THE STATE OF IT RECOVERY FOR SMBS: A SURVEY OF IT PROFESSIONALS

Dimensional Research | October 2014

Introduction

Unscheduled downtime can have dramatic impacts on business results. Outages are detrimental to any business, regardless of its size. With increasingly complex and critical IT environments, SMBs are seeking ways to implement reliable backup and recovery solutions to protect their businesses. The cloud has emerged as a desirable alternative to traditional backup and disaster recovery. This survey investigates the current state of backup and disaster recovery with SMBs, with a focus on evaluating the impact of cloud backup solutions.

The following report, sponsored by Axcient, is based on a survey of 453 IT professionals conducted in the United States and Canada. All participants worked at companies with between 50 and 1000 employees. The goal of the survey was to capture data on current trends and experiences with IT backup and recovery among SMBs.
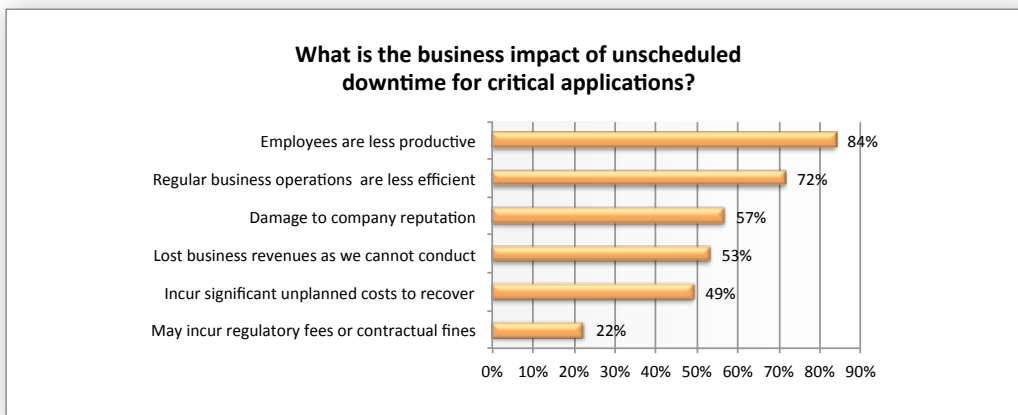
Key Findings

- **Backup is critical, but incomplete for most SMBs**
  - Unscheduled downtime has significant business implications
  - 71% back up both data and applications
  - Only 24% back up all data and all applications
  - Only 27% of small companies back up all applications compared to 48% of mid-sized companies
  - Only 43% back up laptops and desktops
- **Disasters do happen, and IT is held responsible for recovery failures**
  - 79% have had a major IT failure in the past two years
  - Only 8% could recover from a major IT failure within a hour
  - Only 7% were very confident that they could recover operations within 2 hours
  - 96% say IT staff can be held personally responsible for recovery problems
  - 69% report mid-level IT staff would be held responsible if there were a major recovery problem
  - Only 14% of IT executives would blame admins for lost data, but 57% of admins think they would be held responsible
  - 51% say someone could lose their job if critical data could not be recovered
- **Fragmented backup tools cause significant problems**
  - 90% of SMBs have multiple backup and recovery tools
  - 61% have backup and recovery tools with duplicate functionality
  - 91% report using multiple backup and recovery tools creates challenges
  - 71% report using multiple backup and recovery tools can increase risk
- **Cloud recovery very desirable, although adoption is early**
  - 38% use cloud-based backup and recovery
  - 89% see value in cloud-based disaster recovery
  - Cloud backup and recovery users recover faster from failures than those with traditional solutions
  - 79% of those with a non-cloud secondary disaster recovery site would make a change if they had resources

dimensional research

Sponsored by AXCIENT™

Dimensional Research | October 2014
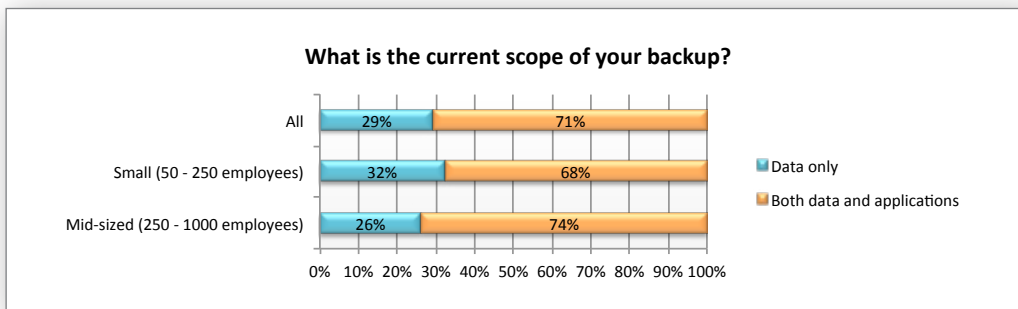
Detailed Findings

Unscheduled downtime has significant business implications for SMBs

IT professionals were asked about the business impact of unscheduled downtime for critical applications. Most reported that unscheduled downtime has significant business implications. The most cited implication (84%) was employee productivity, followed by less efficient business operations (72%) and damage to the company's reputation (57%). More than half (53%) reported that business revenues would be lost during the unscheduled downtime and almost half (49%) said they would incur unplanned costs to recover systems.

What is the business impact of unscheduled downtime for critical applications?

Employees are less productive	84%
Regular business operations are less efficient	72%
Damage to company reputation	57%
Lost business revenues as we cannot conduct	53%
Incur significant unplanned costs to recover	49%
May incur regulatory fees or contractual fines	22%

Applications matter: SMBs are backing up more than just data

SMBs report that the scope of their backup is more than just data. The number of companies who back up both data and applications is 71% as opposed to 29% who only back up data. Medium-sized companies were most likely to back up both data and applications (74%) than smaller companies (68%),
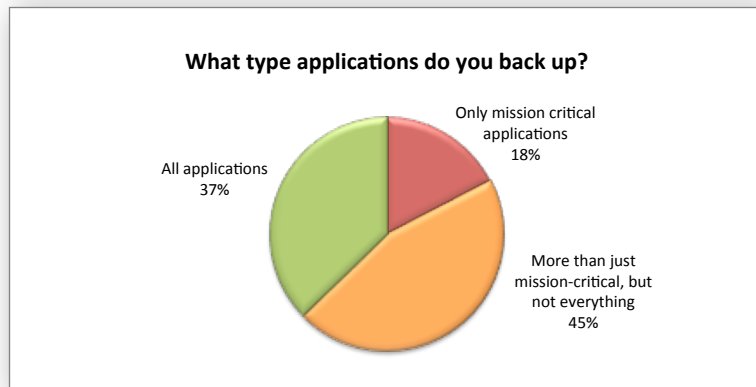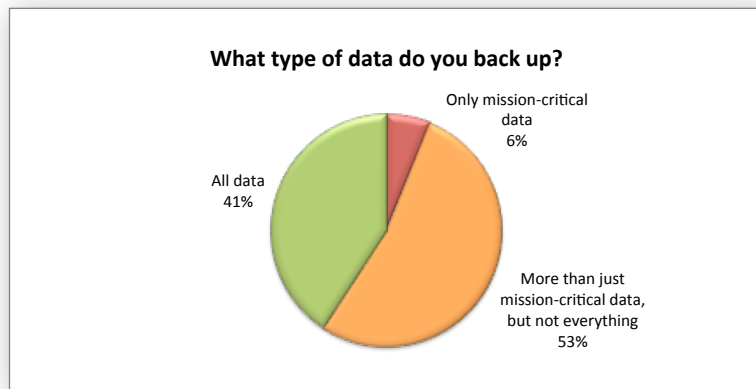
What is the current scope of your backup?

	Data only	Both data and applications
All	29%	71%
Small (50 - 250 employees)	32%	68%
Mid-sized (250 - 1000 employees)	26%	74%

Backup has moved beyond only the most mission-critical data and applications, but significant gaps remain

SMBs are backing up more than just mission-critical data and applications, but few are doing a complete backup of all data and applications. Data backup is more advanced with 41% of IT professionals reporting that they back up all of their data, and only 6% backing up only mission-critical data. On the applications side, the backup situation is not as good. Only 37% back up all applications, 18% back up only their mission-critical applications and 45% back up their mission-critical applications but not all of their applications. Overall, only 24% back up all of their data and all of their applications.

What type of data do you back up?

- Only mission-critical data — 6%
- All data — 41%
- More than just mission-critical data, but not everything — 53%

What type applications do you back up?

- Only mission critical applications — 18%
- All applications — 37%
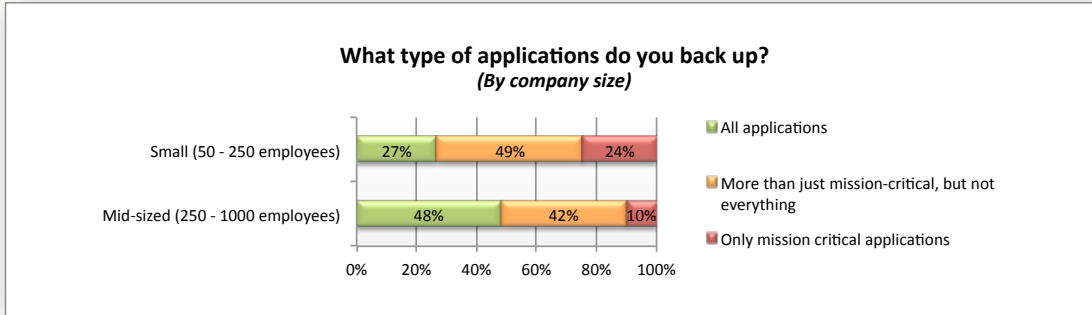- More than just mission-critical, but not everything — 45%

The smaller the company, the more likely they were to only back up mission-critical applications. The study found that small companies backed up only their mission-critical applications (24%) as opposed to medium-size companies (250 to 1,000 employees) of whom only 10% said they only backed up mission-critical applications. Conversely, 48% of medium-sized companies said they backed up all of their applications as opposed to just 27% of small-sized companies.

What type of applications do you back up?
(By company size)

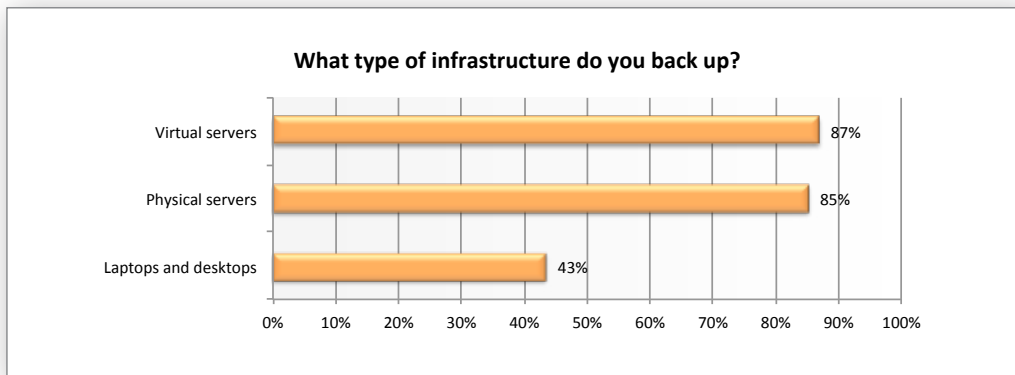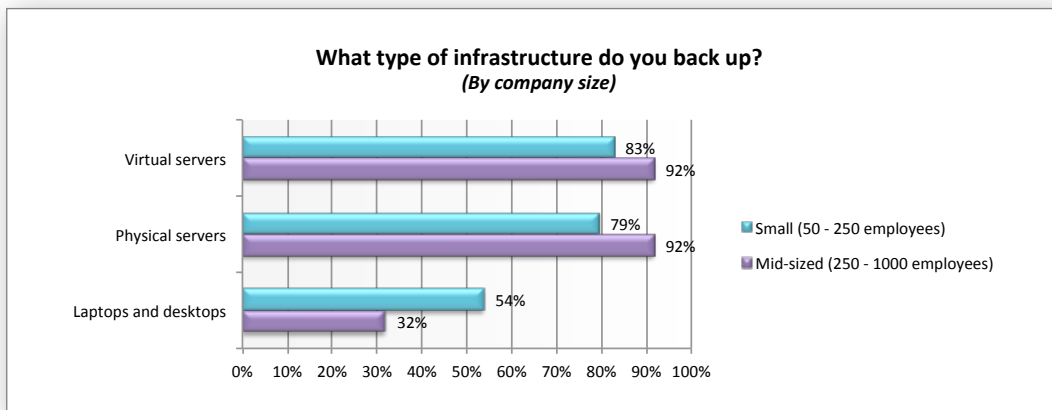|	All applications	More than just mission-critical, but not everything	Only mission critical applications
Small (50 - 250 employees)	27%	49%	24%
Mid-sized (250 - 1000 employees)	48%	42%	10%

Server backup much more common than desktop backup

SMB IT organizations reported significant differences in backup of different types of infrastructure. While the majority back up their servers – both physical (85%) and virtual (87%), less than half back up their end user's desktops and laptops.

What type of infrastructure do you back up?

Virtual servers	87%
Physical servers	85%
Laptops and desktops	43%

This pattern of backing up servers more often than desktops was true of both sized companies evaluated in the survey. Interestingly, while small companies were behind in backup of their physical and virtual servers, they were actually ahead of mid-sized companies in desktop backup.

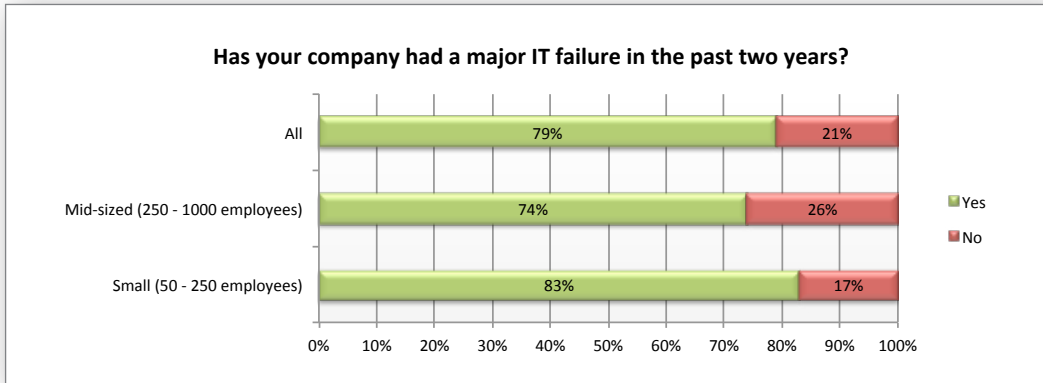**What type of infrastructure do you back up?**
(By company size)

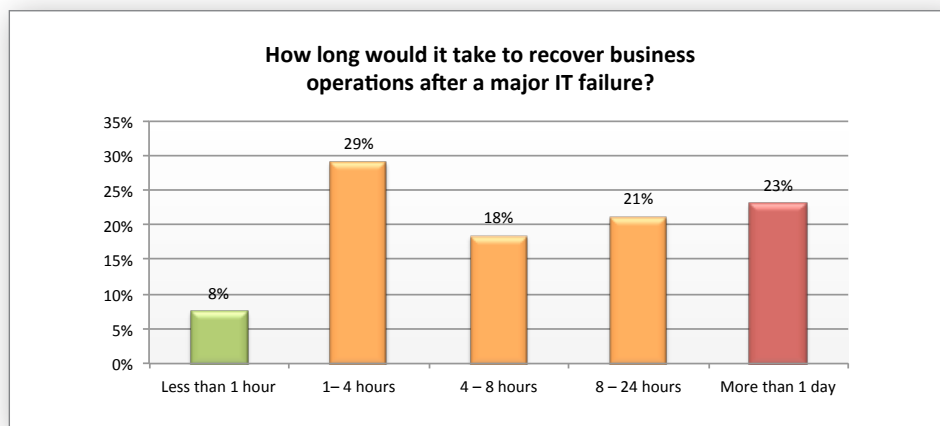|	Small (50 - 250 employees)	Mid-sized (250 - 1000 employees)
Virtual servers	83%	92%
Physical servers	79%	92%
Laptops and desktops	54%	32%

Major IT failures are a fact of life for SMBs; especially small companies

Major IT failures are a harsh reality for SMBs with 79% reporting they'd had a major IT failure in the past two years. The number was even higher for small companies of whom 83% reported a major failure as opposed to 74% of medium-size companies.

Has your company had a major IT failure in the past two years?

	Yes	No
All	79%	21%
Mid-sized (250 - 1000 employees)	74%	26%
Small (50 - 250 employees)	83%	17%

Very few SMBs could recover from a major IT failure within an hour

IT professionals were asked how long it would take for them to fully recover business operations after a major IT failure. The widely varying range of answers provided reflected the varying approaches to backup and recovery among these companies. Very few, 8%, could recover in under one hour, while almost a quarter (23%) said it would take more than one day to fully recover from a major it failure.
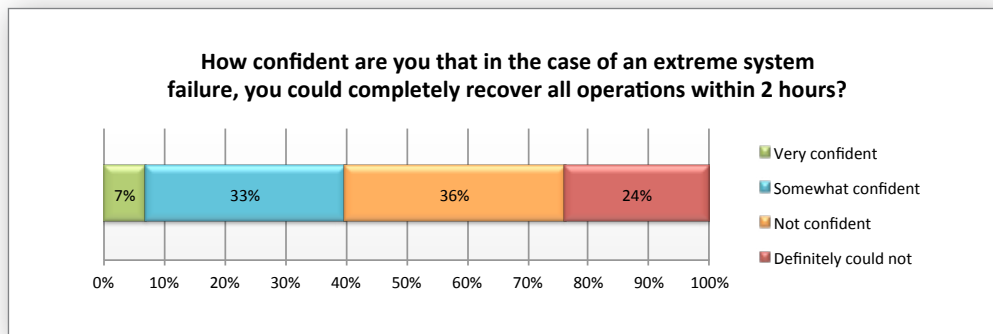
How long would it take to recover business operations after a major IT failure?

Less than 1 hour	1– 4 hours	4 – 8 hours	8 – 24 hours	More than 1 day
8%	29%	18%	21%	23%

Little confidence among SMBs that they could recover operations quickly

IT professionals lack confidence that operations could be recovered quickly after an extreme system failure. When asked about how confident they were in their recovery abilities, only 7% were very confident that they could recover all operations within two hours after a significant system failure. A full 60% were not at all confident in their ability to recover within two hours.

How confident are you that in the case of an extreme system failure, you could completely recover all operations within 2 hours?

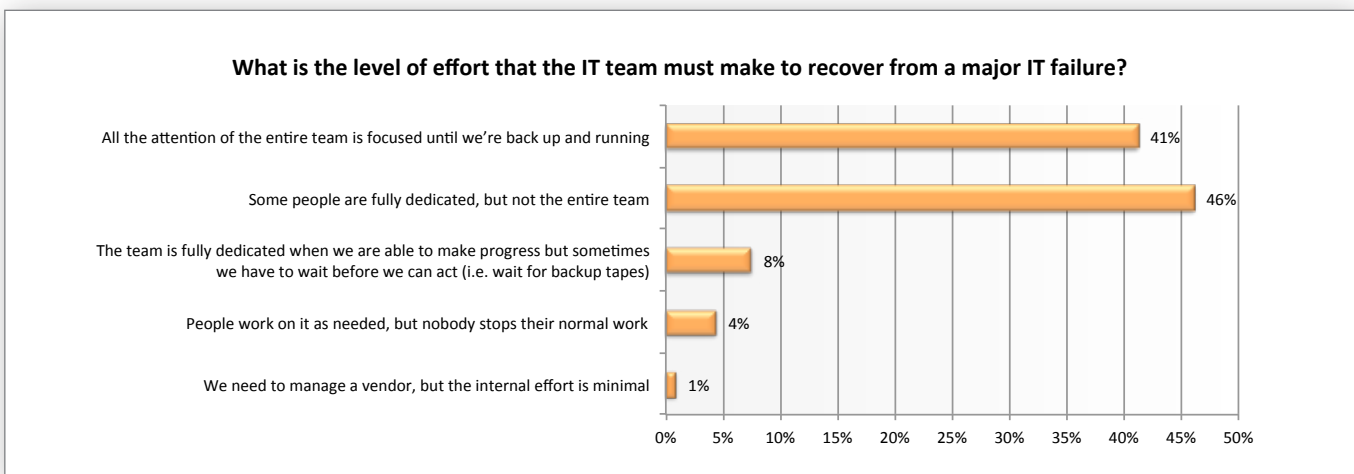|	
Very confident	7%
Somewhat confident	33%
Not confident	36%
Definitely could not	24%

Recovery very disruptive to the IT team

IT teams at small and medium-sized companies are very impacted by major IT failures. Recovery is very disruptive to the IT team. Most participants report that IT staff time is fully dedicated to recovery until things are resolved including 41% who report that all of the attention of the entire team is focused on recovery until they're vup and running and 46% report that some team members are fully dedicated, although not the entire team.

Mid-level IT staff held responsible for lost data

When it comes to blame if a problem caused critical data to be lost after a system disaster, the majority of individuals (69%) reported that mid-level IT staff such as IT directors or other IT team managers would be held responsible for lost data. Mid-level IT staff were considered to be held responsible much more than the CIO or other IT executives (41%) or admins and other front-line IT staff (33%).

What is the level of effort that the IT team must make to recover from a major IT failure?

All the attention of the entire team is focused until we're back up and running	41%
Some people are fully dedicated, but not the entire team	46%
The team is fully dedicated when we are able to make progress but sometimes we have to wait before we can act (i.e. wait for backup tapes)	8%
People work on it as needed, but nobody stops their normal work	4%
We need to manage a vendor, but the internal effort is minimal	1%

Mid-level IT most likely to be held responsible for problems with recovery

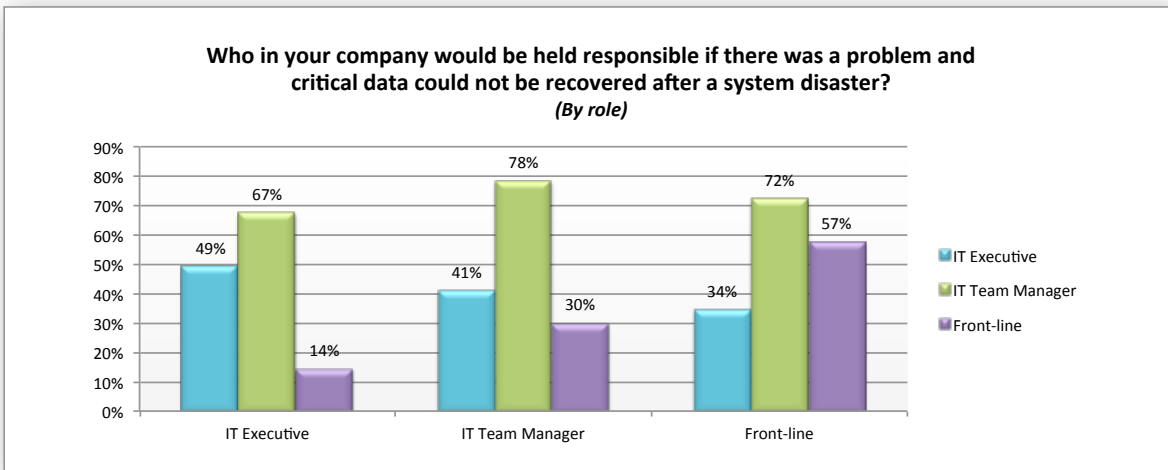IT professionals can be personally held responsible for problems with disaster recovery, and most of the responsibility lies with mid-level IT staff. The vast majority of IT professionals, 96%, said that someone in their company would be responsible if data could not be recovered. Most participants, 69%, indicated IT directors or other IT team managers would be the ones held responsible, more than IT executives (41%) or frontline staff (33%).

Who in your company would be held responsible if there was a problem and critical data could not be recovered after a system disaster?

CIO or other IT executive	41%
IT director or other IT team manager	69%
Admins or other front-line IT staff	33%
Consultant or vendor	11%
Non-IT executive	11%
No one in our company has individual responsibility if there is a problem with recovery	4%

Interestingly, different levels of the organization had different opinions about who would be held responsible for lost data. All three levels of IT professionals – executives, mid-level, and front-line - consistently put the bulk of responsibility on the mid-level managers, including mid-level managers themselves. However, when comparing IT executives' and front-line staff such as system admins, more than half of admins (57%) believed they would be held responsible, while very few executives (14%) would blame their admins.
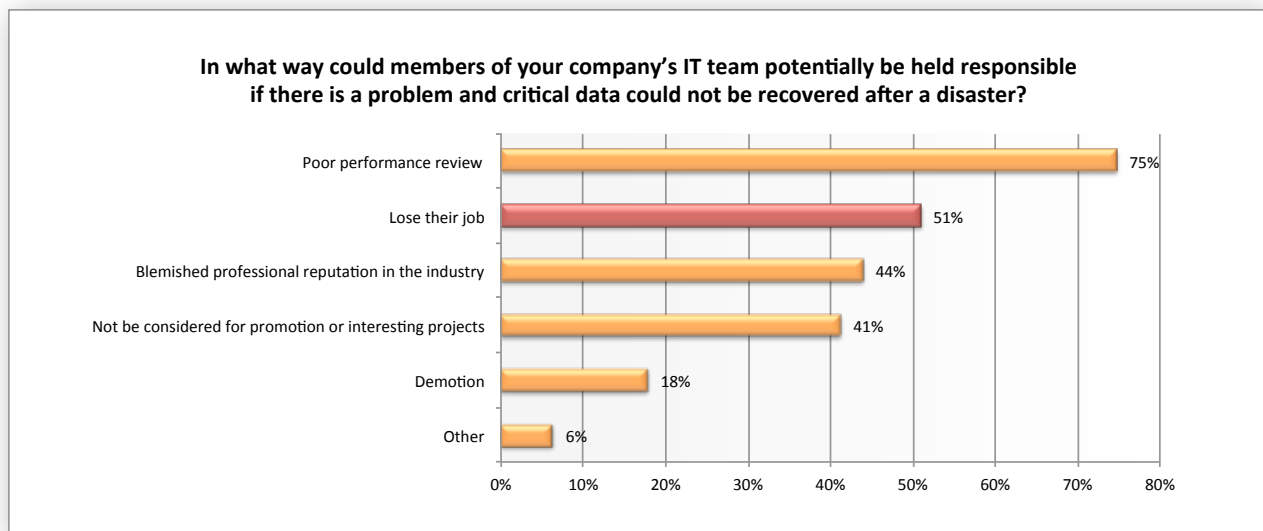
Who in your company would be held responsible if there was a problem and critical data could not be recovered after a system disaster?
(By role)

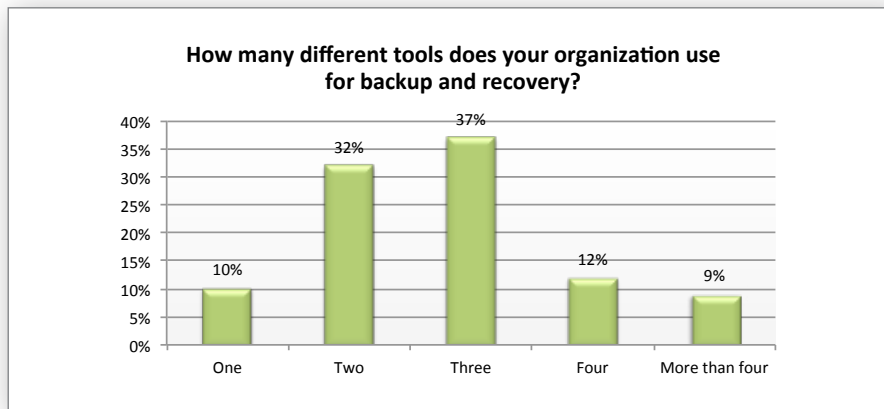|	IT Executive	IT Team Manager	Front-line
IT Executive	49%	67%	14%
IT Team Manager	41%	78%	30%
Front-line	34%	72%	57%

Half say someone could lose their job if data were lost

IT professionals believe the stakes are high for team members if critical data could not be recovered after a disaster. Some of the ways IT team members could be held responsible if there was a problem and data was lost included a poor performance review (75%), a blemished professional reputation in the industry (44%), lost opportunities for a promotion (41%), demotion and more. Slightly more than half (51%) believed someone could lose their job if data was lost after a disaster. "Other" answers include required training, writing action plan for future, and public humiliation.

In what way could members of your company's IT team potentially be held responsible if there is a problem and critical data could not be recovered after a disaster?

Poor performance review	75%
Lose their job	51%
Blemished professional reputation in the industry	44%
Not be considered for promotion or interesting projects	41%
Demotion	18%
Other	6%

Most SMBs have multiple backup and recovery tools that duplicate functionality

Backup and recovery is an area in IT that is tool-heavy. When asked about the number of solutions used for backup, 90% of SMBs report that they have more than one backup and recovery tool in place. This includes products for backup, replication, deduplication, and recovery.
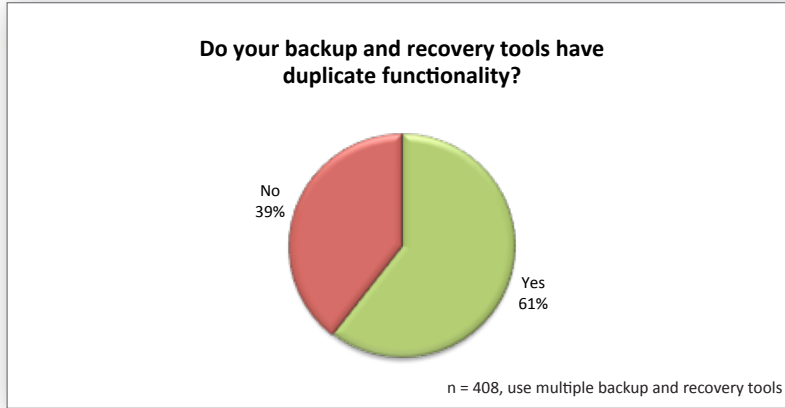
How many different tools does your organization use for backup and recovery?

One	Two	Three	Four	More than four
10%	32%	37%	12%	9%

Among IT organizations that have multiple tools, most of them (61%) say those tools provide duplicate functionality.

**Do your backup and recovery tools have duplicate functionality?**

No
39%

Yes
61%

n = 408, use multiple backup and recovery tools
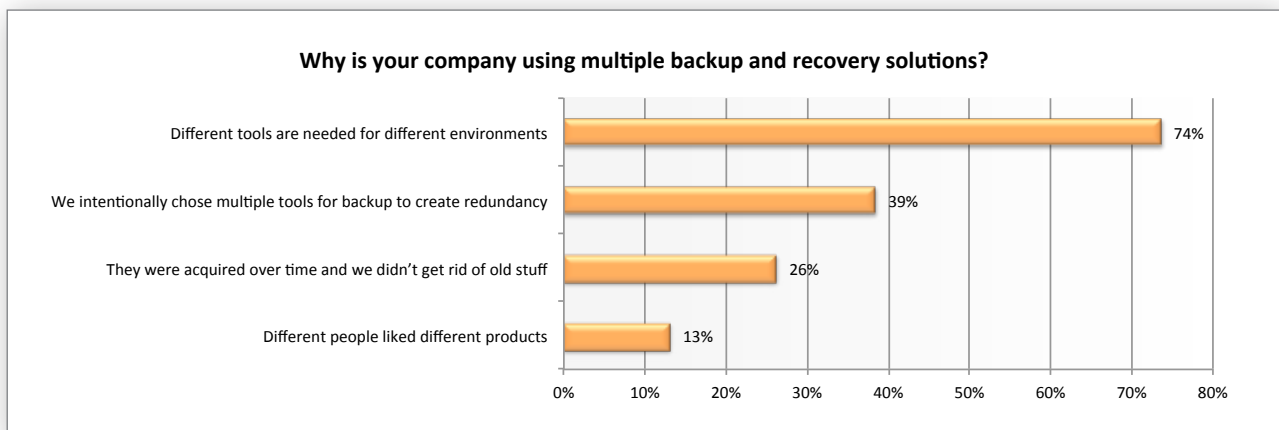
One example of backup and recovery tools with duplicate functionality can be seen in the types of tools SMBs use to back up physical and virtual servers. More than half (54%) reported they use different tools to back up physical verses virtual servers while 46% reported they used the same tools for both.

Does your company have different tools for backup of physical and virtual servers?

Different
54%

Same
46%

n=408, use multiple backup and recovery tools
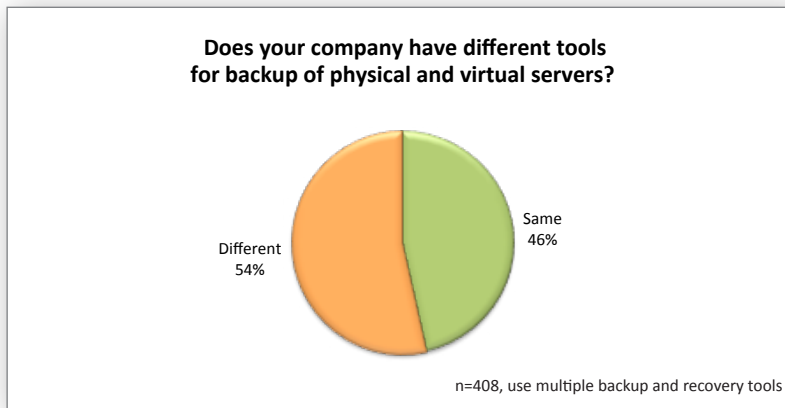
IT professionals reported a wide range of reasons for these different tools with overlapping functionality. The most frequent answer give is that different tools are needed for different environments (74%).
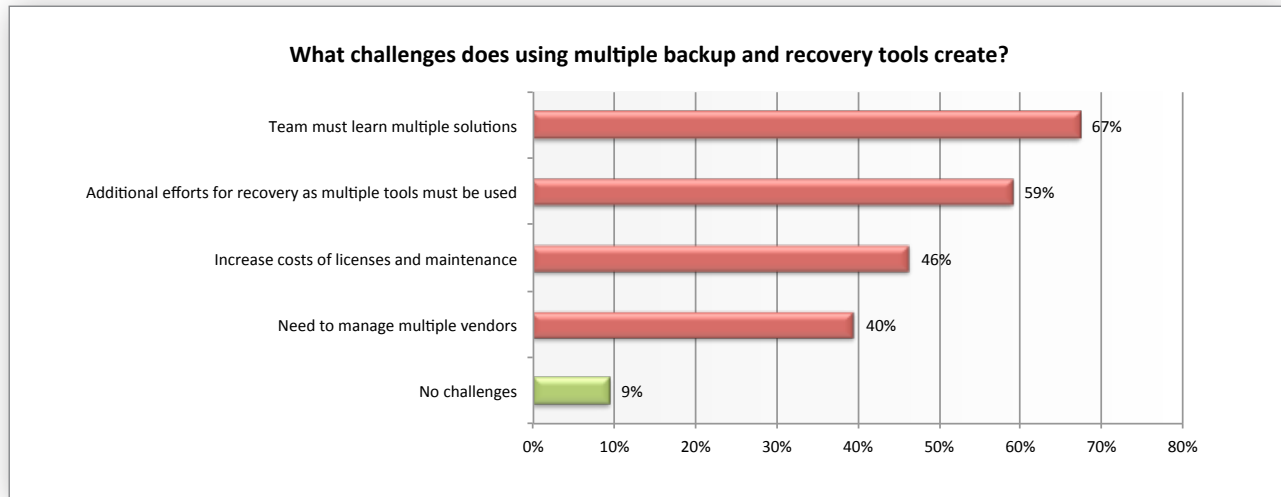
Why is your company using multiple backup and recovery solutions?

Different tools are needed for different environments	74%
We intentionally chose multiple tools for backup to create redundancy	39%
They were acquired over time and we didn't get rid of old stuff	26%
Different people liked different products	13%

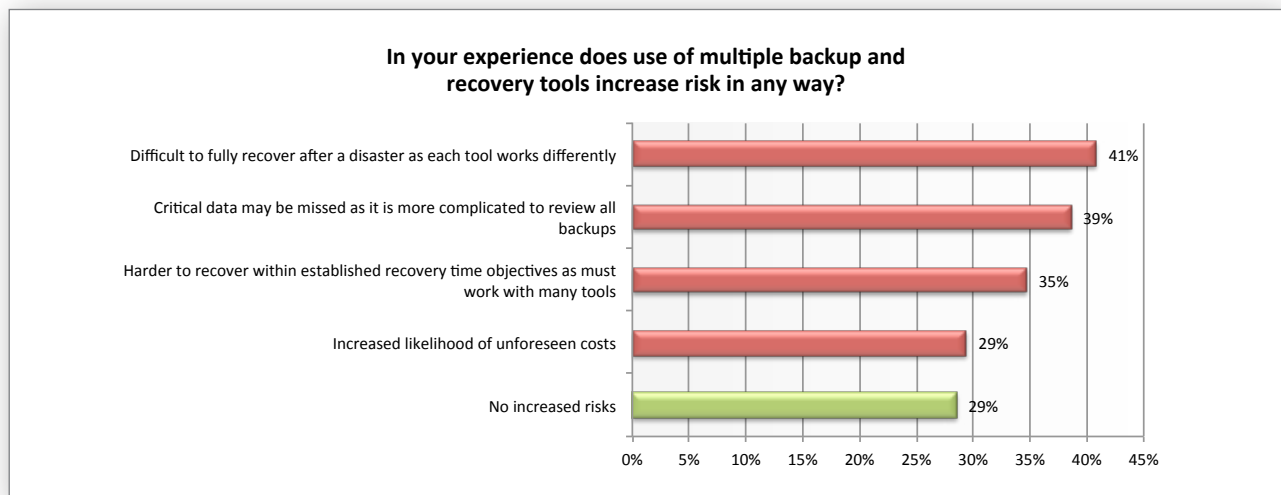0%   10%   20%   30%   40%   50%   60%   70%   80%

Use of multiple backup and recovery tools creates many challenges

While SMBs reported that different tools are needed for backup and recovery, 91% report that using multiple tools creates challenges. The most frequent challenge cited (67%) was that teams would have to learn multiple solutions. In addition to learning multiple solutions, 59% reported that additional efforts would be required for recovery when multiple solutions were used. Another challenge reported was the increased cost of licenses and maintenance (46%) when multiple backup and recovery tools were in place and 40% named the challenge of managing multiple vendors.

What challenges does using multiple backup and recovery tools create?

Team must learn multiple solutions	67%
Additional efforts for recovery as multiple tools must be used	59%
Increase costs of licenses and maintenance	46%
Need to manage multiple vendors	40%
No challenges	9%

0% 10% 20% 30% 40% 50% 60% 70% 80%

Multiple backup tools can increase risk

Some companies intentionally choose to use multiple tools for backup and recovery because they believe it reduces risk. However the majority of IT professionals, 71%, report using multiple backup and recovery tools may also increase risk. The ways using multiple backup tools can increase risk include: difficulty to fully recover after a disaster because each tool works differently (41%), critical data may be missed because it is more complicated to review all backups (39%), it's more difficult to recover within established recovery time objectives because they must work with many tools (35%) and there is increased likelihood of unforeseen costs (29%).

In your experience does use of multiple backup and recovery tools increase risk in any way?

Difficult to fully recover after a disaster as each tool works differently	41%
Critical data may be missed as it is more complicated to review all backups	39%
Harder to recover within established recovery time objectives as must work with many tools	35%
Increased likelihood of unforeseen costs	29%
No increased risks	29%

0% 5% 10% 15% 20% 25% 30% 35% 40% 45%

More than one-third of SMBs use cloud-based backup and recovery, mostly for data
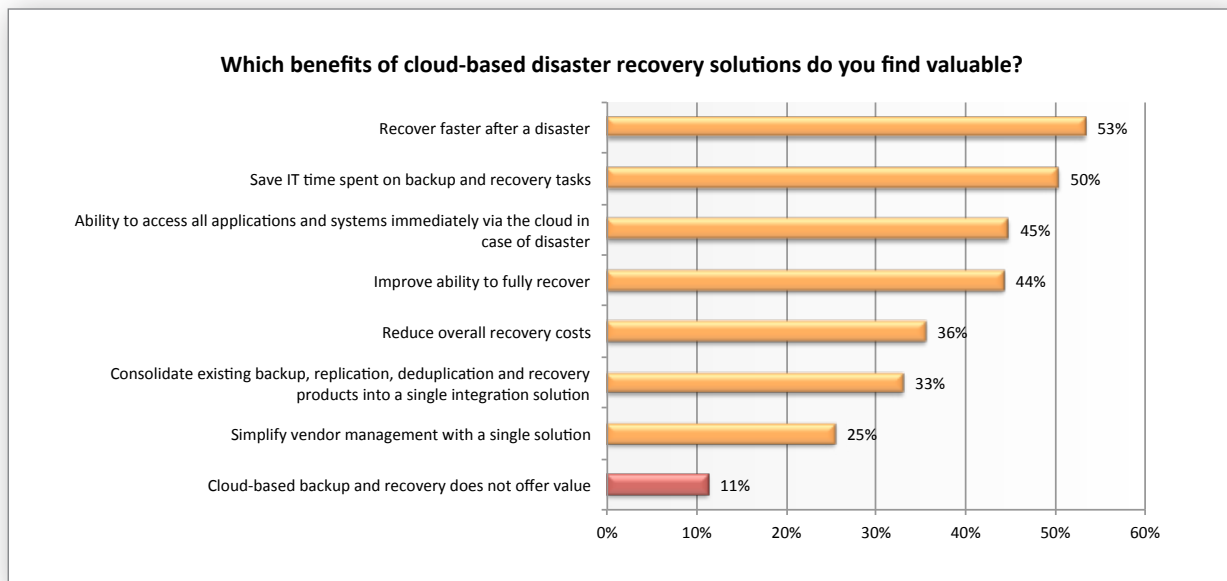
The use of cloud-based backup and recovery solutions has emerged as a compelling option for SMBs. Currently, just over one-third of SMB IT organizations (38%) are using cloud-based backup and recovery. Of these, most are using cloud backup for data, with only a few (14%) using cloud-based recovery solutions for their applications.

Does your company use any cloud-based backup and recovery solutions?

- Yes – data only 24%
- Yes – both data and application 14%
- No 62%
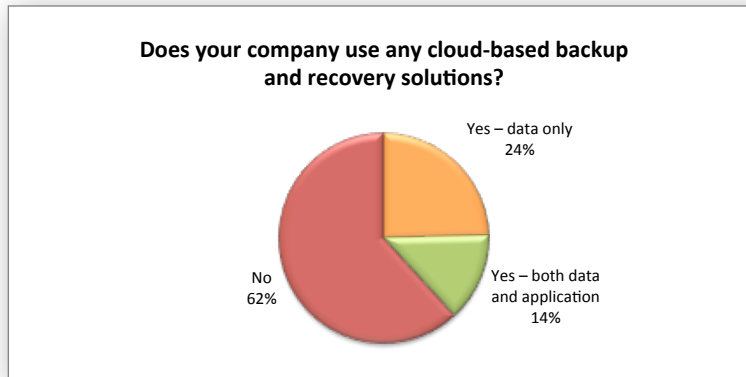
Small companies (44%) are more likely than medium-sized companies (32%) to use cloud-based solutions for backup and recovery of their data and applications.

IT recognizes potential value of cloud-based disaster recovery

The vast majority (89%) of SMBs see value in cloud-based disaster recovery. The top benefits they report include: faster recovery after a disaster (53%), saving IT time spent on backup and recovery tasks (50%), ability to access all applications and data immediately via the cloud in the event of disaster (45%), improve ability to fully recover (44%) and reduce overall recovery costs (36%). Additional benefits cited were consolidating existing backup, replication, deduplication and recovery products into a single integrated solution (33%) and simplifying vendor management with a single platform (25%).
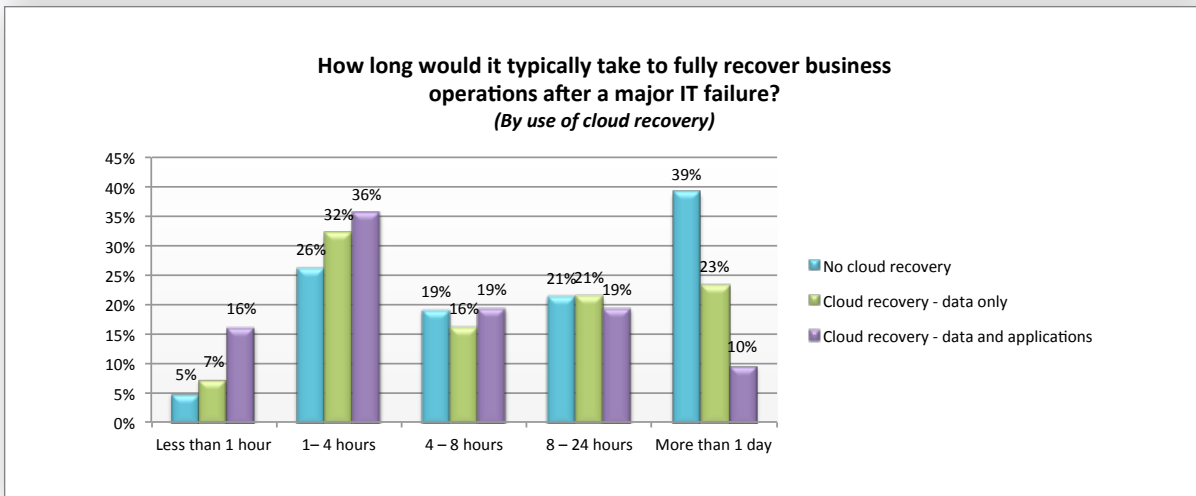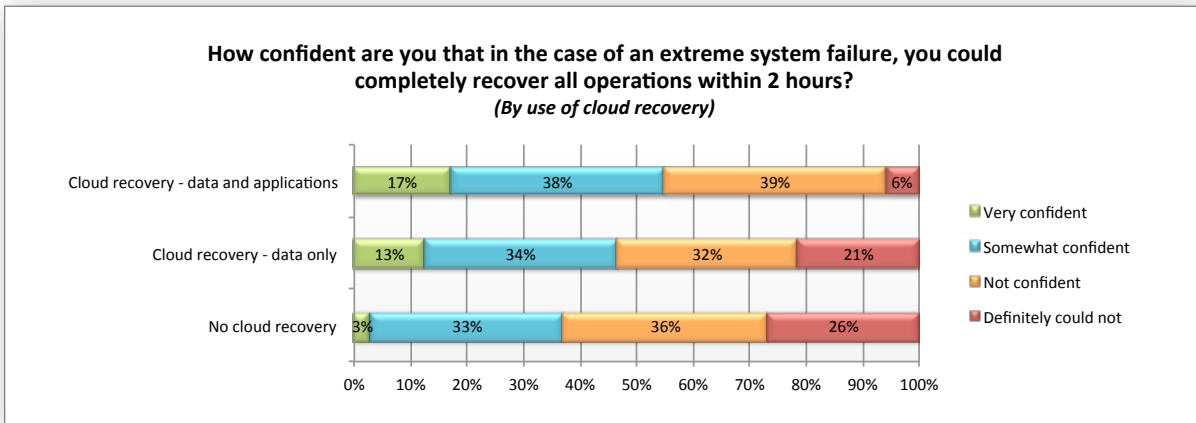
Which benefits of cloud-based disaster recovery solutions do you find valuable?

Benefit	Percentage
Recover faster after a disaster	53%
Save IT time spent on backup and recovery tasks	50%
Ability to access all applications and systems immediately via the cloud in case of disaster	45%
Improve ability to fully recover	44%
Reduce overall recovery costs	36%
Consolidate existing backup, replication, deduplication and recovery products into a single integration solution	33%
Simplify vendor management with a single solution	25%
Cloud-based backup and recovery does not offer value	11%

Use of cloud recovery speeds recovery time

To compare the results cloud-based recovery to traditional methods, we compared the answers given to questions about recovery time and confidence by IT professionals currently using cloud-based recovery, and those who are using traditional methods. In both cases, cloud-based recovery showed noticeably stronger outcomes, particularly among those who backup both applications and data.

How confident are you that in the case of an extreme system failure, you could completely recover all operations within 2 hours?
(By use of cloud recovery)

How long would it typically take to fully recover business operations after a major IT failure?
*(By use of cloud recovery)*

IT not happy with use of non-cloud secondary disaster recovery sites

Today, the most common approach to disaster recovery is to have a secondary site. The majority of IT organizations, 74%, report that they have a non-cloud based secondary site for disaster recovery. The types of secondary sites used most commonly were a separate branch office or other company-owned location (44%) and colocation at a data center (39%). A few (3%) reported other locations not owned by the company such as a partner's office. The remaining 26% do not currently have a non-cloud secondary site for recovery.

Dimensional Research | October 2014

What type of secondary site does your company use for disaster recovery?

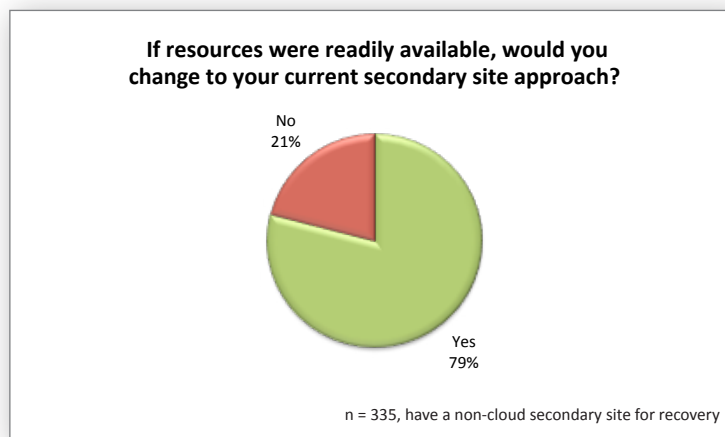|	
Separate branch office or other company-owned location	44%
Colocation at a datacenter	39%
Other	3%
We do not have a secondary site for recovery	26%
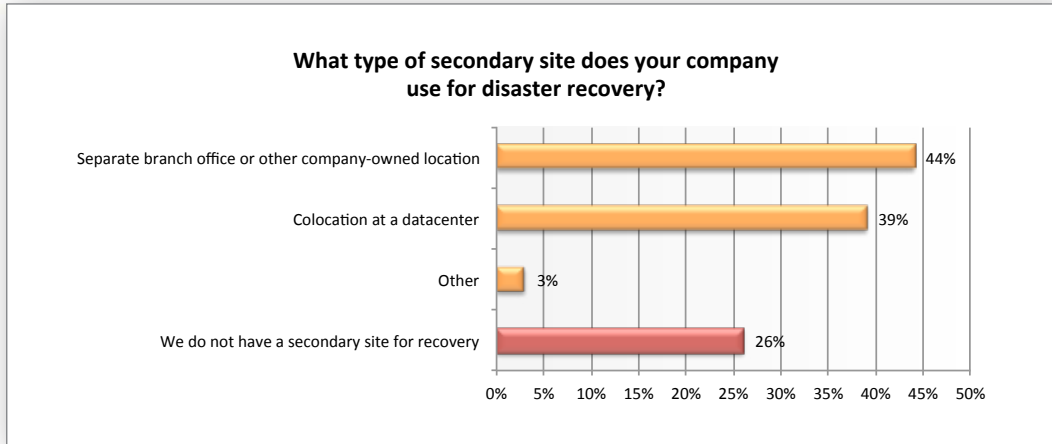
Mid-sized companies were more likely than small companies to use a secondary site for disaster recovery. Just over half of mid-sized companies (51%) said they used a separate branch office or other company-owned location as opposed to just over a third (36%) of small companies. Similarly 40% of mid-sized companies named collation at a datacenter as opposed to 36% of small companies.

However, these IT organizations are not satisfied with their current approach. When asked if they would change their current approach, the majority (79%) said they would make a change to their current secondary site approach if resources were readily available.
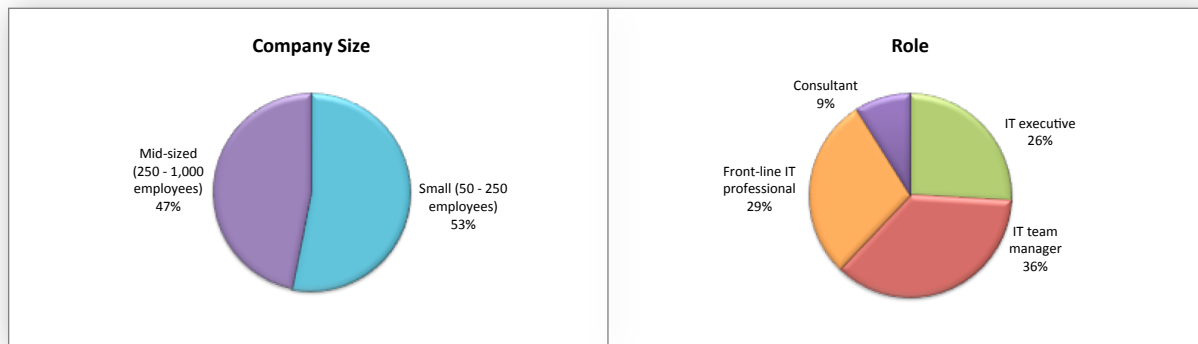
If resources were readily available, would you change to your current secondary site approach?

No
21%

Yes
79%

n = 335, have a non-cloud secondary site for recovery

www.dimensionalresearch.com

Survey Methodology

An independent database of IT professionals was invited to participate in a web survey on the topic of IT backup and recovery for SMBs. A total of 453 respondents across the United States and Canada who worked at companies with between 50 and 1,000 employees completed the survey. Each respondent had responsibility for backup and recovery of data and applications. Participants included IT executives, IT team managers, hands-on IT professionals, and consultants and represented a wide range of industry verticals.

Company Size

Mid-sized (250 - 1,000 employees) 47%

Small (50 - 250 employees) 53%

Role

Consultant 9%

IT executive 26%

Front-line IT professional 29%

IT team manager 36%

About Dimensional Research

Dimensional Research® provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information visit www.dimensionalresearch.com.

About Axcient

Axcient's cloud platform eliminates data loss, keeps applications up and running, and makes sure that IT infrastructures never go down. Designed for today's always-on business, Axcient replaces legacy backup, business continuity, and disaster recovery software and hardware, and reduces the amount of expensive copy data in an organization by as much as 80 percent. By mirroring an entire business in the cloud, Axcient makes it simple to access and restore data from any device, failover IT systems, and virtualize your entire office with a click – all from a single duplicated copy. Trusted by thousands of businesses to store and protect more than 10 billion files and applications, Axcient maximizes productivity, reduces cost, and eliminates risk. The company is headquartered in Mountain View, Calif.