MOVE YOUR EMAIL To The Cloud With Confidence

Best Practices for Managing Risk in an Office 365™ World

mimecast®

Making email safer for business

There is a major shift in the world of enterprise technology happening right now. Many businesses are trading in their focus and investment in the LAN for the cloud, a move that brings virtually limitless data scalability, storage and accessibility – at a lower cost and with reduced complexity. In fact, enterprise adoption of numerous cloud applications, such as Microsoft Office 365™ and Salesforce, has almost doubled – and in some cases, even tripled – since 2014.

If you're a longtime Microsoft user, the logical first step in making the journey from on-premises to the cloud is to move your email to Office 365. You aren't alone. Office 365 is Microsoft's fastest-growing service, ever. And a recent study reveals Office 365 has overtaken Google Apps as the top vendor of cloud-based office productivity software.

QUICK FACTS:

35% of the Microsoft Exchange™ installed-base has already migrated to Office 365. Office 365

Results of a recent Mimecast poll indicated planned Exchange migration in excess of **50%** within two years.

Office 365 has been named "the most used cloud service" among **4,000** cloud applications.

So what’s the issue? If Office 365 is the cloud email management service of choice for a growing majority of businesses, it must be pretty flawless and risk-free, right? On the surface, it seems to check all the right boxes: resilient architecture, ease-of-use, decent security features, to name a few. However, what isn’t as obvious is the potentially risky new relationship you enter into when you become an Office 365 customer. The reality is, you become fully reliant on a single vendor – a world often referred to as a monoculture.

WELCOME TO THE SaaS Monoculture

Let’s talk about customer relationship management (CRM) software for a minute. Once you make the decision to work with a leading vendor, you experience what it’s like to live in a monoculture – one vendor for all, calling the shots, setting the security standards and establishing price at will. Barriers to switching vendors are pretty high, which puts you, the buyer, at a major disadvantage.

This same scenario is starting to take shape with Office 365. As more businesses move their mailboxes to the cloud, new risks become exposed. We depend heavily on email to do our jobs, and so much vital information is stored there. Choose Office 365, but consider the risks and impact this may have on security, continuity and data assurance.

As more businesses move their mailboxes to the cloud, new risks become exposed.

HERE ARE 3 RISKS To Consider

1

One Lock to Pick

An external-facing service, like Office 365, presents a potential open window for cyber-criminals. This multi-tenant environment introduces several points of attack – mailboxes, like yours – versus individual Exchange servers per company. The same single-vendor security protection for all Office 365 customers means a single lock to pick, and this increases each organization's risk exposure and vulnerability to attack. As Office 365 adoption grows, Microsoft and all of its customers become a more appealing target. Think back to when you were on-premises: you likely had multiple layers of protection – why would you forgo this practice when moving your mailbox to the cloud? You didn't rely solely on Microsoft to protect you then. Why would you now?

TOP 5 OFFICE 365 SECURITY GAPS

1 Security threats facing email evolve rapidly. And the security community identifies new threat vectors every day. One vendor won't quickly catch them all; the same is true of Microsoft.

2 The quality of Exchange Online Protect (EOP) is lacking, and it has no built-in overlay option or alternative.

3 Attacks on specific Office 365 accounts expose potential grid-level exposure for all users operating without additional security overlays.

4 Microsoft does not immediately solve vulnerabilities. With no overlay security cover, there's no protection while patches are developed and applied.

5 Sufficient security protection for threats, like spear-phishing, are not addressed by the default Office 365 offering.

2

Everyone's Eggs in the Same Basket

Office 365 is a real-time data environment and trusting it with all your email data is risky. Although Microsoft stores multiple copies, remember – they all reside within the same architecture and platform. This is a single point of failure. Email requires an independent backup and validation reference of critical, often regulated, information. If data is lost due to employee or admin error, corruption or technical failure, it may be irretrievable. In some cases, it may not be Microsoft's fault. But the fact remains: your data will be lost or corrupted for good without the right backup plan in place. You can't rely on Microsoft to keep an independent, verifiable copy of your data.

TOP 5 OFFICE 365 DATA GAPS: WHY YOU NEED A "PLAN B"

1. Misconfiguration of the Office 365 service retention rules, if unnoticed, could result in significant data loss or damage – you have to prepare for human error.
2. There is an inability to independently locate, review or verify the completeness and accuracy of data stored within Office 365.
3. Data loss or damage caused by technology failure could go undetected for extended periods of time.
4. Malicious authorized or unauthorized (stolen credentials) access to Office 365 could result in data loss or damage.
5. Office 365 does not allow you to restore all, part or point-in-time data by any other means other than using Office 365 data itself.

3 No Backup Plan for Your Email

With corporate email dependent on Office 365 being up, what happens when it goes down? It does, and will continue to, go down. System-wide, regional, feature-level and even tenant-specific failures can mean no email and no data while you wait for Microsoft to restore its service. This can impact both employee access to email and admin access to settings, policies and reporting. This is your responsibility, not Microsoft's. After all, the impact of downtime affects your business. And what happens when an entire market vertical, government entity, or even region of the world, experiences downtime at the same time? It is not a case of if this will happen, but when it will happen. As Office 365 adoption continues to grow, everyone needs to prepare for such a seismic event.

TOP 5 OFFICE 365 CONTINUITY GAPS

1. Risk of significant and long-term regional outage due to broadly impacting technical issues related to Office 365, such as feature updates or usage spikes.
2. Risk of significant outages due to isolated issues with Exchange Online, such as unknown technical glitches.
3. Client-level outages caused by hard-to-diagnose misconfigurations of the Office 365 environment by system administrators or Microsoft service administrators.
4. The increasing risk from DDoS attacks and other security breaches on Office 365 infrastructure, service or applications can result in significant and long-term outages.
5. Planned maintenance can result in an outage.

BEST PRACTICES FOR Managing Office 365 Risk

By now, you likely feel that moving your email to Office 365 can be risky for your business. But it doesn't have to be this way. You have options, like using an additional third-party complementary cloud service to help defend against cyber-attacks, downtime and data loss. How you manage risk from the outset plays a major role here: Do you have a "Plan B" in place if Microsoft is breached or goes offline?

There are two sides of the equation when it comes to risk management in the cloud. Use this checklist to find out if you follow adequate risk management practices.

Checklist: The Hope Club vs. The Plan Club

THE HOPE CLUB	THE PLAN CLUB
Hopefully, nothing will go wrong.	I know something will go wrong.
Risk management is Microsoft's responsibility.	It's my business, so risk management is my responsibility.
It's OK to act after disaster strikes.	I predict failure and prepare before an incident occurs.
It's OK to only have a "Plan A."	I have a "Plan B."
Management budget is not a priority.	Management budget is a must – I understand the potential cost of not taking action.
Cloud best practices are different from on-site.	Cloud best practices are the same as on-site.
Other companies might have a risk management strategy, but I don't need one.	Other companies have a risk management strategy, so I might be at a disadvantage without one.
I trust Microsoft when it says I don't need another environment.	I use an additional third-party cloud service to mitigate the risks of a single environment.

Whether you are a risk management hopeful or planner, we all have a role to play when it comes to protecting email and data in the cloud. Turning a blind eye to the pitfalls that come with relying on a single vendor unnecessarily increases your risk profile and potential for disaster. With the right planning and third-party cloud services, you can reduce your continuity, security and data-integrity risk and make the move to Office 365 with confidence.

Learn how Mimecast makes Office 365 safer for business.

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.