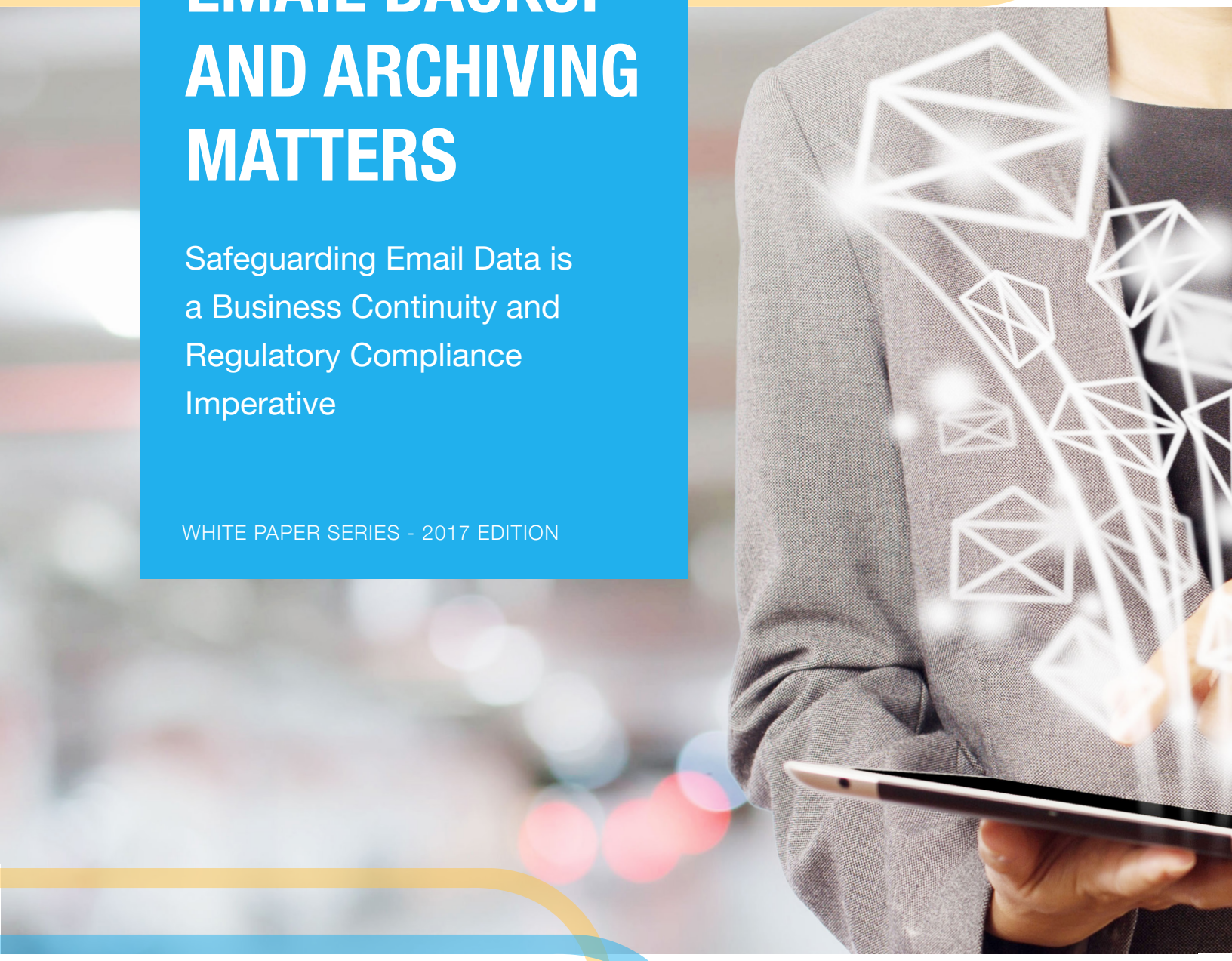
Dropsuite

EMAIL BACKUP AND ARCHIVING MATTERS

Safeguarding Email Data is a Business Continuity and Regulatory Compliance Imperative

WHITE PAPER SERIES - 2017 EDITION



Contents

SMBs Run on Email

Small to Mid-Sized Businesses (SMBs) are the growth engine of economies around the world. The great majority of SMBs depend on Information Technology to run operations, engage and retain customers, manage supply chains, and deliver products and services. For most, email technology is the critical means of business communication. A recent study sponsored by Dropsuite found SMB respondents describing the potential total loss of their email data as “severe” and “devastating” to their business, particularly for any aspect of the business involving customer interaction[1].

But email also has another dimension—business protection. Compliance demands are escalating, as are lawsuits. Privacy protections are on the rise globally. With SMBs struggling to keep up with the endlessly growing scope of business demands, changes in technology, and increasing regulations, proper protection of email, which is integral to proper protection of the business, can be overlooked. Many SMBs aren’t even aware of the breadth of risks.

Because many SMBs turn to solution providers— Managed Service Providers (MSPs), web hosters and Internet Service Providers (ISPs)—to manage or even completely outsource their IT, those solution providers have an opportunity, and perhaps even a responsibility, to guide their SMB customers about thorough email protection practices. They themselves must understand the business needs and risks around email backup, archiving and eDiscovery, especially in highly regulated industries, to deliver the reliable, inclusive solutions SMB customers are counting on. This paper offers a primer on some of the principle concerns.

[1] Source: The Perception Gap: How SMBs and MSPs See Data Protection Differently © Dropsuite - 2017

How Is SMB Email Vulnerable?

There are three main areas of risk that should compel SMBs to archive their emails as a business protection best practice: data breaches, lawsuits and compliance.

Data Breaches – Not Just for Big Business

While major breaches like Yahoo, Anthem and Target get big headlines, in reality, cyber criminals are increasingly targeting smaller businesses. SMBs often lack the security awareness and defense mechanisms that large enterprises have, making them easier to penetrate. For a smaller business with tight resources, the effects of a breach can be far more detrimental than for a larger corporation who has better reserves to weather such a storm. In fact, according to Security Magazine, about 60 percent of hacked SMBs go out of business after six months.

As of mid-2016, only 31 percent of smaller businesses reported taking active measures to guard against breaches; 41 percent were unaware of the risks coming from human error; and 22 percent were willing to improve their security measures from 2015. Yet the costs of a breach can be substantial, averaging $36,000-$50,000 per incident.

Financial Services Incidents, 2016

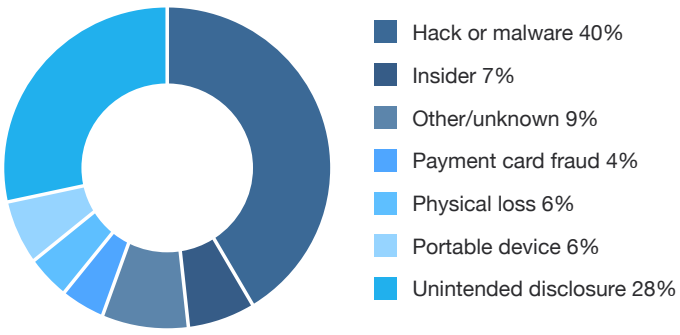
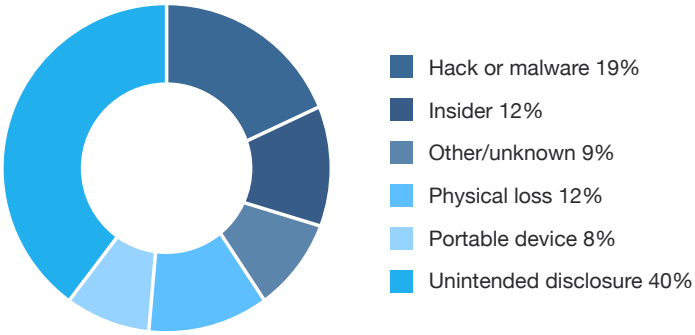


Chart source: Beazley Data Breach Insights Jan 2017

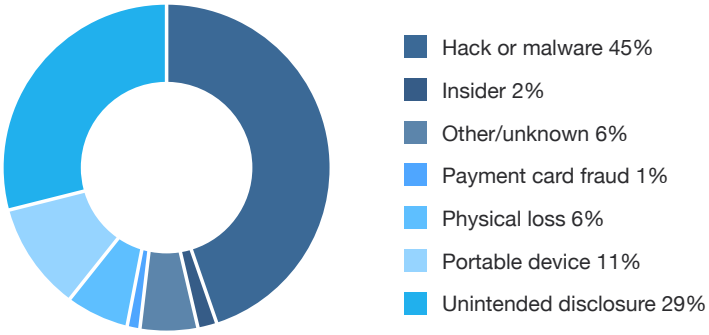
Those costs stem from a broad range of breach consequences: loss of data, loss of finances, loss of customers, legal fees, fines, and the costs associated with mandatory breach notification steps. Longer term, there can be lawsuits, reputational damage, added technical infrastructure costs and other costs associated with additional third party services that may be called into the mix.

Healthcare Incidents, 2016



Among the most common threats that successfully penetrate SMBs are email phishing attacks. For example, go-cart racing business Maine Indoor Karting was hit by a phishing scam in 2015 that resulted in its bank account being wiped out. The theft was discovered on a payday, creating a huge problem for business owner Rick Snow and his employees who were depending on those paychecks. Snow noted during Congressional testimony in 2016 that "Phishing can happen to anyone, phishing attacks are meant to scare you and make you act without thinking, and given the right circumstances, anyone can be lured by them. I am certainly no exception.[1]"

Higher Education Incidents, 2016



Many SMBs fail to realize that hackers aren't just targeting large organizations worth millions in annual revenue. They're also infiltrating small businesses because circumventing company firewalls, antivirus software, and other security measures can sometimes be easier — tough safeguards may be less prevelant — requiring less time and effort to breach.

[1] http://www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-businesses-on-rise.html

Email is especially vulnerable to security breach intrusions because SMB staff may be more easily lured into traps laid by external bad actors. SMBs often don't have strong threat mitigation policies and procedures in place — and if they do, they often don't conduct enough awareness training or conduct regular audit activities.

Email is a critical business communication tool. Essential company information, intellectual property, and documents are easily forwarded with one mouse click. Data such as personally identifiable customer information, banking & investment details, health stats, and technology schematics are susceptible to rogue third-party hacker breaches. Corporate email data is not something business leaders want falling into the wrong hands.

Email backup protects SMBs if a data breach should ever destroy/infect email data such as email communications, attachments or calendars. Email data that has been backed up remotely can be retrievable to a date prior to the breach, ensuring that a full email restore will be hacker-free.

Email archiving is the act of preserving and making searchable all email to/from an individual. So if you have a data breach, the archiving feature of your email backup may help shine a "forensics light" on the point of entry for the breach.

In the same way you insure your home or automobile against unexpected losses, smart businesses regularly backup and archive their email information to protect their livelihood and stay one step ahead of the bad guys.

Make no mistake — cyber criminals are targeting your emails and want to inflict harm on your business so they can profit. It's no longer a matter of if an attack on your data infrastructure will happen — it's only a matter of when.

Healthcare accounted for one-third of 2016 data breaches, with employee error and subcontractor issues being key factors… According to Beazley, accidental email or internet exposure was the second

Lawsuits on the Rise

Another significant risk to SMBs is lawsuits. Annually, over 50 percent of all US civil lawsuits target small businesses. Any business can be sued at any time for a broad range of reasons. Whether suits are frivolous or grounded, a response is always required, and a defense frequently is. For SMBs, the most common suits are around employee claims of discrimination, wrongful termination, or wage and hours violations. Contract disputes are also a leading cause, accounting for about 60 percent of 20 million cases filed each year in the US[2].

In 2014, more than one in ten (13%) of small business owners had been sued by an employee, customer or vendor. Of those, nearly half (47%) admitted the lawsuit negatively affected their business financially (29%), resulted in the loss of customers (13%) or negatively affected the business' reputation (12%).

According to legal services firm Rocket Lawyer, keeping good records is a critical step in protecting a business in the event of a lawsuit. They note that "there's nothing like having well-documented facts on your side to prove your argument or to avoid conflict all together." Part of those well-documented facts should include a thorough email trail, accessible through eDiscovery of thoroughly archived email correspondence.

[2] http://richardpalumbo.com/lawyer/2016/06/06/Business-Law/Common-Frivolous-Suits-Filed-Against-Small-Businesses_bl25399.htm

Compliance—a Bane of Many SMBs' Existence

Perhaps the most challenging area of risk for SMBs is the increasing amount of regulation and oversight to which many are subject. Email backup, eDiscovery and compliance are particularly important for those in heavily regulated industries who deal in sensitive information such as healthcare, government and financial services.

While 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 SMBs may not be fully aware of all the regulations affecting them, so may be at risk of violation.

Solution providers who can educate their SMBs clients about the risks of non-compliance will help them avoid costly fines, revoked permits or other repercussions. They will also establish themselves as trusted advisors who stand to reap long-term relationships with those customers.

In late 2015, the US Financial Industry Regulatory Authority (FINRA) fined discount brokerage firm Scottrade $2.6M for failing to retain a large number of securities-related electronic records in the required format, and for failing to retain certain categories of outgoing emails.

Scottrade (now acquired by TD Ameritrade) relies on a network of independent registered investment advisors to represent its investment products. Email is a primary means of communication with that channel[3].

Compliance Requirements Vary by Industry, Country

There are a wide range of local, federal and international regulations involving data archiving and record keeping. SMBs must be aware of what governs their business, both where it is geographically located and where it may transact, and take steps to ensure they remain compliant. Some of the most important US regulations include:

Federal Rules of Civil Procedure (FRCP). These regulations affect all industries and require that companies be prepared to present electronic records in the event of a lawsuit. Recent changes to FRCP narrow the eDiscovery window, requiring companies to produce records more quickly but also limiting the scope of records that are required. This means that SMBs must now store a smaller amount of information than before, but in more readily available formats.

Health Insurance Portability and Accountability Act (HIPAA). Healthcare providers are subject to federal regulations that require patient health information (PHI) to be kept in an encrypted format. It is important for organizations to ensure their employees are using a secure and encrypted platform when handling PHI.

The Sarbanes-Oxley Act (SOX). This law requires all publicly traded companies in the United States to keep their electronic data for up to seven years, depending on the type of data. For larger companies this can run into thousands of petabytes of data and cost many hundreds of thousands of dollars.

[3] Source: https://www.forbes.com/sites/anthonynitti/2013/03/25/what-are-your-odds-of-being-audited-by-the-irs/#575d9bfe5d97

Financial Regulations. The US financial services industry is one of the most heavily regulated with regards to data archiving. The plethora of financial regulations means that financial services companies must have a strong email archiving solution that enables them to stay in compliance and access email records easily if audited.

- The Financial Industry Regulatory Authority (FINRA) regulates 3,800 broker-dealers with 635,000 brokers, and requires organizations to monitor and archive broker communications.
- The Securities and Exchange Commission (SEC) Rules 17a-3 & 17a-4 require a dealer or broker to preserve documents and records for three to six years, and for the first two years they must be in an accessible location.
- The Gramm-Leach-Bliley Act requires financial institutions to protect the security, confidentiality and integrity of non-public customer information through administrative, technical and physical safeguards

The European Union General Data Protection Regulation

For businesses transacting in the European Union, May 25, 2018 will bring a significant change with the enactment of the General Data Protection Regulation (GDPR). This sweeping new law (a significant step beyond the old General Data Protection Directive) provides a rigorous framework for protecting the data of EU citizens, and will define good business practices around handling that data. The GDPR applies to any organization, wherever it is located, that handles personal data of EU citizens and legal residents, wherever they reside. Provisions affecting data access, consent, data portability and mandatory breach notification will require changes to many companies' data handling practices. One of the more significant requirements is the obligation to report a data breach to the regulator and those affected by the breach within just 72 hours of it happening. The law also allows for enormous fines up to 4 percent of annual revenues for non-compliance. Clearly any company doing business in or with the European Union needs to pay careful attention to data collection and handling – including email data.

Table 1 lists some of the most important laws and regulations governing businesses operating in the US. Table 2 shows just a few of many regulations governing business in other parts of the world. It is particularly important for organizations doing business in these sectors and countries to archive and preserve their email communication so it can be easily recoverable via eDiscovery if needed.

Table 1. Laws and Regulations Governing US Entities (Partial List)

All Companies	Internal Revenue Services – income tax
All Federal and State Agencies	Freedom of Information Act (FOIA)
All Public Companies	Sarbanes-Oxley Act (SOX)
Banks and Financial Institutions	Federal Deposit Insurance Corporation (FDIC)
Banks	Federal Deposit Insurance Corporation (FDIC)
Credit Card and Card Processing Companies	Payment Card Industry Data Security Standard (PCI DSS) (self-regulatory)
Department of Defense Contractors	DOD 5015.2
Healthcare	Health Insurance Portability and Accountability Act (HIPAA)
Investment Advisors	Securities and Exchange Commission (SEC) 204-2
Pharmaceuticals, Biological Products, Food Manufacturers	Food and Drug Administration (FDA) Title 21, Part 11
Securities Firms, Investment Bankers, Brokers eand Dealers; Insurance Agents	Securities and Exchange Commission (SEC) 17a(3) and 17a(4)
Telecommunications	Federal Communications Commission (FCC) Title 47, Part 2

Note: All organizations should consult legal and financial professionals to ensure they fully understand their obligations.

When assessing appropriate fines for disciplinary sanctions, the US Financial Industry Regulatory Authority (FINRA) FINRA has advised adjudicators to consider a firm's size with a view towards ensuring that sanctions are remedial in nature and designed to deter misconduct instead of being punitive. However, though adjudicators are given leeway to consider the firm's size, FINRA also notes that if a violation is egregious in nature, the firm size should not be considered.

Source: https://www.davispolk.com/sites/default/files/schwartz.chehardy.insights.securities.markets.article.dec15.PDF

Table 2. Entities and Regulations Governing Non-US Countries (Partial List)

European Commission	• EU General Data Protection Regulation (GDPR) - Enforcement as of May 2018 • EU-US Privacy Shield
Office of the Australian Information Commissioner	• Australian Privacy Act • Telecommunications Act of 1997 • National Health Act of 1953
APEC Ministers (numerous countries)	Asia-Pacific Economic Cooperation Privacy Framework (voluntary compliance)
Office of the Privacy Commissioner of Canada	Personal Information Protection and Electronic Documents Act of 2000 (PIPEDA)
Japan Ministry of Internal Affairs and Communications	Multiple communications Acts
Hong Kong Office of the Privacy Commissioner for Personal Data	Personal Data Ordinance

What are a business' chances of an Internal Revenue Service audit?[4]

Type of Return: Corporate	**# of Returns Filed**	**# of Returns Filed**	**% Audited**
Total	2,000,000	33,000	1.6%
Assets under $1,000,000	1,200,000	11,000	0.9%
Assets > $1,000,000 but < $10,000,000	1,200,000	11,000	0.9%
Assets > $10,000,000	58,000	10,000	17.2%

Type of Return: Pass-through	**# of Returns Filed**	**# Audited**	**% Audited**
Partnership return	3,500,000	16,700	0.5%
S Corporation return	4,400,000	22,000	0.5%

[4] Source: Internal Revenue Service 2014

Attaining Effective Compliance

Companies looking to optimize their compliance practices should strive to balance three key goals: reducing their data footprint, reducing their risk and increasing their productivity. In many cases, these three goals can be at odds if SMBs are not engaging in best practices. Service providers can help their SMB customers attain compliance by both offering guidance on best practices and implementing technology solutions needed to affect them.

Reducing Data Footprint

To minimize cost and maximize efficiency, all companies should keep only the data that is necessary for normal business operations. This practice requires discipline, a knowledge and understanding of all relevant regulations, and a system that automatically retains data for the required amount of time. This combination will allow companies to reduce their storage expenses while minimizing their risk.

- Understand relevant regulations – Having a solid grasp of regulations governing their industry will enable all businesses to determine how long data needs to be stored and in what formats.
- Implement a comprehensive data archiving system – The electronic data storage system in use should be able to automatically delete data or transfer it to long term storage after the relevant time has passed. If any data is pertinent to an ongoing investigation or litigation, the data storage system should also be able to automatically prevent that data from being deleted, even if it is past its retention date. A strong data archiving solution will help ensure that the minimum amount of data is stored on expensive mediums, while requiring very little user input. This will help reduce risk of error and user workload.

Maximizing Productivity

Compliance takes time, but observing best practices will keep wasted time to a minimum. Best practices include implementing systems that make the process of archiving, eDiscovery and backup simpler.

- Provide easy-to-use features – Users should be able to search, perform eDiscovery and restore backed-up data easily through their chosen archiving platform. Its features should be simple to use, with comprehensive functionality for the actions that users need to perform.
- Enable email integration – Archiving systems should integrate with the company's current email solution, such as Office 365. This will allow for seamless archiving, eDiscovery and backup without users having to learn additional programs.

Reducing Risk

The ultimate goal of compliance is reducing risk. Systems that control access, retain data for only as long as truly necessary, and provide strong encryption will help organizations avoid breaches, non-compliance sanctions and other risks.

- Use strong encryption – At a minimum, modern solutions should use AES 256 bit encryption with Transport Layer Security (TLS) for data at rest and in-transit. This will keep data storage compliant with HIPAA and most other regulations.
- Control unauthorized access – Data should be protected both from unauthorized access and tampering. Unauthorized users must be prevented from viewing sensitive data, altering data or deleting data. This requires having a system that enables full access controls, with the ability to easily add or remove users. File access should also be monitored and user access traceable. This will provide additional safeguards against tampering, and allows for recourse in the event that unauthorized access occurs.

Office 365 – A Popular but Often Misunderstood Email Choice for SMBs

Microsoft Office 365 is one of the most comprehensive office productivity solutions available on the market today. This cloud-based suite allows companies to manage their emails, documents, and productivity tasks faster and more effectively than ever before. As a result, adoption of Office 365 is steeply accelerating.

The new security and compliance features in Office 365 are very thorough —- Microsoft has covered pretty much everything. Unfortunately, most SMBs don't have the domain knowledge or skillset to manage the breadth of functionality available to correctly set up Office 365 for handling the range of regulations that may apply to their industry. This is complex to understand even with a seasoned IT professional leading the effort.

Possible SMB Challenges Utilizing Office 365

- **Cumbersome legal hold** - If a mailbox is on legal hold, messages in it can still be deleted, but recoverable from recoverable Items folders until the hold expires. It is however, difficult to search messages in the recoverable items folders which would cause a delay in messages recovery.
- **Limited insights** – In order to ensure compliance, legal representatives or auditors might need to review some communications coming into and going out of the company. In Office 365, designated users can generate some reports about communication activities, such as when a user receives an email or when they move an email to a different folder, but they may not be able to ascertain whether a specific email was read or viewed.

The Office 365 installed base has increased to 85 million commercial users and 24 million consumer users — with 50,000 small business customers being added every month.

Even so, less than 15 percent of US-based small and medium-sized businesses currently use Office 365, creating significant potential for future upside.

Source: Microsoft's earnings report Q1 2017

- **Difficult migration** – Office 365 only allows users to migrate emails using Personal Storage Table (PST) download and upload. This creates additional risk because data can be tampered with via PST.
- **Difficult setup** – Office 365's archiving setup is very time intensive and difficult. Users must manage retention tags, policies and controls to ensure emails are properly archived. This requires a significant amount of time and resources, which most SMBs simply don't have.
- **Mobile disconnect** - Online Archive is not accessible from the Office 365 Mobile App (at least not yet). With mobile B2B use at a record high, why settle for being disconnected from your online archived emails?
- **Eggs in same basket** - Office 365 Archive resides in the same location as Mailbox. This is not a data backup best practice. Ideally, your businesses email data should be multiple, redundant locations.

With native Office 365 features insufficient or too difficult to use for daily compliance needs, SMBs can be left exposed to fines, litigation, inefficiency and other business risks. It's imperative for many companies — especially SMBs — to find alternative solutions that complement and enhance Office 365's native backup, recovery and archiving capabilities. This provides another opportunity for MSPs and other providers to fill the gap.

Better Email Backup, Archiving and eDiscovery

If you are an IT solutions provider, how can you determine if your end user customers need to augment native Office 365 backup and archiving with additional solutions?

It's the job of an IT administrator or MSP to make sure that email backups are performed on a regular basis and that restores are verified. But before you begin, you'll need to determine if the native Office 365 backup and archiving solution meets your client's requirements. A good way to start is either during the new client pitch process or during a current client status review when you have the chance to ask probing questions that will help you determine a client's full email backup, archiving and eDiscovery needs. This next section provides some ideas on how to go about this.

Assess True Customer Needs

Start by looking at your SMB client's practices, regulations and industry to determine what their email archiving, backup and eDiscovery needs truly are.

- Look at how the customer uses their current solution (if they even have one). Each SMB organization has unique operational needs and practices. MSPs can meet with customers to determine which features they value and those they can live without.
- Perform a cyberthreat assessment test. Ask 10-12 simple questions that can help you assess client/prospect preparedness against cyberthreats. Those who score low are ideal candidates to pitch security, backup, compliance and redundant cloud recovery solutions as part of your client service packages. Here are four sample questions:

    1. My company has performed an 'asset tracking' inventory of all known hardware devices, such as laptops, company phones and database servers within the past 12 months. YES / NO / UNKNOWN
    2. My company has cyberthreat security policies in place, and has conducted awareness training and testing with all staff within the past 12 months. YES / NO / UNKNOWN
    3. My company has successfully conducted a data restore/data recovery test on its website databases, servers and email files within the past week. YES / NO / UNKNOWN
    4. My company has successfully conducted a sanctioned penetration test into our core company systems, devices, software and databases within the past 3 months. YES / NO / UNKNOWN

- Consider company size. Very large companies may be able get by with native Office 365 functionality because their IT departments are able to utilize a host of backup, recovery and archiving tools in their arsenal. However, SMBs often lack the manpower and tools required to sufficiently backup and archive email data according to industry standards. They need help — and it's the MSP that can guide them toward a professional email preservation and compliance solution.
- Assess their industry. Companies in highly regulated industries like financial services, legal services and healthcare will almost certainly need something more than Office 365's standard email backup offering. They will likely need to regularly perform eDiscovery and adhere to the many regulations imposed on them. To do that, they need solutions that are comprehensive and easy-to-use.

Questions Savvy SMBs Might Ask MSPs About Email Backup/Archiving

Are you prepared to answer the tough questions your more savvy SMBs might ask you about the email backup solution(s) you include in your standard service offerings? Here are a few topics that every MSP should be prepared to talk about.

What will it cost? An SMB that needs a robust email archiving system may be concerned about the fees an MSPs might charge them to set up, migrate and maintain an email backup and archiving solution. Many MSPs bundle this cost into their overall monthly service fee and then pitch email backup/archiving as a cost saver. The data migration process itself presents a unique opportunity to free up storage space by utilizing de-duplication. Less storage space needed usually equates to less storage fees over time. Once migrated, an SMB's lost emails can be restored much more quickly by the MSP, reducing IT hourly labor costs. The advanced search tools available in an email backup and archiving solution can also streamline litigation or audit preparation, reducing time/costs as well. In the long term, the threat of large liability costs decrease, thereby reducing actual costs related to legal or regulatory inquiries (people, processes and time reduction).

How does your archiver ensure the security of its data? An SMB's email documents should have the minimal baseline security safeguards in place such as:

- AES-256bit encryption
- DDOS mitigation technics such as SYN cookies and connection limiting protection
- Secure Socket Layer SSL encryption for data in transit
- Geo-distributed data centers with over 99% availability
- Compliant with common information security standards

How quickly can your archiver migrate pre-existing data? While this is by no means the most important software feature to look into, the average intake speed for migrating pre-existing email records is something an SBM may ask an MSP — so this is a product feature MSPs should ask their vendors about. A data processing architecture that was designed to cope with large amounts of data flow will yield better throughput performance metrics — speeding up the processing time for the initial migration of historical data. A quality email archiving vendor, such as a cloud backup and recovery firm, will be able to provide data throughput sustainability metrics that will demonstrate resiliency during the initial data set up process.

Does your archiver provide a professional feature set? There are different quality levels of email archiving. Professional grade email backup and archiving tools are a bit more advanced than the standard tools that some vendors provide. Examples include: eDiscovery, Boolean searching, search by attachment, legal hold, unlimited storage, alert creation, user access control management, attachment managers, advanced reporting, and more. MSPs should ask their data software vendors which professional grade, compliance archiving features are included in the email backup and archiving software they offer. Better to have these features ready at your disposal — especialy if your clients include companies in regulated industries who may be required by law to manage emails with professional grade compliance features.

Help SMBs Understand Compliance Best Practices

Best practices of email backup, archiving and eDiscovery may require a foundational restructuring of corporate policies, employee awareness training, and auditing activities. MSPs and other resellers can help their customers with these needs by advising them on how to stay compliant and improve their operations. This expert guidance will help SMBs adhere to best practices and perform these tasks as effectively as possible.

- Talk to key stakeholders throughout the company to understand their needs. End users are at the front lines of compliance, so their opinions are important. This will help make sure corporate policies are in tune with how the business works, and will improve policy adherence.
- Create effective policies. Creating well-crafted policies for email security, archiving and backup is a critical step to reduce risk and improve organizational productivity. These policies should cover all electronic messages, attachments and the systems that support them, accounting for any relevant regulations. If there is any confusion about rules, the SMB should consult with the enforcement agency to ensure its policies are compliant.
- Engage in awareness training. Policies are not effective unless employees are aware of and fully understand them. So, companies must engage in comprehensive awareness training for email handling best practices. All users should understand the rules and areas of risk so that email is handled properly. This is not a one-time practice. Regularly update training to make sure employees stay current.
- Conduct internal audits. SMBs should regularly conduct internal audits of their security and email handling practices to identify potential problem areas and prepare for audits by enforcement agencies. Internal audits should verify that all necessary emails are archived, secured and stored on the proper medium. They should also check for any evidence of impropriety, such as record tampering or unsecure transmission of sensitive data.
- Evaluate customer practices regularly. SMBs should always be improving their email archiving, backup and eDiscovery practices, but often lack the bandwidth to do so. By helping customers regularly review risks, identify issues and benchmark performance, solution providers have a high value-add opportunity to help customers improve and establish long-term trusted relationships.

Whenever possible, cloud solution providers should steer their customers toward low cost, easy to use, high-impact email message management tools that will help SMBs more effectively backup, archive and utilize eDiscovery. The right solution, combined with Office 365's robust functionality, will solve a wide range of real business problems.

References: [1] http://searchsecurity.techtarget.com/tip/Strategies-for-email-archiving-and-meeting-compliance-regulations

APPENDIX


Dropmyemail
archive@dropmyemail.com
DASHBOARD
ADVANCED SEARCH
EMAIL ATTACHMENTS
BACKUP STATUS
INSIGHTS
Dashboard
Add Email
2 seats of 10 seats used
Backup Emails
Search email account
View
Migrate
Restore
Download
Edit
De-Activate
Email Account
Number of Emails
Space Used
Last System Backup
charil@dropmysite.com
1200
25.5 MB
Jan 27, 2016 03:27 PM
john@hatcher.com
200
240 KB
Jan 10, 2016 02:59 PM
ron@dropmysite.com
1320
15.2 MB
Feb 12, 2016 04:40 PM
ridley@hatcher.com
200
240 KB
Jan 10, 2016 02:59 PM
Pending Invited Users
Resend Invitation
Delete
Email
User Attemps
Last Invitation Send
misuzu@dropmysite.com
0
Jan 21, 2016 14:32 PM
© Copyright 2012-2016 Dropmysite Pte Ltd.

How Dropsuite's Email Backup and Archiving Can Help

Dropsuite is a global cloud software platform enabling SMBs in over 100 countries to easily backup, recover and protect their digital assets.

OUR MISSION IS TO ENSURE SMALL BUSINESSES NEVER LOSE DATA AGAIN. DROPSUITE HELPS BUSINESSES STAY IN BUSINESS.

Our network of preferred reseller partners has a combined customer reach of millions of small and medium-sized businesses worldwide.

We work with some of the biggest names in website hosting and the managed services market such as Ingram Micro, the world's largest distributor of computer and technology products; GoDaddy the world's largest hosting company; Blacknight Solutions; the #1 hosting company in Ireland; GMO Internet, the #1 hosting company in Japan; HostPapa, the #1 hosting company in Canada; Singtel; the #1 telco in Singapore; and leading domain name registrar Crazy Domains in Australia/UAE.

Our cloud products include:

- Dropsuite Website Backup
- Dropsuite Email Backup & Archiving (Office 365 compatible)
- Dropsuite Server Backup

We are integrated with many popular control panels such as Ingram Micro, WHMCS, Plesk, cPanel, Odin, Hostbill, Parallels and more -- meaning we can perform lightning fast integrations to get you up and running as a reseller in days.

Dropsuite Email Backup and Archiving is fully compatible with most popular email platforms, from Office 365 to Microsoft Exchange, Gmail and more.

The sales and revenue opportunity for reselling email backup is huge and growing, especially for solution providers already selling Office 365 products. To learn more about how Dropsuite can help you meet your customers' email backup, archiving and eDiscovery needs, contact **sales@dropsuite.com** or visit our website **dropsuite.com**.

Dropsuite

www.dropsuite.com