Government
Business
Council

Identity Management: The Next Generation of Security

A Candid Survey of State & Local Leaders

Underwritten by

Symantec.

August 2017

Table of Contents

Overview

Purpose

State-of-the-art technologies are paving the way toward better, more efficient government — but with transformation comes a host of increasingly sophisticated cyber threats. In an effort to ensure both progress and security, state and local governments are turning their attention toward identity management: ensuring that critical organization data can only be accessed by the right people, at the right time, and for the right reasons. To learn more about ongoing efforts, Government Business Council and Symantec launched an in-depth research study in June 2017.

Methodology

Government Business Council and Symantec released a survey on June 8 2017 to a random sample of state and local government employees. 305 respondents representing all levels of state and local government — including municipal, county, township, and special district governments — completed the survey.

> “One of the most fundamental issues everyone has to grapple with is identity-proofing — your business process for proving that you’re you or I’m me.

Steve Nichols, Georgia Chief Technology Officer

NASCIO Panel, April 2017

Executive Summary

State and local employees are confident in their organization's data security

A majority of respondents express confidence in their organization's identity management processes. Accordingly, over 70% of respondents agree or strongly agree that their organization is capable of ensuring appropriate access to critical data, while nearly 60% believe that their organization provides citizens with full, secure access to online services.

Organizations still have room for improvement when it comes to identity management

In spite of confidence from employees, it appears that gaps still remain in organization identity management processes. Nearly a quarter of respondents say that their organization does not plan to leverage big data/analytics in the foreseeable future to combat fraud, waste, and abuse; in addition, just 22% feel that implementing a cohesive platform for managing citizen identities is a high or critical priority in their organization.

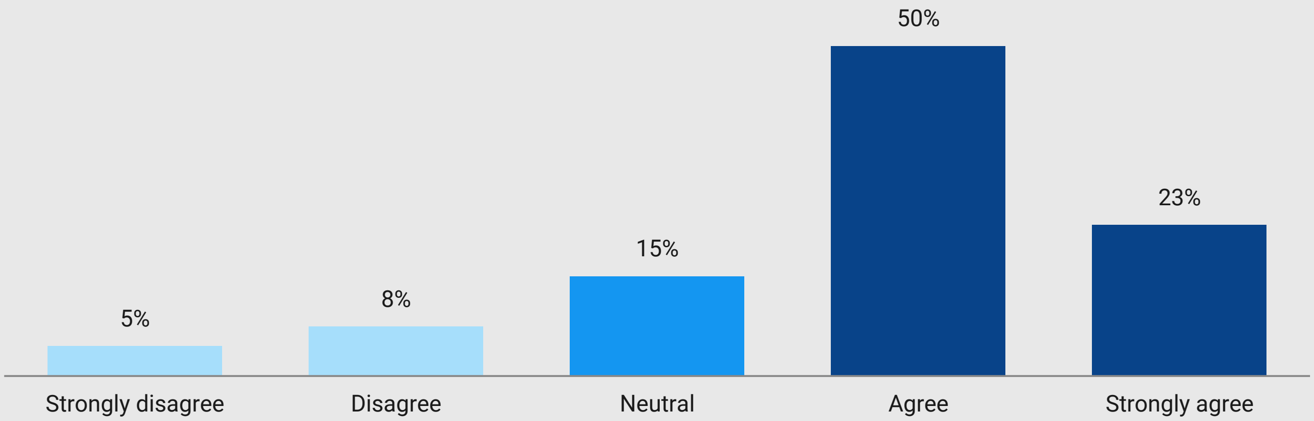
Respondents are largely optimistic when it comes to the prospect of a comprehensive identity management platform

State and local employees feel that implementation of an organization identity management platform could yield a host of benefits — particularly improved customer service and security/privacy. Despite various bureaucratic and structural barriers, respondents are also largely confident that such a platform could be created: over half believe that a cohesive identity management platform could feasibly be achieved within the next ten years.

Research Findings

A majority feel that their organization is capable of ensuring appropriate data access

To what extent do you agree or disagree with the following statement: "My organization is capable of ensuring appropriate user access to critical data."



Percentage of respondents, n=292
Note: Percentages may not add up to 100% due to rounding

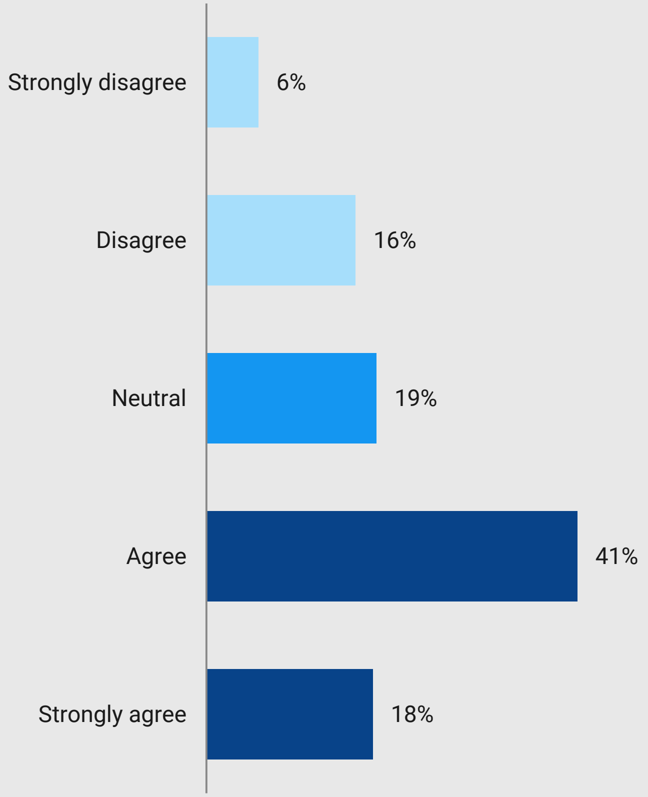
73% of state and local employees agree or strongly agree with the statement "My organization is capable of ensuring appropriate user access to critical data," 13% disagree or strongly disagree, and 15% are neutral.

Over 70%

of respondents feel confident in their organization's ability to secure data against inappropriate access.

Governments still have room for improvement when it comes to citizen access to online services

Please indicate the extent to which you agree or disagree with the following statement: "My organization provides citizens with full, secure access to all online services."



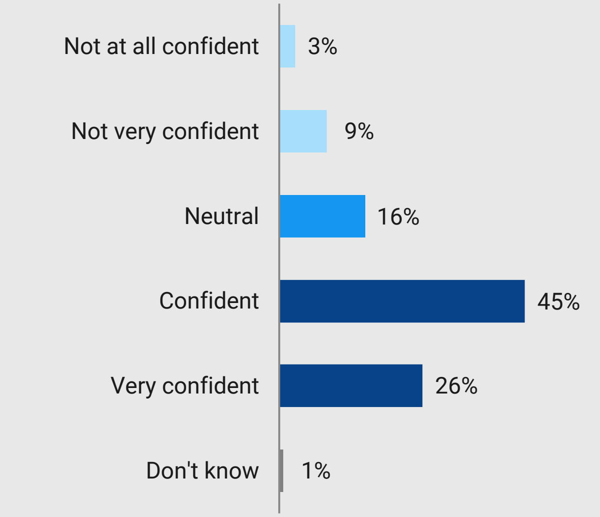
Percentage of respondents, n=262
Note: Percentages may not add up to 100% due to rounding

Nearly 60%
are confident in their organization's ability to provide citizens with online services.

However, nearly a quarter of respondents (22%) disagree or strongly disagree that their organization is able to ensure full, secure access to all online services.

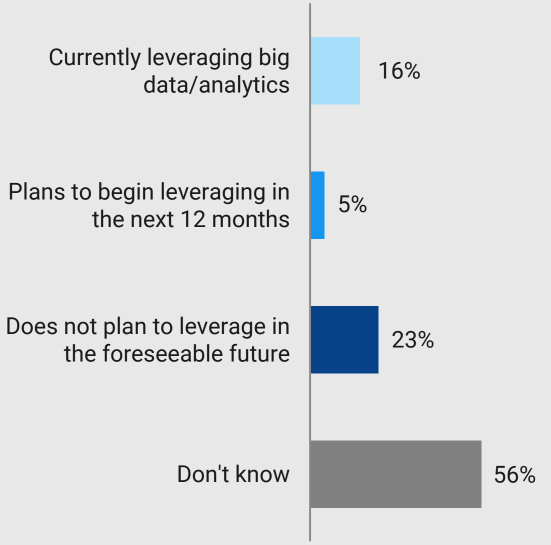
Many organizations have yet to explore new methods of combatting fraud, waste, and abuse

How confident are you in your organization's ability to manage internal fraud, waste, and abuse?



Percentage of respondents, n=276
Note: Percentages may not add up to 100% due to rounding

Is your organization leveraging big data/analytics to combat fraud, waste, and abuse (FWA)?



Percentage of respondents, n=275
Respondents were asked to select all that apply

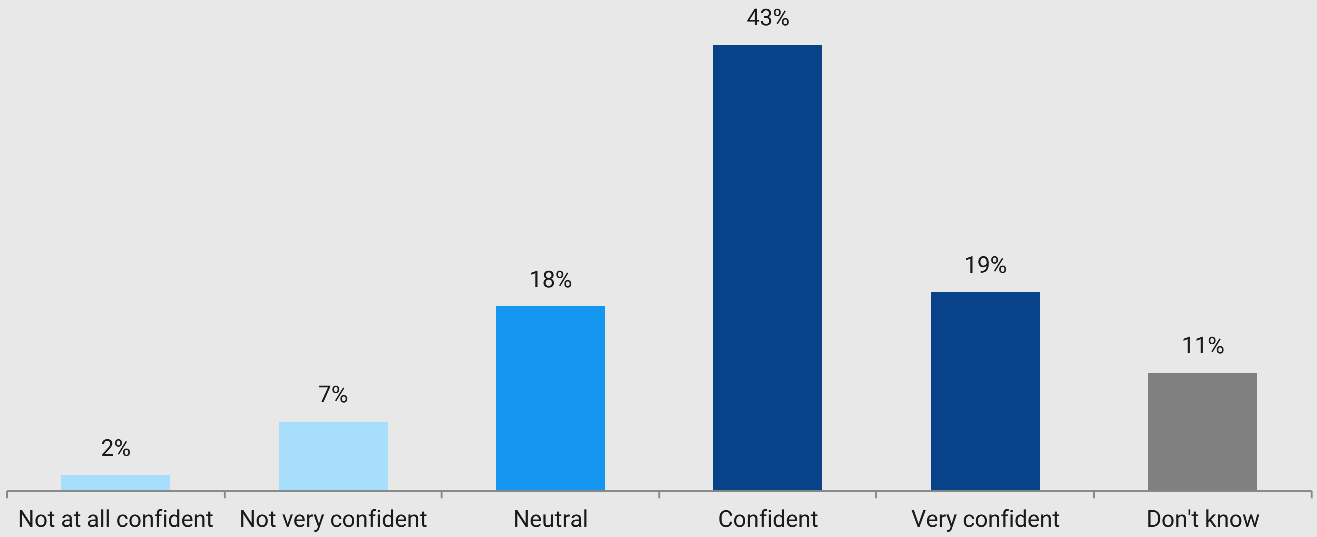
Over 70% of respondents report being confident or very confident in their organization's ability to manage internal fraud, waste, and abuse (FWA). However, this doesn't mean that organizations don't have room to grow: nearly a quarter say that their organization doesn't plan to leverage big data/analytics to combat FWA in the foreseeable future, indicating that many organizations have yet to fully consider exploring new, state-of-the-art security capabilities.

Nearly 25%

of respondents say that their organization doesn't plan on leveraging analytics to combat fraud, waste, and abuse

Most respondents are confident in their organization’s identity management processes

How confident are you in your organization’s identity management processes (e.g., security practices that ensure access by the right people, at the right time, and for the right reasons)?



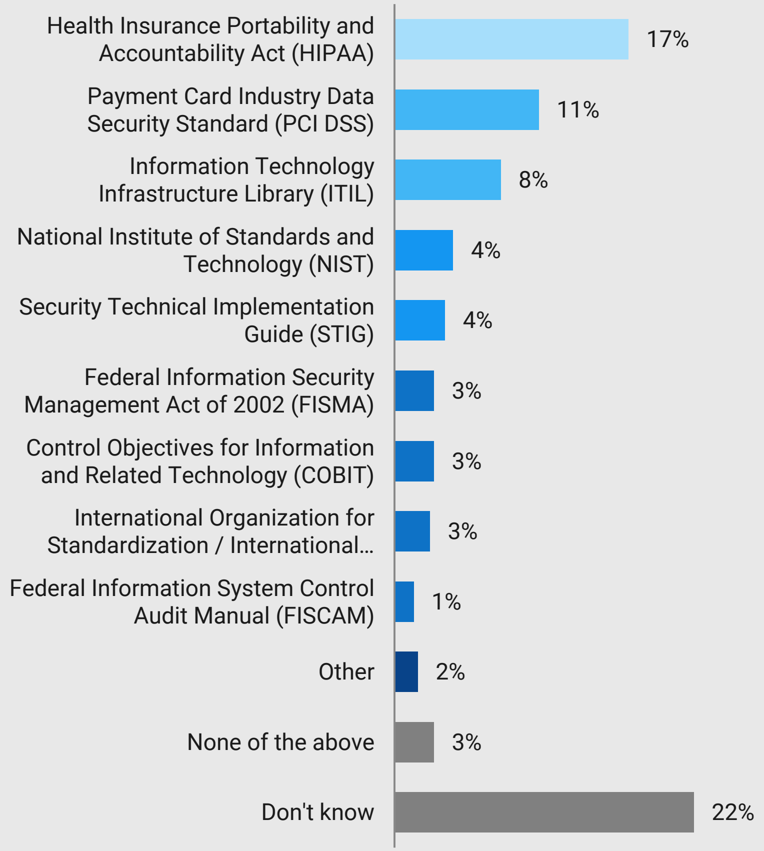
Percentage of respondents, n=271
Note: Percentages may not add up to 100% due to rounding

62% of respondents say that they are confident or very confident in their organization’s identity management processes, 9% are not very or not at all confident, and 18% are neutral.

Over 60%
express confidence in their organization’s identity management processes

Respondents most commonly identify HIPAA as providing their organization with security guidance

To the best of your knowledge, which of the following does your organization leverage as guidance for security protocols?



Percentage of respondents, n=348
Respondents were asked to select all that apply

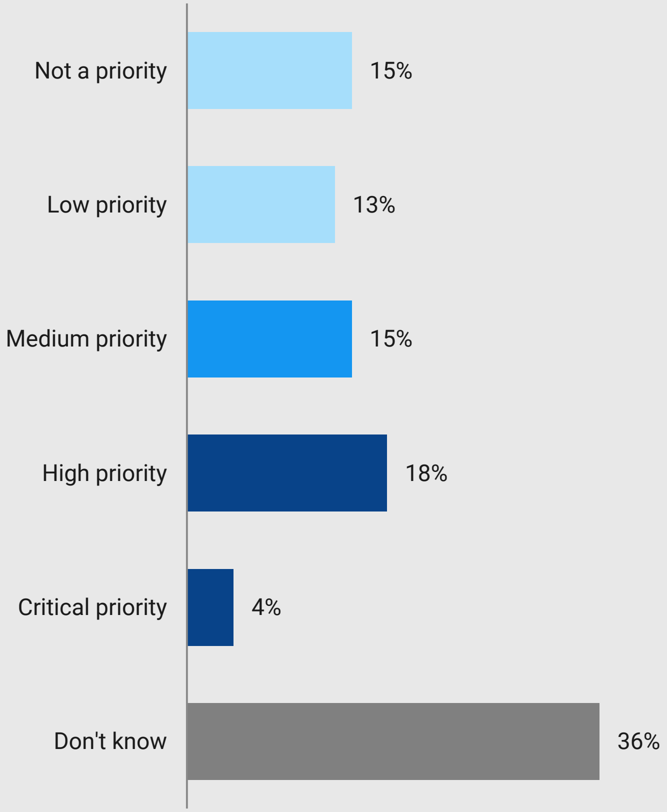
17%

of respondents identify HIPAA as one of the pieces of legislation their organization uses as guidance for implementing security protocols.

However, a plurality (22%) aren't sure what rules/standards their organization leverages.

Many organizations have yet to make identity management a priority

How does implementing a cohesive platform for managing citizen identities (e.g., single sign-on, uniform citizen profile across departments, etc.) rank among your organization's IT priorities?



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

Just 22%

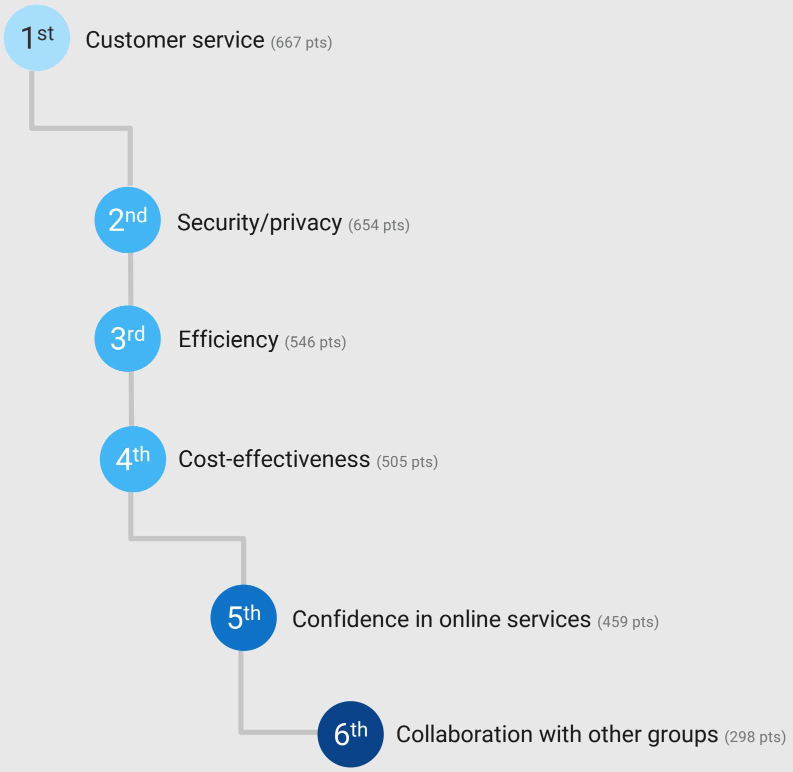
Say that implementing a cohesive citizen identity management platform is a high or critical priority in their organization.

28% say that it is not a priority or a low priority, while 15% classify it as a medium priority. A plurality of respondents (36%) don't know how it ranks among their organization's IT priorities.

Streamlining identity management processes can yield a range of benefits

Identity Management: Benefits

Ranked by respondents according to potential impact in improving organization effectiveness



1st Customer service (667 pts)

2nd Security/privacy (654 pts)

3rd Efficiency (546 pts)

4th Cost-effectiveness (505 pts)

5th Confidence in online services (459 pts)

6th Collaboration with other groups (298 pts)

Ranked by Borda count, n=149

Organizations can expect a variety of benefits from the creation of an enterprise-wide identity management platform.

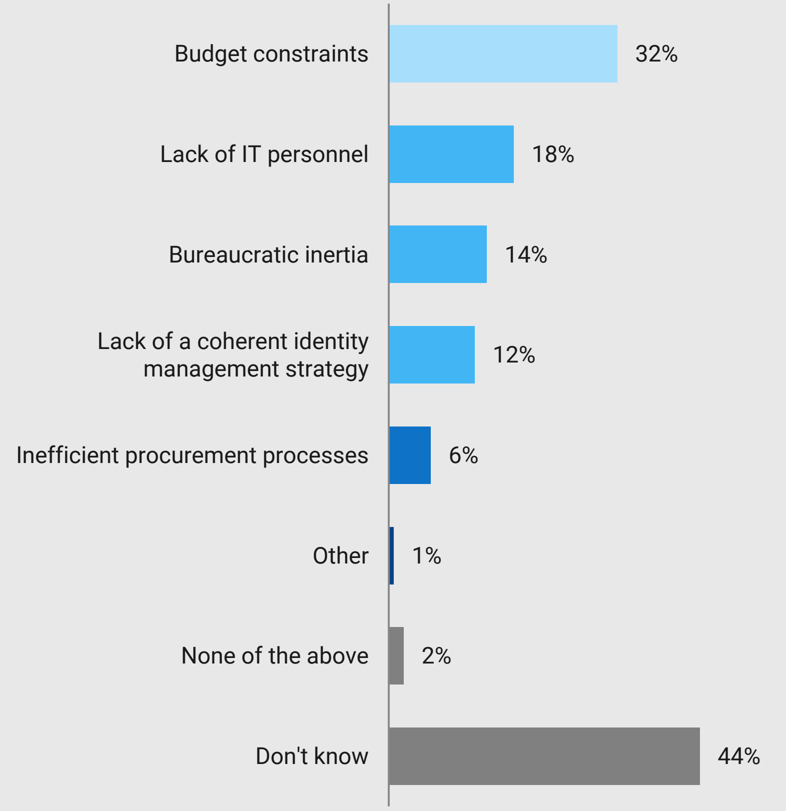
When asked to rank benefits according to the impact they would have on organization effectiveness, most respondents select customer service as holding the most potential weight, followed by security/privacy, efficiency, cost-effectiveness, confidence in online services, and collaboration with other groups.

Respondents were asked: “Please rank the following according to their potential impact in improving your organization’s effectiveness.”

Rankings and total scores are displayed here using the Borda count method, where each answer choice earns points based on the order in which respondents placed them. Each respondent’s top answer choice receives the maximum score of n points for that respondent, where n is equal to the total number of options. Each subsequent choice receives 1 less point than the one ranked ahead of it. Unranked answer choices receive zero points. Please see Appendix for further detail.

Identity management progress is hindered by various barriers

Which of the following represent the greatest barriers to the creation of a common identity management platform within your organization?



Percentage of respondents, n=289
Respondents were asked to select all that apply

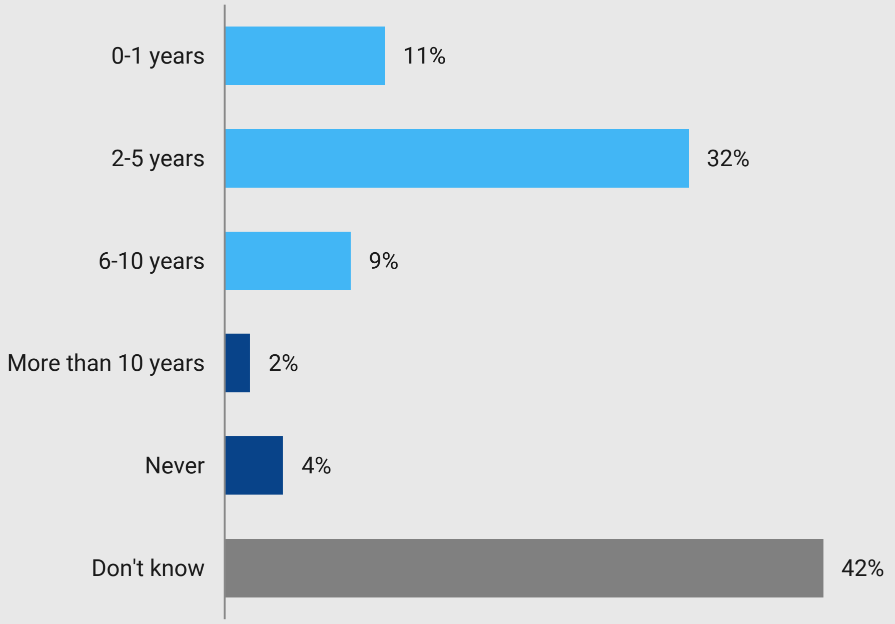
Nearly 1 in 3

respondents select budget constraints as one of the greatest barriers to the creation of a common identity management platform in their organization.

Other identified hurdles include lack of IT personnel (18%) and bureaucratic inertia (14%).

Most respondents believe a common identity management platform can be achieved in the near future

How soon do you think your organization could achieve a common identity management platform?



Percentage of respondents, n=271
Note: Percentages may not add up to 100% due to rounding

In spite of barriers, a majority of state and local employees believe that their organization could achieve an a common identity management platform within the next 10 years. 6% believe that the undertaking won't be realized or will take more than 10 years, while 42% don't know.

52%

of respondents believe that a common identity management platform can be achieved in the next 10 years.

Final Considerations

Looking ahead, state and local organizations should…

Explore new ways to strengthen existing security processes

Survey-takers express confidence in their organization's data security processes; however, the findings indicate that these processes could continue to evolve. It is essential that organizations explore how transformational technologies — such as big data/analytics — can help propel fraud detection, threat mitigation, and more. However, organizations need to first overcome structural and bureaucratic hurdles (i.e., budget constraints, lack of IT personnel, and bureaucratic inertia) before they can fully implement and harness state-of-the-art tools and systems.

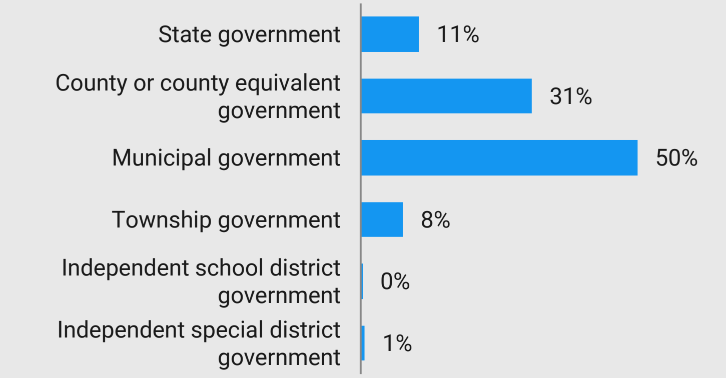
Consider adopting a single, secure identity management platform

In spite of existing barriers, most respondents are supportive of the prospect of a uniform, organization-wide identity management environment. Possible benefits of such a platform — including improved customer service, security/privacy, efficiency, cost-effectiveness, confidence in online services, and collaboration with other groups — could profoundly bolster organization effectiveness. By exploring the implementation of a secure, single sign-on environment, state and local organizations could manage to achieve an essential balance between security and enhanced data access.

Respondent Profile

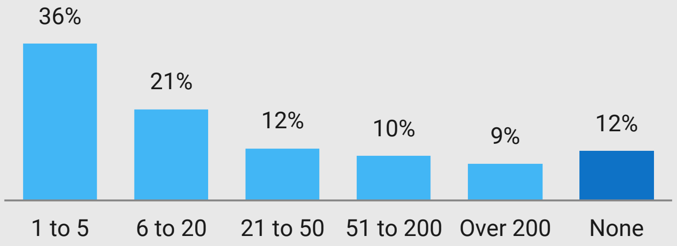
Most respondents are supervisors within their organization

Employment situation



Percentage of respondents, n=304
Note: Percentages may not add up to 100% due to rounding

Reports/oversees



Percentage of respondents, n=165
Note: Percentages may not add up to 100% due to rounding

90%

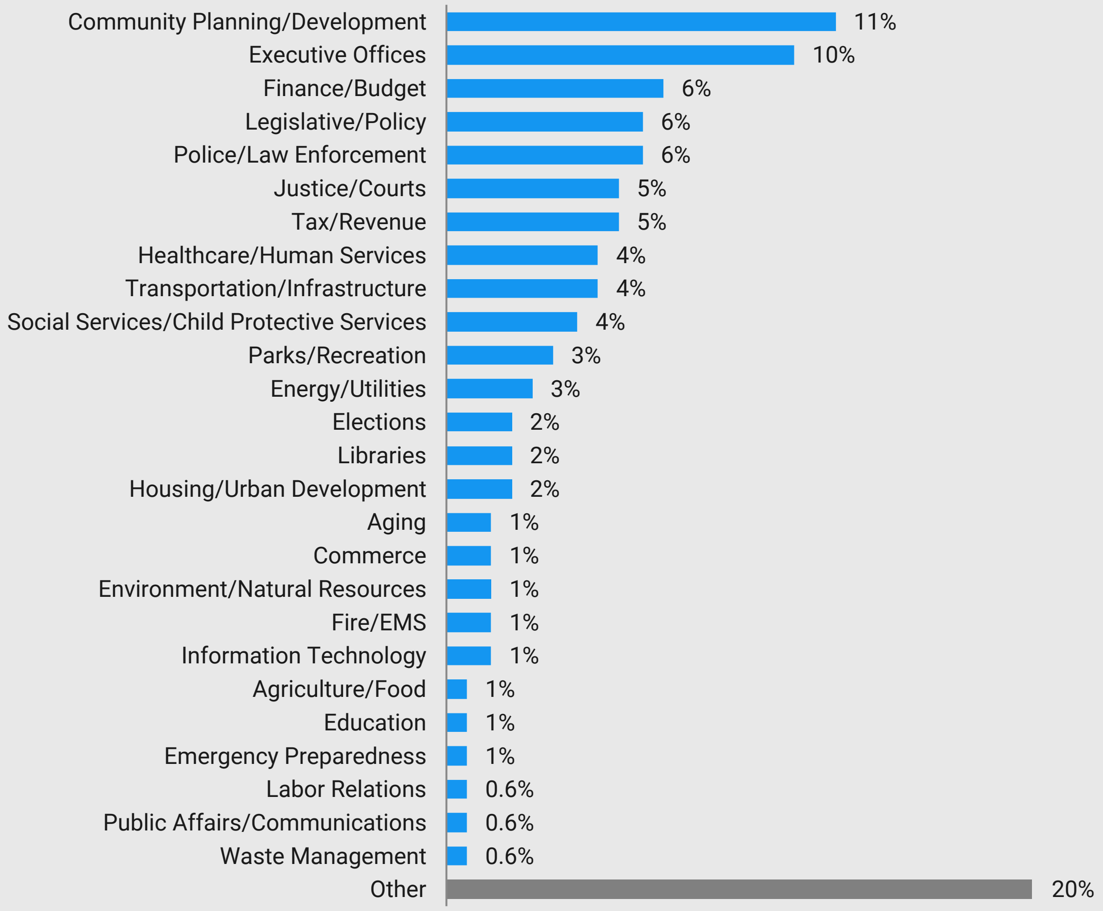
of respondents hold positions in local government positions, whether at the county, municipal, township, or independent district levels.

88%

of respondents are supervisors who oversee at least one employee, either directly or through direct reports.

Respondents represent a wide range of job functions and geographical regions

Job function



Percentage of respondents, n=159
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.

Appendix

The creation of an enterprise-wide identity management platform may yield a variety of benefits. Please rank the following according to their potential impact in improving your organization's effectiveness.

	Count per rank						Total	Borda count
	1	**2**	**3**	**4**	**5**	**6**		
Customer service	49	27	36	26	5	6	149	667
Security/privacy	50	35	20	18	19	7	149	654
Efficiency	14	33	36	33	21	12	149	546
Cost-effectiveness	16	27	26	27	36	17	149	505
Confidence in online services	16	17	19	30	45	22	149	459
Collaboration with other groups	4	10	12	15	23	85	149	298
Number of respondents	149	149	149	149	149	149	-	-

Ranked by Borda count, n=149

Rankings and total scores are displayed here using the Borda count method, where each answer choice earns points based on the order in which respondents placed them. Each respondent's top answer choice receives the maximum score of n points for that respondent, where n is equal to the total number of options. Each subsequent choice receives 1 less point than the one ranked ahead of it. Unranked answer choices receive zero points.

For instance, if a respondent's ranked choices were 1) Confidence in online services, 2) collaboration with other groups, and 3) efficiency, those responses would receive 6, 5, and 4 points respectively. These points would be added to Borda count of each answer choice.

With 307 respondents and 7 choices, the maximum score possible for any single answer choice (i.e., if every respondent ranked it as their top outcome) is equal to 2,149 points (307 x 7).

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.

Report Author: Rina Li

Contact

Nicholas McClusky
Director, Research & Strategic Insights
Government Executive Media Group
Tel: 202.266.7841
Email: nmcclusky@govexec.com

govexec.com/insights
@GovExecInsights

Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.