE Consultation for ICAEW members
call 0800 040 7228 and quote ICAEW1

iomart

www.iomart.com/storage

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 144,000 chartered accountants worldwide. We provide qualifications and professional development, share our knowledge, insight and technical expertise, and protect the quality and integrity of the accountancy and finance profession.

As leaders in accountancy, finance and business our members have the knowledge, skills and commitment to maintain the highest professional standards and integrity. Together we contribute to the success of individuals, organisations, communities and economies around the world.

Because of us, people can do business with confidence.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com

ICAEW
Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK

T +44 (0)20 7920 8481
E itfac@icaew.com
icaew.com/itfac

linkedin.com – find ICAEW
twitter.com/icaew_ITFaculty
facebook.com/icaew

ISBN 978-1-78363-191-9 **£25**