WHITE PAPER

# Planning a Successful
# Move to Office 365

**By Tony Bradley**

## TABLE OF CONTENTS

Most businesses rely on the Microsoft Office productivity suite in some way, but the world of technology has shifted and Microsoft has adapted Office to shift as well with Office 365. You get the same software with either the traditional Microsoft Office license or the Office 365 subscription, but there are a variety of unique features and perks that make Office 365 a wise choice for most organizations. There are also some elements of Office 365 that raise security concerns as well, so it's important to understand what they are and what you need to know in order to make an informed decision about Office 365 and make the migration to Office 365 as smooth as possible.

*There are also some elements of Office 365 that raise security concerns, so it's important to understand what they are and what you need to know.*

## Office 365 Overview

Let's start with a brief overview of Office 365. Microsoft offers a variety of Office 365 plans. The exact pricing and features will vary depending on which plan you choose, but there are some core features and benefits that span most of the plans.

Most of the Office 365 business plans include licenses for the complete Microsoft Office suite for each paid subscription, including Word, Excel, PowerPoint, Outlook, Publisher and OneNote. Some of the higher plans also include Microsoft Access. Additionally, each business user can install and use Microsoft Office on up to five different PCs or Macs. Users also have access to the cloud-based Office Online versions of the core applications. Office 365 users also gain access to the full features and capabilities of the Microsoft Office mobile apps on tablets and smartphones.

Office 365 business plans come with hosted Exchange—which provides business class email, calendar and contacts with a 50GB inbox allocation, 1TB of file storage and sharing per user, and Skype for Business (formerly Lync)—with unlimited instant messaging and HD video conferencing.

## Moving to Office 365

So you've made a decision to move to Office 365 and take advantage of the unique perks and benefits. What impact or cascade effect will that have on your IT and data security? Should you expect to have less control?

If you're used to managing your own Exchange, SharePoint, or other servers in house the move to Office 365 is a bit of a culture shift. While Microsoft Office applications (i.e. Outlook) can still be installed locally on PCs, with Microsoft Office 365, Microsoft is now managing the servers (such as i.e. Exchange) for you in the cloud. There are a couple issues you should consider.

First is failover and recovery. How much will service degradation or downtime impact your organization? How much can you withstand? For example, for many, email service is mission critical. Take a look at how you've addressed those issues when managing your own servers and data internally and determine what measures you need to put in place to ensure an acceptable level of business continuity under Office 365.

The second thing to think about is where your data is stored. Data stored in the cloud in SharePoint or OneDrive for Business is exposed to a different set of potential risks than data stored in your own data center. Because Microsoft is managing the servers themselves you may have reduced visibility and fewer controls available—especially when it comes to installing and using third-party tools.

***Data stored in the cloud in SharePoint or OneDrive for Business is exposed to a different set of potential risks than data stored in your own data center.***

## Cloud or Bust?

Some organizations are more cautious than others when it comes to sensitive data and communications and may have reservations about moving to hosted, cloud-based services. The good news is that the managed services provided by Microsoft through Office 365 are not an all-or-nothing proposition. You can choose to keep some things in your local data center.

You can look at each of the Office 365 capabilities separately and determine on a case-by-case basis whether to take advantage of the Microsoft hosted services, continue managing it yourself internally, or take a hybrid approach.

You could keep email accounts for executives or other users that communicate about sensitive or confidential topics in-house while moving the vast majority of the company to the managed Exchange hosting provided with Office 365. Microsoft allows you to integrate the Office 365 services with internal systems—routing email through an SMTP relay for example. You may also choose to utilize the hosted Exchange for email, but manage your SharePoint server locally to keep sensitive data more secure.

If these scenarios apply to your organization you have to be prepared to monitor and support dual environments. The need to continue managing internal servers erodes the business case for Office 365 to some extent, but administrative overhead would be less with most accounts managed by Microsoft and the cost savings from switching to Office 365 could be used to offset risk and maintain a centralized view.

*The need to continue managing internal servers erodes the business case for Office 365 to some extent.*

## The Reality of Office 365 Adoption

Sales of Office 365 have been strong. However, there's a difference between buying the subscriptions and fully implementing all of the applications and services.

Microsoft Office speaks for itself, and the additional perks and benefits of Office 365 make it a tremendous value and a great suite of cloud productivity tools. Many organizations have paid for Office 365 but are reluctant to embrace it completely due primarily to potential security concerns.

One approach is to eat the proverbial elephant one bite at a time. It can be daunting to consider moving your entire productivity infrastructure to the cloud at once. Instead, implement one aspect of Office 365 at a time. Start with moving email to the hosted Exchange service provided by Microsoft through Office 365, then move on to other capabilities like document management or file sharing.

## Office 365 Security Considerations

The right time to weigh the security risks and implications of switching to Office 365 is before you begin the roll out. You should do your due diligence up front—ideally you should have considered the security ramifications before making a decision to purchase Office 365 at all so that security is factored into the budget. It is exceptionally difficult to go back and ask for more money after the budget has already been approved.

Microsoft is very conscientious when it comes to security so the default security measures put in place on Office 365 may be sufficient for many organizations. It's important to analyze the security measures available from Microsoft and determine whether or not they're sufficient for your organization.

Some specific threats or security concerns you should consider are:

- Protecting against targeted malware or phishing attacks via email
- Filtering and blocking unwanted spam—including snowshoe spam attacks
- Increased exposure to malware threats and potential compromise in the cloud
- Whether or not data in the cloud is encrypted while at rest and who manages the encryption keys
- How to prevent sensitive data from being uploaded to the cloud, and how data loss prevention policies applies beyond Office 365.
- Who has access to the servers and data

*Microsoft's AV engine and security policy updates can take an hour to propagate and the threat response window for the real-time protection is two hours.*

## Define "Real-time"

Microsoft claims that it provides 24/7 real-time protection. That sounds great at face value, but when you dig into the details it turns out that Microsoft's definition of "real-time" is different than you might think.

Microsoft's AV engine and security policy updates can take an hour to propagate and the threat response window for the real-time protection is two hours. A malware attack can yield significant damage in two hours, so you might want to choose to add third-party security controls that can detect and respond to threats in real-time in minutes.

## Tighter Security is Needed

Just as "real-time" has different meanings the approach to security itself varies from company to company. There are some industries that demand more security as a function of the information they deal in—things like banking and finance, or healthcare related companies. The truth of the matter, though, is that no IT admin thinks "We don't have very sensitive data so mediocre security is fine for us." Every organization wants the best security.

There is a difference generally between how smaller companies approach security as opposed to larger enterprises. Small and medium businesses just want security issues solved as quickly as possible and to return to normal business operations. They're typically not interested in the how or why behind the attack. Large enterprises, on the other hand, tend to want to investigate the root cause and source of the attack. They want to understand how the attack happened, who was behind it, and what the motive was.

*Organizations should make sure that the tools they choose for layered security are able to work seamlessly together.*

In either case it makes sense to take a layered approach to security for stronger protection. An attack that gets past one level of defense will hopefully be blocked by the next level. Organizations should make sure that the tools they choose for layered security are able to work seamlessly together. A centralized view and collaborative threat intelligence are both important elements of an effective layered security approach.

## Advice on Getting to Office 365

Trying to figure out how to get to the cloud is a primary concern. Don't make the mistake of focusing on thinking about how you're going to get there, or how long it will take, while completely overlooking how you'll get there securely.

It's rare for an established organization to do a forklift migration. Businesses have tools and processes in place already so moving to Office 365 is a process that takes time. The goal is migrate as efficiently as possible without sacrificing security.

Ease of management is important as well—especially when it comes to data protection and compliance.  Think beyond Office 365. Do you have sensitive data going to other cloud apps (Box, Dropbox), or need to protect data from day-to-day user actions such as printing, and removable devices. Consider how this may impact your security strategy.

## Keeping Perspective

Security is crucial. There are many potential security concerns when moving from locally managed servers to Office 365, but don't let that stop you. Statistically speaking, using on-premises hardware you manage yourself isn't necessarily more secure than cloud security applications or

Office 365. Some of the worst data breaches that have occurred happened to on-premises environments.

You shouldn't let security concerns prevent you from taking advantage of the cost savings and unique perks and benefits of Office 365. Just do your due diligence and understand what the risks and concerns are, and strengthen its capabilities with additional third-party controls where needed, so you're prepared to migrate smoothly and securely to Office 365.

***You shouldn't let security concerns prevent you from taking advantage of the cost savings and unique perks and benefits of Office 365.***

***Tony Bradley*** *is a technology author, speaker and trainer. Tony is a Houston-based independent analyst, marketing consultant and writer. He follows news and trends across all facets of technology, and helps people understand how the changing tech landscape affects them. He works with businesses to identify market opportunities and develops effective content marketing strategies to take advantage of them. Tony worked in the trenches as an information security consultant, an IT manager and a marketing executive. That real world experience gives him a unique point of view that lets him see things from the business perspective. He's been a CISSP for 13 years, and recognized by Microsoft as an MVP for 9 consecutive years.*

intel® Security