Keys to the Kingdom:

Managing Privileged Users and Accounts in State & Local Government

Privileged users and accounts have access to a government agency's most sensitive digital infrastructures. Because of this, they represent high-value targets to enemies seeking to exploit, manipulate, and steal sensitive data.

While the federal government has issued guidelines on how to manage privileged users and accounts, the situation at the state and local level is less certain.

The Privileged User

The Facts

Agency employees with higher level access to systems, networks, admin rights

They hold the "keys to the kingdom"

They can be both an organization's greatest asset and greatest liability

In The News

2014: Hackers take control of an OPM contractor's privileged account and steal personal data from over 21.5 million feds.

2015: Cited as a "clerical error," Georgia's Sec. of State leaks personal data of over 6 million voters to 12 state organizations

Managing privileged users and accounts in state and local government effectively requires leveraging a variety of techniques. **This can include...**

Delegation

Admins are only given sufficient rights to do their job

Session Audit

Monitoring activity performed with admin credentials

Password Vaulting

Automated storage, issuance, and changing of admin credentials

However, challenges remain.

According to a recent GBC survey of state and local leaders...

Only 11% of respondents say their organization uses all three of these practices

25% say their organization "never" changes its administrator passwords

To learn how state and local governments are managing privileged user access, read the full report.

Government Business Council

ONE IDENTITY

About GBC

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

About 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 www.oneidentity.com

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.

Click here for the full results.

Sources

1. "Managing Privileged Access Is Crucial to Preventing Data Breaches." Security Magazine, June 2016
2. "Best Practices for Privileged User PIV Authentication." NIST, April 2016
3. "OPM Hack May Finally End Overuse of Privileged User Access." CSMonitor, June 2015.
4. "Data Breach in Georgia Could Affect 6 Million Voters" myAJC, Nov. 2015.