



GIGAOM RESEARCH

Shadow IT: data protection and cloud security

George Crump

November 17, 2014

This report is underwritten by CipherCloud.

TABLE OF CONTENTS

Executive summary	3
Views on shadow IT and data security from within the enterprise	4
Percentage of IT spending at organizations on cloud services	5
Top challenges holding back cloud projects.....	7
Requests from business users for new cloud services each month.....	8
Three cloud services business users request most frequently.....	9
Pressured on IT to approve applications or devices that don't meet security or compliance requirements	10
Number of shadow IT apps in use.....	10
C-level concern about the security of data residing in the cloud	10
Insider threat incidents	10
Top security issues facing companies	11
Company policies on acceptable cloud usage	12
Cloud security-awareness training programs	12
Key takeaways	13
Methodology	14
About George Crump	15
About Gigaom Research	15

Executive summary

Shadow IT is a term describing users or whole lines of business, who go outside of their organization's IT group to meet their IT needs. A disconnect often exists between what IT users feel they need and what the IT services group is prepared to deliver. Shadow IT's destination is often the cloud, where a company credit card can access all kinds of IT as a service, including cloud-based file-sync-and-share, laptop data protection, CRM, project management, or back-office kinds of software.

Shadow IT may seem like an easy solution for an organization, because users and lines of business meet their needs and IT has one less problem, but in reality, both stakeholders can end up with less than they wanted and in the process, they put the organization's important data assets at risk by compromising data security. The truth is that the consumerization of IT will likely come back to haunt IT.

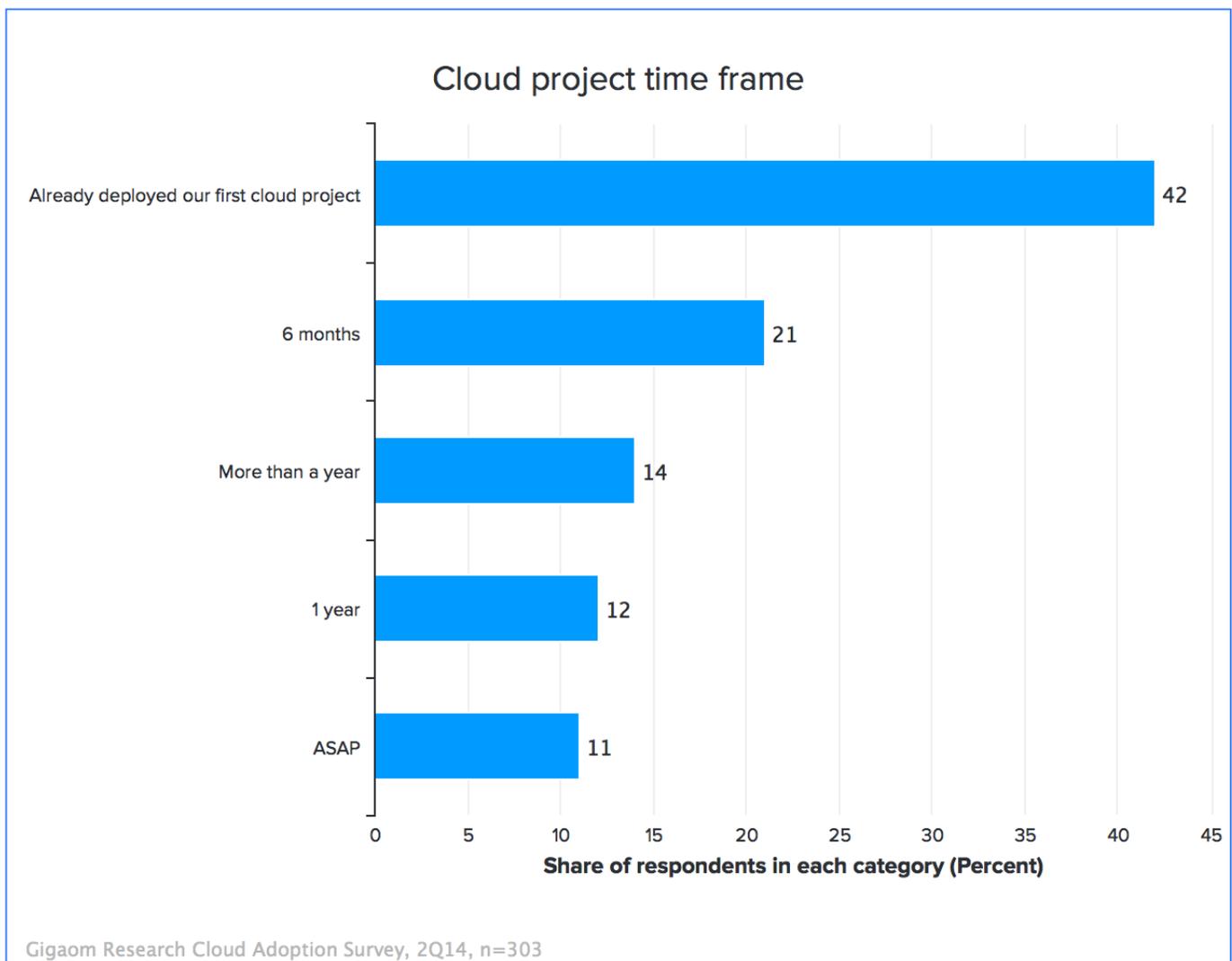
Instead of divesting itself of responsibility, IT organizations should get in front of shadow IT and prevent its spread. When IT takes control of an organization's cloud usage it provides better cloud utilization, which in turn, allows cloud compute and storage to reach its full potential. At the same time, IT keeps the organization's data better protected and more secure.

This report reviews data from three surveys that Gigaom Research conducted between September 2013 and June 2014. It will help IT organizations understand the extent of shadow IT and avoid its pitfalls.

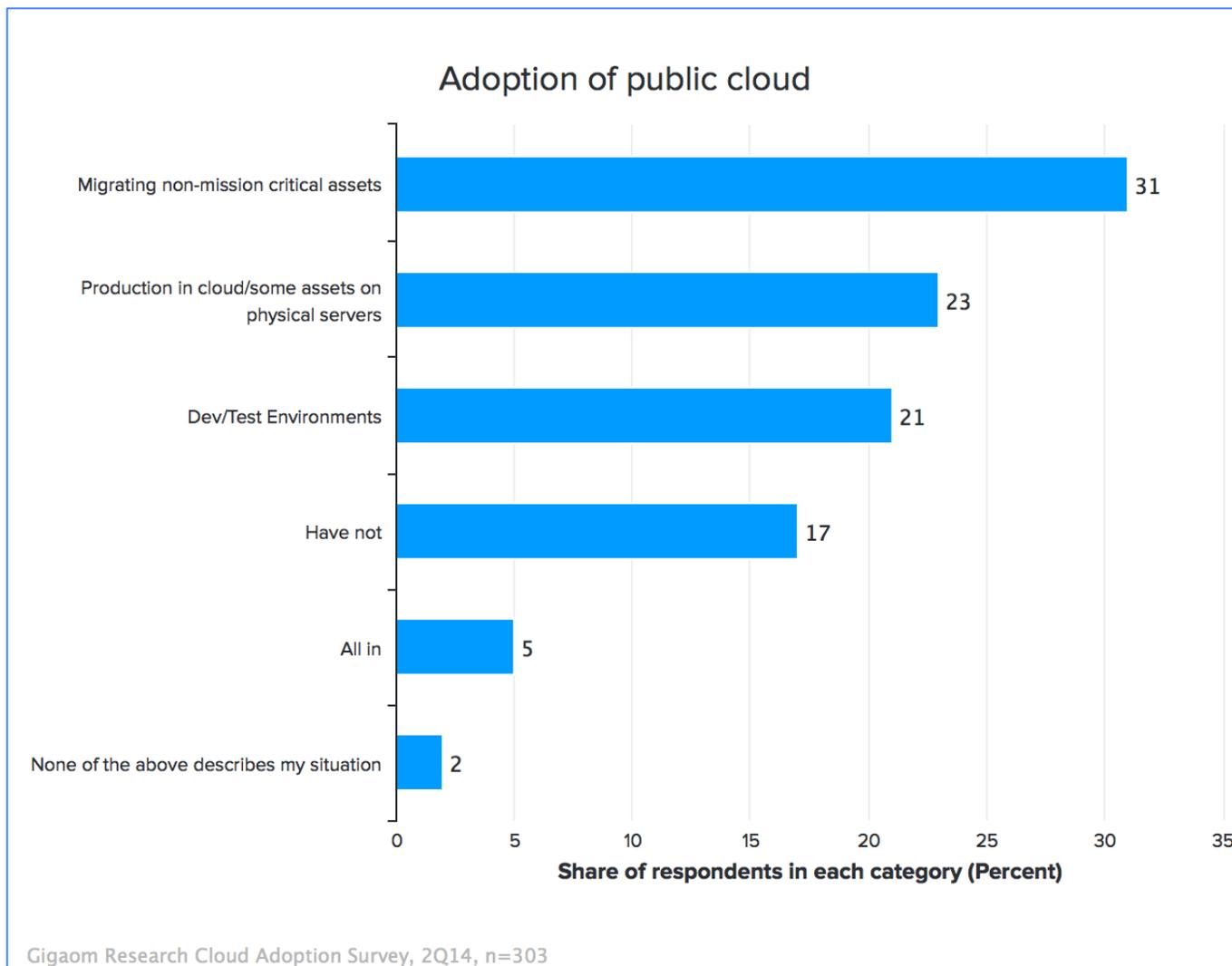
- 83 percent of organizations have adopted the cloud for some function, but few are using the cloud to deploy complex enterprise applications.
- Security (62 percent), application performance (44 percent), and time required to develop related skills (41 percent) top the list of cloud concerns.
- More than half of enterprises have at least 10 public cloud instances in production.
- 81 percent of line-of-business employees admitted to using unauthorized SaaS applications with 38 percent deliberately using unsanctioned apps because of the IT-approval process.
- 70 percent of unauthorized access to data is committed by an organization's own employees.

Views on shadow IT and data security from within the enterprise

Most organizations have embraced the cloud to some extent. The first survey question we're considering in this report, "What is your timeframe for implementing your first cloud project," showed that 42 percent of respondents have already completed their first project and another 44 percent indicated plans to have their first project done within the year. Responding to a different question, 83 percent of survey respondents reported that they have adopted the cloud for some function. How many of these initiatives are endorsed by IT is not clear, but it seems that shadow IT drives a great many of these cloud initiatives.



This positive attitude toward cloud services continues to the public cloud. As the results in the following chart indicate, all but 17 percent of the respondents have adopted public cloud.



Percentage of IT spending at organizations on cloud services

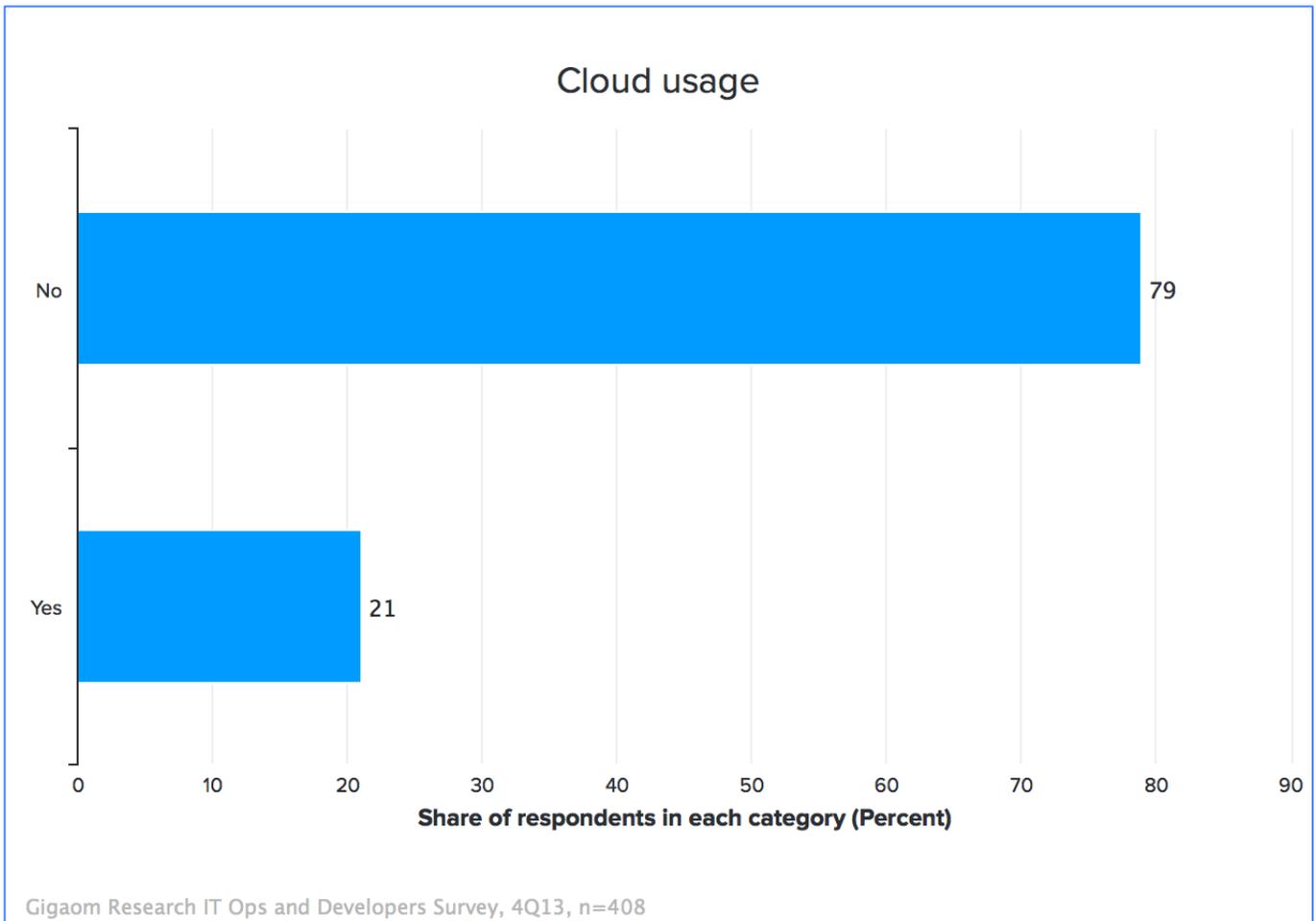
Organizations are moving beyond curiosity about the cloud to actual deployment. Our survey results indicate that the cloud market will grow about 126.5 percent this year and that the majority of growth will be in two areas:

- **Software-as-a-Service (SaaS) is growing at 199 percent.** We find that SaaS is the typical home for shadow IT. It is growing because end-users are impatient with IT and looking for

alternatives. With SaaS, the organizations can access easy alternatives with a credit card. Much of this spending is still to come, as our survey indicates that almost 79 percent of organizations are not yet using the cloud to deploy complex enterprise applications. In other words, shadow IT is a concern now, but will be a much larger problem in the near future.

- **Infrastructure-as-a-Service (IaaS) is growing at 122 percent.** This is an excellent indicator that IT is also embracing cloud and may be attempting to respond to shadow IT.

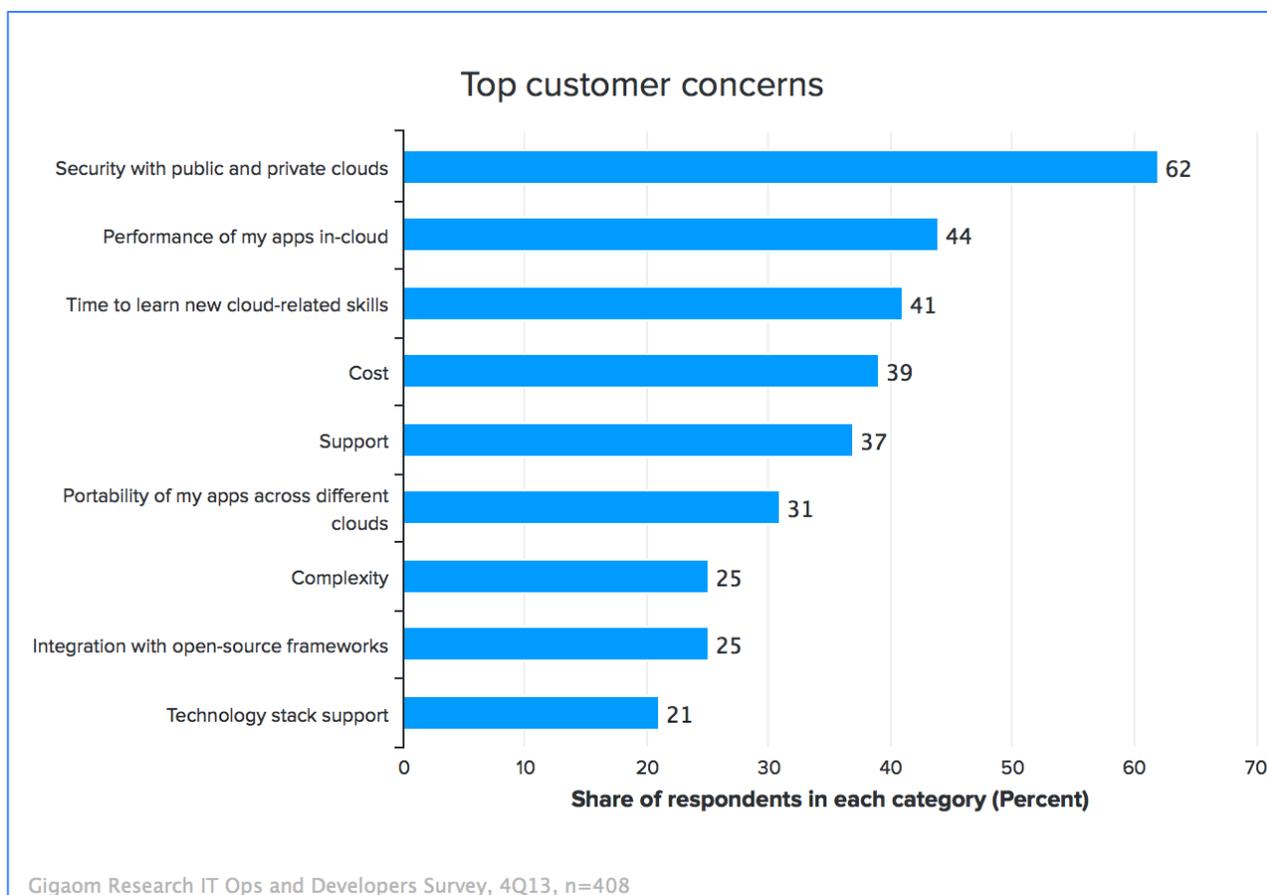
Are you currently using the cloud to develop enterprise apps?



Top challenges holding back cloud projects

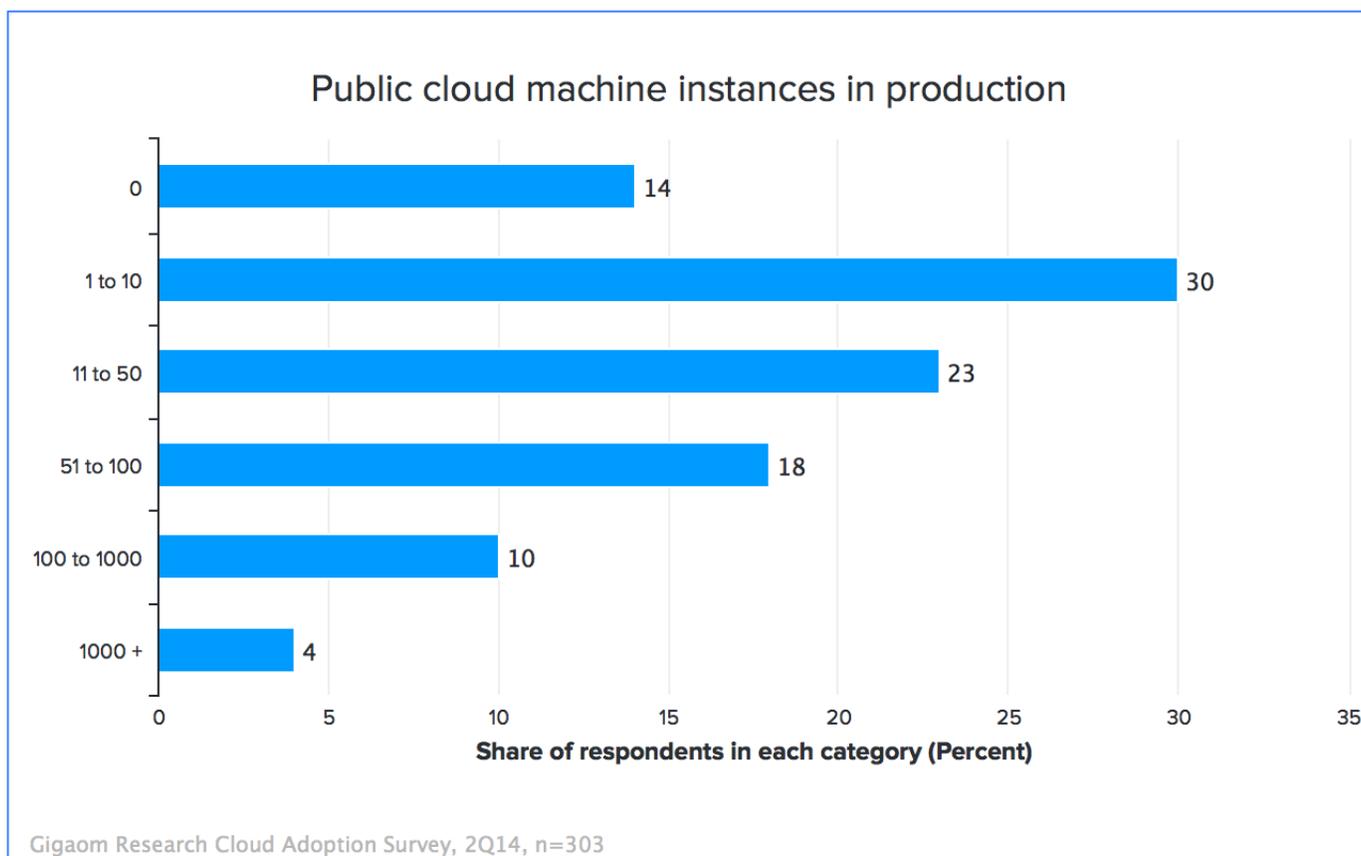
Security is the number-one concern for IT professionals as they continue their cloud journey, with 62 percent selecting it as the top concern. Second and third were performance of those applications (44 percent) and developing cloud-related skills (41 percent). Understanding what “secure” means to respondents can be a challenge. Some IT professionals consider encryption as the only necessary aspect of security. But encryption must be end-to-end from the moment the data leaves the organization’s network infrastructure to the data being stored in the cloud – potentially for decades.

Understanding who will hold and maintain the encryption keys is very important, because that group controls who can read the data – a decision that should rest with the organization and not with the cloud provider. The organization should be the *sole* encryption key holder. Physical-premises security at the cloud provider’s facility should also be high on the consideration list, because most data-loss events happen from inside an organization.



Requests from business users for new cloud services each month

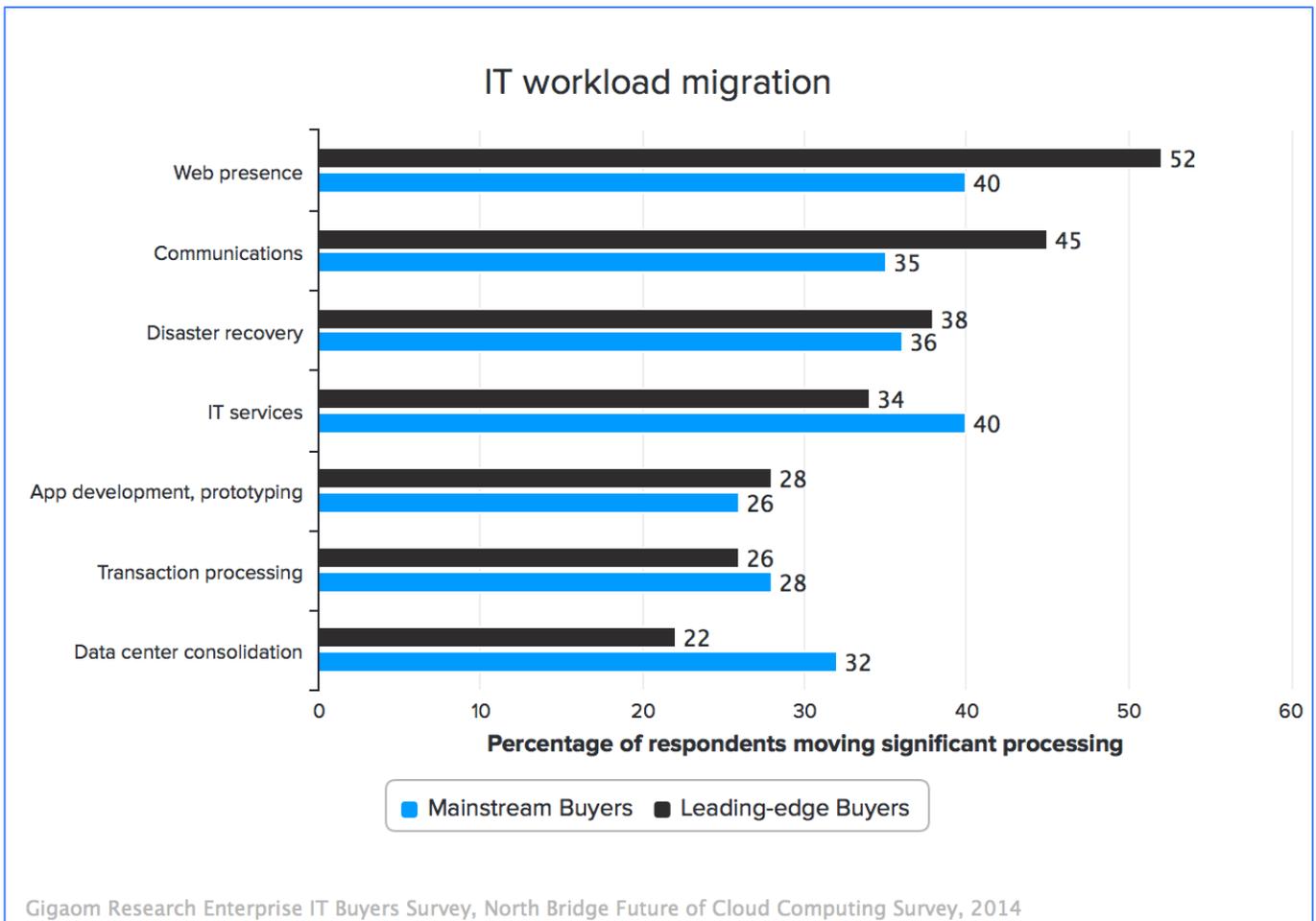
Cloud usage is clearly on the rise within most organizations, with only 14 percent indicating no cloud deployment. Over half of the survey respondents indicated that they had more than 10 cloud instances in production, while a surprising 32 percent indicated significant use (51 or more instances) of the cloud for production applications. Note that this data only includes the cloud instances that IT knows about; it does not include the shadow IT cloud instances that business units or employees solicit on their own.



Three cloud services business users request most frequently

Typically, the most commonly requested cloud services are related to increased web-presence communications (workforce productivity), file sync-and-share, and disaster recovery (DR).

The second most requested cloud service is an application, hence the growth in Application-as-a-Service (AaaS). Most of these applications enhance productivity and include CRM or sales-automation tools, messaging tools, and cloud-based email.



Pressured on IT to approve applications or devices that don't meet security or compliance requirements

Another of IT's concerns is pressure to approve an application or device that does not meet the organization's security or compliance requirements. Many of these initiatives start in the business unit, independent of IT oversight. Once the business unit becomes excited about a cloud service's potential, IT is battling up hill to halt implementation.

The larger problem, though, may not be the pressure on IT, but rather users acting on their own without IT's knowledge. One finding revealed that 38 percent of line-of-business employees surveyed use unauthorized cloud apps because the IT-approval processes in their companies are too slow.

Number of shadow IT apps in use

A big challenge for IT professionals is accounting for shadow IT projects that are in progress within their organizations. Often IT only identifies a shadow-IT project when a member of the IT group overhears someone talking about it or when something goes wrong with the service and the business unit asks IT to bail it out because of a compliance or security violation.

Among line-of-business employees, 81 percent admitted to using unauthorized SaaS applications. Among consumer-grade file-sharing solutions, individuals or groups were using Dropbox without IT department approval in 38 percent of the organizations responding to the survey and nearly one in four (24 percent) responding companies reported having experienced unauthorized access to a Dropbox account.

C-level concern about the security of data residing in the cloud

If an organization is to be successful securing its cloud-based assets, data security in the cloud must be a top-down priority in the organization. IT alone cannot properly enforce a strict security standard because to be successful, data security must cut across a business's organizational lines. Justification for this executive-level involvement can be found in current headlines that report organizations like Target and Home Depot having to make significant C-level changes as a result of a security breach.

Insider threat incidents

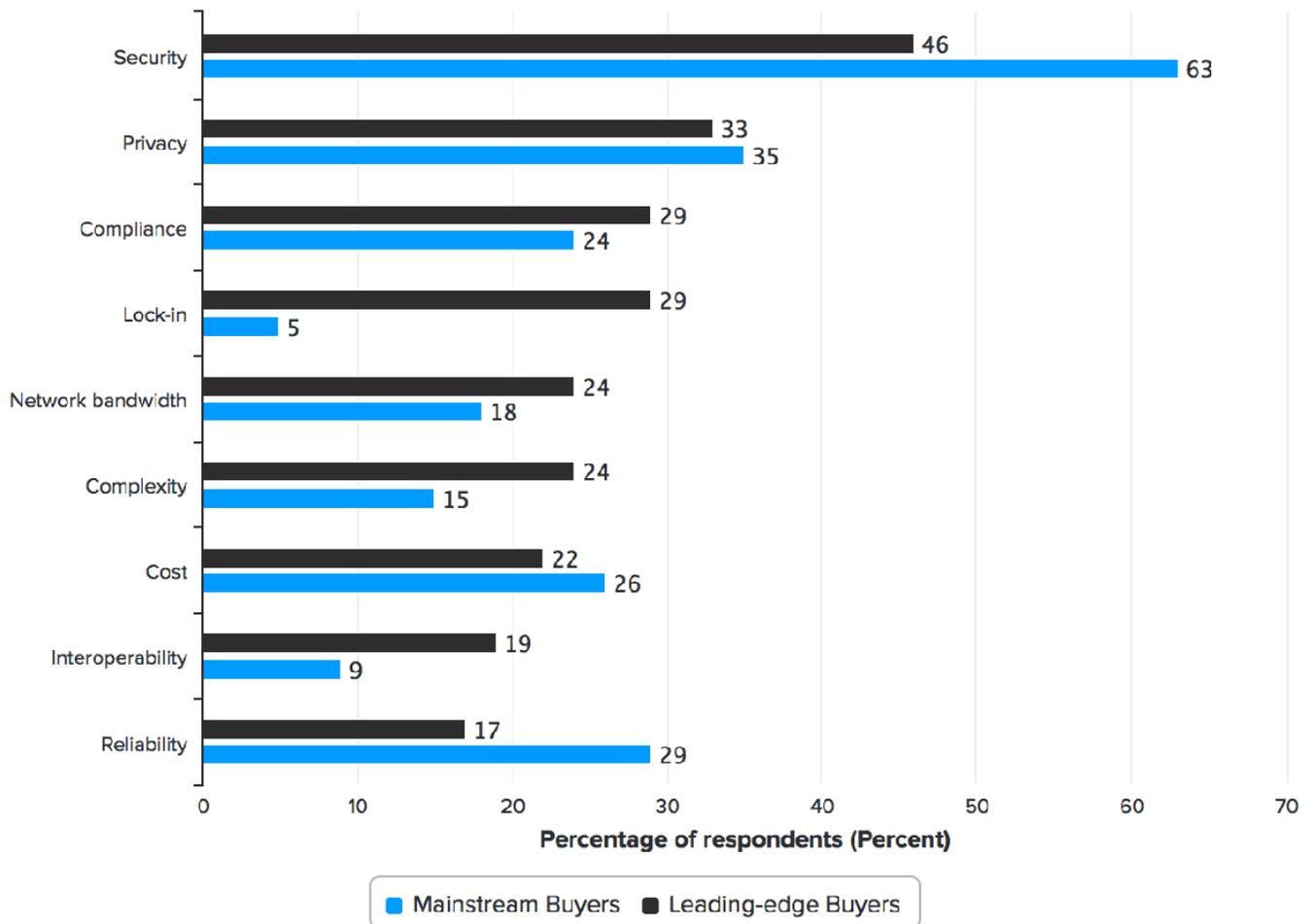
While most IT departments expend a lot of effort mitigating the threat to data as it leaves the organization and heads to the cloud, the reality is that the insider threat is the larger challenge. More than

70 percent of unauthorized access to data is committed by an organization's own employees and ranges from naive mistakes like leaving a remote-access session open while in public to disheartened employees maliciously attempting to remove data.

Top security issues facing companies

The other top inhibitors listed in Gigaom Research’s survey data – privacy, compliance, and lock-in – are actually a subset of the survey winner: security.

Top inhibitors of cloud computing, 2014



Gigaom Research Enterprise IT Buyers Survey, North Bridge Future of Cloud Computing Survey, 2014

Company policies on acceptable cloud usage

To some extent, shadow IT occurs because many companies do not have a policy on acceptable cloud usage in place or the policy is a blanket “don't use the cloud at all,” which isn't practical. IT can eliminate the shadow IT's growth by simply implementing a cloud-usage policy and then adopting tools that will allow it to monitor for adherence.

Cloud security-awareness training programs

IT can add tremendous value by initiating a cloud-security awareness program that not only teaches users how to protect the organization from cloud-delivered security threats, but also how to protect themselves (personally) from similar threats. The public is surprisingly naïve about cloud security. Most employees should be very receptive to a training program that appealed to both organizational issues and their personal issues.

Key takeaways

- In many organizations, shadow IT seems like a shortcut to improved IT services but in reality, it is often an expensive road to disaster. If shadow IT is allowed to run amok, multiple business units will solicit various IT services to meet their individual group's needs. The most immediate impact is the organization being left to sort through a plethora of applications, many of which overlap. For example, a single organization may be running dozens of file-sync-and-share applications.
- Beyond the sheer number of applications in use is the challenge of managing multiple security implementations for each application and each business unit. An organization should apply the same policy throughout business units for all data regardless of the level of sensitivity. This is a best practice for management as well as for data-security.
- As businesses move more and more data into the cloud, and count on the cloud to deliver key services, IT must be a leader ensuring that the organization is using those resources correctly.
- The cloud is not going to replace IT. Instead, the cloud is simply another vehicle for which IT delivers services to users – and IT should use it appropriately.

Methodology

The data in this report is derived from surveys that Gigaom Research and partners conducted between September 2013 and June 2014.

IT Ops and Development Survey, 4Q 2013. The 408 survey respondents came from more than 30 industries, with the top ones including computer software, banking and financial services, government, health care and medical, manufacturing, and insurance. Of those surveyed, 60 percent work in organizations of more than 10,000 people and 98 percent work in organizations with more than 1,000 people. While all respondents work in IT, 62 percent said they were in software-application development while 24 percent said they were in operations including systems and network engineering, help desk, and data centers.

Cloud Adoption Survey, 2Q14. In order to determine the progress of enterprises' journey to the public cloud, Gigaom Research surveyed 303 IT decision-makers to understand what is happening within enterprises that are adopting public cloud computing. This survey was designed to determine emerging patterns of use and patterns of adoption, which, until now, have not been well understood, even by the enterprises themselves.

Enterprise IT Buyers Survey, North Bridge Future of Cloud Computing Survey, 2014. For 2014, Gigaom Research fielded similar questions in two second-quarter (May through June, 2014) surveys:

- One was with a panel of 502 IT decision makers at companies with 500 or more employees (more than half of which included more than 5,000 employees), across a broad range of industries.
- The other survey was in collaboration with North Bridge Venture Partners, which included 369 web-recruited respondents as well as customers of North Bridge startups. Gigaom Research considers the North Bridge survey participants to be more leading-edge, given that they are enterprise customers of tech startups. The North Bridge survey also includes more smaller businesses than in the direct Gigaom Research survey, and a good number of very large organizations, as well.

About George Crump

George Crump is an Analyst for Gigaom Research and the President and Founder of Storage Switzerland. With 25 years of experience designing storage solutions for data centers across the US, he has seen the birth of such technologies as RAID, NAS and SAN. Prior to founding Storage Switzerland he was CTO at one the nations largest storage integrators where he was in charge of technology testing, integration and product selection.

About Gigaom Research

Gigaom Research gives you insider access to expert industry insights on emerging markets. Focused on delivering highly relevant and timely research to the people who need it most, our analysis, reports, and original research come from the most respected voices in the industry. Whether you're beginning to learn about a new market or are an industry insider, Gigaom Research addresses the need for relevant, illuminating insights into the industry's most dynamic markets.

Visit us at: research.gigaom.com.

© 2014 Giga Omni Media, Inc. All Rights Reserved.

This publication may be used only as expressly permitted by license from Gigaom and may not be accessed, used, copied, distributed, published, sold, publicly displayed, or otherwise exploited without the express prior written permission of Gigaom. For licensing information, please [contact us](#).