mimecast®

PLANNING FOR OFFICE 365 GAPS

Don't Hope for Cyber Resilience . . . ***Plan for It***

There is a major shift happening in the world of enterprise IT systems.

Many organizations are trading on-premises systems for cloud-based solutions, a move that brings virtually limitless scalability, storage and accessibility – usually at a lower cost and with reduced complexity. Global adoption of cloud enterprise productivity platforms hit an all-time high of 81% in 2018, up from 24% in 2014.*

If you're a longtime Microsoft customer, a logical first step in making the journey from on-premises to the cloud is to move your email to Microsoft Office 365™. You aren't alone. Office 365 is Microsoft's fastest-growing business, ever. According to Gartner, 84% of IT decision makers indicated that they are currently using or planning to use Office 365 in the next six months.

*Bitglass survey, May 2018.

So, what's the issue?

If Office 365 is the cloud email management service of choice for a growing majority of organizations, 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, and security features, to name a few. However, what isn't as obvious is the resilience gaps that occur when you become an Office 365 customer. The reality is, you become fully reliant on a single vendor for security, data retention and email continuity.

PLAN A CYBER RESILIENT MOVE TO **OFFICE 365**

Email-borne threats, such as phishing, ransomware and impersonation attacks, are leading to unprecedented financial and data loss, as well as negatively impacting productivity.

The best way to protect your organization is to implement a cyber resilience strategy for Office 365 that protects users, and reduces the risks resulting from technology failure, human error, or malicious intent. These risks only increase as more organizations migrate to Office 365, making it a higher-value target for cybercriminals.

What's an organization to do? The answer not to postpone your move to Office 365 but rather to plan the move carefully. Make sure you have a cyber resilience strategy that can address diverse set of email-borne threats; robust continuity options that solve for unplanned downtime; and the ability to recover lost, deleted, or corrupted data after an attack.

Three Office 365 Risks to Consider:

Ignoring the pitfalls that come with relying on a single vendor for resilience increases your risk profile and potential for business impacting losses. With the right planning, cyber resilience strategy and third-party cloud services, you can make the move to Office 365 with confidence. Consider the following three risks.

SECURITY

THE PROBLEM:

Cyberattacks Can Cripple Your Business and Cost You Millions

Cyberattacks , particularly those via email, are on the rise, and they are only getting more targeted, sophisticated and damaging. They can cost your organization millions of dollars, cripple employee productivity, result in downtime, and compromise your data. For example, actual and attempted dollar losses attributable to impersonation attacks have topped $12 Billion since 2013.

A massive multitenant environment, such as Office 365, can unfortunately lead to more risk. Because there are so many customers using the service, attackers will be especially drawn to it. The same single-vendor security protection for all Office 365 customers means there is a single lock to pick, increasing each organization's risk and vulnerability to cyberattacks.

THE SOLUTION:

Layered Cloud Security

Think back to when you were on-premises for your email. You likely had multiple layers of protection – why would you forgo this practice when moving your mailboxes to the cloud? You didn't rely solely on Microsoft to protect you then, so why would you now that you're in the cloud?

TOP OFFICE 365 Security Gaps

1. New email security threats emerge daily, and one solution that often relies on static lists, won't catch them all.
2. Office 365, protected by a single security layer on a single domain, could expose you to further threats.
3. Organizations with hybrid email deployments may not receive the security protection they need when using Office 365 alone.

ARCHIVING

THE PROBLEM:

Mistaking Data Redundancy for a Data Archive

Office 365 is a real-time data environment, and trusting it with all your email data is risky. Although Microsoft stores multiple copies of data it's important to remember that they all reside in the same architecture and platform, which creates a single-point-of-failure. If data is lost or deleted most solutions like Office 365, Salesforce and Workday aren't responsible. They can't control your administrators, users, or cybercriminals, so you need a plan to archive and recover the data that can't be lost.

THE SOLUTION:

Independent Archive

You can't rely on Microsoft alone to keep an independent, verifiable copy of your data. That isn't their gig. And, without the right backup plan in place, your data could be lost or corrupted due to human error, malicious intent, technical failure or cyberattack. Only by layering in a third-party cloud archive can you provide the best possible protection for your data.

TOP OFFICE 365 Data Protection Gaps

1. Office 365 users cannot easily locate, review or verify the completeness and accuracy of data stored within the platform.
2. Data loss or damage caused by technology failure could go undetected for extended periods of time.
3. Malicious or unauthorized access (stolen credentials) to Office 365 could result in data loss or damage.

CONTINUITY

THE PROBLEM:

Email Uptime is Essential for Productivity

Corporate email is dependent on Office 365, so what happens when it goes down? **It does**, and will continue to have outages or delays that can seriously impact productivity. Office 365 is a complex system with many components that must work together , including sending and receiving email; maintaining access to administrative tasks that control the service; and enabling access to archives and Active Directory for user authentication. If there is an outage, waiting for Office 365 to restore service can cripple productivity and frustrate users. You need to take control of your business continuity and not be relegated to tweeting about downtime.

THE SOLUTION:

Email Continuity in the Cloud

When email was on-premises, you relied on multiple instances of Exchange to keep the service running at all times. Now that you're in the cloud, you're completely reliant on a single platform with no secondary service in the event of an outage. The only way to ensure business continuity for your messaging platform is to layer in a third-party cloud solution that provides ongoing email service.

TOP OFFICE 365 Continuity Gaps

1. Office 365 carries the risk of significant and long-term regional outage due to technical issues or maintenance related to Office 365.
2. Azure Active Directory is a common approach to authenticate many Office 365 users. However, should Azure go offline, users are no longer able to authenticate, and in turn, access their email.
3. Various aspects of Office 365 go offline on a regular basis. And, while this may not be your live email feed, having long periods of downtime for administration or archive access can expose your business to risk.

Whether you plan for proper risk management or hope for it, we all have a role to play when it comes to protecting email and data in the cloud.

Ignoring the gaps that come with relying on a single vendor dramatically increases your risk profile and potential for a negative business impact. It doesn't have to be this way. With proper cyber resilience planning and the right third-party cloud services, you can reduce risk, protect productivity, and make the move to Office 365 with confidence.

mimecast

THE STATE OF EMAIL SECURITY REPORT 2019

Get answers to your greatest email security challenges.

LEARN MORE

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience.