KeepItSafe®
ONLINE BACKUP

MANAGING THE DAILY DATA BLIZZARD:

WHY BUSINESSES NEED CLOUD BACKUP MORE THAN EVER

TABLE OF CONTENTS

INTRODUCTION

Welcome to the digital universe.

The volume of corporate data your IT department has to manage is exploding. And corporate data is more critical to business success than ever before:

INFORMED DECISION MAKING | CUSTOMER ORDERS | COMPLIANCE | REVENUE | THE BUSINESS'S CORE

According to a recent report by Forbes, more data has been created in the past two years than had been generated previously in all of human history combined.[1] In related research, IDC estimates that the amount of data an enterprise generates doubles every 18 months.[2] In other words, just keeping track of all of your corporate data is an increasingly difficult undertaking.

Moreover, this challenge will only grow more difficult year after year. According to the Forbes report cited above, by the year 2020 about 1.7 megabytes of new data will be generated per second for every human being on the planet. [3]

But the challenge goes beyond just managing an ever-growing volume of data. The growth rate of your business data also directly correlates to the number of locations where the data resides.

To cite a couple of examples, a 2016 study by researchers at the Ponemon Institute and digital security firm Gemalto found that half of all corporate data stored in cloud apps and services are not controlled by the companies' IT departments. Even more troubling, that study also found that in nearly 80% of company decisions to purchase new cloud apps for employee use, the IT and security teams are not even involved.[4]

Additionally, about 28% of all enterprise data resides solely on endpoint devices, and the volume of this endpoint-only company data is doubling every 14 months.[5]

These challenges facing you today as a corporate IT professional are unique in the history of your field. Protecting and preserving business-critical data — and keeping track of this data even as it expands exponentially and across a wider array of apps — raise an important question. **Is there a simple, cost-effective way to track, save and secure all of your corporate data — no matter how many places it resides, no matter how fast it grows, and no matter how large it gets?**

The answer is yes: a cloud backup and disaster recovery solution from a reputable, proven provider.

This paper will discuss the current challenges in securely overseeing your company's rapidly expanding data, explore your options for backing up this data, and offer our recommendation — based on decades of real-world experience — that your company leverage a fully managed and actively monitored cloud backup and recovery partner.

YOUR DATA IS EVERYWHERE

Before we delve into a discussion of your options for data backup and recovery, let's frame the challenge. Simply put, your data is scattered across too many locations, platforms and devices for you and your team to effectively manage and protect it.

The intersection of the Internet, cloud services and mobile technology has made corporate IT management far more complicated than it was just a few years ago. Today, your corporate data no longer resides only on the company-issued desktops, laptops and servers that you manage directly. It is also being stored on and transmitted from employees' personal mobile devices, their home computers, virtual servers hosted by third-party cloud providers, and of course an ever-increasing list of Software-as-a-Service platforms like Microsoft Office 365 and Salesforce.

A recent study by IBM Security found that one in every three employees at Fortune 1000 companies regularly saves and shares company data using cloud platforms and apps (think Google Drive and Dropbox).[6]

As *SecurityIntelligence*, the magazine reporting the study, explained in its article, "By using these third-party cloud applications, organizations can neither see, manage nor secure the information employees are sharing outside of company policy. While it's a violation of most corporations' security policies, the fact is employees are using these cloud services to get their jobs done."[7]

Although the focus of the IBM Security study was clearly the protection of corporations' data against cyber theft, these findings reveal another important truth for your company — even if you're with a small firm not in the Fortune 1000. When your employees use devices and apps not under your IT team's control to store business data, that data is at risk of more than simply being hacked by cybercriminals. It is also at risk of being lost or corrupted if the platform on which it is stored suffers a technical issue.

What's more, if your IT team is not able to control this company data, you are also not able to back it up. A loss of business-critical data in an unauthorized cloud app can often mean that the data is lost forever.

THE VALUE OF YOUR DATA…
AND WHAT LOSING IT CAN COST

So, what happens when a company loses mission-critical business data?

One helpful explanation comes from a paper published by Pepperdine University's Graziadio School of Business and Management. The author, an associate professor of economics, explains that there are two possible outcomes (and costs associated with both).

Outcome 1: The company will spend time and resources to recover the data, and will do so successfully. In this case, the costs to the company will be the costs of the IT or data professionals needed to retrieve the data, as well as the lost company productivity as a result of the downtime without use of this critical data.

Outcome 2: The company will spend time and resources to recover the data, but won't be able to do so. They will conclude the data is lost forever. In this case, the costs to the company will be the costs of the IT or data professionals attempting to retrieve the data, the lost productivity resulting from the downtime without the use of the data — and the additional costs of employees needing to recreate the data as best they can.[8]

This hypothetical data-loss walkthrough is useful as far as it goes. But it misses the far more significant loss to the company that we discussed in the introduction. More and more, businesses are leveraging their corporate data as true assets — actionable insights into their customers, valuable guides as to what products to build (and which ones to sunset), and clues as to where to deploy resources to capture new opportunities. Which means that the responsibility on your IT team is also greater than ever to protect this data, and to ensure it's always accessible when needed.

With the proliferation of sophisticated tools for data analytics and business intelligence, your company's data is growing more valuable every year. Because applications can now analyze raw data to uncover actionable intelligence, your organization's digital intellectual property is more important than it's ever been.

For example, that Forbes article we cited in the introduction also points out that retail companies that leverage the full power of big data could increase their operating margins by as much as 60%.[9]

In other words, your data is often far more valuable than the costs to recreate it, the costs to retrieve it if it's accidentally deleted, and even the costs measured in downtime as your company is forced to go without it.

One great illustration of this is Intel's "Billion Dollar Lost Laptop Study."

THE BILLION DOLLAR LOST LAPTOP

A few years ago Intel partnered with the Ponemon Institute to determine the true cost to a business of losing a company-issued laptop. As you might expect, the key cost was not the actual amount of money needed to replace the laptop; indeed, this represented the smallest portion of the overall cost.

And what was the average overall cost to a business of an employee losing a laptop? A staggering $49,246!

That's because the study took into account some of the factors a typical business might overlook in assessing how much it had actually lost when an employee returned to work from a business trip and reported that he'd lost his laptop on the road. Among the true costs of a lost company laptop, the reported pointed out, are lost intellectual property, and legal and regulatory expenses.[10]

For a business in a heavily regulated industry, such as a healthcare organization, we'd add yet another cost component to a lost laptop: Damage to the company's reputation and goodwill with the public.

To cite one recent example, Indiana-based Premier Healthcare had one of its laptops —which was unencrypted — stolen in early 2016, and the data on that machine allowed hackers access to more than 200,000 patients' personal medical records. [11]

Although Premier Healthcare could face steep fines from federal regulators for violating mandates of the Health Insurance Portability and Accountability Act (HIPAA) — to the tune of tens of thousands of dollars — the negative publicity the breach has created for Premier has already proven far more expensive. Clearly, this is one laptop loss that will cost its owners more than $49,246.

To sum up, the loss of your business's critical data can't be measured merely by calculating the resources your company will need to recreate it. Indeed, losing critical data can be catastrophic — resulting in loss of irretrievable intellectual property and competitive advantage, not to mention the potential legal, regulatory and public-reputation implications of a major data loss.

Of course, your IT team's inability to track all of the data your employees are creating and sharing in the cloud — and therefore to back up that information — is only one reason you could lose mission-critical data. There are several other ways your company is at ongoing risk of data loss.

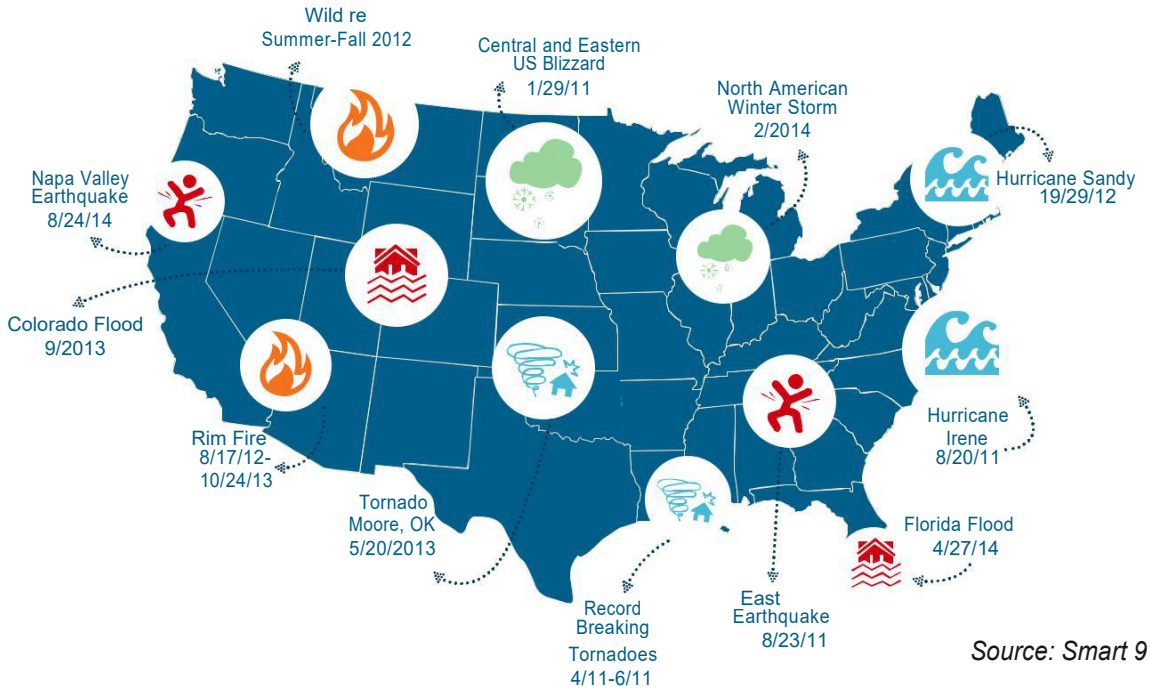
Let's briefly review them here — because each will play a role in our recommendation for the specific type of backup solution your company should deploy.

4 COMMON CAUSES OF DATA LOSS

1. NATURAL DISASTER

One of the important reminders from the tragic Louisiana flood of 2016 is the risk that businesses face when they fail to duplicate their digital assets and keep them securely stored in more than one location — ideally in more than one geographical region.

A view of the map below, provided by disaster-preparedness service Smart 911, illustrates that every region of the United States has suffered a major natural disaster of some sort since 2011.



Source: Smart 911

And according to a feature in Business2Community magazine, the last time this region faced flooding of similar magnitude — due to hurricanes Katrina and Rita — 60% of Mississippi's small businesses were forced to close permanently.[12] And in many cases, because these businesses neglected the "worst-case scenario" planning when it came to their data, it was in fact the irretrievable loss of mission-critical company data that forced the permanent shutdowns.

Natural disasters can strike anywhere, anytime. Earthquakes, floods, hurricanes, tornadoes, fires — the list goes on. Which is one reason it can be so dangerous to store all data — and backed-up data — in the same physical location.

2. RANSOMWARE ATTACK

As *The Los Angeles Times* recently reported, when an employee of LA-based Hollywood Presbyterian Medical Center attempted to log in to his work computer, he found a terrifying message — a ransomware note. The message alerted the employee that hackers had seized control of the institution's entire computer network and were demanding money (paid in bitcoin) before they would return control of the hospital's data back to its rightful owners.[13]

The ransomware threat is growing every day. According to a 2016 ransomware report conducted by the Kaspersky Security Network, between April 2015 and March 2016 ransomware attacks worldwide rose nearly 18%, up to a jaw-dropping 2,315,931 incidents.[14]

Of course, when a hospital or other healthcare entity has its data hacked and stolen, the organization has other worries — its patients' security, noncompliance with federal regulations, damage to its reputation. But in the case of most businesses in most industries, knowing that their corporate data is continually backed up, securely, offsite and in multiple locations will mitigate at least some of the concern about being victimized by a ransomware attack. It will mean, in other words, that the chances of such an attack dealing a fatal blow to the victimized company are minimal.

3. HARDWARE FAILURE

Of course, most causes of corporate data loss are far less dramatic than the ransomware attack.

What if an employee simply drops a computer? Or someone spills coffee on a company flash drive? Or one of the many data-storing computers around your organization — laptops, desktops, tablets, smart phones, servers, etc. — simply gives out?

According to a report from BetaNews, about two-thirds of business data loss is attributable to some sort of hardware failure, like drive crashes. And if you're thinking your company is okay because you back up your data onsite, consider also that your backup devices are also prone to failure — tapes can become corrupted from mishandling or overuse, for example, and drives can fail due to inadequate cleaning.

Furthermore, this report also found that 27% of businesses that lost some of their data also suffered a disruption to their normal operations as a result. [15]

What this all points to, like the previous examples, is that the safest and smartest approach to data backup and recovery is to find a cloud-based solution that lets you continually and automatically back up your data offsite, in multiple, geographically distinct facilities.

4. HUMAN ERROR

Finally, there's always human error.

You can secure your network, encrypt your files with the most sophisticated protocols available, implement a mobile device management program, protect your systems with an intrusion prevention system, and make sure all of your organization's hardware and software are always cutting edge. But none of that will matter when you hear "Oops!" from the cubicle of an employee and look up to see him standing over his computer, all of the color drained from his face.

According to a 2015 article in Computer Business Review, human error is responsible for a third of data loss — often from simple mistakes such as accidentally deleting files. [16]

These mistakes are compounded, of course, when the company itself does not have a continual, automatic system for backing up all corporate data. In such a scenario, a simple tap of the wrong key on an employee's office computer can permanently and irretrievably wipe out a company's mission-critical data.

DATA BACKUP OPTIONS

In all of these examples above, the damages could have been minimized — if not eliminated entirely — if the businesses had implemented a comprehensive solution for data backup, disaster recovery and endpoint protection.

When it comes to data backup, broadly speaking businesses have two options — onsite backup and cloud backup. (There are variations of these, including a hybrid model that employs both onsite and offsite backups, but we will focus on these two primary categories.)

IN-HOUSE DATA BACKUP SYSTEM

Internally managed data backup has been the standard for businesses for decades. The primary tools include backup tapes, disks and servers. And although these systems can work well under ideal conditions, they pull IT resources away from more forward-looking initiatives to manage, troubleshoot and manually perform the data backups on a regular basis.

And those are under the best conditions — when nothing threatens the company's systems or physical location.

But remember, we've established that under many of the most common causes of data loss, having a full backup of all corporate data onsite would likely do little or no good — because that backup hardware would also be at risk.

In the case of a natural disaster, for example, even the most sophisticated and reliable backup tape, disk or server system onsite won't help the company resume normal business operations quickly — because that backup hardware will be at just as much physical risk as the other IT infrastructure at the company's facilities.

The story is similar for a ransomware attack. In the first part of these two-part attacks, the hackers first implement malware, a virus or some other intrusion method to seize control of the company's digital network. If the hackers were successful in gaining control of the company's primary network systems, it's entirely possible that they would simultaneously gain control of the onsite backup system as well.

Moreover, onsite backup is also subject to all manner of human error. An IT staffer might forget to place in a new backup tape in the evening before going home. Or he might place in a non-blank tape and rewrite over mission-critical business data. He might also simply forget to clean the drives and, as a result, cause a future tape backup to fail.

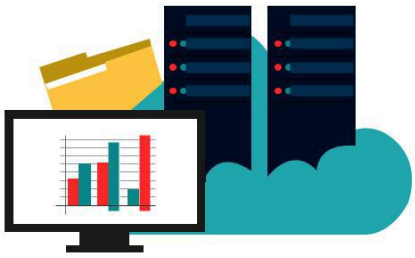
Finally, there is the matter of regulatory compliance. Many of the federal data privacy regulations governing businesses that handle customers' or patients' personally identifiable information demand that these businesses store this sensitive data offsite, in secure data centers.

For all of these reasons — as well as the ongoing costs of maintaining an in-house backup infrastructure — we recommend a hosted, cloud backup and recovery solution.

CLOUD DATA BACKUP AND RECOVERY SYSTEM

Cloud backup, sometimes called online backup, is the process of backing up data by sending a copy securely over a network — either a private network or the public Internet, using encryption in either case to protect the data in transit — to an offsite server hosted by a cloud backup provider.

Cloud backup has emerged in recent years as a secure, cost-effective and more reliable method of backing up mission-critical business data than maintaining an onsite backup infrastructure.



This helps explain why a survey conducted by IT community Spiceworks found that, of those businesses planning in 2015 to deploy new cloud solutions, backup and recovery solutions topped the list.[17]

WHY CLOUD DATA BACKUP AND RECOVERY IS SUPERIOR

There are many benefits to deploying a cloud-based solution, rather than an onsite and internally-managed system, for data backup and recovery. Here are just some of them.

1. YOU CAN LEVERAGE YOUR EXISTING INFRASTRUCTURE

A cloud backup and recovery solution doesn't require buying or installing expensive equipment — or maintaining and upgrading it, if you've already rolled out an in-house backup system.

Instead, a cloud solution lets you leverage your existing network to transmit your corporate data securely to an offsite location (or, with the best-in-class providers, to several locations) and not worry about managing any in-house backup hardware.

2. YOU'LL USE YOUR IT RESOURCES MORE WISELY

A cloud solution lets your business redirect IT resources away from the reactive, tedious tasks of managing and troubleshooting in-house backup hardware, and onto more forward-focused technology initiatives that can truly improve the company's bottom line.

3. YOU CAN IMPROVE YOUR RECOVERY TIME OBJECTIVES

The right cloud backup and recovery provider will be able to help your business get back up and running quickly after a data disaster — and the best-in-class providers will often be able to get your team access to lost or compromised data within minutes.

Because such a system boosts the speed and reliability of your data recovery, you can use a cloud backup service to improve your recovery time objectives.

4. YOU CAN SET IT AND FORGET IT — AND LOWER YOUR OPERATING COSTS

When you partner with the right cloud backup provider, you'll be able to set a backup schedule that's right for your company, and from that point forward your data will be saved and backed up automatically — without your team having to perform any steps to make this backup happen on an ongoing basis.

This set-it-and-forget-it method will result in lower operational and administrative costs for your company.

5. YOU'LL ALWAYS HAVE DATA BACKUP EXPERTS WATCHING OVER YOUR DATA — AND ALERTING YOU IMMEDIATELY OF ANY TROUBLE

When you sign up with the right cloud backup and recovery partner, you'll be purchasing much more than a "backup system," the way you would if you were buying onsite tape drives and tapes. With the right cloud backup provider, by contrast, you'll be entering into a true partnership — one in which your data will be not only backed up automatically and securely to multiple locations for redundancy, but also actively monitored 24/7 by a team of trained support engineers who know how to spot any data irregularities and how to handle the situation when they do.

In other words, with the right cloud backup solution, you will enjoy around-the-clock digital as well as human protection of your data.

6. YOU'LL BE MUCH BETTER ALIGNED WITH YOUR INDUSTRY'S REGULATORY REQUIREMENTS

Finally, when you deploy the right cloud backup and recovery system, your company will be in an enhanced position with regard to your industry's federal data privacy regulations. The right cloud backup provider will know how to customize a compliant solution for virtually any company in any regulated industry.

Furthermore, the right cloud backup provider will also be willing to (pardon the pun) back up their claim to such regulatory expertise by signing the relevant industry agreements to demonstrate their willingness to share responsibility with your company to meet your industry's privacy regulations.

INTRODUCING KEEPITSAFE

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

We offer a fully managed and monitored service for cloud backup, recovery and business continuity —and we are among the only global recovery 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. Forbes — “Big Data: 20 Mind-Blowing Facts Everyone Must Read” http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#5d27b7ff6c1d
2. InfoWorld —“How to Survive the Data Explosion” http://www.infoworld.com/article/2608297/infrastructure-storage/how-to-survive-the-data-explosion.html
3. Forbes — “Big Data: 20 Mind-Blowing Facts Everyone Must Read” http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#5d27b7ff6c1d
4. Gemalto and Ponemon Institute — “Cloud Data is Still a Challenge for Many Companies” http://www.gemalto.com/press/Pages/Gemalto-Ponemon-Institute-Study-Cloud-data-security-still-a-challenge-for-many-companies.aspx
5. Montcrieff Technology Solution http://www.moncrieff.com.au/partner-list/druva_coud-based_endpoint_back-up/
6. SecurityIntelligence — “To the Cloud! Whether it’s Allowed or Not” https://securityintelligence.com/to-the-cloud-whether-its-allowed-or-not/
7. SecurityIntelligence — “To the Cloud! Whether it’s Allowed or Not” https://securityintelligence.com/to-the-cloud-whether-its-allowed-or-not/
8. Graziadio Business Review (Pepperdine University) — “The Cost of Lost Data” https://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/
9. Forbes — “Big Data: 20 Mind-Blowing Facts Everyone Must Read” http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#5d27b7ff6c1d
10. Intel Newsroom — “The Billion Dollar Lost Laptop Problem” https://newsroom.intel.com/wp-content/uploads/sites/11/2016/01/The_Billion_Dollar_Lost_Laptop_Study.pdf
11. HealthcareITNews — “Premier Healthcare Faces Possible Data Breach” http://www.healthcareitnews.com/news/premier-healthcare-faces-possible-data-breach-could-affect-200000-patients
12. Business2Community — “Preventing Devastating Business Loss” http://www.business2community.com/tech-gadgets/preventing-devastating-business-loss-the-top-causes-for-data-disasters-0398563#Yj3DSW6HBcPosomX.97
13. LA Times — “Hollywood Hospital Pays $17,000 in Bitcoin to Hackers” http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
14. Kapersky Security Network Ransomware Report https://securelist.com/analysis/publications/75145/pc-ransomware-in-2014-2016/
15. BetaNews — “Hard Drive Failure Responsible for Two-Thirds of Data Loss” http://betanews.com/2014/06/11/hard-drive-failure-responsible-for-two-thirds-of-data-loss/
16. Computer Business Review—“Human Error Causes a Third of Data Loss” http://www.cbronline.com/news/human-error-causes-a-third-of-data-loss-4507688
17. Spiceworks — “Tough Choices Ahead for Cash-Strapped IT Departments in 2015” https://www.spiceworks.com/press/releases/2015-01-21/