RESEARCH REPORT 2017

Dropsuite

THE PERCEPTION GAP:

HOW SMBs AND MSPs SEE DATA PROTECTION DIFFERENTLY

Contents

Methodology

This study utilized qualitative research to gain an understanding of the underlying reasons, opinions, and motivations of the target subjects, which were Managed Service Providers (MSPs) and Small to Medium-sized Businesses (SMBs). Qualitative research is characterized by its methods to elicit in-depth discussion that yields understanding into underlying reasons, opinions and motivations of the respondents. The qualitative approach was chosen to probe our hypothesis that there was a potential perception gap between SMBs and MSPs around the topic of data backup.

One-on-one phone interviews were conducted to flesh out SMB and MSP experiences and opinions around the hypothesis. All participates freely consented to participation, and their confidentiality was guaranteed to ensure a free flow of ideas. SMBs were sourced and screened from across the United States by noted research firm Fieldwork, a leader in world-class marketing research services and facilities for over 35 years. SMBs were compensated with an honorarium for their time. MSPs were sourced by Dialog Research & Communications, a noted research company that has served clients from the Silicon Valley to Washington DC for over 20 years. MSPs were not compensated for their time, but were provided with a complimentary copy of this research report.

Samples sizes were small (less than Samples sizes were small (less than 50 participants) and not necessarily representative of the broader population, so the results should not be generalized. However, participants in this study were recruited using specific criteria that made their responses highly relevant to the research topic. A maximum variation sampling approach was utilized, which involved selecting key demographic variables that were thought to provide diverse variations, helping to identify common patterns that cut across variations.

An MSP was defined as a company that remotely manages a customer's IT infrastructure and/or applications, such as email. In most cases, the solution provided included ongoing service and support, typically on a proactive basis and under a subscription model. Participants were product manager level employees or above, which included CEOs, heads of IT, and vice-presidents of operations.

An SMB was defined as having annual revenues of greater than $500,000 and less than $10M, a business not in the computer backup and/or security systems and services industries, that uses email, that has a website consisting of more content than just a blog, and that utilizes an outsourced IT service to maintain their company tech infrastructure, website management, and email communications. Participants were owner-operators, CEOs and heads of operations.

Introduction

The IT Managed Service Provider landscape is experiencing tremendous change. Technology's wicked fast evolution has left consumers expecting instant, reliable and transparent results, businesses struggling to digitize and lower their costs, and Managed Service Providers forced to evolve out of their comfort zones to better serve and protect their clients—and fend off rigorous competition from encroaching cloud service providers. Data is at the heart of this evolving ecosystem – a critical asset but also a big vulnerability for whomever is holding it.

As the MSP channel's model continues its evolution, Dropsuite was curious to know if MSPs and the Small to Mid-Sized Businesses (SMBs) they serve were aligned in how they approached the protection of data assets – especially email and website data, which are vital to most SMBs' viability.

In Winter of 2017, we undertook a series of conversations with respondents from both sides of the equation to explore what's working and where there are gaps between these two groups, who today depend on each other more than ever for their very business existence. This paper discusses the perception gap we uncovered and the steps MSPs can take to enhance their service offerings to both secure new business clients, boost Average Revenue per User (ARPU) and reduce churn.

Key Findings Summary

Our discussions with respondents from both the SMB and MSP communities revealed complex needs, beliefs, expectations and even a few worries. There are some meaningful gaps in how the two perceive each other's roles and responsibilities in these dynamic, interdependent relationships.

	Finding	Gap	Opportunity
1	**MSP SELECTION CRITERIA IS IMPORTANT AND EVOLVING** — Choosing an MSP is a critical decision for SMBs, as the MSP will be integral to the technology and support SMBs rely on. Dependability of the company and ready availability of support are the most important criteria in their selection.	With the costs of changing providers so high, SMBs look at choice of MSP as a long-term partnership decision. But it is difficult for SMBs to know before committing who the best vendors are; there is never 100% trust.	MSPs should consider how to better position themselves as trusted partners — dependability and support are two key areas of focus, but to differentiate MSP offerings, other areas of specialty may need to be promoted such as data security, technology strategy, or the like.
2	**TRUST INCREASES DATA RISKS** — Because many SMB owners lack technical skills, and all are time-deprived, they value the ability to hand off "responsibility" for their data and systems to a 3rd party. They simply trust MSPs are doing the right thing.	MSP responsibility is not a free pass. The prevalence of user-caused security errors, breadth of data storage devices, and liability limitations in many MSP contracts mean the responsibility is shared. Even though an MSP may have a written backup and disaster recovery plan in place with a client, these plans are often untested — increasing risk on both sides.	MSPs should consider how to better position themselves as trusted partners — dependability and support are two key areas of focus, but to differentiate MSP offerings, other areas of specialty may need to be promoted such as data security, technology strategy, or the like.
3	**DATA ASSUMPTONS MAY NOT BE ALIGNED WITH REALITY** — SMBs simply expect MSPs to handle their data safely.	As data creators, especially of sensitive or Personally Identifiable Information, first line of protection of the data is still the SMB's responsibility. Often they lack standards, processes and training, creating a perfect storm of data issues which can, down the line, become a big problem for their MSP.	MSPs should be diligent stewards of the data they may hold on premise, in the cloud, as well as in any value chain where data may be shared — including upstream within the SMB. Forward-thinking MSPs should offer IT security strategy, guidance, procedures, testing, and training to improve SMBs data handling processes.

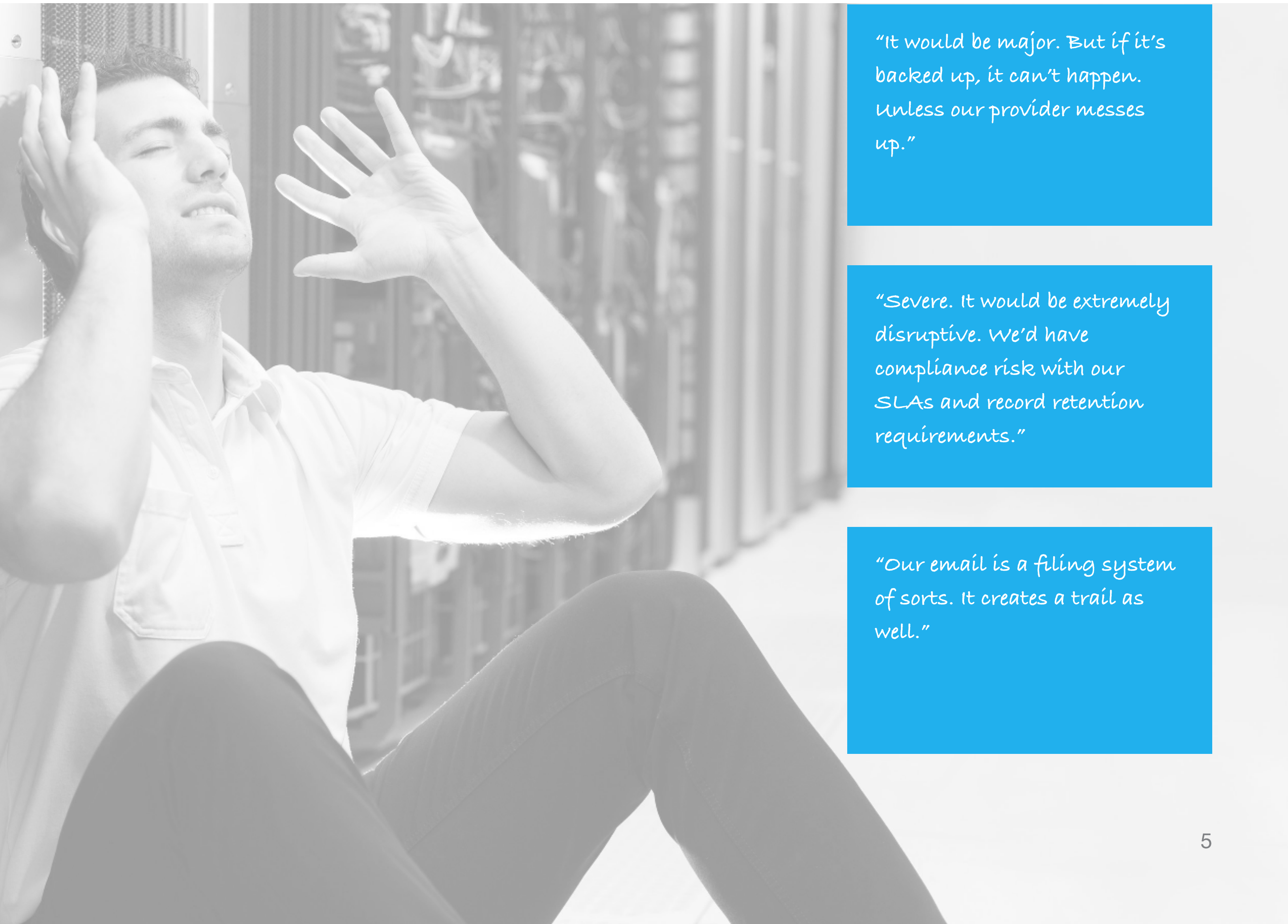
4	**EMAIL AND WEBSITE DATA ARE AMONG THE MOST ESSENTIAL TO SMBs** — This data is often housed across a variety of repositories – from laptops to thumb drives to the cloud – compounding the overhead of managing and protecting it.	SMBs lack a simpler, more comprehensive and safe approach to data management, even when engaging MSPs.	Proactive MSPs may want to provide and promote email and website backup and management services that allow some degree of self-service capability — in monitoring, backup, recovery, ediscover regulatory compliance and/or reporting.
5	**LACK OF DATA EDUCATION & VERIFICATION INSTILLS SMB DOUBT & WORRY** — Many SMBs expect that their data would be restorable by their MSP, whether they're paying for backups or not. Even if they are paying, SMBs can have nagging doubts – is the data really there?	The cost and overhead burden of backing up data makes it difficult for MSPs to do this without getting paid for the service. But there is a trade-off of potential losing a customer or suffering reputational damage if data is needed – and it's not there.	Having SMB customer review and sign something that clearly defines minimum standards can help raise customer awareness and protect the MSP. Another consideration is factoring costs for basic backups into bundled solutions.
6	**SMBs' DATA MAY NOT BE AS IRONCLAD SAFE AS THEY THINK IT IS** — SMBs pay for services but often don't ask for proof of performance. They have no knowledge of, or seeming interest in, what technologies are used by their MSP to backup or secure their data. But whatever is used, they expect it to be ironclad.	SMBs are trusting that their MSPs know what they're doing and what tools to use regarding data backup and security; yet they often don't ask for proof – unless there's a problem.	Proactive MSPs may want to provide and promote services such as audit reports, threat detection, and proof of data backup as a way to stake a market position as a "security-first" MSP.
7	**RANSOMWARE IS A MISUNDERSTOOD THREAT FOR MANY SMBs** — They feel smaller businesses are less at risk, and think security solutions should filter it out. MSPs know smaller businesses are at as much risk as larger ones, and sometimes attribute blame to user error.	This pervasive and growing threat puts both the SMB and the MSP at risk. Training and awareness among SMB staff go a long way to preventing attacks, but neither SMBs nor MSPs are doing enough user education here.	To protect their business reputations and minimize lawsuit threats if they are blamed for losing SMB data, MSPs may want to be extra diligent by deploying a full backup so disks can be wiped and data can be restored if needed.
8	**SMB EMPOWERMENT IS INFLUENCING EXPECTATIONS & SERVICE DEMANDS** — Many SMBs have been empowered by new cloud-based tools that make their businesses easier to manage without IT assistance — either self-sourced or via their web hosting providers. They are demanding MSPs provide them with faster answers and more self-serve capabilities — which many MSPs cannot provide them.	MSPs need to accept the fact that SMBs are getting smarter about IT because the tools to manage certain aspects of tech management are getting faster, easier to use and cheaper — which could lead to customer attrition or demands to lower pricing.	Smart MSPs will adapt by offering more cloud-based solutions that allow SMBs to utilize self-serve tools, or access reports and systems. The encroachment threat from cloud hosting providers is real and needs a thorough counter-strategy.

Today's SMBs –
Swimming and Drowning in Technology

SMBs are in challenging times, technologically speaking. Regardless of the industry or product, end user customer expectations have never been higher for tech-enabled relationships. This dynamic often forces overly busy or non-tech savvy business owners into foreign and uncomfortable territory.

While many have traditionally relied on their 'IT guy', lone individuals are often no longer enough to keep up with the endlessly increasing scope of demands and changes in technology. Many SMBs are now turning to the MSP channel for a greater breadth of services—yet always with a mind to cost.

What would be the impact of a complete loss of email data to your business?



"It would be major. But if it's backed up, it can't happen. Unless our provider messes up."

"Severe. It would be extremely disruptive. We'd have compliance risk with our SLAs and record retention requirements."

"Our email is a filing system of sorts. It creates a trail as well."

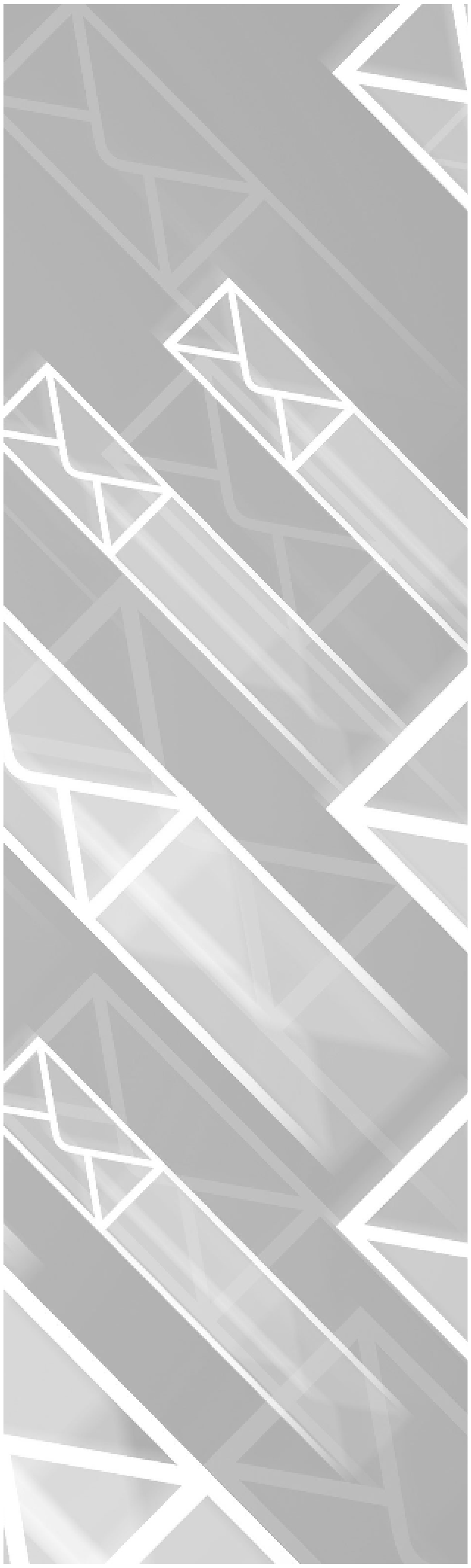
The Importance of Email and Website Data

Two technologies on which SMBs heavily rely are their email and their websites. Email is certainly the most critical. The idea of a complete loss of email data was described as potentially “severe” and “devastating” to the business, particularly for any aspect of the business involving customer interaction. Few if any companies today can rely on customer face-to-face time as being sufficient, or even feasible.

The use of MSPs or cloud-based email services like Office 365 make SMBs feel more secure about their email, as many believe their use of these providers would make loss of email data virtually impossible. The more savvy, or perhaps the more fearful, however, take extra precautions, deploying some redundant local backup option for their most critical email data.

Loss of website data would also be very significant for SMBs, who rely on websites for everything from glorified brochureware to critical information dissemination to e-commerce. The potential impact of website data loss of course varies with how the website is used, and our research indicated that websites are slightly less critical than email. But loss of website data would still pose at a minimum significant inconvenience and at a maximum big revenue loss. For a smaller business, even one day offline can have a serious impact.

While both email and website data are important to SMBs, our respondents entrust these capabilities to different service providers and/or hosting companies, complicating back-up requirements and third party responsibilities.



Choosing a Vendor

SMBs have many requirements for their outsourced providers. When choosing an MSP, our respondents indicated that while they may have a month-to-month payment arrangement with their provider, they are really looking for a long-term partner who will know them, understand their business, and be available when needed. The considerable resource and time investment required to switch MSPs means high expectations—and big responsibility—for the vendor.

The factors most frequently mentioned by our respondents in their choice of MSP were dependability of the company and availability of support. They want it when they want it, whenever that is. Safe data handling was not mentioned as a criterion—because it is assumed. When specifically asked about this factor, all respondents unequivocally agreed that it is very important.

As smaller businesses, they know they don't get the same level of benefits that larger companies would receive. But they in effect have more at stake than larger companies, as it is more difficult to weather the costs of downtime, data loss or slow service. Choice of an MSP vendor is therefore strategic and critical – but also a risk. With so many companies in this channel making similar claims about their capabilities and high quality levels, SMBs apply a variety of filters – from gut sense to word-of-mouth recommendations to google searches including the company name and the word 'fraud' – in making their choice.

> "I want to know up front the level of service the MSP can deliver. The cost of changing a service provider is just too high."

KEY FINDING

Safe data handling is a default SMB expectation for any vendor, which behooves MSPs to be careful data stewards within their own operations as well as in any value chain where data may be shared.

SMB OPINIONS ABOUT MSPs

NOT RANKED

What’s Most Valued?

- Having an external party be responsible for their IT. Someone else fixes the problems
- Having a well-trained team that is knowledgeable about current technology
- The flexibility and scalability to make changes as needed
- Availability when help is needed, 24x7
- Timeliness of response
- Ease of interaction
- Service level that justifies the cost
- Data protection
- Ease of IT management, being able to outsource what they’re not good at
- Compliance capability for regulations such as HIPAA
- Stability, integrity, longevity

What’s Lacking?

- Inadequate insight into payment vs. actual service performance
- Not getting options and benefits that larger companies get
- Lack of upfront market insight into who the best service providers are
- Field staff competence not on par with HQ staff
- Non-dedicated service representatives; lack of account familiarity, insight and history
- Smaller companies get less face time with their providers
- Lack of Office 365 expertise
- Billing and administrative issues
- Self-service capabilities in certain areas
- Deeper strategic guidance on threat protection, backup and recovery — and verification that data is truly safe

Security Practices

Security is a top-of-mind issue, with many respondents proactively mentioning concerns about hacking. Levels of sophistication around security solutions vary greatly, ranging from common desktop applications like McAfee and Norton to firewalls and encryption on in-house servers. While many SMBs rely on their MSP to manage their security needs, they had no awareness of what solutions their MSP was using on their behalf.

Security is also an area where SMBs know they need to invest, and most anticipate having to spend more on security in 2017. Concerns about staying on the leading edge, complying with governmental mandates, and annual subscription cost increases have SMBs factoring security as an important budget item.

SMBs are very aware that their own staff, even well-intentioned as the great majority are, remain a source of risk. User errors, phishing attacks and infected downloads can cause big problems. MSPs we talked to suggest that business owners themselves are often the guilty party in these mistakes.

Some of our SMB respondents noted that they technically prohibit their employees from downloading anything onto company computers as a preventive measure. Training and awareness-raising are also important tools for combatting bad habits. However, few companies — especially smaller, resource-constrained organizations — have established a cybersecurity culture. It's an area that needs improvement.

In fact, previous research published by Cisco showed that 22 percent of SMBs with fewer than 500 employees don't have an executive with direct responsibility and accountability for security because they don't view themselves as high value targets. That same report showed SMBs less likely than large enterprises to have incident response and threat intelligence staff. And their use of certain threat defenses like mobile security and vulnerability scanning were also in decline.

How often does your business backup its data?

"Nightly. If it's not recorded, it didn't happen."

"Every day, automatically. Our SP backs it up in the cloud, but I backup locally to be extra sure."

"My finance person keeps a copy of emails on a zip drive and takes it home. It's the same data as the Service Provider has."

"Because it's outsourced, the provider takes care of all of that. I don't know what they use."

"We are not where we should be. My laptop is not secure."

[1] Cisco 2016 Annual Security Report

Backup Practices

All SMB respondents acknowledge that backing up business data is critical. Most claim to have diligent backup practices in place – or are relying on their MSP for this service. In-house practices involve a mixed bag – from having allocated servers to using flash drives or even keeping paper printouts of the most critical data. Email data may be left to Microsoft OneDrive or some other cloud solution, while core business data may be on a server or a laptop. Clearly a simple-to-use yet robust and comprehensive backup solution would go a long way in helping SMBs more easily meet their backup needs and feel protected.

For most of our respondents, their MSPs are an important element of their backup strategy, but the cost for this service was not top of mind. It's been accepted and mentally processed as a necessary expense.

The actual backup implementation seems to go on faith. None of our respondents knew how their Service Provider was performing backups; none mentioned receiving reports or other evidence of backups being performed as contracted. Some were unsure that their MSP was doing backups at all. Others assumed they must be, but didn't recall if they paid for this service or not.

Respondents also have no knowledge of or interest in the backup technology involved in securing their data. It is again a matter of trust that the MSP is using a reliable solution.

KEY FINDING

A subtle discomfort persists for many SMBs about outsourced backups of their data – is it really there? There is an assumption of responsibility for the MSP. Many SMBs expect that their data would be restorable, whether they're paying for backups or not.

Do you know how your Service Provider backs it up?

"Our MSP does the backup as part of their business recovery plan, so they're responsible."

"I know they backup to their servers, then back those up to another location. This is their responsibility. I never thought about how they do it. They have to do it. What are they going to tell customers? I'd wonder why they wouldn't do it right away. Do they want me on CNN saying they lost my data?"

"I don't know how they do it. I'm just told it's being done. But it's still on faith-one of those 'trust me' moments. It's in the back of my mind – is it really there?"

Where's the Data?

Audits

Data audits are a daunting task for any organization, and SMBs are no exception. Our respondents do not conduct data audits in a formal way. Most know in their heads where their data is, or rely on an in-house IT person, administrator or their outsourced MSP to keep track of data repositories. This casual approach can be more prone to errors, over-reliance on laptop hard drives, or retention of unnecessary data for too long, thereby increasing risk in the event of a breach.

Despite not knowing exactly what they have, respondents factor growth requirements into their MSP evaluation process, seeking an MSP that could scale with their increasing business needs.

Data Loss

None of our respondents reported experiencing a significant data loss in their current business environment. Many have suffered minor incidents, such as a laptop being compromised or deleting emails which were not archived or recoverable. Some respondents had endured a bad experience at a previous organization they worked for, or at a time well in the past, so they learned hard lessons that now prompt them to better protect themselves.

To that end, many respondents keep their most sensitive and/or frequently used data on some local storage device – external hard drives, thumb drives, a server, or on paper – even if their MSP is holding it too. Different staff members may be responsible for securing different pieces of critical data, such as financial or customer-centric information.

While people across industries reported locally backing up sensitive data, it is particularly important in regulated sectors which have compliance regulations, such as for the handling of Protected Health Information (PHI).

Unfortunately, the breadth of storage options employed and the kludgy approach to data management increases SMB overhead and confuses accountability.

Have you experienced a data loss?

"I had a data loss with some email data I had thought was archived, but it wasn't. It took me two weeks to understand that it was gone. Then I'd missed the recovery window."

"I have had people hack at our WordPress account…we did lose some data, but were able to recover it, at expense. There was downtime as well. Your Google page rank goes down if your site goes down."

"We haven't had this issue with my company, but did with the previous organization I worked at. Everything should have been on the shared drive, but a lot of people kept stuff on their PCs. We weren't able to recover everything. Sometimes you don't know what you don't know."

The Cloud

Cloud acceptance is increasing among SMBs given the convenience, the cost-benefit, and the breadth of services offered by large, highly trusted brands like Microsoft and Google. There are lingering doubts among respondents about cloud security, but all were willing to overcome at least some of those doubts and adopt cloud services – whether for an email solution, a full product suite such as Office 365, or for backing up critical data. None of our respondents reported having had a major cloud problem, which buoys their confidence. A few of the more tech savvy had no reservations about the cloud at all.

Concerns that do endure are around the intangibility of the cloud and not knowing where one's data actually is, around security vulnerability and the prevalence of hackers, and even around government intrusion. Despite that, respondents acknowledged and accepted that the cloud is the way of the future and will only become more prevalent.

KEY FINDING

SMB data is housed across a variety of repositories, compounding the overhead of managing, stewarding and protecting it. MSPs may enjoy a business opportunity by helping SMBs devise and deploy a more consistent and safe approach to data management.

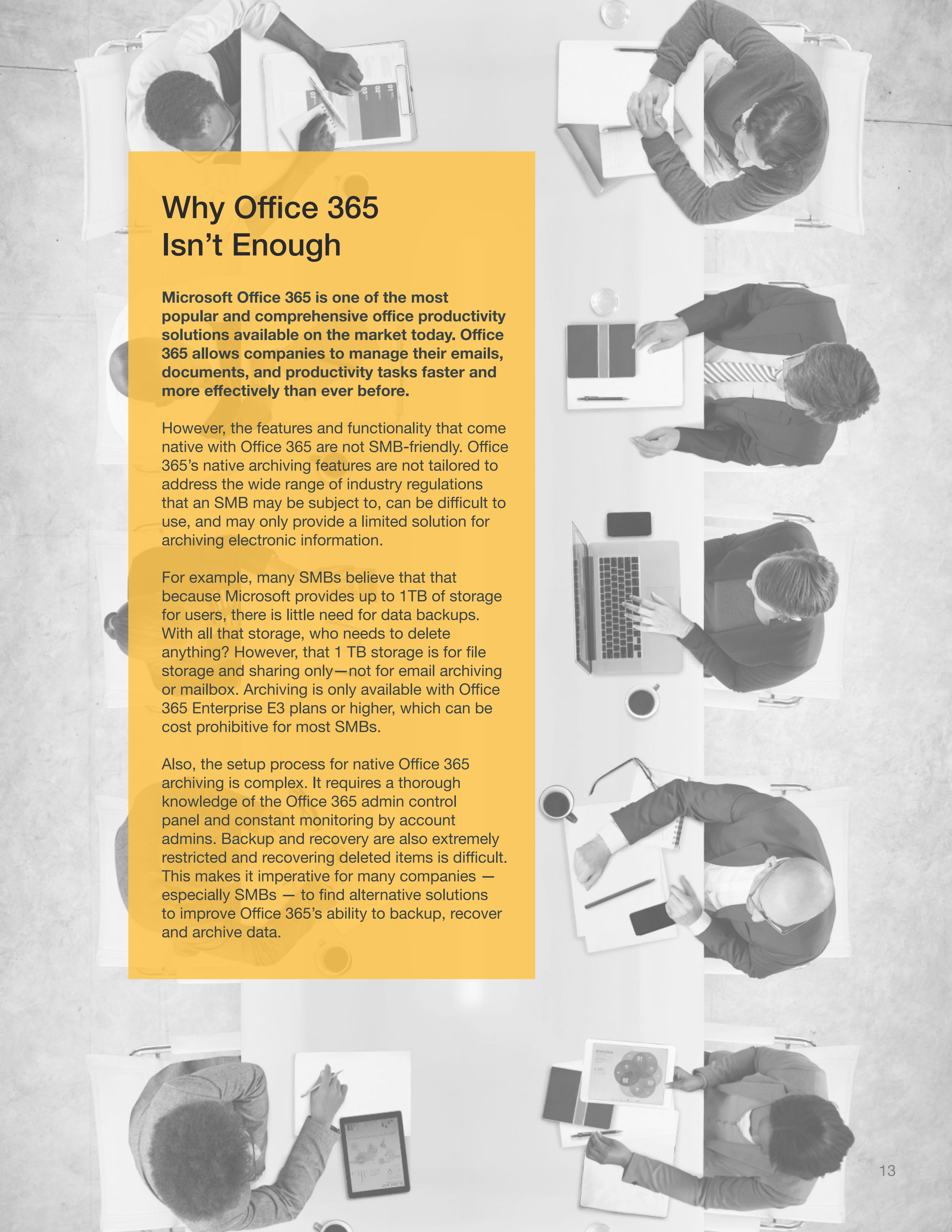
Have you experienced a data loss?

"I've grown more comfortable. Redundancy and backup are key. The carriers are behind. Like the cable companies, they think you need them but you don't."

"The cloud is where it's going. Everything is updated and stored all the time. But virtual means you can't see or feel it. Will the cloud company go out of business? Are you over-paying?"

"You always wonder. I'm not savvy with that kind of stuff. If they have the right security, I guess I'm ok with it. Nothing has happened that I'm aware of so far."

"As much as you can be. I do talk to people who are paranoid. We see the world differently after Snowden. Tech companies may provide the government back doors."



Why Office 365 Isn't Enough

Microsoft Office 365 is one of the most popular and comprehensive office productivity solutions available on the market today. Office 365 allows companies to manage their emails, documents, and productivity tasks faster and more effectively than ever before.

However, the features and functionality that come native with Office 365 are not SMB-friendly. Office 365's native archiving features are not tailored to address the wide range of industry regulations that an SMB may be subject to, can be difficult to use, and may only provide a limited solution for archiving electronic information.

For example, many SMBs believe that that because Microsoft provides up to 1TB of storage for users, there is little need for data backups. With all that storage, who needs to delete anything? However, that 1 TB storage is for file storage and sharing only—not for email archiving or mailbox. Archiving is only available with Office 365 Enterprise E3 plans or higher, which can be cost prohibitive for most SMBs.

Also, the setup process for native Office 365 archiving is complex. It requires a thorough knowledge of the Office 365 admin control panel and constant monitoring by account admins. Backup and recovery are also extremely restricted and recovering deleted items is difficult. This makes it imperative for many companies — especially SMBs — to find alternative solutions to improve Office 365's ability to backup, recover and archive data.

Ransomware

Despite the growing number of ransomware attacks, this phenomenon is still vague for many SMBs. Most respondents recognized the term, generally defining it as being attacked by a malware and having a computer held for a ransom payment. Their opinions are formed from news headlines about big attacks.

Interestingly, most see this problem as a technology issue, which the right security products should help prevent by not letting the malware through in the first place. They also expect help in combatting these threats from their MSPs, who they feel should be addressing ransomware within their security strategies. None of our respondents recalled ransomware defense as a specific selling point in their MSP's marketing and sales efforts.

Perhaps because opinions are formed by news headlines, SMBs don't see themselves as necessarily vulnerable to ransomware attacks. Our respondents see big business as more at risk, because bigger businesses have more at stake and would be more lucrative for attackers to pursue. However, the very act of discussing ransomware with our researcher gave respondents pause on this issue, with many vowing to learn more about it as a result.

Further, respondents had not given thought to their MSP's own ransomware vulnerability, defaulting to a sense of security that MSPs would know how to protect themselves. Over the course of discussions on this topic, they became more circumspect.

KEY FINDING

Ransomware is a misunderstood threat or not considered a serious threat to small businesses by many SMBs. Proactively discussing this threat will help better protect clients and may increase MSP revenue opportunities.

"Have other people who know what they're doing put things in place, manage your security."

"I guess security software is the best way to prevent this kind of attack, and making sure the MSP is up to speed on all that. There's a level of trust. You hire these people to handle this for you. I have other things to worry about."

"You have to be large enough to be worth the effort."

"The size of your business denotes the importance of your data. SMBs might get a slight pass."

"If the government is not 100% safe, what makes you think you are?"

"They're a large provider. They should be safe."

"I don't lose sleep over it, but you don't want to trust anybody too much."

"At this point I don't know. Just like I can't verify our backups are 100%."

Conflicting Perspectives on Ransomware

It's their fault!

SMB's

- Don't understand it
- Feel smaller business is less at risk
- Expect security solutions to filter it out
- Neglect employee education

It's their fault!

MSP's

- Attribute blame to user error, often the SMB leader/owner
- Don't use this threat in their marketing messaging
- Don't do enough to educate customers

Today's MSPs –
Plenty of Upside, Plenty of Risk

IT Channels have had a long and colorful history since the mass adoption of computing technology. From the early beginnings of online business to today's migration to the cloud, service providers have morphed along with immense changes in technology and customer requirements. As IT capabilities and market expectations have advanced, so has the need for more sophisticated and rich service offerings.

With the evolution of the Managed Service Provider channel, many MSP companies now sell a wide range of services to SMB customers, from strategy consultation and planning (virtual CIO) to fully outsourced IT, network management and fail over, remote monitoring, cloud services, disaster recovery, security, helpdesk, voice and even compliance management.

Their preferred mode is to engage in partnership with the SMB customer, getting to know each company's business and becoming an extended part of the team. As a result, the cost of recruiting a customer is high, as are customer expectations for what kind of service they'll get. This makes relationship preservation a top priority. Even if a customer is at fault on an issue, MSPs recognize a need to accommodate the situation or it can ultimately damage the relationship. Reputation matters. Going the extra mile whenever possible helps.

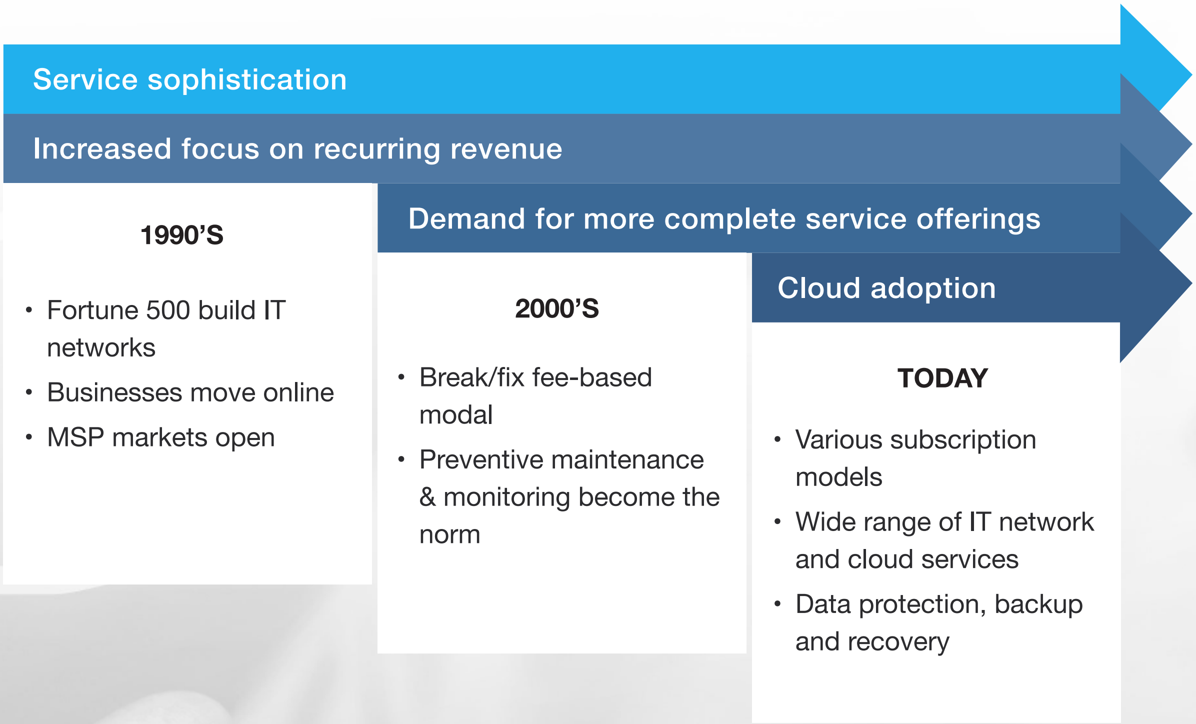
MSP service levels and pricing can vary significantly, from a high cost "white glove" experience to simply setting up Office 365. As SMBs mature and their needs grow, MSPs want to be well positioned to stay on the journey with them.

"We try to be as honest as we can with customers, and tell them that nothing is 100% guaranteed, and there is no way an MSP can honestly say they will never lose client data. But we do everything we can to ensure data loss never happens."

"I educate customers during my sales process; backup is a discussion point. They don't ask for proof. Even on break/fix, I'm not getting these requests. They just want to set and forget.

"You must have a written backup and disaster recovery plan or people will panic in a problem. Have table top exercises; make people feel confident in what they need to do. It's important for clients to be able to help themselves in a disaster."

A Brief History of Managed Service Providers



Service sophistication

Increased focus on recurring revenue

Demand for more complete service offerings

Cloud adoption

1990'S

- Fortune 500 build IT networks
- Businesses move online
- MSP markets open

2000'S

- Break/fix fee-based modal
- Preventive maintenance & monitoring become the norm

TODAY

- Various subscription models
- Wide range of IT network and cloud services
- Data protection, backup and recovery

The Backup Business

Backup has become a core MSP service offering, but our MSP respondents are taking a low-key approach to pitching it. Backup service is commonly now worked into broader discussions during the sales cycle, and either priced into a full package of IT services or included in an add-on disaster recovery or business continuity offering. Many providers tier pricing levels by things like frequency of response time or performing backups. By consultatively exploring an SMB prospect's full range of needs during the selling process, it is easier for MSPs to factor backup into the overall contractual model.

MSPs perform customer backups daily or continuously, depending on customer cost preferences. Most MSPs offer Service Level Agreements (SLAs) for recovery times, ranging from as fast as 30 minutes to several hours or longer, also varying by price.

Customers generally do not ask MSPs for proof that backups are being performed. Earlier ranks of unscrupulous companies who got caught not fulfilling this contracted obligation were driven out of the market. Still, proactive reporting does not seem to be standard operating procedure. One particularly proud MSP strongly advised that SMBs negotiate to receive monthly reports from their MSP for any contracted services, ensuring accountability.

> *"As we continue our transition to MSP, I want to cut out the break/fix customers. They're a liability waiting to happen."*

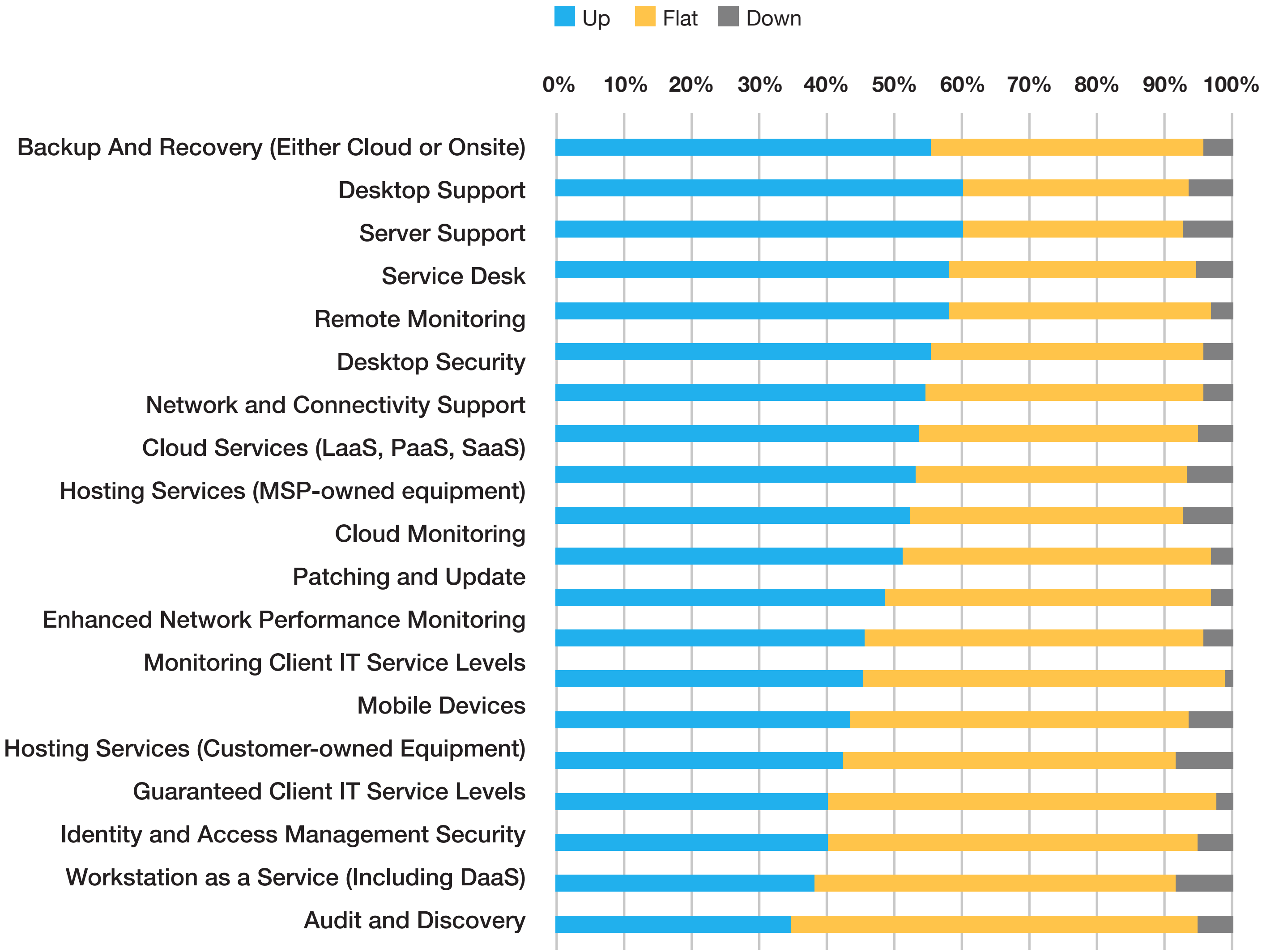
> *"These customers have a different mentality – it's reactive. They don't like recurring fees. If they see data loss and downtime directly affecting profitability, they become a good candidate for managed services. They fret over price otherwise, unless there's a crisis."*

KEY FINDING

Proactively offering regular reports on backup services performed will increase customer confidence and can be a competitive differentiator.

MSP Services 2017

Service Reveneu for past vs. previous 12 month



Source: MSP Global Pricing Survey Kanseya 2017 Report, January 2017

Managed Service vs. Break/Fix

Break/fix service offerings have long provided a good living for service providers, but many of today's MSPs are trying to move away from this model for several reasons.

In traditional hosting arrangements, customers often assume that the hoster is backing up their files, even when this is often not the case. This expectation can extend to an MSP, increasing their cost and risk.

And although most every SMB owner today will acknowledge the vulnerability of malware, hacking and user errors, there is a class of customer that still objects to seeing a backup fee on the monthly bill. Maturity of the business is not necessarily a determining factor of this behavior, as some MSP respondents cited examples of highly successful SMB clients arguing over even small incremental fees.

Exiting the break/fix business may become a process of elimination over time, if the cost of more problematic customers become too burdensome. As MSPs look to increase their service sophistication, they seek more savvy customers, and may eventually leave the break/fix to hosters.

> "Large organizations can do best practice training, technical controls – small companies don't do that. User accounts have more permissions than they need. Users aren't well trained. It's like dry tinder and a spark."

Customer Data and Security

Our MSP respondents were very prideful of their security practices and the integrity of customer data they hold. All claimed they had never experienced a breach; given statistics on rampant breaches, this across-the-board claim gives pause.

MSPs noted that education and training are the first line of defense against cyber attacks. Most politely assign blame for errors to the customer. Several employ encryption as another safeguard, both for data in transit and at rest. One respondent specifically noted that only their customer had the encryption key for the customer's data, so no one at the MSP could access it, reducing liability.

Respondents stressed the importance of maintaining current backups so that in the event of a problem, data could be quickly restored or disks could be wiped clean and repopulated, with minimal to no data loss. They noted this is particularly important in the event of ransomware attacks.

Most MSPs maintain onsite servers and redundant hot spots in remote locations. Other frequently mentioned security best practices included two-factor authentication, encrypting data at rest, encrypting data to which only the customer has the key, and deploying robust firewalls and antivirus software.

MSPs know that user training is especially important in raising awareness about risky online behaviors and combatting issues like ransomware. There is increasing use of 'white hat' phishing techniques that catch SMB customers' staff in high risk actions and warning them off repeating such behaviors.

Even with the best preventive measures, errors still occur. It is common practice for MSPs to contractually limit their liability. SMBs should read the fine print to understand where the line is. But as mentioned earlier in this paper, most MSPs understand the need to extend themselves as much as possible on the customer's behalf to preserve he long term relationship. This is a balancing act.

> *"Large organizations can do best practice training, technical controls – small companies don't do that. User accounts have more permissions than they need. Users aren't well trained. It's like dry tinder and a spark."*

Ransomware

Ransomware is a type of rogue software that has been designed to prevent access to your website until “ransom” money is paid to the attacker.

According to Kaspersky Lab, every 40 seconds a business gets attacked by ransomware. And 42% of SMBs have experienced a ransomware incident in the past 12 months.

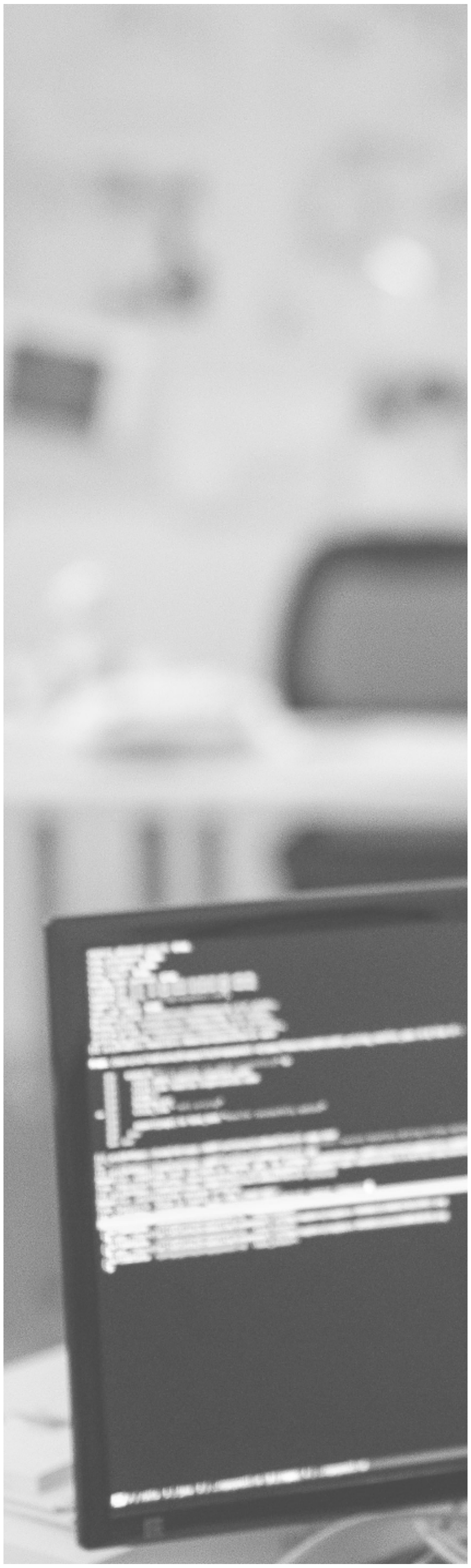
Our MSP respondents noted that their SMB customers are not asking about ransomware. Rather than call this out as a current and pervasive threat trend, MSPs factor ransomware into the broad scope of other malwares to be addressed through security solutions.

MSPs are keenly aware that successful ransomware attacks are mainly employee-triggered, and that education and awareness play a huge role in combatting this threat.

Yet these are practices that smaller companies often neglect to their own peril.

Ransomware costs to SMBs include:

- Cost of the ransom paid
- Lost sales
- Staff productivity losses from being unable to perform their work
- Overtime/consulting costs to MSPs tasked with fixing the problem
- Future sales loses due to reputation damage
- Future sales loses due to reduced search engine rankings due to blacklisting



Cloud-based Services

MSPs have seen a big rise in demand among SMBs for cloud application suites like Microsoft Office 365 and Google G Suite. Expertise in these solutions pays off for MSPs who set clients up and service their related needs. While customers proceed under the belief that these cloud providers have their data backed up, MSPs understand that is not necessarily the case. For instance, the 1 TB of storage offered with Office 365 does not cover email data, and the redundant server model behind these apps only provides cloud data availability for 30-days. This is not a true backup solution. While the gap creates another MSP revenue opportunity in offering customer backups to the MSP's premises, there is still an education curve to get customers to understand this situation.

Cloud advocates note that giants like Google and Microsoft have robust security, making their cloud offerings very safe. But others warn against vulnerability with free cloud services like non-business versions of Dropbox or Box.net. One respondent cited an amusing anecdote about an SMB customer of his who kept personal data on free Dropbox. He stopped this practice when he noticed a photo of his family he had kept in a folder called 'family vacation' being used in an advertisement at an airport.

"Any MSP owner will say Office 365 is less burdensome than on premise Exchange. But Office 365 does not back up the system. Just because it's in the cloud doesn't mean it's being backed up. Customers think that it is."

KEY FINDING

SMBs, do you know where your data is? As a data collector, especially of Personally Identifiable or sensitive information, protecting the data is the SMB's responsibility. When selecting a service provider, SMBs would be well advised to think through their comfort level and fiduciary and compliance responsibilities in regard to where their data is held.

MSP Needs and Challenges with Current Backup Solutions

With the wide variety of client requirements, computing environments, applications and data repositories, MSPs need to have a variety of backup technologies that fit different situations. While SMB customers express no interest in knowing what backup technologies are used on their behalf, they expect that their MSP is using an ironclad solution, so that data is available if and when it is needed, fast.

MSPs must grapple with the variety of backup products, each with its own learning curve. Thus ease of use is an attractive attribute for products they choose.

MSPs are judged by customers in terms of how fast they help customers return to normal operations following a disruption. But a solution's speed in downloading restores or other fixes is constrained by the SMB's own internet bandwidth. So while speed is an important backup solution criterion, its importance to the MSP can vary by the rate of the customer's connection.

Some respondents noted flaws in certain technologies where backups degrade to the point where the data becomes "garbage", slowing to a halt but not quite failing. Another gap mentioned was the lack of consolidation of cloud and on premise data into a single backup solution.

As they review new backup product offerings, these channel members will look to solutions that help them increase revenue and reliably protect data without adding engineering overhead.

Bridging the Gap

There is a complex, interdependent dynamic between SMBs and the MSP channel that wants to serve them. SMBs are struggling to keep up with constant changes in technology, data management and cyber risk, while keeping their core business competitively viable and growing. As they turn to MSPs for help, they are entrusting them with critical data assets, creating high expectations for responsibility and trust. An MSP's reliability can greatly enhance—or severely damage—an SMB's business.

In the gaps our research identified, we see opportunities for MSPs to enhance service offerings that will increase customer confidence, minimize risk on both sides, and ultimately secure more clients for the long term:

- With SMB data being stored across so many different devices, often as 'insurance' backups for the most needed information, they would greatly benefit from a simpler, more comprehensive data management approach. MSPs could help devise easy-to-use cloud-based options accessible from anywhere with an online connection.

- MSPs should proactively offer regular, simple-to-understand reports on backup, monitoring and other services performed. This will increase SMB customer confidence and can be a competitive differentiator for MSPs.

- Ransomware is a misunderstood threat for many SMBs. Proactively discussing this threat will help better protect clients and may increase MSP revenue opportunities. Provide SMBs with educational materials, teach onsite classes, share news stories – become a proactive partner in developing a cyber security culture.

- As data collectors, the legal buck stops with the SMB, regardless of who's housing PII or sensitive data at any given time. When selecting a service provider, SMBs would be well advised to think through their comfort level as well as fiduciary and compliance responsibilities in regard to where their data is held.

- To help manage SMB budget constraints, MSPs might adopt a hybrid offering of full service and self-service tools.

- Office 365 is acting like a catalyst for change—forcing many SMBs to adopt cloud email services, and presenting both a challenge and an opportunity for MSPs. They need to help SMBs understand that additional methods for email backup and archiving may be required to ensure business compliance, yet who will assume the extra costs? How can SMBs be empowered to do their own e-discovery or retrieval for accidental deletions without needing to contact their MSP directly? When MSPs help migrate their clients to Office 365, this is often the best time to implement additional, complimentary email backup and archiving solutions — yet many MSPs are not doing this yet.

About Dropsuite

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.

To learn more about our reseller pricing or to demo our product, contact sales@dropsuite.com or visit: dropsuite.com

Dropsuite

www.dropsuite.com