ARTICLE

LIMITED RESOURCES
MARKETING AND SALES ISSUES
DIGITAL RISK AND THREAT ACTORS
ACCIDENTAL DELETIONS
COMPLIANCE AND REGULATORY ISSUES

Five Key Obstacles for Managed Service Providers

(and How Backup and Archiving Can Help)

Managed service providers (MSPs) often handle hundreds of clients from various industries with complex needs. This creates a host of management challenges.

The most common challenges MSPs face are the proliferation of digital risks and threat actors, insider threats and accidental deletions, limited resources, compliance and regulatory concerns, and marketing and sales issues.

Certain technologies, however, can help MSPs address these challenges and empower them to keep their customers safe and compliant. Key amongst these technologies are data backup, recovery, and archiving.

The Key Challenges Faced by Managed Service Providers

Managed service providers (MSPs) are third-party companies that remotely manage the information technology (IT) infrastructure and end-user systems of a range of organizations – from small and medium-sized businesses (SMBs), nonprofits, and government agencies.

Most MSPs handle multiple clients at one time. This means they have access and control over business-critical infrastructures of companies and are also providers of solutions that address the needs of their clientele.

The demand for managed service providers has grown exponentially over the past few years. In the two years before the onset of the COVID-19 pandemic, the global managed services market was valued at $166.8B (in 2018) and $200.3B (in 2019)

In 2020, like every other business, the managed services industry underwent a slump, its value going down to $196.5B. But as the era of remote working spurred, 2021 saw the value rise to $239.71B. Now, it is expected to expand at a compound annual growth rate (CAGR) of 13.4% from 2022 to 2030.

This growth in demand is fantastic – but for MSPs to succeed, they need to utilize the very best tools in the tech stacks they offer and manage. Because of the complexity of the services they offer, managed service providers face various technical challenges. The industry has become increasingly competitive, and MSPs need to master these challenges if they want to differentiate themselves from their competitors.

Let's take a look at what those challenges are.

Challenge #1: Accidental Deletions

Business clients of managed service providers are especially susceptible to all manner of digital threats. But often, the biggest challenges that both MSPs and their clients face come from within.

Human error is still the most common reason for data loss, and the most common error that humans make is accidental deletion.

Approximately 88 percent of all data breaches are caused by an employee mistake.

So what are the most common reasons for accidental deletion?

1. **Simple, human error** – Employees are prone to accidentally deleting vital files or overwriting data and failing to realize what they did until it's too late.
2. **Data sprawl** – This is when users save files in progress in non-approved locations, such as their desktops, mobile devices, and more. This puts data at risk of being accidentally deleted and being irrecoverable.
3. **Unsynced mobile devices** – Users that save company data into their personal mobile phones often forget to sync or backup that information to the cloud.
4. **Employee turnover and administrative errors** – Without a proper turnover process, data handled by previous employees will not be preserved and governed properly. Disgruntled employees can even use that data for nefarious purposes or delete it maliciously, putting the company in jeopardy.
5. **Equipment loss or theft** – According to the Kensington Computer Product Group:
   - One laptop is stolen every 53 seconds.
   - 70 million smartphones are lost each year, with only 7 percent recovered.
   - 4.3 percent of company-issued smartphones are lost or stolen every year.
   - 80 percent of the cost of a lost laptop is from a data breach.
   - 52 percent of devices are stolen from the office/ workplace, and 24 percent from conferences.

There are two main actions that businesses can take to address accidental deletions:

1. Proper employee onboarding and offboarding

Businesses need to streamline their entire onboarding and turnover processes.

Part of the employee onboarding should be to orient them on using the proper equipment and software to safeguard company data and assets. If your company employs a bring-your-own-device (BYOD) system, get your employees' buy-in to install multi-factor authentication (MFA) and security systems to protect their phones in case of loss or theft.

For offboarding and turnovers, make sure the leaving employee surrenders all sensitive data in their possession.

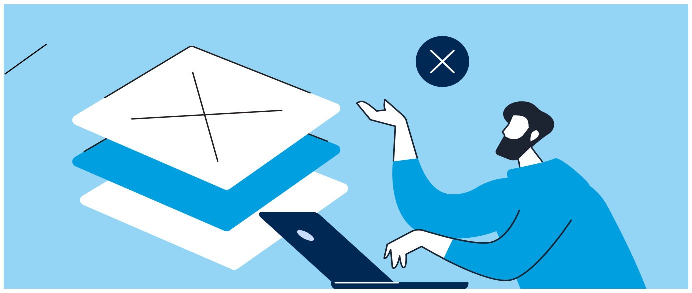
2. Install backup and archiving solutions

Onboarding / offboarding employees securely and efficiently only gets you halfway. The other half is effective preservation and recovery of the company's intellectual property and employee work product.

Important content needs to be surrendered to the right personnel and, at the same time, properly stored or archived. It is also vital that mobile devices containing sensitive information are immediately synced to a cloud location for backup.

Read more about accidental data deletion with our blog series entry: 5 Most Common Causes of Accidental Data Deletion

Challenge #2: Barriers to Scaling



Scaling is important for every business – and in every vertical, it has its challenges. MSPs are no different. This is especially true for less mature MSPs that want to scale toward becoming a strategic solutions bundle provider – but are reluctant to risk changing their business model and overhauling established MSP marketing plans and sales efforts.

Here's what we consistently hear from MSPs about the difficulties of scaling:

- Some customers think that it's a detriment to them when their choices become limited, especially when they're dealing with service providers with a dedicated tech stack.
- For others, it's a "if it's not broken" situation: the current system works, and has been working for years, so why change it?
- Others still are stuck in the mindset that their current investments still have more to give.

Still, the benefits of increased scalability and profitability often outweigh the risks. Scaling a small business just requires a little more creativity and resourcefulness. Here are some tips for scaling, even with limited resources:

1. **Standardize**. The diversity of solutions that solve the

same problem can be overwhelming. To address this, look for a particular solution that best fits your business model and stick to that. Training personnel across a standard set of solutions is easier, makes scaling faster, and enables high-quality service.

2. **Automate your processes.** With a standard tech stack, you can now enable various forms of automation. Leverage remote monitoring and management (RMM) tools to automate routine tasks. Enable integration between tools to deliver a higher level of service and support.

3. **Document everything**. And by everything, we mean everything. Look into solutions that provide a single source of truth for critical IT infrastructure details. Create a single and secure repository of key details and configurations. Deploying an automated backup and archiving system will also help.

4. **Partner with a master MSP**. Leverage the capabilities of a master managed service provider to handle labor-intensive tasks that you as a client-facing MSP will have a hard time dealing with. Make them an extension of your staff, which allows you to do more with less.

5. **Embrace remote work.** The COVID-19 pandemic has accelerated the movement into a remote work / hybrid environment. Use that to your advantage and leverage talent not just locally, but from all over the country, or even the world.

More insights about these recommendations are in our blog here: 5 Ways to Grow Your MSP Business When Resources are Limited

Challenge #3: Digital Risks and Threats

Managed service providers work with multiple clients, holding massive amounts of information and data. Gaining access to their systems means a high chance of obtaining access to thousands of business systems.

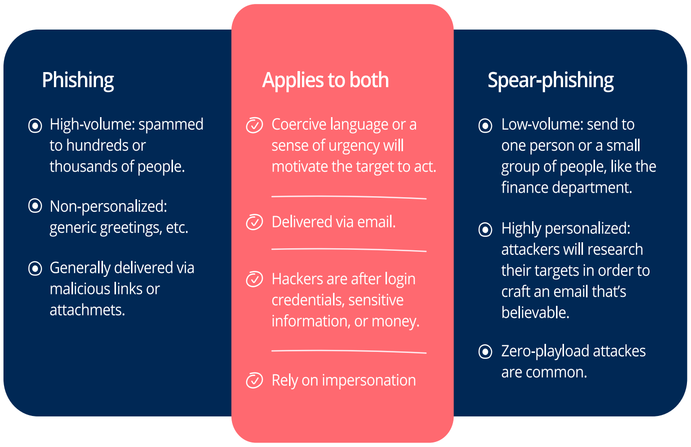
This is why MSPs are prone to many digital threats and risks – especially the following five:

Ransomware

Ransomware threats have become more frequent and more lucrative for bad actors. The main drivers of the growth of ransomware are cryptocurrencies, the existence of ransomware-as-a-service (RaaS), and ransomware group safe havens outside the country. Reports reveal 60% of MSP client incidents were related to ransomware threats.

Social engineering

98% of attacks rely on the rapport and connection that are established as the social engineering attack progresses. These exploits are effective about 80% of the time. One example of an extremely effective social engineering attack is spear-phishing.



Phishing

- High-volume: spammed to hundreds or thousands of people.
- Non-personalized: generic greetings, etc.
- Generally delivered via malicious links or attachments.

Applies to both

- Coercive language or a sense of urgency will motivate the target to act.
- Delivered via email.
- Hackers are after login credentials, sensitive information, or money.
- Rely on impersonation

Spear-phishing

- Low-volume: send to one person or a small group of people, like the finance department.
- Highly personalized: attackers will research their targets in order to craft an email that's believable.
- Zero-playload attackes are common.

DDos attacks

A distributed denial of service (DDoS) attack 'floods' a web source with requests until it is overwhelmed and cannot function properly. DDoS-for-hire services have spurred in number recently, partly because of the remote working setup during the pandemic.

Remote work issues

As more companies look at distributed and hybrid models of work, their IT requirements complexify, and they need professional guidance.

The work-from-home setup has greatly benefited managed service providers these past years. According to Fortune Business Insights, businesses are "adopting [MSPs] to upgrade and innovate their infrastructure," and to meet the growing demand for end-to-hosting software. However, it has also expanded their risk surfaces.

Users now access their workplace tools like Slack and Teams with their personal devices. This puts sensitive company information at risk of being stolen or unintentionally exposed. A report details that 52% of businesses find mobile devices to be a major cybersecurity challenge.

IoT vulnerabilities

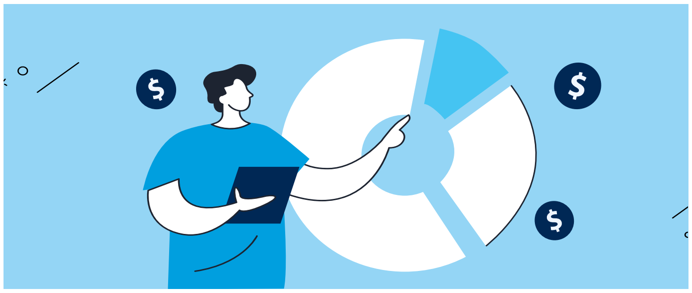
Internet of Things (IoT) cyberattacks have increased year over year. The intent of these attacks range from DDoS to crypto mining to data theft.

The cost of security breaches can be damagingly high for MSPs. Fortunately, they can protect themselves. Here's what both MSPs and their clients can do:

- **Deploy a security solution that provides a multi-layered, in-depth** protection against digital threats like social engineering, DDoS and ransomware attacks, as well as system vulnerabilities.
- **Identify potential risks** beforehand with extended threat detection and response solutions.
- **Plan and perform security exercises** to keep personnel adept at dealing with and responding to security breaches and cyberattacks.
- **Deploy automated cloud backup and archiving systems** to secure reliable backups and mitigate repercussions of potential data loss.

Discover more about these digital threats with our article here: The Five Key MSP Cybersecurity Threats You Need to Understand in 2022

Challenge #4: Addressing Marketing and Sales Issues



We tend to always think about MSPs from the angle of security – but often, the issue can be elsewhere. Sometimes, MSPs just need to look into their marketing and sales tactics to find out what the challenges are in growing their business.

An MSP may have originally targeted businesses with 20-200 employees in a specific region – but eventually discovered most of those businesses already have a service provider that provides a better service, and lost the sale. From a marketing perspective, these competitors may have been writing online content that does not resonate with their prospects, or isn't optimized for the right keywords. From a sales perspective, perhaps they haven't been leveraging the full sales potential of the solutions they've deployed.

How can MSPs address common sales and marketing challenges?

Here's a short checklist of the best practices for your marketing and sales approach:

☑ **Do you know who your clients are? Do you have an ideal client profile (ICP)?**

An ideal client profile (also referred to as a persona) is a fictionalized embodiment of your best client based on interviews and research from your current and past clients, prospects, and staff. It helps to narrow down the clients you should be targeting – who they are, where they are located, and/or how many they are.

☑ **Do you use any sales intelligence software? If you are, are you certain it's the right one?**

Once you narrow down your ICP, your B2B data investments become more manageable and affordable.

☑ **Is your website a lead generation machine?**

Your website can be the most beautiful website in the world, but if it can't capture leads, then you're doing it wrong.

☑ **Is your content 'search engine optimized'?**

Make your website relevant by making it a treasure trove of rich, informative content that is optimized for search engines. Construct content pieces that are SEO-friendly.

☑ **Have you 'maximized' your vendors?**

If you haven't, then you're missing out. Find out how you can maximize the services and products that your vendor delivers. It also helps to focus on either a single vertical or a dedicated tech stack. This way, you'll get your money's worth and grow your business further.

☑ **Is your MSP sales process properly mapped?**

Don't rely on the sales superstar. Learn from the mistakes of others and map out your sales process. Also, make sure it also evolves as your company grows.

☑ **Do you have the right people for the job?**

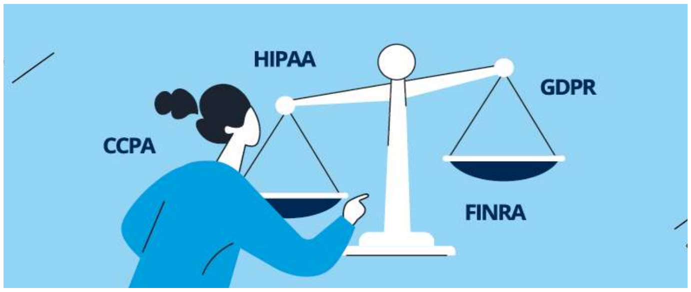
With the help of the MSP sales process map, you can pinpoint the right people with the right qualities, for the right roles.

Want more information about this checklist? Here are expanded versions of these tips:

- 5 Key Ingredients for MSP Marketing Success
- 3 Key Ingredients for MSP Sales Success

Want more information about this checklist? Here are expanded versions of these tips: 5 Key Ingredients for MSP Marketing Success, 3 Key Ingredients for MSP Sales Success

Challenge #5: Non-Compliance and Regulatory Issues



Public awareness of the importance of data privacy helped spur the creation of the most relevant data regulations that businesses need to comply with. These are:

- **General Data Protection Regulation (GDPR)** – a legal framework that sets guidelines for the collection and processing of personal information from individuals, especially those who live in the European Union (EU).
- **California Consumer Privacy Act (CCPA)** – an act that gives consumers in California additional rights and protections regarding how businesses may use their personal information; often referred to as California's counterpart of EU's GDPR.
- **Health Insurance Portability and Accountability Act (HIPAA)** – an act created by the US Congress in 1996 to protect individuals covered by health insurance and to set standards for the storage and privacy of personal medical data.
- **Financial Industry Regulatory Authority (FINRA)** – a self-regulatory organization for U.S. broker-dealers overseeing more than 624,000 brokers and analyzing billions of daily market events to ensure business compliance.
- **Lei Geral de Proteção de Dados (LGPD)** – a comprehensive business compliance law that is the Brazilian counterpart of the European Union's GDPR.

These regulations protect a managed service provider's clients, but it also requires them to have the right technologies to be compliant:

1. **Identity and Access Management (IAM)** – IAM is the process of making sure the right people have the right access to the right resources (applications or data) inside an organization. IAM technologies prevent hackers and cybercriminals from accessing unauthorized systems, software tools, or other data such as an employee's personal identifiable information (PII).
2. **Encryption** – This ensures that if data is lost or stolen, it won't result in a breach of PII, but it should be applied for both data in transit and at rest.
3. **Mobile Device Management (MDM)** – MDM technology enables organizations to protect and govern company information that often resides on employee mobile devices, such as smartphones or tablets.
4. **Email Security** – Email security should not just be about phishing and spam defense; it should also be about providing outbound security. Email security systems can be configured to detect and block the unauthorized transmission of PII by email by employees or cybercriminals who may have breached a corporate email system.
5. **Data Loss Prevention (DLP)** – Similar to outbound email security, DLP technologies defend against the mass exfiltration of data by employees, hackers or cybercriminals. It can also simply govern the movement of data inside an organization and its software systems, preventing data from moving where it shouldn't be.
6. **Backup, Disaster Recovery, and Data Retention** – The most significant solution that businesses often overlook. GDPR, in particular, stipulates that companies need to have "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident." Therefore, businesses should have robust backup and recovery procedures in place that enable them to recover from a wide range of business disruptions.

Find out more about how these technologies ensure your business compliance here: Business Compliance: A Look Behind and Beyond the Acronyms

The Importance of Backup and Archiving

> “A good backup system is considered the most efficient solution to data loss, as it increases the chances of data recovery.”
>
> – Corporate Finance Institute

For all of these five challenges, a state-of-the-art backup and recovery system can help. In addition to enabling compliance with relevant privacy laws, an automated backup and recovery system:

- Protects businesses from the damaging effects of accidental deletions,
- Enables companies to keep data safe, especially when resources are limited,
- Mitigates the damage of digital threats and data breaches; and,
- Enhances a managed service provider’s marketing and sales strategies.

More often than not, people in the industry confuse backup and archiving as the same thing. However, they are ultimately not the same:

A backup is designed to be a short-term insurance policy to facilitate the quick recovery of files not readily available due to circumstances like data loss.

With backups, users can typically select a date in time and restore a copy of the missing files from a prior date in time. Currently, the fastest and most convenient way to perform this is through the cloud.

Archiving, on the other hand, is more long-term, providing ongoing, rapid access to years, possibly decades, worth of business information. Like backup, archiving can also secure mail files, attachments, calendars and more.

This is especially important to companies in regulated industries such as financial services, healthcare, or law firms. Archiving is required by law because it provides specialized tools for making data records tamper-proof, searchable and retrievable in the event of an audit, HR inquiry or lawsuit.

Debunking Myths About Backup and Archiving

Businesses, including managed service providers, have their own misconceptions about backup and archiving. Either they’ve heard it from a friend of a friend, or they’ve had a bad experience with it. In any case, it’s best to clear the air and bust those myths now.

Myth #1: We don’t need backup and archiving because Google Workspace / Microsoft 365 does it already.

False. Microsoft 365 (formerly known as Office 365) only saves deleted emails and files them in the recycle bin for up to 90 days. Meanwhile, Google Workspace (also known as GSuite) deletes end-users’ Drive files and emails in the Trash and Spam folders after keeping them for 30 days. Moreover, it only allows admins to restore items deleted from a user’s trash for up to 25 days.

Both solutions/providers **do not assure full recovery of your data** in case of user error, data corruption, or ransomware threats.

Myth #2: Backup and archiving are too expensive.

False. With the right solution, it isn’t. Certain solutions can offer non-disruptive data protection for a few dollars per seat per month. Moreover, the cost of security breaches massively outweighs the expenses needed to ensure data security.

Myth #3: Only regulated businesses need it.

False. Not necessarily. Non-regulated businesses can find value in data backup and archiving, too:

- Audits may require them to provide full and accurate data that may go back many years.
- Lawsuits or regulator investigations may require Microsoft 365 / Google Workspace 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 solutions in one action. Time-saving tools are valuable assets.

Myth #4: Backup and archiving is overhyped and not actually a priority.

False. It may not be a priority, right up until it becomes one. Many businesses – some still existing, others closed down – realized this the hard way.

Myth #5: All backup and archiving solutions are the same.

False. They are not. The facts, however, are:

- A lot of solutions in the market are clunky, with poor UX design.

- Not all of them are born in the cloud; a lot of these solutions need to be downloaded as an agent to work.
- Most vendors don't offer backup and archiving together.
- A lot of these solutions are also sold as modules, which can be very costly.
- Only a few backup and archiving solutions offer insights and analytics based on the data that is stored and/or archived.
- Moreover, most solutions do not back up everything, such as Microsoft Teams 1:1 chats, calendars, and tasks, among others.

Myth #6: You need to pay to get your data back.

False. This might be true for most, but **there are solutions available that don't force this on their customers**. Part of choosing the right solution should be asking if they 'take your data hostage' – that is, if your provider charges you to get your data back when you decide to move on to another solution or service.

At the end of the day, it's still your data, and you shouldn't be hassled into paying to get it back, especially when you find another backup or archiving solution that suits your operational needs better.

Myth #7: Backup and archiving solutions are slow.

False. They can be… if they don't have efficient workflows. Most automated backup systems back up everything you have chaotically. But some sophisticated solutions actually prioritize backing up recently updated or added files to speed up the entire process. With the right tools at your disposal, you can expedite the process and ensure your data is fully secured and backed up.

Myth #8: Backup and archiving tools are just that – they backup, and they archive.

False. While most solutions can be limited in terms of what they can do, certain tools have features that go beyond backup and archiving.

Key example: some tools include advanced features like eDiscovery and fast searches, allowing users to easily sift through their backups or archives and pull important data for compliance reviews, company audits, criminal investigations, and other legal procedures.

There are also solutions that provide business insights and analytics from your stored and archived data – solutions capable of producing productivity reports and visual relationship graphs to help you run your business more efficiently and securely.

Overcoming MSP Challenges with the Right Solution

For managed service providers and their clients, overcoming the challenges mentioned here should be top priority.

In terms of digital threats, there are powerful cybersecurity solutions online that do protect businesses from ransomware, DDoS attacks, and system vulnerabilities. Unfortunately, these tools can't guarantee 100% security.

The same goes for accidental deletions and human error. At the end of the day, employees are just human, and mistakes will be made. These mistakes, no matter how small, can result in non-compliance and regulatory issues. They may even affect your MSP marketing plans and sales efforts.

Furthermore, businesses usually cannot just throw money at these problems, especially when resources are limited, and times are hard. Buying every solution in the market to 'secure' the business would be illogical and wasteful.

So, what can MSPs and their clients do? They need to evaluate their business and narrow down the solutions they need. Moreover, as a catch-all, they need technologies that will act as their 'safety net' – data backup, recovery, and archiving.

This is where Dropsuite can help:

Dropsuite provides cloud-based solutions for regulatory compliance, data security including archiving and data retrieval, plus advanced analytics to uncover hidden data and turn it into actionable insights to improve business processes for MSPs and their clients.

- Microsoft 365 Backup and Archiving automatically protects your most important M365 data in the cloud and restores any file on demand.
- Google Workspace Backup and Archiving protects your data where Google does not, and ensures your data is backed up to meet most regulatory specifications.
- Dropsuite's eDiscovery solution provides discovery and access for business-critical data in an electronic form for litigation or other compliance needs.
- Insights BI Email Analytics provides a robust analytics toolset that turns complex and extensive email data sets into simple, actionable reports, graphs and charts.

To learn more about Dropsuite's services
Talk to Our Experts

More Reading:

Here are some more insightful resources for MSPs:

1. Why MSPs Should Offer Cloud Backup and Archiving for Office 365
2. SMB Channel Services Transformation
3. 4 Considerations to Maximize Your MSP Value
4. The Four Step Process to Build Your MSP Blog Editorial Calendar

CONTACT US

For more information, please contact us:
www.dropsuite.com | sales@dropsuite.com