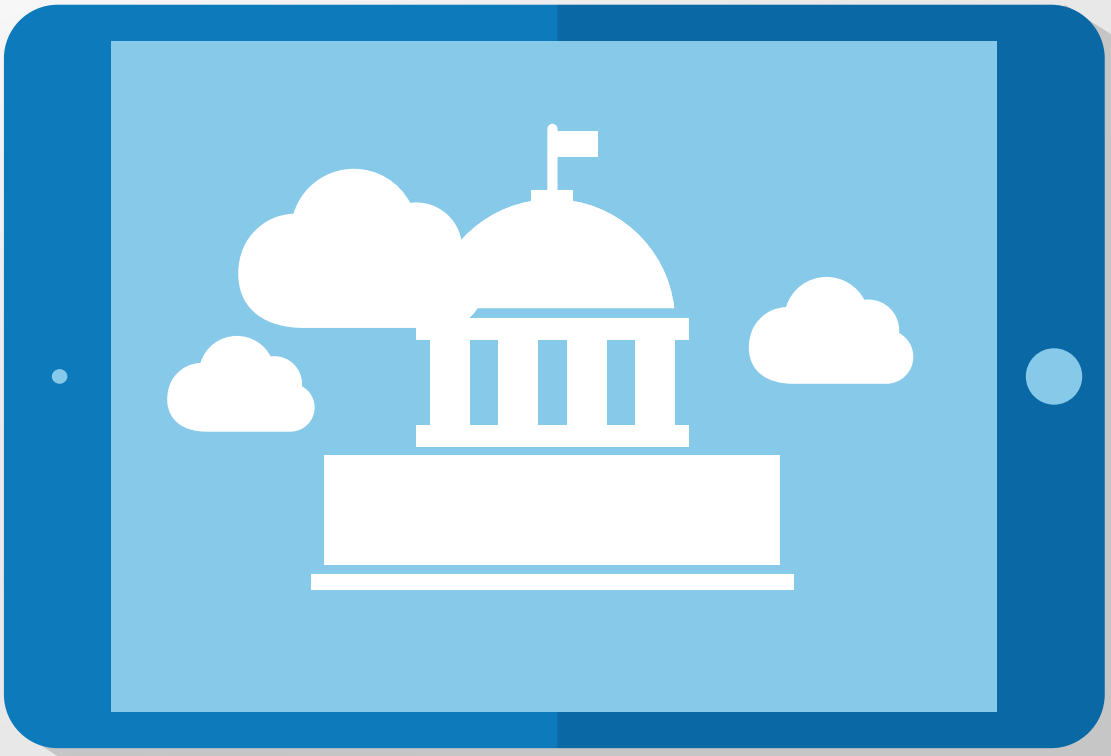
CLOUD ADOPTION & RISK IN GOVERMENT REPORT

Q1 2015

Published Q2 2015



skyhigh

TABLE OF CONTENTS

INTRODUCTION

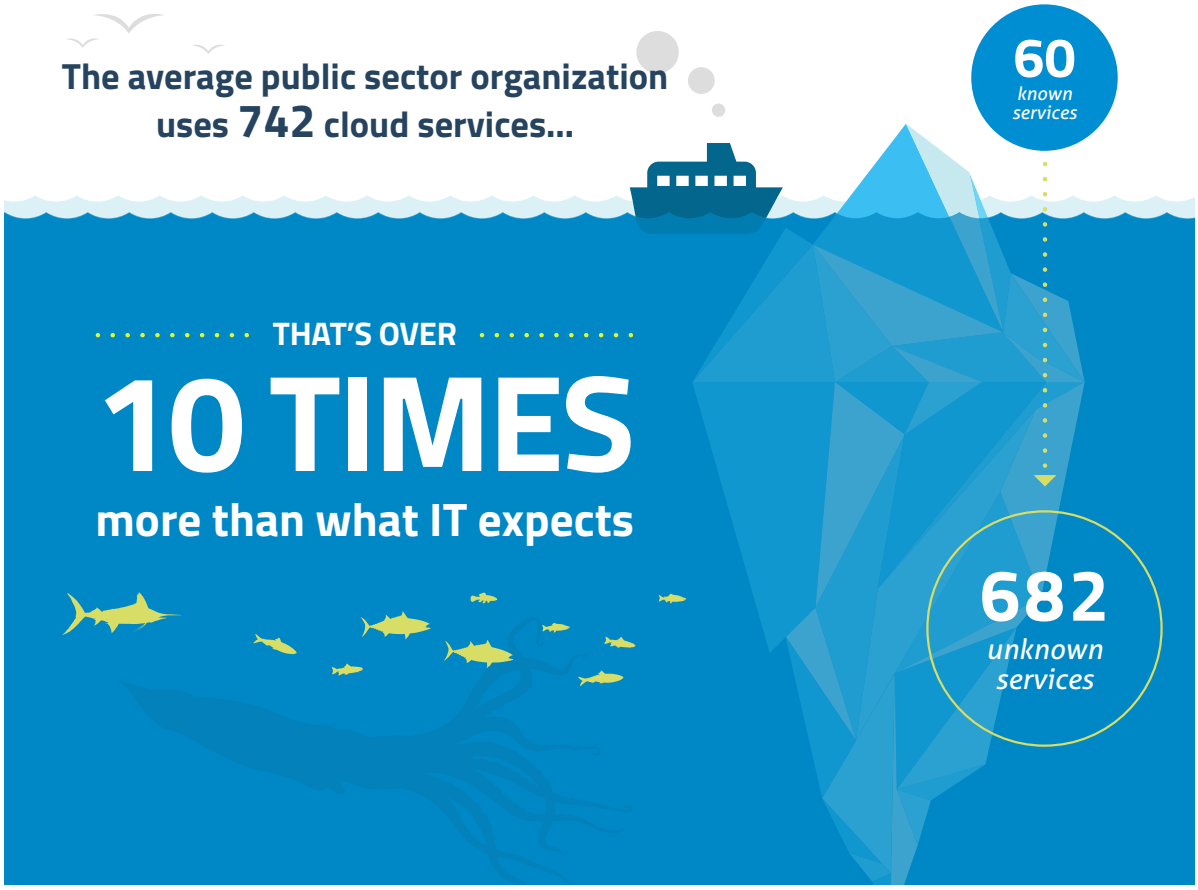
Federal, state, and local governments are migrating to cloud services to take advantage of greater collaboration, agility, and innovation at lower cost. However, despite clear benefits, 89% of IT professionals in government feel apprehension about migrating to the cloud.[1] That being said, many public sector employees are less apprehensive and are adopting cloud services on their own, creating shadow IT. Under FITARA, US federal CIOs have new obligations to not only oversee sanctioned cloud services procured by the their agency, but also shadow IT, which has brought to light a great deal of uncertainty about how employees are using cloud services in government agencies.

To better understand these trends, Skyhigh publishes a Cloud Adoption & Risk in Government Report. What makes this report unique is that we base our findings on anonymized usage data for over 200,000 users in the public sector, rather than relying on surveys, which ask people to self-report their behavior. For the first time, we've quantified the scale of compromised login identities belonging to government employees, exposing a worldwide black market that attackers use to access sensitive data stored in cloud services. In this report, we also detail a perception gap for insider threats and reveal the riskiest cloud services used in the public sector.

[1] Meritalk "The Fabric of Your Data: How to Manage Data in a Multi-Cloud, Multi-Vendor Environment"

OVERVIEW OF CLOUD ADOPTION AND RISK

The Q1 report is based on data from 200,000 public sector employees in the United States and Canada. Both governments have a cloud-first IT policy, but strict security requirements are a barrier to cloud adoption. Another challenge is procurement. The average US Federal agency takes 18 months to define and procure a new software solution, and 54% of employees say their agency is not able to acquire IT in a timely manner.[2] This drives employees to find their own solution, producing "shadow IT". The average public sector organization now uses 742 cloud services, which is 10-20 more than what is known by the IT department.

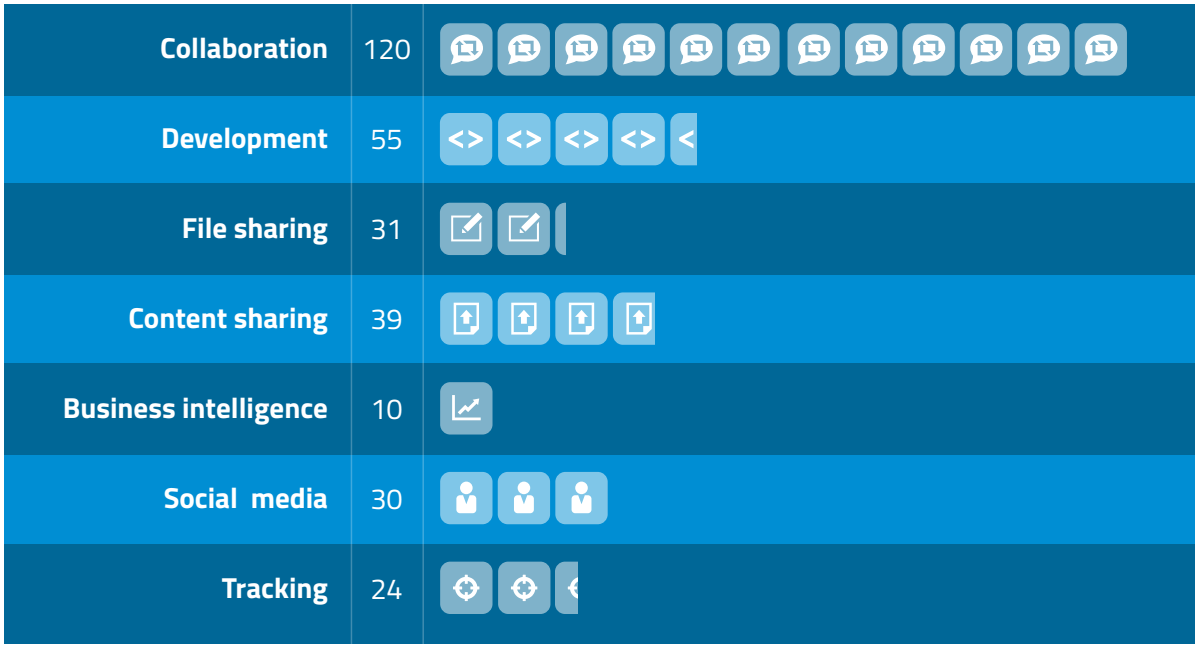


[2] Meritalk "Innovation Inspiration: Can Software Save IT"

By far, the top category of cloud usage in the public sector is collaboration. The average organization uses 120 distinct collaboration services (e.g. Microsoft Office 365, Gmail, etc.), followed by 55 software development services (e.g. SourceForge, GitHub, etc.), 31 file sharing services (e.g. Dropbox, Google Drive, etc.), and 39 content sharing services (e.g. YouTube, LiveLeak, etc.). The average employee uses 16.8 cloud services including 2.9 content sharing services, 2.8 collaboration services, 2.6 social media services, and 1.3 file sharing services. Troublingly, the average public sector employee's movements online are being monitored by 2.7 advertising and web analytics tracking services, which are increasingly used by cyber criminals to inform watering hole attacks.

The average public sector organization uses

many cloud services in each category



CALCULATED RISK

Public sector organizations have unique security concerns. US federal agencies estimate that 32% of their data cannot be moved to the cloud due to security and data sovereignty issues.[3] Of course, the security controls offered by cloud providers vary widely. Analyzing more than 10,000 cloud services across over 50 attributes of enterprise-readiness developed with the Cloud Security Alliance, Skyhigh found that just 9.3% achieved the highest CloudTrust Rating of Enterprise-Ready. Only 10% of cloud services encrypt data stored at rest, 15% support multi-factor authentication, and 6% have ISO 27001 certification.

TOP 10 HIGH-RISK SERVICES *in Government*

BASED ON DATA UPLOADED

1. Smallpdf
2. LiveLeak
3. SourceForge
4. Skypath-Imageshack
5. FilePi
6. DiffNow
7. Convert JPG to PDF
8. JSCompress
9. Online Convert
10. Pdf2jpg.net

BASED ON NUMBER OF USERS

1. DocumentCloud
2. LiveLeak
3. Skypath-Imageshack
4. Use.com
5. KickassTorrents
6. Mixi
7. 4shared
8. Zippyshare
9. Mega
10. ShareBeast

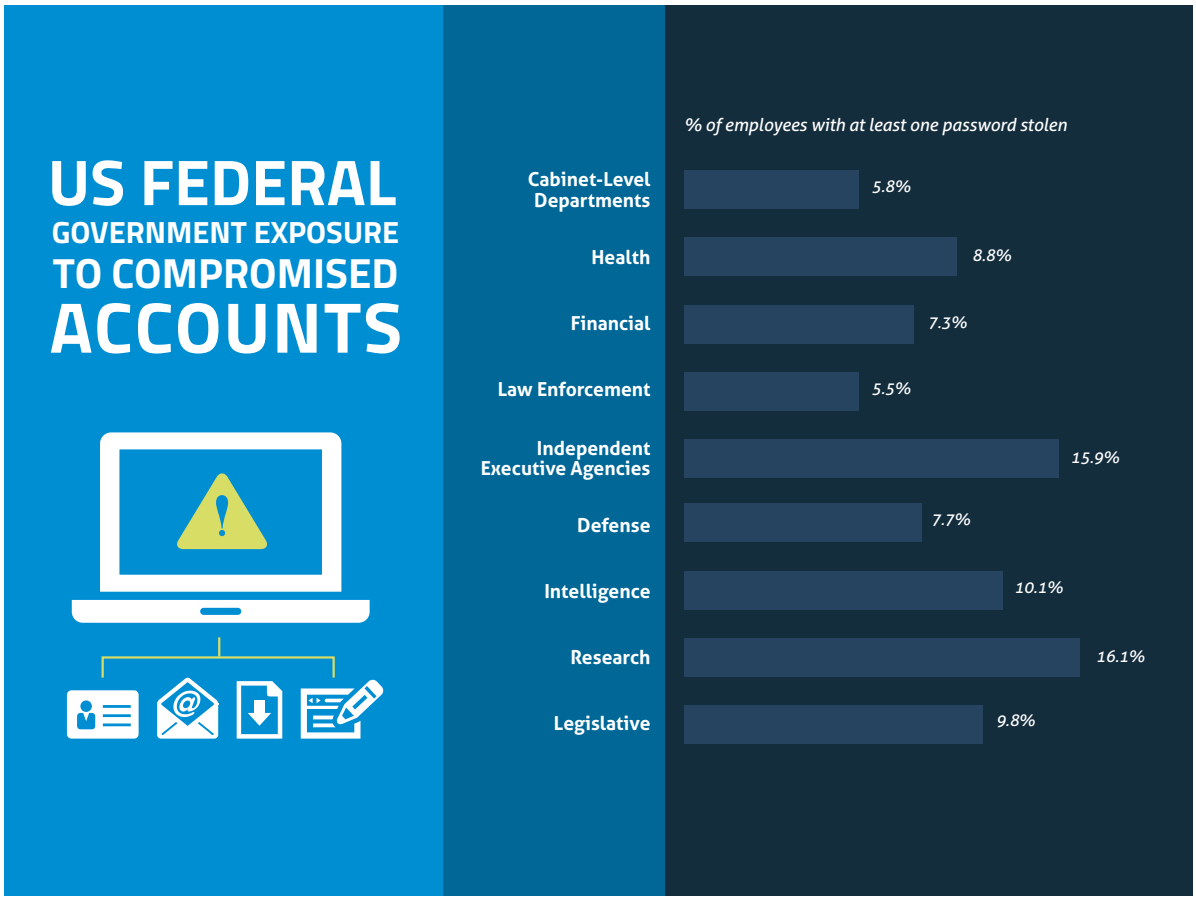
[3] Meritalk 2015 "Cloud Without the Commitment"

While it's now possible to inject additional security controls such as encryption, data loss prevention, and access control on top of cloud applications, some services are simply too risky to permit within public sector organizations. The highest-risk services are hosted in export controlled or embargoed countries, claim ownership of IP uploaded to them, retain data on account termination, or have experienced recent data breaches. We've summarized the top high-risk services based on data uploads and user count in the public sector so organizations can assess the value of these services against their risk and make a decision on whether to allow them or not.

COMPROMISED IDENTITIES

In 2014, there were more software vulnerabilities discovered and more data breaches than any year on record. Following one of the largest breaches of the year, eBay asked 145 million users to change their passwords after attackers stole millions of login credentials. The theft of a username and password in the cloud era is significant because an attacker can gain access to all the data that user has access to in that service. That could include their own data as well as public sector data. Furthermore, a study by Joseph Bonneau at the University of Cambridge showed that 31% of passwords are reused in multiple places.

The implication here is that, for 31% of compromised identities, an attacker could not only gain access to all the data in that cloud service, but potentially all the data in the other cloud services in use by that person as well. Considering the average public sector employee uses more than 16 cloud services, and 37% of users upload sensitive data to cloud file sharing services, the impact of one compromised account can be immense. We investigated this occurrence by looking at anomaly detection data that shows an attacker attempting to login to a compromised account and cross-referencing that with data on user identities for sale on darknet.



We found that 96.2% of public sector organizations have users with compromised identities. At the average organization, 6.4% of users have at least one account that has been compromised. At the time of our analysis, we found that some accounts had been updated with new passwords, while many others remained active with compromised identities. The availability of stolen credentials online is widespread. Anecdotally, we identified one US cabinet-level department with a staggering 55,080 compromised identities. Despite all areas of government being affected, research, health, intelligence, and legislative bodies were particularly at risk. Until more cloud providers enable multi-factor authentication, we recommend users create a unique, strong password for each cloud service and change them regularly.

PERCEPTION VS. REALITY FOR INSIDER THREATS

The most well known example of insider threat is former NSA contractor Edward Snowden, who released classified NSA documents to the press. Your organization may worry about a similar malicious insider leaking data to the media, but more often than not, insider threats are quiet and tend to fly under the radar. Consider an employee taking sensitive data with them when they leave their job for the private sector. In many cases, an organization has no way of detecting this type of insider threat. Since most organizations are focused around a highly visible whistleblower, like Edward Snowden, the perception is that insider threats are rare.

Just 7%

of public sector organizations surveyed reported an insider threat incident in the last year

But 82%

of organizations had behavior indicative of an insider threat

With the Cloud Security Alliance, we surveyed IT and IT security professionals in the public sector and found that only 7% indicated that their organization had experienced an insider threat in the last 12 months. However, looking at actual anomaly detection data, we found 82% of companies had behavior indicative of an insider threat in the last quarter alone. While not all insider threats involve leaking data to the media, the risk of malicious and careless insiders is much higher previously believed.

TOP 20 ENTERPRISE CLOUD SERVICES LIST

The cloud has freed developers to reimagine enterprise software with delightful user experiences, innovative new features, and access from any internet-connected device in the world. With faster release cycles and updates that occur immediately across customers, cloud-delivered software is not only more cost-effective, in many cases it's also first to market with innovative new features. That's why many organizations today choose the top cloud solutions. Not because they're the best cloud option available, but because they're the best software available, period. That's why this list has become one of the most shared findings in our report.

1. Microsoft Office 365
2. Yammer
3. Cisco WebEx
4. ServiceNow
5. SAP ERP
6. Salesforce
7. DocuSign
8. NetSuite
9. Oracle Taleo
10. SharePoint Online
11. TimeTrade
12. Hightail
13. Box
14. GoToMeeting
15. ADP
16. OneDrive
17. Jive
18. Concur
19. Syncplicity
20. SuccessFactors

The top 20 list is dominated by cloud heavyweights: Microsoft (Office 365, Yammer, SharePoint Online, OneDrive), SAP (ERP, SuccessFactors, Concur), Cisco (WebEx), Oracle (Taleo), and Salesforce. It also includes several independent companies that have gone public in the last several years including ServiceNow, Box, and Jive. The list is heavily weighted toward collaboration (6 services), file sharing (4 services), and finance services (4 services). Of the top 20 enterprise cloud services, 17 are delivered by companies headquartered in the United States.

TOP 20 CONSUMER APPS IN THE ENTERPRISE

Today, many consumer applications are so useful, employees use them in their everyday work. This can cause headaches for IT if government data is stored in unsanctioned cloud services known as “shadow IT.” Attackers can also use these services as vehicles to exfiltrate data. For example, Skyhigh discovered attacks that target sensitive company IP, and then leveraged Twitter to exfiltrate the stolen data 140 characters at a time. Our security intelligence team also identified a novel attack that steals sensitive data by encoding the data into video files before uploading them to YouTube where attackers can then download the information and decode it.

Consumer apps can be used for official business, such as Facebook and Twitter to reach constituents and LinkedIn for recruiting. Increasingly, consumer application companies such as Facebook, Dropbox, and Google, are also offering enterprise versions of their services, which include additional security and support features. Despite the fact that many apps may have a legitimate business purpose or enterprise-grade security capabilities, organizations should be cautious and reach a balance between user-centric policies and data security.

TOP 10 FILE SHARING, COLLABORATION, AND SOCIAL MEDIA

File sharing and collaboration cloud services are often a focus of IT and security teams. Social media is highly visible and occupies a significant amount of mind-share with IT departments and executives. Given these trends, this section will review each category in greater detail, along with the top services in use.

TOP SERVICES
by category in Government

	FILE SHARING	COLLABORATION	SOCIAL MEDIA
1.	Google Drive	Microsoft Office 365	Twitter
2.	Dropbox	Yammer	Facebook
3.	Hightail	Cisco WebEx	LinkedIn
4.	Box	Gmail	Tumblr
5.	WeTransfer	AOL	Myspace
6.	OneDrive	Yahoo! Mail	Ning
7.	Syncplicity	Evernote	Meetup
8.	Yandex.disk	Hotmail	LiveJournal
9.	ShareFile	Prezi	Nextdoor
10.	4shared	GoToMeeting	XING

FILE SHARING

The average public sector organization uses 31 file sharing services and the average employee uses 1.3 services. Well-known services Google Drive and Dropbox top the list this quarter. US government organizations may be troubled to find Russian-hosted Yandex. disk on the list and may want to investigate what data employees upload to this service.

COLLABORATION

The use of collaboration services in government is pervasive. The average organization uses 120 services and the average employee regularly uses 2.8 distinct collaboration services. Microsoft takes three spots on the list with Office 365, Yammer, and Hotmail. Conferencing service Cisco WebEx continues to lead GoToMeeting.

SOCIAL MEDIA

The average public sector organization uses 30 social media services and the average employee regularly uses 2.6 services. Twitter, Facebook, and LinkedIn continue to top the list. A relatively new service, Tumblr, is a micro-blogging platform that allows governments to connect with constituents in a new way.

ABOUT SKYHIGH NETWORKS

Skyhigh Networks, the cloud security and enablement company, helps enterprises safely adopt cloud services while meeting their security, compliance, and governance requirements. Over 350 enterprises including Aetna, Cisco, DIRECTV, HP, and Western Union use Skyhigh to gain visibility into all cloud services in use and their associated risk; analyze cloud usage to identify security breaches, compromised accounts, and insider threats; and seamlessly enforce security policies with encryption, data loss prevention, contextual access control, and activity monitoring. Headquartered in Campbell, Calif., Skyhigh Networks is backed by Greylock Partners, Sequoia Capital, and Salesforce.com. For more information, visit us at **www.skyhighnetworks.com** or follow us on Twitter **@skyhighnetworks**.

UNCOVER SHADOW IT

If you'd like to learn the scope of Shadow IT at your organization, including detailed statistics profiled in this report, sign up for a complimentary cloud audit

REQUEST COMPLIMENTARY CLOUD AUDIT

bit.ly/ComplimentaryCloudAudit

"With Skyhigh we discovered a wide range of services, allowing us to understand their associated risks and put in place policies to protect corporate data."

CISCO

Steve Martino
VP Information Security