# Conversational
# Office 365
# Cyber Resilience

A ConversationalGeek® Book

Sponsored by mimecast


## Learn about:

- The value of a cyber resilience strategy for Office 365
- The security, data assurance and continuity gaps that exist in Office 365
- How a third-party solution like Mimecast can reduce risk and add resilience

2nd Edition

**By J. Peter Bruzzese** (Microsoft Office Apps and Services MVP)

## Sponsored by Mimecast

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

Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, compliance risk, human error and technical failure.


www.mimecast.com

# Conversational Office 365 Cyber Resilience

By J. Peter Bruzzese




ConversationalGeek®

J. Peter Bruzzese

# Conversational Office 365 Cyber Resilience

**Published by Conversational Geek® Inc.**

**www.conversationalgeek.com**



## Trademarks



## Warning and Disclaimer



## Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

## Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

| | |
|---|---|
| Author: | J. Peter Bruzzese |
| Project Editor: | Nick Cavalancia |
| Copy Editor: | Steven Zimmerman |
| Content Reviewers: | David Hood<br>Kelley Kirby |

# Note from the Author

Greetings!

You may find this hard to believe, considering the fact that I'm an 8x Microsoft MVP awardee for Office 365, but there was a time when I campaigned adamantly against going 'cloud' for your enterprise grade server services. I was Mr. Anti-Cloud. Nothing could change my mind. And then… I changed my mind.

I started to see the companies I consult with seriously considering the move to the cloud. CIOs were mandating the move, and IT admins were stuck trying to figure out how to make it happen and how to prepare for the worst. I made the decision to go 'all in' and immerse myself in Office 365 in order to be able to assist my clients to a greater degree. And in all honesty, I fell in love with it.

After nearly 2 decades (a score, if you will) of Exchange on-premises focus, I found it so much easier to let others worry about the hardware, upgrades, availability and so forth. However, I discovered there were some gaps. Areas of concern I had to mitigate. The before, during and after an attack/outage worries that every admin ponders. Risks that I didn't want to just hope and pray wouldn't hurt me. I isolated those risks… and found ways to mitigate them. This book will tell you what I discovered.

J. Peter Bruzzese

## The "Conversational" Method

We have two objectives when we create a "Conversational" book: First, to make sure it's written in a conversational tone so it's fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

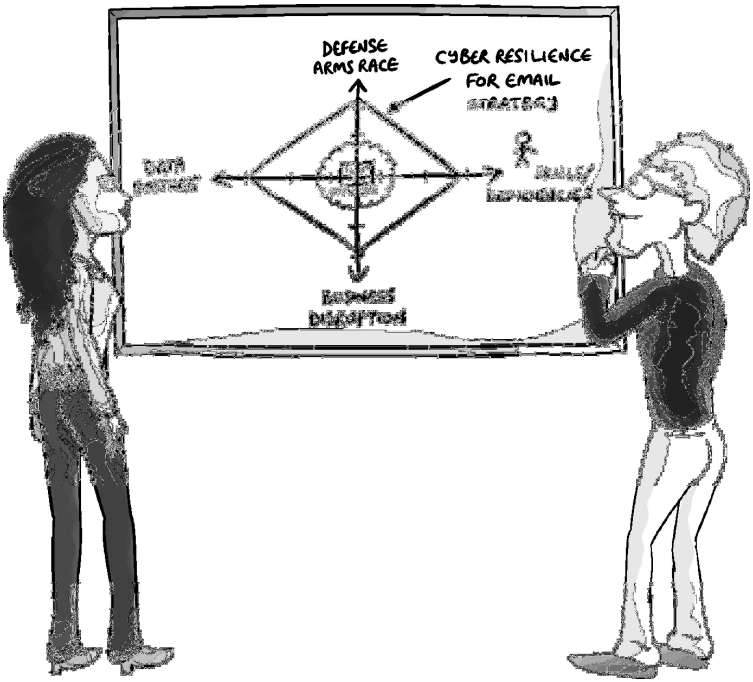
These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

## "Geek in the Mirror" Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it's the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these "geek in the mirror" boxes are not to be skipped.

Greetings. They call me J. Within these boxes I can share just about anything on the subject at hand. Read 'em!

# Cyber Resilience: Before, During, After




Email, arguably the most mission critical application, has always been at the intersection of a massive amount of risk. With on-premises Exchange servers we mitigated that risk by surrounding our Exchange server(s) with an ecosystem set of solutions from third-party vendors. We bolted on rather than make do with what was built-in. The objective? Resilience.

Exchange admins would purchase a security solution(s) with a secure gateway component. For compliance and eDiscovery we might have an archive solution. Perhaps a monitoring solution to ensure services are up. A must-have backup and recovery solution for DR and point-in-time restore capabilities. And the list continues.

We could choose a different vendor for each solution… or a single vendor if they had multiple solutions bundled together that met the criteria we were looking for (i.e. best of breed, best in class, personal favorite, Gartner magic quadrant, etc.). What we didn't do was deploy Exchange alone. You never see that in an enterprise environment. An Exchange server or servers…. and nothing else.

Moving our email to the cloud with Office 365 doesn't eliminate risk. One might say the risks not only remain but expand by moving to the cloud. Email continues to be the number one attack vector for cyber criminals. And the hackers, they have the advantage and it's a bit of a defense arms race.

Fear, Uncertainty, Doubt (FUD) is a common approach these days in selling bolt-on solutions. I'm not a fan of this morbid FUD approach. However, I do believe a realistic and healthy amount of fear, uncertainty and doubt (healthy FUD) is warranted when you consider the reported number of breaches, successful attacks and outages.

How do organizations address the challenges associated with changing infrastructure and ever-growing attacks? My advice is go back to what you know! Back to what works… but with a twist.

## Before

Looking at Office 365 from a security perspective it makes sense to ensure your security is layered. A defense in depth approach that considers a) the budget limitations you have, b) the number of solutions you can reasonably manage and c) the top risks addressed first and foremost.

Companies invest in data feeds and security analytics, they then need personnel to analyze the trends, assess risks and determine threats. Machine learning and AI aren't quite there yet, although we're seeing advancement in that area.

Budget varies, as does the number of solutions you can reasonably manage. As for top risks, some may think this is debatable and yet over and over it's been confirmed that 90+% of all modern-day attacks start with e-mail. A quote in the Wall Street Journal put the percentage at 97%. No matter the exact percentage, it gives us a focus point. We must do our best to place deterrents that give our people a chance against ransomware/malware, spear phishing, impersonation attacks and the like.

But we cannot have a defense-only strategy. In addition to secure gateway solutions we should be considering ways of strengthening the human firewall (the end-user) which has consistently been labeled the weakest link (and rightly so).

We need solutions that will help your human firewall to be more vigilant to bridge the skills/deficiencies gap. And you know what? There will still be breaches… still be outages… still be human error. So, no matter what you do BEFORE an attack/outage/error… you have to also prepare for the DURING and AFTER.

## During

When there is a breach, a successful attack or an outage business disruption… how do you ensure durability… or continuity… or availability?

After a breach or outage it can take hours to get your system back up. How do you continue the flow of email to your users,

while also maintaining the same high level of inbound and outbound defense and compliance?

Again, being defense-only in focus will not give you a during/after plan. Some think "well, if there is an outage I just have to sit and wait for Microsoft to fix it". Do you? Are there no other options to continue working? Where is the 'cyber resilience' in that plan? When has IT ever happily sat back and done nothing while waiting for a fix?

For example, most organizations realize and appreciate that Internet access is a 24/7/365 must have. But they know their primary provider may have an outage. Therefore, they allocate budget for a secondary connection with a third-party. That's resilience. A redundant connection. All organizations need to ponder the same line of thought in building their own redundancy, rather than rely on a single vendor.

## After

After a breach or outage event, how can you recover your lost email? Is your data being held hostage by a ransomware attacker? Do you have a way to recover it or are you going to have to pay and pray?

Can you recover your email, contacts, calendar, attachments? Can you go back to a point in time?

For this kind of protection, you can't simply trust a one-dimensional solution from any vendor. With today's sophisticated threats, and the precarious nature of SaaS solutions (no matter the vendor) anything can, and probably will, happen.

## The Big Takeaways

Microsoft provides a solid suite of solutions (with email at the forefront) in Office 365. At this point any organization type (government, finance, healthcare, etc.) has and should consider deploying it. At the time of this writing there are over 180+ million users.

Microsoft provides a measure of security, compliance and continuity (or availability) as part of their service level agreements to their customers. However, it's up to you to guarantee the overall stability of your entire email environment before, during, and after an incident. Just like we've done with on-premises Exchange.

In the on-premises Exchange days we bolted on enhancement solutions to ensure resilience. With on-premises you could bolt on different solutions to solve your needs… however, in a cloud-based world you want and need an all-in-one cyber resilient ecosystem. You don't want to daisy chain multiple solutions on to the front end of Office 365. That will lead to multiple points of failure and added latency. No… you need a solution that can wrap itself around Office 365 and provide true cyber resilience.

You can only do that with a cloud service that supports a cyber resilience strategy for email with total coverage across every dimension of your email environment.

# Cyber Resilience and Office 365

*"What happens if my chute doesn't open?!"*

Although I'm a supporter of Office 365 as a communication and collaboration solution, I don't believe a single-cloud approach is resilient. Two clouds are better than one. But there are reasons behind that thinking. It's not simply a matter of "well, I've always used third party solutions to fill the gaps and so I will continue to do more of the same". Obviously, the cloud brings change. I'm not buying the hardware or doing the upgrades (so I'm not adverse to positive change). But is Office 365 the be all and end all of resilience? I don't believe so and what I find odd is how many companies are simply folding their hands and sleepwalking into Office 365.

## Sleepwalking into Office 365

As mentioned, with our on-premises experience we rarely (ahem… never) see a greenfield or long-term deployment of Exchange that simply used what Exchange had to offer without reaching out toward ecosystem partners to provide improved services to surround and support Exchange. To enhance it.

So why is it when we move to the cloud, and move to Office 365, we fold our hands and just accept what is provided or built in? Why are we sleepwalking into Office 365?

Solutions architects need to re-invent themselves going forward to become cyber resilience experts. They shouldn't just give up, thinking 'oh well, it's all in Office 365 now, my job is dead'. They need to embrace their new place in the universe.

There are things Microsoft can do with a multi-tenant cloud-based version of hosted Exchange they couldn't do with the on-premises flavor. Because they have full control of the infrastructure, they can provide high availability using 'native data protection' that allows for multiple passive (and lagged) copies of your databases across datacenters to provide a fantastic high availability offering that would cost a company time/money/personnel to provide in-house. That's one of the many reasons I encourage folks to move to Office 365.

However, there are still gaps in the services provided that require a third-party solution (a unique, all-in-one solution) to help ensure the type of 1-to-1 experience you typically see on-premises due to the combination of Exchange and third-party bolt-on enhancements.

## Four Key Areas for Concern

We're not going to pick apart every little thing about Office 365 and Exchange Online. There is no point in doing that. It's a great solution, and priced right. I'm only going to hit the risk areas that make people nervous about Office 365. I'll explain what is built-in and why a third-party bolt-on would be better to enhance the overall solution.

## Security

Exchange on-premises (2013/2016/2019) includes an anti-malware solution and anti-spam agents. These offer very basic protection, so most enterprise deployments of Exchange look to a third party on-premises appliance or cloud-based solution to really cover themselves against all the bad stuff: spam, malware, phishing, spear phishing, whaling, impersonation attacks, ransomware attacks and so on.

Spear phishing is becoming a focal point for attackers looking to breach organizations' defenses, and it is very treacherous. It's targeted against a specific company, and has led to some major, high-publicity hacks, because there were no solutions in place to help detect the spear phishing attack.

Exchange Online comes with a free solution called Exchange Online Protection (EOP). It's enabled by default and provides basic anti-spam/malware/spoofing protection. Does it work? It does… and the EOP dev team is aggressively seeking to improve the solution. However, the last thing you want is to get pulled into a security monoculture, or homogenous solution. The term monoculture is defined as a community of computers that all run identical software and have similar vulnerabilities. Office 365 might be considered a SaaS Security

Monoculture if utilized without a third-party layered security solution approach.

On-premises, every company handles security a little differently, with a combination of vendors involved, multiple locks to pick and each company its own target. With Office 365 all tenants are together under the same security codebase, providing a very target rich environment.

Dan Geer, a risk management specialist and cyber-security expert, has repeatedly pointed out the problem of a security monoculture, especially with regard to Microsoft. His primary focus was on the number of Microsoft workstations connected to the Internet. But an even greater threat is to have a multi-tenant email solution monopoly (which is inevitable at this point) with a single security solution code base protecting all the tenants.

Think of the illustration "don't put all your eggs in one basket". Well, with Office 365 you're putting all your eggs and everyone else's eggs all in one big basket. Am I the only one who gets nervous about that?

EOP on its own doesn't protect against some of the recent attack types with weaponized attachments and links that make it through the first line of defense and into an end-user's mailbox. So, Microsoft offers a for-pay solution called Advanced Threat Protection (ATP). ATP is included with an E5 plan, or can be purchased per user (Plan 1 or Plan 2).

The threats that keep me up at night include spear phishing, ransomware/malware and impersonation attacks. And in my opinion both EOP and ATP aren't enough to allow me to sleep easy. I need more.

## Advanced Threat Protection (ATP)

ATP offers several additional protection features called Safe Attachments, Safe Links and Anti-Phishing. The concept is simple. Three ways the bad guys get to your end users (besides the easy-to-spot spam and attached known-virus attachments) are with attachments (that may appear suspicious but aren't KNOWN to be bad), with URL links that lead to sites that are "ok" when they first come through, but may become harmful on the back-end due to a targeted spear phishing attack, and with social engineering impersonation.

Safe Attachments: Safe attachments uses a sandbox 'detonation chamber' to check if the attachment is harmless. During the scan the users can view the attachment through 'dynamic delivery' if supported for that attachment type. Sandboxing offers the promise of zero-day detection capabilities (meaning it can spot a new threat if done properly). Sandboxing has its place, but it has a few holes in the use of the technology. For example, malware may know when it's in a sandbox and remains dormant. Microsoft's sandbox solution uses virtualization with Azure VMs to check for weaponized attachments. Virtualized sandboxing is easier for malware to evade whereas full system emulation is a better approach to avoiding detection and evasion of malware.

Safe Links: When a user receives an email, ATP analyzes URLs against a block list to start as part of a URL reputation check. At the time-of-click, it will perform a URL scan within a virtual detonation environment to check for a lure before allowing the user to continue to the site.

Anti-phishing: Detects impersonation attempts and custom domains.

Long story short, Exchange Online Protection (with or without the Advanced Threat Protection piece) is lacking. And it's lacking not just due to a feature comparison with third-party

options, because over time the gap in features will close. BUT… it will still be a single lock to pick, a security monoculture, and that is where a secondary bolt-on solution should be seriously considered. Don't just hope you're safe, know you're safe. PLAN to be safe.

I believe in defense-in-depth and the wisdom of a layered security approach. I promote end-point protection, DNS level protection, user behavior analytics, etc. And I'm a huge proponent of a third-party cloud-based security gateway with Exchange/O365. Especially if you're in a hybrid environment where some of the security features don't span multi-platform/vendor scenarios.

## Low Hanging Fruit (MXToolbox)

Imagine you're a thief looking to rob a home and you're looking at two big beautiful houses. The first sits on a wide-open property with no gates, no security system signs, no "Beware of Dog" or "Beware of Owner" signs, really nothing to indicate protection. And the second has a massive gate and fencing system with security cameras, a sign for a security solution that is noted as the best around, a "Beware of Dog" sign out front, and a "No Trespassing" sign. Now, which would you rob?

It's the same with attackers going after a company. Unless the motive is revenge (a disgruntled former employee perhaps) or corporate espionage/attack (competitive cyber warfare) many attackers are just looking for low hanging fruit. An easy target.

To start they might use a simple tool like MXToolbox.com. You can type in a domain name and quickly see where a company's MX records are pointing. Note the following results for two companies (Company A and Company B)

- Company A comes back as pointing to protection.outlook.com and the email service provider is listed as Office 365.

- Company B comes back with multiple MX points to a third-party security solution called Mimecast and the email service provider is listed as Mimecast (although it's actually Office 365).

Which would you choose to attack? The first one is using nothing beyond EOP/ATP. The second has an investment in security for all to see. You might assume, as the bad guy, that Company A is either unaware of the risk or gaps, or simply not willing to pay for better protection. That's interesting to you. What else are they NOT doing? Are they NOT training their end users? Do they NOT have other solutions to protect themselves? For lack of a better word, they are looking "tasty" to you as a cyber-criminal.

Some have asked, "if I pay for third-party security, am I not just paying twice for the same thing if I have EOP? Or EOP and ATP?" Well, if you are calling all three options "fences" then yes, you're paying for the same thing. But fences vary in size/strength/effectiveness. EOP is like a 2-foot fence that helps keep the anti-spam/malware critters out. ATP is more like a 5-foot fence that will help prevent mass malware/ransomware-type attacks, opportunistic attacks and such. But if you want a 10-foot fence with security cameras and sentinels and such you will need to seek a third-party solution.

## Recreate the Vault

Another factor to consider is the ability of the cyber-criminal to recreate your environment should they wish to test their attack methods out before hitting their target. We call it recreating the vault.

Have you ever seen Oceans 11? In the beginning of the movie George Clooney and Brad Pitt are stealing the plans for the vault. To rob it? Well, yes. But not at first. First they recreate the vault in a warehouse so they can practice robbing it first. See?

If you're using straight out-of-the-box EOP/ATP it costs less than $100 to register a domain name and set up a portal to play with that includes multiple account types. Now you can toss stuff at it and see what makes it through.

## Efficacy: One Drop of Poison

It's not what your security solution can *stop* that matters. It's what it lets through that you need to worry about. The efficacy (aka usefulness or value) of a solution cannot be determined by looking at a list of check boxes. "Does your solution do a, b and c?" Answer: "Yep! We can do a, b and c!" Check! Rather, the efficacy of a solution must be determined through genuine testing and impartial solution review.

EOP and ATP do work. They DO stop stuff. Spam/malware/ransomware and malicious links or impersonation attacks. They check some of the security boxes. But in testing I've seen results that indicate that it misses way too much for my comfort levels. Are you ok with that? Are you ok with having your human firewall, the end-users, be your last line of defense against modern threats?

In other words, are you ok with a glass of water that isn't *filled* with poison but just a drop or two? Drink up! Ahem… probably not. A third-party solution is a key bolt-on necessity to mitigate security risk in moving to Office 365.

In a recent whitepaper by Osterman Research it said, "many third-party solutions include the next-generation of detection mechanisms, such as recursive analysis of embedded documents, deep content inspection, static file analysis" and more.

## Data Assurance Archiving

Years back we didn't worry so much about archiving data, we worried only about backing it up. But with the many scandals (think Enron) and lawsuits cropping up that required the requesting of all email communication within a company, a need arose to provide eDiscovery in a much easier manner than going through backup tapes. The advent of archive solutions and eDiscovery allowed IT admins to prove compliance through discovery of data.

On-premises Exchange administrators reach out to the ecosystem of third-party solutions (software based, hardware appliance-based, cloud-based) to provide an archive of data. Assured data retention = discoverability = compliance (which means no fear of fines or jail time for the IT admin).

Exchange on-premises does NOT include an enterprise grade archive solution. And guess what? Neither does Exchange Online.

I say this and I can hear some of you responding with "but wait… doesn't Exchange have an 'in-place archive' feature?" I cannot tell you how frustrating that naming is to me. Yes, it does have that feature. And I like it. But it's poorly named in

my opinion. I believe it should be called a 'pst repository' feature. Let me explain.

In an on-premises environment, you can have a high-performance storage solution you want to run your mailbox databases off of. And even though every edition of Exchange over the last 10+ years (2007, 2010, 2013, 2016 and 2019) has improved database performance tremendously (in part because they pulled out SIS - single instance storage) and JBOD arrays should be more than adequate for your environment, in my experience for most organizations, there are still plenty of folks who want high performance disk for their databases.

However, if they wish to eliminate pst files and allow users to bloat their mailboxes a bit, the 'in-place archive' feature allows admins to use a secondary database location (typically on cheaper, slower disks) for that data. To the end user, it all looks like one mailbox (the Inbox and In-Place Archive), but in reality, the data could be in two separate databases, on two separate storage solutions.

What does this mean? It means you can eliminate that .pst nightmare in your organization. Does it provide an enterprise grade archive? Not at all. Because if we say an archive is all about retention, discoverability and compliance, then the basic flaw of the Exchange Inbox and In-Place Archive in that role is that by default, end users can delete the data in either one. If the user can delete data, then you cannot ensure discoverability and the solution cannot be compliant. Game over.

Ah… but Microsoft knows this. They know it and have a solution to ensure discoverability, Legal (or In-place) Hold. If you place all mailboxes on legal or in-place hold from day one in Office 365 then no email can be deleted from the system and it will always be discoverable (in theory).

The method and manner you choose to put these mailboxes on hold has changed over time. Currently the Microsoft 365 admin center has a dashboard called the Security and Compliance Center and that allows you to create data governance retention policies that include email (along with public folders, Office 365 groups, OneDrive and SharePoint documents). But under the hood, at least for the email side, the solution is still a form of hold.

One note on this, if you did this with an on-premises environment you would bloat out your storage and would not be pleased. But with Office 365, you can bloat that storage out and you, the admin, don't have to worry about it. Microsoft WANTS you to do this because the larger your data grows, the less likely you are to ever leave their system. The stress of doing so would make it prohibitive. I call this the "Hotel California" approach to customer retention. You can check out any time you like, but because the data bloat is excessive, making the move a nightmare, "you can never leave". Brilliant really.

Legal/In-Place Hold is a band-aid solution here. Legal Hold was designed to be a proactive (or reactive) approach to situations where HR is approached with some form of litigation against Mr. Nasty in your company who has been sending harassing emails to a staff member and you need to stop him from permanently deleting such content from his mailbox so you can provide discoverability of it (if it does indeed exist… innocent until proven… and all that). Mr. Nasty isn't even aware his mail is on hold. If he tried to delete email it simply goes into a hidden Recoverable Items folder that can be searched during eDiscovery by those with the proper permissions.

Microsoft recently stopped talking about "holds" on data and is now calling their solution "intelligent data governance" with preservation and retention policies. That's fine, but under the hood it's still using "hold" solutions to make it happen.

With a legal hold scenario, the whole mailbox is on hold until the hold is lifted. With in-place hold there is some flexibility in terms of what you hold and for how long. And these solutions have an absolute place in the world of compliance. It's a good feature just like 'In-place Archive' (aka .pst repository) is. But it's not what we've come to expect from a genuine, enterprise grade archive solution.

Modern archive solutions keep a secondary copy of the data (which can also be used for recoverability, if necessary). Typically, end-users have read-only or interactive rights to the data (so they can find and interact or recover emails from their past but not delete those emails), something you cannot do with the 'hold' solutions in Office 365.

In addition, in some cases a business may be required to purge data (for example, in the case of litigation where the judge determines there is a need to purge the existing data, or in a GDPR 'right to be forgotten' scenario). Most enterprise grade archive solutions can do that. The 'hold' options cannot do it easily nor can they do it without losing immutability and/or without the possibility of a human error causing lost data.

In short, I prefer a separate data bank for my archive because it provides me with a greater level of comfort due to a) my ability to switch services without getting stuck in a "Hotel California" situation… so I like the data agility/portability aspect of it, b) my end users have the ability to search and interact with their read-only archive, c) purging data is easier and less prone to user error and, d) since Office 365 doesn't have a backup of the

data, it gives me peace of mind knowing I have a second copy of email, should I need to restore it.

Wait… what? No backup of Office 365? We'll circle back to that.

## Continuity or Availability

Every vendor offering a cloud-based solution pours ungodly amounts of money into redundancy to ensure a single failure or even multiple failures go unnoticed by customers connected to their services. For months it appears as if nothing can go wrong. And then…it does. Human error, technical failure, massive storms and lightning strikes. The reasons vary, and the length of time is unpredictable. And it happens to all vendors, so there is no point in bashing Microsoft for downtime of Office 365 pieces (including Exchange Online), because every major/minor vendor has dealt with it. There is no perfect vendor with a perfect amount of uptime (that's impossible).

However, I still consider this to be a gap and an area for cyber resilience, because it comes down to whether or not you have options when/if the service is down. It's like jumping out of a plane. You have a primary chute and hope it works. But every once in a while, it may not (for whatever reason). It sure is a life saver knowing you have that backup chute in place.

Continuity or Availability is not just about users being able to work. They'll work even if their email is down. I mean, if you're in the middle of an important deal and emails are flying fast and furious… do you stop working because your email is down? Nope, you switch to Gmail. And in doing so you slip outside your company's security and compliance umbrella.

When Exchange Online goes down it will be immediately apparent to your end-users that something is wrong, but it may not be immediately apparent that the problem is Microsoft. Your first inclination is to check the Microsoft 365 Admin Center and see if they are reporting an outage. And they may not appear to be. That's because before they turn their little light from Green to Red they have to determine if the problem is a server, a server rack, a pod, or a datacenter. In other words, before they flip that switch and admit to a problem they need to know how big a problem they have. It's not about you and your tenant (not on that level).

Some may wonder how they might obtain Office 365 outage/issue information. Is it public knowledge? Microsoft publishes to an Office 365 Health Twitter feed. @MSFT365Status. It's not the easiest way to gain information but it works. And the Twitter updates link to the Service Portal for your Office 365. Other ways to determine outages include downdetector.com or Reddit.

## Backup/Recovery

Microsoft does a fantastic job of data protection management through their native data protection solution. This utilizes the Exchange database availability group (DAG) feature to ensure the active database has multiple passive copies (lagged) split between datacenters. On the plus side, this eliminates a lot of risk over your existing data. But there are a few things this doesn't provide. It doesn't offer a backup of data so you can restore to a point in time.

Having an archive solution is great for eDiscovery and can assist should mail be missing and appear lost. But it's not the best solution for a mailbox restore. There is no point-in-time

recovery solution built into Office 365 and Microsoft doesn't back-up the email data.

If you aren't sure about the need for a third-party solution that assists with backup/recovery for Office 365 mailboxes you might want to watch this scary demo by Kevin Mitnick (infamous FBI hacker turned good guy) where he showed how an email that includes social engineering techniques combined with an opt-in from the end user and a "bad guy" could encrypt your online mailbox and request a ransom. Without a backup of that mailbox, you're forced to pay that ransom. If you want to see the 5 minute demo just search YouTube for "Ransomcloud".

## Understanding the Stakes

It's easy to talk about the gaps in security, compliance, continuity, recovery and such. But that keeps the conversation focused on the technology. I think it's important to also grasp the impact of a data leak or a security breach or massive outage.

A data breach, for example, can have all sorts of consequences. It can trigger regulatory violations from one of the scary acronyms for regulations like GDPR, FINRA, CCPA, and others. In addition, it can cause loss of reputation for the organization that leaked the data, reputational damage (or job loss) for the C-level folks who are to blame (or become the scape goats). It can cost the company money either through loss of consumer confidence (sales are down) or a stock hit.

The stakes are high. Because the potential impact is deep. A significant breach can change your company's entire trajectory.

## The Big Takeaways

Office 365 is a fantastic solution, especially Exchange Online. More and more organizations of all sizes and business requirements are making the move to Office 365, primarily due to its email offering.

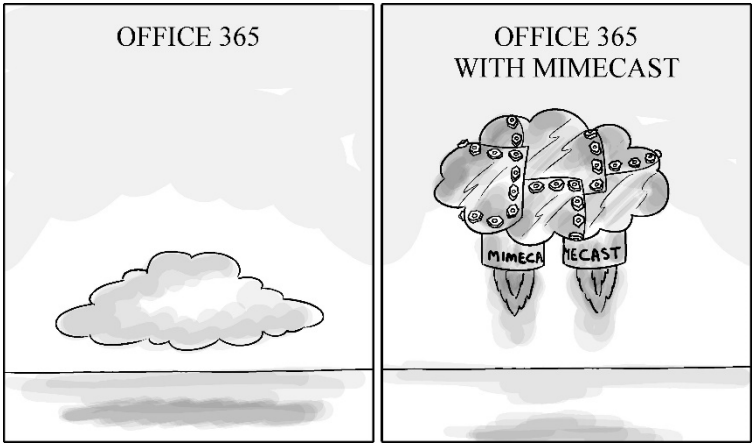
Although Microsoft has more control over Exchange Online because it's hosted in their cloud and they can enhance, improve, develop and tweak it all day long… there are still gaps. There are risks. And these reside primarily in the areas of security, data assurance, continuity and backup/recovery.

It's obvious these risks cause fear, uncertainty and doubt (fud). But they don't have to. My encouragement to any Office 365 current customer or potential customer is to look once again to the ecosystem to find ways to mitigate the risks. Look for an all-in-one, bolt-on solution that can address the pain points and enhance what Microsoft provides. It takes us back to the theme of cyber resilience.

Why an all-in-one? Well, unlike on-premises where email can move through your bolt-on pieces in a nanosecond, with the cloud you cannot have (or don't wish to have) email bounding from one datacenter to another, from one solution to another, before reaching the Microsoft datacenter that holds your mailboxes. That level of latency would be prohibitive. And you're introducing multiple points of failure. Rather, look for a single solution that does it all. But does such a solution exist?

I want to be clear that there is no 'silver bullet' to security. No all-in-one for all things. When I say a single solution, I'm referring to gap-filling Office 365. However, that solution should also be based on an extensible architecture that allows it to work in tandem with other solutions (think API).

# Vendor Sponsor: Mimecast's Cyber Resilience for Office 365




A multi-dimensional problem deserves a multi-dimensional solution.

Most information you read about when it comes to a third-party solution is written by the third-party. They tell you "we're awesome! And here is a document that proves it! <cough><cough> written by us <said in a whisper>". Even if it is true it certainly does cause an eyebrow to rise and the cynical side to us comes out. Doesn't it?

That's why I told my friends at Mimecast I wanted them to let me write this up in my way. I want you to see their solution through my eyes. I won't be able to give you every last bell and whistle, but I will certainly be able to tell you how it will add value to either your Office 365 Exchange Online, hybrid or on-premises environment.

Mimecast was founded in 2003 by Peter Bauer and Neil Murray. These were regular people (albeit super geniuses), IT/Dev admins that saw a problem and went to work fixing it. The problem they saw was that email was becoming more and

more complex to handle. They built a cloud-based solution to the problem that provided email management and risk mitigation – and the company took off.

## Security

Email management can mean so many things, so what is it REALLY that Mimecast provides? Well, for starters, anti-spam and anti-malware. Keep the junk from ever reaching your on-premises Exchange or Office 365 servers. Mimecast's solution sits between your organization and the Internet and provides solid protection from spam, viruses, malware, whaling, zero-day attacks, ransomware, phishing, spear phishing and data leaks.

Mimecast has a service called Targeted Threat Protection (TTP) which focuses on real-time, whaling, ransomware, spear-phishing and other advanced threats. One way it does this (that I think is brilliant) is by converting incoming documents to PDF. So rather than send every document through a sandbox detonation chamber (i.e. a virtual machine to open that document and see if it will do harm) it will convert it to PDF, thus rendering harmless any malicious code within. And then if the person WANTS the original document it can be sandboxed (using full system hardware emulation-based sandboxing). A very creative approach to eliminate the latency of trying to sandbox every single incoming document.

In 8/2018 Mimecast acquired Solebit, an Israeli security software developer that, amongst many other cool things, has a solution for static file analysis. This goes beyond signature-based solutions and looks for any form of machine code within a data object. It's agnostic to file type, client-side application type, client OS and so forth.

Mimecast also rewrites every inbound URL for on-click protection. And identifies whaling emails that use impersonation and/or domain spoofing to try and steal money or data. Those are just some of the protective features in TTP.

But it doesn't stop there. Mimecast has a secure messaging solution that is very customizable and easy to work with. They also have a 'large file send' (LFS) solution so end-users can send files up to 2GB in size right through their Outlook client (if the plug-in is used).

The Mimecast Secure Email Gateway (SEG) uses several detection engines for a multi-layered approach. It includes the ability to deploy policies that assist with data leak prevention (DLP) and content control, a serious sore spot for most organizations. So, Mimecast keeps the company data confidential while keeping the bad guys out at the same time. And it does this no matter where the person is connected (LAN/Wi-Fi/Internet) and no matter which device (desktop, laptop, mobile/tablet).

I mentioned earlier that there is no silver bullet to security. In a defense in depth plan it's ok to utilize multiple solutions (based on need/budget) so long as they can work together through an extensible architecture. The Mimecast platform, MIME OS, provides API integration so you can connect Mimecast with existing investments you've already made so you can leverage the best technologies collectively. It's as close to a silver bullet as we can.

## Web Security

I know we've spent all our time on email security and with good reason. It's the number one means of attack. However,

there are other attack types. Files with harmful links might be shared through OneDrive, Dropbox and such. Links can be sent in IM and through other means and email security won't assist in these cases.

A layer that's often forgotten as an excellent means of protection from harmful links, sites and such… is the DNS layer. Protecting your organization at the DNS layer using a solution that pulls in threat intelligence from a variety of different sources (dark web scanning and such) Mimecast has a DNS secure gateway solution, called Web Security, that helps cover yet another aspect of cyber security.

## Archive

Mimecast provides an independent, enterprise-grade archive solution with a powerful, high-performance eDiscovery service. This reduces your on-premises storage costs because the archive ensures you always have an accessible copy of that data.

Let me explain this a bit further because I don't think everyone understands the value of this solution. Using Microsoft's in-place archive solution is great for eliminating PST files but not great for enterprise archive and regulatory compliance protection. Why? Because end-users can delete whatever they want. And for that to stop you have to enable a form of legal hold (litigation hold or In-Place Legal Hold) now called a retention policy through the Security and Compliance Center. This creates more storage bloat but does stop end-users from deleting things permanently. It's just not flexible and not interactive. And if you're in a hybrid environment there is no single pane of glass for searching both on-prem and cloud at the same time.

Outlook has never performed well with bloated mailboxes. While 2016/2019 is better than predecessors… complaints about performance and app crashes continue.

With the Mimecast solution you have email archived before it even reaches your on-prem/O365 servers. Users can delete whatever they want from their Inbox. Not a big deal. You already have an archive. Now the cool thing is this is an accessible/interactive archive, not backup tapes that sit in a vault. End-users are given tools that integrate with Outlook so they can peruse their archive and find emails they may have deleted accidentally and restore them (no IT intervention required… just a little training). BUT… if they want to delete an email that may be incriminating… nope, not possible! Note: Mobile apps are also available.

I like to call this "preventative litigation". Think about it. If you know, as an end-user, that everything you send and receive is being archived, is non-deletable, is easily located with eDiscovery… how stupid would you have to be to send something inappropriate? Hence, preventative litigation. A strong deterrent, if you will.

With an immutable, separate data archive you can run a lean mailbox, which typically leads to improved Outlook performance.

Knowing folks needed help getting their data from existing services over to the Mimecast Cloud Archive they acquired a solution called Simply Migrate. With it you can transmit your data either rover the wire or through drive shipping over to Mimecast.

## Continuity

So, you have all these different types of Service Level Agreements from Microsoft. SLA's promise many things and one of them is availability of your services. But what happens if/when the service goes down? It happens. It happens with on-premises Exchange and it happens with hosted solutions and even Office 365. Sure, the SLA typically offers some kind of restitution, but what if you don't want restitution, you want availability of service? Microsoft cannot be its own continuity backup solution.

The 2018/2019 outages have been interesting. September 4th, 2018 a lightning strike took out a datacenter in North America, causing an issue with identity management (Azure AD) services, and correspondingly Office 365 services. There have been other service interruptions for email due to Azure AD and Azure DNS issues. There have been MFA troubles and more. I don't highlight these as a deterrent to Office 365 but simply as a reason to pursue options.

Here is where Mimecast is a brilliant solution. They keep users working during on-prem or cloud outages. Like a backup parachute, should the primary not open… you don't have to free fall, you can pull the secondary cord and glide to safety.

So, let's say the Office 365 service goes down. First off, rather than having you guess if there is a disruption and possibly obtaining mixed data from the Microsoft Admin Center, Mimecast provides outage/disruption detection. Through a 'heart beat' approach Mimecast monitors for high latency and failed deliveries. If a problem is detected, based on set thresholds, Mimecast will trigger an alert to admins via SMS or a secondary email. From there the admin can kick off a

continuity event which allows end-users to keep working through Outlook, webmail portal or mobile applications.

With Mimecast, your end-users will have no idea there is a problem. They can continue to send and receive email as if there was no failure. So they just keep working. Once your servers come back online, Mimecast will sync up with them and the world keeps turning.

And, coolest part in my opinion, if Mimecast is also your security and archive solution, having an outage that requires a continuity assist from Mimecast doesn't alter your security and archive capabilities in the slightest. You are still just as protected and compliant.

## Sync & Recover for Exchange and Office 365

If you recall, I mentioned in the last chapter that Office 365 doesn't have a point-in-time backup/recovery solution. It's one reason why I feel a separate data bank archive is valuable in the event something "bad" happens – be it human error, technical failure, a ransomware strike that requires a restore to a point in time, whatever it might be.

In addition, there are some who need more than an archive. There are some who are backing up to on-premises infrastructure or using some cloud-based backup solution because Microsoft simply doesn't back up the data and they want/need that.

Mimecast is expanding their solution to include other communication and collaboration types (Teams, OneDrive and more).

With Mimecast's 'Sync & Recover' solution they can back up email, calendar and contacts (and more recently notes and tasks) without additional hardware or software. This solution assists should data be lost due to corruption, accidental deletion or cyberattacks.

## Security Awareness

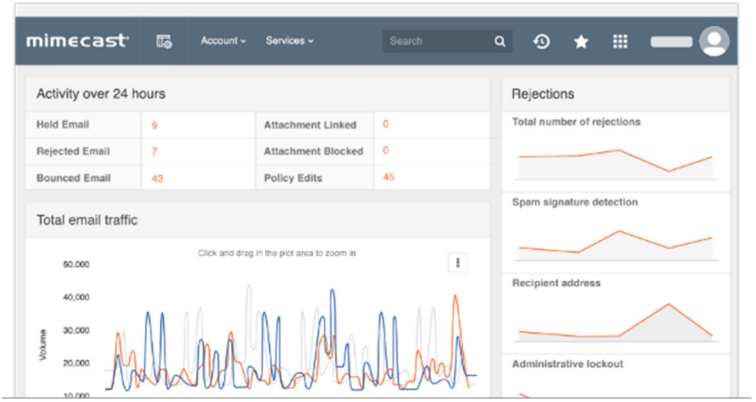
I know what you're thinking. Death-by-PowerPoint security awareness training? No thanks! I thought the same thing when I heard Mimecast acquired Ataata's awareness training and simulation tools. But this is a really engaging approach. Unique compared to other training solutions. It's clear that when your users aren't engaged, they don't pay attention to the training, never learn and become somewhat dismissive toward security in general. So, how do you engage folks? Humor.

Mimecast uses short videos (3-5 minutes) that are quite funny. And while they are designed to make you laugh, they're also designed to make you think. Users get an email reminder to watch the lesson. They get a single question at the end of the module to ensure they got the point. A risk score is determined based on how your users do and you can locate your riskiest people and provide them more help *before* they make a mistake (or *another* mistake).

Feel free to try them out yourself.
**https://tinyurl.com/mimecastsecurityawareness**

## The Big Takeaways

Despite the risks of moving to the cloud, by adding a third-party all-in-one solution like Mimecast you can mitigate those risks, eliminate the FUD, and plan for success rather than hope for it.




The Mimecast Admin Console

So, that's my personal opinion on Mimecast's Cyber Resilience Solution for Office 365. I'd recommend you check them out. The added value you will receive at such a reasonable price point is unbelievable.

NOTES

NOTES

## Easily “converse” about Office 365 cyber resilience in any setting.

If you are moving to or already using Office 365 then it's essential for you to formulate a plan toward a risk-free cyber resilience experience. Doing so will protect your organization from security threats, compliance concerns, unplanned outages and more. To mitigate concerns and form a resilient strategy you have to first KNOW the risks. This book will ensure you do in no time.

### About J. Peter Bruzzese

J. Peter, an eight-time Microsoft MVP awardee (Exchange/Office365), is an internationally-recognized journalist, published author, and speaker. He is co-founder of both Conversational Geek and ClipTraining. Follow him on Twitter @JPBruzzese.

ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.