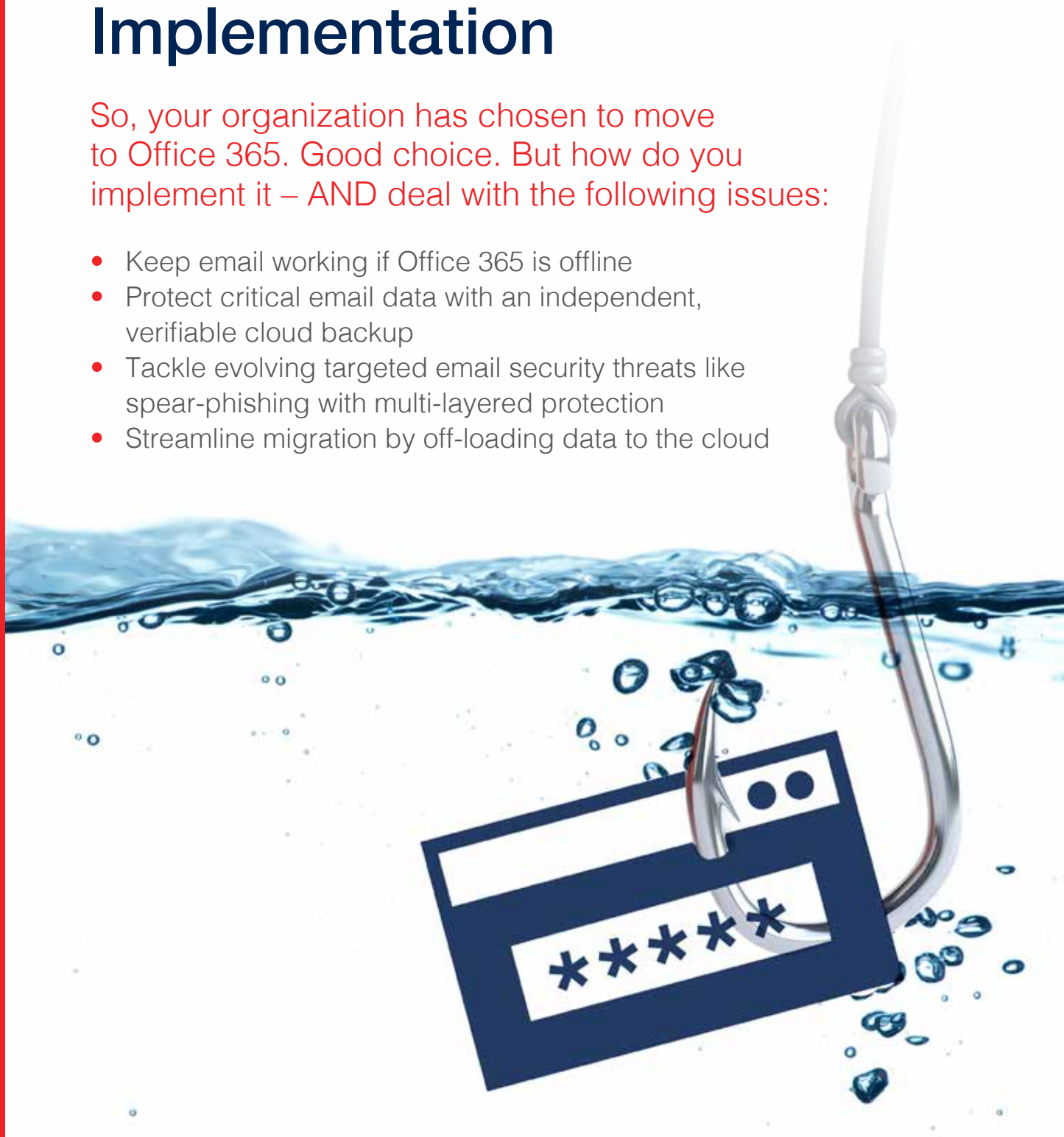
4 Critical Risks Facing Microsoft® Office365™ Implementation

So, your organization has chosen to move to Office 365. Good choice. But how do you implement it – AND deal with the following issues:

- Keep email working if Office 365 is offline
- Protect critical email data with an independent, verifiable cloud backup
- Tackle evolving targeted email security threats like spear-phishing with multi-layered protection
- Streamline migration by off-loading data to the cloud



Find out in this whitepaper.

CONCENTRATED TECH

Written by: Jason Helmick

In association with: mimecast®

It seems nearly every technology discussion today somehow involves the cloud – whether positive or negative, the cloud is a viable option in nearly every aspect of IT. With Microsoft's push to move Exchange environments to Office 365, the backbone in your corporate communication is now on the cloud "table" for discussion.

Now, this paper isn't about whether you should move to Office 365, or whether the cloud is the right strategy for your company - we're assuming you've already made that decision. But with that decision comes the need to plan both the migration and also how to ensure the same level of administration, security and message hygiene you've come to enjoy with your on-premises implementation.

There are a few considerations you should address internally when planning and implementing the move to Office 365. Often these considerations are missed in the rush to just hand over the keys to Microsoft, and make it their problem. It's worth taking the time to really think through some of the risks involved and how you can avoid them.

Consideration 1:

Mitigating Risk

With on-premises messaging, you've become comfortable planning and implementing multiple layers that provide high availability and disaster recovery - from server clusters and database availability groups, to redundant storage and networking, etc. Moving to Office 365, in essence, becomes the new single point of failure. Yes, there are redundancies built into Office 365, but from the standpoint of your business, either you can access Office 365, or you can't. It doesn't matter during a failure whether it's a server, a firewall, a storage array, whatever – all you know is you don't have access to email.

And the risk is real. We all hear the marketing about "five 9's of availability" from cloud-based vendors, but the reality is even those vendors go down. Two examples; Microsoft's recent nine hour outage of Office 365 in June of 2014 along with Google's brief outage in 2013 caused dramatic effect. Does having an outage like that mean you shouldn't move to Office 365 or use Google? Of course not. But it does illuminate the need to ensure you have a plan to maintain business continuity during these rare events.

Messaging Availability

You may have just read this and thought "Hold on a minute. Isn't that what I'm going to Office 365 for in the first place?" But, as it's been pointed out, even Office 365 can go down - as can any cloud provider. With Office 365, you have a number of places where failure can occur – email, online protection, even just authentication can all be subject to failure – so if you acknowledge the possibility of Office 365 being down, you'll need a plan on how your users will access and use email during that downtime.

With your own on-premises solution for Exchange, you likely have multiple servers, multiple data centers in different locations, backups kept with a third-party, and the flexibility to bypass any part of your infrastructure - including hygiene and security vendor solutions – easily, should any of it fail.

But when you move to Office 365, you no longer enjoy that same granular level of control. So how do you regain the control to ensure availability?

Just as you planned and implemented high availability in the past, along with multiple vendor support, you can do the same with Office 365 by inserting resilience from a third-party vendor. Unfortunately, in a scenario that involves your company moving to Office 365, there are no real good answers that don't involve a third-party solution to provide the messaging service availability you need - but in many cases the additional cost is minimal and easily justified.

Data Resiliency

Let's say Office 365 does go down, and you have a failover solution in place to allow your users to access their email. Messages come in (thanks to those custom MX records) and email can be sent.

But what about when Office 365 comes back online?

While it's a rather simple task to keep the failover solution's email up to date at the time of an Office 365 failure, it's an entirely different challenge to synchronize from failover solution to Office 365 when it comes back online.

Like the Messaging Availability, the answer lies with a third-party solution that addresses these challenges, as there are no solid "do it yourself" solutions.

Considering the Right Solution

Ideally, if/when you have an outage with email, online protection or even just authentication, your users shouldn't know the difference. The right solution should address rerouting of your email, provide seamless access (or at very least a web-based interface), integrate with your current authentication methods and automatically sync everything back when the lights come back on over at Microsoft.

The third-party solution should also have policies and procedures for efficiently handling an outage when they go down. It's just as important to have protection regardless if Office 365 or your third-party solution fails. In effect, you want to ensure that with at least one cloud vendor up and operating, your users and business will be protected.

Consideration 2:

Messaging Security & Hygiene

With on-premises Exchange, there are many choices of vendors to provide layers of security and hygiene for your messaging - some based at the gateway and some on the client. But when moving to Office 365, the options diminish significantly.

And that's a challenge, given that the threats of the day are not widespread like spam and viruses anymore; today's threats are far more insidious - targeted threats like DDOS and directory harvest attacks, or advanced persistent threat entry points such as spear-phishing. Emails actually housing a virus are rare these days, and often it's an attempt to get you to visit somewhere on the web that will infect you in order to gain access to the client machine.

Office 365 does utilize Exchange Online Protection, which will help address the spam and malware concerns, but it won't address the more advanced attacks that are realized at the connection level as well as at the email content level.

Considering the Solution

This Office 365 consideration is a bit easier to solve, however, be careful not to get drawn back into a traditional on-premises based security solution. Companies have been utilizing external email gateways for years, so the concept is nothing new. Because all email passes through these external cloud gateways, there is an opportunity for externally hosted message hygiene to compliment Exchange Online Protection. For most companies, the two differentiators a given hygiene solution will focus on beyond that of Exchange Online Protection are:

- **The range of threats it protects against** - sure, spam and viruses should be removed, but a threat can take other forms that require watching more than just attachments. The right solution will be watching for both widespread and targeted threats. In addition, strong and comprehensive protection from the cloud vendor lessens the need to manage locally installed anti-virus software. This is essential with mobile clients, such as phones, that may not have that software installed.
- **Storage of processed email** - legal and compliance issues concern themselves with emails with sensitive content being processed and remaining on the gateway any longer than required. The right solution receives, examines and sends on an email, without keeping any form of it resident on the gateway.

Consideration 3:

Archiving

When you think about it, Office 365 is a service that is always in the "now". That is, the service is about meeting your emailing needs as they exist today. If you were to want to retrieve a backup of a mailbox from last week, that's not in the "now" and is something Office 365 simply can't provide you.

You see, Office 365 has no tape with your company name on it, so there are, essentially, no backups or data resilience. Of course, Microsoft is backing up your data, but you have no access to it. The multi-tenant architecture of Office 365 doesn't allow your company to be able to retrieve a point in time for a specific set of data, as it is a real-time service only. Your data resilience plan should include a third-party vendor that can provide a store of data that can be recovered as needed.

Now that we've level set the backup capability, the topic of archiving suddenly moved from something of interest of "those companies with compliance or legal needs" to basically every company. In the case of Office 365, archiving is as much about retrieving data from a backup as it is about searching through archives of emails from the last few years. Now, Office 365 does offer Exchange Online Archiving that includes eDiscovery capabilities, but even that solution has limits to its retention. Additionally, given that you have no real ability to backup (and, therefore, recover) email to an earlier point in time, in the world of Office 365, the archive should be considered as a backup as well. Additionally, some companies may have a problem with the email and the archive being from the same vendor and want to see a different vendor solution providing the archive to ensure retention. Even if you choose to utilize a third-party solution, there are still some challenges you're going to face when switching from an on-premises Exchange environment to Office 365.

What to do With Your On-Premises Archive?

The first challenge you'll need to address is what happens to the archive you already have? It's not a clear-cut answer. Your on-premises archive houses email from years ago using a solution intended for use in your existing Exchange environment.

Moving to Office 365 may break some of that pretty quickly. For example, when you move mailboxes to Office 365, attachment stubs are broken, which makes your old archive somewhat useless. So you may decide to migrate everything – at which point, you'll find you have a ton of archived emails that have no value whatsoever (that should have just remained in the original archive) and will take a long time to complete a migration of a mailbox.

Should You Migrate Your Archive?

Most companies desire to make their messaging database as small as possible prior to moving to Office 365. But what if you actually do want to put your existing database and your archive into Office 365. You obviously can, but it's going to take some serious effort, time and thinking about the best way to ingest that data. You can't migrate terabytes of data over a wire quickly, so having a third-party solution that permits you to ship them a hard drive to build the archive quickly is something to consider.

What About Geography, Chains of Custody and eDiscovery?

For those of you with much larger enterprises that span multiple countries, you'll want to consider the ramifications of keeping your archives securely stored in specific geographic regions to protect your data from extradition while still providing proper access for eDiscovery.

Considering the Solution

There isn't an easy answer for this one. You've likely invested heavily into an on-premises solution and, quite frankly, once you move to Office 365, you're going to once again need to invest in a solution specifically designed to support Office 365. The issues of migrating your old data and/or archive, and facilitating desired access to those archives all need consideration. Look at the third-party solutions that assist in getting the archive built quickly and more importantly provide point in time recovery options. Having both the historical, and recoverable data, in the same place as current archive data provides a wealth of searchable and discoverable information.

Consideration 4:

Migrations

The actual migration to Office 365 will either be the easiest thing you've ever done, or one of the most challenging. One of the deciding factors is the size and complexity of your environment. If you are small enough, and on the latest version of Exchange you can simply "flip the switch" over, say, a weekend. Or, if you're so large or complex, you'll probably run in hybrid mode for a long duration of time. There are a number of factors (more than fit into this whitepaper) that will impact your migration strategy and plan, but we will stick to some of the higher level issues that definitely need to be addressed.

Multiple Instances of Exchange

To make this process even more complex, if your Exchange environment is large enough, you already think of the many instances of Exchange in terms of locations, regions, or administrative teams. So you'll need to determine what is the best way to make universal changes (such as your MX records) that impact the entire environment, while still being able to provide messaging to those same subdivisions of your current Exchange environment.

Multiple Versions of Exchange

While in dwindling numbers, it's not uncommon to still see Exchange 2003 or even 5.5 still out in production. This provides yet another level of complexity in that you may need to upgrade the on-premises solution first, before moving to Office 365. And if you've ever performed an Exchange migration of any kind, you can only imagine the challenges ahead if you're trying to migrate a number of instances of Exchange, each with a different version running, all at the same time.

Other Complexities

There are a lot of other smaller complexities that will come into play. Some of you will need to migrate over a period of years, all the while still requiring the unified administration, security and hygiene you enjoyed when using a strictly on-premises environment. You'll need to have administrative access to Office 365 and the supporting security and hygiene gateways that attempt to mirror what's in place today, while taking advantage of new policies and features you may want to implement as part of Office 365.

Considering the Solution

While on-premises Exchange and Office 365 provide (in a general sense) the same services, they are two completely separate platforms, each requiring administration. To address the administrative and security challenges alone when migrating, especially during a longer migration, neither Office 365 nor Exchange will be of help if you're looking for a unified answer. The right solution is going to further federate your Exchange and Office 365 environments.

CONCENTRATED TECH

Moving to Office 365:

You're Going to Need Help

Microsoft has worked to provide a robust and secure offering in the cloud that meets most business' needs. But if you are trying to create as much parity to your on-premises offering as is possible, you'll need to face the fact that additional third-party solutions are going to be needed. This includes the migration to Office 365, and the administration, security, and message hygiene you are used to today. The risk mitigation of data loss and outage are the most commonly overlooked aspects of moving to the cloud, and you may not want Microsoft to hold all of your eggs in their basket.

Your first step is to take a good look at what Office 365 offers for migration and operations, and identify the pieces that are missing from your current environment. Once you've done that, filling in those gaps with as few third-party solutions as possible will make your migration to and running of Office 365 a far smoother process, and one that keeps the business moving forward well into the future.

Jason Helmick
Senior Technologist,
Concentrated Technology