

CPD - IT Services - Communications & Hardware

Jamie Warner, CEO, e-Nerds

Now let's talk about your communications. Moving to Voice Over IP (VoIP) may mean cost savings for all your phone calls. A cloud PABX will mean that the PABX in the corner could be made redundant.

Upgrading phone systems, handsets and your internet connection is a big investment and I encourage people to consider the age of your PABX and leases on this equipment before considering a complete replacement.

Though Cloud PABXs and VoIP is the future, there are still many reasons why an in-house PABX system is better suited.

Last but not least, we'll discuss your hardware.

What role does your computer hardware have when considering the Cloud?

As mentioned previously in the cloud video, the most common IT setup turns out to be a hybrid of on-premises infrastructure and cloud services.

To ensure you have the right design for your IT hardware, I recommend that you assess your IT requirements in the following categories:

Servers

Networking devices

Backup and Disaster Recovery

Security and your Devices (Desktops/ Laptops/ Thin Clients/ Smart Phones or Macs.)

Here are my top tips for each of these categories:

Servers

Tip 1

Check the age of the hardware. If it's out of warranty, this could represent a business risk.

Parts can become scarce on older machines, which means longer down times or even data loss should there be hardware failure.

Tip 2

If your servers are getting old, but they are still in warranty and are functioning well, then moving some applications to the cloud can reduce load on aging equipment.

Tip 3

If you need to upgrade your server, moving some applications to the cloud can reduce the cost of the new hardware upgrade.

Networking devices

Tip 1

As I've said previously, you need to have the right router, but in particular the right firewall. The right firewall can load balance between multiple internet connections, provide content filtering, for antivirus, antispam and traffic prioritization, so you can allocate bandwidth for specific tasks like VoIP.

■ Backup and Disaster Recovery

Tip 1

A UPS or uninterruptible power supply will protect your equipment from power surges, spikes or downtime.

Tip 2

Ensure you always backup your data either to the cloud or to a Network Attached Storage device or Server to prevent loss of client files.

Tip 3

The biggest advancement over the last 10 years is disaster recovery imaging software. This software takes a snap shot of your server's applications and data up to every 15 minutes.

In the event of a disaster you can 'mount' the image on another server and have your business operational within hours instead of days.

Tip 4

For security you need to check your Firewall to ensure it has the latest protection and content filtering. You also need to ensure you have an anti-virus and anti-spam solution for your email and for your desktops and laptops.

■ Security and your Devices

Tip 1

I always recommend you replace your staff's computers every 3-5 years and ensure they have matching warranties. This means you're providing your staff with maximum productivity as your applications and operating systems become obsolete over time.

Tip 2

You can also consider whether Bring Your Own Device (BYOD) is a good strategy for your business to reduce infrastructure overheads, however, you need to address the security and standardization issues which come with BYOD.

Once you confirm your business requirements as it relates to your hardware and software, you can then decide what the best design for your network will be, which these days, usually means a hybrid between on-premises and the cloud.

Thanks for watching this video.

These categories and key considerations are explored in more detail in Module 13 on the digital business kit or join in the conversation on LinkedIn.