UNITRENDS

THE STATE OF CLOUD & DATA PROTECTION 2018

Survey Results: 10 Findings on how over 800 IT Pros handle Disaster Recovery & Cloud Adoption.

INTRODUCTION

The Unitrends 2018 annual survey of IT professionals about the challenges they face in protecting their data and business-critical applications culminated in July with over 800 survey respondents from companies of all sizes. The survey's questions focused on two aspects of IT, first the current state of data protection and disaster recovery, and secondly attitudes towards and usage of the cloud.

The survey found that many organizations are not even following minimal best practices for data protection and disaster recovery, while at the opposite end of the spectrum leaders in DR are increasingly using the cloud to play a critical role in business continuity. Ten major findings stand out from the survey responses. This report is divided into two sections. Section one focuses on the current state of data protection and disaster recovery. The second section highlights the growing acceptance and wider use of the cloud.

As part of the survey, we asked IT Admins "What advice would you give to someone just starting to use the cloud for backup and recovery?" You will find their answers along the blue margins. Spoiler Alert – Survey results highlight that in 2018 data centers continue to grow in size and complexity. The need for data protection and recovery solutions continues while the cloud is becoming a much larger part of the solution.

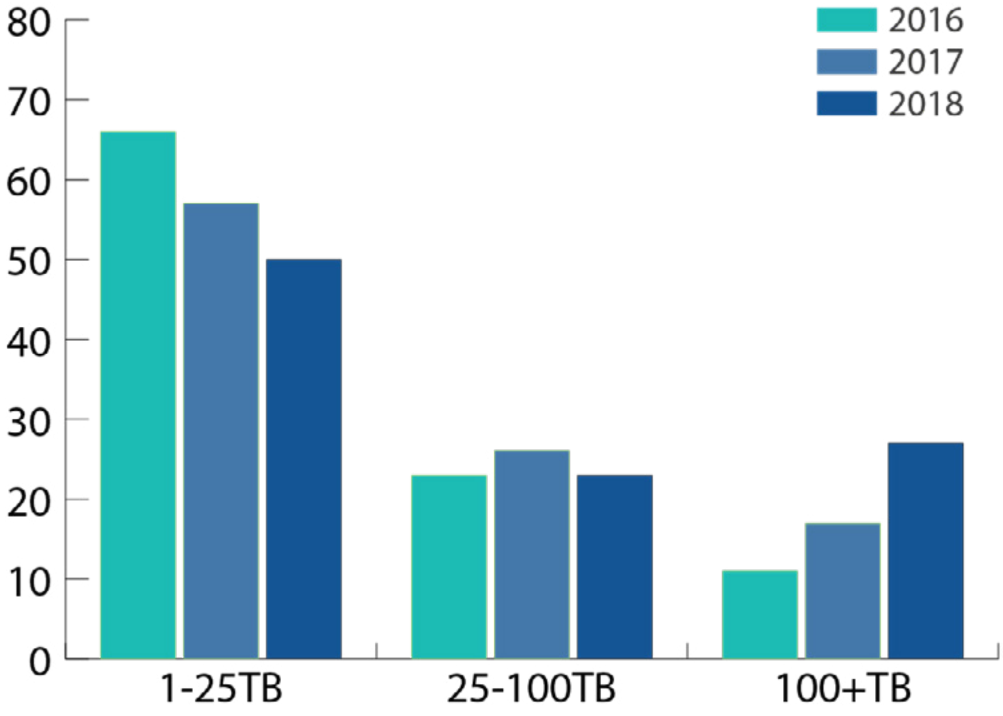
SECTION 1 – THE STATE OF DATA PROTECTION AND BUSINESS CONTINUITY

FINDING #1 – CONTINUED EXPONENTIAL DATA GROWTH

Since 2016, **the percentage of companies reporting they need to protect more than 100 TB** of data has doubled.

One challenge IT professionals of all industries face is the growing size and complexity of their environments. For example, a majority of 2018 survey respondents are required to protect both physical servers (73%) and virtual servers (67%). Another large challenge is the need to protect growing volumes of data. With similar-sized organizations responding across all three years of the survey, 2018 respondents show that a full 27% reported having over 100TB of data, more than double the percentage from 2016. Correspondingly, there is a significant decline in the percentage of respondents that protect volumes under 25TB. There is no sign that this trend won't continue going forward. Enterprises will need to keep investing in new storage and data protection services to stay even with the growing amounts of data they are required to protect. Without the right tools, the entire data protection and business continuity process will be longer, more complex, and costly.

How Much Data Do You Back Up?
2016, 2017, 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

"It is imperative to begin your investigation immediately and get a solution in place for your company's IP and data protection."

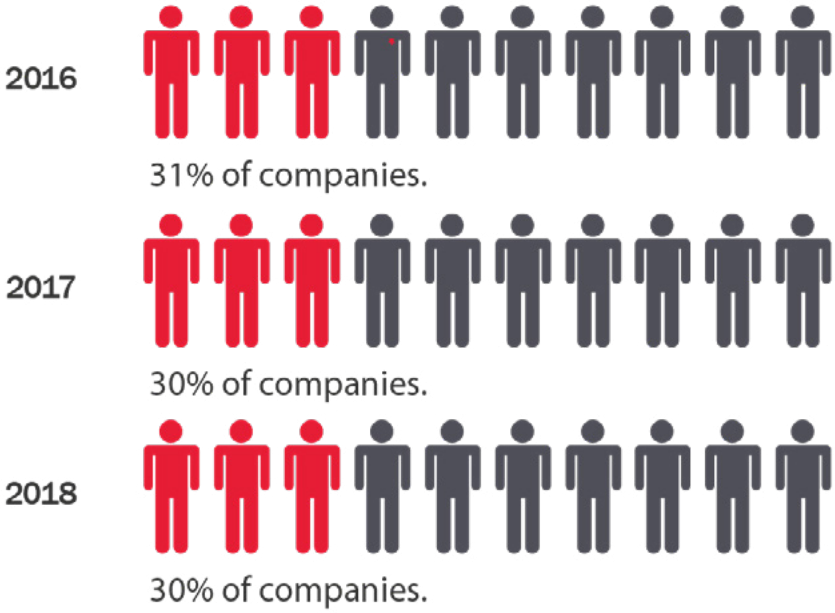
Systems Admin,
Small US
Technology
Provider

FINDING #2 – DATA LOSS CONTINUES AT AN UNACCEPTABLY HIGH RATE

The technology of data protection and business continuity continues to mature and get more efficient. New tools emerge all the time that can identify ransomware attacks, shorten RPO and speed recovery times. However, threats against enterprises' data also continue to evolve.

Data loss continues at an unacceptably high rate. **Almost the exact same percentage of respondents (30%) reported losing data across all three years of the survey.** Whether the cause is the rise and continuing threat of ransomware, natural disasters, or internal threats, every year one third of organizations report losing at least some of their data.

Percent of Companies That Experience Data Loss over the Last Year?
2016, 2017, 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

> "Don't do everything at once. Do proofs of concept and test everything."

Network Admin,
Large US
Construction
Company

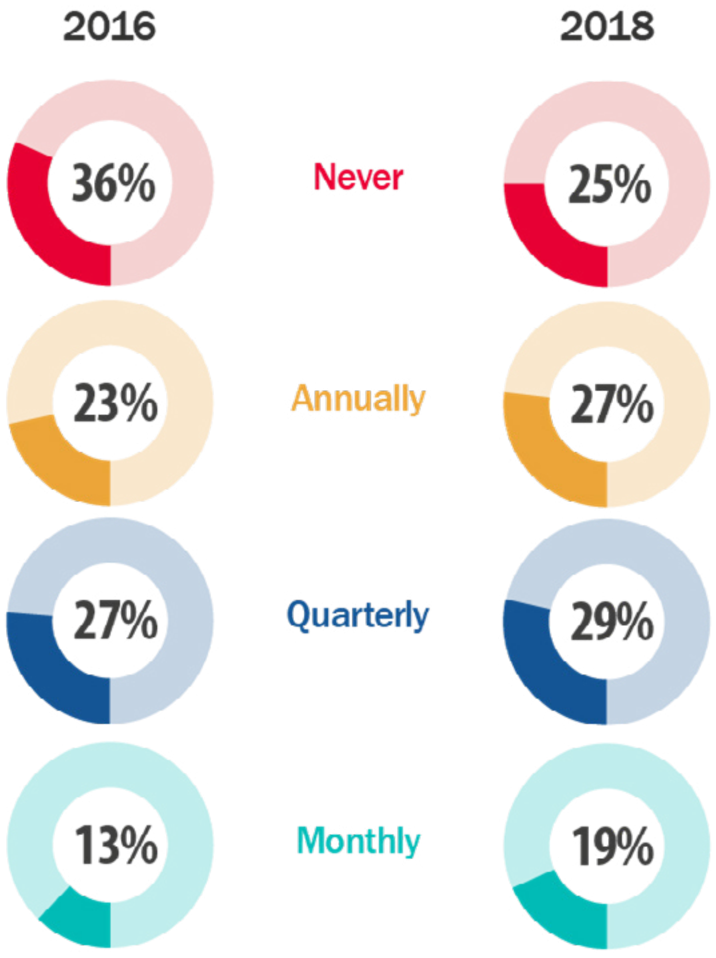
FINDING #3 –DR TESTING IS INCREASING IN FREQUENCY

The critical need for DR testing seems to finally be getting recognition.

In 2016 a majority (59%) of survey respondents reported that they tested their DR plans only once per year or not at all. In 2018 a majority of respondents still reported poor testing performance but that number decreased by 12% to 52%. This increased focus on testing extends to the frequency as well. There was a **46% increase in companies reporting that they test every month** and 7% increase in companies testing every quarter. Today a **full 75% report at least annual DR testing vs. just 64% in 2016.**

The only way to know if your failed applications can be restored to business performance is to test, find and fix recovery issues and then test again. The good news is that there are strong tools to make recovery testing automatic and easy, with high quality reports to identify what parts of the process have recovery issues. Many industries such as healthcare require all companies to know and document their recovery times. For more on this very important topic, please read Disaster Recovery Testing, Your Excuses, and How to Win. With 52% reporting they test only once per year or less, there is much room for corporate improvement on this topic.

How Often Do You Test Your DR Plan?
2016 vs 2018



Vendors of backup and recovery technology may support only lower levels of testing, yet claim they have full testing capabilities.

LEARN MORE ABOUT DR TESTING

FINDING #4 – FEWER ORGANIZATIONS HAVE NO SECONDARY RECOVERY SITE

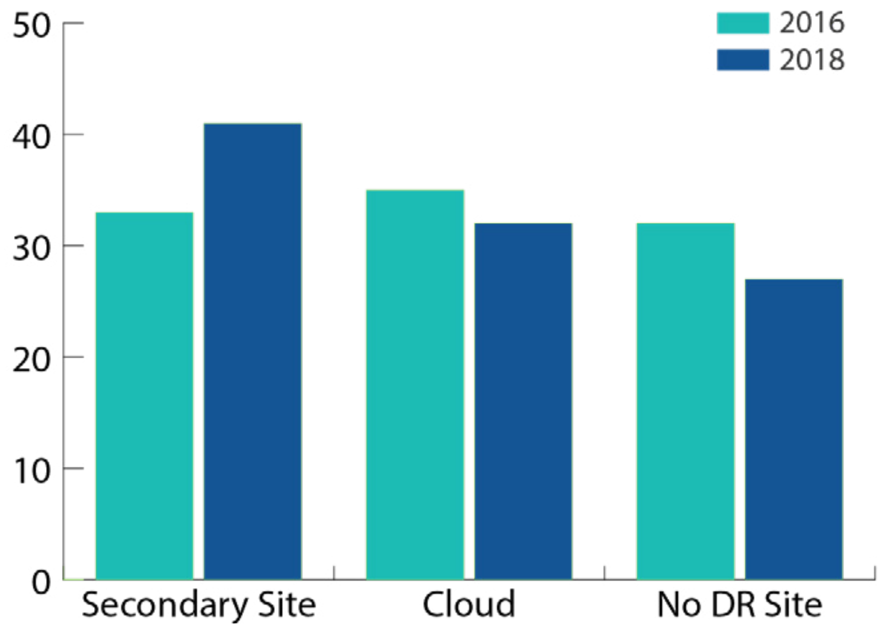
A secondary location is critical to protect backups and host recovery operations.

Data protection best practices include a 3-2-1 data protection strategy. Organizations should have three copies of their data, in two different formats, with one copy located at a remote site.

The good news is there has been a **16% reduction in the number of organizations that report that they have no secondary recovery site** to store data copies or host recovery operations. For the remaining 27%, not having a secondary site is risky as multiple types of events, such as an electrical failure, flood, hurricane, or fire can take out an entire location. With no secondary location, recovering applications can take much longer since companies will be required to restore their basic infrastructure before they can even begin to recover data, reinstall software, restore the network, and get the business back up and running.

In 2018, 24% more respondents reported using their own site or a co-location facility as their secondary DR site than in 2016. There was a slight reduction in the number of companies using the cloud. For small enterprises the cloud can offer many advantages compared to creating and managing a full, remote data center. In the cloud compute capacity and storage are not purchased outright but charged-for based on actual usage, potentially saving valuable budget dollars. Superior cloud providers will also offer a recovery Service Level Agreement (SLA) guaranteeing that business applications will be available in a known time period after a disaster is declared.

Do You Have a DR Site?
2016 vs 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

"You're way behind the ball if you're just starting now. Get started yesterday and don't stop until all of your clients are protected with offsite Disaster Recovery"

VP IT, US Financial Services Company

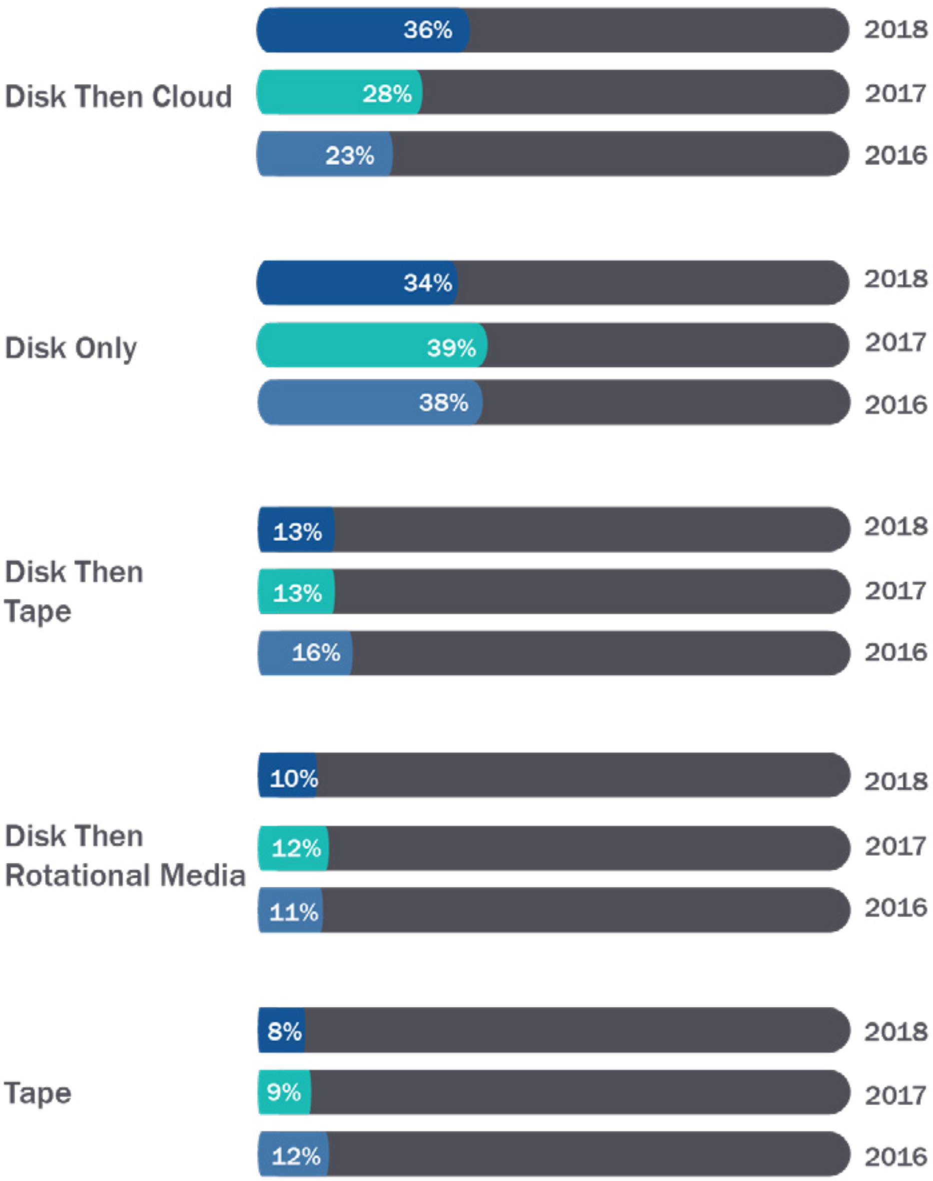
FINDING #5 – CLOUD'S ROLE IN BACKUP IS GROWING

We saw a big jump in the number of organizations using cloud to house copies of their backups.

The role of physical media (tape, removable disks, or optical media) is continuing to decline. Physical media can be very expensive, especially if you include the time and effort of transporting the media off site and the cost of physical storage.

Cloud is replacing physical as the backup media of choice. More organizations report storing backups in the cloud (36%) than using physical media (disk to tape, removable, tape) combined (31%). The cost of cloud storage has declined over the last few years and organizations are taking advantage of it to make cloud the most widely used long term retention option in 2018.

What Primary Method of Backup Do You Use?
2016, 2017, 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

"Find a reputable company with a proven track record to provide the best cloud backup and recovery solution."

Manager IT,
Mid-sized US
Bank

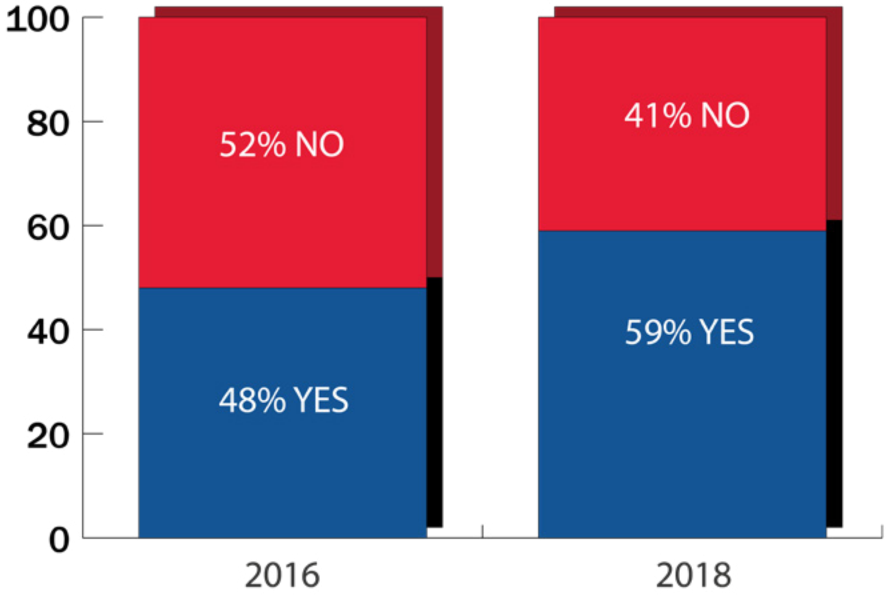
SECTION 2 – THE GROWING ACCEPTANCE OF CLOUD

FINDING #6 – GREATER ROLE FOR CLOUD IN DATA PROTECTION

Now a majority of companies use the cloud for some form of disaster recovery.

Every year, the survey respondents were asked if they are currently using the cloud for data backup, archiving or disaster recovery. The percentage of organizations responding that they do use the cloud has risen each year. Now a majority of respondents trust the cloud enough to use it for data protection and business continuity. That **22% more companies use the cloud for DR /BC in just three years** is a strong vote of confidence in a relatively new technology.

Are You Using Cloud for Backup, Archive, or Recovery?
2016 vs 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

> “I would strongly recommend cloud backup vs tape backup.”

IT Manager, Mid-sized Technology Services Company

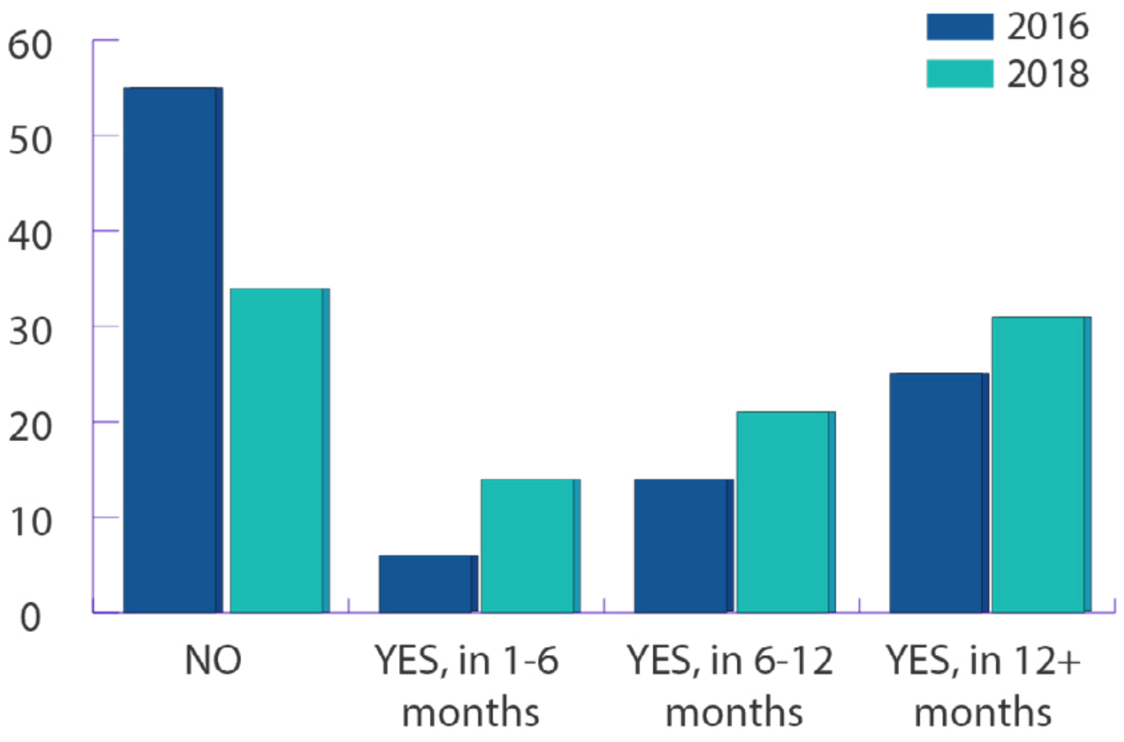
FINDING #7 – GROWING CLOUD ACCEPTANCE EXTENDS EVEN TO NON-USERS

More of those who are not currently using cloud today plan to do so much sooner than in the past.

The survey was constructed so that respondents who are not currently using the cloud were then routed to a series of questions on their plans for future cloud use. 34% of all survey respondents reported that their company was not using the cloud as of early 2018. Of those not using cloud, 34% reported they have no plans to use cloud in the future. One third not using cloud currently planned to add cloud within a year and the final third reported they planned to add cloud longer than a year from now.

These percentages are very different than those from 2016. In 2016, IT admins showed a stronger reluctance to adding cloud **55% of them having no plans to do so. In 2018, more survey respondents plan to add cloud to their IT mix,** and to do it sooner rather than later. The reasons for this change in attitude is highlighted in their response to the next question.

Are You Planning To Adopt Cloud?
2016 vs 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

> "Don't wait, I wish I had started using the cloud sooner."
>
> IT Admin,
> Mid-sized US
> Retail Company

FINDING #8 – RESISTANCE TO CLOUD HAS SETTLED AROUND COST

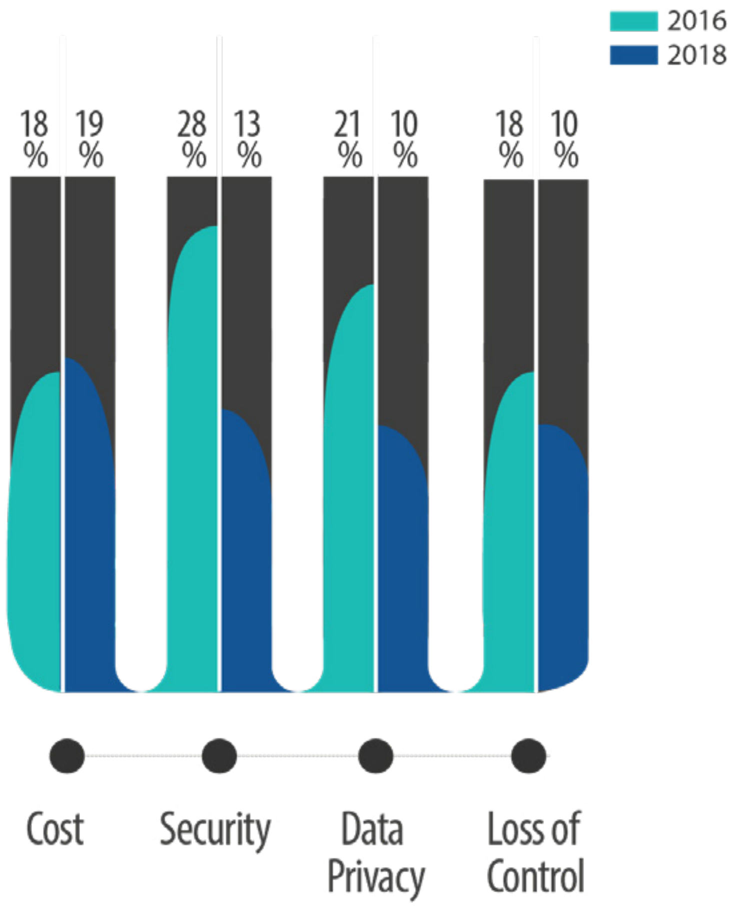
Technical concerns, once dominant, have diminished.

The survey requested respondents to identify their reasons for not using the cloud, with the question being designed as “select all that apply” so responses will not total 100%. While the top 4 answers were consistent with 2016, the response rates varied dramatically.

In 2016, there was strong distrust that the cloud functionally could perform as marketed. 28% of 2016 respondents felt the cloud was not secure, 21% thought their data would not be private and 18% thought they could lose control of their data. The issue of cost was tied with loss of data control for third or fourth.

There seems to have been a major shift in the acceptance of the cloud’s capabilities. Today, cost is the most frequently cited reason for not using the cloud with functional concerns dropping dramatically from 2016 levels. Perhaps with the absence of major cloud failures and hearing cloud success stories from their IT counterparts trust for the cloud seems to have risen substantially among even non-users.

Why Don’t You Use Cloud Today?
2016 vs 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

> “Cloud adoptions is now much easier than ever before, and they are indeed affordable.”
>
> IT Manager, Large Technology Provider

WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

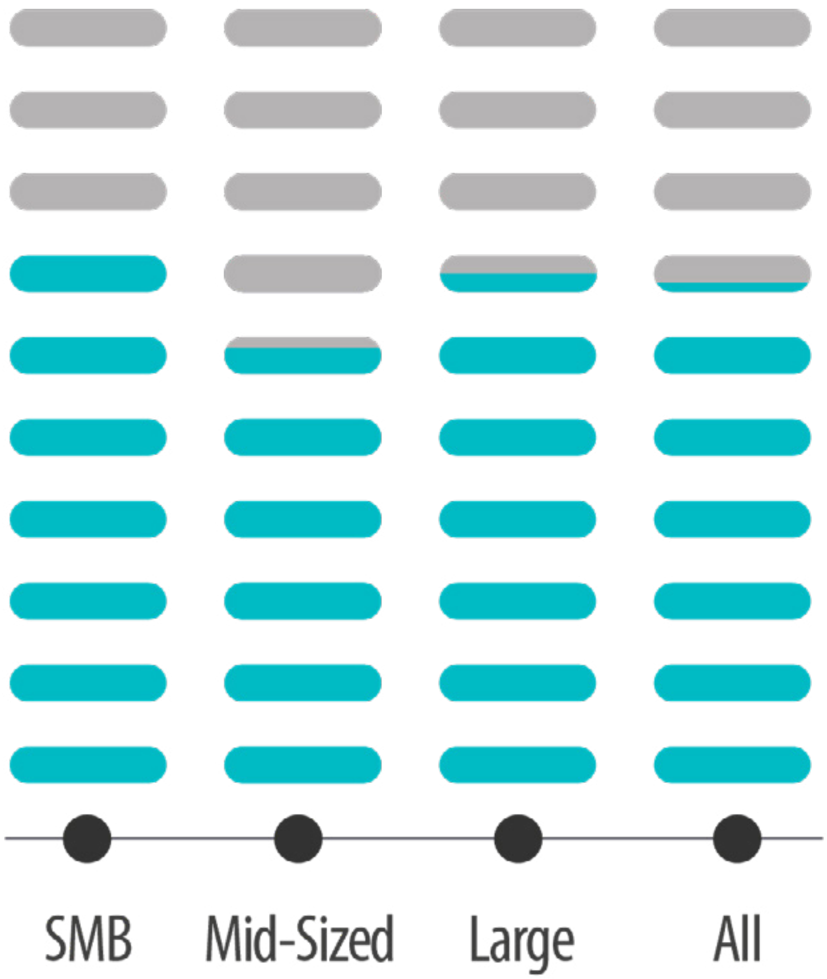
“Plan, Plan, Plan! You will fail without a comprehensive adoption plan.”

IT Manager, Large Medical Provider in the US

FINDING #9 – MID-SIZED COMPANIES LAG IN CLOUD ADOPTION

Cloud adoption rates are not equal across companies of different sizes. 70% of small enterprises (1-50 employees), 57% of mid-sized corporations (51 – 1000 employees), and 65% of large enterprises (1001+ employees) reported using the cloud for DR/BC. **Mid-sized corporate adoption of the cloud is 12% to 18% lower than smaller and larger organizations.** Mid-sized organizations are large enough to have a secondary location to host data protections but, unlike large enterprises, may not have the IT resources and technical knowledge to use the cloud. Still a majority of mid-sized organizations report using the cloud, so financial and operational advantages can be gained by enterprises of all sizes.

Are You Using Cloud for Backup, Archive, or Recovery?
Split by Company Size 2018

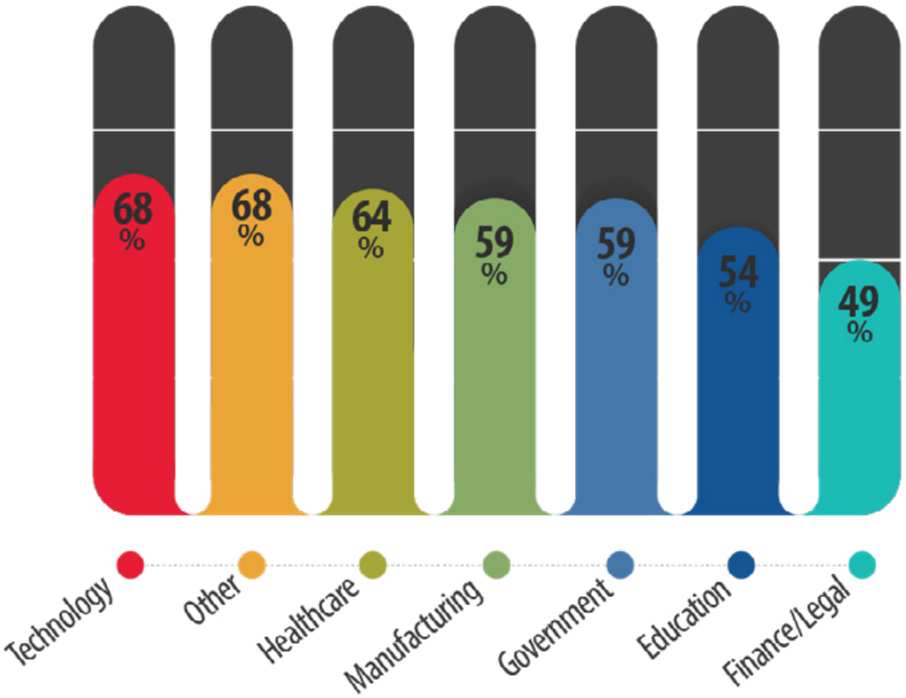


FINDING #10 – CLOUD USAGE VARIES GREATLY BY INDUSTRY

In 2018 it is not a surprise that **technology companies lead cloud adoption with 68% of respondents reporting that they use the cloud for DR / BC purposes**. “Other” industries (retail, construction, engineering, services, wholesale, utilities, etc.) also have a high rate of adoption. Finance / Legal have the lowest cloud usage as the industry deals with highly proprietary data and is often conservative in adopting new technologies, especially one where they seem to lose control and potentially increase the exposure of their very private information. Still almost half of all finance, insurance and legal organizations reported using the cloud.

Interestingly, while healthcare data is also proprietary and sensitive, this industry leads the list of cloud adopters, perhaps as a result of HIPAA and ARRA incentives.

Are You Using Cloud for Backup, Archive, or Recovery?
By Industry 2018



WHAT ADVICE WOULD YOU GIVE TO SOMEONE JUST STARTING TO USE THE CLOUD FOR BACKUP AND RECOVERY?

> “Do your research to find the cloud that fits your needs best.”

CTO, Large Medical Provider in the US

CONCLUSIONS

Your business is at a greater risk of an outage than ever before. As the volumes of data requiring protection increase and the complexity of data centers grow, the chances of a fast recovery diminish unless you are prepared, equipped, and trained in recovery. This includes following industry best practices of establishing recovery goals, conducting regular backups, replicating data to remote locations, and regularly testing backup procedures. The Unitrends 2018 Cloud Survey shows that a larger percentage of enterprises are following best DR practices, including trusting the cloud.

The survey also shows that leaders in disaster recovery are using the cloud as a cost effective and efficient tool in their data protection and business continuity program. They are trusting the cloud more often to help them meet their RTO and RPO objectives. If the responses of your peers leads you to want to learn more about the role cloud can play in data protection and disaster recovery then consider reading the Unitrends Backup and DRaaS Buyers Guide.

BACKUP & DRaaS BUYER GUIDE