A COMPLETE GUIDE

DEFENDING YOUR OFFICE 365 DATA: Five Threats That Microsoft Can't Defend Against, But You Can

datto | backupify

Table of Contents

Table of Contents (continued)

Introduction

Why should I read this?

Office 365 is the fastest-growing platform Microsoft has ever released (surpassing SharePoint and even Microsoft Office growth rates!) with a powerful set of collaboration features for individuals and teams. While there are many benefits to using the Office 365 platform, there are some legitimate risks associated with any software-as-a-service (SaaS) application suite or platform, including Office 365. The fact remains that three-out-of-five companies that suffer a major data loss will shut down within six months. To mitigate the risks associated with using any cloud platform, you should first understand the risks – and the steps you can take to protect your intellectual property. As the saying goes, knowledge is power!

Should I be concerned about moving to the cloud?

Microsoft, as with most other major technology providers, are quite bullish on the cloud – and they are taking every measure possible to reduce the risks and threats to your data so that moving to the cloud is seamless and, ultimately, more cost effective and secure than what you can manage on your own. Having said that, there are definitely customers who have had issues with lost data. How can this be?

The odds of you permanently losing Office 365 data because of Microsoft mistakes is incredibly low – but the odds of losing that data through end user or administrator error are not uncommon. People within your organization will inevitably make mistakes, but Microsoft has taken a number of steps to help minimize those risks and help you secure your data while hosted in Office 365.

Do I need to speak 'geek' to use this ebook?

No, don't worry – the material within should inform you without acronym overload. And to be clear, the purpose of this ebook is not to pick holes in the data security of Office 365, but to point out the fact that the vast majority of data loss scenarios come from improper use or intentional abuse of the tools. Office 365 can provide your business with tremendous value, but these unintentional losses could cost your company. This ebook is designed to provide you with an overview of what could happen, and to help you mitigate those risks and plan ahead.

Rather than bore you with technical jargon, we'll give you the information required to proactively manage the platform, and point you toward the right supplementary sites and content to satisfy your additional geeky data needs.

DATA THREAT #1:

A User Makes An Error

What is user error?

Think of user error as the "deadly oops" – a simple, honest mistake with disastrous consequences. According to a recent 2013 Aberdeen report "SaaS Data Loss: The Problem You Didn't Know You Had" one third of SaaS users reported losing their data from an application like Office 365.

User error falls into two general types: accidentally deleting information, or intentionally deleting data only to need it later.

In the first case, it could simply be a matter of deleting an Outlook message when you thought you archived it. (Many organizations retain their deleted messages for 30 days, but by default Office 365 retains these emails indefinitely – unless otherwise determined by an administrator.) The same holds true for SharePoint and One Drive for Business documents. Calendar events and Contacts entries, however, have no trash folder from which you can rescue mistakenly deleted data. A simple slip of the mouse or misunderstanding of how Office 365 works could lead to a major loss of business data.

In the second case, you or a colleague could erase a document or message you were certain was no longer necessary only to later find that data is vital, but cannot be restored. This happens often when projects end or employees depart; shared data gets deleted because the owner is done with it, never suspecting that someone else in the organization still has a need for the information. Occasionally, that "someone else" is very scary and very important, like the IRS or an industry regulator. These groups don't tend to accept the "Microsoft ate my homework" excuse.

Why Microsoft can't stop user error

Microsoft can't protect you from yourself. You told Office 365 to delete data, and the platform did what you asked. To abuse an analogy, even the safest car on the road will suffer damage if you absentmindedly drive it into a wall.

What user error can cost you

Most of the time, an accidental deletion involves a single item. In our own past research, we found that the average email is worth about $2.11 and the average document is worth about

$217.20, based on the time and money needed to recreate the lost data. The average user deletes a critical item roughly three to four times per year. That means in any given year, you could lose as little as $6 to well over $800 for every user on your domain.

How to defend against user error

A "no deletion" information policy is the best place to start in defending against user error, as it should answer the "should I purge this or keep it?" question every user is supposed to ask before clicking the delete button. Office 365 makes it easy by keeping items in the Deleted Items folder indefinitely. Unfortunately, not every user bothers to ask that question before gunning zealously for an empty inbox or emptying their Deleted Items folder. But at least from an administration standpoint, Office 365 does not automatically delete (unless you tell it to). Regularly scheduled backups of your Office 365 data are your safest protection against user error. The best way to keep your data out of harm's way is to keep a copy of it where it can't ever be deleted. Of course, it is important to include data standards and best practices as part of your regular employee training – especially part of your new employee onboarding, ensuring that everyone is aware of how the system works, and what the company expects as far as data handling and deletion policies around sensitive data.

Microsoft is very good at avoiding their own errors. And chances are, they won't lose your data. But there are some situations where Microsoft can't help, and its up to you to be proactive.

> "Office 365 supports the most rigorous global and regional standards such as ISO 27001, SAS70 Type II, EU Safe Harbor, EU Model Clauses, the US Health Insurance Portability and Accountability Act (HIPAA), the US Family Educational Rights and Privacy Act (FERPA), and the US Federal Information Security Management Act (FISMA). To meet evolving needs, we also plan to support IPv6 in Office 365 for Government by September of this year, and we're taking steps to soon support Criminal Justice Information Security (CJIS) policies."-Kirk Koenigsbauer, Corporate Vice President at Microsoft

DATA THREAT #2:

There's a security breach

What is a security breach?

A security breach occurs anytime an unwanted person gains access to your Office 365 account. If anyone other than one of your end users signs into one of your Office 365 accounts, that's a security breach.

There are two kinds of security breaches: a "hard" breach and a "soft" breach.
A hard breach occurs when the software itself is compromised. In other words, hackers have found a way to get around your defenses and get at your data. While Microsoft have architected and built their data centers from the ground up to protect user data from both physical and digital intrusion, most security breaches are not the result of an attack against the data center – but in errors on the customer end of the connection. Microsoft secures their data centers through restricted access, biometric scanners, 24/7 continuous video surveillance, and two-factor authentication methods. But show your users a list of the most popular easily guessed passwords and see if their faces go pale with recognition.

A soft breach occurs when an attacker tricks one of your users into granting him "legitimate" access to your Office 365 domain. These techniques are known as social engineering, where the attack focuses on people rather than technology. The most common form of soft breach is caused by phishing, where users are duped into revealing passwords by way of emails or web pages that are designed to look like "real" login screens. Microsoft asks that you report all suspected spam and phishing to them so that they can continue to improve their defenses and halt future attacks.

Why Office 365 can't stop every security breach

When it comes to hard breaches, Office 365 has so far been very successful. Unfortunately, there are no real software defenses against soft breaches. It doesn't matter how sturdy the lock is if you give a burglar the key, and soft breaches are always about convincing you to let attackers in so that they don't have to deal with Microsoft's highly effective security measures.

What security breaches can cost you

If a hacker obtains an account password, he or she can effectively corrupt or delete all the data in that account. Depending on what they are able to access, the damage to your business could be minor....or huge. That's why it is so important to take a proactive approach to data security.

How to defend against security breaches

The best bang for your buck in preventing security breaches is actually training your Office 365 users on security best practices. Being with password policies. Simple things like "don't tell anyone your password, ever" and "check the web address of any page that asks you to log in" can stop the vast majority of social engineering attacks. You'd be surprised at how many users – even very technically sophisticated ones – don't know these basic rules.

Beyond bringing your staff up to speed on good Internet safety habits, implementing Office 365 security best practices is a pretty good idea. Office 365 administrators should have backup email accounts and phone numbers in case their primary account gets locked out or compromised. All Office 365 users should be required to use strong passwords. Two-factor authentication, which requires users to input both a password and a time-sensitive code to log into Office 365, renders even stolen passwords useless.

Through Microsoft Azure Rights Management, Office 365 also offers Information Rights Management (IRM) and Message Encryption options, allowing organizations to establish automated policies to further protect against unauthorized access to data whether online or offline.

What is included in Office 365's continuous compliance services?

Microsoft is continually reviewing its own data handling policies and procedures to ensure that evolving customer and industry standards are being upheld, including the following continuous compliance services:

- Each customer agreement details privacy, security, and data handling processes so that customers can more easily comply with local data regulations
- Over 900 controls in the Office 365 compliance framework, enabling the platform to be able to stay current to evolving industry standards
- Constant review of changing standards
- Legal hold and eDiscovery built into the system to help you find, preserve, analyze, and package electronic content for legal request or investigation
- Data Loss Prevention (DLP) to help you identify, monitor, and protect sensitive information

DATA THREAT #3:

An error is made during a migration

What are migration errors?

A common scenario for Office 365 users is to move content into the platform from older on-premises versions of Exchange and SharePoint, from file shares or line of business (LOB) applications, or from competing collaborative platforms. Sometimes these moves or migrations are performed with the help of third-party solutions (from independent software vendors, or ISVs), or manually on their own. As part of this migration activity, data can be mislabeled or misplaced, resulting in lost productivity or improper handling of important information assets. While Microsoft works closely with the ISV partner community to develop fast and flexible tools to help migrate and manage content within the Office 365 platform, these third-party applications are not managed by Office 365 in any way. You can find tools to help you automatically provision new Exchange mailboxes, move public folders regardless of size, and migrate your documents and personal archives while maintaining all metadata and permissions, but as with any other process or tool that requires human interaction, there is room for error during these migration activities.

Unfortunately, sometimes these applications are configured incorrectly or aren't employed according to the developer's directions. (It's almost comical how often cries of "your app deleted all my data" are followed by "the setup guide stated 'if you do X you'll overwrite existing data.'") Office 365 cannot and does not guarantee that the third-party solutions available through the partner ecosystem will be foolproof. Like any software, third-party solutions occasionally have bugs, and even the ones that don't are often quite easy to misuse. The danger lies in the amount of access these applications have to your Office 365 data.

When you use third-party solutions in conjunction with your Office 365 environment, you grant those applications a specific – and usually quite broad – set of permissions. If an email migration solution can provision and add content to your Office 365 account, it can also delete those accounts – or populate them with the wrong data. The same problems can happen to solutions that support SharePoint Online, OneDrive for Business, or the Office suite of tools.

Why Office 365 can't stop migration errors

Just as Microsoft can't tell good commands from bad ones when they come from individual users, Office 365 is blind to correct and incorrect instructions from third-party solutions. For all Office 365 knows, you actually want your migration tools to overwrite all of your existing data and start fresh, or wipe out your extensive taxonomy structure with today's date as the creation date and "Administrator" as the document creator. Only you know the difference, and odds are you won't notice an improperly configured solution until after it has inflicted its damage.

What migration errors can cost you

You can sum up what's at risk with migration errors in one word: Everything. Migration errors are amongst the most dangerous threats to Office 365 data because third-party solutions can touch an entire service or an entire domain.

While most migration solutions handle just part of your overall move to Office 365, all of them can affect enough of your critical business information to do serious damage not just to Office 365, but to your entire business.

How to defend against migration errors

The best defense is to have a plan – which begins with an understanding of what it is you're planning to move, who owns it, how it should be handled, and where it should all go. The Office 365 community has plenty of information on how to plan for a successful migration to the cloud, and most third-party solution providers will also have ample documentation on running a pre-migration inventory analysis to help you better understand what you have. Of course, a secure, independent backup of your data is strongly recommended, and will allow you to start over should a malfunctioning third-party solution (or, more likely, a malfunctioning administrator) overwrites, mislabels, or deletes your data.

(It should be pointed out that third-party backups are, by definition, third-party solutions – and most of them require the same read/write permissions that make other solutions dangerous. The key to evaluating a good third-party backup and restore application is to ensure it performs non-destructive restores. That's the technical term for restoring data without overwriting existing data. A good third-party backup solution will restore a backup copy of an Office 365 document alongside an old one, rather than paving over the data in place. If a backup and restore app is limited to non-destructive restores, it can't harm your existing data.)

DATA THREAT #4:

You Have A Rogue Employee

What is a rogue employee?

Imagine user error that isn't accidental; that's the threat of a rogue employee. While some disgruntled users make headlines for violent acts against their co-workers, the vast majority of revenge-seeking employees act out by stealing office supplies, cursing their managers, or by sabotaging company computer systems.

Typically, rogue employees damage Office 365 environments in cases where administrators can't or don't know to lock the departing employee out of Office 365 before the worker is notified of her termination. When the departing employee returns to clean out his desk, he can also clean out his Exchange inbox (full of vital client emails), personal folders (home to several shared, irreplaceable sales spreadsheets), contacts (filled with vital supplier email addresses) and calendar (where delivery schedules are maintained).

It may not require a firing; employees can "burn" a domain before leaving for another job, or simply because they feel slighted by your organization. Regardless, imagine all the damage random user error can inflict, but magnified by an angry employee who knows exactly what data your company can least afford to lose.

Why Office 365 can't stop rogue employees

We've said it before and we'll say it again: Microsoft can't distinguish between "good" employees and "bad" any more than it can distinguish between intentional or accidental commands. If someone with legitimate access to your Office 365 data wants to do it harm, there's nothing Microsoft can do to stop it.

What a rogue employee can cost you

Much like a security breach, a rogue employee can delete all the data in a single Office 365 account. Damages might range from a minor inconvenience (contact information is lost) to a major impact (customer account details could be deleted or compromised), which is why organizations need to be vigilant,

How to defend against rogue employees

The most effective defense against rogue employees is also the easiest: Change an employee's password or suspend an employee's Office 365 account before firing him. It should be policy that the first person to find out an employee has been terminated should be the HR department, followed by the Office 365 administrator, then followed by the employee. Any other order gives the employee time to do damage to your data before his or her access is suspended.
In addition, if the employee used Office 365 via a mobile device, you can remove or remotely wipe their device from the Admin console.

Organizations should also be more proactive in monitoring user behavior on the platform. If an employee is suddenly downloading sensitive information from multiple project sites, outside of normal site usage or historical patterns, that may be a sign of rogue behavior. Regular audits of usage patterns can often identify these kinds of irregularities before they get out of hand.

How does Office 365 keep my data private and secure? Here's how:

1. Restriction of physical data center access to authorized personnel, implementing multiple layers of physical security
2. Enabling encryption of data both at rest and via the network as it is transmitted between a data center and a user.
3. Will not mine or access your data for advertising purposes.
4. Use of customer data only to provide the service.
5. Regular back up your data.
6. Will not delete all the data in your account at the end of your service term until you have had time to take advantage of the offered data portability options.
7. Customer data hosted in-region.
8. Enforcement of "hard" passwords to increase security of your data.
9. Allow you to turn off and on privacy impacting features to meet your needs.
10. Contractually commit to the promises made here with the data processing agreement (DPA).

DATA THREAT #5:

You Experience A Service Error

What is an Office 365 service error?

Microsoft has spent a tremendous amount of time and resources to build up trust in the cloud. In fact, the best way to get a clear picture of the strides Microsoft has gone through to build confidence in the Office 365 platform you only need to browse through the many case studies, customer scenarios, and service-level agreements outlined in the Office 365 Trust Center site. Microsoft touts a 99.99% uptime, and a continuous compliance model.

Even so, there are two major types of Office 365 service errors: service outages and erroneous account suspensions.

Ok, to be fair – these are not "errors" but, more or less, activities within the scope of service operations that can impact data integrity. Service outages are pretty straightforward. Occasionally, some percentage of Office 365 customers will experience downtime to their services. If part of your Office 365 environment seems to be down, administrators can access their Office 365 Service Health Dashboard within the administration console, as Microsoft does not make this data public. These outages are generally brief, but in some cases an outage can last for hours, even days.

A much more common form of service error is the account suspension. Microsoft reserves the right to suspend or terminate, without notice, any Office 365 account at any time, per the Terms of Service. If Microsoft suspects one of your Office 365 users is violating its terms, it can shut down that user account indefinitely. The clause is there to ensure that Office 365 accounts aren't used to support criminal activity or actions that could harm Microsoft's systems – like running a spam operation off your Outlook account – but Microsoft has the authority to suspend first, ask questions later.

It's in Microsoft's best interest to preemptively lock up accounts for suspicious activity while it investigates threats. There are documented cases of this process. It can take days to unlock accounts, as the burden of proof is on you to convince Microsoft your account isn't secretly harboring criminal data. Again, these instances are generally rare, but they are common enough that you need to prepare for them as part of your business continuity plan.

Why Microsoft can't stop service errors

Microsoft isn't trying to cause errors, but when you operate at Microsoft's scale of close to 100 million (estimated) user accounts, even a miniscule error rate can result in dozens, hundreds, or thousands of wronged customers and gigabytes of misplaced data every day. Microsoft can't protect you from yourself, and Microsoft can't always protect you from itself, either.

What Microsoft service errors can cost you

The actual cost of Office 365 errors are, frankly, almost impossible to calculate because eventually, everyone gets their data back. The cost of data lost to Office 365 service errors is based on opportunities and productivity lost when your organization is denied access to your information. How do you put a dollar figure on not having access to your Office 365 inbox in the middle of a client negotiation, or the loss of an accounting spreadsheet in the midst of a tax audit?

How to defend against Office 365 service errors

Every user on your Office 365 environment should set up account recovery options, which allow you to list a mobile phone number and alternate email address, which Microsoft can contact to verify your identity. If Microsoft suspects your account has been hijacked, this is where it will send alerts and begin the process of returning control of your Office 365 account. Accounts that don't have recovery options set up face much longer roads back from account suspension – those users should contact Office 365 support directly to reset access controls.

There is no administrative setting to defend against an Office 365 service outage. The only remedy for a lack of access to your Office 365 environment is a backup copy of your Office 365 data. With an adequate third-party backup tool, you should still refer to and act upon your business information – look up emails, download documents, check calendar schedules – even when Office 365 itself isn't accessible (because you'll be able to log-in to your separate backup tool).

Conclusion

With all of these risks, why would I ever move to the cloud?

Don't freak out. Office 365 is still one of the safest places on earth for your business data. When weighed against the fact that Microsoft has spent serious dollars and time on ensuring their data centers and platforms meet all of the stringent data standards of some of the most data security-conscious countries in the world, your ability to secure your data on-premises falls far short. Still, to return to our previous car analogy, even if you buy the safest car on the market and follow all the rules or the road, you still want a few bits of safety gear close at hand. Nothing in this report should stop you from driving Office 365 off the dealer lot. You should, however, make sure you've got the computer-security equivalent of jumper cables in the trunk, a flashlight and first aid kit in the glove box, and your insurance card in your wallet. Also, you may want to give your users some driving lessons before letting them loose on the information superhighway.

Know what you're buying

Still need to convince your management team that the greater risk is staying on-premises? Spend some time trying to understand the built-in security measures within the Office 365 platform.

- **Physical security** – From 24-hour monitoring and restricted physical access, to multi-factor authentication and biometric scanning for data center access.
- **Logical** – Dedicated threat management teams, port and perimeter scanning, and intrusion detection to prevent malicious access.
- **Data** – Encryption at rest and in transit, constant security management, and data/file integrity detection services.
- **Admin and user controls** – Rights Management Services (RMS), certificate-based email access, Data Loss Prevention (DLP) controls, and message encryption to protect sensitive data.

So what's the bottom line?

Don't put all your eggs in one basket. Your Office 365 data needs a third-party backup solution, period.

Even if you enable all of the Office 365 security settings, train your staff well, and observe all the industry best practices – and, yes, all those old-school on-premises best practices still apply to data stored in the cloud – it still isn't a good idea to have all your irreplaceable business data in one place. A secure second copy of Office 365 data means that no matter what Microsoft or hackers or your own employees do to your Office 365 environment, a copy of your data is kept safely somewhere else.

Christian Buckley is an Office365 MVP, internationally recognized author and speaker, and a Top 10 SharePoint and Office 365 Influencer. He is Managing Director at GTconsult, a consulting and managed services provider with offices in the US and South Africa, and runs the Bellevue, Washington office. Prior to GTconsult, he was Chief Evangelist for two of the biggest names in SharePoint, Axceler and Metalogix, and was instrumental in the acquisitions of echoTechnology (2010) and Axceler (2013). He was part of the Microsoft team that launched SharePoint Online (now part of Office365), and worked with some of the world's largest technology companies to build and deploy social, collaboration, and supply chain solutions. Co-author of 2 SharePoint books and 3 books on software configuration management, Christian can be found online at www.buckleyplanet.com.

Resources

- Office 365 Trust Center
- What is 'Continuous Compliance'?
- Security in Office 365 (whitepaper)

About Datto

Datto is the leading provider of comprehensive data backup, recovery and business continuity solutions with over five million customers and 8,000 partners worldwide. With its Total Data Protection Platform, business data is protected everywhere it resides, whether on-premise, in virtualized environments, in the cloud, and software-as-a-service (SaaS) applications, including Salesforce, Google Apps, and more. To learn more go to datto.com or datto.com/backupify, follow on Twitter @Datto or connect with us on LinkedIn.