KeepItSafe®
ONLINE BACKUP

WHITEPAPER

The Reseller Question:

Develop Your Own Backup Solution

For Clients, or Find a Partner?

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Imagine you received the following panicked phone call from an executive at one of your client companies — and consider how you'd want to be prepared to handle it.

Your client's CEO calls to tell you his staff has been locked out of their network and all of their data, and that the screens are all displaying a ransomware message demanding a big payday in bitcoin or the hackers will destroy the company's data permanently. You can hear the urgency in his voice. His business is at stake. And your reputation. This is why he's engaged you.

As his go-to technology service partner you have a redundant, cloud-based backup solution deployed to cover him for just such an emergency — thank goodness!

The question for you: *In this exact moment, what type of backup system would you hope to have for your client? Would it be a solution you've set up and manage in-house, or a third-party cloud backup service you've outsourced to an industry expert?*

The aim of this paper is to give you a more thorough understanding of your options when it comes to adding a cloud-backup service to your technology portfolio, and to present for you the pros and cons of each.

Of course, there are a range of scenarios you could face. Perhaps your client had its offices in the region ravaged by Hurricane Matthew, and they lost all of their onsite hardware and data storage. Or perhaps they simply accidentally deleted an important folder. The point is your clients face a number of risks to their mission-critical data — from malicious actors, accidents and natural disasters. The question isn't whether they need offsite backup; they do. The question is which type of solution will make sense for their business — and for yours.

There isn't necessarily a one-size-fits-all-technology-providers' answer to this question of whether to outsource or build your own cloud backup and disaster recovery offering. This decision will require your business to weigh many factors. For example: If you maintained the backup system in-house, you'd command 100% of the profit. But that would require you to staff and pay for a team of support reps to be available 24/7. After all, what if that CEO's call came at 10:30pm Sunday night? There's a lot to consider before you make a decision.

But one point we need to make at the outset: Given the degree to which your clients increasingly depend on their digital data for normal business operations, and given all of the ongoing threats to that data, if you don't already have a cloud backup and DR solution in your portfolio, you'll want to add this vital and lucrative service as soon as possible — whether you decide to build or outsource it.

INTRODUCTION

“Online backup and recovery leads new cloud purchases.”

That subhead was featured in a recent report by the IT community Spiceworks, based on a survey of IT professionals. The report explains that among those businesses planning to deploy new cloud solutions, backup and recovery tops the list — even ahead of productivity applications.

This is an illuminating data point: Before corporate IT pros will feel prepared to focus on helping their staff become more productive, they first need to ensure that the company’s mission-critical digital assets are safely backed up and retrievable in the event of a disaster.

78%

of IT Organizations Plan to Increase Their Investment in Cloud Services Over the Next 3 Years”

ESG Research Report

Another subhead you might find interesting: **“Managed services see a fair portion of budget dollars.”** This section of the report explains that corporate IT professionals are planning to spend a significant portion of their technology budgets on managed services, and that at the top of that list will be cloud-based storage, backup and archiving services. [1]

What all of this underscores, of course, is that as a technology reseller — MSP, VAR or solution provider — you have a major revenue and business-building opportunity by adding cloud backup and recovery services to your solution portfolio.

With the rapid rise of data breaches, ransomware attacks and other cybercrimes against businesses — not to mention the ongoing threat of natural disasters, software and hardware failure, and simple human error — your clients are always at risk of losing mission-critical data if they are not running a reliable system for backup and disaster recovery.

Moreover, your clients know this. Which is why, as Spiceworks found, cloud backup and recovery are among the highest-priority items on IT departments’ shopping lists.

Given the vast and growing market for cloud backup, and your clients’ understanding that they need to deploy such a solution sooner rather than later, the key question for your company is whether to build and manage your own backup infrastructure, or to find the right backup and recovery provider — and partner with that company.

This paper will help you weigh these options.

CLOUD BACKUP AND RECOVERY: WHAT YOUR CLIENTS NEED

Before we get into a pro-and-con discussion of your options — building your own backup infrastructure or partnering with a cloud backup expert and reselling theirs — let's review the basic components your clients will demand of any backup solution.

Based on the many consultations we've had with businesses that have approached us about their backup and recovery needs, here are the five most common must-have components we've found businesses will demand from any backup solution.

1. THE ABILITY TO MEET RECOVERY TIME OBJECTIVES (RTOS)

In case you're new to the backup world, one of the most important metrics in assessing a backup system's worth is whether it can meet your Recovery Time Objective, or RTO.

An RTO is the maximum time a business will be able to tolerate between a technology or process failure and that system being restored. This length of time is usually based on how long the business can go before the downtime causes material harm to its operations.

According to a report published in SecurityWeek, among businesses that had suffered unexpected downtime in the previous year, the average length was 25 hours. Of those businesses, 36% said that this downtime cost them revenue, and 34% also reported that it resulted in delays in their product development.[2]

Obviously, the length of downtime an organization can experience before it begins to suffer major disruptions will vary for each business. Perhaps some of your clients could weather a 25-hour power outage or other type of imposed downtime without serious consequences. Other clients, by contrast, might begin to suffer significant harm just minutes after losing access to their data or systems.

The point to keep in mind here is that you will need not only a proven, redundant and robust data backup solution for your clients — you will also need an equally robust and reliable disaster recovery solution. Moreover, that recovery solution will need to be scalable, to allow for even the most aggressive RTOs — such as the ability to recover and restore a client's entire digital infrastructure within minutes, if that's what they demand.

2. HIGHLY SECURE DATA STORAGE

Also at the top of the list for any successful backup system is an advanced set of security protocols for keeping your clients' data safe 24/7 from both cyber and physical attacks.

As the value of companies' digital assets grows, those assets face an ever-greater threat of breach, theft, destruction, hijacking and other forms of attack.

To cite just one industry, the publication Modern Healthcare pointed out that 2016 has been called "The Year of Data Security," because in 2015 cyber hackers — from disgruntled former employees to sophisticated ransomware attackers — leveled devastating attacks against many of the largest and highest-profile healthcare enterprises. In fact, the article cites research from the security firm Ponemon Institute stating that nearly 90% of all healthcare companies had suffered a data breach within the prior two years. [3]

Your clients know their mission-critical data is at constant risk from hackers. Which means that when they investigate cloud backup and recovery providers, they'll likely demand proof these systems offer the highest levels of security and encryption for their data.

3. BACKUP AND RECOVERY PROCESSES THAT MEET REGULATORY REQUIREMENTS

For any of your clients that handle personally identifiable information (PII) for their customers — medical history, financial records, student files, etc. — chances are those companies are regulated by at least one of the many federal data privacy laws.

The HIPAA law, for example, governs healthcare and demands all companies in this industry — "covered entities" and their "business associates" — implement steps to safeguard the electronic protected health information (ePHI) under their care. Similar data laws exist for public companies (SOX), educational institutions (FERPA) and financial-services firms (GLB).

The upshot of these federal laws is that many of your clients are legally required to take steps to protect their customers' data. These steps might include encrypting that data both for transmission and storage, implementing controls that limit access only to authorized personnel, documenting a recovery or business continuity plan for a disaster, etc.

Moreover, these regulated businesses could face federal audits at any time and are subject to steep fines and other penalties for any instances of noncompliance.

And perhaps most frustrating for your clients, even if they deploy such processes, they will still have difficulty knowing whether they are compliant — because these laws were written vaguely, to allow for technological changes and new processes.

As a reseller of cloud backup and recovery solutions, then, you will likely be handling and protecting a great deal of your clients' federally regulated data. That will put some of the responsibility on your solution for helping them comply. Your clients will want to know your solution is compliant with their regulators — and that your company (or the company you partner with) has considerable experience dealing with those specific regulatory demands.

4. A BACKUP AND RECOVERY SOLUTION THAT IS FULLY CUSTOMIZABLE

When it comes to data backup, a successful solution will by definition have to be customizable. Every company's backup and recovery needs are different, because there are an infinite number of configurations for a business's technology infrastructure and processes.

Your clients' technological profiles no doubt differ by operating systems, cloud applications, mobile devices, onsite hardware systems, storage capacity, existing data governance rules, and many additional variables.

Let's examine just one of these variables — data governance rules — to gain an understanding of just how flexible and customizable your backup solution will have to be, if you hope to sell such a solution across your client base.

Perhaps some of your clients' companies enforce strict IT policies mandating that no employee may view, store or transmit any proprietary data or sensitive customer information on mobile devices — or to access such data outside the company firewall. In such a case, your backup and recovery solution's focus will likely be on that client's in-house computers, servers and other onsite hardware.

But for a client without such governance, and whose employees frequently access and send proprietary (or even regulated) data via mobile devices and outside the company firewall, you will also need to offer some sort of endpoint protection with your backup solution. This might include, for example, a mobile device management system with geo-locating for lost devices and the ability to remotely wipe data from those devices.

In other words, your system will likely need to be tailored to some degree for every client. There is no one-size-fits-all backup solution.

5. A HIGH LEVEL OF TECHNICAL AND BUSINESS SUPPORT

Finally, most clients will demand a robust support system be built into any data backup and recovery solution they consider purchasing. These services are, by definition, there for emergencies — and in an emergency your client doesn't want to hear a recording on your Customer Support number, telling them you're closed until tomorrow morning.

Cloud backup and recovery vendors run the gamut in quality — from fly-by-night operations with no backing, experience or infrastructure, to longtime experts that provide 24/7 support and even actively monitor your backed-up data so that they can act on a problem even before you know something's gone wrong.

This is one of the key considerations in determining whether to build or buy the cloud backup solution you plan to offer your clients. A key cost of deploying such a solution is to develop a support center of trained engineers, available at all hours of every day, and who can expertly address any data problems your clients face.

If you are not comfortable staffing such an around-the-clock support center, then this alone might be reason enough to investigate your options for partnering with an existing cloud backup provider.

BUILDING YOUR OWN BACKUP AND RECOVERY SYSTEM:

THE PROS AND CONS

As a technology reseller, the relationships you build with your clients over time — and the trust and credibility you earn — are what make you successful. This is why you thoroughly vet every third-party solution you add to your portfolio. You cannot afford to have your credibility as a solution provider undermined by a vendor's failure or inadequacy.

It is also for this reason that you might be considering developing and selling your own backup infrastructure, rather than finding an expert to partner with. Here are the key advantages of going it alone.

1. YOUR COMPANY MAINTAINS COMPLETE CONTROL — INCLUDING QUALITY CONTROL

One perceived advantage of building and selling your own in-house backup and recovery solution is that you will not have to worry that your backup partner isn't up to the job of protecting your clients' data.

That's understandable. As MSPMentor reported back in 2014, a cloud hosting service specifically for coders, called Code Spaces, was hacked. After breaking into the company's Amazon Web Services account, the attackers deleted almost all of the data of Code Spaces and its customers. They even managed to destroy the company's backup files. [4]

If Code Spaces were a third-party cloud service you'd selected to offer your clients for storing their code online — particularly if you maintained the customer relationship and white-labeled the Code Spaces solution — the breach would have reflected poorly on your company and could have caused irreparable harm to your reputation.

When you build your own backup solution, on the other hand, you can oversee every aspect of its development, continue to monitor it 24/7 while it's in service, and ensure its quality is at a level you're comfortable with for your clients.

2. YOU OWN THE CLIENT RELATIONSHIP

Another advantage of offering your own in-house backup solution is that you won't have to worry about your relationship becoming diluted as your clients work closely with another provider — your cloud partner — for their backup and recovery needs.

You have likely found that, because so much of your business is built on the deep relationships you build with your clients, it is valuable to remain your clients' key point of contact for as many of the third-party solutions you sell to them as possible.

This obviously becomes less feasible as your client list grows and the number of solutions they purchase through you grows as well. But to the extent that your company has the resources, it is often beneficial to remain the technology provider of record, which includes remaining each client's key contact, for as long and for as many of your services as you can.

Every touch point you have with a client, after all, gives you and your team another opportunity to demonstrate your value, to gather business intelligence on that client's needs, and to identify other possible solutions to offer them.

For this reason, if you were to investigate partnering with a third-party cloud backup provider, you would want to make sure that such a partner offered flexible options for reselling their solutions — up to and including the ability to own the client relationship to whatever extent worked for your company.

3. YOU WILL NOT HAVE TO SHARE THE PROFITS

Finally, one obvious advantage of developing and selling your own solution is that your company will be able to realize all of the revenue from selling it — rather than having to share that revenue with a partner whose solution you're offering.

A related potential benefit here is that, as the sole owner of your backup solution, your company will also be able to set the pricing for all services related to the infrastructure you've built — cloud backup, disaster recovery, endpoint protection, etc. Certain third-party cloud vendors will box you into their own prices and pricing structures.

Again, if you choose to select a cloud backup and recovery partner, you will want to work only with a provider that offers a high level of pricing flexibility.

THE DRAWBACKS OF BUILDING YOUR OWN BACKUP INFRASTRUCTURE

Now that we've discussed the benefits of developing and selling your own backup and recovery solutions, let's examine the drawbacks.

1. THE COST AND WORK INVOLVED MIGHT BE PROHIBITIVE

We've discussed maintaining control over your backup infrastructure as a benefit. And that's true — rather than having to choose from backup offerings already on the market, you can create and fully control a solution that's just right for your business and clients.

BUT WILL IT BE WORTH THE EFFORT?

Developing an in-house backup and disaster recovery infrastructure will be equivalent to launching a startup business within your company. It will require all of the cost-benefit analysis, talent sourcing, market research and other upfront work and investment capital that goes into starting any new venture. Just some of the research you'll have to do and decisions you'll have to make:

- What will this infrastructure look like? Will we want it all onsite? All offsite? A hybrid?
- What hardware will we need to purchase or lease?
- What about software? Should we license it or develop it in-house?
- Where will we find the talent to staff up our Customer Support center?
- Do we have any in-house experts on backup and recovery? Will we have to hire this?
- How much centralized management will we need to do to oversee our clients' backup services? Will we manage this in-house or outsource it?
- Do we have in-house expertise on backup and recovery compliance? Will we need to hire this?
- What encryption technologies will we need? Will we need to license?

This list could go on and on, of course, and it will have to — if you choose to build and sell your own backup system and you expect to develop the domain knowledge needed to make it successful.

2. DEVELOPING YOUR OWN BACKUP SOLUTION WILL TAKE MUCH LONGER THAN PARTNERING WITH THE RIGHT EXISTING PROVIDER

Consider a few important statistics.

Forbes has reported that only 38% of small businesses have a formal disaster recovery plan in place. [5] And research firm Technavio estimates that the cloud backup and recovery markets will enjoy a substantial 27% compound annual growth between 2016 and 2020. [6]

This means there is a good chance a significant percentage of your clients — perhaps even a majority — do not yet have in place a comprehensive solution for cloud backup and disaster recovery. Moreover, the opportunity to realize substantial revenue from selling backup and recovery solutions exists right now.

If you opt to build your own proprietary solutions, you will likely miss the window to sell these services to many of your clients.

But by identifying the right cloud backup and recovery partner and selling their offerings, you can start realizing those new revenues immediately.

3. YOU RISK BECOMING ANOTHER UNDIFFERENTIATED “ME-TOO” BACKUP PROVIDER

As we’ve pointed out, backup and recovery services run the gamut in terms of quality and legitimacy. Partly because a business can quickly and inexpensively purchase cloud server space, throw up a thin website and call itself a “cloud backup provider,” there has been an exponential increase in such companies.

What will make a backup and disaster recovery business truly stand out among the crowd, then, are its experience, its time in business and its list of satisfied customers. If you develop a backup infrastructure today, it will be years before you are able to truly differentiate that service from the long list of competitive services on the market.

That’s why it is advisable to partner with one of these companies — ideally a backup provider that has been around for many years and successfully serving enterprises around the world.

WHY PARTNERING WITH AN EXISTING BACKUP AND RECOVERY PROVIDER IS THE SMART DECISION

As we’ve tried to point out above, creating and maintaining your own backup and recovery solution will almost certainly be costlier and more time consuming than finding the right partner and adding their solution to your portfolio.

Additionally, during your development phase you’ll miss out on months and perhaps years of generating new revenues selling these much-needed services to your clients and prospects — and as we’ve demonstrated above, they’re looking for these services right now.

Furthermore, unless your company has a great deal of in-house expertise in backup and disaster recovery, or is willing to spend a great deal of upfront capital, the chances are you won’t be able to develop a superior, differentiated solution anyway.

For these and other reasons, we highly recommend putting your research and investigation efforts into studying the cloud backup landscape, looking for providers that offer superior solutions and lucrative partnership programs, and then further narrowing this field to those providers that have a flexible portfolio of reseller arrangements. After all, you might want to merely hand off warm leads today and collect a commission — but then tomorrow become more involved in the sale and servicing of these backup and recovery solutions.

When you partner with the industry-leading KeepItSafe® family of cloud backup and recovery solutions, here are just some of the benefits you'll be able to sell from day one, without having to source, build or manage any of them:

- A proven backup and recovery infrastructure that can be fully tailored for companies of any size and across any industry
- The advanced encryption protocols to protect your clients' data both in transit and at rest
- Compliance expertise to ensure your clients' backup and recovery processes meet the mandates of their industry's specific regulations (including regulations regarding sending data overseas for your international clients)
- A guaranteed uptime for your clients to access their data in the cloud
- Flexible plans to meet any client's Recovery Time Objective — up to and including bare-metal restore and full recovery of all data within minutes
- Flexible retention plans for your clients' data — from days to years
- Support for virtually all operating systems, applications, devices and databases
- White glove service that includes all management, maintenance and troubleshooting
- Sophisticated endpoint protection and mobile device management
- A team of highly trained technical support engineers, monitoring your clients' data 24/7
- **Flexibility in partnership programs — from referral-based commissions to our resellers fully owning the client relationship**
- **Dedicated account managers and complimentary marketing services to help our partners succeed**

If you'd like to learn about how you can begin selling proven, industry-leading cloud solutions for data backup and recovery, please contact us.

INTRODUCING
KEEPITSAFE

For more than a decade, KeepItSafe has been a world leader in compliant cloud backup, disaster recovery and endpoint protection — serving more than 40,000 corporate customers, across four continents, and protecting more than 50 petabytes of mission-critical data every year.

We offer a premium, white-glove service for cloud backup, recovery and business continuity — and we are among the only global recover providers awarded ISO 27001 certification for information security management

Visit our website, **www.KeepItSafe.com,** to learn more about our industry-leading solutions for cloud backup, disaster recovery and endpoint protection.

Or contact us anytime to schedule your free Network Evaluation and Data Protection Assessment, as well as to begin a free trial of our solution.

888 965 9988

info@keepitsafe.com

Sources:

1. **Spiceworks — "Tough Choices Ahead for Cash-Strapped IT Departments in 2015"** https://www.spiceworks.com/press/releases/2015-01-21/

2. **SecurityWeek — "Downtime and Data Loss Cost Enterprises $1.7 Trillion Per Year: EMC"** http://www.securityweek.com/downtime-and-data-loss-cost-enterprises-17-trillion-year-emc

3. **Modern Healthcare — "2016: Year of Data Security"** http://www.modernhealthcare.com/article/20160227/SPONSORED/160229900

4. **MSPMentor — "The Cautionary Tale of Code Spaces"** http://mspmentor.net/infocenter-cloud-based-file-sharing/062714/cautionary-tale-code-spaces

5. **Forbes—"Natural Disasters: Is Your Small Business Prepared?"** http://www.forbes.com/sites/capitalonespark/2013/01/28/natural-disasters-and-emergencies-is-your-small-business-prepared/#1c41b9045b16

6. **Technavio — "Global Backup-as-a-Service Market"** http://www.technavio.com/report/global-cloud-computing-backup-service-market