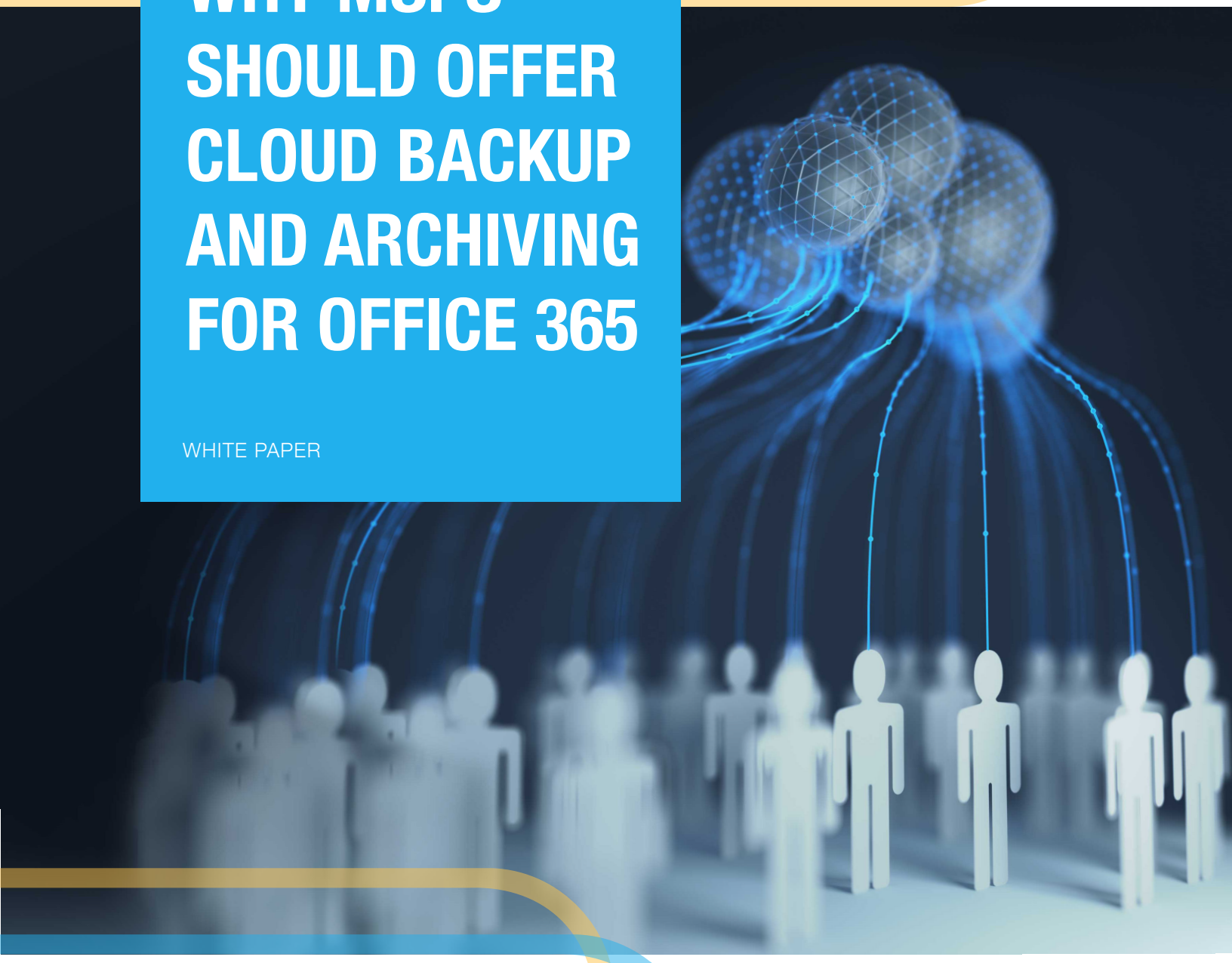
Dropsuite

WHY MSPS SHOULD OFFER CLOUD BACKUP AND ARCHIVING FOR OFFICE 365

WHITE PAPER



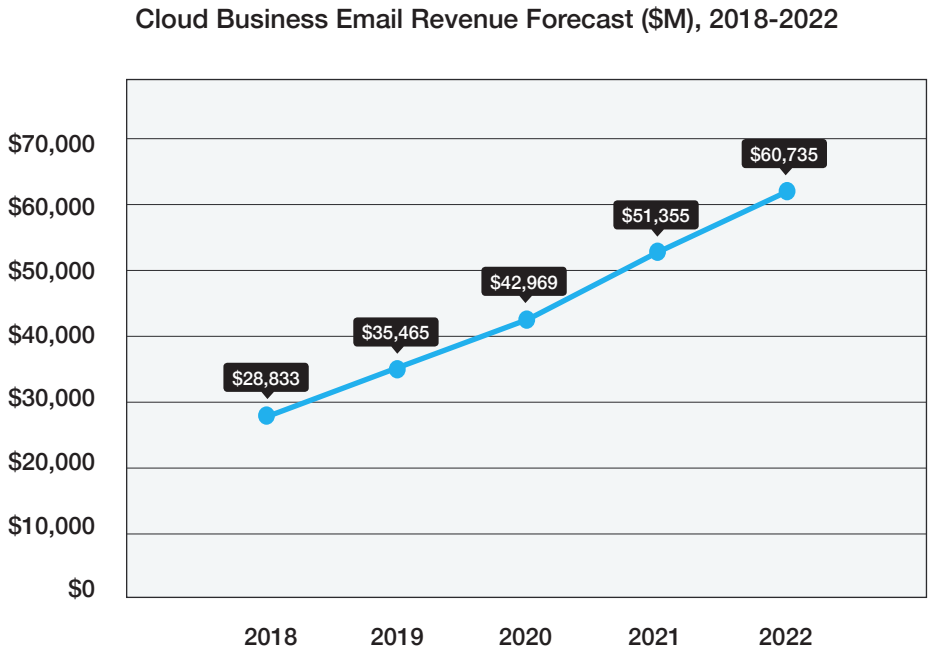
Contents

Why MSPs Should Offer Cloud Backup for Office 365

Office 365 backup and archiving are one of the fastest growing revenue-generating business services for MSPs, Distributors and IT Services firms. Why? Because profiting from the multi-billion-dollar Office 365 backup and archiving industry is easy to do, requires almost no administration, and provides value to customers. As dangers such as ransomware, viruses and accidental or malicious file deletion grow, protecting customers becomes more and more crucial. Perhaps most importantly, offering Office 365 backup and archiving ensures service providers can meet data availability SLAs with minimal effort. By using a cloud-based SaaS backup and archiving solution service providers can profit from incremental revenue, enjoy a stickier relationship with customers and grow their business across channels and verticals.

Storing and accessing email and related business data online has turned into a multi-billion-dollar industry. This creates both challenges and opportunities for MSPs, IT Service providers and other firms offering Office 365 services to their customers.

In fact, just the email portion alone of the cloud business solutions revenue is estimated at $28B for 2018 by technology market research firm Radicati. And that number is forecast to explode to more than $60B by the year 2022[1].This represents an astronomical increase of over 200% in just four years.



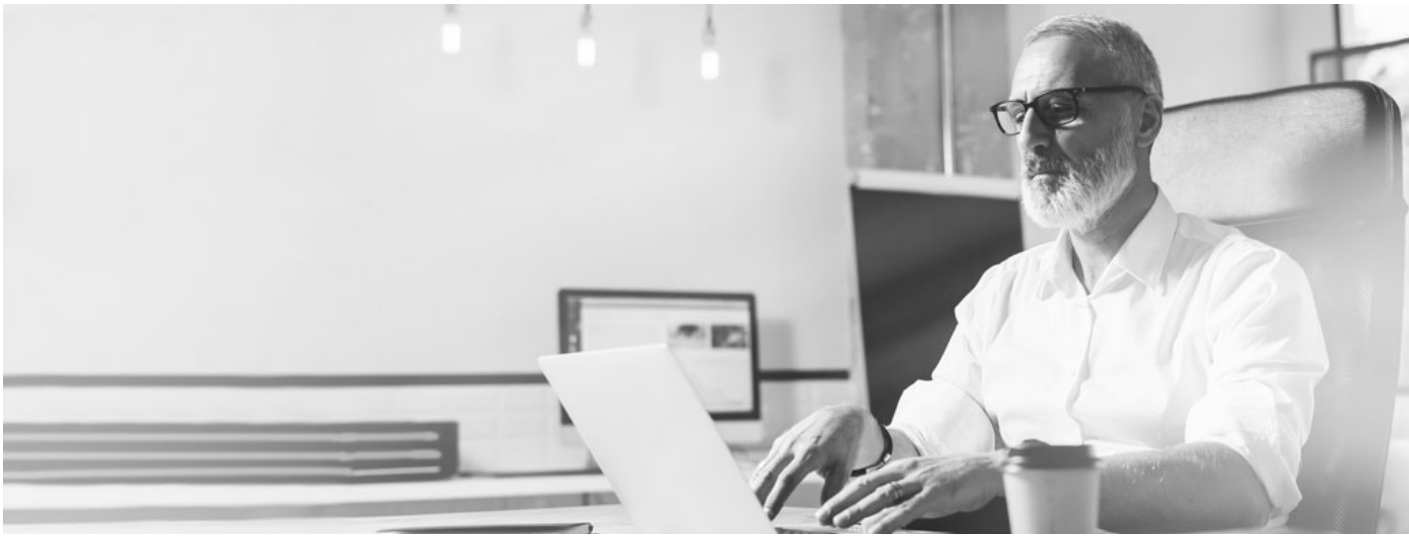
Source: Cloud Business Email Market, 2018-2022, The Radicati Group.

This paper introduces the cloud-based SaaS (Software as a Service) Office 365 backup, archiving and restore model as a means to:

1. Meet the challenges MSPs and IT Servicers face in providing customers with Office 365 data security, business continuity, and data storage in an increasingly threatening cyber criminal environment
2. Ensure SLAs are met should a ransomware or data hack compromises customer O365 systems.
3. Enable a means of offering value-added services to their customers that provide incremental revenue opportunities while limiting the need for extra resources or infrastructure.
4. Provide additional 'stickiness' to the customer relationship by adding security and peace of mind.

Microsoft is responsible for the infrastructure and uptime of the cloud and the Apps within Office 365, but customers are responsible for the access and control of your Office 365 data in Exchange Online, SharePoint, OneDrive, etc. Microsoft is responsible for the IT structural role providing user & admin security, physical security, app security, etc., but customers are responsible for internal data issues such as accidental employee theft and accidental deletion - to external data issues like Phishing and Ransomware.

DANGEROUS MISCONCEPTION OF OFFICE 365 SECURITY BY BUSINESSES

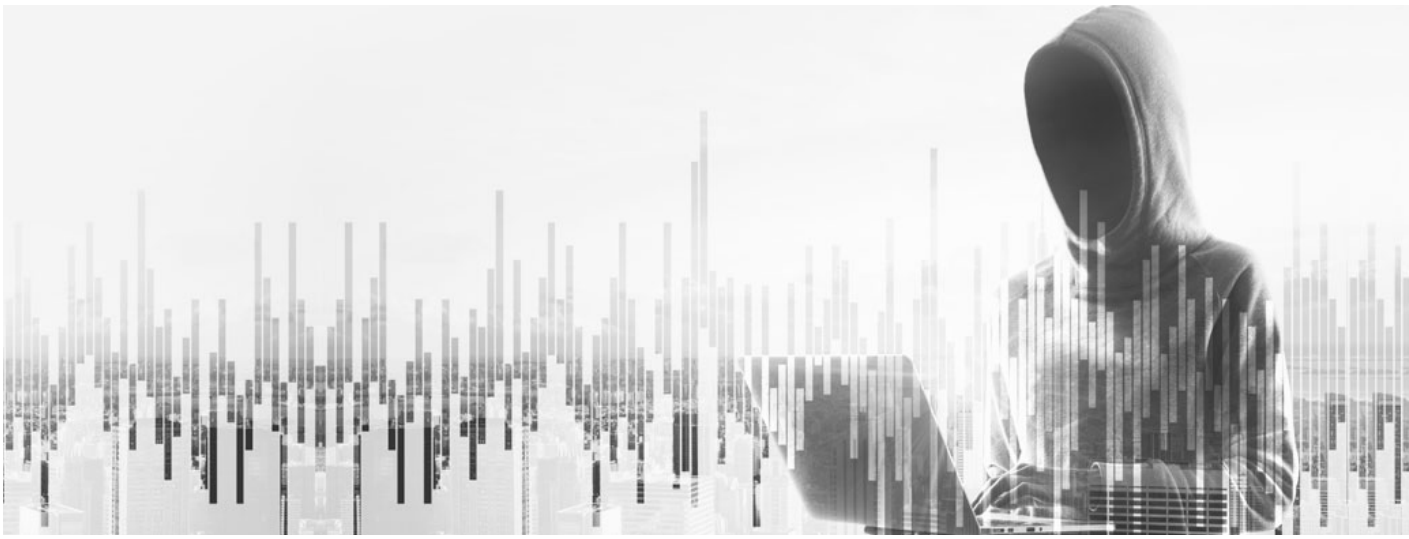


Many businesses using cloud-based environments such as Office 365 assume their email and related data are easily available to restore from backups, because it's all 'in the cloud.' But the reality is, that's not the case. For example, with Office 365 there are default limits for how long email files remain in the recycle bin before being permanently deleted. In addition, ransomware or malicious file deletion can permanently destroy email files in the Office 365 environment. The only way to truly protect cloud-based email data is with separate backups.

Microsoft is not in the data backup on demand business — and with cyberthreats on the rise, businesses can no longer risk exposing their brands to unexpected data loss events such as ransomware, phishing attacks, rogue employee theft, or accidental deletion.

Microsoft is not in the data backup on demand business

INCREASING NUMBER AND COST OF CYBER ATTACKS



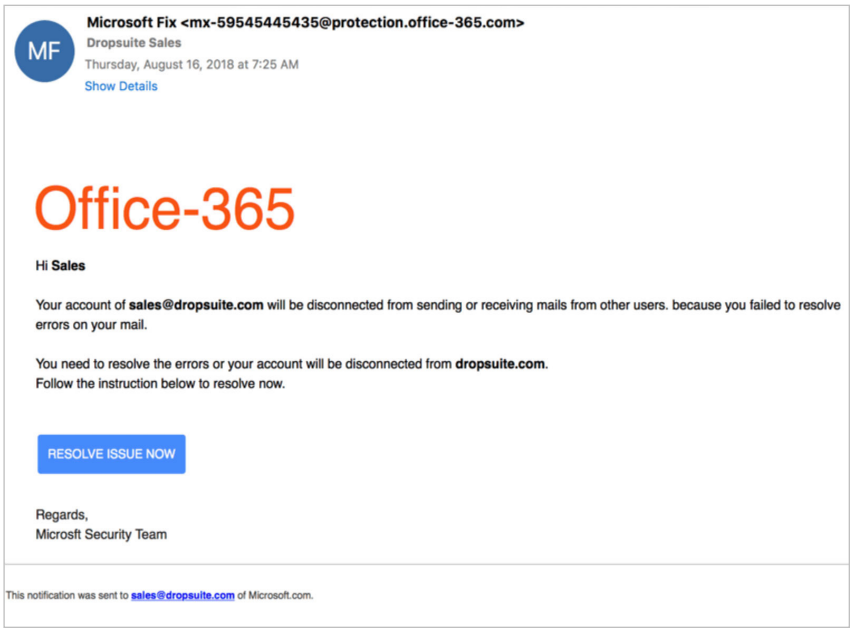
It is a fact that there has been an increasing number of ransomware and cyber attacks on businesses of all sizes, and those attacks have been getting more and more disruptive. The statistics from a survey of business executives speak for themselves[2]:

- 53% of U.S. businesses were cyber attacked in the past year
- 72% of businesses spent $5,000+ to respond to attacks
- 38% of hacked businesses spent more than $50,000 to respond
- 10% spent $100,000 to $250,000
- 7% spent more than $250,000

What is clear from those numbers is the devastating impact a hack can have on a business, especially small businesses with little means to immediately respond with resources and money.

OFFICE 365 AND PHISHING SCHEMES

Finally, there is an alarming increase in the number of businesses receiving phishing emails such as the one Dropsuite received below that look deceptively like an official Office 365 email. All it takes is one employee to accidentally click the button and the Office 365 system can be hacked.



MF

Microsoft Fix <mx-59545445435@protection.office-365.com>
Dropsuite Sales
Thursday, August 16, 2018 at 7:25 AM
Show Details

Office-365

Hi **Sales**

Your account of **sales@dropsuite.com** will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from **dropsuite.com**.
Follow the instruction below to resolve now.

RESOLVE ISSUE NOW

Regards,
Microsft Security Team

This notification was sent to sales@dropsuite.com of Microsoft.com.

THE GOLDEN RULE OF DATA SECURITY

It is important to remember that data security is only as strong as the weakest link in the chain. And remember the golden-rule of data security:

"It's not IF you'll be hacked, it's WHEN."

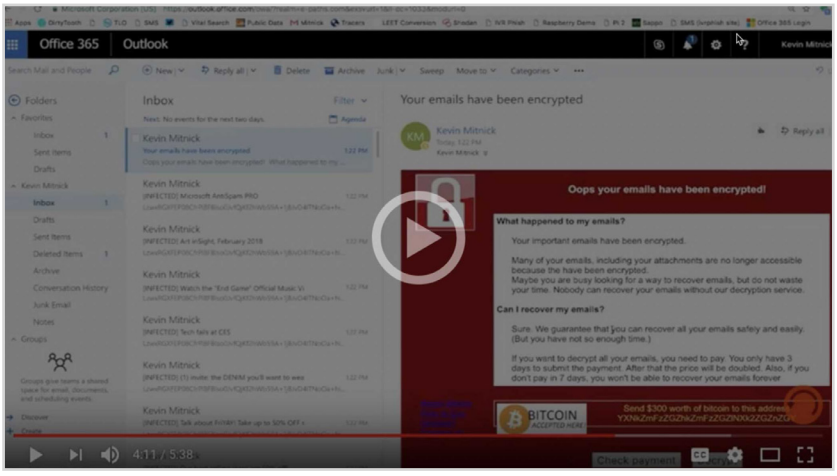
The only way to truly protect Office 365 data is to provide daily backups in a separate location of all of Office 365 files including:

- Exchange Online
- SharePoint/OneDrive
- Calendar
- Tasks
- Contacts
- Teams files

WATCH HOW FAST A HACKER CAN COMPROMISE AN EMAIL SYSTEM

This video from a former hacker, Kevin Mitnick who now uses his skills for good clearly shows how fast an email system can be compromised and encrypted. Once the encryption is complete (a matter of seconds) the ransomware is in place and the demand for payment is sent.

This video (https://youtu.be/VX59Gf-Twwo) provides a sobering view of the reality Office 365 email systems now face, which is a cyber threat will happen too fast for any kind of manual response.



THE DIFFERENCE BETWEEN EMAIL BACKUP AND EMAIL ARCHIVING

The terms email backup and email archiving are often confused within the industry, with many people erroneously believing they are essentially the same thing, when in fact they are not.

EMAIL BACKUP:

Essentially, email backup is designed as a short-term insurance policy to facilitate the quick recovery of email files that may not be readily available due to an unexpected data loss. Data loss can include; accidental deletion of critical email files, a ransomware attack or losing access to emails due to accident, theft, or sabotage. With email backup, users can typically select a date in time and restore a copy of any email or a group of emails from a prior date in time.

The modern way email backup is performed is in the cloud. The cloud is generally faster, cheaper and scalable to meet the changing needs of businesses. Other email backup methods include on premise software backup or external stage devices.

The modern way email backup is performed is in the cloud

EMAIL ARCHIVING:

Email archiving is designed to provide ongoing, rapid access to decades of business information (email files, attachments, calendars

and tasks). For many companies in regulated industries such as financial services, healthcare or law firms, email archiving is required by law because it provides specialized tools for making email records tamper-proof, searchable and retrievable in the event of an audit, HR inquiry or lawsuit.

There are many more features included in email archiving than in email backup, such as:

- Envelope journaling
- Advanced search
- Legal hold
- eDiscovery
- Audit trails
- Customizable retention periods
- Unlimited retention and more

Email archiving is an act of legal preservation, making searchable all email to/from an individual. In the event a company is audited or sued, archiving can help shine a “forensics light” on all content, as well as point of entries and exits.

While email compliance is burdensome, non-compliance can be catastrophic, especially for a smaller company that lacks the resources to endure lengthy audits and pay hefty fines. Many firms may not be fully aware of all the regulations affecting them, so may be at risk of violation.

WHY MSPS SHOULD OFFER OFFICE 365 BACKUP AND ARCHIVING

Now that the differences between backup and archiving are obvious, it is clear why MSPs should choose to offer both to their customers. First, backup is useful for protecting data, but archiving is necessary for preserving data and meeting regulatory or legal obligations. MSPs who offer both ensure their customers are protecting and preserving their data. Second, highly regulated industries such as finance, insurance, law firms, healthcare and more require both email backup and email archiving to meet compliance requirements. This provides opportunities for MSPs to branch into new customer channels and verticals by offering archiving where they may not have had inroads before.

DEBUNKING MYTHS ABOUT EMAIL BACKUP

There are plenty of myths when it comes to backing up email in Office 365. Addressing these myths and educating businesses is more important than ever given the risks.

For just a few dollars per seat per month, firms can protect valuable data and ensure that accidental or malicious data deletion doesn't disrupt business

Myth #1: We don't need email backup and archiving because Office 365 already does this.

Office 365 apps only back up deleted files for up to 30 days.

Microsoft file sharing apps are not backed up. File sharing is built for real-time collaboration with user content, but it is not designed for data recovery in the case of user error, data corruption, or ransomware. Nor does it address archiving or a completely new set of compliance and eDiscovery challenges.

However, if you purchase the E3 license or above, you do get an archiving solution. However, it's expensive and difficult to set up and use. And worse, emails and other files such as attachments can still be deleted unless you put them on litigation hold — so the risk of data loss remains.

Myth #2: Email backup and archiving are too expensive.

The reality is, for just a few dollars per seat per month, firms can protect valuable data and ensure that accidental or malicious data

deletion doesn't disrupt business. Compared to what could happen to a business if their data disappears, is held hostage, or is corrupted, a few dollars a month per seat seems like a very cheap alternative.

In a report released by Ponemon Institute[3], the average SMB data breach is 9,350 records, yielding costs between $841,000 – $2.85 million. The cost of secure backup, archiving and recovery is far cheaper than the cost of trying to recover from a breach.

In that context, the cost of pennies a day to backup and have data restored with the click of a button is not expensive at all.

Myth #3: Only regulated businesses need data backup and archiving.

Most businesses need backup and archiving, whether they know it or not. Although it's true that regulated businesses like Healthcare, Financial Services and Law Firms have additional requirements regarding data backup, archiving and access, all firms should consider using some form of auxiliary backup and compliance data storage.

There are multiple reasons non-regulated businesses might find email archiving features valuable:

- Audits may require them to provide full and accurate data that may go back many years
- Lawsuits or regulator investigations may require Office 365 data to be put on legal hold so that it cannot be altered or deleted
- The fast universal search tools found in archiving systems can speed up search queries across email, SharePoint, OneDrive and Teams in one action. Time saving tools are valuable assets.

Myth #4: Backup is over-hyped and doesn't need to be a priority.

Backup is never a priority, right up until the time something goes wrong. Then, it becomes the most important priority for the business. The reality is, without backup any business is at risk.

Myth #5: All email backup solutions are the same.

In fact, they are not.

- Many solutions are clunky to use, with poor UX designs
- Many were on premise vendors who ported over their software which must be downloaded as an agent for it to work — they were not born in the cloud
- Many email backup vendors don't offer a comprehensive solution - For example: email backup and archiving are not sold as a single product
- If they are comprehensive, their solutions are sold in modules that can be very expensive if a firm wants to have them all
- Few, if any, offer complimentary email business insights and analytics

There are a variety of backup solutions available on the market. From the native solutions that are not comprehensive and require a lot of effort to manage, to cutting edge cloud solutions such as Dropsuite. Dropsuite Office 365 Email Backup is born in the cloud, easy to use, comprehensive, a great value for the money, all data is exportable, and includes a comprehensive email analytics tool – Insights BI, for free.

THE ADVANTAGES OF SELF-SERVE OFFICE 365 BACKUP

What is the Self-Serve SaaS Office 365 backup model?

The model uses Microsoft Graph APIs, EWS and also PowerShell to automatically back up emails and One Drive / SharePoint files. As an MSP or IT Solution Provider, you offer the product to your end-users as a bundled solution or as a opt out offering in your signup process. Your investment in the infrastructure is minimal.

Integration is quick and easy using an API or control panel plugins to set up signup and access. End-users get direct access to their Office 365 backup interface for self-serve administration and account recovery through a single pane of glass interface.

Offer Office 365 Backup to your end-users as a bundled add-on, either at signup or through their control panel

REVENUE OPPORTUNITIES

Opportunity 1

Zero overhead and higher revenue per account

A self-serve Office 365 backup solution creates no-risk revenue opportunities for MSPs, especially when offered as a low-cost add-on as part of a bundled offering.

Since this is a self-service product, MSPs do not need to invest in the human resources necessary to support Office 365 backup and recovery. Even for larger accounts, there will typically be an administrator at the company who will handle issues, just as that person handles issues with regular business systems. It also creates revenue opportunities for a service (Office 365 backup and recovery for data protection) that the MSP customer doesn't even typically buy from the MSP.

Opportunity 2

Increased customer stickiness

As we suggested earlier, MSPs are missing out on the opportunity to generate revenue on Office 365 backup and recovery usage. A self-serve SaaS O365 backup solution is compatible with third-party services but offered by the MSP, typically at the account signup process as a bundled product offering.

Once Office 365 backup is connected to the account, the customer will be less likely to move to a new MSP. The MSP has increased the stickiness of the account, and also helped improve the customer experience by offering a valuable, flexible, business-critical solution at a low cost.

If a disruption occurs for whatever reason, the backup structure of Self-Serve SaaS enables faster recovery through an intuitive interface. Both MSP and end-user (or administrator) can troubleshoot and resolve the issue with minimal business disruption. If the email disruption were to occur at the same time as a website disruption (hacking, malware, etc.), more energy and resources can be put into isolating and cleaning up the website issue because the email disruption is easily managed. It should be noted that Self-Serve SaaS website backup exists for sites and their databases as well, offering the same intuitive interface and benefits for a positive customer experience with their web files.

Opportunity 3

Attract accounts with specialized requirements

Heavily regulated industries such as Accounting/Finance, Healthcare, Law Firms, Manufacturing, Government and more are required to have a specialized product called Email Archiving to meet industry regulations.

Email archiving includes additional email data functions and features that provide among other things:

- eDiscovery
- Audit Trails
- Advanced Search
- Envelope Journaling
- Legal Holds
- Third Party Audits
- And more

This means MSPs who offer fully-compliant email backup and archiving can prospect lucrative verticals that would ordinarily pass over their typical services.

Opportunity 4

Provide an all-in-one Office 365, email backup and archiving and 1-Click restore SaaS solution

Self-serve SaaS Office 365 backup combines all three types of data backup needs into one service. This all-in-one solution includes Office 365, email backup and archiving, and 1-Click restore in a single pane of glass dashboard. Note that most backup providers will only offer single solutions at different product or pricing structures, such as email backup only, email archiving only, limits on backup storage and restores, etc.

However, MSPs should note that all-in-one solutions do exist. An example is Dropsuite's Office 365 Email Backup and Archiving solution which uses a single pane of glass dashboard to manage automated backups, archiving, 1-Click restore and has options for unlimited data storage and restores.

An all-in-one solution includes Office 365, email backup and archiving, and 1-Click restore in a single pane of glass dashboard

CONCLUSION

From the market forecast referenced earlier, we can estimate that there is massive revenue potential for MSPs and IT Service Providers who offer Office 365 backup and archiving as part of their solutions package. There is ample opportunity to capture a share of that market by adding self-serve SaaS email backup and archiving solutions to the service mix, which provides incremental revenue, improved customer retention and the ability to penetrate verticals that are required to have specialized archiving products.

Should You Resell Office 365 Backup?

As an MSP or IT Service Provider, ask yourself these questions:

- Do you want to increase your average revenue per user?
- Are you wanting to increase your margins?
- Would you like to reduce your customer support costs and increase customer stickiness?
- Could you increase customer satisfaction and reduce churn by delighting your customers?
- Are you interested in doubling your money selling Office 365 backup?

If Yes, Review These Dropsuite Reseller Benefits

- Office 365 compatible/easy bundle
- Recurring revenue stream
- Improved customer stickiness
- Reduced support costs
- Zero product development costs
- Cross sell opportunities with flexible pricing

ABOUT DROPSUITE

Dropsuite Ltd (DSE:ASX) safeguards business information. We are a partner-centric company building secure, scaleable and highly usable cloud backup technologies for businesses. Our mission is to ensure organizations never lose data gain. We do this by providing professional-grade, easy-to-use, cloud-to-cloud products such as:

- Office 365 Backup
- Email Archiving
- G Suite Gmail Backup
- Website Backup

For MSPs looking for a more comprehensive data management solution that meets regulatory compliance requirements such as HIPAA and GDPR, an optional, journaling-based email archiving tool can be activated within Dropsuite's single pane of glass control panel for ease of management.

We also offer critical solutions such as:

- Ransomware Protection
- Compliance (GDPR, HIPAA)
- Insights BI (email intelligence)
- eDiscovery

Dropsuite's network of preferred reseller partners has a combined customer reach of millions of businesses worldwide.

References:

(1) Cloud Business Email Market, 2018-2022, The Radicati Group.

(2) Half of U.S. Businesses Report Being Hacked, September 29, 2017, Insurance Journal.

(3) 2017 Ponemon Institute Study Finds SMBs are a Huge Target for Hackers, PR Newswire, September 29, 2018