Government Business Council

One Nation Under Guard

Securing User Identities Across State and Local Government

Underwritten by

One Identity

June 2016

Overview

—

Purpose

According to a report by the Identity Theft Resource Center, nearly 170 million records were compromised last year due to data breaches involving American citizens, with 21.5 million exposed in the Office of Personnel Management alone. In 2016, the government can expect even more sophisticated threats on the horizon, making it all the more imperative that agencies enforce proper identity and access management (IAM) practices.

In order to better measure the current state of IAM at the state and local level, Government Business Council (GBC) conducted an in-depth research study of state and local employees in May 2016. Overall, the results indicate that while state and local audiences are devoting additional resources to improving IAM practices, there is still more that can be done to stem the next wave of cyber attacks.

—

Research Methodology

In May 2016, GBC released a survey on identity and access management to a random sample of print and online subscribers in state and local government. 306 leaders from state and local organizations participated in the survey, 57% of whom self-identify as VP/senior level or higher. Respondents include representatives from at least 26 mission areas. For more information on respondents, please see the Respondent Profile.

Executive Summary

—

Respondents show confidence in IAM practices at their agency

66% of respondents are confident in their agency's ability to ensure access to systems and data is user-appropriate, with 26% overall identifying as "very confident" on this matter. Respondents are similarly favorable when it comes to how their organization manages access privileges for citizens and third party contractors. 81% of respondents trust in the procedures their agency uses to manage access for citizens, and 78% trust in the procedures their agency uses to manage access for third party contractors.

—

Agencies may need to expand IAM tools, including MFA

Over half of all respondents affirm their agency requires periodic password changes (52%) and strong password requirements (52%) to ensure security of user access. While these provide some security, the growing sophistication of cyber attacks has made investing in multifactor authentication increasingly imperative for protecting data. However, only 1 in 10 claim to use hardware or software tokens to cross-check their user access, and even fewer report verifying their identity through SMS (5%) or biometrics (3%). Without such extra security measures in place, agencies leave themselves more vulnerable to cyber attacks that can overcome conventional password safeguards.

—

Top IAM challenges require strong leadership and oversight

Even though respondents are mostly confident in the processes their organizations use to ensure access is appropriate, they also cite governance and authorization as the top IAM challenges (33% and 27%, respectively) facing their organizations. Employees are less likely to cite provisioning, deprovisioning, and authenticating users as IAM challenges, perhaps because these can be construed as functional challenges, potentially treatable through automation. Governance and authorization, however, require leaders who can anticipate IAM vulnerabilities and provide critical oversight to user security.

—

Greater awareness and oversight of privileged users is needed

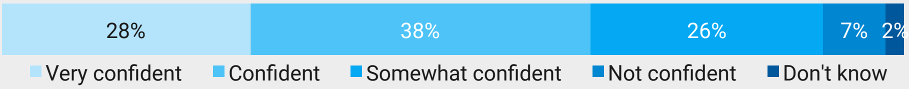
Agency leaders also have an opportunity to address knowledge gaps in IAM practices. 1 in 5 respondents are unaware of what IAM practices their organization uses, and 24% are unsure how often, if at all, their agency enforces password changes. Furthermore, even though one fourth claim their organization never enforces admin password changes, 63% feel that improved oversight of privileged accounts could reduce the likelihood of a security breach.

Research Findings

With few reservations, employees are confident in their agency's ability to assign appropriate IAM

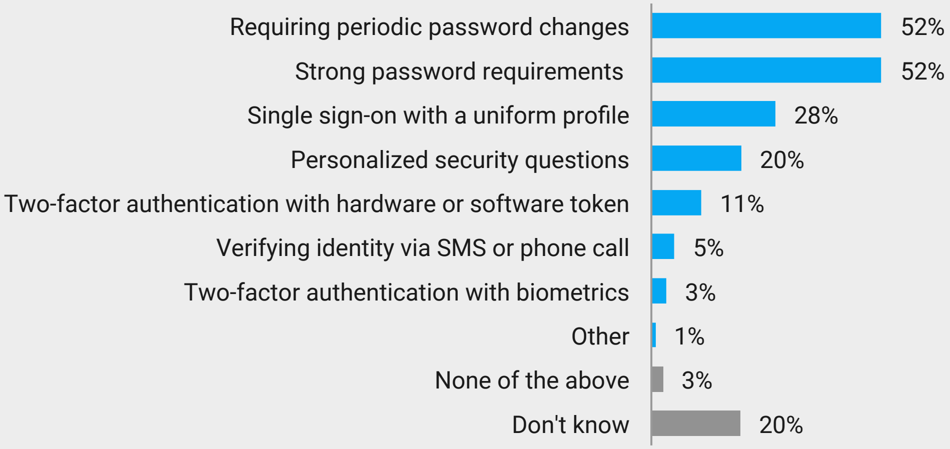
66% of respondents are either confident or very confident in their organization's ability to ensure access to systems and data is appropriate, in that it meets the specific user's security status and role requirements. 26% indicate they are somewhat confident, only 7% indicate they are not confident, and 2% are unsure of their position on this issue.

How confident are you in your organization's ability to ensure access to systems and data is appropriate?



Percentage of respondents, n=233
Note: Percentages may not add up to 100% due to rounding

Which of the following IAM techniques or practices does your organization use to ensure the security of user access?



Percentage of respondents, n=233
Respondents were asked to select all that apply

66%

of respondents are confident in their organization's ability to assign appropriate access.

Over half (52%) of respondents identify both periodic mandatory password changes and strong password requirements as the most common techniques used by their organizations to ensure security of user access. While 28% acknowledge using a "single sign-on with a uniform profile," the use of multifactor authentication to verify this process is less common. Only 1 in 10 indicates the use of hardware or software tokens to cross-check their user access, and even fewer report verifying their identity through SMS (5%) or biometrics (3%).

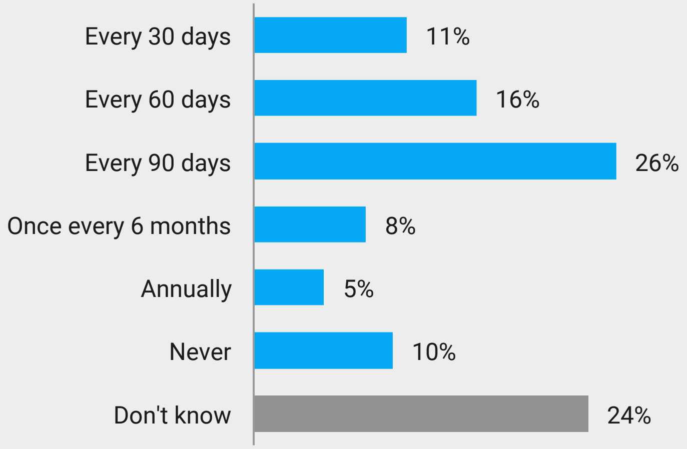
As used in the survey, "appropriate access" is that which meets the specific user's security status and role requirements.

Respondents’ evaluations of updating measures (e.g., password changes) are across the board

When asked how frequently their organization enforces updating measures, such as password changes, to ensure security of user access, responses are mixed. 11% say their organization enforces such updates every 30 days, 16% every 60 days, and 26% every 90 days. Only 13% say these measures occur either “once every 6 months” or “annually”.

Most disconcerting is the finding that 10% have never been required to change their password, and that 24% are not sure if they have ever been asked to or not. That means that approximately 1 in 3 respondents (34%) have either never been forced to update their password or simply have no awareness of the matter.

In your experience, how frequently does your organization enforce updating measures (e.g., password changes) to ensure continued security of user information?



Percentage of respondents, n=225
Note: Percentages may not add up to 100% due to rounding

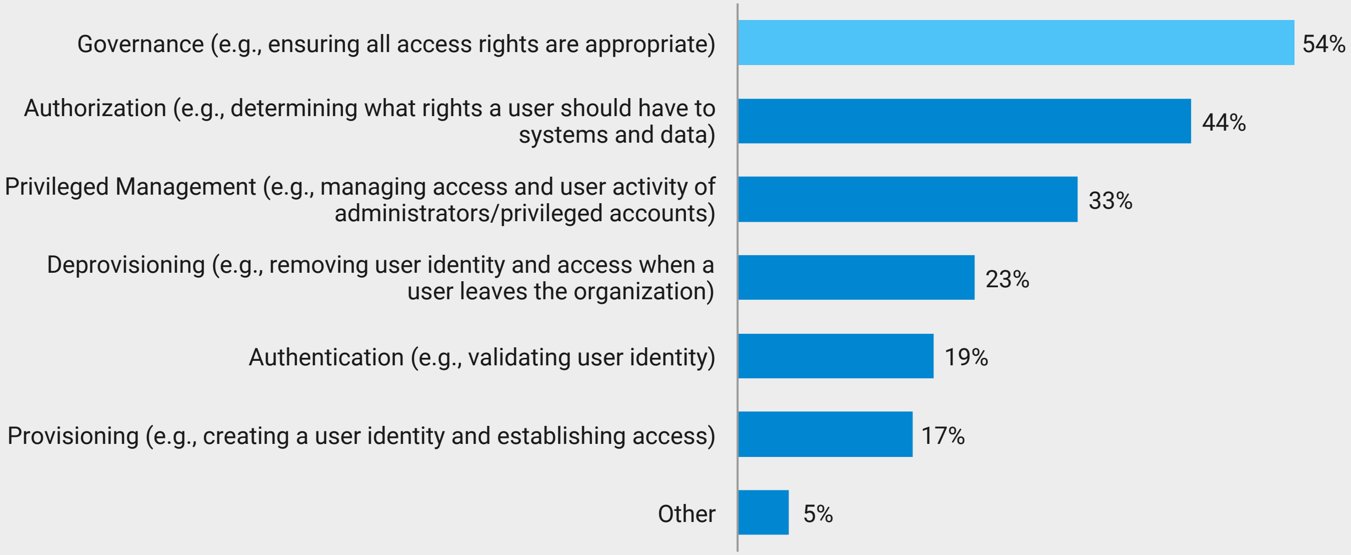
10% of the U.S. Census Bureau’s 2014 census of state and local government employees amounts to approximately 1.4 million full-time whose passwords remain unchanged from year to year.

10%
of respondents say they are never required to change their passwords at all.

Respondents cite governance of appropriate access as top IAM challenge

Even though employees express general confidence in their organization's ability to assign user access appropriately, they also consider governance and authorization of this process to be the most challenging to their IAM practices.

In your opinion, which of the following identity and access management practices are most challenging to your organization?



Percentage of respondents familiar with subject matter, n=123
Respondents were asked to select all that apply

It's possible that respondents regard governance and authorization as most challenging because enacting change to such processes requires greater strategic oversight and buy-in from senior leaders. Other tasks, like deprovisioning (23%) and provisioning (17%), on the other hand, are more functional in nature and potentially less challenging as they can be treated through automation.

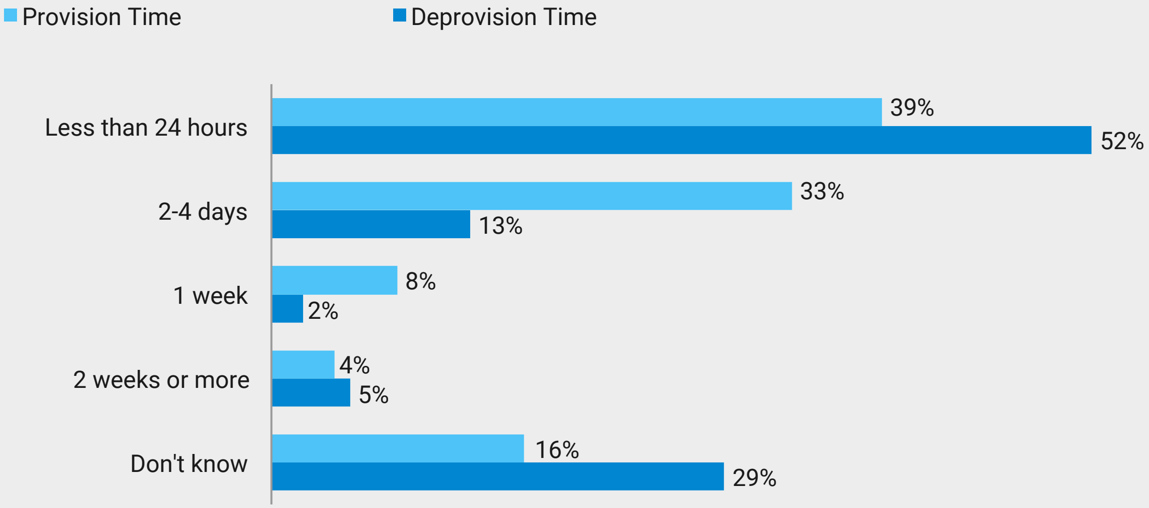
"Other" includes responses such as complying to local mandates for open government, having adequate staff, storage, and revoking rights upon an employee transfer.

54%
of respondents cite governance as the top identity and access management challenge.

Deprovisioning user access is faster, but also more challenging than provisioning

Interestingly, while respondents indicate deprovisioning a user (e.g., removing user identity and access: 14%) is slightly more challenging than provisioning a user (e.g., creating identity and establishing access: 10%), they also report that deprovisioning takes less time.

Organizations take less time to deprovision current users (e.g., retirees, terminations) from appropriate systems than they take to provision new users (e.g., new hires).



Percentage of respondents, n=225 and 223, respectively
Note: Percentages may not add up to 100% due to rounding

Whereas 52% of respondents say it takes less than 24 hours to deprovision a user, 39% say it takes the same amount of time to provision new users. On the other hand, when it comes to provisioning new hires with access, 72% of respondents say this is achieved in less than 4 days. By comparison, 65% say it takes less than 4 days to deprovision user accounts.

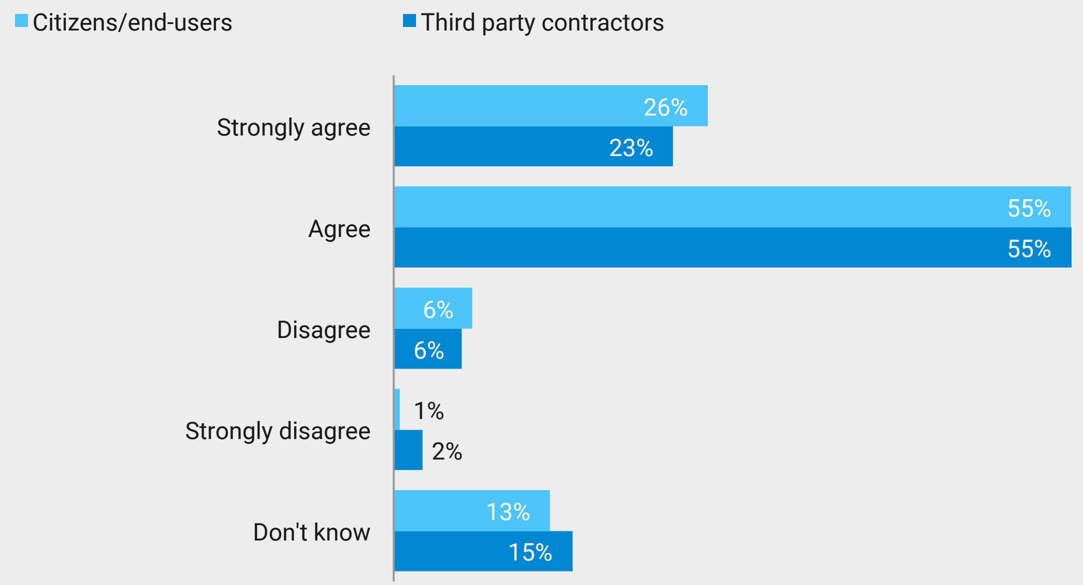
The bottom line: poor or delayed deprovisioning practices constitute a major source of security compromise, therefore any amount of time where a terminated user maintains access should be considered unacceptable.

72%

of respondents say it takes 4 days or less to fully provision a new hire with appropriate access.

Representatives trust the procedures their organization uses to provide access to citizens and third party contractors alike

I trust the procedures my organization has in place for managing access for…



Percentage of respondents, n=220 and 220, respectively
Note: Percentages may not add up to 100% due to rounding

When asked if they trust the procedures their organization has in place for managing access for citizens and end users, 81% of respondents agree or strongly agree that such procedures are trustworthy.

Similarly, 78% agree or strongly agree that the procedures for managing access for third party contractors are also trustworthy. Only 1 or 2% express strong distrust of how their organization manages access for both parties, a sign that - overall - employees are confident in agency IAM processes for external users.

81%

of respondents trust the procedures their organization has in place for managing access for citizens.

Privileged User Management

New guidance in tightening privileged management

In the 2015 Cybersecurity Strategy and Implementation Plan, the U.S. Office of Management and Budget (OMB) highlights the importance of tightening policies and practices for **privileged users** as a method for strengthening cyber defense, among them being:

- inventory and validate privileged account scope and numbers
- minimize the number of privileged users
- limit functions that can be performed when using privileged accounts
- limit the duration that privileged users can be logged in
- limit the privileged functions that can be performed using remote access
- ensure that privileged user activities are logged and regularly reviewed

Understanding the privileged user

Privileged users are employees (e.g., system administrators) who have higher-level access to the administrator accounts on servers, networking devices, operating systems, applications, and/or databases that are used to install, configure, and manage these systems. A privileged user may have access to one or more of the following types of accounts:

- **local administrative accounts** (e.g., provides access to the local host, typically with the same password shared across an organization)
- **privileged user accounts** (e.g., provides admin privileges on one or more systems, typically with a unique and complex password)
- **domain administrative accounts** (e.g., gives privileged admin access across all workstations and servers within a Windows domain)
- **emergency accounts** (e.g., provides unprivileged users with admin access to secure systems in case of an emergency)
- **service accounts** (e.g., gives privileged local or domain access which can be used by an application or service to interact with the operating system)
- **application accounts** (e.g., used by applications to access databases, run batch jobs or scripts, or provide access to other applications, and usually have broad access to underlying company information that resides in applications and databases)

Due to the elevated influence they wield over key infrastructures and accounts, managing and monitoring privileged users is critical to maintaining strong information security. Therefore, given the limited level of access to these types of accounts, some of the questions below include responses only from those who reported some level of familiarity with the subject matter.

> “
> If you’re just coming in to look at data, I don’t care who you are [...] We have to assume that all of our networks are compromised.

Ann Dunkin, CIO at Environmental Protection Agency

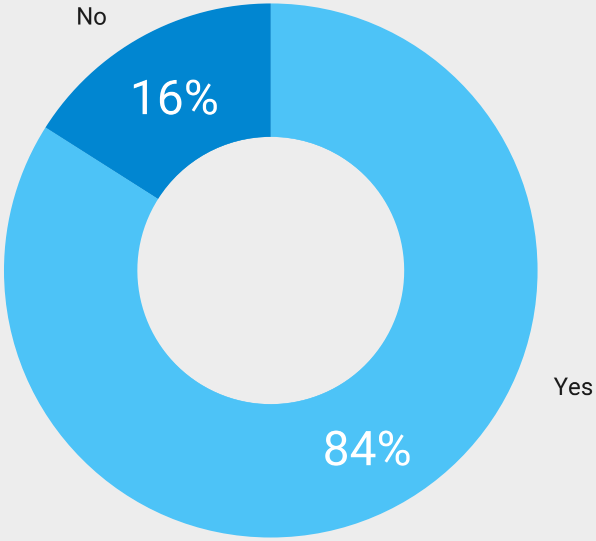
Remarks by the CIO at the Institute for Critical Infrastructure Technology Forum, April 25, 2016.

Administrative Findings

Overall, respondents confirm agency has process in place for changing administrative password

–

Does your organization have an official process for changing the default administrator password that comes with newly installed hardware or software?



Percentage of respondents familiar with subject matter , n=89
Note: Percentages may not add up to 100% due to rounding

84%

of respondents affirm their organization has a process for changing the admin password that usually accompanies newly installed hardware or software.

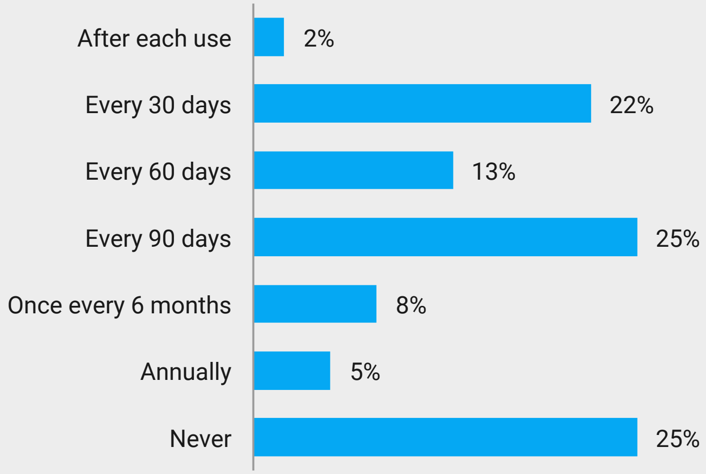
Only 16% say no such process exists.

Respondents indicate negligent administrative password policies

Whereas 53% of general users report changing their passwords at least once every 90 days or less, the statistics for administrative users, who yield much higher access authority and privileges, are no less concerning. Overall, 62% of respondents report their organization changes its administrator password at least once every 90 days or less. 22% of respondents report an update every 30 days, 13% every 60 days, and 25% every 90 days.

However, 13% say the administrator password is changed only every 6 months (8%) or just once every year (5%). And it is telling that 1 in 4 respondents (25%) are confident their organization never changes its administrator passwords at all.

In your experience, how frequently does your organization change its administrator passwords?



Percentage of respondents familiar with subject matter, n=60
Note: Percentages may not add up to 100% due to rounding

Since privileged accounts have elevated access to sensitive data and critical infrastructure, it is particularly crucial that the passwords used to secure access to them abide by more stringent security standards than those expected of general user passwords.

The National Institute of Standards and Technology (NIST) stresses the importance of enforcing proper admin protocol, mentioning that if even "a single machine is compromised, an attacker may be able to recover the password and use it to gain access to all other machines that use the shared password." Therefore, organizations who opt for convenience by sharing passwords among admin accounts and failing to enforce more frequent password updates expose themselves to substantial risk.

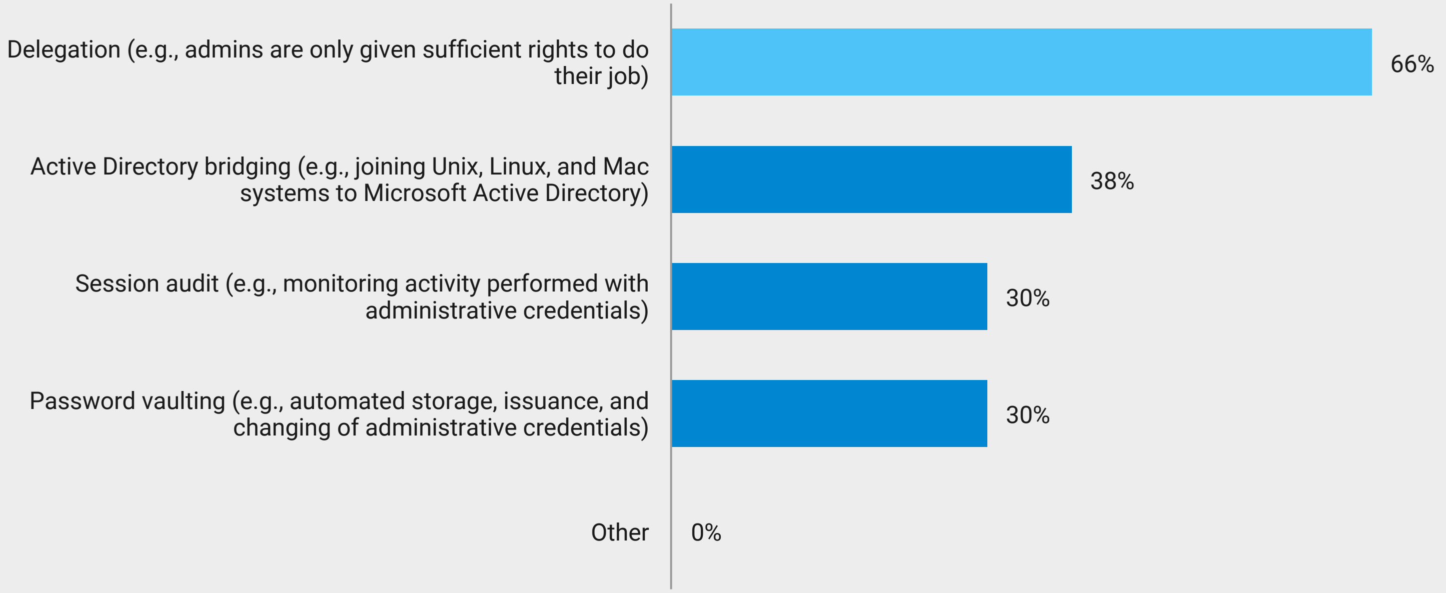
1 in 4

respondents claim their organization never changes its administrator password whatsoever.

Respondents identify delegation as most common management practice for privileged accounts

Among the management practices listed, nearly two thirds of respondents (66%) cite delegation (e.g., implementing a least-privilege model of administrative activity where administrators are only given sufficient rights to do their job) as the technique used to manage access to privileged accounts. This is more popular than alternative practices like Active Directory bridging (38%), session audits (30%), and password vaulting (30%).

Which of the following management practices does your organization currently use to manage access to privileged accounts?



Percentage of respondents familiar with subject matter, n=64
Respondents were asked to select all that apply

It is particularly concerning that only 8% of all respondents report their organization uses all four recommended practices (i.e., delegation, active directory bridging, session audits, password vaulting) when managing access to privileged accounts. Furthermore, the fact that only 2% say their organizations actively change their admin passwords after each use seems to suggest these measures are not being utilized to their intended purpose.

In the survey, delegation entails "implementing a least-privilege model of administrative activity where administrators are only given sufficient rights to do their job."

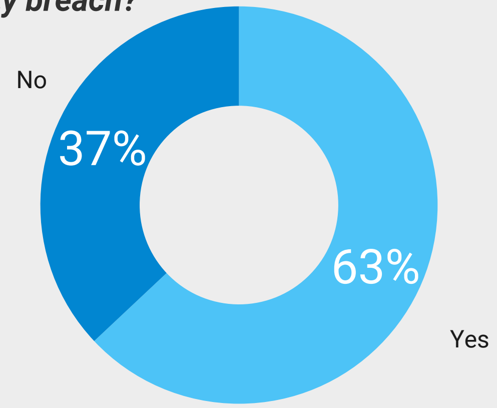
66%

of respondents cite delegation as most commonly used practice for managing privileged accounts.

A majority of respondents favor improved oversight of privileged users to boost security

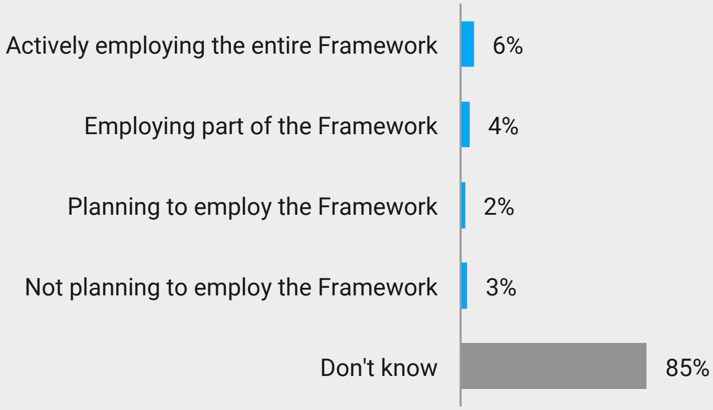
When asked for their opinion on whether improved oversight of privileged accounts would reduce the likelihood of a security breach, nearly two thirds (63%) say that it would versus 37% who believe it would provide no extra security.

In your opinion, would improved oversight of privileged accounts reduce the likelihood of a security breach?



Percentage of respondents familiar with subject matter, n=100
Note: Percentages may not add up to 100% due to rounding

Is your organization currently employing the NIST Cybersecurity Framework for your organization's cybersecurity risk management?



Percentage of respondents, n=206
Note: Percentages may not add up to 100% due to rounding

When asked if their organization is using the **NIST Cybersecurity Framework** to guide their cybersecurity risk management, 10% say they are employing either the entire framework or just part of the framework currently. Only 2% indicate their organization plans to use the framework in the future, and 3% say the framework isn't being used or planning to be used any time soon. A large majority of respondents (85%), however, are unaware of their organization's position regarding the NIST framework.

> “
>
> By Executive Order, the NIST Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

NIST Cybersecurity Framework

“

While we’re all about open data, sharing data, making it available, we [also] need to protect those systems and those types of information. There needs to be a balance between what’s open, what’s shared, and what we actually have to keep in house.

Maria Roat, CTO at Department of Transportation

Remarks by the CTO at the Institute for Critical Infrastructure Technology Forum, April 25, 2016.

Looking Forward

When considering how to improve managing user identities and access privileges:

—

Agencies should expand IAM techniques to prepare for more sophisticated threats

Although employee confidence in agency IAM capabilities is high, employee data will continue to be at risk so long as agencies delay implementing IAM best practices. One area of potential investment is multifactor authentication, to verify user identities by requiring an extra level of authentication unique to that user (e.g. SMS text, biometrics, hardware token). Policies regarding password requirements and periodic password updates also may need to be reinforced, especially when 1 in 10 respondents indicates their organization never enforces such updating measures at all and nearly 1 in 4 admits not knowing how often such measures take place.

—

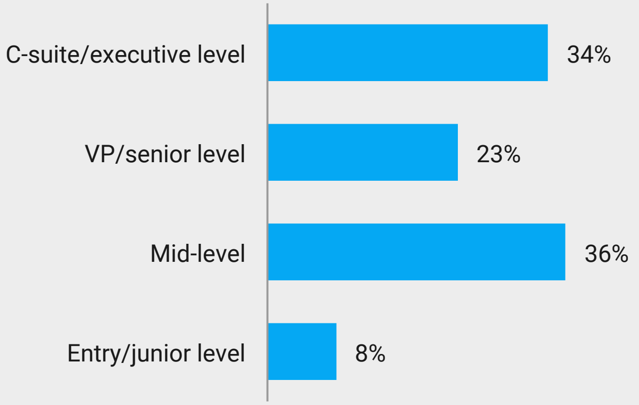
Agency leaders have an opportunity to educate employees in IAM practices, including issues in privileged management

Moving forward, agencies might focus more on making sure employees are cognizant of challenges and best practices in the field of IAM, including privileged access management and administrator account policies. In light of new threats and employee concerns, IT leaders may review the merits of various privileged management practices (e.g., delegation, password vaulting), the ways these practices affect information security, and why improved oversight of these practices can reduce the likelihood of a security breach. Together, both improved processes and stronger internal communication can help agencies more effectively address vulnerabilities and prevent potential information or access breaches.

Respondent Profile

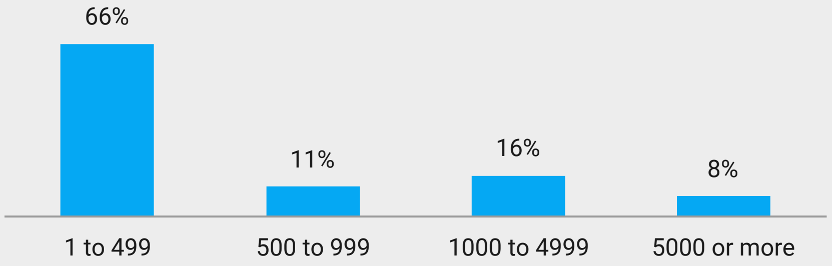
Survey respondents are largely senior state and local leaders

Job grade



Percentage of respondents, n=194
Note: Percentages may not add up to 100% due to rounding

Organization Size



Percentage of respondents, n=194
Note: Percentages may not add up to 100% due to rounding

57%

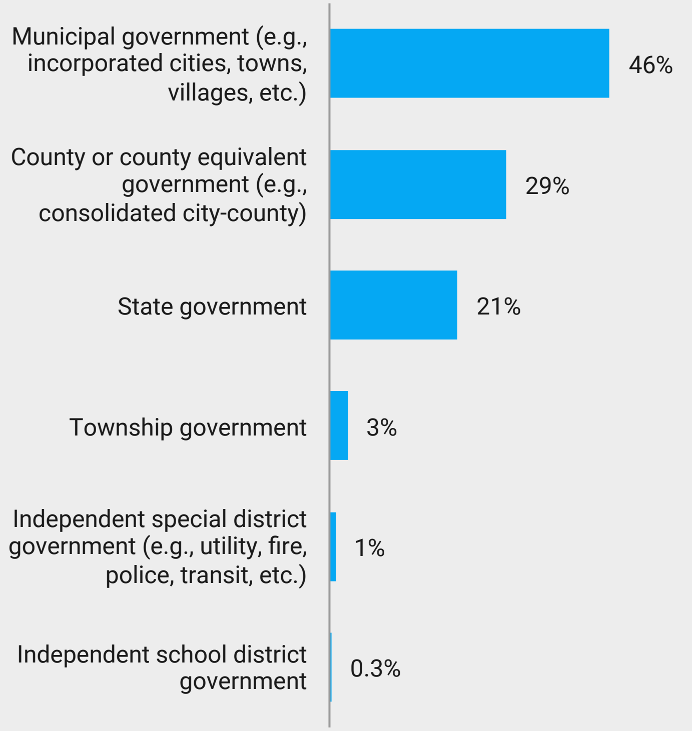
of respondents rank VP/senior level or above.

35%

of respondents work at organizations employing 500 employees or more.

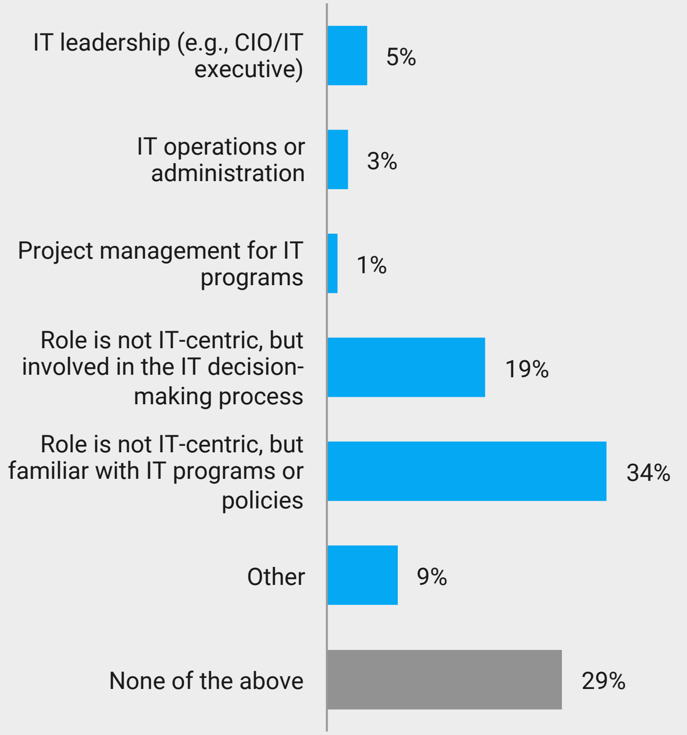
Respondents represent a variety of state and local organizations, plus varying degrees of authority and involvement in IT-related decisions / Respondent Profile

Employment Situation



Percentage of respondents, n=309
Note: Percentages may not add up to 100% due to rounding

IT Involvement



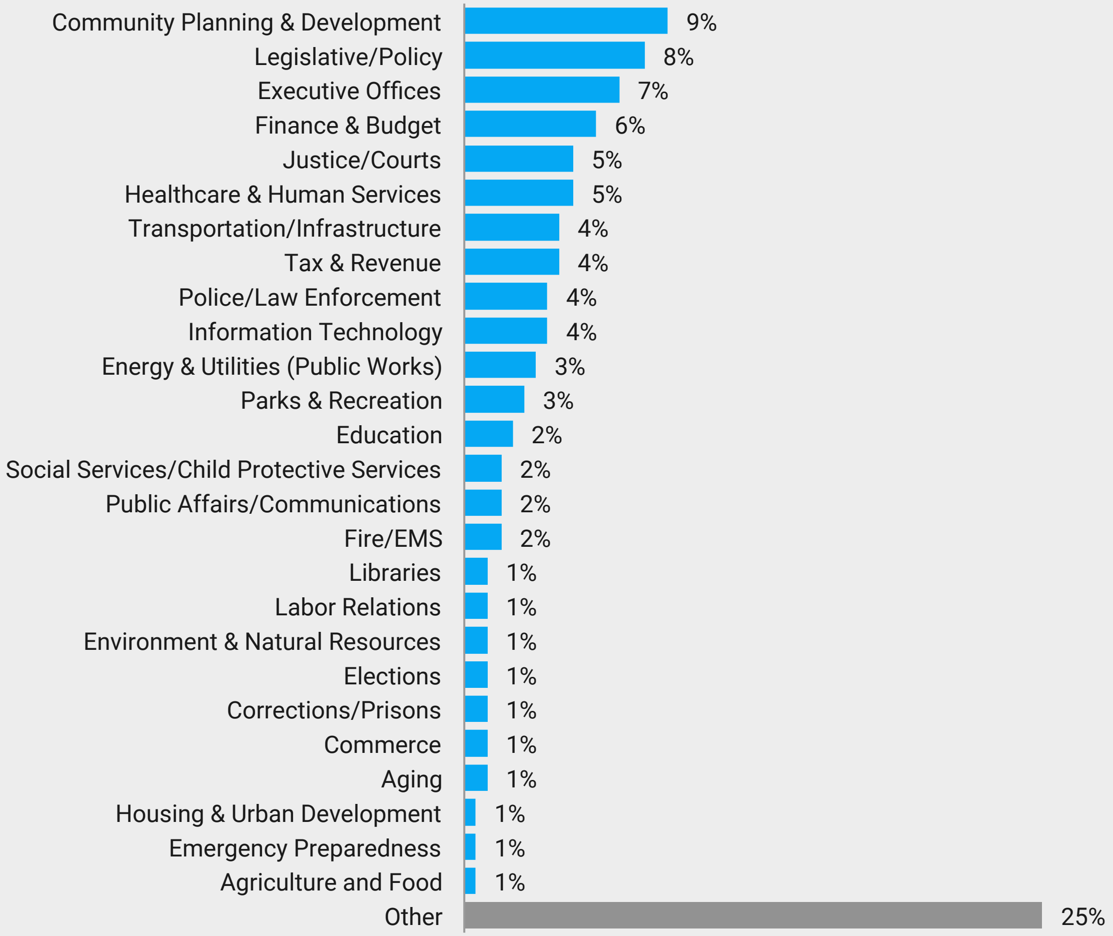
Percentage of respondents, n=309
Note: Percentages may not add up to 100% due to rounding

Respondents were asked to choose which single response best describes their employment situation. Employment situation types are listed in order of frequency.

Respondents were asked which of the following choices best describes their level of involvement with IT in their organization. "Other" includes responses such as information technology professor, property assessor, town administrator, deputy city manager over IT, and business continuity.

Respondents represent a wide range of mission areas / Respondent Profile

Mission area



Percentage of respondents, n=193
Note: Percentages may not add up to 100% due to rounding

Respondents were asked to choose which single response best describes their primary mission area.

About

Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of *Government Executive*'s 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at www.govexec.com/insights

Report Author: Daniel Thomas

Contact

Will Colston
Manager, Operations
Government Executive Media Group
Tel: 202.266.7423
Email: wcolston@govexec.com

govexec.com/insights
@GovExecInsights

One Identity

One Identity eliminates the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our Identity and Access Management (IAM) solutions enhance your organization’s agility while addressing your IAM challenges in on-premises, cloud and hybrid environments.

Learn more about our identity governance, access management, and privileged management solutions at https://oneidentity/solutions/identity-and-access-management/