cloud security alliance®

Cloud Adoption Practices & Priorities Survey Report

January 2015

Acknowledgements

Managing Editors / Researchers
Cameron Coles
John Yeoh

Contributors
Frank Guanco
Ekta Mishra
Luciano Santos

Design/Editing
Kendall Scoboria

Sponsored By

Table of Contents

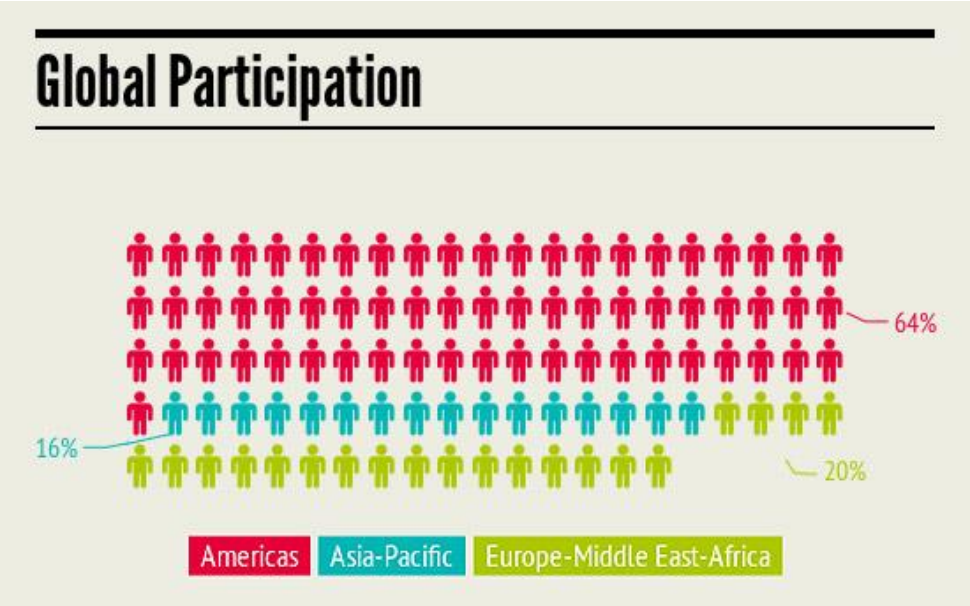
Introduction

The benefits for enterprises moving to the cloud are clear: greater business agility, data availability, collaboration, and cost savings. The cloud is also changing how companies consume technology. Employees are more empowered than ever before to find and use cloud applications, often with limited or no involvement from the IT department, creating what's called "shadow IT." Despite the benefits of cloud computing, companies face numerous challenges including the security and compliance of corporate data, managing employee-led cloud usage, and even the development of necessary skills needed in the cloud era. By understanding the cloud adoption practices and potential risks, companies can better position themselves to be successful in their transition to the cloud.

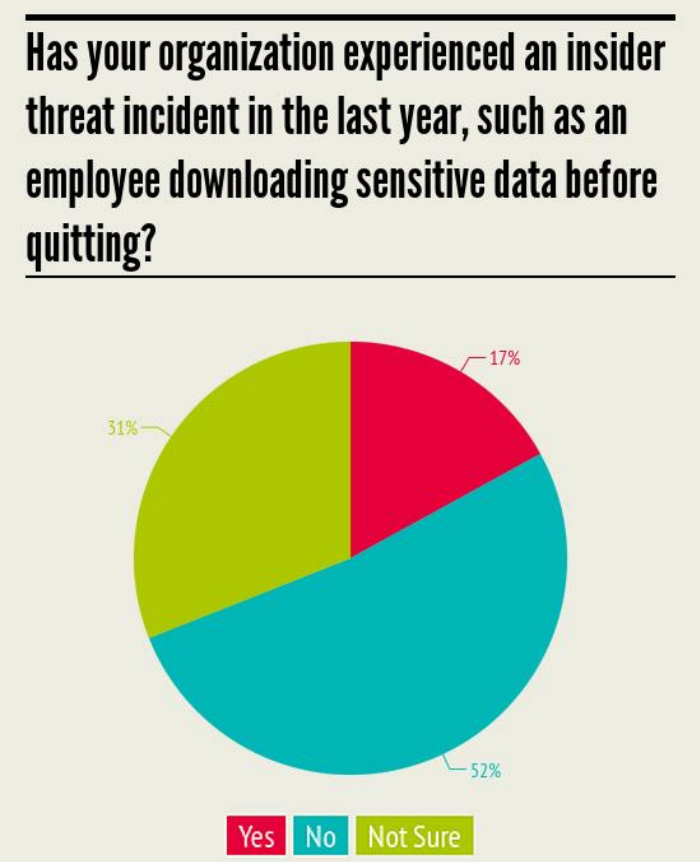
In the 2014 Cloud Adoption Practices and Priorities (CAPP) survey, the Cloud Security Alliance sought to understand how IT organizations approach procurement and security for cloud services and how they perceive and manage employee-led cloud adoption. We asked IT and security professionals for their views on "shadow IT," obstacles preventing cloud adoption, types of cloud services requested and blocked, security priorities, and governance practices. We uncovered stark differences between how companies in North America and Europe approach the cloud, and even how large enterprises differ from their smaller counterparts. As more IT departments look to play a greater role in enabling the safe adoption of cloud services, we hope these findings can provide some guidance.

Survey Participants

The CAPP survey attracted 212 participants globally from IT security (33 percent), IT (25 percent), compliance and audit (10 percent), and other (32 percent) professional roles over a five-week period between the third and fourth quarters of 2014. Participants were spread out globally across 17 different countries and data was compared across the Americas (64 percent), Asia-Pacific (APAC) (16 percent), and Europe-Middle-East-Africa (EMEA) (20 percent) regions.



All major industries were represented in participants from the study, including high tech (21 percent), financial services (13 percent), telecommunications (9 percent), entertainment (8 percent), government (7 percent), healthcare (6 percent), and manufacturing (6 percent). Additionally, organizations ranged in size from 1-5,000 employees (68 percent), 5,001-50,000 employees (19 percent), and 50,001+ employees (14 percent).



State of Security

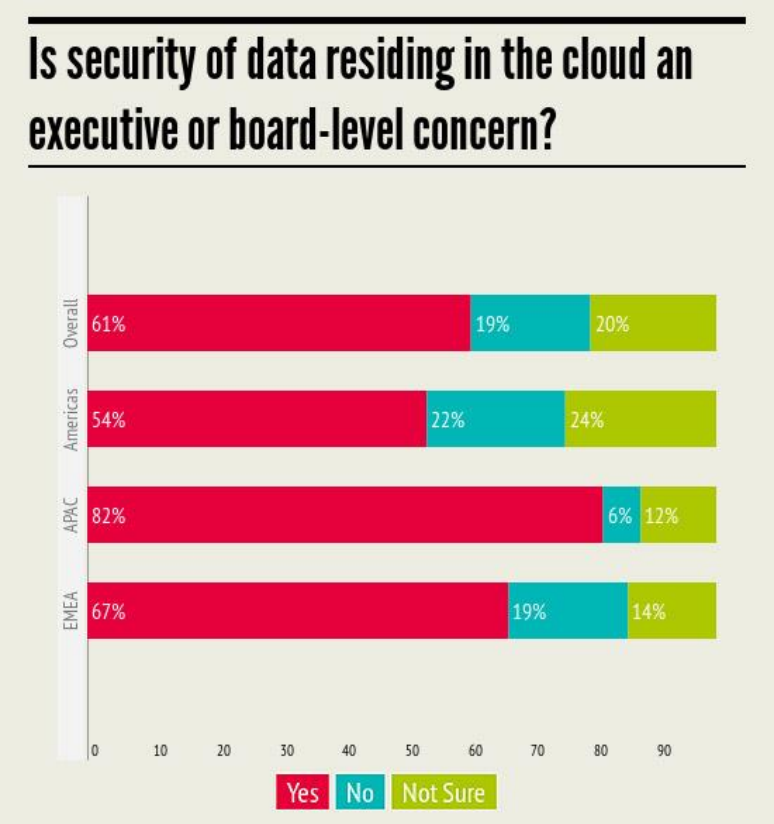
Companies are increasingly under attack as criminal organizations and state-sponsored groups attempt to steal sensitive data. Not surprisingly, IT professionals see the top security issues facing their organizations as malware (63 percent), advanced persistent threats (53 percent), compromised accounts (43 percent), and insider threats (42 percent). Although companies are focused on external threats, 17 percent reported a known insider threat incident in the last 12 months, such as an employee downloading sensitive data before quitting. Troublingly, 31 percent were not sure if such an incident occurred. This uncertainty should raise some concern about whether companies have the right resources to identify and stop these types of threats.

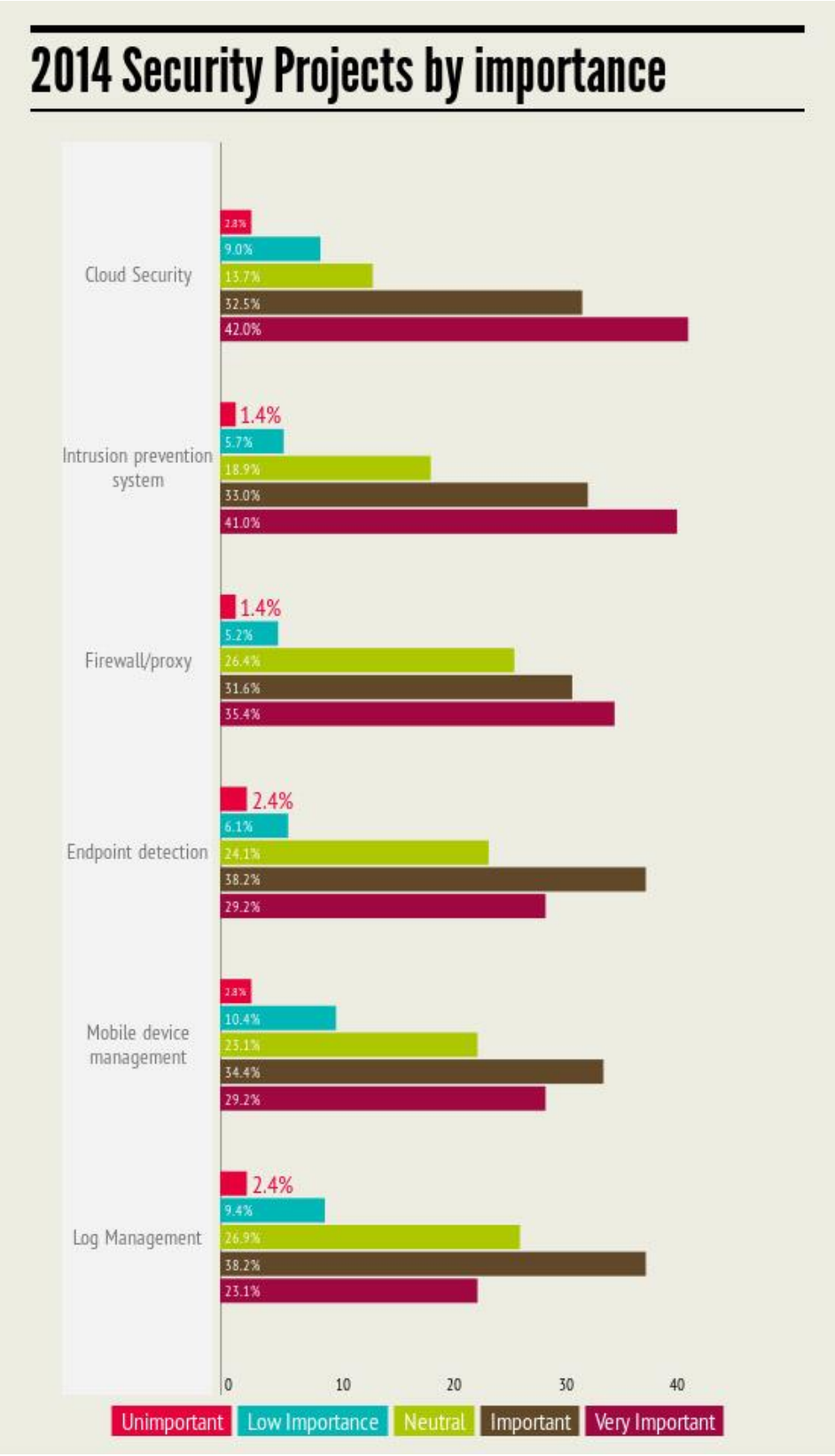
More software vulnerabilities have been uncovered in 2014 than any other year on record.

2014 so far has seen more software vulnerabilities discovered than any previous year and has also seen many attention-grabbing headlines about significant data breaches. But data breaches generate more than bad press. As seen with Target, a large American retail company, they can significantly impact a company's bottom line.

Correspondingly, the security of data in the cloud is now an executive or board-level concern for 61 percent of companies. Executives in the EMEA region are more involved in security discussions, with 68 percent of executives in EMEA concerned about cloud security versus just 54 percent of their counterparts in the Americas. Strict data privacy requirements and suspicion of US surveillance could be driving awareness among EU executives.

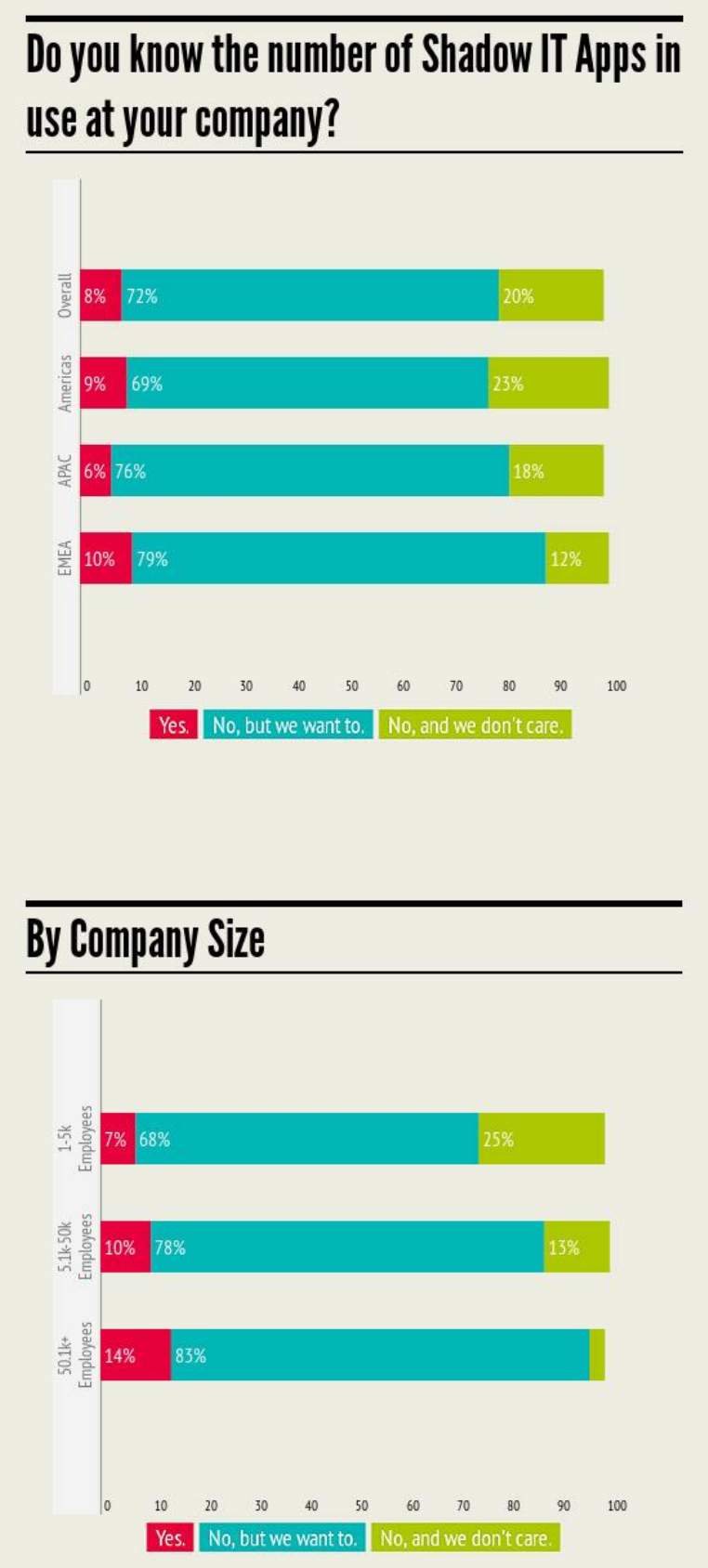
Considering the importance of data in the cloud to executives at companies globally, perhaps it's not surprising that cloud security projects were the





leading IT project in 2014. Globally, 75 percent of companies indicated cloud security projects were important or very important, eclipsing intrusion prevention (74 percent) and firewalls and proxies (65 percent). There are some geographic differences worth noting: 50 percent of companies in Europe view cloud security projects as "very important," versus just 38 percent of counterparts in the Americas. Financial services companies were also much more likely (62 percent) to rate cloud security as very important.

Understanding Shadow IT



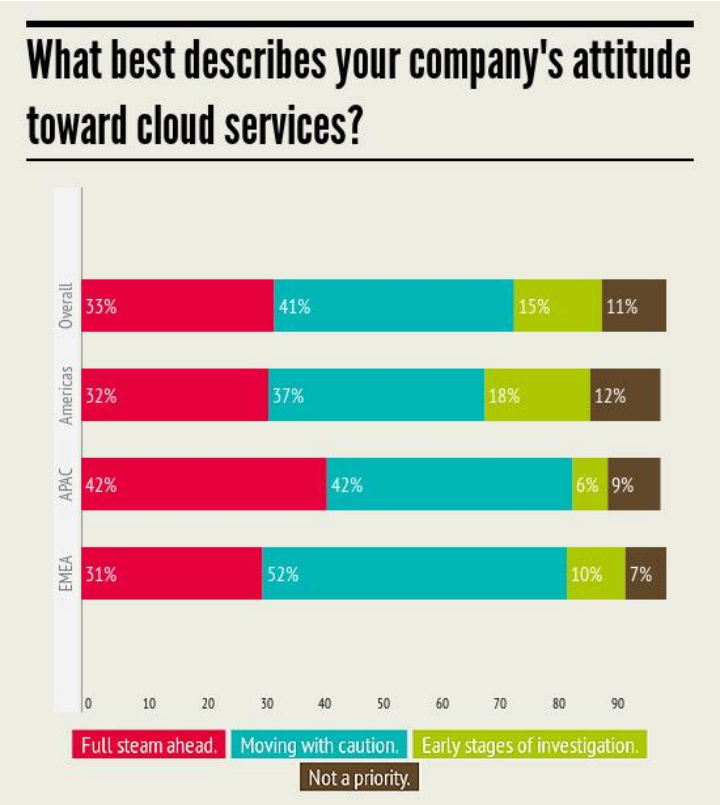
As companies move data to the cloud, they are looking to put in place policies and processes so that employees can take advantage of cloud services that drive business growth without compromising the security, compliance, and governance of corporate data. Companies today are sanctioning the use of some cloud services, but there is also "shadow IT" adoption of cloud apps by individual employees and teams. To understand shadow IT for this survey, a common definition was established for survey participants. Shadow IT was defined as "technology spending and implementation that occurs outside the IT department, including cloud apps adopted by individual employees, teams, and business units."

The survey respondents' primary concerns about Shadow IT are:

- Security of corporate data in the cloud (49 percent)
- Potential compliance violations (25 percent)
- The ability to enforce policies (19 percent)
- Redundant services creating inefficiency (8 percent)

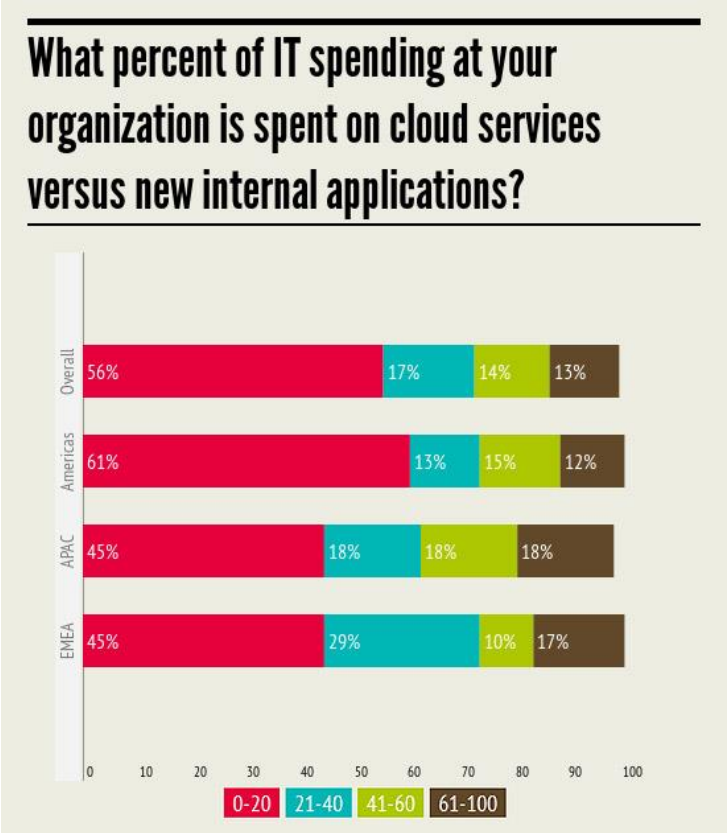
Only 8 percent of companies know the scope of shadow IT at their organizations, and an overwhelming majority (72 percent) of companies surveyed said they did not know the scope of shadow IT but wanted to know. This number is even higher for enterprises with more than 5,000 employees at 80 percent. Globally, 71 percent of respondents were somewhat to very concerned over shadow IT. There are some stark geographic differences, with 85 percent of APAC respondents concerned versus just 66 percent and 68 percent of their Americas and European counterparts, respectively.

Embracing the Cloud

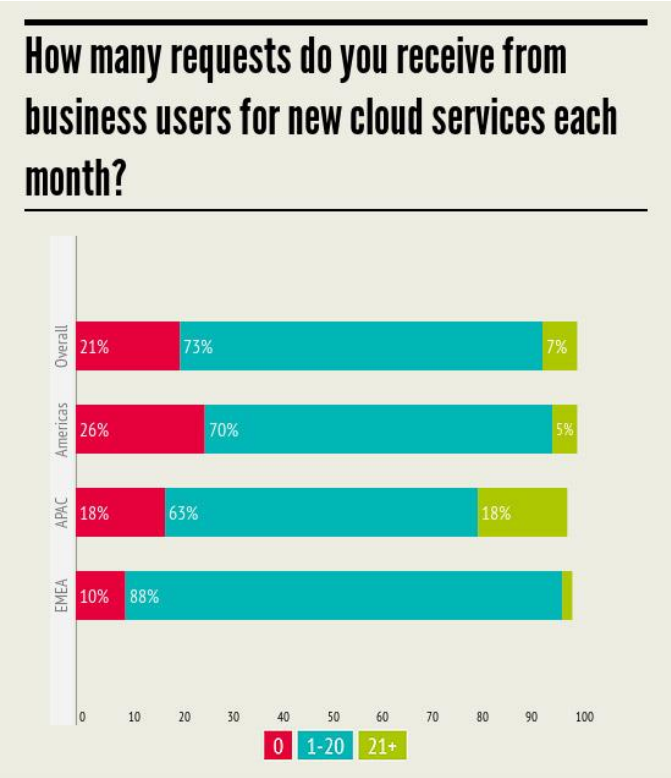


Faced with questions about the security of data in the cloud, IT professionals have been understandably hesitant to take a cloud-first approach to new technology projects. We asked survey participants to describe their company's overall attitude towards cloud services; 33 percent described their attitude as being "full steam ahead" when it comes to cloud services while 41 percent are moving forward with caution. Another 15 percent of companies are in the early stages of investigating cloud services, while 11 percent of companies do not consider cloud a priority. Historically, companies in the US adopt technology earlier than their counterparts in Europe. We found the opposite: 12 percent of companies in the Americas do not consider cloud a priority compared with 9 percent in EMEA and 7 percent in the APAC region. Just 69 percent of companies in the Americas are moving forward with cloud services, compared to 84 percent in other regions.

Globally, 86 percent of companies are spending at least part of their IT budgets on cloud services. However, only 39 percent of companies in the Americas region spend more than 20 percent of their IT budgets on cloud services versus 55 percent in the other regions. The size of the organization also has a significant impact on how much budget is allocated to cloud projects versus on-premises software. Enterprises with more than 5,000 employees spend a lower proportion of their IT budget on the cloud compared with smaller companies. Of companies with more than 5,000 employees, 36 percent spend more than one fifth of their IT budget on cloud services, compared to 49 percent of companies with fewer than 5,000 employees.



IT departments at 79 percent of companies receive requests from the end users each month to buy more cloud applications. Most IT professionals (73 percent) receive between 1 and 20 requests each month while only 21 percent of professionals do not receive any



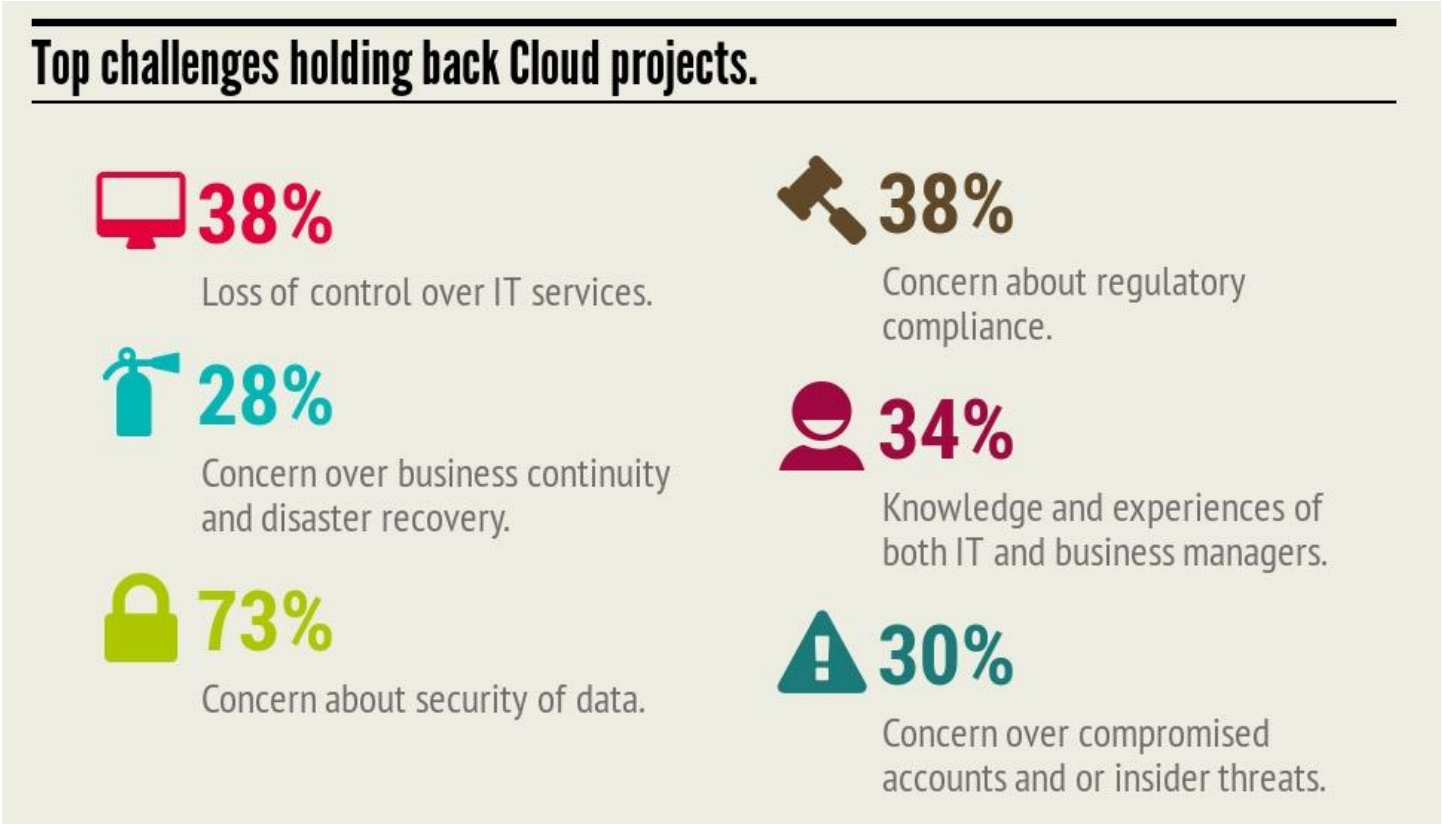
requests. File sharing and collaboration (e.g. Box, Dropbox, Google Docs, Office 365) is by far the most requested cloud category, followed by communication (e.g. HipChat, Skype, WebEx, Yammer), and social media (e.g. Facebook LinkedIn, Twitter).

The list of cloud categories requested includes the most commonly used types of services:

- File Sharing and Collaboration (80 percent)
- Communication (41 percent)
- Social Media (38 percent)
- Content Sharing (27 percent)
- Enterprise Content Management (20 percent)
- Development (20 percent)
- Marketing (20 percent)
- Sales Productivity (18 percent)
- Business Intelligence (16 percent)

Overcoming Challenges

While security remains the top barrier to cloud adoption, a lack of knowledge and experience on the part of IT and business managers is also a significant barrier. This skills gap is an issue for 38 percent of EU companies and 30 percent



of North American companies. IT professionals also face pressure to approve potentially risky technology, with 51 percent of respondents saying they've been pressured to approve an application or device that did not meet the organization's security or compliance requirements. That number grows to 55 percent in Europe and to 73 percent of respondents in the APAC region. This may at least partly explains why 64 percent of APAC respondents had concerns about regulatory compliance compared to 43 percent in the other regions.

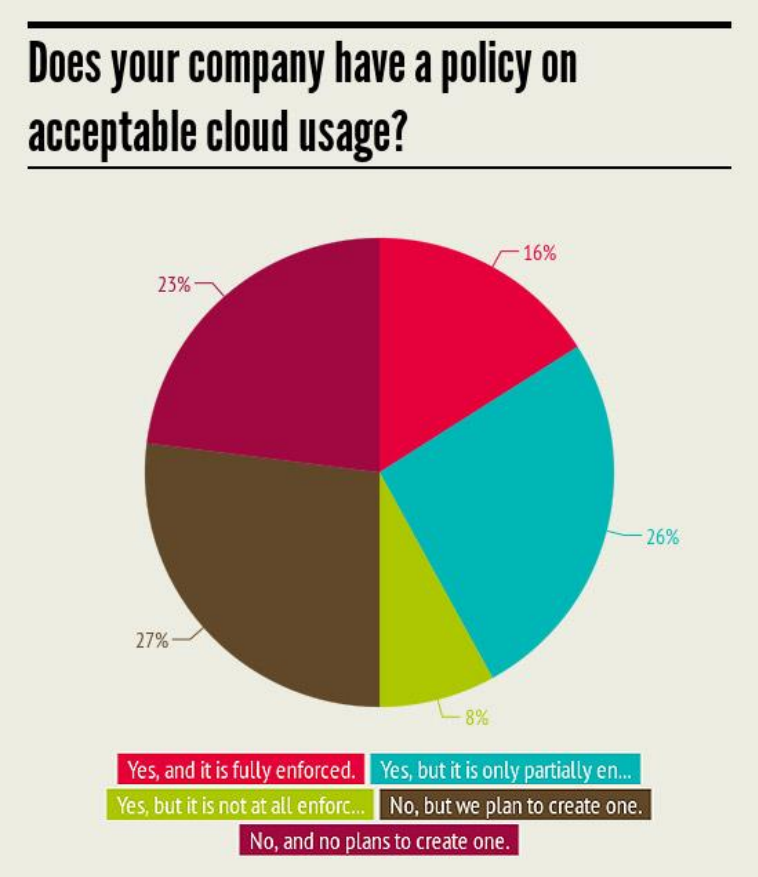
Perhaps due to the perceived challenges around the security of data, regulatory compliance, and control over the cloud, 19 percent of organizations have chosen to block certain cloud services altogether. Survey data revealed that only 7 percent of companies that block cloud apps also know which shadow IT cloud apps are in use at their organization is also problematic. This is problematic; since IT is more likely to block well-known cloud services that tend to have more mature security controls, employees can be forced to find lesser-known but potentially even riskier services to use in their place.

The most-likely cloud services to be blocked include the biggest names in cloud computing:

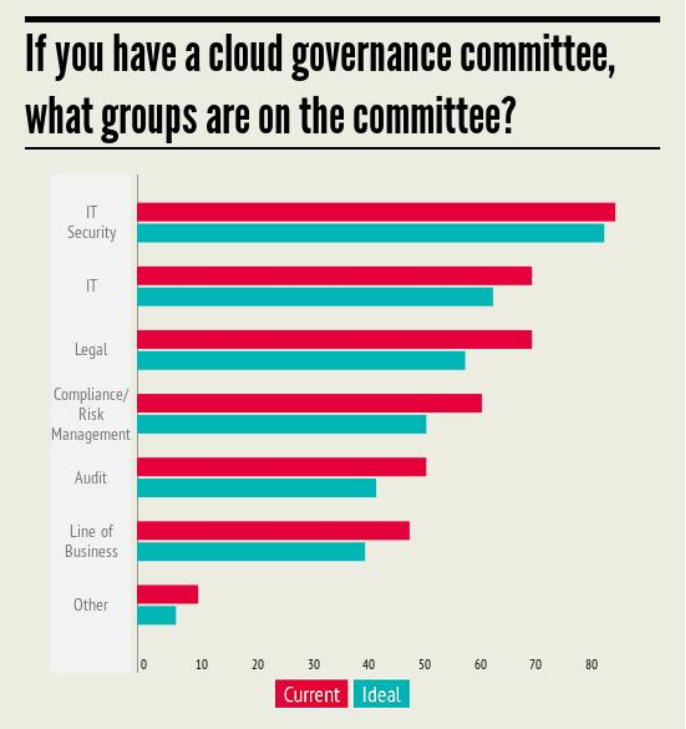
- Dropbox (80 percent)
- Facebook (50 percent)
- Apple iCloud (50 percent)
- Instagram (48 percent)
- Tumblr (45 percent)
- YouTube (40 percent)
- Netflix (40 percent)
- Skype (40 percent)
- Twitter (35 percent)
- Pandora (35 percent)
- LinkedIn (18 percent)

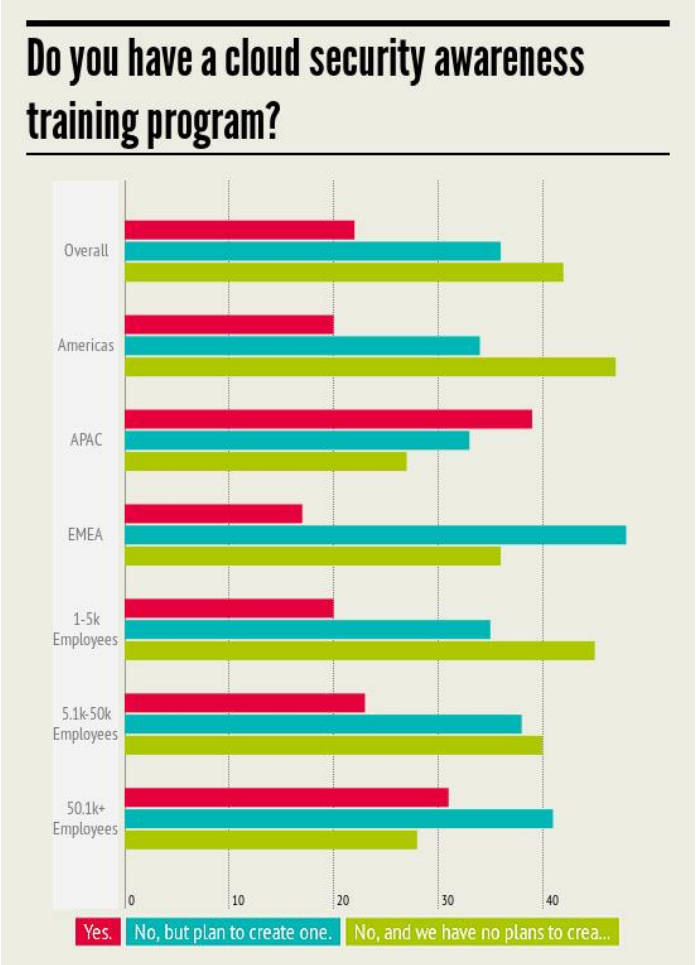
Governing Cloud Usage

As companies develop more mature processes for managing cloud usage, they naturally adopt some of the IT governance practices employed for on-premises applications and data. We found that 50 percent of companies have a policy on acceptable cloud usage today. However, enforcing these policies can be another challenge, as the survey showed that only 16 percent of companies have a policy that is being fully enforced, with another 26 partially enforcing their policy and 8 percent with policies that are not enforced at all.



Fewer companies than expected have a formal cloud governance committee charged with developing and updating policies. Only 21 percent of the companies surveyed have a governance committee, while another 31 percent have plans to create one. Despite the importance of employee-led cloud adoption, the line of business is often left out of the discussion. Line of business leaders were the least likely group to be invited to the table at companies forming a





committee. For companies that already have a committee, only 43 percent include representatives from the line of business. When it comes to enforcing these policies, 63percent of companies prefer to leverage their existing firewall or proxy to control access to cloud services, while a whopping 95 percent of companies with 5,000+ employees prefer this approach versus installing device agents.

To educate employees on the company's policies, 22 percent of organizations have a cloud security awareness training program, while another 36 percent plan to create one. Somewhat paradoxically, although large enterprises lag behind their smaller peers in terms of cloud adoption, they are better positioned to adopt the cloud securely because they have more robust policies and procedures for managing cloud adoption. Companies with more than 5,000 employees are more likely to have a cloud governance committee, have a policy on acceptable cloud usage, and have a security awareness training program compared to companies with fewer than 5,000 employees.

Conclusion

The cloud has clear benefits, but those benefits must be weighed against potential risks. As data moves to the cloud, companies will need to enforce the same security, compliance, and governance policies that they do for data stored on premises. IT will also need to work more collaboratively with business users to understand the motivations behind shadow IT and enable the cloud services that drive employee productivity and growth in the business without sacrificing security. Given both the promise and peril of the cloud, organizations will likely continue investing in the processes and procedures to govern cloud adoption, including security projects that protect data stored in the cloud. Smaller organizations that are rapidly adopting the cloud have the greatest need to invest in these controls, while larger

organizations with more mature governance procedures should seek greater investment in cloud services to maintain a competitive edge against smaller rivals.

About the Cloud Security Alliance

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at http://www.cloudsecurityalliance.org/, and follow us on Twitter @cloudsa.

About Skyhigh Networks

Skyhigh Networks, the Cloud Visibility and Enablement Company, enables enterprises to embrace cloud services with appropriate levels of security, compliance, and governance. Over 200 enterprises including Cisco, DirecTV, Equinix, HP, and Western Union use Skyhigh to manage their “Cloud Adoption Lifecycle” with unparalleled visibility and risk assessment, usage and threat analytics, and seamless policy enforcement. Headquartered in Cupertino, Calif., Skyhigh Networks is backed by Greylock Partners and Sequoia Capital.