Introduction

In 2016, the enterprise ecosystem continued to evolve. In 2017, organizations will face more disruption and potentially more turmoil.

This past year, businesses of every type experienced challenges and corporate system meltdowns, notably failures at Delta and Southwest Airlines, and the Internal Revenue Service 2016 tax processing. Clearly, these vital systems demand robust recovery plans – and more agile means of restoring operations after an outage. Also dominating the news were security breaches within LinkedIn, Oracle, Wendy’s, ADP, Verizon, and the FDIC. With the rise of cyber criminals and internal data breaches, company security and remediation practices have been called into question. All sectors, from government to retail are vulnerable.

Device madness continued to escalate as mobile devices and applications are connected to back-end enterprise systems. Environments are highly complex, and the sheer amount of user data that’s created drives a need for change in the data center. The Internet of Things massively increases the amount of data – with approximately 21 billion connected endpoints by 2020.¹ With the emphasis on the value of corporate data and its explosive growth, IT professionals will be pressed on issues of storage, protection, and security.

Technology professionals are shaping and tiering the data center and want to make deliberate decisions about what software to move to the Cloud. At the same time, business units maneuver around IT to gain more agile Cloud-based applications, leaving companies vulnerable. But IT has to figure out the best way to inventory and manage these apps, rather than trying to root them out.

So how are IT professionals handling this upheaval? Will they have the resources and budget to modernize the data center? Are they leading or following? Will IT departments stand on the sidelines as users adopt their own applications – unknown to IT? As recovery and security take center stage, how fast does IT have to run to keep up? What will happen to companies that are slow to adapt?

This year’s State of Resilience report presents our survey findings – and looks forward to note trends that are emerging. Please enjoy our report and share it with your colleagues.
Respondent Profile and Methodology
Respondent Profile and Methodology

Four Surveys
• High Availability and Disaster Recovery
• Migration
• Data Sharing
• Cloud

Respondents, Distribution and Profile
In total, 1,598 professionals responded to this year’s survey set. Professional titles varied widely, from CIO, CTO, and VP of Information Technology, to Cloud Architect, Systems Administrator, Senior DBA, and Principal Systems Engineer.

Respondents represented a wide range of countries, among them: Saudi Arabia and the United Arab Emirates in the Middle East; Indonesia, Hong Kong, and Malaysia in Asia Pacific; Colombia and Brazil in Latin America; France, Italy, Belgium, and Romania in Europe; and the U.S. and Canada in North America, to name a few.

In addition, this year’s analysis contains some comparisons of IT practices for High Availability and Disaster Recovery between Windows and IBM i operating systems. We wanted to shed light on the experience of IT professionals using these two operating systems, particularly on the topics of tools, practices, and benchmarks. We believe that our analysis could provide more targeted insight for IT teams responsible for these very different operating system environments. Where appropriate, operating system comparisons are shown in sidebars.

Dates
June 2016 to September 2016

Delivery System
Surveys were administered online, using web-based survey tools and targeted to IT professionals.
Central Issues for Information Technology Leaders

Although the media, C-suite, and industry events are abuzz with talk of data center modernization, not all companies are equally prepared for it. In fact, sometimes it might seem to IT professionals that they’re trying to change a tire on a speeding vehicle. Many are caught in the cycle of using traditional practices, while at the same time being pressured by new trends toward zero-downtime recovery, business intelligence, and real-time data access that require new approaches.

Now is the time for professionals to reexamine their companies’ historic practices to promote business growth, expansion, and profitability. This year’s research revealed the fundamental challenges IT leaders face in doing so, along with the opportunities that await them:

Disaster Recovery Planning, Training Should Take the Lead

This year saw progress, as we found more companies quantifying their business cost of downtime. Yet weaknesses were apparent: Company recovery schemes might not be adequate given the data explosion and out-of-control storage growth. Professional’s confidence in their recovery plans is low. Some companies set very low recovery point objectives, yet they exceeded their maximum tolerance for data loss, a vulnerability that must be addressed.

To avert disaster, the best protection is prevention. Companies will become more resilient by testing their recovery plans frequently and using products that provide built-in testing modules. Businesses must build IT bench strength and technical knowledge. Why? If companies plan to continue using internal staffing resources, rather than turning to trained service providers, they must recognize a need for increased staff training.

Migration Outcomes are Unpredictable

Migration is a high wire act for IT professionals, who are balancing the cost of downtime against business risks of delayed or failed migrations. This year the number of migration failures rose. Moreover, findings showed that the majority of professionals had postponed a migration out of concerns about downtime. Migration can also take a toll on company finances and morale: Nearly 9 out of 10 businesses call upon internal staff to help with migrations, primarily after business hours or on weekends. More agile, nearly continuous uptime solutions for migration can reduce downtime and relieve the stress of overused staff resources.
Business Information is a Goldmine, Ensuring Accuracy is a Challenge

IT professionals are operating in a real-time business world where decisions based on data have consequences. The majority of companies are sharing data for the purpose of business intelligence and competitive advantage. Yet, survey respondents voiced serious concerns about inconsistent data in databases – and its impact on business decision making. Professionals manage a considerable number of database types from different vendors, but they’re also still using entrenched tools for data sharing that have been in existence for at least a generation. Overall, findings show that IT professionals have a tough job keeping data sets current and combining data from disparate sources.

Cloud Benefits are Clear, Uncertainties Still Exist

Survey participants noted that Cloud represents an opportunity for businesses to save on operational costs, boost IT efficiency, and grow or shrink IT resource consumption on demand. Although Cloud is no longer completely a new frontier for these professionals, they are still exploring its borders. Legal and technical issues regarding bandwidth, infrastructure control, security, and compliance are likely to keep IT leaders awake at night. This year most businesses were using Hosted Private Clouds, but findings showed that in planning for the future, their preference shifted to Hybrid Clouds. Companies might be keeping “one foot on the ground, one in the Cloud,” to address legal requirements for data privacy and compliance. Findings also showed that some companies have begun to adopt Cloud-based disaster recovery services, relatively new in the IT landscape.
The State of High Availability and Disaster Recovery
The State of High Availability and Disaster Recovery

This year the topic of disaster recovery and high availability has skyrocketed to the top of the agenda in the executive suite and the data center. Though HA/DR has always been a critical issue, the intense media focus on system meltdowns has helped drive the discussion to a fevered pitch. Companies recognize that disaster recovery systems are an investment in terms of software, implementation, and training. But HA/DR systems aren’t an area where organizations should skimp, because nothing less than business viability is at risk.

For several years, Vision Solutions has fielded a survey to learn more about business data protection schemes, their practices, and their plans for the future. This year, 551 professionals responded to our high availability and disaster recovery survey, providing an overall picture of HA/DR and a specific analysis for Windows and IBM i operating systems.

Data Protection Technologies in Use: Year-over-Year Trends

Data protection technologies beyond basic tape have advanced dramatically over the years, offering convenience and cost-savings through methods such as software replication, Cloud-based recovery, and more. Given the diversity of these technologies, we reviewed the data protection landscape in general to learn exactly which methods companies used.²

The 2016 results were clear: Tape is still the foundation of company data protection technologies and a mainstay in the data center. Still, when we compared the data over a seven-year-period, a completely different picture emerged. Tape continued to decline, from 80% in 2010 down to 65% in 2016. Software-based/logical replication was the second most popular data protection technology, and it showed some growth – from 45% in 2015 to 51% in 2016, even though the overall growth pattern was uneven. Although Virtual Tape Library is the least popular protection technology in the data center, VTL showed a surprising pattern of increase – from a low of 19% in 2010 to 30% in 2016.
Digging deeper, we found that companies are hedging their bets, using a range of data protection methods. Most IT organizations use 1 to 3 protection technologies, but over a fifth use 4 to 6. Year over year, the number of protection technologies in use remained about the same. So what do all these findings mean for IT organizations? Clearly, there’s no “one size fits all” formula for data protection. Multiple factors play a role in decisions about data protection, including company business models, cost benefits, and the types of resources to be protected.

**Data Protection Technologies in Use: Year-over-Year Trends**

Note: Data was not collected for built-in hypervisor replication or built-in application replication prior to 2013. As such, those technologies are not shown on the graph which depicts comparisons across seven years of data.
Data Protection Comparison – IBM i and Windows

This year, we dug deeper into the subject of data protection schemes, and we compared companies that have IBM i and Microsoft Windows as their primary operating systems, shown in the graph below.

Businesses that use IBM i as their primary operating system had a higher use of tape (82%) compared to Windows shops (66%). The possible explanation: When IBM-based businesses purchase servers, those tend to be bundled with components that commonly include tape backup. Also, a tape library can cost $50,000 to $100,000 or more; companies might not be accustomed to that kind of spending on a Windows server.

We found that IBM i users tended to use VTL (39%) more than Windows users (27%). IBM i users also were more likely to have made an investment in software-based replication technology (61%), than Windows users (52%).
The Achilles Heel: Failures, Data Loss, Downtime, RTO and RPO

Continuing our analysis, we asked IT professionals about failures, data loss, RTO, and RPO.

First, we found that nearly half of the businesses had experienced a failure (including a natural disaster, server failure, storage failure, or human error) that required their use of an HA/DR solution to resume operations: Within that group, 49% lost data – and not a slight amount. Remarkably, 33% lost up to an hour of data, and 37% lost a day or more worth of data.

These findings are cause for comment: The business impact of extreme data loss on direct revenue, productivity, overtime expenses, and corporate reputation is evident. The impact reverberates far beyond dollars and public image. From airline flight scheduling, to hospital patient care, and government record keeping, severe data loss can have a staggering effect on the welfare of consumers and the general public.

Has your organization ever experienced a failure?

- Yes 49%
- No 51%

How much data did you lose during your most significant loss, expressed in time?

- A few minutes
- Up to 1 hour
- A few hours
- 1 day
- More than a day
- Other (please specify)
Operating System Comparison: Failures and Data Loss

Businesses that use IBM i as their primary operating system were less likely to have experienced a failure (35%) compared to those running Windows (52%). IBM i users were also much less likely to have lost days to hours of data, as shown in the graph below. A survey from ITIC, an independent research group, also echoes these findings: More than 550 corporate enterprise users said IBM server hardware delivered the highest levels of reliability/uptime among 14 server hardware and 11 server hardware virtualization platforms.³

Note that the IBM businesses in our survey were larger and operated more data centers. It’s probable that these giants had fewer failures due to overall system reliability and a higher likelihood of having taken steps to minimize failures and data loss.

Data Loss After a Failure -- IBM i and Windows

![Graph showing data loss after a failure for IBM i and Windows]
Causes of Data Loss: Storage Failure is the Main Culprit

Then, we wanted to understand how data loss occurs, so we provided participants with six options from which to choose. Storage failure was the most common cause of data loss, followed by a missing backup copy (data was lost before it was backed up), as shown in this graph. Evidently, the root causes of data loss are the inherent weaknesses in data center equipment (disks and entire subsystems, such as cooling or power supplies) or the absence of software technology that can provide a real-time backup to a secondary site.

In the previous question, you indicated that you had experienced data loss. What was the primary reason?

The Staff Training Conundrum

In 2017, training could move to the forefront: The lion’s share (73%) of companies use internal staff for HA/DR management, but most professionals acknowledge that staff needs training.
How Much Downtime Did Businesses Experience?

Survey findings on downtime were not particularly positive news for businesses. Among organizations that had experienced a failure, 73% had downtime of 31 minutes or more. 23% had downtime of 30 minutes or less; in this group, only 4% experienced no downtime. The most common amount of downtime organizations experienced was 1-2 hours, as shown in the graph here.

In the previous question, you stated that your organization had experienced a failure that required use of your HA/DR solution to resume business operations. How long were operations down?
Recovery Time Objective (RTO)

Survey findings of business downtime naturally led us to examine IT professionals’ recovery time objectives. For Tier 1 systems, we found that more than half of businesses (52%) had a RTO of an hour or less, as illustrated in the graph. 28% had an RTO of 30 minutes or less.

What is your company’s recovery time objective (RTO) for your Tier 1 (mission-critical) systems and data after a disaster or a complete server or application failure?
Operating System Comparison: Recovery Time Objective

Businesses had similar RTO's across operating systems 6% difference

RTO by Operating System
Recovery Point Objective (RPO)

We gained even greater insight when we examined company recovery point objectives (RPOs) for mission-critical information, as shown in the graph. Companies do set fairly rigorous RPOs: 66% of IT professionals reported a RPO of one hour or less. Roughly a quarter (24%) had an RPO of a few seconds to a few minutes; and more than a quarter (26%) had RPOs of no data loss at all. Then we cross-tabulated findings about RPOs with the question about actual data loss. Although the number of respondents with this combination was small, the results were still troubling: Of those that had an RPO of no data loss and experienced a failure, 57% actually lost between a few minutes and a few hours of data.

As we’ll see in later discussion, IT professionals have low confidence in their company recovery plans. Yet when a disaster strikes, RPO metrics in the plan are the standards that tell professionals how much data they can afford to lose. If RPO metrics are set very low, then professionals must ensure that they deliver on their promises – with the resources and tools to recover quickly. Findings indicate that IT organizations should take a close look at recovery plans and metrics to make sure they’re viable.

What is your company’s recovery point objective (RPO) for mission-critical information, expressed in time?
Operating System Comparison: RPO

Businesses that used IBM i as their primary operating system had more stringent RPOs compared to those running Windows as their primary system. 54% of IBM i users reported RPOs of no data loss or a few seconds in contrast to 33% for Windows. One possible explanation for this finding: IBM is often a workhorse for transaction processing applications in industries such as banking, finance, transportation, and healthcare. The implications of a lost transaction is high for IBM i applications.

RPO by Operating System

No data loss: IBM i 45% Windows 25%
A few seconds: IBM i 15% Windows 10%
A few minutes: IBM i 10% Windows 7%
Up to 1 hour: IBM i 5% Windows 3%
A few hours: IBM i 2% Windows 1%
1 day: IBM i 1% Windows 1%
More than 1 day: IBM i 1% Windows 1%
The Cost: Time is Money, and Downtime is Expensive

Inarguably, businesses cannot afford to ignore the cost of downtime. As mentioned previously, nearly half of all businesses had experienced a failure that required HA/DR intervention to restart operations. Of them, over half reported downtime of an hour or more.

Surprisingly, survey results also showed that roughly half of IT organizations had not crunched the numbers to calculate their hourly downtime costs after a failure. Of those that had calculated the cost, 69% estimated the cost at less than $50,000, but 14% reported more than $500,000.

One positive development: Companies are realizing the importance of quantifying downtime. Year over year, substantially more businesses calculated the cost of downtime: 50% in 2016 versus 42% in 2015. The old adage applies here: If you can measure it, you can manage it.

What was the approximate hourly cost of the downtime experienced by your organization?

![Cost Distribution Chart](image-url)

- Less than $10,000
- $10,000 to $50,000
- $50,001 to $100,000
- $100,001 to $500,000
- More than $500,000
### Typical Cost of Downtime per Hour by Industry (in US dollars)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brokerage</td>
<td>$6.48 million</td>
</tr>
<tr>
<td>Service</td>
<td></td>
</tr>
<tr>
<td>Energy</td>
<td>$2.8 million</td>
</tr>
<tr>
<td>Telecom</td>
<td>$2.0 million</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>$1.6 million</td>
</tr>
<tr>
<td>Retail</td>
<td>$1.1 million</td>
</tr>
<tr>
<td>Healthcare</td>
<td>$636,000</td>
</tr>
<tr>
<td>Media</td>
<td>$90,000</td>
</tr>
</tbody>
</table>

Sources: Networking Computing, The Meta Group, and Contingency Planning Research
Recovery Plans: Big Room for Improvement

Survey findings showed that most IT leaders are not confident in their disaster recovery plans. In total, 84% of professionals had no recovery plan or were less than 100% confident that their recovery plan was complete, tested, and able to meet RTOs and RPOs. Only 16% were completely confident. And, 9% had no plan at all, as shown in the graph.

Regardless of business size, the best practices of recovery planning still apply. Solid HA/DR plans are essential for companies that want to diminish risk, avoid compliance fines, avert damage to reputation, and prevent loss of customers. Businesses will make themselves more resilient by testing their plans more frequently and evaluating recovery products that have built-in capabilities to perform DR testing on demand – without impact on production applications. As we’ll show in a later section of this report, some companies are making Disaster Recovery as a Service a strategic component of protection.

How confident are you that your company’s Disaster Recovery (DR) plan for IT Systems is complete, tested and able to meet your recovery time and recovery point objectives?

% Confidence Level

- We have no DR plan
- 10%
- 25%
- 50%
- 75%
- 90%
- 100%

% of Responses
Operating System Comparison: Confidence in Recovery Plans

Businesses that use IBM i as their primary operating system were more confident in their recovery plans compared to those running Windows.

84% of IBM i users had a confidence level of 50% or more, contrasted with 72% of Windows users, as shown in the graph. One potential explanation is that the IBM i users in the survey might have had more rigorous planning processes or practices for testing recovery schemes.
Industry Insight

Analysts and journalists stress the importance of recovery plan testing, using the 2016 Delta Airlines outage as the “poster child” for recovery plan failure:

“How could a company as technologically savvy and mature with its business processes as Delta not have a working disaster recovery plan? I can’t for a minute believe Delta does not have a disaster recovery plan to deal with an event like this, but it failed. That begs the question as to when it was last tested and how often this plan is reviewed, revised and retested.”

The survey provides a snapshot of companies mixed HA/DR capabilities. Year-over-year, a few areas showed progress, namely that a larger number of companies are quantifying the business cost of downtime. Yet vulnerabilities are evident: Company recovery schemes might not be adequate, given the data explosion and out-of-control storage growth. Some businesses are not meeting their recovery point objectives for mission critical applications – indicating that their metrics might not be reasonable or their DR systems are weak. Most troubling of all, recovery planning and testing are shortcomings. IT professionals must seek out robust solutions – technologies and services – to reduce data loss, meet recovery goals, and improve their disaster recovery plans.

**Key Takeaway:**

HA/DR
The State of Migration

Performance concerns, server consolidation, and upgrade or replacement of older systems are all compelling reasons that drive organizations to migrate from one platform to another. Yet even when IT professionals have business directives to migrate, the outcomes are not always predictable: Downtime and data loss are ever-present risks. What’s more, migration strains IT resources, with internal staff primarily working on weekends or after hours.

In the 2017 State of Resilience, we asked IT professionals about company practices, system downtime, and the challenges that they face during migration. Responses from 428 professionals tell the story completely.

Top Three Drivers for Migration

As a starting point for the survey, we wanted to identify company goals for migration. The three top drivers for migration were the need to replace unsupported or outdated server hardware (56%), improve performance (46%), and upgrade storage hardware (45%)

What were the objectives for your organization’s last migration?

- Replace unsupported or outdated server hardware
- Improve performance
- Upgrade storage hardware
- Consolidate servers
- Adopt virtualization technology
- Move to a different data center(s)
- Reduce cost of management
- Migrate to different database or application platform
- Adopt a cloud platform
- Consolidate databases
- Change virtualization and/or cloud strategy
- Conserve data center resources
- Switch to hosting at a Managed Services Provider
- “Green” computing concerns
- Other (please specify)

LEARN MORE ABOUT MIGRATIONS
Because the top three company migration objectives demand significant IT effort, we also asked professionals to tell us what staff resources they had used to perform migration projects. Almost half of respondents (47%) indicated that they use internal staff for migration; 41% also reported that they use a combination of third party consultants and staff. So in total, almost 90% of respondents call upon internal staff to help with migrations.

As explored in later discussion, personnel spend extra time working after hours or on weekends on migration projects – a practice that can have an impact on the financial and human resources of a company.

Astonishingly, the incidence of migration failure rose from 36% in 2014 to 51% in 2016
Migrations often involve different types of hardware and software assets, planning, testing, staffing, and scheduling, so it’s no surprise that they can fail. So we asked IT professionals if they had experienced a migration failure, then we compared responses from 2014 through 2016. Astonishingly, the incidence of migration failure rose from 36% in 2014, 44% in 2015 and 51% in 2016 -- a 42% increase, shown in the graph.

What’s more, we found that the largest companies (1,000 employees or more) were more likely to have experienced a migration failure (60%) versus 44% for all others. No doubt, large organizations have more complex systems and are migrating many servers and databases, as well as applications.

These numbers alone don’t tell the entire story of migration failure. We examined the reasons for failures and found that the top two were:

- Unable to start applications on the new server in the required timeframe, cited by a majority of 60%
- Lack of testing resulted in late discovery of issues (39%)

These findings indicate that the root causes of failed migration are likely poor, unrealistic planning and goal setting, and faulty testing procedures. While inadequate tools might account for some of these migration failures, it’s clear that the human factor – including training and planning – plays a vital role.
**Migration Challenges:**
*Delayed Migrations, Focus on System Downtime and Staff Overtime*

As shown in the graph, staff working overtime (44%) and system downtime (42%) were clearly the biggest issues that IT professionals faced during migration. But these numbers call for deeper analysis, so we asked respondents how many had postponed a migration. In fact, 66% had postponed a migration. The primary cause of delays? Concerns about downtime.

What’s more, we found that during migration companies work their staff overtime – a practice that can add to cost and negatively affect staff morale. The majority of IT professionals worked 25 hours or more during migration.

Downtime concerns cause some organizations to postpone deploying new technology. The risk? When businesses use hardware or software that’s beyond its end-of-service-life, there can be performance degradation, operational inefficiencies, data loss, equipment failures or added costs as leases overlap.

Considering the last time your organization performed a migration, what were some of the challenges the organization experienced?
The High Cost of Migration Downtime: Year-over-year Rise

Migrations must be non-disruptive and give IT professionals the benefit of moving workloads – while at the same time offering users continuous access to data and applications.

Years of surveys have shown us that downtime is a common occurrence during migration. So, we asked professionals to estimate their average cost per hour of migration downtime activity – including the costs of lost productivity, direct revenue loss, damage to reputation, overtime expenses. This year, an astonishing 62% of businesses in the survey had not estimated their average hourly migration downtime costs.

Then, we examined the year-over-year costs of those businesses that had experienced migration downtime. Between 2015 and 2016, we saw some evidence of an increase in cost, but not much: The hourly estimated cost of downtime rose by 5% for everything above $10,000.

Fast Facts

- 66% of professionals had postponed a migration, primarily a result of downtime fears.
- The majority of professionals worked 25 hours or more during migration.
System Downtime: The X Factor

As we’ve seen, migration is unpredictable and error prone, given that many organizations do not adequately test or plan for it. So we wondered, how much downtime did businesses actually experience?

Fully 58% of professionals reported migration downtime of an hour or more. Only 17% had not experienced any downtime during migration. We surmise that this small group plans better, tests earlier, and has access to a migration tool that enables continuous uptime during migration.

Taken together, findings regarding the expense of downtime and amount of downtime show how expensive migration can be. As discussed previously, the costs can add up to thousands or millions of dollars, depending upon the industry.

The last time your organization performed a migration, how long were your systems down?

- Systems were not down
- Less than an hour
- 1 to 2 Hours
- 3 to 5 Hours
- 6 to 12 Hours
- 13 to 24 Hours
- 25 to 48 Hours
- More than 48 Hours
- Don’t know
Key Takeaway: Migrations

Between downtime, costs, failure, and other factors, there’s a lot about migration that keeps IT professionals up at night. This year, more migrations failed (notably in larger companies), and the hourly cost of migration increased at the higher dollar levels. What’s more, businesses are delaying migrations because they are skittish about the system downtime involved. Without a doubt, migration is a juggling act for IT professionals who must balance the cost of downtime against the business risks of delayed or failed migrations – overlap of leases and system performance problems. But IT professionals can take the guesswork out of migration: They should adopt a unified approach that includes planning, testing, and deploying continuous uptime solutions that remove risk.
The State of Data Sharing

Strategic decision making. Business intelligence. Competitive advantage. Data has become a strategic weapon in the business arsenal for such diverse enterprises as sports franchises, retail establishments, and manufacturers. Without a doubt, IT leaders have mandates to deliver synchronized, accurate, near real-time data for their companies. But how well are professionals prepared to meet that demand?

To answer these questions, we fielded an entire survey on business data sharing practices, the methods they use, and the roadblocks they encounter. Nearly 300 IT professionals responded to the survey, showing that the topic resonates deeply with them.

A Snapshot of Data Sharing

To start, we wanted a sharp picture of our respondents’ data sharing environments. How many have multiple databases and how many were sharing data between these?

We learned that 80% of survey participants had multiple databases, including those associated with business applications. Of these, 73% share data among databases.

Taking our investigation further, we found that IT departments manage diverse combinations of databases from different vendors, including Oracle, Microsoft SQL Server, MySQL, and IBM DB2, among others. Almost one-quarter manage four different types and nearly 8 in 10 use three or more. Only 8% manage a single vendor’s database. Inarguably, in these highly diverse database environments, data sharing becomes more challenging, and certainly adds complexity – and potentially more risk – to IT management.

For the purposes of this survey, data sharing is defined as moving copies of data from one database to another. Does your organization share data between multiple databases?

- Yes
- No
- I don’t know

73% Yes
20% No
7% I don’t know
Reasons for Data Sharing

We also wanted to learn more about organizational reasons for data sharing, as shown in the graph below. The three chief reasons, chosen by the majority of professionals, were to consolidate data from multiple sources into a single data warehouse; perform Business Intelligence on data offloaded from the production database; and, report on data offloaded from the production databases.

Later in the survey, we asked professionals to rate the business justifications for sharing data. They ranked the top ones as:

1. Using our data to better provide my company with a competitive advantage.
2. Integrating data so it is closer to real-time accuracy across the business.
3. Sharing data currently isolated in departmental applications across the business.

All of these are ambitious goals, and so we wondered, “Is the data center environment prepared to deliver the business intelligence that companies want?” So we took a closer look at business procedures and tools for data sharing.

For what purposes does your organization share data between databases?
Redundant Data: Inconsistencies Impact Business Performance

Our next questions addressed the topic of redundant data and its negative effect on business performance. We discovered that 70% of IT professionals with multiple databases had redundant data stored in them, but a quarter of those did not have processes in place to synchronize the data. Digging deeper, we found that 70% of those who had redundant data were concerned about inconsistent information stored in databases.

It’s important to note that redundancy in itself isn’t a problem: Reliable replication schemes can ensure data accuracy and redundancy across data centers to protect vital information against system failures or loss. The real problem is inconsistent data: It affects businesses when they struggle to reconcile conflicting data for decision making, as highlighted in the following discussion.

70% of those who had redundant data were concerned about inconsistent information stored in databases.

LEARN HOW DATABASE CONSOLIDATION WORKS
MiMIX Share, Database Consolidation
Hot Button: The Impact of Inconsistent Data

IT professionals who have multiple databases were asked about the business effect of data inconsistencies. They identified three main problems, as shown in the graph below: delayed decision-making (44%), significant time and effort spent reconciling inconsistent information (36%), and low confidence in decisions that are made (23%).

Paradoxically, in another survey question, professionals said that data is shared for the purpose of “Business Intelligence” Delayed decision making and reconciling inconsistencies to diminish the value that can be gained from the date to provide Business Intelligence.”

How does inconsistent information stored in your databases impact decision making for your business?

- Decisions have to be delayed in order to reconcile conflicting information
- We spend a significant amount of time and effort reconciling inconsistent information
- Timely decisions are made, but our confidence in those decisions is low
- We have had compliance issues, e.g. stemming from inconsistent information in databases
- No impact on our business decision making
- Decisions are not based on actionable information
- I don’t know
- Other (please specify)
Data Sharing is Complex, but Tools and Approaches Lag

Concern about data inconsistencies was so widespread in businesses that we wanted to know exactly how professionals shared data between databases. Were company tools and methods partly responsible for data discrepancies that exist?

As shown in the graph, the majority of IT professionals use FTP/SCP/file transfers (54%), followed by those who use manual scripting (50%), and backup restore processes/snapshots (43%). These traditional tools come with a price tag, because they consume time and resources. FTP and file transfers can be slow and vulnerable to error. Home-grown scripts require development effort, testing, and maintenance. Also, when a database changes or is upgraded, scripts must be retested.

What’s more, the process of sharing data becomes exponentially complex when companies use older methods to share data between heterogeneous databases. As noted previously, almost 8 in 10 have three or more different database types. In sum, we conclude that IT professionals are facing steep challenges in keeping data sets up-to-date and integrating data from different sources.

What techniques does your organization use to share data between databases?
SaaS: Are Database Applications Jumping to the Cloud?

Petabytes of structured and unstructured data are being created at lightning speed, driving an escalating demand for storage. To a certain extent, Cloud technology gives companies greater storage capacity for databases and frees them from investing in hardware. For this reason, we asked professionals about their organizational plans for using SaaS (Cloud) for primary database applications.

We assume that companies are being deliberately selective about the types of database applications they decide to migrate to the Cloud. Considerations could include the size of the respondents’ business or databases, bandwidth, response time, compliance regulations, or sharing the data with other on-premises applications.

Results also indicate that companies might be biding their time – either getting by with in-house equipment and resources or still using their “iron” to keep up with database growth. Still, considering the data explosion, we predict that businesses looking to slice hardware costs and realize big benefits in agility will eventually adopt SaaS for database apps.
Results showed that companies are still in the very early adoption stage of hosting databases in the Cloud – though there is movement in that direction. SaaS use for databases fell into three categories:

- Slight move to SaaS: 4% report they have moved to SaaS for primary database applications; another 11% say they’ve moved “select” database applications to SaaS.
- Evaluating SaaS now or within the year: 13% are evaluating now; 10% within a year.
- No plans for SaaS: 43% report that they have no plans to adopt SaaS models for database applications; another 6% report that they have evaluated SaaS models, but have no plans to adopt them.

What are your organization’s plans for adopting SaaS for your solutions for your primary database applications?
Key Takeaway: Data Sharing

Survey results indicate a clear need for a paradigm shift in database management and data sharing. Businesses are at risk when faulty data is used or decisions are delayed because time is spent reconciling data inconsistencies.

IT professionals noted that they had business directives to integrate data for real-time accuracy across their organizations – and to use data for competitive advantage. Yet, the tools and processes they use to manage data are lagging, so organizations aren’t moving quickly enough to capitalize on its strategic value. Companies must take aggressive steps to align their data sharing schemes strategically and operationally with business directives.
The State of Cloud

Cloud has been one of the most disruptive, but at the same time most valuable technologies in terms of business agility, cost effectiveness, and efficiency. For many companies, Cloud has delivered on its promise of always-on connectivity, scalable computing power, and reduced hardware costs.

Yet, certain aspects of Cloud are still evolving and will challenge companies in years to come. Executive leadership and IT professionals are demanding answers to such questions as, “Where should our Cloud-based data be stored geographically?” “What is the right set of protection products to ensure data security in the Cloud?” And, “if we decide to configure systems for disaster recovery in the Cloud, will our Cloud provider have the WAN bandwidth to support us?”

In this year’s State of Resilience, we posed questions about Cloud use, Cloud-based services and applications, governmental regulation of data, and the uncertainties that continue to confront IT professionals.

Industry Insight

“By 2020, a corporate “no-Cloud” policy will be as rare as a “no-internet” policy is today.”

June 22, 2016, Gartner Inc. Press Release
Cloud Adoption: Mature and Growing

Cloud has passed the tipping point – the stage at which an evolving situation leads to an irreversible change. As shown in the graph below, about two-thirds of respondents use Cloud, a number roughly consistent with last year’s survey. This presents a stark contrast to our first Cloud survey in 2010, when only 22% of businesses had adopted it, and the rest were “playing the waiting game” to see how the technology would develop. Now, the question for late adopters is no longer “whether to adopt Cloud” but “when and how.” Our survey results reflect this sentiment; of those without Cloud, more than three-quarters will deploy within the next 5 years.

Are you currently using Cloud services?

- Yes 65%
- No 35%

READ BLOG
Cloud is Here to Stay!
Types of Clouds: Hosted Private Clouds Prevail

Even though Cloud adoption has soared, IT professionals must weigh risks versus rewards when choosing the right type of Cloud for their organizations. Issues such as regulatory compliance, privacy laws, data location, operating costs, and staff resources all are critical considerations. Choosing the right Cloud model can be a challenge, so we wanted to gather baseline information about the types of Cloud delivery systems companies used.

As shown in the graph below, the majority of companies use Hosted Private Clouds (52%), followed by Public Clouds (46%), Hybrid Clouds (40%), and On-Premises Private Clouds (35%).

Unsurprisingly, we found that size counts when it comes to choosing a Cloud delivery model. Crunching the numbers, we found that the smallest companies (1-10 employees) tended to use Public Clouds (56%), compared to the largest companies – those with over 1,000 employees (48%). The largest companies also preferred Hosted Private Clouds above all other types (60%). No doubt, mega corporations have greater internal resources and staff for managing Private Clouds.

Does your company currently use any of the following Cloud types?
Cloud Types:  
A View of the Future Hybrid Cloud Popularity:  
One Foot on the Ground, One in the Cloud

When it comes to company Cloud plans for the future, the surveys showed a different picture – a shift in preferences to Hybrid Clouds, followed by Hosted Private Clouds.

- 33% plan to use Hybrid Clouds
- 26% plan to use Hosted Private Clouds

Hybrid Clouds are one solution to compliance and security issues for companies in regulated industries, such as financial services and healthcare. Companies can keep regulated data locally and store non-sensitive data with Cloud providers. Our finding is in line with predictions of analyst organizations, such as Gartner, who foresee that most companies will adopt a Hybrid Cloud strategy, but will require Public Clouds to be a part of their overall plan.
Most Popular: Software as a Service, Infrastructure as a Service

Software as a Service (SaaS) was used by the majority of businesses (57%), followed by Infrastructure as a Service (IaaS) chosen by half.

Does your company currently use any of the following cloud services?
SaaS has been accepted by companies both large and small. Small companies can leverage the benefits of sophisticated applications – accounting or payroll, for example – without sinking capital into in-house software. Larger IT companies often view SaaS as a simpler, cost-effective solution to their resource constraints.

IaaS – the second most prevalent Cloud service – generally keeps infrastructure components, such as storage, computing power, and networking, in the hands of the Cloud provider, while the customer has control over the operating systems and applications – and potentially some components such as firewalls. This on-demand, elastic model is projected to have a tremendous growth rate: Revenues are expected to more than triple, from $12.6 billion in 2015 to $43.6 billion in 2020, with a compound annual growth rate of 28.2% over the five-year forecast period.

On a final note: Recovery as a Service (DRaaS/RaaS) was the Cloud service that businesses used the least (22%). However, it’s important to put this number in context. DRaaS offerings are new to the market, and companies are in the early stage of adoption. Companies evaluating DRaaS are carefully considering service level agreements for outages, visibility into critical HA metrics, and data privacy issues. Analyst organizations also note that smaller organizations are more likely to adopt DRaaS sooner than large ones. Why is this the case? Most big companies typically have multiple data centers used for backups, and closing a data center takes years to plan. In addition, larger companies are more cautious buyers and still own many physical servers. Despite these hurdles, DRaaS/RaaS revenue is projected to grow dramatically over the next three years.

Industry Insight

DRaaS revenue was $1.3B in 2015, and is expected to grow 20+% annually over the next three years.

Application Tiers in the Cloud: Businesses Entrust Vital Assets

Substantial numbers of businesses place a high level of trust in Cloud systems, as illustrated in the graph. Of companies that use Cloud, 33% are entrusting their most mission-critical (Tier 1) applications to it. 32% use or protect Tier 2 applications in the Cloud.

Although professionals express deep concerns about security and privacy in the Cloud, they’ve evidently decided that the rewards outweigh the risks. The survey asked respondents to rank the most important benefits of Cloud, and the top three were:

1. IT capacity on demand
2. IT efficiency
3. Operational cost savings

Clearly, companies are choosing Cloud so they can deploy applications on demand, satisfy their user communities, and reduce operational costs.

What application tiers does your company currently USE in, or PROTECT to, the Cloud?

- Tier 1 (most critical)
- Tier 2
- Tier 3
- Tier 4 (least critical)
- We do not use or protect applications in the Cloud
- Don’t know

READ WHITEPAPER
Migrating Workloads to and from the Cloud with Platform Independent Replication
Cloud Challenges: Infrastructure Control, Data Protection are Biggest Headaches

The majority of IT professionals (52%) reported that their chief concern about Cloud is maintaining infrastructure control, followed by 45% percent who are worried about preventing access to their data by other Cloud customers. As highlighted in the following discussion, worries about software inventory management, privacy laws, and tightening global regulations are likely to make them more cautious adopters of Cloud.

What are the challenges you see in using or planning to increase your organization’s use of Cloud computing?

- Desire to maintain internal control of infrastructure
- Concerns about protecting data from access by other Cloud customers
- Increase in total cost
- Governmental regulations restricting the geographic location of confidential data
- Concerns that incident response times will not meet requirements
- Insufficient performance
- Fear of being tied to a single Cloud provider
- Inadequate Service Level Agreements
- Concerns stemming from public reports of Cloud failures
- Other (please specify)

“Off the Radar” Software is a Threat

- About 25% of professionals surveyed admit their business users run Cloud applications outside the control of IT.
- More than 33% say they just don’t know if users run Cloud applications outside IT control.

Companies run the risks of unapproved software: Lack of standards and change control, compliance issues, intellectual property loss.
Physical Location of Data: Governed by Law

Many survey respondents (41%) said their companies are subject to governmental regulations on where their data can physically reside. This might explain our finding that many are planning Hybrid Clouds – keeping “one foot on the ground, one foot in the Cloud.”

Global Industry Insight
The Battle Continues: Data Protection, Privacy, and Storage in the Cloud

CEOs and CIOs take notice. In June 2016, the European Union launched E.U.-U.S. Privacy Shield, an international agreement that gives stronger protection to EU citizens for transatlantic data flows. Now U.S. technology giants are investing billions of dollars to build data centers in Europe to store user data locally – responding to regulatory watchdogs’ growing concerns about data security.

But there’s another reason for this robust investment: Europe’s market for Cloud application services is projected to more than double, to $16.1 billion, by the end of the decade, according to Gartner. It’s a big business opportunity.

Even outside the European Union, technology companies that fail to conform to country regulations could feel the pain: In November 2016, Russian courts prepared to block LinkedIn, the business social networking site, from Russian users because it violated the country’s data protection laws requiring local data storage.

This is an evolving story, but fines and loss of business are possibilities for multinational businesses that don’t comply with country regulations.


Who’s Accountable for Public Cloud Protection? IT Professionals Differ

Professionals hold divergent opinions regarding who’s responsible for protecting data and applications in a Public Cloud. Of those who used Cloud:

- 43% felt that the Public Cloud provider was responsible
- 39% felt that the internal IT organization was responsible

In reality, the blame can fall on an internal IT department if a Public Cloud fails. Service-level agreements with Public Cloud providers must pinpoint responsibility for protection and liability after a breach.

Even so, many analysts believe that well-crafted service agreements alone don’t provide protection: Internal company processes and procedures might be the biggest issue for Cloud customers. A report from Gartner, Inc. asserts that through 2020, 95% of Cloud security failures will be the customer’s fault. Why is this the case? Professionals’ naïve beliefs that SaaS providers are liable for their customer security leads them to ignore the way employees use external applications. Employees can improperly share large amounts of data with other employees and outsiders. In sum, technological decisions are just one piece of the Cloud puzzle: Company guidelines and best practices need attention too.
Most companies have jumped into the Cloud now, so that’s not news. What is news though is that Cloud is still a rapidly evolving technology, and professionals have to race to keep up with new products and services that emerge. This year’s data showed that many companies are planning to implement Hybrid or Hosted Private Clouds – perhaps to address security and compliance issues. Still, findings indicate weaknesses in company Cloud schemes and a list of “to dos” for professionals, namely:

- Reviewing SLAs with Cloud providers
- Establishing controls over users’ Cloud apps
- Understanding regulatory requirements
- Evaluating emerging services, such as DRaaS
Conclusion: Looking Back, Moving Forward

In 2017, Vision Solutions celebrates 10 years of conducting State of Resilience research, so it’s fitting that we review the developments of a decade, while summarizing this year’s findings.

Over the years, we’ve seen data centers on the East Coast of the U.S. ravaged by Hurricane Sandy, noted system melt-downs in global corporate giants, and observed IT environments evolve dramatically into multi-vendor systems and service models. We’ve also witnessed the graying of the IT workforce in some businesses, with an associated loss of technical knowledge as workers retire. Also on our radar screen were the rise of mobile technology and the demand for an enhanced user experience – developments that have driven IT professionals to offer “always on,” 24/7 access to backend systems.

In 2007 and 2008, we surveyed over 2,000 professionals on the technologies and methods for data protection and system optimizations for the Power Systems line of platforms. In 2009, our research program examined the impact of a long, cold economic downturn on IT hiring, purchasing, and training. Since 2010, our surveys have tracked the rise of Cloud adoption – from a low of 22% to this year’s high of 65%. Also since 2010, we’ve reported on IT leaders’ mounting anxiety about data recovery, protection, and security – no doubt driven by the greater complexity of IT systems and smarter cybercriminals.

So, yes, a decade has brought tremendous change, and still we are optimistic about enterprise technology for several reasons.

This year we witnessed more disruption in IT departments and slow forward progress at the same time. More companies are quantifying downtime costs, the majority are using Cloud services such as SaaS for mission-critical applications, and others have just started to experiment with DRaaS.

Despite these developments, why does change appear to occur slowly? Many companies in our surveys operate multiple data centers. It’s a fact that most data centers have long lifecycles, and new technologies take time to plan and implement. Some IT organizations are using 20-year-old tools for data sharing, such as FTP and home-grown scripts. Most are still running data onto tape for offsite storage, while continuing to adopt more agile protection technologies. So although businesses do need more innovative approaches to data center design, we expect progress to proceed at a measured pace.

In reality, technology is just one part of the entire solution: Technology helps the world rise, but it’s the people behind the systems that truly bring about transformation – whether they’re in the trenches or in the boardroom. IT professionals thrive by being flexible and innovative, riding the wave of change that’s occurring.

Our IT leaders do face challenges: They deal with day-to-day operations and disruption, all while thinking 3 to 5 years out. But despite difficulties, through budget crunches and natural disasters, through hiring booms and expansions, we’ve seen technologists hold firm to professional commitments.

Will IT professionals face steep hurdles in making their companies more resilient? No doubt. But are they up to the task? Absolutely. They are staying strong.
As a final note, we’d particularly to thank all the IT professionals who took the time to participate in our surveys over the past decade. Whether you are a CIO, CTO, VP of Information Technology, Cloud Architect, Systems Administrator, Senior DBA, Principal Systems Engineer, or Network Specialist, we’ve appreciated your feedback. Your responses help contribute to greater knowledge and understanding of the industry. We’re looking forward to your insights in the coming year.

Footnotes


2 Data was not collected for built-in hypervisor replication or built-in application replication prior to 2013. As such, those technologies are not shown on the graph which depicts comparisons across seven years of data.


4 One key point to note about Hosted Private Clouds: This type gives companies the advantage of “renting” a Cloud solution off-premises: Although though the customer/renter does not manage or control the underlying Cloud infrastructure such as the hardware or WAN, the renter can control the operating systems, storage, and deployed applications.


MODERNIZE IT™

Vision Solutions is the premier provider of software solutions designed to protect data, minimize downtime and maximize resources for the modern data center.

We are the leading provider of IT Modernization solutions – high availability, disaster recovery, migration and data sharing – for IBM i, AIX, Windows and Linux operating systems. For more than 25 years, customers and partners have trusted Vision to protect and modernize their environments, whether on-premises or in the cloud.

For more information call: 1.800.957.4511 (toll-free U.S. and Canada) or visit visionsolutions.com

Also find us on: Facebook: http://www.facebook.com/VisionDoubleTake
Twitter: https://twitter.com/VSI_Power
Twitter: http://twitter.com/#!/VSI_DoubleTake
YouTube: http://www.youtube.com/VisionDoubleTake