



FORTUNE FAVORS THE PREPARED

5 Questions to Ask Before Selecting Office 365™

Moving to Office 365 can bring many benefits to your organization. But just because productivity applications are in the cloud, it doesn't mean Office 365 can single-handedly protect your organization from socially engineered scams, costly downtime and data loss. IT is responsible for protecting the organization, no matter how the software is deployed, and for having a backup plan when something goes wrong. Additionally, end users will turn to IT, not to Microsoft, for help. IT professionals know that the same best practices for on-premises software deployments apply to the cloud, and they should be wary when considering Office 365. Here are five questions to ask before deployment.

1. Should I be worried about advanced threats like phishing, spear-phishing and whaling in Office 365?

The short answer is a resounding yes. Hackers don't care if your deployment is on-premises or in the cloud; they're still going to try to find a way into your system. You could even argue that going into a multi-tenant solution like Office 365 could expose your organization to even *more* risk. Millions of organizations are under that same security umbrella, so the payoff for a successful attack is greater.

The same security best practices that protect you on-premises are required for an Office 365 deployment. Email security breaches can cost your organization millions and destroy your brand's reputation. Implement multiple security layers to ensure you're protected from spear-phishing, whaling, social engineering and other threats if you move to Office 365.



2. Do I really need disaster recovery in Office 365?

No technology is foolproof, even from a company like Microsoft. Add in the human element, and there is always a chance for something to go wrong. Office 365 is no exception; it's run in data centers staffed by humans that, while highly trained, aren't perfect.

In the on-premises world, backups are standard, and not just for disasters. It was possible to go back to a known point in time and recover data that was inadvertently deleted. The cloud is no different; problems and mistakes happen and data could be lost.



3. Does Office 365 experience email downtime?

Every system experiences downtime, especially highly complex multi-tenant systems that are frequently updated. Customer service, productivity and overall revenue can suffer during downtime. Microsoft constantly releases new features, and over 50,000 customers are added to the platform every month. It's not a question of "if" but "when."

Every organization needs to consider and plan for Office 365 outages and take the necessary precautions for their unique requirements. If downtime strikes at 2 a.m. on a Sunday the impact will be minimal, but when it's in the middle of normal working hours, it could be a serious blow to the business – and result in very irate end-users. Consider how your business can stay up and running even if Office 365 goes down.



4. Is an independent archive important?

Putting all your eggs in one basket can seem very convenient, but Office 365 doesn't offer 50GB mailboxes because storage is cheap. Once it has your data, you're locked in to its basket.

But consider the future: Five years ago, you weren't even thinking about cloud collaboration software. It didn't exist. In five years, what will Office 365 look like – and will your organization still want to use it? With the way technology changes, it's wise to use an independent data archive to ensure portability, with an extra copy of the data in case something goes wrong.



5. Are the risks of an on-premises environment different than Office 365?

Email environments have changed a lot since the first email was sent over 40 years ago. As email emerged as the number one business communication platform, administrators added risk management and backup tools around their mail servers. Multiple code bases, redundancy and layers of security became standard operating procedure, despite the cost. It was required.

Now, with cloud-based services, it's tempting to skip the reinforcements used in on-premises environments. Some think you can trust a single vendor and a single company to handle the service, security and data. But that's a mistake, as the cloud requires just as much risk mitigation as on-premises software.



Snap Out Of It: Ask the Right Questions Before Selecting Office 365

Ultimately, Office 365 can be a great addition to an enterprise's IT portfolio, but it's not a magic cloud that will require little to no attention. Savvy IT pros will take the best practices for deploying and managing software on-premises and adapt them to their cloud systems. After all, you're not just migrating email to the cloud: your users, data and critical communication services are also being migrated. When Office 365 and Mimecast are combined, you have an additional layer of protection against security threats, service outages and data loss.

Let us show you how Mimecast can help you mitigate Office 365 risks while driving down costs. Visit www.mimecast.com or call 800-660-1194.

About Mimecast

Mimecast makes business email and data safer for thousands of customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email, and deliver comprehensive email risk management in a single, fully integrated subscription service. Mimecast reduces email risk and the complexity and cost of managing the array of point solutions traditionally used to protect email and its data. For customers that have migrated to cloud services like Microsoft Office 365™, Mimecast mitigates single vendor exposure by strengthening security coverage, combating downtime and improving archiving.

Mimecast Email Security protects against malware, spam, advanced phishing and other emerging attacks, while preventing data leaks. Mimecast Mailbox Continuity enables employees to continue using email during planned and unplanned outages. Mimecast Enterprise Information Archiving unifies email, file and instant messaging data to support e-discovery and give employees fast access to their personal archive via PC, Mac and mobile apps.

To learn more, visit www.mimecast.com.

