SPANNING BACKUP FOR OFFICE 365

THE ROI OF MICROSOFT OFFICE 365 BACKUP

—

HOW WILL A MICROSOFT OFFICE 365 BACKUP SOLUTION IMPROVE THE BUSINESS?

TABLE OF CONTENTS

INTRODUCTION

"How will a Microsoft Office 365 backup solution improve the business?"

This is a very common - and valid - question asked by decision-makers for which IT managers rarely have the right answer. It's a real struggle for IT managers to quantify the value of an Office 365 backup, and then communicate it to an audience that's hardly interested.

Our eBook will help IT professionals educate decision-makers on why their business needs an Office 365 backup solution. That's not all! We want to take a step further and help you quantify the value of an Office 365 backup. The Spanning ROI calculator will enable IT professionals to justify the costs of an Office 365 backup, improving the odds of getting budget approvals.

OFFICE 365 SECURITY: TACKLING FALSE PERCEPTIONS

Perception is NOT reality.

‘Perception is reality’ a euphemism often thrown around to justify one’s reality as the reality. Perception and reality are two separate entities. Decision-makers often struggle with this problem where they turn their belief into reality.

This is especially true for protecting data stored in the cloud. Many decision-makers believe cloud applications like Microsoft Office 365 don’t need backup. This comes from critical knowledge gaps around Microsoft’s role in data protection.

Decision-makers fill up these gaps with perceptions, mostly false perceptions. These misconceptions are so ingrained that decision-makers piggyback on Microsoft’s brand value to justify their beliefs.

What’s wrong with perception departing from reality?

Perception is the lens through which decision-makers process, decide, and act on reality. The problem is the lens is warped, and so is the reality that comes out of it. Decision-makers will be wavering between illusions and delusions. Such situations can put your Office 365 data at risk and the worst bit is — you wouldn’t even know.

It’s time to break the glass of false perceptions to make smart decisions that keep your Office 365 data secured.

Perception #1: My Office 365 is *really, really* secure

Microsoft Office 365 has best-in-class security: disaster recovery capabilities against infrastructure threats like hardware and software failure, power outages, and natural disasters.

Reality: Microsoft cannot protect you from attacks at your end.

HUMAN ERROR: Constitutes one quarter of data loss including your precious Office 365 data.[1]

SYNC ERROR: Third-party apps in Office 365 can ruin valuable data with no option to undo.

RANSOMWARE: SharePoint that makes Office 365 a great collaboration platform also allows for ransomware to proliferate easily.

INSIDER THREAT: Even Office 365's sophisticated security infrastructure cannot predict employees' intentions, making such employees an effective cyberattack vector.

Perception#2: Microsoft is responsible for my data

Office 365 holds your business data, so the responsibility comes on Microsoft's shoulders to keep your data safe.

Reality: Microsoft is not responsible for your data. Remember the terms of service you signed (probably without reading)?[2] Here's the disclaimer you missed:

"You are **solely responsible** for the content of all Customer Data. You will secure and maintain all rights in Customer Data necessary for us to provide the Online Services to you without violating the rights of any third party or otherwise obligating Microsoft to you or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to your use of the Product."

Perception #3: My Office 365 has a built-in backup

Yes, Office 365 does have built-in features like Recycle Bin and shadow copies to store deleted data.

Reality: They are temporary archival solutions, not a backup solution. That means deleted data is stored for a limited period, the backup is not as comprehensive as one would hope, and restoring data can be a nightmare.

THE BUSINESS VALUE OF A MICROSOFT OFFICE 365 BACKUP SOLUTION

Relying solely on Office 365 will not mitigate risks, period. You need a robust backup and recovery solution to provide the additional layer of security your Office 365 data needs.

Yet, decision-makers would think a thousand times before assigning a budget for a backup and recovery solution. Why?

They don’t trust backup solution vendors. Part of the blame goes to vendors who have tried to trick businesses with exaggerated statistics as a marketing gimmick. The other aspect is they don’t see the value in an Office 365 backup.

Use these insights to get your point across to decision-makers on the real value a robust backup and recovery solution brings to a business.

Direct costs of cyberattack

Post an attack, businesses go in investigative mode, trying to find the what, how, and why. For businesses still living on the trial-and-error approach, their investigation often leads to three conclusions: close to accuracy, inaccurate, or multiple reasonings with a high degree of variability. That's a lot of working hours put in an investigation whose conclusions are full of errors.

The faulty conclusions will be used to make faulty decisions, with the expectation of avoiding similar attacks in the future — that never happens.

Here's the direct cost or the cost your business incurs right after an attack:

Total Direct Cost = Loss from attack (like ransomware or hardware malfunction) + Working hours investigating attacks + Loss from potential attacks

An Office 365 backup solution enables you to adopt a proactive approach to dealing with cyberattacks.

For instance, Spanning Backup allows you to monitor the most recent Office 365 backups. You can view the backup health for each Office 365 user within their domain and drill down to identify and resolve issues before they impact the integrity of your data. You can opt to receive daily, weekly, or monthly email notifications to keep you on top of your Office 365 backup status.

With Spanning Backup, this is the cost your business will incur right after an attack:

Total Direct Cost = *Zilch*

Hidden costs of cyberattacks

Ever noticed why publicized data breaches report losses in millions? That number comprises of direct costs and hidden costs. These are indirect costs that affect the bottom line of the business, and they have been steadily increasing over the past five years.[3] These include loss of business, disruption of business operations, lost productivity, to name a few.

- **Loss of business:** Whether you are a small ad agency that has lost its latest creative work or a retail giant that lost an entire month's order, sudden data loss can cripple any business of any size. Moreover, each data loss incident forces a business to pay an average of $92 (£71) per record.[4] Expenses piling up and no revenue stream pushes the situation to the extreme — permanent business shutdown.

- **Business disruption:** Money is just the tip of the iceberg. The real cruelty of data loss is that it snatches 'time' away from you. Recovering lost data can take hours, putting all the ongoing work in a logjam. It creates a ripple effect, delaying work across departments.

- **Lost productivity:** In many ways, workplace productivity is the first casualty of data loss. When you lose your data, the IT department might need to work overtime to recover data. Whether they succeed or not, you'll have to pay for overtime for doing a job that has no impact on your profit margins.

Cost of insider threats

One bad apple can cost your business BIG! Here's how:

IMPACTS MARKET VALUE

When Harold Martin, a former contractor for Booz Allen Hamilton was arrested, the consulting firm's shares saw an immediate dip of 5%.[5]

RISKS THE COMPANY'S FUTURE

Due to the ease of access, insider attacks tend to focus on stealing intellectual property. With nothing to compete on, the future for your business becomes dicey.

INCREASED OVERHEADS

Restructuring security infrastructure, employee retraining, new employee hiring, etc. end up being huge operational expenses.

GIVE WAY TO BAD CULTURE

Insider threats create a breach of trust, leading to a decline in morale. Bad workplace culture results in higher turnovers and hiring costs.

- Unfortunately, insider threats cannot be avoided. However, a good backup solution like Spanning Backup can mitigate it.

  Spanning Backup provides transparency and accountability by recording every Office 365 backup activity. Get detailed insights on every action done by the user and report suspicious activities that can compromise your data.

Cost of downtime

To quantify the impact of downtime on a business, you need to understand the recovery time objective (RTO).

> RTO is the amount of time your business can afford to lose after a disaster strikes until normal operation resumes.

Without a realistic RTO in place, you'll spend time in developing an action plan which only delays actual recovery time. The impact of downtime increases with the duration of downtime.

A typical RTO plan comprises of the following:

- **DISASTER DECLARATION:** Who is authorized to declare the disaster and what are the measures they must take before making the declaration
- **SYSTEM SETUP:** The time it takes to set up an operational system at a secondary site during a disaster scenario
- **RECOVERY EXECUTION:** The amount of time it will take to get the right people to execute recovery
- **BACKUP ACCESS:** The time it would take to gain access to the backup data.
- **TRANSFER:** The additional time it takes to transfer the data
- **SYSTEM RESTART:** The time it takes to restart servers, launch applications, and load the data into the production site

- Recovery vs restore
  When it comes to Office 365 backup, data recovery is not the same as data restoration.

  Recovery gets your data back, probably not in the original format as you lost it. This means longer periods of downtime and additional man-hours to hunt for lost files, rebuild file structure, and manually import lost data back into Office 365.

  Restore gets your data back – in the original format which is automatically imported to your Office 365. That's the highlight feature that has made Spanning loved by over 10,000 businesses globally because it enables business continuity even during a disaster.

Reputation costs

Would you associate yourself with a business that's been breached? Can you overcome the disappointment of having your confidential data exposed? Would you be okay with no explanation as to why your data went missing? Probably not.

Why should you expect any other treatment when your business is under the data breach spotlight?

Fixing the reputation of your business after a data loss is a tough nut to crack. In fact, reputation management can have a huge impact on your margins. Not only do you lose on current customers but, with poor credibility and bad publicity, potential customers would never come knocking on your door. It's no surprise, 41% of businesses lose out on revenue due to negative reputation.[6]

Cost of non-compliance

Compliance has always been a pre-requisite for regulated industries like healthcare and finance. However, with GDPR and CCPA, the need for compliance is extending to non-regulated industries as well.

Non-compliance costs 2.71 times the cost of maintaining compliance requirements; too many variables to non-compliance costs that cannot be ignored.[7]

COMPLIANCE LEGISLATION	PENALTIES
HIPAA	Fines up to $250k and 10 years of imprisonment.
GDPR	20 million Euros or 4% of the total global turnover of the previous fiscal year, whichever is higher.
CCPA	Civil penalties of up to $7500 for each violation and the maximum fine for other violations is $2500 per violation.

- Legal fees
  Fighting penalties means dealing with a pile of legal paperwork and courts. Add to that, potential civil lawsuits. For instance, a European citizen whose data was leaked decides to sue your business. This leads to a mountain of legal fees that can exceed more than the penalty itself.

- Recertification Costs
  A non-compliant business is expected to recertify employees in compliance training. This can be an overwhelming expense for a business that's already dealing with penalties and legal costs.

Find the real value of Office 365 Backup with our ROI calculator

Spanning offers the Office 365 Backup ROI calculator to help find the X amount of dollars you'll be able to save or earn. Calculate in real-time the amount of money you'll save on employee and overall IT productivity along with knowing potential returns. The insights will help you make decisions that are rooted in reality, not perceptions. Ready to make smart decisions?

GET ROI ON MY OFFICE 365 BACKUP

Sources:

1. https://threatpost.com/quarter-of-breaches-human-error/146662/
2. https://www.varonis.com/blog/cybersecurity-statistics/
3. https://www.ibm.com/security/data-breach
4. https://www.workspace.co.uk/community/homework/technology/opinion-what-is-the-true-cost-of-lost-data-to-bus
5. https://www.federaltimes.com/2016/10/05/fbi-arrested-contractor-for-theft-of-nsa-code-docs/
6. https://statuslabs.com/reputation-management-stats-2019/
7. https://securityboulevard.com/2018/04/costs-of-non-compliance-are-getting-higher/

SPANNING
A Kaseya COMPANY

Spanning Cloud Apps, a Kaseya company, is the leader in SaaS Cloud-to-Cloud Backup, proven and trusted by more than 10,000 organizations across the globe to provide enterprise-class data protection. Spanning's cloud-native, purpose-built solutions for Office 365, G Suite, and Salesforce provide easy-to-use yet powerful capabilities for end-users and administrators and meet the rigorous requirements for listing on Microsoft AppSource, Salesforce AppExchange and G Suite Marketplace.

START A FREE 14-DAY TRIAL AT
SPANNING.COM/START-FREE-TRIAL

@SPANNINGBACKUP

FOLLOW US ON LINKEDIN

READ OUR BLOG

WWW.SPANNING.COM

+1 (512) 236-1277