The 2018 State of Resilience

The New IT Landscape for Executives: Threats, Opportunities, and Best Practices

Final Version: December 15, 2017

syncsort

VISION SOLUTIONS

Table of Contents

Introduction: Is IT Turbulence the New Norm?

This has been a turbulent year for IT professionals and their companies. Resilience has been in the top headlines of industry media for months because scores of organizations have been disrupted by technology-related disasters.

Malevolent state- and non-state actors have breached corporate and governmental systems alike: Equifax and the IRS experienced hacking attacks, while Target, Home Depot, Anthem, and others incurred stiff compliance fines for data breaches. These complex hacking attacks, viruses, and related failures across multiple systems present serious risks to business operations and information integrity.

Non-hacking failures also afflicted companies such as British Airways, when a power outage resulted in cancelled flights that affected 75,000 passengers, and it took days for systems to regain normalcy. Amazon's Simple Storage Web service too went down for several hours as a result of human error.

Another formidable adversary of IT resilience is Mother Nature. Disruptive natural disasters this year, such as hurricanes Irma, Harvey, and Maria, and raging California wildfires, all underscored the need for HA/DR, solid backup systems, and preparedness.

At the same time, a data tsunami and escalating storage needs, driven by phenomena such as the Internet of Things (IOT) and online commerce, confront professionals. Indeed, analysts have predicted that the world will create 180 zettabytes of data (or 180 trillion gigabytes) in 2025, up from less than 10 zettabytes in 2015. As a result, inventory management, storage, access, and security will be continuous challenges.

Against these strong headwinds, IT professionals are called upon to provide an enterprise infrastructure that can sustain severe shocks, protect information, and enable the insight and intelligence that their companies need. What does their scorecard look like? Do they have the tools and support to meet the future rushing toward them?

This report reveals the technologies that professionals use and analyzes companies' strengths and vulnerabilities. We anchor our observations in the research we've completed and provide insights into the practices of IT professionals and their organizations. Read on to discover how your organization stacks up against others. Please enjoy the report and share it with your colleagues.

Respondent Profile and Methodology

Respondent Profile and Methodology

6 Survey Topics

- **IT Trends**
- **High Availability and Disaster Recovery**
- **Security**
- **Migration**
- **Data Sharing**
- **Cloud**

Respondents, Distribution and Profile

In total, 5,632 professionals responded to the surveys detailed in this report. Professionals' titles varied widely, from CIO, CTO, Global Director of IT Infrastructure, and VP of Technical Support, to Senior Infrastructure Architect, Cloud Engineer, Database Administrator, and Manager of Server Operations.

Respondents represented a wide range of countries, including: Indonesia, Hong Kong, Australia, and Malaysia in the Asia Pacific; Peru and Columbia in Latin America; Saudi Arabia and the United Arab Emirates in the Middle East; Spain, Germany, and the Netherlands in Europe; and the U.S. and Canada in North America, to name a few.

Respondents also used a wide range of operating systems, including Windows, Linux, IBM i, IBM z/OS, IBM AIX, and Linux on IBM Power Systems.

In addition, this year's analysis contains information on some practices of companies that use IBM Power Systems. In particular, we wanted to shed light on their tools and processes, with the goal of providing targeted insights for IT teams that manage these systems. Where appropriate, results for IBM Power Systems are shown in separate sidebars.

Date

Throughout 2017

Delivery System

Surveys were administered online, using web-based survey tools and targeting IT professionals.

Central Issues for Executives

As the future comes toward IT leaders, it's both an exciting and a disruptive time for them. Professionals are expected to keep traditional systems running like clockwork, all while the industry is pushing the limits of technology. This year's research uncovered fundamental difficulties facing IT leaders, as well as opportunities they foresee.

IT Trends: What's in Store?

Many companies are moving forward energetically to launch new initiatives. Security, business continuity, and disaster recovery are flashpoints for professionals and also the focus of most technology initiatives in the next 24 months. Intriguingly, financial issues, such as IT expense control and return on investment were not highest on the list of IT concerns or performance measures for the year. It's possible that after some years of overseeing skinny data center budgets, professionals and their companies feel optimistic enough to spend on IT for greater efficiency or to support new business opportunities. Our finding is supported by reports of industry analysts who project substantial growth in the enterprise sector alone through 2018.[1]

High Availability and Disaster Recovery in the Spotlight

Research showed that companies are generally using a mix of data protection technologies, with hardware/storage replication, tape backup, and software/logical replication most common. Overall, IT departments exceeded their maximum tolerance for downtime during a failure, a weakness that must be addressed. Findings also showed that professionals lack confidence in the effectiveness of their disaster recovery plans. Moreover, the lion's share of companies use internal staff for HA/DR, yet most will not increase staffing levels or train HA/DR staff in the next year. Appropriate staffing, workforce training, better recovery planning and testing are needed to "bulletproof" company systems. This is especially true, since a considerable majority of companies have HA/DR initiatives planned for the coming year.

[1] Worldwide spending on enterprise software alone between 2017 and 2018 is projected to grow 9.4%. Gartner, Inc. Global Spending on IT Expected to Reach $3.7 Trillion in 2018, October 3, 2017. https://www.gartner.com/newsroom/id/3811363

A Hot Button: Security Policies, Procedures, and Education

Security emerged as the chief initiative—and headache—of professionals in the coming months. Yet, businesses seem to be investing primarily in the basic underpinnings of security: virus protection, malware protection, patch management, and intrusion detection. Other investments, such as user/two factor authentication, secure file transfer, and security training for company personnel did not rank as high on the agenda of projects. In particular, the lack of emphasis on training is troubling, because professionals noted that staff education, policies, and procedures would most help them address their security challenges. Breaches originating inside a business are difficult to prevent and identify using traditional perimeter defenses. Clearly, IT departments must work across the company—and not just within the data center—to help develop a culture of security.

Business Intelligence is the Goal, Data Management the Challenge

Business intelligence and analytics are the main goals for data sharing in organizations. It's good news that the majority of companies use technologies that guarantee real-time data sharing. Still, deeper examination of results showed that many businesses still use less effective legacy technologies; periodic data sharing methods also caused some businesses to delay business decision making and spend time reconciling data inconsistencies. What's more, heterogeneous database environments are a reality that complicates the work of IT staff--especially those using older data sharing tools. Given new developments in data science and analytics, database diversity, and the data explosion, IT leaders must explore advanced solutions for data synchronization.

Migration Practices Stalled, Need to Get in Gear

Migration technology has seen many game changing innovations in recent years, but findings showed that most organizations have not adopted state-of-the-art migration practices. Many migrations fail, and a majority are delayed due to fears of downtime. What's more, IT professionals are forced to weigh the risk of downtime and staff overtime against the very real business impact of using hardware or software reaching its end-of-service life. IT leaders can take a strategic approach to migration by adopting tools that provide near-zero downtime, improve performance, and ease the strain on staff who perform migrations on weekends or after hours.

Cloud Rules, But Technology Leaders Have Concerns

Cloud is now a robust and mature platform—no longer an early-stage technology. Professionals recognize the business benefits, and they perceive reduced capital expenditure as the biggest one. Many are entrusting critical or near critical applications to the cloud. At the same time, they're juggling choices about cloud's greater cost savings and higher performance against serious concerns about data privacy and sovereignty.Findings also showed that multi-cloud management is a reality: Of companies that use cloud, nearly half manage two or more cloud types and almost a quarter manage three or more. No doubt, this means more vendor management, complex purchasing decisions, and risk for professionals.


The State of IT Trends

The State of IT Trends

IT professionals are presented with a wealth of innovations to explore, from machine learning and artificial intelligence, to virtual reality, Big Data, and more. Yet there's typically a gap between the time a technology emerges and companies recognize a need, assess their requirements, and proceed down the path of adoption. Some technologies seem light-years away, and the adoption rate is often five years to actual data center implementation. In this year's State of Resilience, we posed questions about new initiatives and technologies. Still, given the dynamic nature of technical innovation, we tended to look at initiatives and issues with a shorter timeline—1 to 2 years ahead. More than 1,300 professionals responded to the survey, with revealing results.

Top Technology Initiatives—Next Two Years

When IT professionals look ahead twenty four months, they note that security (49%) is the chief IT initiative, closely followed by high availability/disaster recovery (45%), and cloud computing (43%), shown in the graph.

It's no surprise that companies are focusing on security initiatives. Cybercrime is in the spotlight these days, and no business can afford to ignore it. Moreover, compliance concerns could be driving companies to respond strongly to threats and the risks they pose: security is an ongoing project for regulated businesses. The Security Survey revealed that roughly 80% to 90% of regulated companies have formal security plans and perform security audits on their systems versus 53% for unregulated companies. Companies that fail to keep up with security controls can pay steep fines for lapses or data breaches.

High availability/disaster recovery is an evergreen project for IT leaders. The majority are planning new initiatives—expanding their solutions, tuning a current solution, or adopting new HA/DR technology—as discussed in further sections of this report.

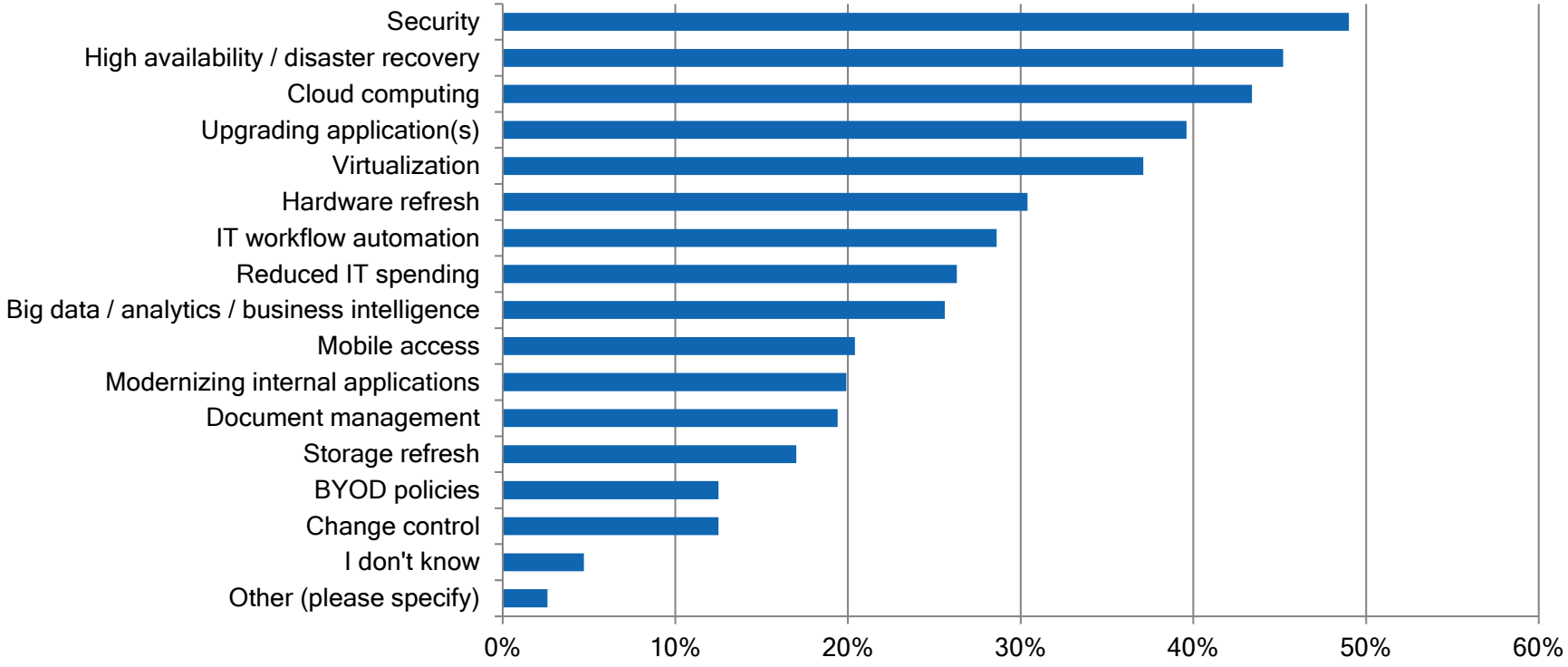
Many companies are undertaking cloud initiatives--and cloud now has a solid footing in businesses, as they adopt cloud for its efficiency and agility. Although cloud is no longer a nascent technology, it still presents challenges to IT leaders, namely privacy, data sovereignty, access control, and service level agreements with third party providers. The Cloud section of this report explores these pressing issues in more detail.

Fast Facts

An Eye on the Averages: How Are Companies Gearing Up?

- IT Initiatives: Companies will launch an average of about 4 initiatives in the next 24 months.
- Security: Security is high on the list of technology projects for the majority of businesses. 56% are undertaking 4 or more security initiatives in the coming year.
- Database Initiatives: Companies are planning an average of 1 database initiative in the next 24 months, but larger companies are planning more.

What are your company's top IT initiatives for the next 24 months? Choose all that apply.



Industry Insight

IBM Power Insight: Compliance Auditing and Reporting

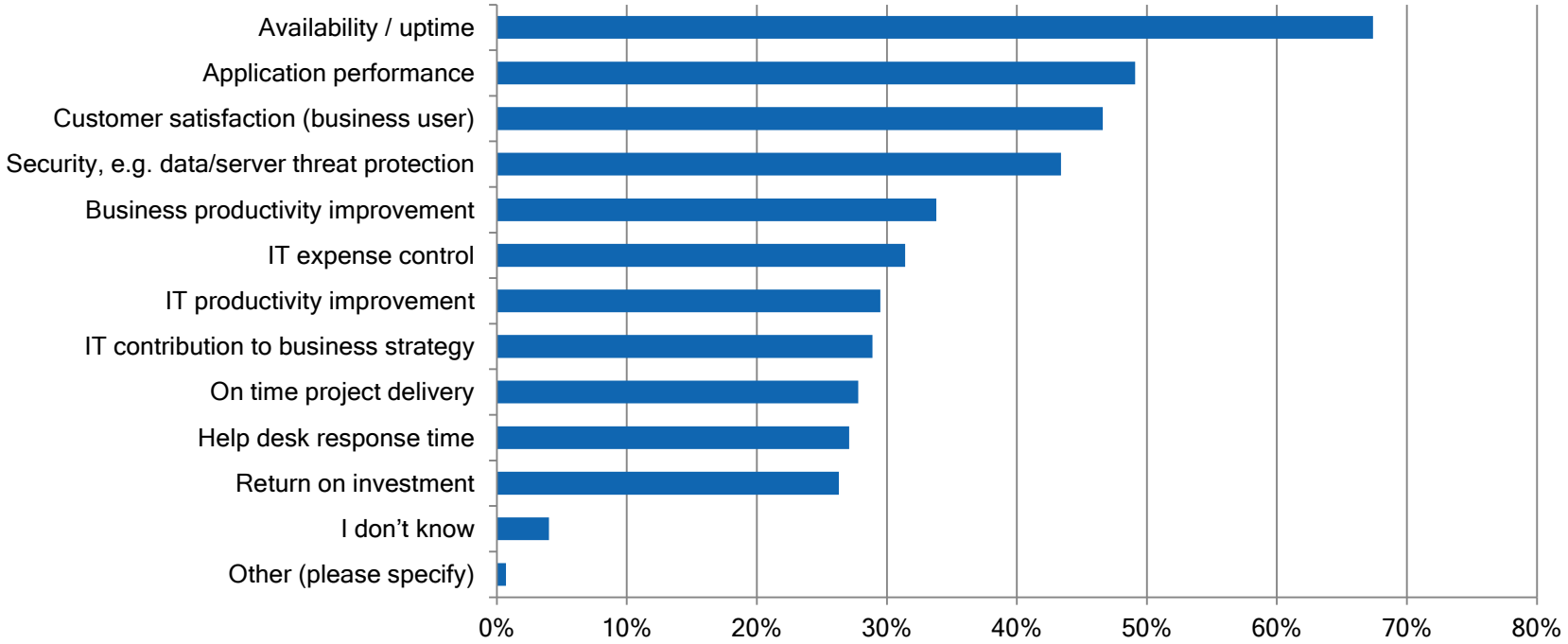
For the majority of IBM Power users (52%), the trend toward security investments in the coming year will focus on compliance auditing and reporting. Compliance standards such as NIST 800-53, PCI DSS, FISMA, GLBA, SOX, STIG and HIPAA require organizations to secure their networks, harden servers and desktop computers for their confidential enterprise assets, and provide network compliance reports to auditors when demanded. Notably, 12% of IBM Power respondents in the study are in the banking industry, which has strict regulatory requirements.

Gauging IT Performance

Digging deeper, we wanted to learn about the chief "yardsticks" used to measure IT performance. Results showed that availability/uptime outstripped all others at 67%, as illustrated in the graph. Application performance (49%) and customer satisfaction (47%) followed. It's a positive sign that the top measures not only assess IT performance in functional disciplines like uptime and application performance, but that they also gauge the satisfaction of customers/business users—a metric that can make or break IT departments and careers.

Remarkably, return on investment received the lowest rating as a performance metric (26%). We conjecture that some survey participants might not have ROI responsibility or find difficulty in measuring ROI; it's also possible that after years of uncertainty and managing razor-thin budgets, companies are now giving IT professionals more latitude in spending, thus they are less concerned about ROI.

What are the top measures of IT performance in your organization? Choose all that apply.

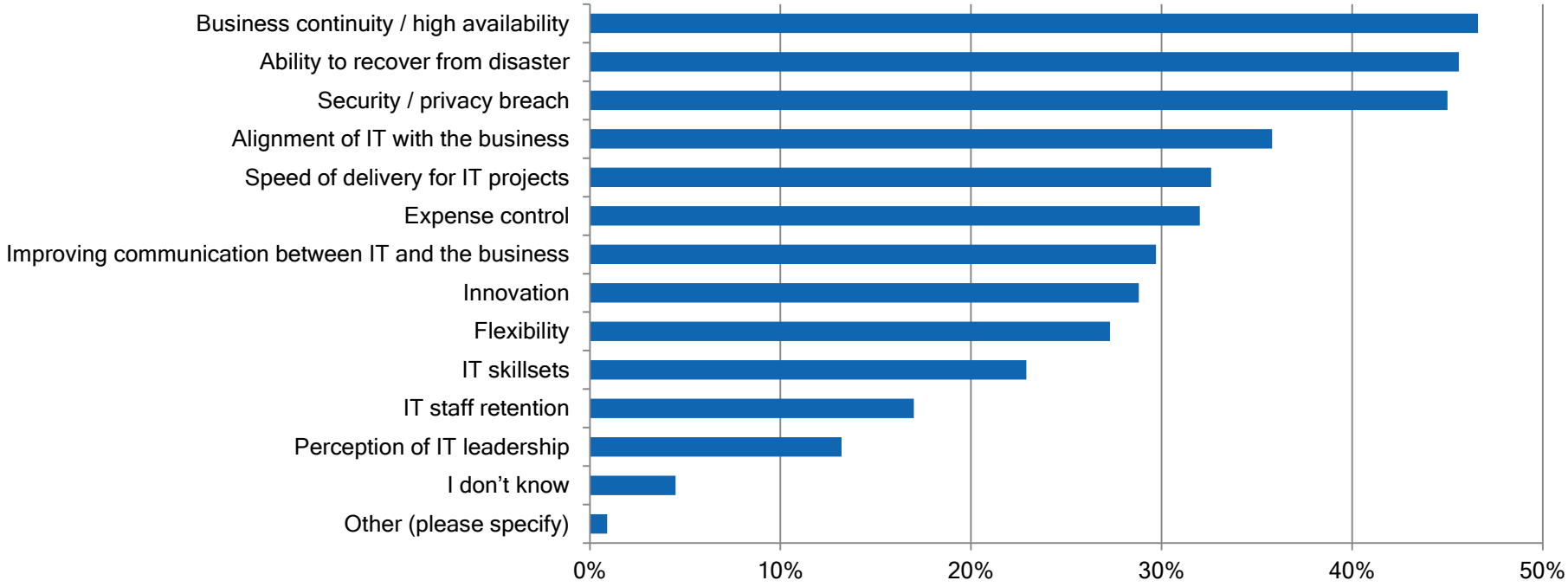


Headaches for IT Leaders: Top Issues

Analysis of respondent's chief concerns revealed a nearly three-way tie for business continuity/high availability (47%), ability to recover from disaster (46%), and security/privacy breaches (45%).

Surely, it's no coincidence that these issues recur throughout all the surveys and are interconnected. A system security strategy is an integral part of any organization's overall plan for continuity, recovery, and resilience.

What are the top IT issues that concern your company in the coming year? Choose all that apply.



Key Takeaway:

Companies will be fairly aggressive in launching initiatives in the coming months. Security, business continuity, and disaster recovery are predominant themes that emerged in the survey results; these are the major concerns of IT this year and also the focus of technology initiatives. Remarkably, financial issues, such as IT expense control and return on investment were not highest on the list of this year's IT concerns or performance measures.

The State of High Availability/Disaster Recovery

The State of High Availability/ Disaster Recovery

Data is the life force of every enterprise, yet, if that data becomes unavailable, corrupted, or lost, then business profitability, productivity, staff morale, and reputation suffer. If disaster strikes, IT professionals must have planned, designed, and managed resources so that they can resist stress or interruption—and continue deliver the data that drives business success.

Because the need to protect, access, and trust systems and data is so critical to organizations, we fielded a survey on High Availability and Disaster Recovery. We wanted to discover what kinds of protection schemes companies use, how they define their recovery metrics, and what their plans are for the future. 1,730 professionals responded, evidence that HA/DR is a topic that resonates deeply with them.

Professionals Identify Data Protection Technologies in Use

In recent years, new architectures and technologies on the scene have revolutionized the way IT departments approach loss prevention, business continuity, and recovery. Protection technologies have evolved rapidly, including advances in performance and cost of ownership. At the same time, IT professionals can choose from a wide array of technologies, from cloud-based recovery to real-time replication, along with legacy technologies, such as tape. For all these reasons, we asked respondents about the protection and archiving schemes they used.

2017 results show that hardware/storage replication is used by the majority of organizations, followed by tape backup, and software/ logical replication, as shown in the graph.

The top choice of hardware/storage replication presents intriguing challenges to IT departments. Hardware/storage-based replication is perceived by some industry analysts as easier to implement, yet more difficult for IT users to integrate overall, because it is dependent upon a particular vendor's brand of hardware. Moreover, it may be less scalable in the case of high-volume data growth in a production application, and there can be single points of failure inherent in some of these configurations.

Results also showed that tape backup is not going the way of the dinosaur, despite its slower recovery time and operational complexity. Still, with the data explosion in so many companies, a legacy solution like tape requires careful management. Reviewing data protection technologies by company size, we saw that the largest companies tended to use tape more than mid-sized or smaller ones. It's possible that the largest companies continue to use tape for archiving and other technologies for protection.

Software/logical replication was the third most common choice—a technology that offers significant benefits and protection to IT departments. Replication software maintains exact duplicates of a system's object in real-time or near real-time. Business agility increases because information is available at any time for analysis. And if disaster strikes, replication servers at remote sites can keep the business's doors open.

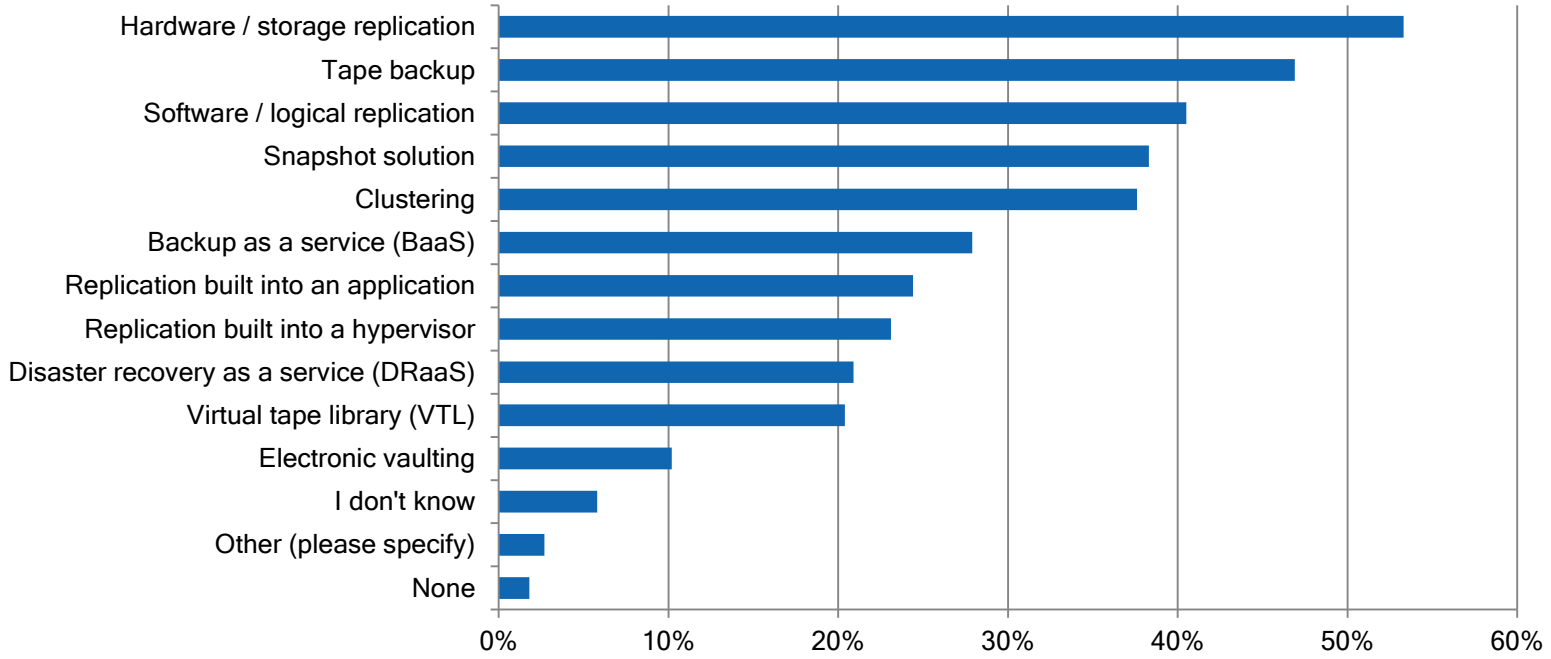
This year's findings also show that there's not a single, all-purpose protection solution used to cover all scenarios. Many companies use between 1 to 3 protection schemes, and more than a quarter use 4 to 6. Companies must make deliberate decisions about recovery, based on their business models, budgets, and systems to be protected. We found that the average number of data protection technologies increases with company size: Those companies with 1 to 10 employees use roughly 2 technologies, and those with more than 1,000 employees use more than 4. Evidently, the largest businesses have more complex environments and greater resources for purchasing and managing diverse protection technologies.

IBM Power Insight

Among IBM Power users, tape is the predominant protection and/or archiving technology (71%), followed by software/logical replication (53%), and hardware/ storage replication (51%).

One possible explanation for the high use of tape: When IBM-based businesses purchase servers, those tend to be bundled with components that commonly include tape backup.

Which of the following technologies does your company currently use for data protection and/or archiving? Select all that apply.

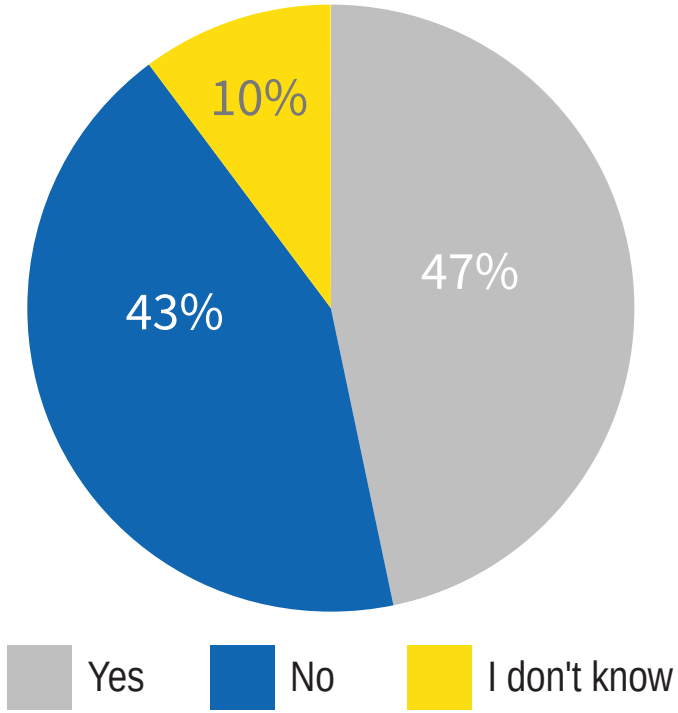


Shortcomings: Failures, Data Loss, RTO, and RPO

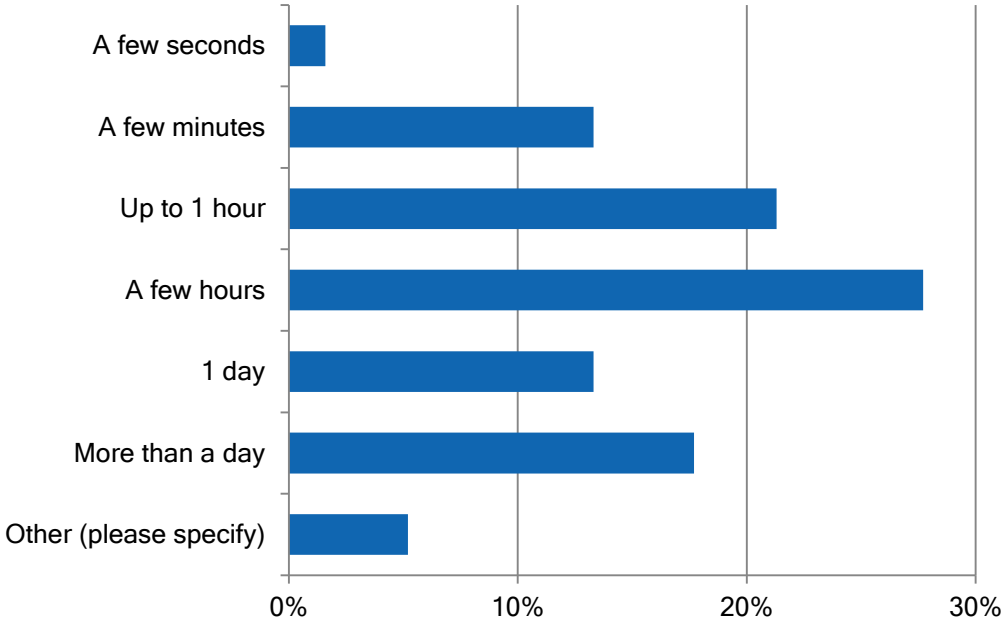
Continuing our analysis of recovery capabilities, we asked professionals about failures, downtime, data loss, recovery time objectives (RTOs), and recovery point objectives (RPOs). [2]

Findings revealed that nearly half of businesses experienced a failure that required use of an HA/DR solution to resume operations—shown in the graph. Within that group, more than a third lost data, and not a trivial amount. For those who lost data, 35% lost between a few minutes and an hour of data. Another 28% lost a few hours, and 31% lost a day or more of data.

Has your organization ever experienced a failure (including natural disaster, server failure, storage failure, application failure, human error, etc.) that required use of your HA/DR solution to resume operations?



Expressed in time, how much data was lost in your most significant incident?



[2] In the survey, the RTO question focused on the maximum tolerable length of time set for recovery of a company's most critical systems and data after an outage. The RPO question focused on the maximum acceptable tolerance for loss of critical data and transactions, expressed in time.

Data Loss: Old Backup Copies the Chief Issue

Then, we wanted to understand the causes of data loss, so we gave respondents nine different reasons from which to choose. The most common reason for loss was old backup copies (data was created or changed since the last backup), followed by human error, as shown in the following graph. In fact, five of the reasons for data loss relate to the lack of good quality backup copies. Quality and operational issues seem to be the primary reasons data is lost. Perhaps those companies lack the software to provide real-time backup to a secondary site, do not have sound backup procedures, or staff was simply careless in making or storing backup copies. Yet, the question remains: Is there group ownership for data loss, individual accountability, or answerability up the chain of command? Data loss certainly impacts an entire company—not just the IT organization.

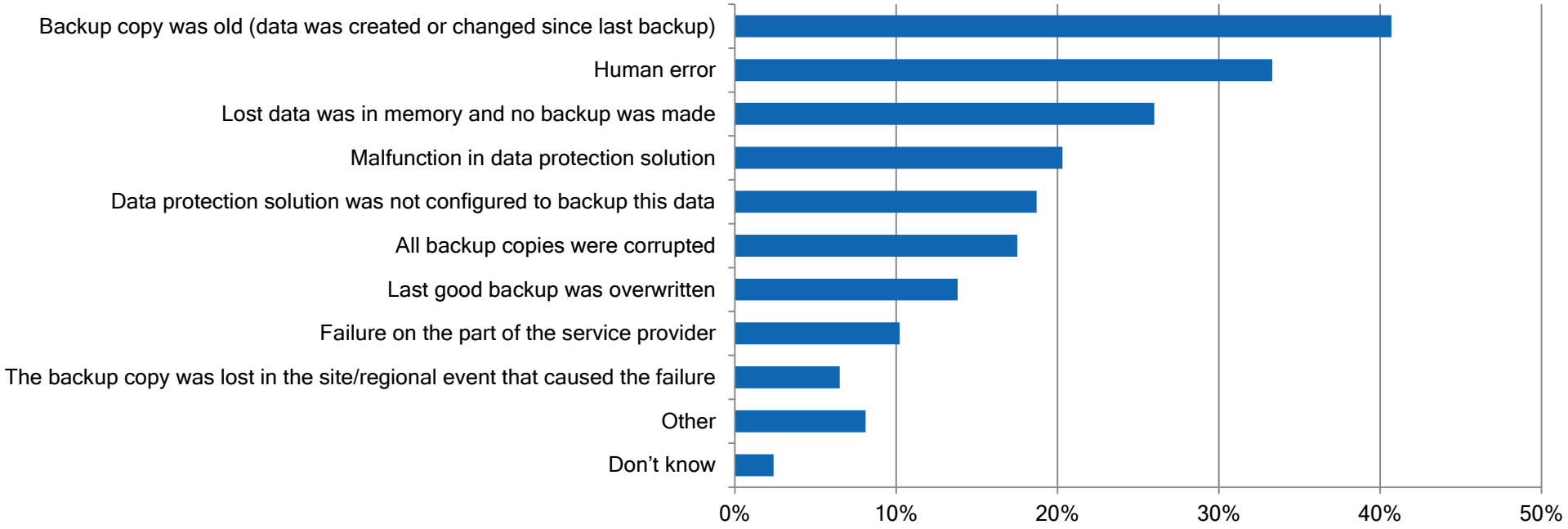
Fast Facts

Who is managing HA/DR?

- 82% of respondents use internal staff.
- 27% use third party consulting services.
- 20% use Cloud or managed services provider.

Yet only 16% plan additional staff training within the coming year.

What were the primary reasons that data was lost? Select all that apply.



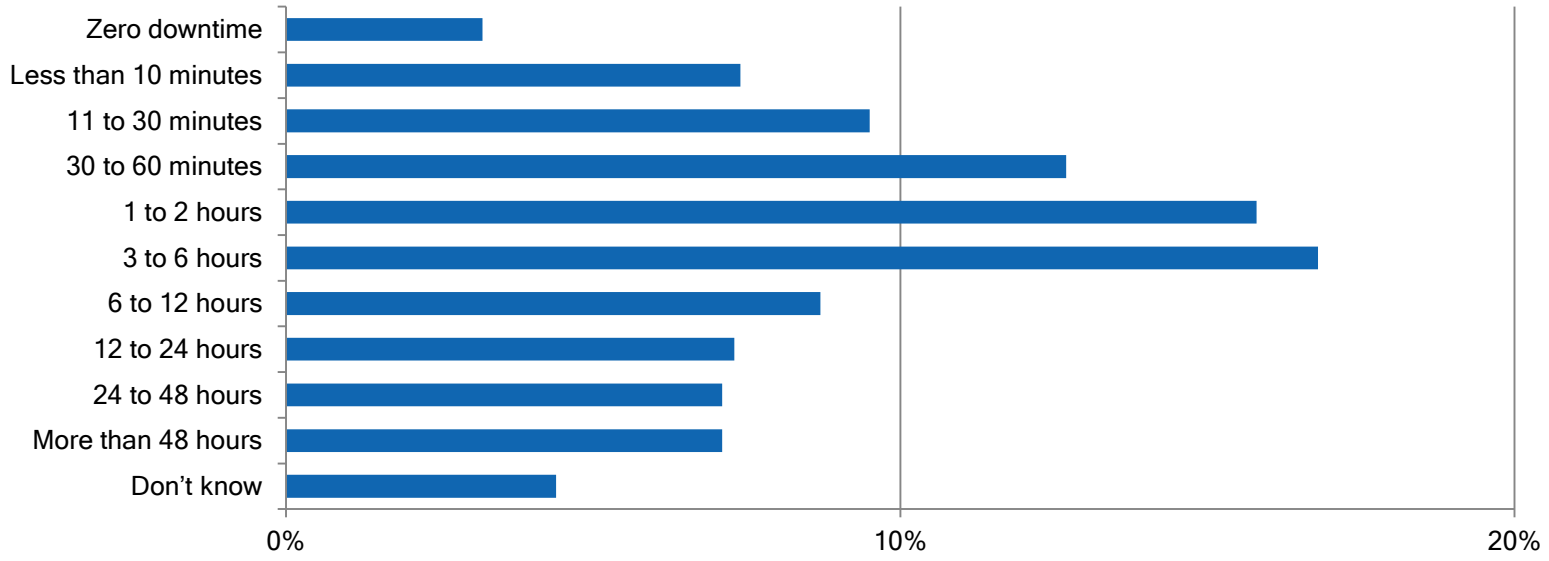
How Much Downtime Did Businesses Experience?

Then we examined survey findings concerning downtime after a failure. Of those companies that had to use an HA/DR solution to restart their systems, nearly half (45%) had a recovery time between 30 minutes and 6 hours. Only 3% experienced zero downtime, as shown in the graph.

Is there a relationship between downtime and company size? We found that the average downtime for companies between 11 and 1,000 employees was 8 hours. Still another result was surprising: The smallest companies (less than 11 employees) and the largest companies (more than 1,000 employees) had average downtimes of 11 hours--at least three hours longer than moderately sized organizations. One interpretation is that the largest organizations naturally have more complex recovery environments, including servers, software, and hundreds of components such as cooling and power; the smallest businesses might have less efficient recovery systems.

This finding bears more consideration, because small and large businesses alike can be affected by downtime: In a small business, downtime could drive customers to seek out the competition, affecting the bottom line. For larger online retailers, government agencies, medical institutions, airlines, and brokerage firms, a few hours of unplanned downtime are nothing less than catastrophic. The global economy, and indeed national security, healthcare, and finance, are dependent upon continuous access to enterprise systems: Even a few seconds of downtime can have severe consequences for citizens, consumers, and businesses.

In the previous question, you stated that your organization had experienced a failure that required use of your HA/DR solution. What was the recovery time for your longest downtime incident?



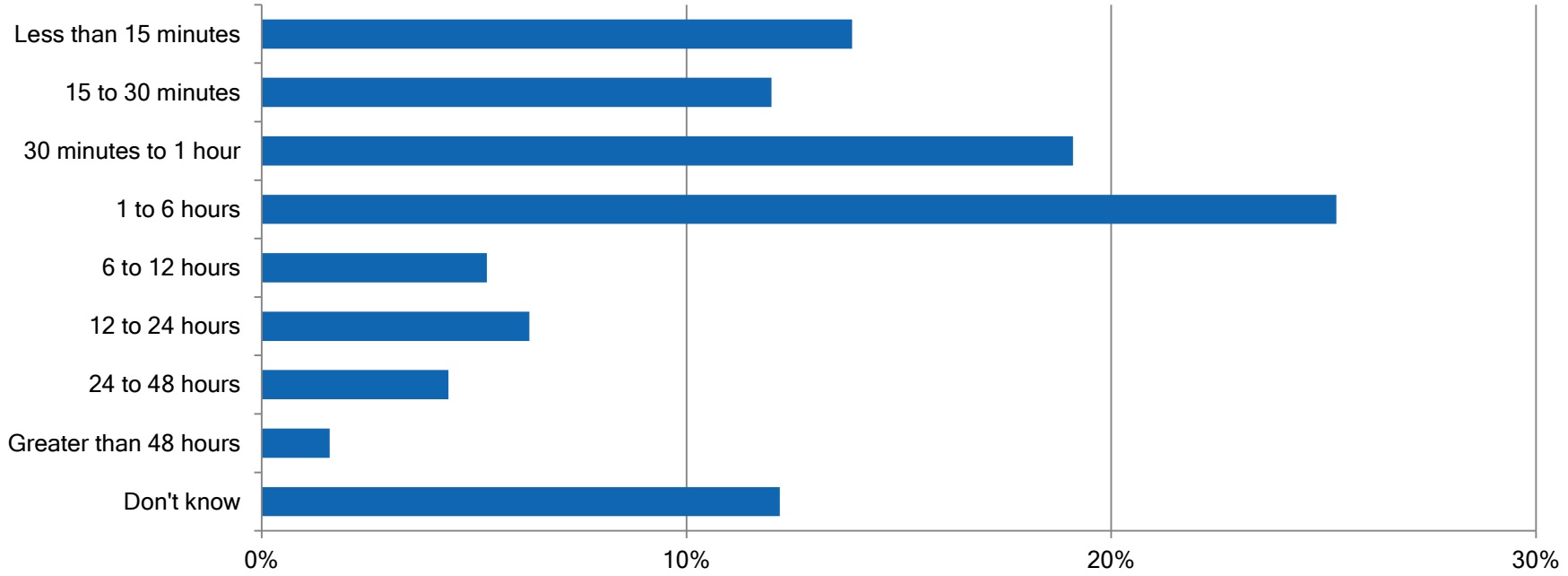
RTOs: Are Companies Meeting Them?

The survey findings on downtime led us to analyze businesses' RTOs. As the graph shows, 45% had an RTO of an hour or less for mission-critical systems and data after a disaster or a complete server or application failure. 26% had recovery times of less than 30 minutes.

Yet we wondered: Are businesses meeting their RTOs? To answer this question, we cross tabulated data between companies' RTOs and their actual recovery times after a failure. The findings were troubling: Roughly half of respondents met their RTOs and half did not.

A possible explanation for this result is as follows: A considerable majority of IT departments are using internal staff for HA/DR management, but training is not high on the agendas of most companies. In addition, 39% will not change staffing levels in 1 – 2 years, and only 27% plan to increase internal staffing. At the same time, 41% lost data due to outdated backup copies, and 33% lost it as a result of human error. When taken together, these results indicate that accelerated staff training and staffing resources are critical to ensuring resilience in recovery times.

What is your company's recovery time objective (RTO) for your most critical systems and data after an outage (storage failure, server failure, regional disaster, etc.)?



RPOs Are Stringent

Naturally, the findings about RTOs led us to analyze businesses' RPOs for critical data and transactions. We found that RPOs are fairly stringent: nearly a quarter had an RPO of no data loss; 43% of respondents had an RPO of a few minutes or less, as shown in the graph.

These numbers, however, don't tell the whole story. We cross tabulated the findings about RPOs with actual data loss. Intriguingly, we found that the majority of companies are meeting or exceeding their RPO objectives (74%).

Still, a smaller number of companies (26%) did NOT meet their RPO objectives. Of those that had an RPO of no data loss and experienced a failure, 39% actually lost from a few seconds to more than a day.

Industry Insight

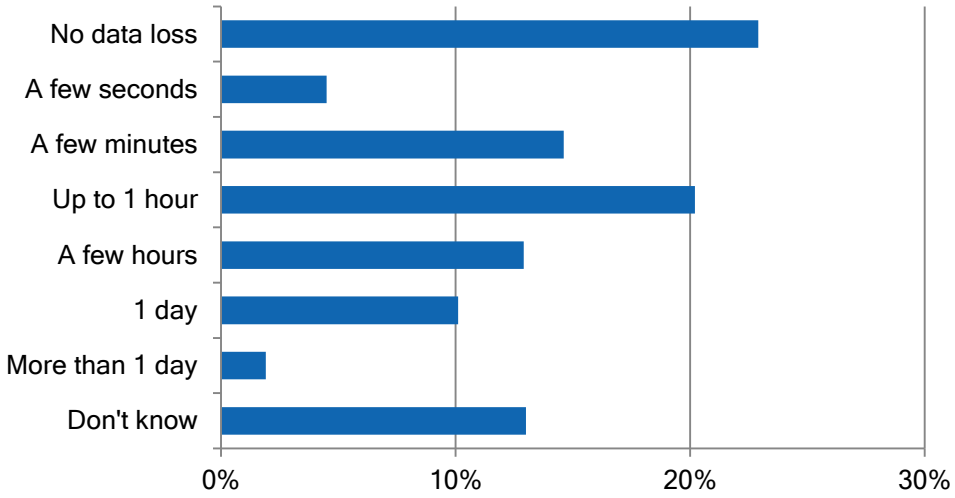
Time is Money, Downtime is Costly

The most expensive cost of an unplanned outage is over $17,000 per minute. On average, the cost of an unplanned outage per minute is nearly $9,000 per incident.

Source: Ponemon Institute Research Report, sponsored by Emerson Network Power, 2016. Numbers were computed from 63 data centers.

RPO metrics are the standards by which businesses measure their tolerance for data loss. If companies set the RPO standard at zero data loss, then professionals must be prepared to deliver on this promise—and be equipped with the tools and resources needed to recover rapidly. Otherwise, zero data loss is not a practical or realistic goal. IT professionals can bridge the gap between reality and expectations by revisiting their recovery plans after an incident to determine appropriate RPOs for different types of disaster scenarios.

What is your company's recovery point objective (RPO) for critical data and transactions, expressed in time? In other words, how many minutes or hours' worth of lost data is acceptable to your organization in the event of an outage or failure?

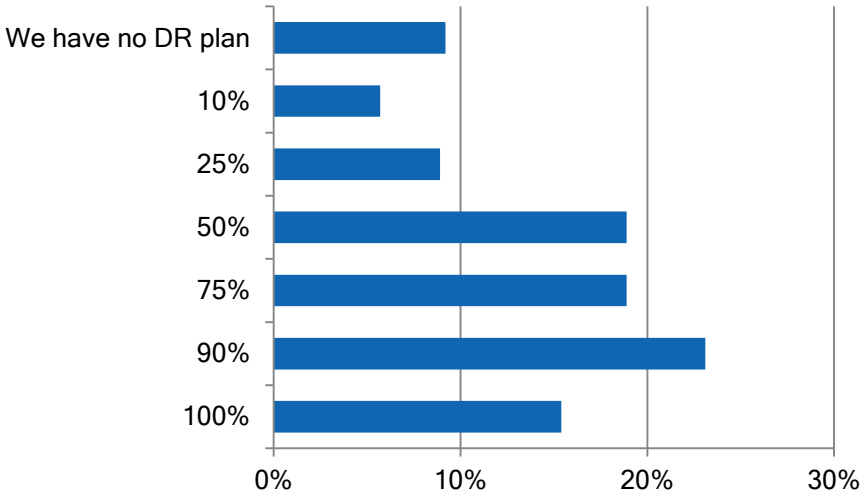


Recovery Plan Confidence Low, Some without Plans

Survey results revealed that most professionals lack confidence that their recovery plans are complete, tested, and able to meet RTOs and RPOs. In total, 85% of professionals had no recovery plan or were less than 100% confident in their plan.

This lack of confidence might be linked to companies' schedules for testing recovery plans. In another survey question, we asked respondents how often they test their plans. Nearly a third said they test once a year. Yet, an annual schedule for testing might not be sufficient in many data center environments where software and hardware change quickly. Thus, within a quarter's time, test plans may no longer be valid. This is particularly true, as professionals in Vision's Security Survey noted rapidly evolving threats to data integrity, privacy, and uptime.

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?

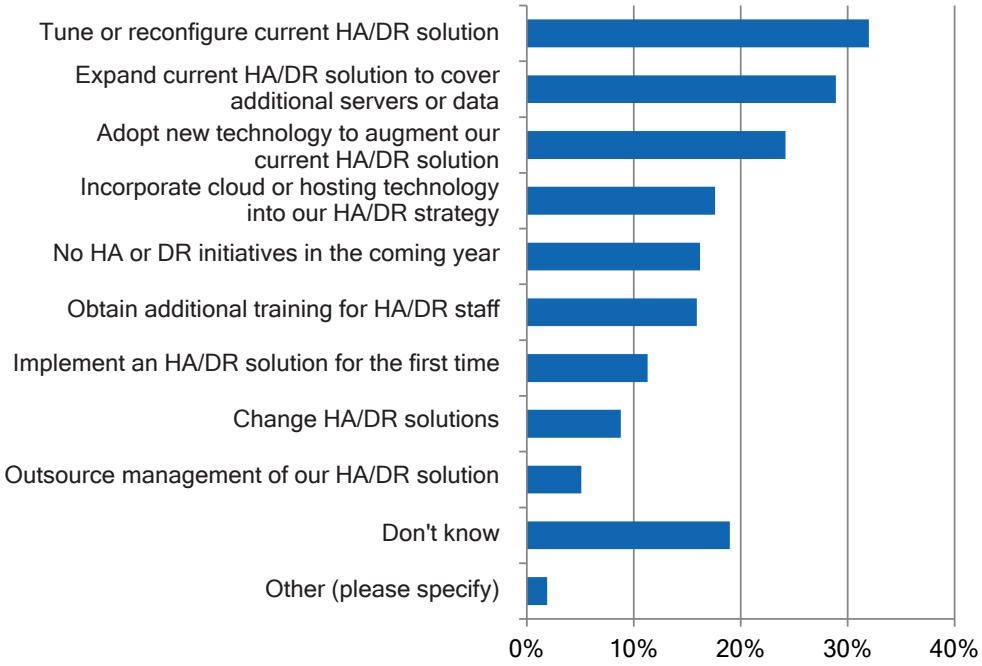


Top HA/DR Initiatives in the Coming Year

Previous discussions on the IT trends survey revealed that business continuity and the ability to recover from disaster were the leading issues for professionals in the coming year. But are companies aggressive in addressing these issues?

Results showed that a majority of respondents (82%) indicated they had HA/DR initiatives planned for the coming year. As illustrated in the graph, top initiatives were: tuning or reconfiguring the current solution (32%), expanding the current HA/DR solution to cover more servers or data (29%), and adopting new HA/DR technology to augment the current solution (24%). Consistent with other survey results regarding the tendency to use internal staff, the lowest response was to outsource HA/DR management at 5%.

What initiatives does your business have regarding high availability or disaster recovery solutions in the coming year? Select all that apply.



Key Takeaway:

The survey showed mixed results regarding companies' HA/DR environments. A considerable majority (82%) are moving ahead with HA/DR initiatives for the coming year. However, findings indicate that the plans and solutions of many companies require re-evaluation. Many businesses still cling to older technologies, such as tape, for protection and archiving. Moreover, almost half of companies that experienced failure are not meeting their RTOs. Clearly, businesses must focus more intently on staff resources and training, given that flawed processes and human error are the main causes of data loss.


The State of IT Security

The State of IT Security

Recently there's been a perfect storm in the media, government, and corporations surrounding cyber security—the actions of malevolent criminals who have opened doors to data breaches, identity theft, and ransomware. Certainly, cybersecurity in these times can seem like unknown territory, an uncharted, dark space filled with unseen dangers. Against this backdrop of well-publicized, evolving threats, we wondered: What types of investments in security are companies making? Are they meeting their metrics for detection and response? And what do they perceive as major challenges? The following results of our IT Security Survey address these questions and more.[3]

The New Frontier of Risk: Top Security Challenges

Professionals noted that their chief security challenges in the coming year are the adoption of cloud services (43%), sophistication of attacks (37%), and ransomware (35%), as illustrated in the graph.

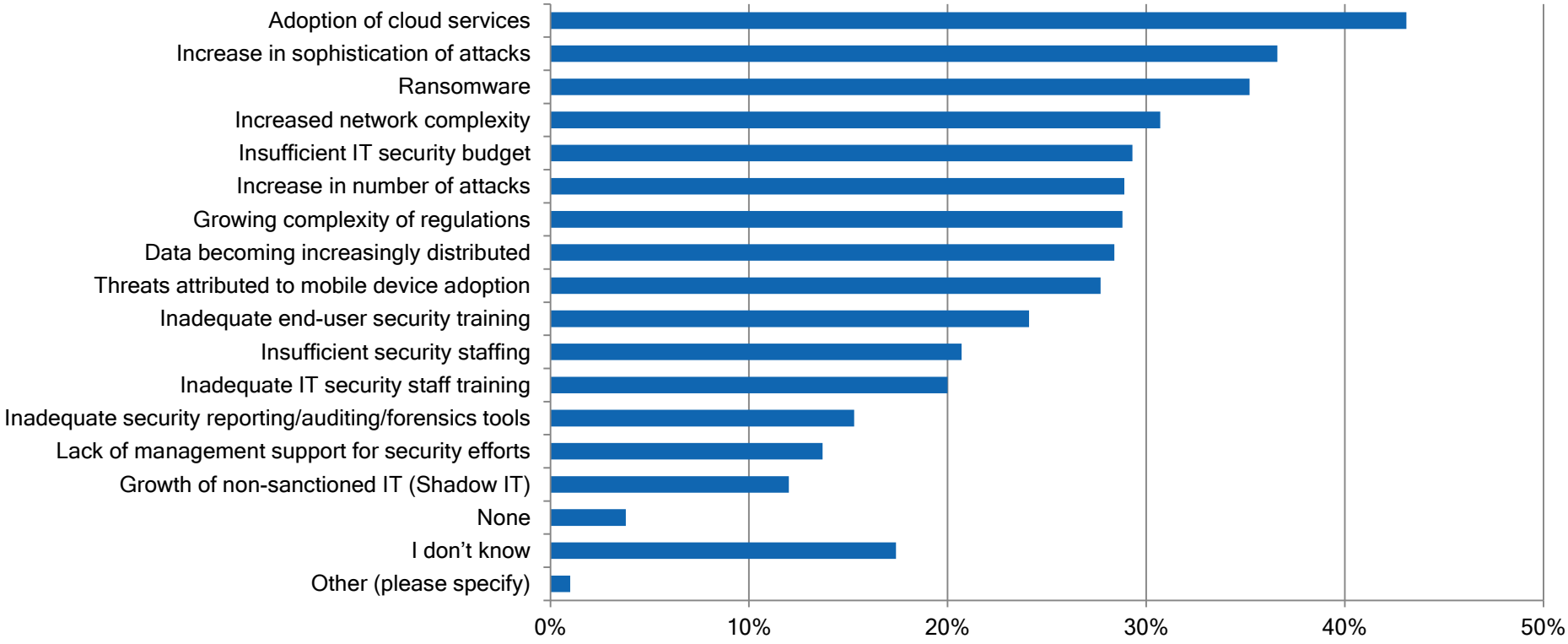
Cloud has been a transformative technology for businesses, yet IT professionals cite it as their greatest security concern. Certainly, the shared resource pools and "always on" features of cloud have introduced the possibility of new security breaches--including data loss, weak identity management, insecure APIs, denial of service attacks, account hijacking, and advanced persistent attacks, which infiltrate systems over a period of time.[4]

The #2 security challenge professionals said they face is the increased sophistication of attacks. This concern is well-founded: Cunning criminals have sharpened their craft, conducting exploratory raids over months, invading systems, hiding their tracks, and deploying malware that can fool customers with bogus messages or extract and steal valuable data—the lifeblood of most companies.[5]

Ransomware appeared as the #3 challenge confronting respondents. IT professionals are naturally aware of this phenomenon, as a result of worldwide media coverage. Yet, a considerable majority of professionals in this study had never been attacked by ransomware or were not aware that they had been; a miniscule number had paid to get data back, as mentioned in a subsequent section of this report. It remains to be seen whether ransomware is the "flavor of the moment," or will be a recurring trend.

[3] This section includes excerpts from Vision Solutions' IT Security survey. Please refer to the 2017 whitepaper, The State of IT Security: A Report from the Front Lines, for a comprehensive review of the survey results.
[4] "The Treacherous Twelve Top Cloud Computing Threats of 2016." Cloud Security Alliance, an industry not-for-profit that maintains working groups on cloud security and promotes cloud education. Clousecurityalliance.org.
[5] A notable example of scale and sophistication was the theft of $81 million USD from the Bank of Bangladesh in 2016, when criminals altered transaction records. "Cyberthreats are evolving –and so must your defenses." Ernst and Young, 2016

What security challenges does your IT organization anticipate in the coming year? Choose all that apply.



Today's Leading Four Investments in Security

As shown in the graph, the majority of professionals chose virus protection (71%), malware protection (67%), patch management (53%), and intrusion detection and prevention (52%) as their top organizational investments in security today.

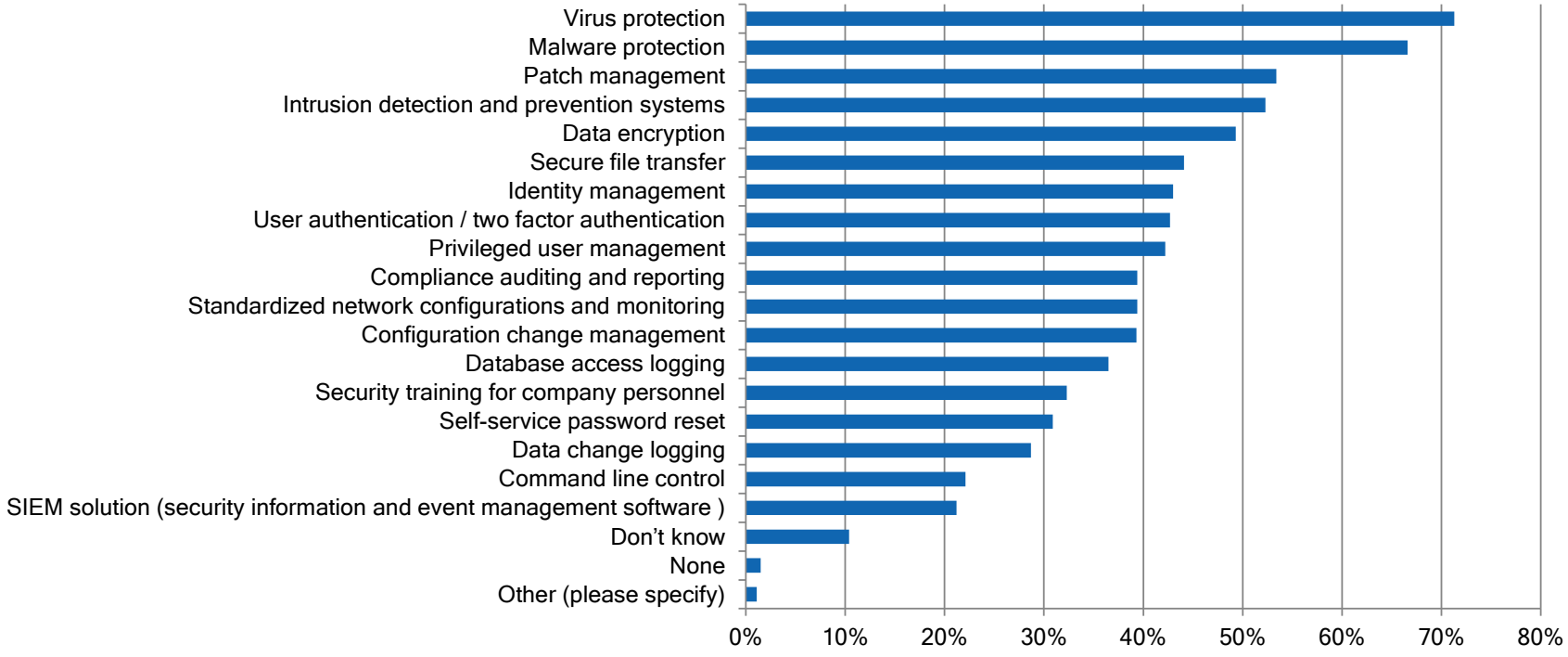
This is not really news: Security architecture starts with protection and prevention, basic monitoring, managing vulnerabilities, and updating security software. Virus protection and malware protection are the basics of corporate security. Patch management supports intrusion prevention; hundreds of patches might be available for complex IT systems, and professionals must prioritize the need for security controls on each.

What we did find intriguing, however, is that all other investments received less than 50% response, including items such as secure file transfer, database access logging, identity management, privileged user management, and security training for company personnel (later noted as a high priority for professionals). Findings suggest that some businesses may not be taking full advantage of the wide range of security technologies available—and may not have layers of cybersecurity controls in place.

Fast Facts

Who's Minding Security in the Shop?
88% of companies use in-house staff for security. Yet only about a third have invested in training for company personnel.

What security measures has your organization invested in today? Choose all that apply.



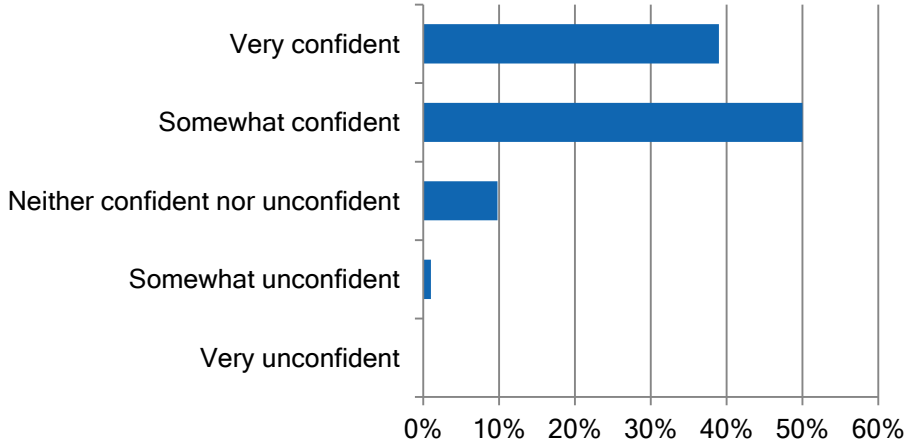
IT Professionals: Assurance or Overconfidence? Results Are Mixed

The survey showed that IT professionals' confidence in security programs is high. Of those who had formal security programs in place, 89% were either somewhat confident or very confident in their programs' effectiveness, shown in the graph.

Then we asked all respondents whether they had experienced a breach in the past year. The majority (61%) reported that they have not experienced a security breach in the past year. Only 12% had experienced a single breach, and 9% had multiple breaches.

When we took a closer look at the data, however, the findings were troubling. Of those that experienced breaches, 67% experienced downtime and almost a third were down for an hour or more. So although a small number experienced breaches, a considerable majority of those did not meet their recovery objectives.

How confident are you in the effectiveness of your organization's security program?



Case in Point

The Exorbitant Cost of Breaches

The global container shipping giant, A.P. Moller Maersk, estimated that its loss from a June 2017 cyberattack would range between $200 and $300 million (USD). The company took two days to get back on track following the breach, and business volumes were negatively affected for a couple of weeks.

Source: CNBC, August 16, 2017, Interview with CEO, A.P. Moller Maersk

Fast Facts

Missed Metrics
Of those who had breaches, only 37% met their mean time to resolution, 35% met their mean time to response, and 33% met their mean time to detection. Only 14% met all their metrics. 16% do not have metrics.

Ransomware: Hype or Reality?

Despite the buzz about ransomware in industry media, we were surprised to discover that nearly three-quarters of respondents had not been victimized by ransomware or were unaware that they had been. Paying for ransomware was also a rare event: Only 3% of respondents indicated a dollar payment for ransomware. Nonetheless, many analyst and security groups—and survey respondents --regard ransomware as a credible threat. One of the best ways for any company to avoid being a victim of ransomware is to invest in solid recovery and backup systems that will provide up-to-date, clean copies of data.

How Often Do Companies Audit?

It's good news that nearly two-thirds of companies in the study perform security audits on their systems. Yet digging deeper, we discovered that for those who perform audits, the most common schedule was annual (39%), and another 10% audit every 2 years or more. Annual auditing schedules imply that many professionals trust that nothing has changed in the infrastructure or the environment over a year that could cause security to fail. Given an ever-changing IT environment, annual audits—or less frequent audits—could potentially expose a company to risk.

66% of IT systems are audited for security. Of these, 39% are audited annually.

IBM Power Insight

73% of IBM Power professionals had their systems audited for security. 42% audit once a year. This finding dovetails with a clear trend toward compliance among Power users: The majority will focus on compliance auditing and reporting as security investments in the coming year. In addition, IBM businesses in the survey were large: Nearly half had more than 1,000 employees. It's possible that these giants have rigorous auditing schedules and procedures designed to reduce the likelihood of breaches.

Meeting Security-Related Challenges

We wanted to know what kinds of measures or actions IT leaders thought would most help them address security challenges in their companies. Education heads the list of items that would most alleviate organizations' security issues. The top pick of the majority of professionals was "increased education on current security software, strategy, and policies in place."

Fast Facts

Education Tops Professionals' Wish List

56% of IT pros want increased education on current security software, strategy and policies in place.

47% ask for increased budget for security.

As mentioned previously, education is a vital element of protection and defense, particularly since companies rely heavily on IT staff for security. However, participants' responses show that education for IT staff alone isn't sufficient. Everyone in the corporation—from staff to line managers and executives—must support a sound strategy and company-wide policies. IT must work across the corporation to help develop a security-oriented culture.

Security initiatives: What's Ahead?

The survey asked participants "In what security measures will your organization invest in the coming year?" Their top-ranked responses (each above 30%) were:

- Malware protection (36%)
- Virus protection (34%)
- Intrusion detection and prevention (30%)

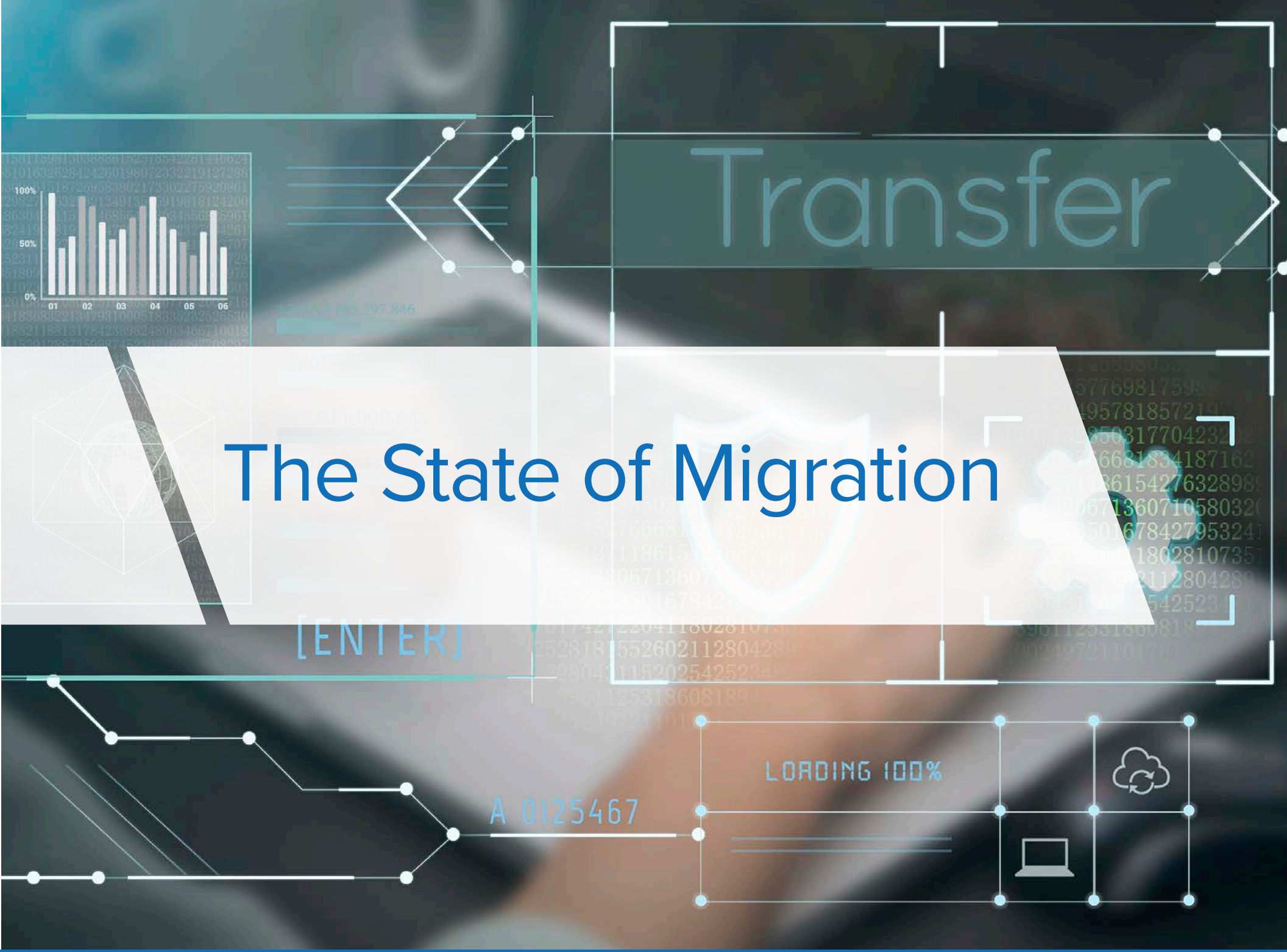
As discussed previously, businesses appear to be investing chiefly in fundamental applications and approaches—the basic underpinnings of security. Other planned investments, such as user authentication, identity management, secure file transfer, and security training for company personnel received less than 30% of the response. Again, these findings suggest that companies are not planning to leverage the full range of security tools available within the coming year.

Fast Facts

Perimeter defenses won't help if the company lacks a culture of security—education, policies, and support, from the bottom to top of the organization.

Key Takeaway:

Companies have made substantial investments in security; still, the landscape is evolving and demands constant vigilance–and more sophisticated tools and methods of protection. Survey results could be viewed as a glass-half-full or half-empty scenario, depending upon your perspective. Security audits are most commonly performed every year, though the environment changes rapidly and hackers develop increasingly sophisticated methods to exploit vulnerabilities. IT strategy must include more than just perimeter defenses: Results indicate that IT leaders must continually assess security practices, tools, and develop stringent policies for the entire corporation.



The State of Migration

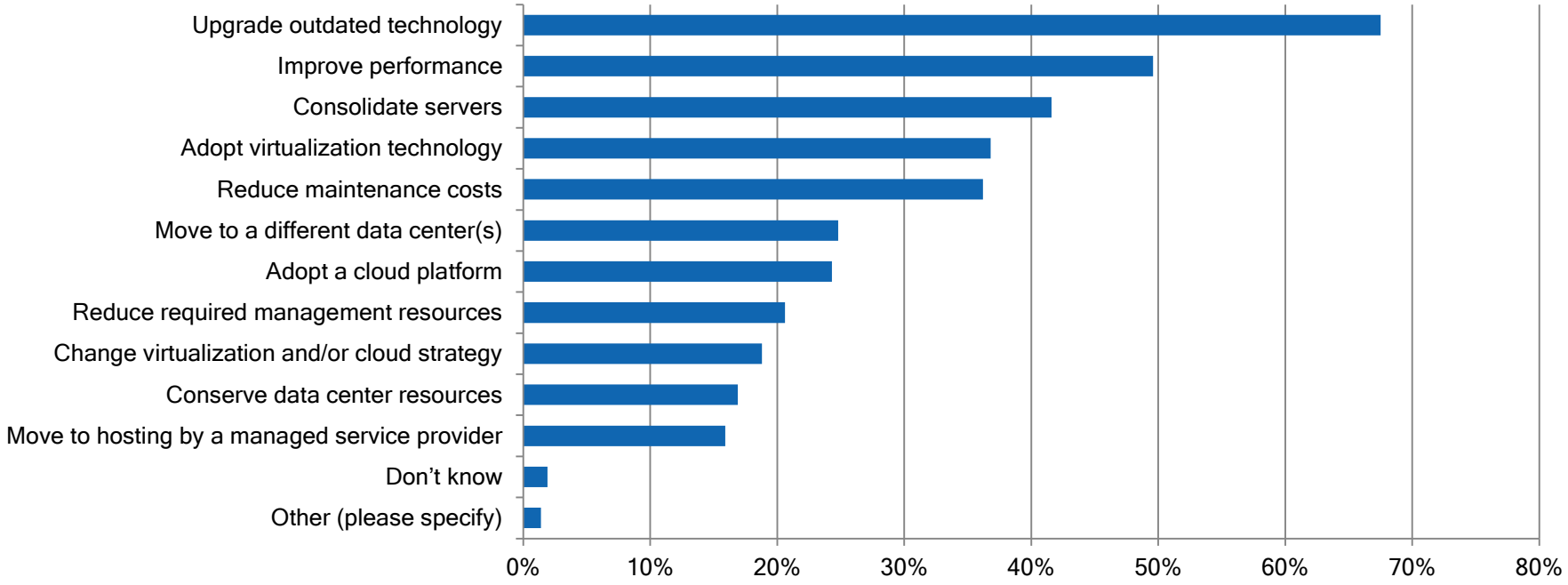
The State of Migration

Data overload, server consolidation, and concerns about system performance put pressure on IT professionals to adopt more efficient management practices and solutions. Organizations are grappling with the replacement of outdated systems, along with the need to migrate data to and from physical, virtual, and cloud platforms. At the same time, IT leaders must ensure that their teams have the expertise to handle this demanding work. In this year's State of Resilience, we posed questions about organizations' migration objectives and outcomes, including system downtime. Responses from more than 1,000 professionals provide a thorough story.

Top Three Drivers for Migration

At the outset of the survey, we wanted to determine organizations' objectives for migration. Findings showed that the majority migrate to upgrade outdated technology (68%). Half migrate to improve performance, followed by those that migrate to consolidate servers (42%).

What were the objectives for your organization's last migration? Please check all that apply.



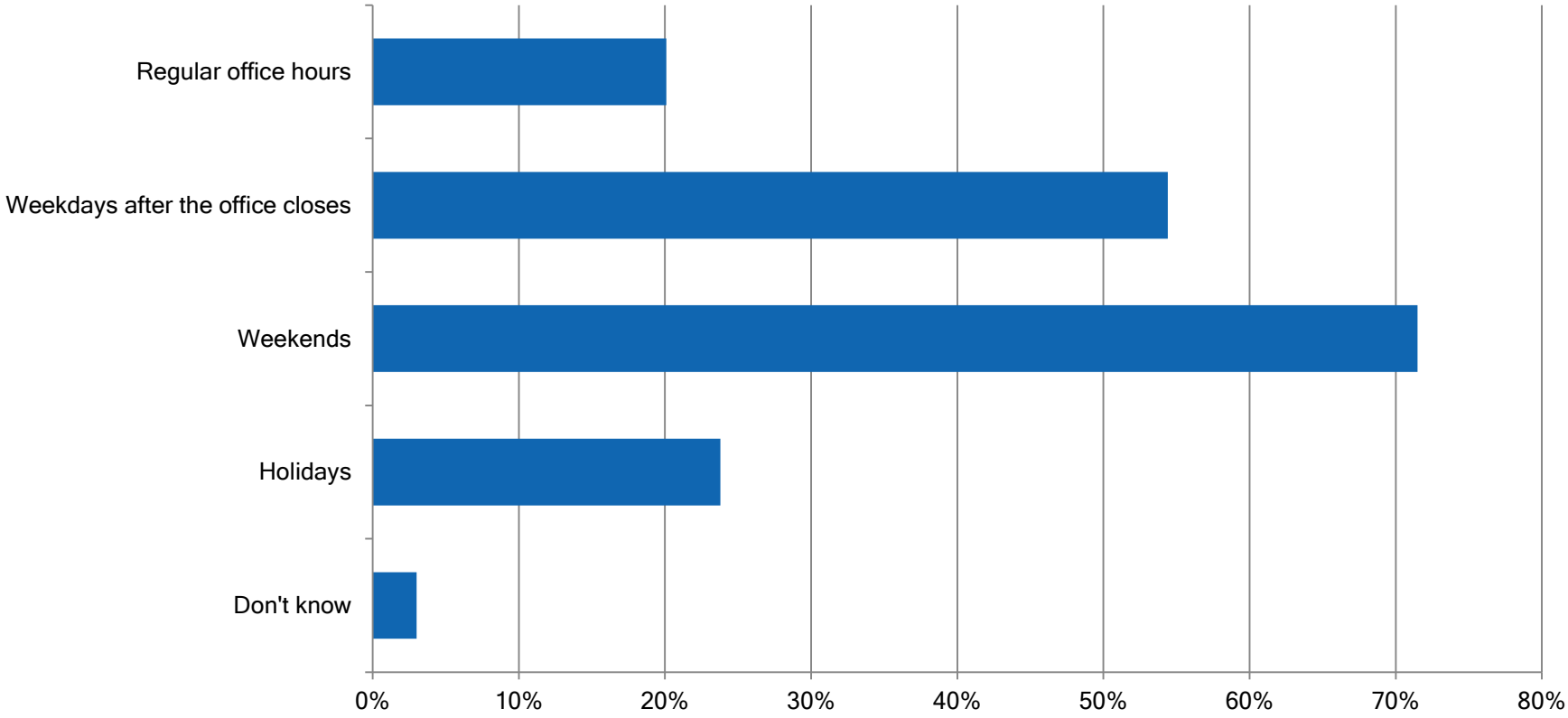
Migration: A Staffing, Scheduling Challenge

Because companies' three top migration goals demand significant planning and effort from IT professionals, we wanted to know how they staffed migration projects. We found that a vast majority (92%) use internal staff for migration. 50% use third party consulting services.

To get a more complete picture of the work involved, we asked: When are migration cutovers performed? The results were revealing. A remarkable 72% performed migrations on weekends, and 54% migrated on weekdays after the office closed. Only 20% performed migrations during office hours, illustrated in the graph.

Certainly, migration cutovers during off hours put pressure on internal staff, which can drain employee resources and damage morale. If third-party consultants are used, overtime expenses can add up.

When does your organization perform migration cutovers? Please check all that apply.

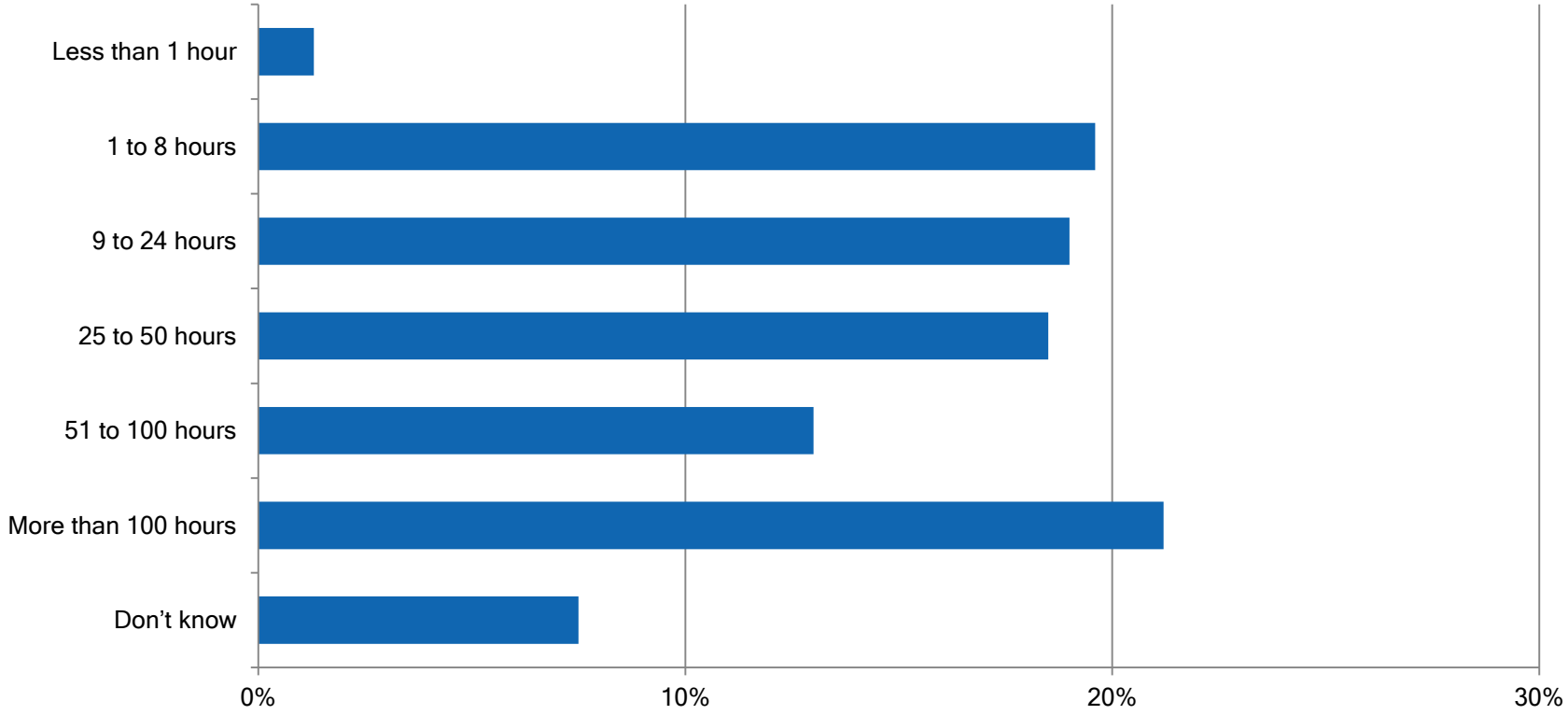


Migration Time: Not Trivial

Taking our inquiry a step further, we wanted to understand the average time needed for a migration, including planning, migration, testing, and cutover. As the graph shows, results regarding migration hours were fairly evenly split. Roughly 20% of respondents (each) selected the options from 1 to 50 hours or more than 100 hours.

Migration involves many different types of software and hardware assets, including databases, applications, servers, and operating system tables, to name a few. Naturally, the time required for a migration depends upon processor speeds, the type of asset being migrated, and in the case of servers, the hardware configuration. We observed that larger companies spend more time on migration than smaller ones, but both can reap significant benefits of state-of-the-art techniques. Updates to technology and cross-platform migrations can be more labor intensive, but the right tools can reduce time, complexity, and errors during the process.

For your last migration project, what was the average number of hours required to perform the entire migration project including planning, migration, testing and cutover?



Vulnerabilities: Migration Failures and Delays

Migration failures and delays are a threat to business resilience. When companies experience a migration failure or postpone a migration, system performance, productivity, and even revenues and reputation are at risk.

Migration Failures and Causes: Late Discovery of Issues, Inability to Restart Applications

As shown in the graph, many professionals had experienced a migration failure (42%). When a migration failed, the most common action they took was to delay the migration and attempt it at a later date.

Probing further, we discovered the two overarching reasons for migration failure:

- Late discovery of issues in the process (43%)
- The inability to restart applications (38%)

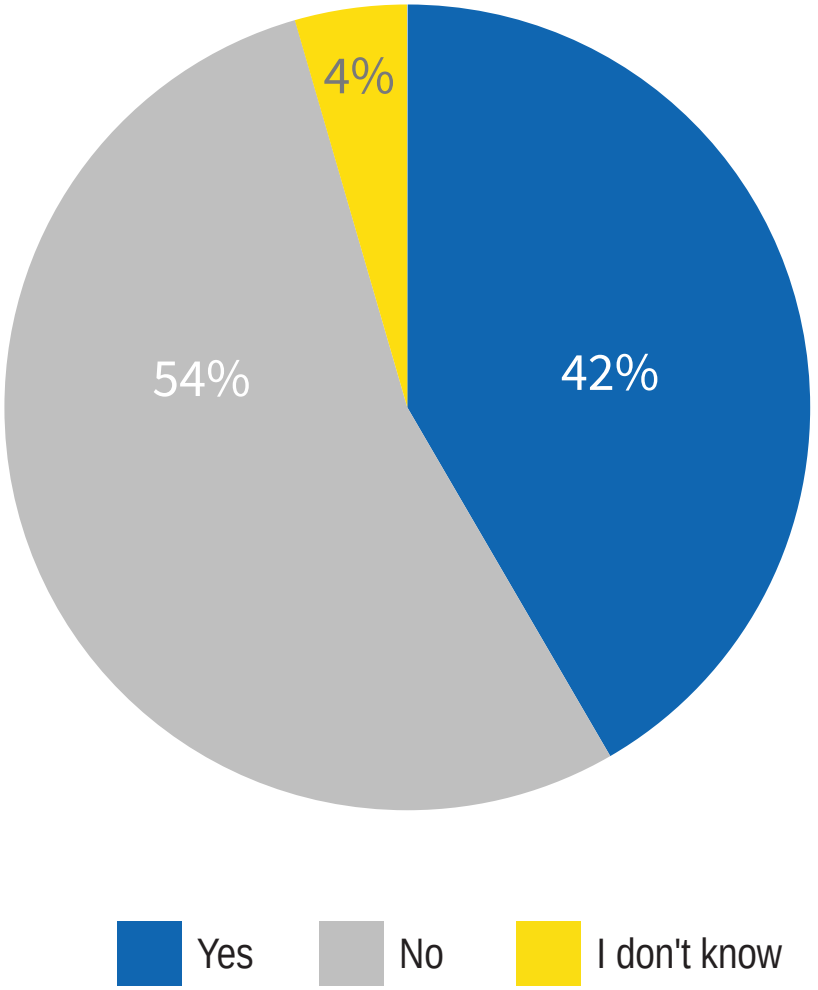
These findings point to a flawed early planning process, lack of preparation, or inadequate testing. Some organizations may not have configured the environment to ensure that applications run properly after migration. Although some migration failures can be attributed to sloppy procedures, it's likely that other human factors, such as training, play a part.

Fast Facts

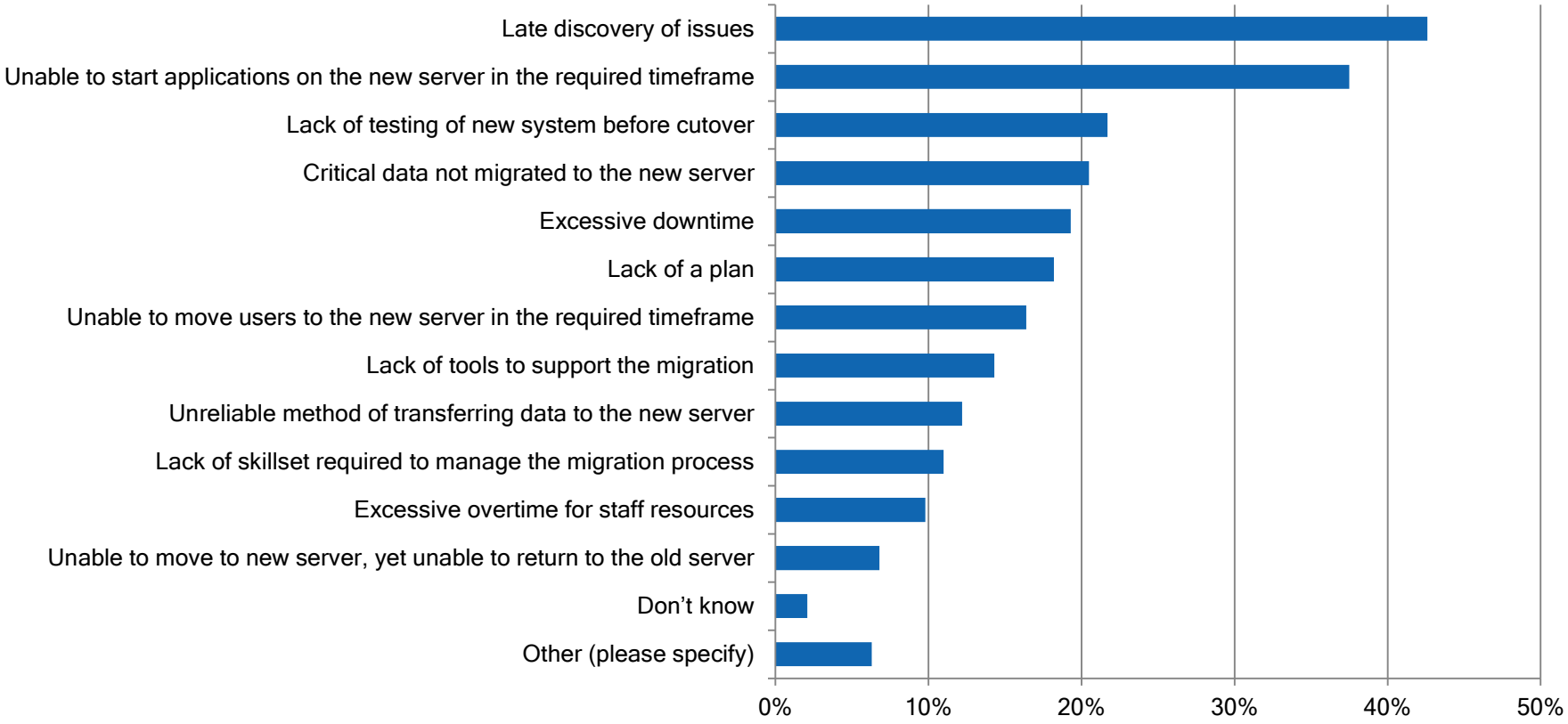
Zero Downtime Not a Reality for Most

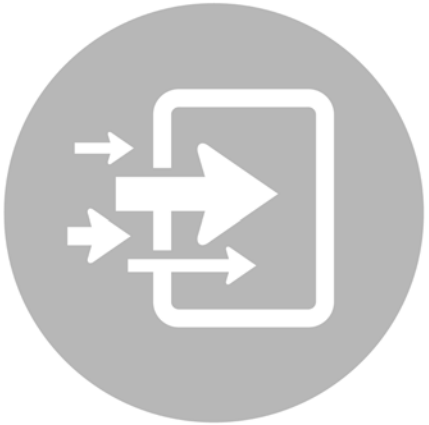
64% of professionals reported that their systems were actually down between 1 and 48 hours during their last migration. Nearly half noted that their systems were down between 1 and 12 hours.

Have you ever experienced a migration failure?



In the previous question, you indicated you had experienced a failed migration. What were the causes of that failure? Please check all that apply.





IBM Power Insight

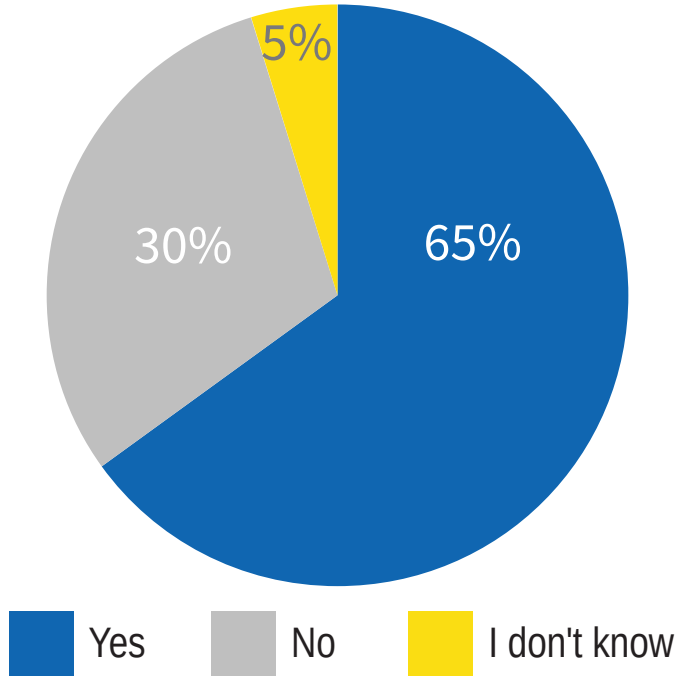
The majority of IBM Power users (66%) had not experienced a migration failure. 31% had. These systems are workhorses for high transaction processing applications in banking, finance, manufacturing, and retail. The consequence of failure in these industries is serious, so perhaps these organizations plan migration more carefully to avoid performance problems and higher costs.

Delayed Migration and Downtime Concerns

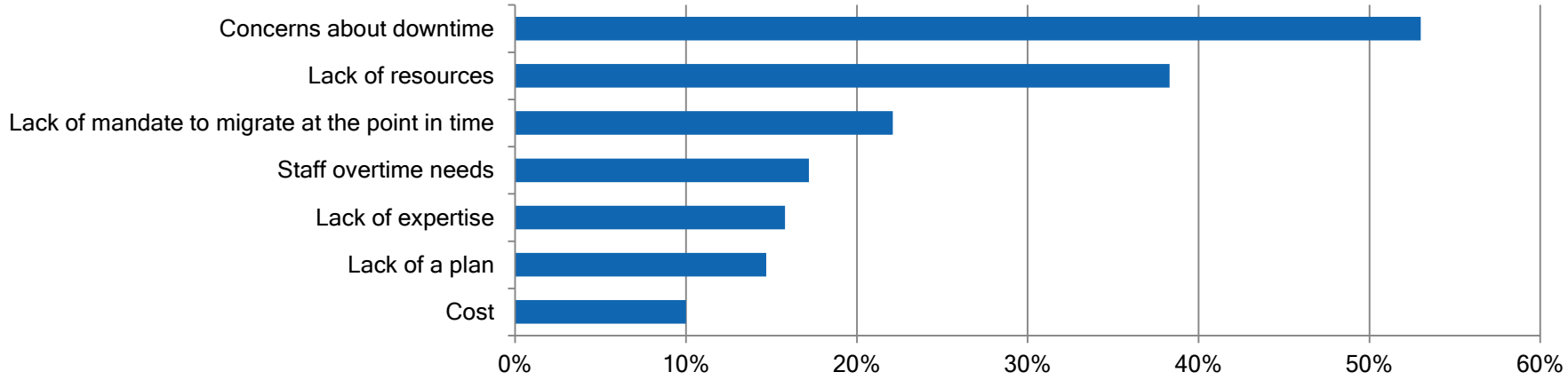
The findings about postponed migrations were more troubling. As the first graph shows, a substantial number of professionals--nearly two thirds--had delayed a migration. The second graph shows why this occurred: Concerns about downtime and lack of resources.

As discussed previously, a large number of organizations prefer to migrate after hours or on weekends, undoubtedly to mitigate risk or ensure system availability to users. Clearly, professionals are not assured that the migration process will go smoothly during peak system use. Though technologies are available to reduce downtime, we infer that professionals are not familiar with them or haven't implemented them yet.

Have you ever experienced delayed migration?

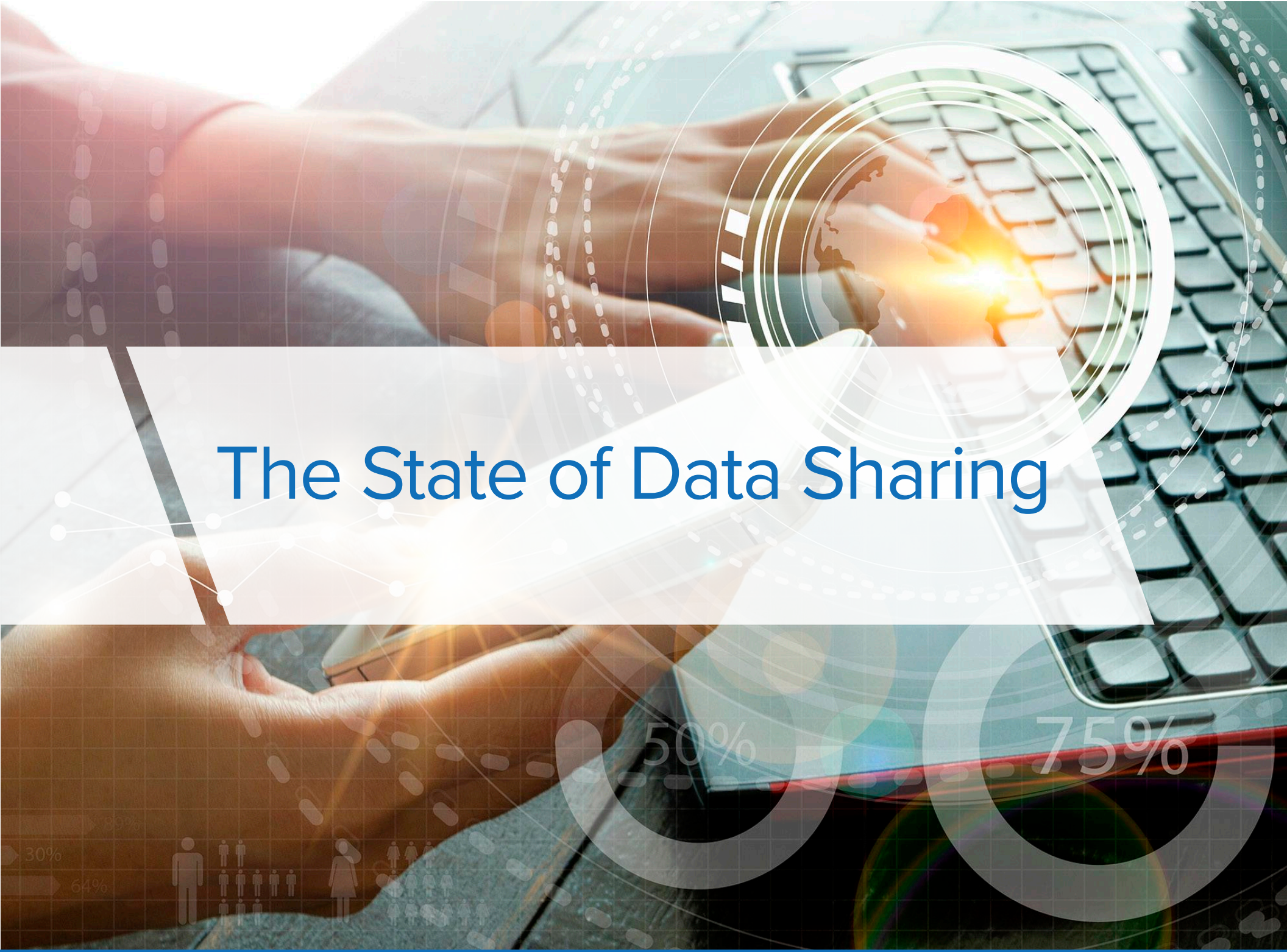


In the previous question you said that you had delayed a migration. What were the reasons for the delay? Please check all that apply.



Key Takeaway:

Migration is a process that demands closer attention. Results showed that organizations are not resilient or cutting-edge when it comes to migration practices. Why? Migration outcomes are not predictable. Delaying migrations is a common occurrence, a result of worries about downtime. Few organizations achieved zero-downtime during migrations. Because a majority of companies migrate to replace outdated hardware and software, potential business impacts of failure or delay can include performance issues and higher costs to run out-of-service-life systems. IT organizations can build greater resilience during migration by adopting tools, testing processes, and technologies that mitigate risk.



The State of Data Sharing

The State of Data Sharing

Data is a goldmine, a treasured source that can produce insights and competitive advantage for organizations. Executives, knowledge workers, doctors, and consumers rely on it as a basis for decision making, stock trades, diagnosis, flight bookings, and online retail purchases. Yet, data becomes a sinkhole if it is of poor quality. IT leaders today are charged with the tough task of ensuring that data is trusted, current, and correct, regardless of the source. That's why we wanted to learn about organizations' goals for sharing data, their methods, and their plans for future database initiatives.

A View of Data Sharing

To begin, we wanted a baseline of companies' database environments. How many were sharing databases? And what kinds of databases are they managing?

We found that 53% had multiple databases and share data, versus 23% that have databases but do not share data, as shown in the graph.

In highly diverse, heterogeneous environments, data sharing is a challenging task. Most businesses used Microsoft SQL Server (72%), followed by Oracle (42%) as databases. But a quick sampling showed a surprising mix of databases in some organizations: For example, Oracle and SAP in one; IBM DB2, Oracle, and Microsoft SQL Server in another; SQLite, IBM DB2, MySQL, and Microsoft SQL Server in yet another. Organizations are confronted with the complex work of having IT staff manage multiple database environments.[6] And when IT staff use older manual methods, synchronization is a burden and data accuracy can become a source of concern.

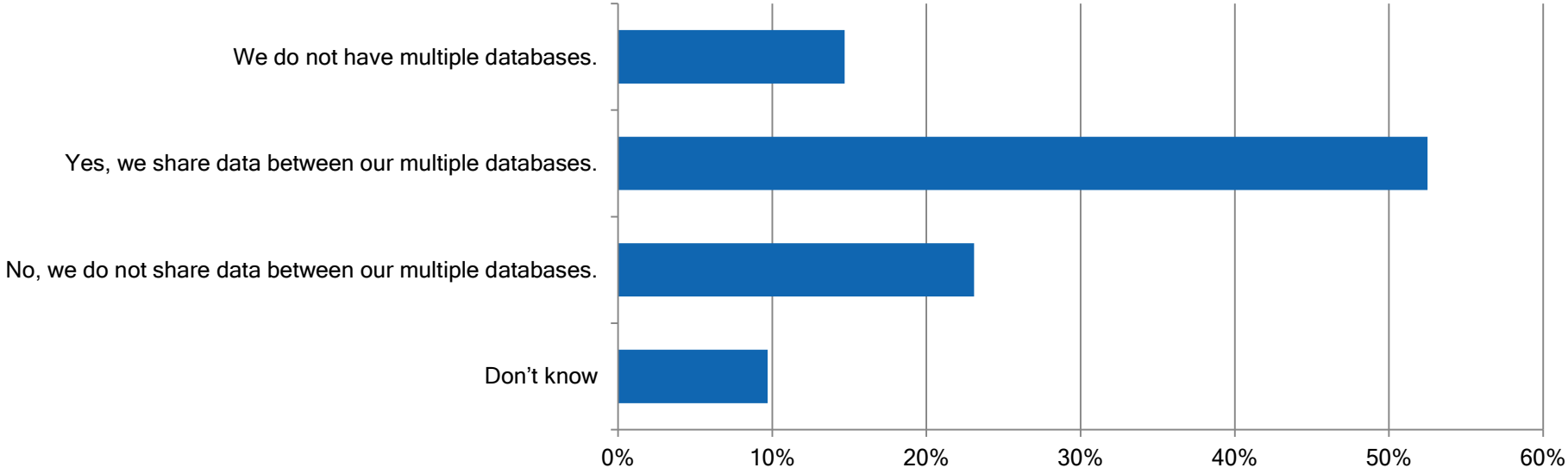
Industry Insight

Poor data quality costs the U.S. economy about $3.1 trillion per year.

Source: IBM Corporation estimate, Infographic, 2016.
http://www.ibmbigdatahub.com/sites/default/files/infographic_file/4-Vs-of-big-data.jpg

[6] 73% manage 2 or more database types. 54% manage 3 or more.

Does your organization share data between multiple databases?



How Global Giants Are Consolidating Really Big Data

Walmart, the world's biggest retailer, is in the process of building the world's largest private cloud to process 2.5 petabytes of data every hour, combining information from over 200 sources, including sales transactions, meteorological data, Nielsen ratings, gas prices, and local events.

Source: "Really Big Data at Walmart," Bernard Marr, Forbes Magazine, January 2017

Objectives for Data Sharing

What are the reasons organizations share data between databases?

Five reasons received 40% or more response:

1. BI or analytics on data offloaded from the production database
2. Synchronizing databases used by different applications
3. Reporting or performing queries on data offloaded from the production database
4. Consolidating data into a data warehouse
5. Administrative use, i.e. backup, testing, development

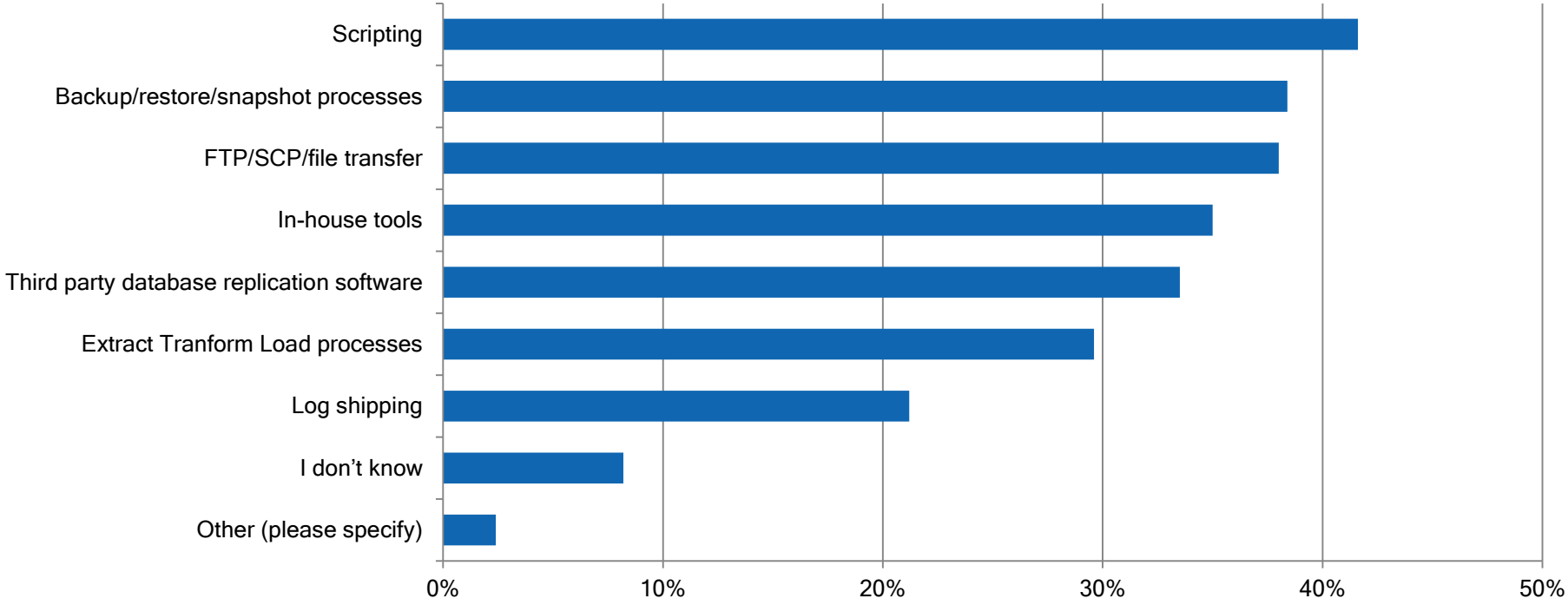
Because these goals for data sharing demand a fair amount of staff effort, we wondered what tools professionals use in their work—and whether they thought their techniques are effective.

Some Techniques for Data Sharing: Decades-Old

As shown in the graph, we found that the most common data sharing method was scripting (42%), followed by backup/restore/snapshot processes, and FTP/SCP/file transfer at 38% each. These data sharing methods come with cautions: Scripts can require development effort, testing, and maintenance, and when databases change, scripts must be retested. Backup/restore/snapshot processes can be fast and flexible, but they vary from vendor to vendor, and some variants can gobble up storage space. FTP and file transfers can be sluggish and vulnerable to error.

What's more, the data sharing process becomes exponentially more complex when companies use multiple methods to share data among databases. When we looked at the number of methods professionals used, we discovered that on average respondents used approximately 2 data sharing methods. Naturally, the number of methods increased with the size of the organization.

In the previous question, you indicated that your organization shares data between databases. What methods are used? Choose all that apply.



Clearly, every organization has unique requirements when it comes to choosing data sharing technology. Yet, a question remains: Some of the data sharing techniques IT organizations use are over 30 years old. Are technologists being hampered by using 20th century methods into the 21st century—the equivalent of using a buggy whip and cart, when a Tesla is called for? For this reason, we wondered about the impact of their data sharing methods on businesses.

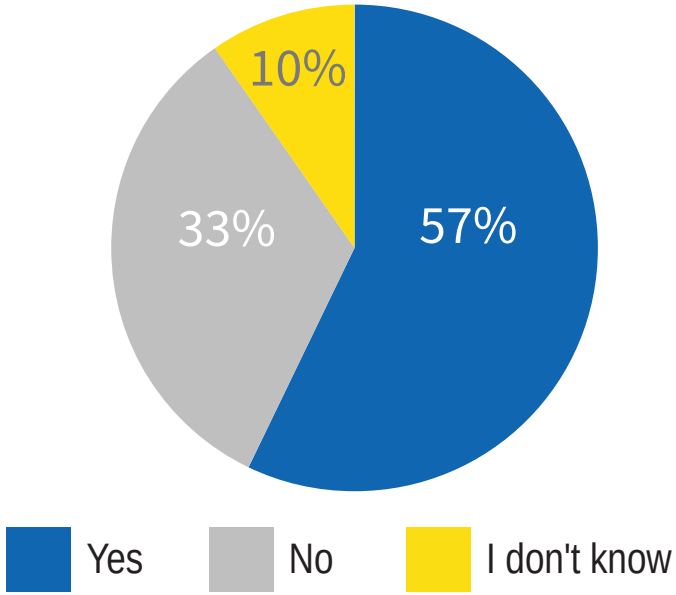
IBM Power Insight

Among IBM Power users, the most common method for sharing data between databases was FTP/SCP/file transfer (52%). This was followed by third party database replication software (42%). Only 29% use scripts.

Periodic or Real-time Transfer of Data: The Impact

We asked professionals whether their data sharing methods delivered changed data in real-time to the target database—or used periodic transfer of data. As shown in the graph, a majority of respondents indicated that their method updated the target database in real time (57%). 33% noted that their data sharing method did not.

Does your data sharing method deliver changed data to the target database in real time?



We probed further to learn whether periodic methods of delivering data had an impact on business decision making. Of those companies that use periodic transfer of data, rather than transfer in real-time, nearly half the respondents said this practice had no effect on decision making. But one-third indicated that decisions may be delayed in order to obtain the most accurate data, and one-quarter noted that a significant amount of time and effort can be spent reconciling differing views of data.

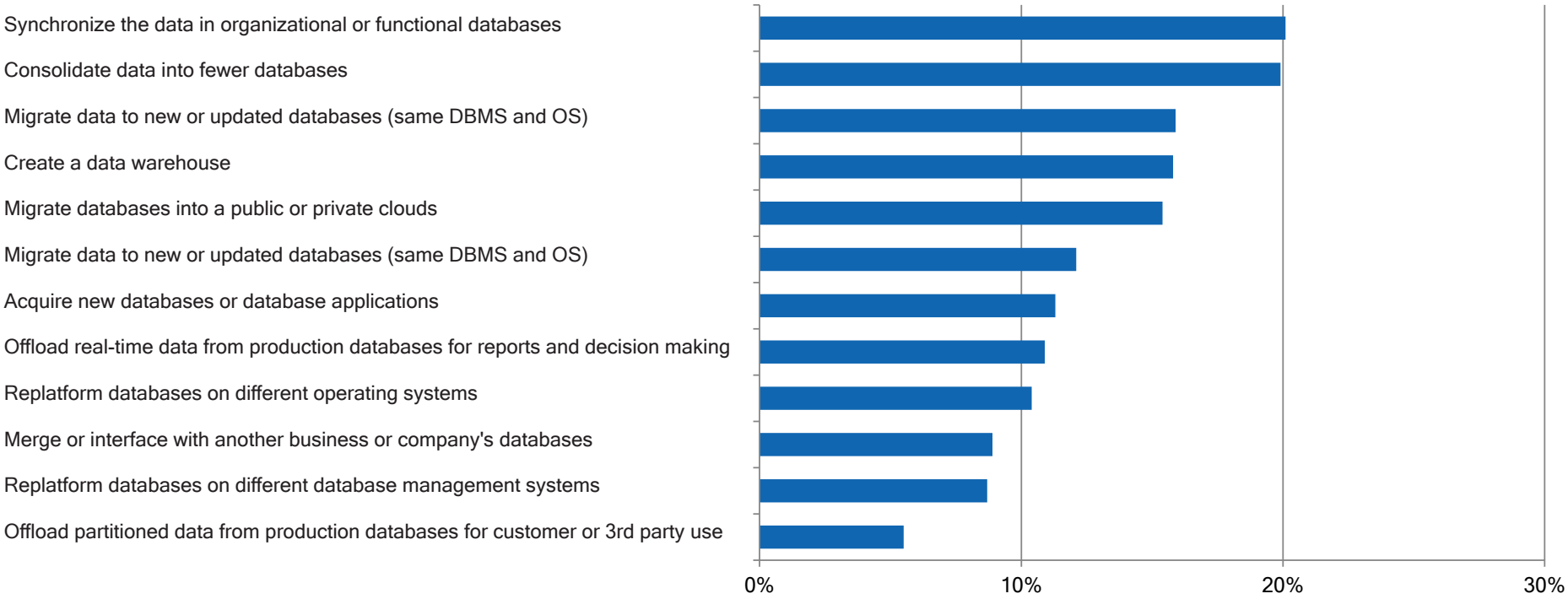
Obviously, periodic data sharing methods can be a headache for some IT professionals, increasing staff workload and slowing down productivity. What's more, if data is shared periodically and not updated concurrently, sound business decision making is jeopardized. In sum, IT professionals need the appropriate technology to ensure that data is current and trustworthy to support the goal of providing business intelligence.

A Glimpse of the Future

The two most common database initiatives IT leaders plan in the next 24 months are synchronizing the data in organizational or functional databases and consolidating data into fewer databases, each at 20%. Illustrated in the graph, these percentages and those of others were fairly low: This led us to question whether database projects were a high priority, despite organizational directives to use data for business intelligence.

So, we crunched the numbers and found that companies are planning an average of 1 database initiative in the next 24 months, with larger companies planning more. One possible explanation is that many IT leaders are holding the line on database initiatives, making deliberate decisions about where to apply resources and budget. Or, perhaps companies are undertaking highly complex projects, involving large numbers of databases, which require more planning and thought. In contrast, however, security initiatives rated much higher on the list of companies' priorities than database projects.

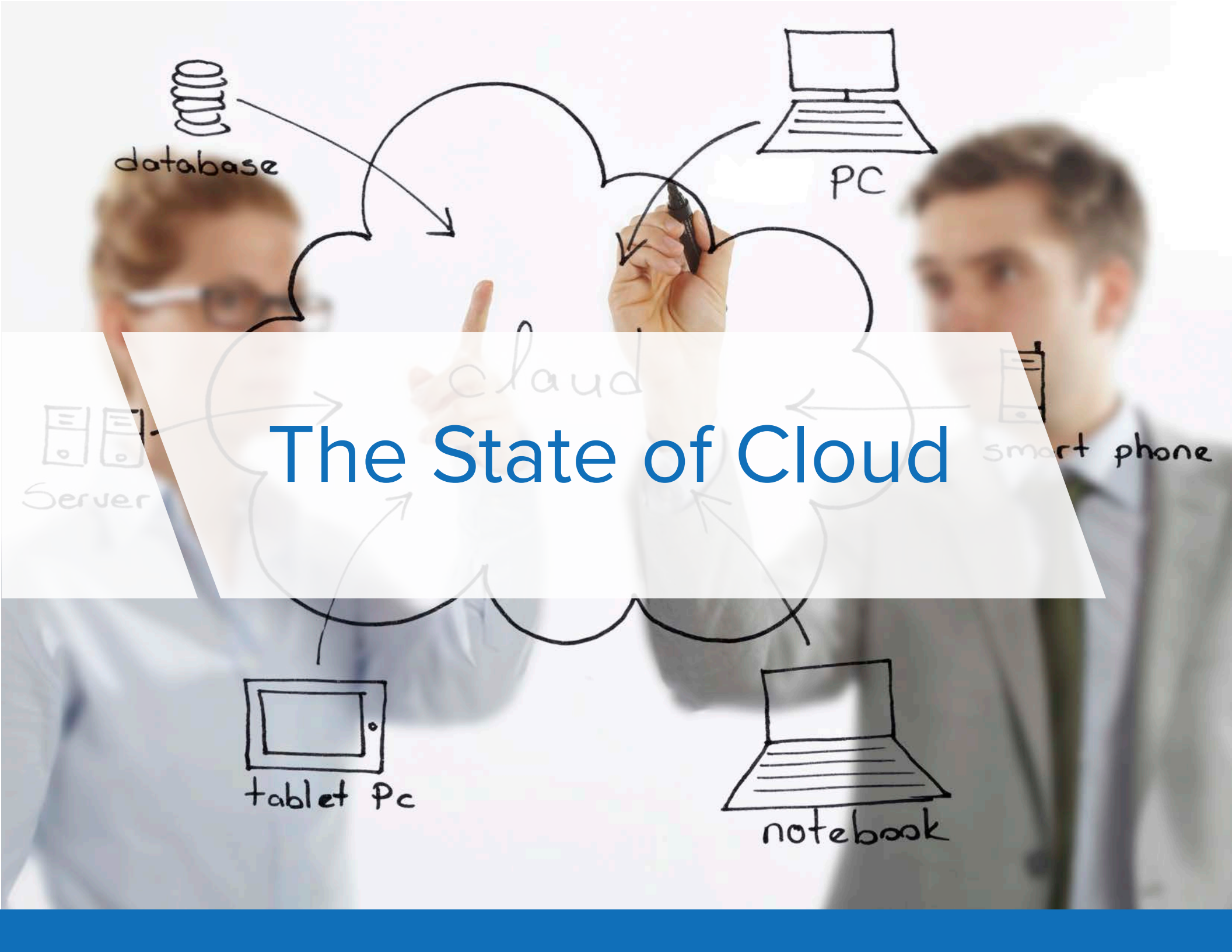
What database initiatives does your organization plan in the coming 24 months? Choose all that apply.



Key Takeaway:

In broadest terms, results about data sharing were positive. Many companies recognize the power and value of data for business intelligence or analytics. Most are using methods that deliver data between databases in real-time. Moreover, almost half of those who use periodic data transfer indicate that their methods are effective.

Yet deeper analysis showed that older data sharing technologies are still common; and periodic data sharing methods caused some businesses to delay decision making because of inconsistent data. Though these legacy techniques might still serve the business, there's a need for professionals to reevaluate their tools and plans, so they can deliver the speedy access to accurate data that their companies demand.



The State of Cloud

The State of Cloud

Cloud has emerged as the foundation of business infrastructure and services, yet IT leaders continue to grapple with the strategy and complex decisions it presents. They're balancing potential risks, such as data privacy and vendor management, with benefits, such as elasticity and cost containment. To complicate matters further, cloud is evolving rapidly as a platform for many innovative technologies—specifically IoT, Big Data analytics, and virtual reality applications—so businesses must plan for future as well as present requirements.

In this year's State of Resilience report, we wanted to determine what kinds of clouds are in use, the types of applications running in the cloud, and how professionals perceive the challenges it presents—among many other pressing issues.

The Cloud: Maturing Market, Private Clouds Dominate

First, we wanted to establish a baseline of how many companies in the survey used cloud and what kinds of clouds they had adopted. We found that cloud computing is pervasive, used by the majority of respondents (83%). Companies are no longer taking a "wait and see" approach to cloud, rather they've embraced it as a fundamental technology.

Choosing the right cloud delivery model is a major decision for IT organizations implementing the cloud. So we wondered what types of clouds they were using.

As the graph shows, private clouds are most popular: Roughly 40% of respondents (each) indicated that they currently use an on premise private cloud or a hosted private cloud. Another 32% use hybrid cloud and 30% a public cloud.

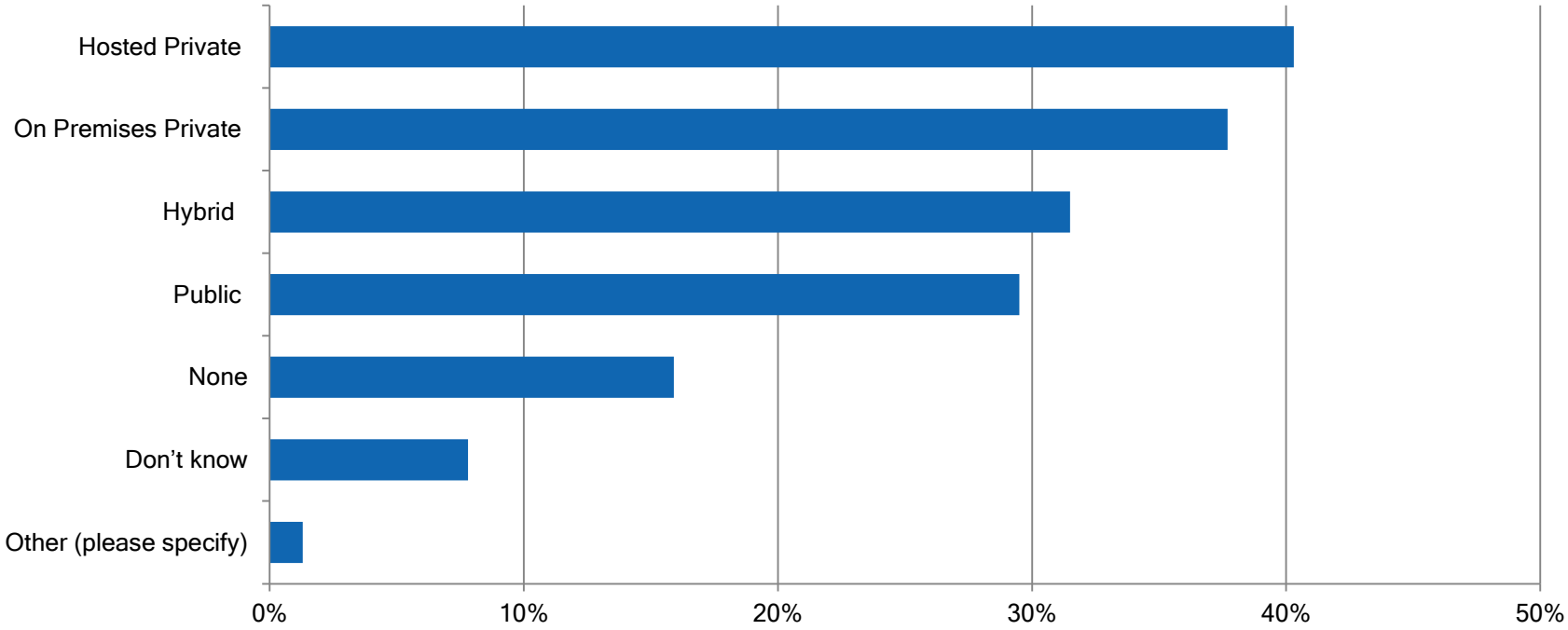
Perhaps the popularity of private clouds reflects a business reality. Survey results, highlighted later in this discussion, show that privacy of data in the cloud keeps the majority of professionals on edge. Their worries about data privacy might have influenced their choice of on premise and hosted private clouds; though the market appears mature, these concerns about cloud have not been fully addressed.

Notably, hybrid clouds were the third most popular choice. Hybrid clouds are a sound way to span traditional data center practices: They enable companies to store regulated customer information or intellectual property in a private cloud, but locate less critical information in a public cloud.

Finally, analysts predict that multi-cloud management is on the rise. In fact, we discovered that 46% of cloud users are running two cloud types, and 22% are running three or more. Inarguably, multi-platform cloud environments add complexity—and more risk—to IT management. [7]

[7] By 2020, over 90% of Enterprises Will Use Multiple Cloud Services and Platforms — a Transition Supported by Investments to Manage Resources Across Platforms. IDC FutureScape: Worldwide Cloud 2018 Predictions

Does your company currently use any of the following cloud types? Select all that apply.



IBM Power Users Jump on the Cloud

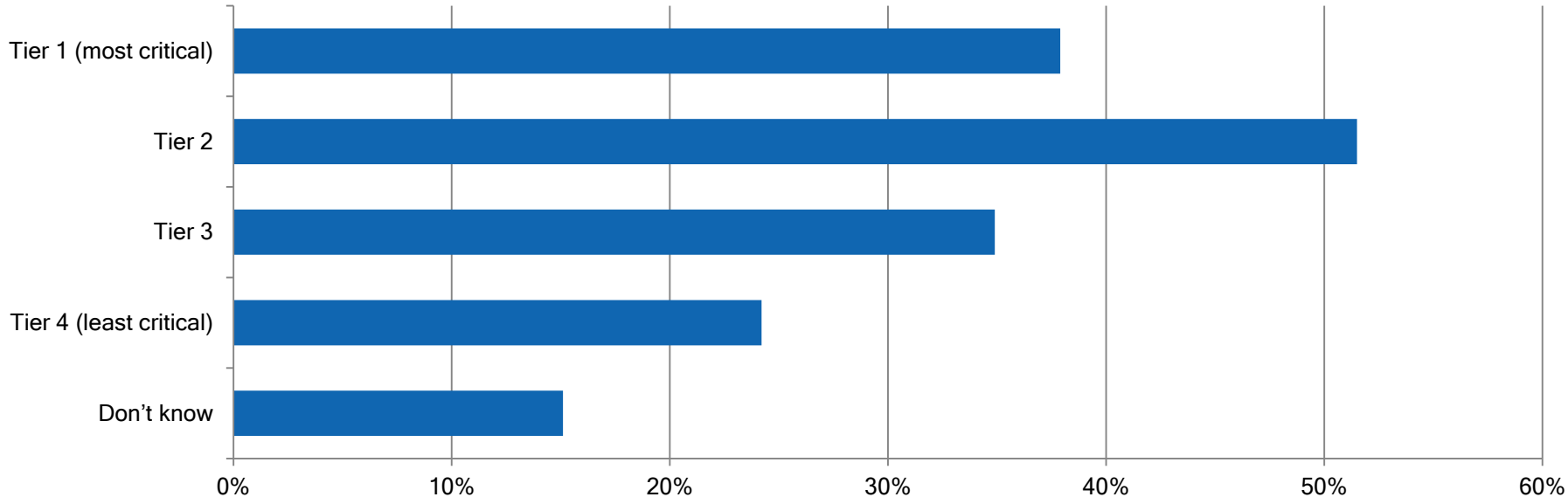
The majority of IBM Power respondents use some type of Cloud (71%). Private cloud is the model they prefer. Roughly 35% indicated they currently use a hosted private cloud and 26% use an on premises private cloud. Their pattern of use is similar to that of all participants in the survey, regardless of operating system.

Top Application Tiers in the Cloud

Professionals throughout the surveys expressed concerns about security and privacy in the cloud. Despite these reservations, IT organizations have invested trust in cloud systems. Of companies that adopted cloud, 38% use cloud for Tier 1 applications (most critical), and the majority (52%) use cloud for Tier 2 applications, as shown in the graph. 35% run Tier 3 applications, and only 24% of respondents reported that they run Tier 4 applications (least critical) in the cloud.

As with any technology, risks come with rewards. IT leaders must make strategic decisions about the right cloud model for their companies' business, assets, and resources—both human and financial. As explored in the following discussion, professionals are assessing cloud's risks to privacy against the benefits of cost savings and IT elasticity.

For which application tiers has your organization adopted a cloud computing model? Select all that apply.

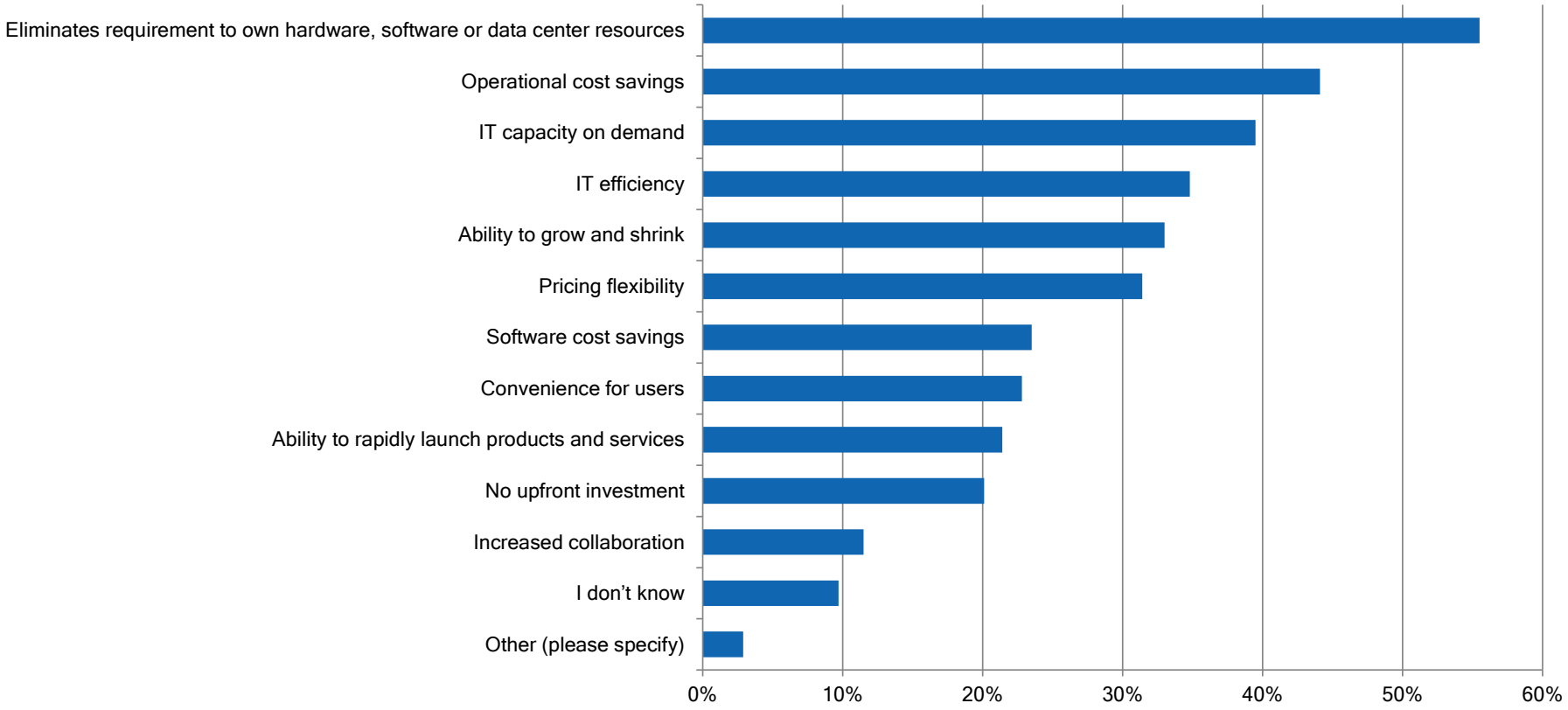


Reduced Capital Expenditures Seen as Biggest Cloud Benefit

IT leaders reported that the greatest advantages of cloud were "hard benefits," e.g. financial ones. Overwhelmingly, respondents perceived that cloud eliminates the requirement to own hardware, software, or data center resources (56%). While cloud computing increases a company's operational expenses, a considerable number of respondents (44%) also reported that they saved in that respect, as well, shown in the graph.

These findings also echo the reports of the industry media and analysts, who note that hosted clouds in particular enable CTOs and CIOs to reduce spending on equipment and bricks and mortar (CAPEX or capital expenditures) and maintenance, power, payroll, and insurance (OPEX or operating expenditures). Moreover, for companies highly concerned about privacy and control, data center providers typically offer IT organizations the choice of hosting single tenant architecture, in which an environment can be built with dedicated hardware and security.

What does your organization view as the most important benefits of cloud computing? Please check up to the top five benefits most important to your organization.

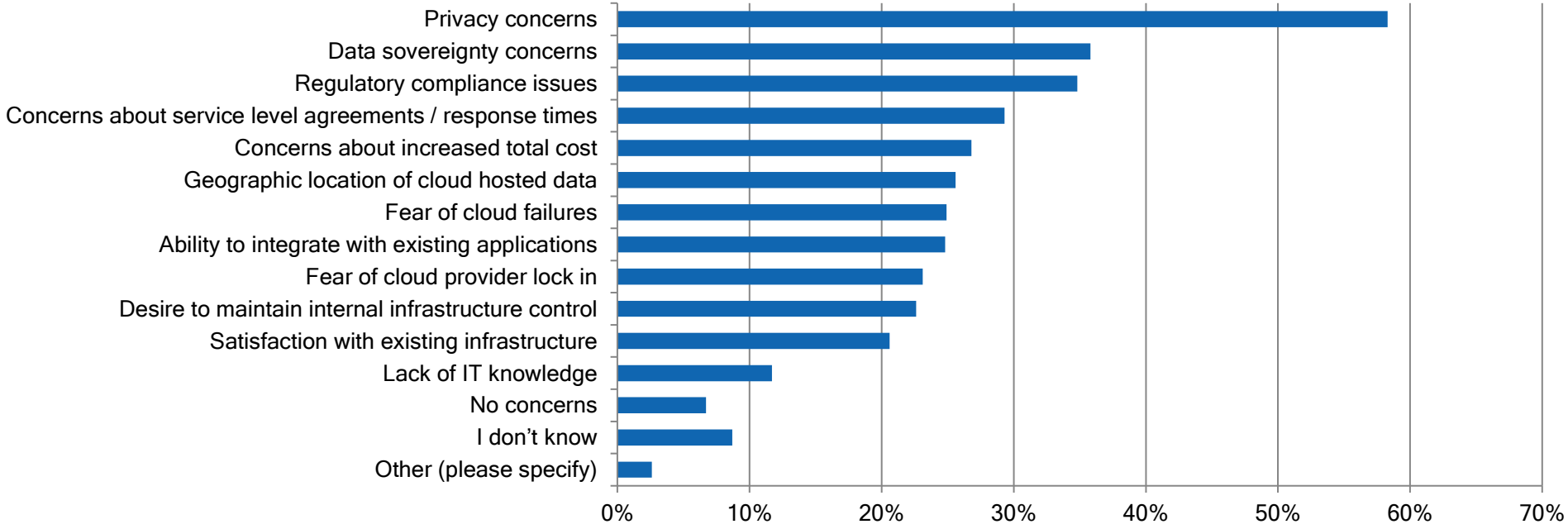


Top Cloud Challenges: Where Professionals Feel the Pain

Because cloud is such a pervasive strategy, we wondered what kinds of hurdles professionals face in implementing it. Unequivocally, the majority reported that privacy in the cloud is their chief concern—outstripping all others (58%). Data sovereignty concerns (36%) and regulatory compliance issues (35%) followed, illustrated in the graph.

Compliance with privacy laws, greater regulation, and liability issues are no doubt reasons why IT leaders put these items at the top of their list. Clearly, professionals are aware that the on-demand, shared resource nature of some cloud models can open up companies to data leaks, breaches, and litigation. Violations of privacy and sovereignty laws carry severe penalties.

What concerns does your organization face in using cloud services or considering additional cloud solutions? Select all that apply.



Navigating the Data Localization Landscape

The surveys we conducted included respondents from large and small companies around the world. Results showed that many are subject to compliance regulations concerning data privacy. This issue is particularly complex for global companies because every country--and even some provinces within countries--can have their own privacy and data sovereignty laws.

The situation becomes even murkier in the case of cloud technology: For example, a company may be running a public cloud locally, but the data could be backed up in a cloud anywhere in the world, including India, China, Brazil, or Singapore.

Industry Insight

Device and Data Explosion: Is Cloud a Solution?

Endpoints of the IoT will grow at a 33% compound annual growth rate from 2015 through 2020, reaching an installed base of 20.4 billion units, with almost two-thirds of them consumer applications. Spending on networked consumer and business endpoints will displace non-networked, growing at a 20% CAGR to $2.9 trillion.

Source: Gartner, Inc. Forecast,
Peter Middleton, February 10, 2017

Here are just a few legal developments regarding privacy and sovereignty that have consequences for technology companies:

- China, which has the most stringent data localization laws, mandated in June 2017 that Chinese users' personal information must be stored on servers within China. China's law reinforces the requirement for data storage on local cloud computing services.
- The business networking site, LinkedIn, left the Russian market In November 2016, rather than store Russian users' data in-country.
- The European Union General Data Protection Standard goes into effect in May 2018, and member states must transpose it into their own laws.
- Australia mandates that all personal health records must be stored in-country.
- Canada, Turkey, Brazil, and South Korea have all passed in-country laws with varying degrees of stringency. [8]

Whether these regulations are good for commerce and good for users remains to be seen. Still, before bringing their business to the cloud, IT professionals must consult with service providers and with legal counsel to ensure that their cloud systems are in compliance with local laws.

[8] "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Nigel Cory, May 1, 2017, Information Technology and Innovation Foundation.
"Companies push back on foreign-must-store-data-here rule," Roger Yu, USA Today, August 12, 2017
https://www.usatoday. com/story/money/2017/08/12/more-u-s-companies-push-back-foreign-must-store-data-here-rule/558702001/

Disaster Recovery as a Service: Not Yet Mainstream

Disaster recovery in the cloud is where the rubber meets the road. Companies that invest in it are banking on reliability and resilience of the cloud—and the vendors they choose. Because so many companies were running near critical or critical applications in the cloud, we particularly wondered how many companies were willing to embrace disaster recovery as a service. DRaaS has some traction as a data protection technology, but it is not pervasive. As shown previously in this report, 21% have adopted it.

We also asked about enterprises' plans for the service. For those who do not use DRaaS, results were as follows:

- 4% will adopt it in less than a year.
- 12% in 1 to 2 years.
- 36% have no plans to adopt DRaaS at all.

We might have expected that DRaaS would be more widespread. Though early adopters have implemented DRaaS, many others have yet to jump on the bandwagon. And, the low percentages for future use indicate that adoption rates will be gradual.

A situation analysis sheds more light on these findings: Analyst organizations note that most big organizations haven't yet adopted DRaaS. The reasons? Large companies typically have multiple data centers used for backups, and closing a data center takes years to plan; moreover, these businesses tend to be more conservative in purchasing new technology and own many physical servers.[9]

Perhaps the flurry of bad press about this year's natural disasters —fires, floods, and hurricanes—could cause companies to consider moving recovery operations to the cloud or secondary facilities to keep business running. Downtime concerns and skyrocketing growth of data might also drive future DRaaS adoption.

[9] "Next Generation Disaster Recovery, A Cloudy Forecast," Werner Zurcher, Gartner Inc., August 2016

Key Takeaway:

Most companies have jumped onto the cloud, and IT leaders view it as offering big benefits for organizations, particularly financial benefits. Many businesses have already entrusted mission critical applications to the cloud. Yet, concerns about privacy and data sovereignty in the cloud loom large. Results indicate that professionals still have some "heavy lifting" to do—adopting practices and methods to make cloud schemes more resilient, such as:

- Vetting third party data center providers and hosting services, including facilities, security, networks, servers, and history of outages.
- Reviewing service level agreements for responsibility in the event of privacy breaches.
- Consulting with legal departments about data localization laws applicable to global companies.

The Last Word

At the outset of this report, we noted that IT leaders must provide an enterprise infrastructure that can sustain severe threats, secure vital information, and enable the business intelligence their companies require. After analysis of responses from professionals this year, what insights have we gained?

If we learned any lesson from the surveys, it's that resilience is multi-faceted. It's a complex combination of technologies, policies, process, and culture that help organizations withstand shocks and sustain success.

We realize that the road to technology adoption isn't straightforward. A substantial gulf can exist between the time organizations recognize a need for technology, prepare a business case, develop a budget, and move to implementation. We found uneven progress to be the case in our surveys: Some businesses are charging ahead—implementing multiple initiatives, running diverse cloud types, and engaging in new trends; others are lagging, using legacy tools and experiencing unacceptable amounts of downtime. No two companies are alike, and each must make calculated decisions about innovation based on requirements, budget, and talent. What is certain though is that yesterday's technologies will not be adequate for tomorrow's businesses.

We discovered that company culture too can be a major impediment to resilience, particularly as it relates to security and disaster recovery. The majority of companies will continue to use internal staff for these vital functions and do not place training plans high on their agendas. Businesses are vulnerable to human error and internal and external threats when they lack company-wide security awareness, employee education, and reliable disaster recovery plans.

We also found that the most intense pressure on IT leaders will come from three fronts: security, HA/DR, and data management. This is no surprise because these disciplines are interconnected: data management and security are integral components of a strong high availability and recovery strategy. Though some IT organizations are keeping the pace in these critical areas, many are not leveraging the wide range of technologies available to ensure continuous availability and protection of company data.

In sum, the bar for IT professionals is high. They are expected to be pacesetters who drive business priorities forward. Their companies demand agile solutions that deliver a constant stream of secure, high quality data for business intelligence and analysis. These goals can only be achieved with the right tools, staffing, infrastructure, and policies. Herein lies the daily work of IT leaders and the challenge: Keeping one foot in the present, deciding what is achievable now, while moving their organizations into the future—without exhausting their staff, breaking the bank, or incurring too much risk.

As a final note, we'd like to thank all the professionals around the globe who took the time to participate in our surveys. Whether you are a CTO, CIO, V.P. of Information Technology, Senior Security Engineer, System Architect, DBA, or Help Desk Manager, we've appreciated your feedback. Your responses contribute to a greater knowledge of the industry. We're looking forward to hearing from you again in the coming year.

877.700.0970
www.syncsort.com

ABOUT SYNCSORT

Syncsort is a trusted enterprise software provider and the global leader in Big Iron to Big Data solutions. More than 6,000 organizations, including 84 of the Fortune 100, use the company's products to solve their most complex data management challenges, on premise and in the cloud. Syncsort helps customers optimize traditional data systems and deliver mission-critical data from these systems to next-generation analytic environments. Its Big Iron to Big Data portfolio now features the #1 high availability product for IBM i Power Systems, powerful cross-platform capacity management, best-in-class mainframe app and machine data access & integration, and market-leading data quality capabilities. Rediscover Syncsort at www.syncsort.com.