

July

2019

In this issue...

Server
Replacement

Microsoft
Support End of
Life

Better Ways to
Use Office 365

Comparing Top
Business
Dashboards

Keeping Your
Email Safe



Considerations for server replacement

If you're thinking about replacing a server for your small business, then that probably means your company is experiencing success and is starting to grow. That's great news. But is it really time to invest in a new one? Or does waiting too long risk slowing your business down? Either way, it's important to consider your decision carefully. As a business owner, you should take the time to answer the following questions before deciding on your aging server.

When do my servers need to be replaced?

This is a difficult question, but there are two factors you will want to consider — age and performance. The useful life of a server is around three years. While it's not unheard of for servers to function properly beyond year three, relying on them beyond this point can be risky as hardware problems occur more often. This means you will have to deal with costly repairs and possible unpredictable downtime.


Performance is another factor to consider. Even if your servers are only a year old, it doesn't make sense to keep them around until year three if they are slow and too costly to maintain. It's important to do a cost-benefit analysis in these situations and look at how much money you will lose in repairs and downtime and then compare it to the cost of buying new hardware.

Do I have an alternative to buying new servers?

Believe it or not, the answer to your server problems might not necessarily be purchasing more physical hardware. One way to avoid this is by embracing virtualization. This process allows your servers to be stored and maintained off-site with everything being delivered to your office via the internet.



Microsoft Support End Of Life January 14, 2020

A photograph of a silver laptop with a black screen, sitting on a dark wooden desk. Next to the laptop is a small, clear glass hourglass with a small amount of yellow sand at the bottom. The background is dark and out of focus.

PRODUCTS:
Windows 7
Windows Server 2008 R2
Exchange Server 2010

END OF LIFE DANGERS:

- ✓ Security Vulnerabilities
- ✓ Software Incompatibility
- ✓ Compliance Issues
- ✓ High Operating Costs
- ✓ Poor Performance and Reliability
- ✓ Replacement Products Backorders

E-Safe is prepared and ready to help you transition to the latest operating systems and computers!!!

Stay ahead of the curve and contact us for a Microsoft End of Life Assessment to start planning your transition to avoid placing your business, users and customers at risk!

www.e-safetech.com

There are two notable benefits of virtualizing your servers. First, you don't have to spend a ton of money on new equipment. Second, virtualization is a scalable technology, meaning you only pay for the data capacity you use. For instance, if you only need two and a half servers, you can do that. This is in contrast to having physical equipment which would require your business to either make do with two servers or splurge and buy the third one even if you didn't need all of that space.

Of course there are a few things you need to consider before making the switch to server virtualization. One of the biggest issues is security. Ask yourself if you feel comfortable keeping all of your data off-site. While this isn't a concern for some companies, others may not see this as palatable. There are several workarounds to this issue, including the hybrid option where you keep sensitive data on-site and everything else off-site.

Can I do anything to prevent a full-scale server replacement?

Yes. It's certainly possible for you to buy some time and give your current servers additional life, but these are short-term fixes, not long-term solutions. Server upgrades are a good place to start if your servers are less than three years old but are degrading in performance. Installing additional CPUs or memory may increase server performance at a fraction of the cost of buying new servers.

You can also utilize old servers for non-critical workloads. It's possible to extend the life of servers that may have four or five years of wear-and-tear on them via repurposing. Instead of swapping out all of your servers, use the old ones for non-critical processes and purchase new ones to handle critical workloads. This will help you get a better ROI on your technology while avoiding a wholesale hardware purchase which could cripple your budget.

If you have any questions about your servers and how you can increase their performance, get in touch with us today. We can help you procure new hardware or show you the benefits of virtualization.



Better ways to use Office 365

With Office 365, your business can gain a lot, but you won't benefit from it if you don't know how to use this service. Do you want your employees to be more productive? You can't go wrong if you follow these simple steps to boost your business.

Get the staff aboard

To maximize your company's productivity with Office 365, make sure that every employee with a computer uses it. While this may be easier said than done, you can easily promote the service by encouraging the officers of your company to use it first. When your executives, managers, and top employees use Office 365, others will be persuaded to do the same.

Train employees

If your employees don't know how to use Office 365, they won't be productive, and the cloud service becomes a wasted investment. This is why training is vital. Teach your staff the ins and outs of the platform so they can take full advantage of it.

One way to train your staff is to make or assemble short training videos. These are easy to digest and will be remembered by employees. They can be viewed over and over again and used anytime. This saves management the trouble of training people.

Utilize core tools

When you first used Office 365, what did you like about it? You were probably sold on the idea that it increases staff productivity since it allows employees to work and collaborate anywhere. If you're not utilizing this service for that purpose, now is the perfect time to do so.

Some of the tools that increase productivity are OneDrive for Business (OD4B), SharePoint, and Skype for Business. OD4B and SharePoint allow employees to upload and save documents to a virtual drive, share that document with another group or user, and edit it at the same time. This gives everyone the ability to access that document and work wherever they want.

Because it is a flexible communication channel, Skype for Business also enhances productivity since employees, colleagues, and customers can communicate easily. From online meetings to conference calls, video calls to instant messaging, you have a wealth of options for instant communication.

Be more secure

Not only can a security breach cost you money, it can also destroy your business. While Office 365 already has built-in security with Azure Active Directory, it's always wise to be cautious of the files you add and share on the service. If you upload files with sensitive company information to the platform, make sure you control them.

These four productivity tips can help your business grow. If you'd like to learn more, or need additional training on Office 365, give us a call. We are happy to help you!



Comparing the top business dashboards

A dashboard is a single display that provides all the information you need to make important business decisions and manage your company. While dashboards are generally helpful, you need to choose the one that works best for your company's objectives and goals. Here are three types of business dashboards to consider.

Strategic dashboards

Ideal for senior managers and executives, strategic dashboards are designed to help identify potential opportunities for business expansion and improvement. This type of dashboard gives a bird's-eye view of your business and track performance metrics against enterprise-wide strategic goals.

They summarize performance over set time frames: past month, quarter, or year. They can contain anything from overall sales numbers to sales and revenue comparisons to inventory levels, making it easy for executives to understand the overall health of the organization and monitor the long-term company strategy.

Operational dashboards

Business owners use operational dashboards to monitor and measure in real time the effectiveness and efficiency of their employees' progress in relation to their targets. Since these dashboards focus on tracking operational processes, they are often more detailed than strategic dashboards and are usually viewed by junior levels of management multiple times throughout the day.

Analytical dashboards

When it comes to creating and implementing strong business strategies, understanding the trends and events in your data is crucial.

Analytical dashboards use volumes of data collected over time so you could compare current against historic data, enjoy in-depth analysis, identify patterns and opportunities, and determine why processes are working in certain departments. These dashboards present complex data, utilizing complex models and what-if statements, so they are commonly just used by staff with advanced training such as business analysts.

How do I know which dashboard to choose?

To help you choose which dashboard best suits your needs, you can ask yourself the following questions:

#1. What business problems are we trying to solve?

- Strategic dashboards – Top-line or organizational KPIs
- Operational dashboards – Data awareness and time-sensitive data
- Analytical dashboards – Trends or deeper insights

#2. Who will be using the dashboards?

- Strategic dashboards – Executives, directors
- Operational dashboards – Business managers
- Analytical dashboards – Business analysts, data analysts

#3. What are our goals?

- Strategic dashboards – Strategic goals, such as achieving KPI targets
- Operational dashboards – Employee awareness and tracking against goals
- Analytical dashboards – Analytic goals, such as visibility into key processes



Keeping your email safe

If you think your email is safe from hackers, think again. A lack of sufficient email security measures can result in data theft, unauthorized access to sensitive information, and malware attacks. Here are some tips to secure your email account from unwanted intruders and the many troubles that come with them.

Use separate email accounts

Most people use a single email account for all their personal needs. As a result, information from websites, newsletters, shopping deals, and messages from work get sent to this one inbox. But what happens when someone breaks into it? There's a good chance they would be able to gain access to everything else.

Having at least two separate email accounts will not only boost your security, but will also increase your productivity. You can have a personal account to communicate with your friends and family, while another is used solely for work-related communications.

Set strong passwords

Too many email accounts have predictable passwords. You might be surprised to learn that email passwords like "123456," "qwerty," and "password" are still the most common around. For the sake of security, set longer passwords (or passphrases) that contain a good mix of upper- and lowercase letters, numbers, and special characters. Make sure these passwords are unique to that account to keep all your other password-protected accounts safe.

You should also consider enabling multifactor authentication (MFA). This creates an extra layer of security by requesting for another method to verify your identity like a fingerprint scan or a temporary activation code sent to your mobile phone.



Beware of email scams

When you see a link in an email, don't click on it unless you've assessed its authenticity. You never know where those links might lead you. Sometimes they can be safe, but other times they can infect your computer with malware.

If you're expecting a file from your friend or family, then go ahead and open the attachment. It's always good to know the person sending the file. But be wary of attachments in emails from strangers. Even if the file name looks like a JPEG image, you should never open it. Attached files may seem harmless, but they may actually be a malicious program ready to latch itself onto your computer the moment you click on it.

These types of attacks are known as phishing and they can be remarkably clever. For example, cybercriminals may masquerade as high-profile companies like Amazon, Facebook, or the Bank of America to catch their victims off guard. They might even create a sense of urgency by claiming that there's an issue with your account, and that you should send them information or click on a dangerous link to "confirm" your personal details. Even if there was a genuine issue with your account, these companies would never ask something so suspicious over email. If you get these messages, contact the company directly through a verified website or phone number — not the contact details on the email.

Monitor account activity

Periodically watch over your account activity. Make sure to limit access privileges to apps if you want to ensure maximum privacy and security. Also, check for any suspicious activities in your logs like unusual devices and IP addresses that have accessed your account. This indicates that hackers may have successfully broken into your account. If this is the case, sign out of all web sessions and change your password as soon as possible.

Encrypt emails and update your software

Email encryption ensures that any message you send won't be intercepted and viewed by unauthorized users. Meanwhile, installing the latest updates for your anti-malware, firewalls, and email security software filters potential email scams and fixes any vulnerabilities hackers can exploit.

Protecting your email accounts from various threats can be a daunting process, but with the right support, it should be effortless. Talk to us today for all your cybersecurity needs.