What to Know Before You Migrate

By Lauren Gibbons Paul

One of IT's biggest balancing acts is to make data transactions easily available to authorized users while preventing all others from accessing its data assets. With high-profile data security breaches splashed across headlines nearly every day, CIOs are understandably worried about protecting their data. And for IT leaders who are considering moving their business to the cloud it is critical to ensure the provider they select has undertaken full and robust measures for physical and logical security.

Enterprise security is at the top of IT leaders' list of worries. Three-quarters of surveyed CIOs view cyber threats as having the second potentially most severe impact on their organizations, next to a global recession, according to the 2014 State of the CIO report (see Figure 1). Research has shown that one of the biggest concerns about operating in the cloud is security. The public cloud in particular is a source of worry for CIOs, but private and hybrid cloud services carry security concerns, too. While moving to the cloud carries a wide variety of benefits, such as enabling business agility, security remains a persistent worry.

Seven out of 10 CIOs See Growing Threat to Enterprise Security
FIGURE 1

QUESTION:

How do you anticipate the following business and economic issues will impact your organization within the next 3 years?
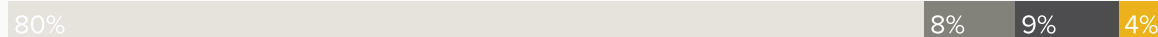
75%
AGREE THAT THE BOARD OF DIRECTORS IS MORE INTERESTED IN IT TODAY THAN 3 YEARS AGO

64%
OF BOARD DIRECTORS ARE MORE CURIOUS ABOUT THE ROLE OF IT IN BUSINESS

BROADER UNDERSTANDING OF IT BY NON-IT COLLEAGUES

| 80% | 8% | 9% | 4% |

GROWING ECONOMIC STRENGTH IN EMERGING ECONOMIES SUCH AS CHINA AND INDIA

| 38% | 31% | 24% | 7% |

GROWING THREAT TO ENTERPRISE SECURITY

| 16% | 9% | 70% | 5% |

STAGNANT U.S. JOB GROWTH

| 10% | 28% | 56% | 7% |

GLOBAL RECESSION

| 7% | 9% | 82% | 2% |

| POSITIVE IMPACT (NET) | NEGATIVE IMPACT (NET) | NO IMPACT | NOT SURE |

QTS® / Data Centers Powered by People   CIO

While 44 percent of IT budgets were spent on cloud services in 2013, according to the IDG Enterprise Cloud Study 2013, the majority of surveyed IT leaders listed security concerns as the top challenge to implementing a cloud strategy (see Figure 2). Once they take the leap into the cloud, however, security worries seem to dissipate a bit as their confidence grows that the data is safe. After all, most cloud providers have more robust layers of security protection than an individual company could afford to provide on its own. For CIOs who have already made the move to the cloud, most (78%) felt "very confident" or "somewhat confident" in the security of their information assets in the cloud.

Security Concerns Top IT Leaders' Cloud Barriers
FIGURE 2

QUESTION:

What are the top three challenges or barriers to implementing a cloud computing strategy for your IT organization?

In your opinion, what do your copmany's non-IT business leaders see as the top three challenges in implementing a cloud computing strategy?

CHALLENGES TO IMPLEMENTING A CLOUD STRATEGY	IT REALITY	IT PERCEPTION OF LOB
Concerns about the security of cloud computing solutions (risk of unauthorized access, data integrity and protection)	66%	53%
Concerns surrounding integration (making information available to applications outside the cloud preserving a uniform set of access privileges)	47%	27%
Concerns about the ability of cloud computing solutions to meet enterprise and/or industry standards	35%	35%
Concerns about information governance (eDiscovery and other information management requirements)	34%	30%
Difficulty measuring ROI/determining accurate economic value of cloud solutions	33%	38%
Lack of clear strategy or help from key vendors in adapting their applications to cloud computing platforms	22%	22%
Business leaders are not receptive to cloud computingsolutions	9%	13%
Employees are not receptive to cloud computing solutions	8%	14%

SOURCE: **2013 IDG** *ENTERPRISE CLOUD COMPUTING STUDY*

QTS
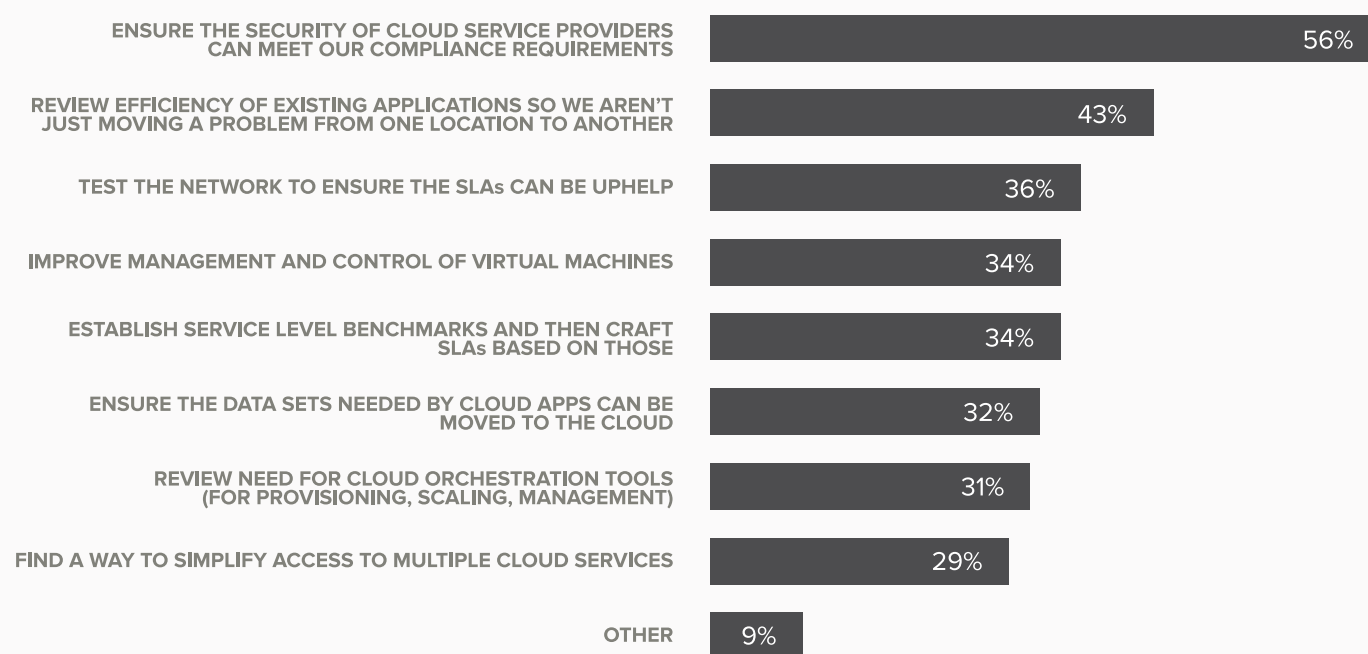
Data Centers Powered by People

CIO

When selecting a cloud services provider, in addition to ensuring the company uses state-of-the-art physical and logical security provisions, the majority of CIOs surveyed in the IDG Enterprise Cloud Study 2013 also worry their provider can meet their individual compliance requirements (see Figure 3).

CIOs Need Assurances from Potential Cloud Partners
FIGURE 3

QUESTION:

What issues does your organization need to address or resolve before it can more fully embrace data?

ENSURE THE SECURITY OF CLOUD SERVICE PROVIDERS CAN MEET OUR COMPLIANCE REQUIREMENTS	56%
REVIEW EFFICIENCY OF EXISTING APPLICATIONS SO WE AREN'T JUST MOVING A PROBLEM FROM ONE LOCATION TO ANOTHER	43%
TEST THE NETWORK TO ENSURE THE SLAs CAN BE UPHELP	36%
IMPROVE MANAGEMENT AND CONTROL OF VIRTUAL MACHINES	34%
ESTABLISH SERVICE LEVEL BENCHMARKS AND THEN CRAFT SLAs BASED ON THOSE	34%
ENSURE THE DATA SETS NEEDED BY CLOUD APPS CAN BE MOVED TO THE CLOUD	32%
REVIEW NEED FOR CLOUD ORCHESTRATION TOOLS (FOR PROVISIONING, SCALING, MANAGEMENT)	31%
FIND A WAY TO SIMPLIFY ACCESS TO MULTIPLE CLOUD SERVICES	29%
OTHER	9%

SOURCE: **2013 IDG** *ENTERPRISE CLOUD COMPUTING STUDY*

Three years into the cloud phenomenon, security concerns are still paramount for CIOs. This is especially true when they are searching for a cloud provider, says Brian Johnston. Johnston is chief technology officer for QTS in Overland Park, Kansas, a provider of data center solutions, Infrastructure as a Service (IaaS) offerings, and fully managed services. The key is knowing the right questions to ask, he adds.

"Compliance should be a particularly important area of questioning," says Johnston. "Fully understanding complex compliance standards and requirements can be difficult. CIOs should seek providers that have dedicated security and compliance resources that can help educate prospective clients."

Choosing a Cloud Provider: Ask the Right Questions

The stakes are high when it comes to the safety of your data. When selecting a cloud provider, it is important to open a dialog with your prospective providers in which you can learn about their approach to security. Your list of questions will be specific to your organization, industry and compliance requirement but should start with these basics:

+ How much experience do you have in data center services? And in what industries?
+ Do you have experience in our industry with customers that have similar compliance needs?
+ Where will my cloud data reside? Do you own your data centers, or do you lease from a third party?
+ Do you have industry-leading physical and logical security? Describe technologies used and best practices for both types of security.
+ Do you use industry standard methodologies like ITIL (Information Technology Infrastructure Library)?
+ What is your security and data reliability track record?
+ How fast could you recover in the event of a successful attack or disaster?
+ How transparent are you with customers?
+ Do you have a third party certify your security measures and compliance with industry regulations like SOx?

Conclusion
The QTS Difference

QTS provides its cloud and managed services clients with the highest possible physical, logical and information security. It is audited by trusted third parties and certified for security compliance with industry regulations including SOx and PCI (coming in 2015).

QTS offers two cloud IaaS solutions: QTS Federal Cloud for government agencies and QTS Enterprise Cloud for more general-purpose needs. QTS is one of the largest and fastest-growing data center providers in the United States.

QTS Enterprise Cloud customer data is housed in premium, secure, compliant QTS-owned data centers leveraging best-of-breed platform technologies from VMware, EMC and Cisco. QTS Enterprise Cloud offers secure and compliant infrastructure for companies in highly regulated industries.

For governmental organizations and contractors, the QTS Federal Cloud offers infrastructure services that comply with the Federal Data Center Consolidation Initiative (FDCCI), Cloud First and Shared Services, and in mid-2014, the Federal Risk and Authorization Management Program known as FedRAMP. This physically isolated cloud is housed in two of the world's largest and most secure data centers: the QTS Richmond Data Center and the QTS Atlanta-Metro Data Center.

CIOs have the comfort of knowing QTS owns the facilities that house its data centers and thus has superior physical security.

"This is a capital-intensive industry," says Johnston. "We have much better motivation to make necessary security enhancements and technical adjustments that will be needed in the future and to evolve our infrastructure … to support future client needs."

Lauren Gibbons Paul is a freelance business/technology journalist in Waban, Mass., who writes frequently on cloud and collaboration. She was a staff writer at PC Week and has written for industry publications including CIO, CFO, CSO, CMO, Computerworld, Channel Pro and Network World.

Data Centers Powered by People