13

Module 13

Hardware and connectivity

An increasing number of businesses are moving their software applications and storage to the cloud (see Module 8). Generally, this is faster, more secure, and easier to manage.

Before you jump ahead and make the change, you need to make a plan so that transitioning to the cloud is seamless and effortless.

In this module, you'll learn about internet connections and choosing the right service for your business, the benefits of cloud telecommunications, and how to make your current systems and hardware work effectively with the cloud.

Part 1: Internet Connections

Asymmetric Digital Subscriber Line (ADSL)

Most small businesses run an ADSL2+ Internet connection. ADSL is a shared Internet service that has a fast download speed and a slow upload speed. And because it's low cost, it makes a good choice for users who simply browse the Internet.

The quality and speed of ADSL is dependent on the number of businesses using the service at any given time. This makes both the speed and service unreliable, especially when making business phone calls through the Internet. It's also not recommended for sending and receiving large files.

Dedicated data services

If you are considering adopting cloud services such as remote storage, VoIP (which means…)and software applications that are delivered through the internet, then you will need a business grade dedicated data service to run these services in a reliable manner.

The following connections will give you the minimum service levels required:

- Symmetrical high-speed digital subscriber line (SHDSL)
- Ethernet over copper (EOC)
- Optical fibre to the premises (FTTP)
- National Broadband Network (NBN)

Redundancy

Redundancy means having two connections, should one fail.

If you're accessing cloud services, the internet connection has to deliver maximum uptime availability, so redundancy is extremely important.

When an upgrade to a more robust connection is purchased, most businesses retain their existing slower (ADSL) internet link for redundancy and configure their firewall to load balance if the primary connection goes off-line.

Modems, routers and firewalls

Dedicated services like SHDSL and Fibre will give you consistent upload and download speeds, which is necessary if you're going to use the cloud as a business tool.

As you transition to the cloud, you'll most likely need to upgrade your firewall to support:

- Load balancing (a networking solution that distributes incoming traffic across multiple servers, preventing any single resource from overloading);
- Traffic prioritisation (certain types of traffic are prioritised in busy times to ensure your network operates efficiently);
- Redundancy (an extra connection in case other connections fail).

This new hardware needs to be able to manage the following business processes, in conjunction with your upgraded internet connection:

- Manage day-to-day business use, including Internet browsing, accessing online software applications and transferring emails and files;
- Store your files off site and back new files up each day;
- Make phone calls and video calls of a business grade.

Part 2: Business systems hardware

Telecommunications

Moving to a cloud Private Branch Exchange (PBX), and a Voice Over IP (VoIP), has many advantages:

- Can replace a traditional phone system
- Easy to install with little downtime
- Can be self-managed
- Can run on multiple separate servers, which means no single point of failure
- As your business grows, you can add capacity to your cloud-based PBX
- Staff can access phone numbers from anywhere, at any time

It's important to note that upgrading your phone systems and handsets, and purchasing the dedicated data service you need to use VoIP, is a big investment. So before you start replacing your traditional PBX, consider its age and the lease on this equipment. It may be worth waiting until your current phone service is no longer adequate.

Servers, workstations and infrastructure

The most common IT setup is a hybrid of on- premises infrastructure and cloud services.

To ensure you have the right design for your IT hardware, you should review these categories: servers, networking devices, backup and disaster recovery, security, as well as your desktops, laptops, thin clients (a low-cost, centrally managed computer with no CD-ROM players, hard drives and expansion slots), smart phones or Macs.

Servers

A server is a central computer that is connected to your desktops (workstations, laptops, thin clients and tablets). A file server is typically used to stores files so that users can access and share these files from one location. A server can also run programs that many users share. These servers are called 'application' servers. Application servers run programs like email, accounting, and administration systems such as customer relationship management (CRM) databases.

If your server is over five years old, you might want to move some applications to the cloud, like accounting and email. You could also purchase a new server if you need to access large amounts of data.

When reviewing your server, remember to look at:

- the age of the hardware;
- associated warranties;
- hardware performance;
- how your server is being used for your business;
- what software you need to run or access; and
- remote access or multi-site access requirements.

If your server is still functioning well, make sure your on-site warranties are up-to-date, and that you have an access card for remote support.

Networking devices

When reviewing your networking devices, look at your router (usually supplied by your Internet Service Provider) and firewall.

In the cloud, it's important to have a redundant Internet connection (remember, this is a backup connection) as well as an appropriate firewall that can distribute traffic between multiple connections, provide content filtering, and offer anti-virus, anti-spam and traffic prioritisation. This way, you can allocate bandwidth for specific tasks like VoIP.

Backup and disaster recovery

When reviewing your backup and disaster recovery hardware, make sure you have an Uninterruptible Power Supply (UPS) that you can plug in to protect you from power surges, spikes or downtime.

Back up your data to the cloud or to a server. This ensures you'll never lose data, even in the event of a fire, theft or other disaster.

One of the best developments over the last 10 years is imaging software, a type of backup software that does more than just copy your data. Imaging software makes a full, exact copy of your hard drive every 15 minutes, including the operating system, applications, data and file organisation. When things go wrong, you'll have an instant fix – simply restore the image to the same drive or a new drive, and you're done. No valuable data is lost, and you can have your business up and running again within hours instead of days.

For security, check your firewall has the latest protection and content filtering, as well as an anti-virus and anti-spam solution for your email, desktops and laptops.

Desktops

When reviewing your desktops, laptops and hardware, think about replacing them every three to five years and make sure they have matching warranties.

Bringing your desktops, their operating systems and software applications up to date will mean lower support costs over time and greater efficiencies for your staff, because they will be working with the latest tools available to them.

Disparity between computers in the workplace, as well as between your business and your clients can reduce productivity by causing incompatibility of files and programs.

Bring Your Own Device

There's a growing trend called Bring Your Own Device (BYOD), which encourages employees to work on a device of their choosing. They could access corporate emails on their smartphone (iPhone or Android) or use a tablet such as an iPad to view documents.

It's a good strategy if you want to reduce infrastructure overheads, increase productivity and gain happier employees. However, keep in mind the security and standardisation issues that come with BYOD, in particular how corporate data is accessed on personal devices that you have little or no control over.

The most common BYOD policy extends to staff and company mobile phones. Consider having a mobile device management plan. What data can employees have access to? What security measures are in place if the phone is lost or stolen? How do you protect devices from hackers and viruses?

Further resources

If you want more information about protecting your customers and your business online, these resources may help. All information was current at the time of writing.

communications.gov.au/what-we-do/internet/stay-smart-online/computers/secure-your-computers - Online security and safety information for businesses.