December 2017

State and Local Government Cybersecurity and Compliance:

The Importance of a Complete Identity and Access Management Strategy

CONTENTS:

INTRODUCTION

State and local public-sector organizations contend with a daily onslaught of increasingly frequent, evolving and sophisticated cyberattacks. The sensitive citizen data managed at the state level — ranging from Social Security numbers and driver's license records, to health and tax information — demand strong investment in digital transformation to deliver security-oriented IT environments. Such transformation would minimize data exposure risks while preserving end-user functionality. In selecting tools and technologies to advance this type of digital transformation, state and local government IT officials place a premium on security, scalability, cost efficiency and compliance with complex regulatory requirements.

Strings of cyberattacks targeting state and local government agencies, which act as stewards of citizens' personally identifiable information (PII), are commanding increased executive-level attention and fostering an environment favorable to cybersecurity progress[1].

PII EXPOSURE

Attackers hacked a state-level Department of Revenue, exposing roughly 3.6 million Social Security numbers, along with 387,000 credit and debit card numbers belonging to state taxpayers. In an interview with PC World, security evangelist Stephen Cobb labeled the breach "exceptional," both in terms of records compromised and potential for damage to confidence in state government[2]. The resulting lawsuits and demand for state-sponsored identity protection services cost upwards of $25 million.

HACKTIVISM

Hacktivists operating under the Anonymous banner targeted a city police department following the death of Freddie Gray, expressing their support for those protesting the police by disclosing the names, email addresses, and IP addresses of local officers.

POLITICAL INTERFERENCE

In the 2016 U.S. presidential election, Russian operatives allegedly took advantage of online vulnerabilities in America's state election databases to gain access to voter data. Though no evidence of vote alteration was found, a part-time contractor for the Illinois state board of elections noticed unauthorized data leaving the network. The contractor told *Bloomberg* the data contained personal information — including names, birthdays, genders and partial Social Security numbers — of around 15 million people[3]. Despite Obama Administration assurances that the attempted interference was not sufficient to compromise the election's integrity, the alleged Russian campaign successfully targeted 39 states.

These breaches shared one crucial commonality: identity as a threat vector. Launched by a diverse set of attackers with motivations spanning financial gain, activism, terrorism, thrill factor and political influence, each attack relied on weak identity and access management controls for success.

[1] In July 2017, 38 U.S. governors signed on to a "Compact to Improve State Cybersecurity." https://nordicinnovationlabs.com/2017/07/18/38-governors-sign-compact-improve-state-cybersecurity/

[2] http://www.pcworld.com/article/2013186/south-carolina-reveals-massive-data-breach.html

[3] "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg, June 2017

To take advantage of heightened senior administrator level awareness of cybersecurity challenges and vulnerabilities, state and local government risk management personnel must bolster their identity governance capabilities. Identity governance serves as the foundation of any credible effort to effectively manage cybersecurity risks. It addresses numerous pain points experienced at the state and local levels — including tight fiscal and budgetary environments, conflicting IT priorities and burdensome regulatory landscapes. Identity governance solutions unify discreet identity management technology by centralizing identity data and providing a single place to model roles, policies and risk, thereby supporting compliance and provisioning processes across an organization. By defining appropriate access levels for regular and privileged users, and automating provisioning and de-provisioning for those accounts, identity governance solutions deliver immediate security, privacy, compliance and efficiency benefits to agencies responsible for safeguarding sensitive citizen data.

Beyond identifying the unique cybersecurity impediments to state- and local-level cyber maturity, this whitepaper will evaluate the role of identity governance solutions in strengthening cybersecurity risk management — which state CIOs identified as their single top priority for 2017[4]. More specifically, this paper will speak to the value of identity governance platforms in ensuring secure employee access to state and local government networks, driving cost and business process efficiencies, and facilitating compliance with regulations, including HIPAA, IRS 1075 and PCI.

CHALLENGES AND THREATS FACING STATE AND LOCAL GOVERNMENTS

Security Scorecard's 2016 Cybersecurity Report noted that, "compared to the cybersecurity performance of 17 other major industries, government organizations ranked at the bottom of all major performers, coming in below information services, financial services, transportation and healthcare[5]." State and local governments contend with significant budgetary restrictions, talent shortages, aging and outdated IT infrastructure, and compliance obligations that compound cybersecurity risks to their IT systems and often force state officials into point-solution implementations designed to put out near-term fires, rather than comprehensively addressing a broader set of cybersecurity priorities.

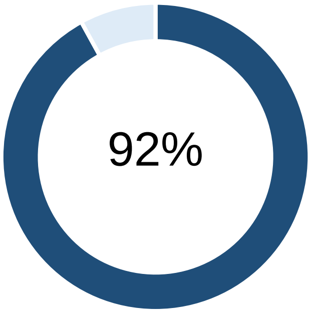
According to *Government Technology*, the average state or local government agency spends less than five percent of its IT budget on cybersecurity, relative to the typical 10 percent among commercial enterprises. State CISOs struggle to allocate these already-limited funds across the increasingly saturated cybersecurity technology landscape, wherein multiple products from multiple vendors require complex integrations, prohibitively expensive implementations and ongoing management.

[4] https://www.nascio.org/Publications/ArtMID/485/userid/5071/ArticleID/441/State-CIO-Top-Ten-Policy-and-Technology-Priorities-for-2017

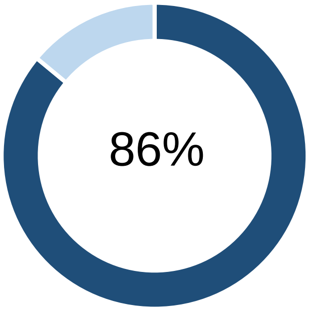
[5] http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html

On top of budgetary concerns, state and local government agencies face entrenched security staffing and know-how challenges across their workforce. Agencies struggle to match compensation and benefits offered to cybersecurity employees working in both private and federal public sectors. Noting that cybersecurity salaries in his state run 20 percent below market rate, Michigan Chief Technology Officer Rod Davenport told *Government Technology* that attracting cyber talent requires appealing "to folks' sense of the nobility of public service[6]."

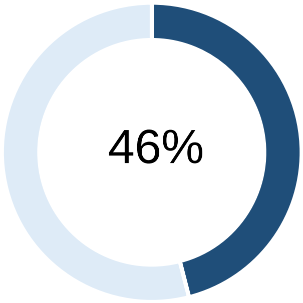
A survey conducted by the National Association of State CIOs (NASCIO) suggests that these challenges will only get tougher[7]. In 2015, 92 percent of states identified salary as an obstacle to attracting and retaining qualified employees. Furthermore, 86 percent of states spoke of difficulty recruiting qualified candidates to fill vacant slots, up from 55 percent in 2011. Finally, 46 percent of states reported an average timeframe of three to five months to fill senior-level positions.



States that identify salary as an impediment to employing and retaining cyber talent



States that struggle to recruit qualified cyber personnel



States that require three to five months to fill senior-level positions

State and local governments are responsible for protecting critical infrastructure and computer systems from intrusion, as well as providing critical citizen-facing IT services. However, budgetary and staffing challenges often force them to provide these services while simultaneously struggling to maintain and secure technology that is no longer supported by vendors with updates and patches. Furthermore, these systems and applications are poorly tracked and documented by the agencies, and hidden from view by end users.

Despite these challenges, state and local IT and security administrators hesitate to overhaul systems that perform their required functions. While private-sector IT refresh cycles typically fall within the three-to-five-year range, most state systems' cycles are measured in decades. A 2012 survey by the National Association of State Workforce Agencies found that most IT systems supporting unemployment insurance programs are based on outmoded programming languages — on average, 22 years old[8].

[6] http://www.govtech.com/security/Cybersecurity-Workforce-Gap.html

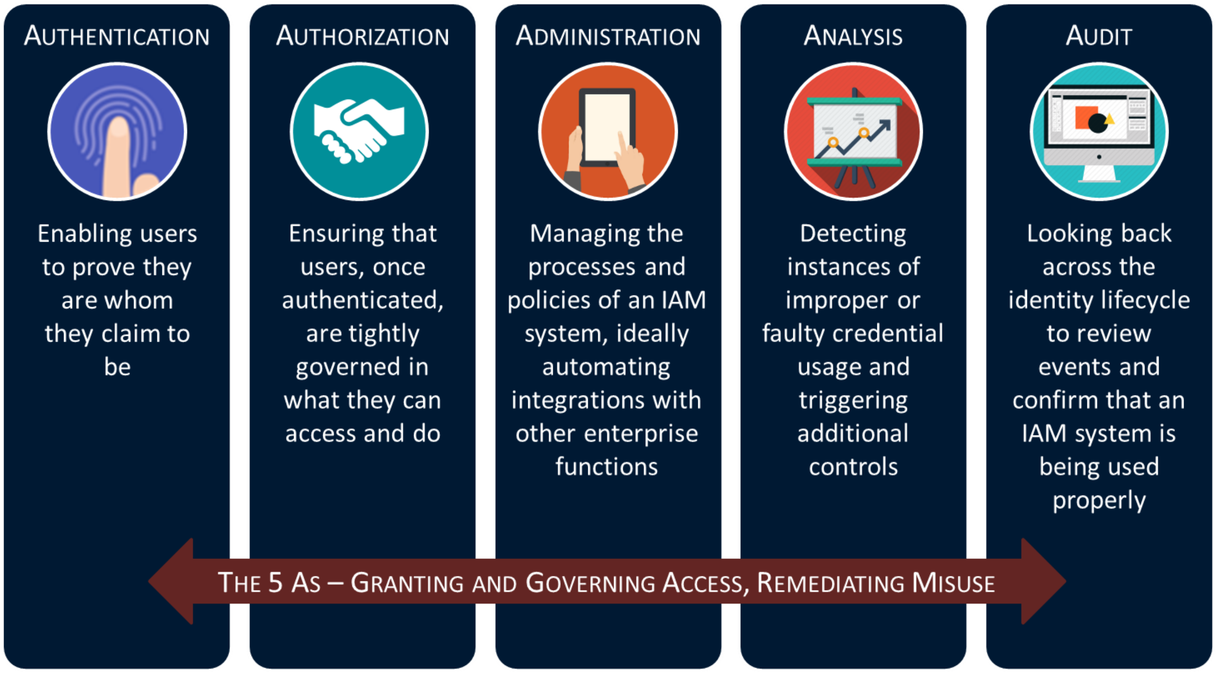
[7] https://www.nascio.org/Publications/ArtMID/485/ArticleID/79/State-IT-Workforce-Facing-Reality-with-Innovation

[8] http://www.uwcstrategy.org/wp-content/uploads/2014/06/Presentation-for-UWC-Conference-Savannah-Final-1-Joe-Vitale.pdf

In a pitch for a $54,000 investment from his county legislature to install a more secure and reliable IT system, Bedford County (Virginia) IT Director Robert Floyd spoke of “inefficiencies” and “outages that span over several days” that result from dependence on legacy systems[9]. “The core infrastructure is very important and it must operate, and when it doesn’t, people can’t work,” Floyd told *StateTech* in March 2017[10]. Legacy IT systems not only lack the improved speed, security and functionality of modern systems, but are also expensive to maintain and difficult to secure.

THE FIVE As OF IDENTITY MANAGEMENT

A holistic approach to securely managing access to sensitive information — one rooted in governance — not only offers state and local governments an opportunity to reduce the extent to which identity offers an entrée into their systems, but also provides an integrated solution to several of the challenges that have historically stunted state and local cybersecurity maturity. To truly address the full range of acces risks to state and local government systems, agencies must prioritize solutions that address each of “The Five As” of identity security.



Authentication

Enabling users to prove they are whom they claim to be

Authorization

Ensuring that users, once authenticated, are tightly governed in what they can access and do

Administration

Managing the processes and policies of an IAM system, ideally automating integrations with other enterprise functions

Analysis

Detecting instances of improper or faulty credential usage and triggering additional controls

Audit

Looking back across the identity lifecycle to review events and confirm that an IAM system is being used properly

The 5 As – Granting and Governing Access, Remediating Misuse

To account for specific budgetary, talent and infrastructure challenges associated with state-level cybersecurity maturity, state and local IT security chiefs must prioritize multi-purpose cybersecurity solutions. Strong identity and access management offers one such solution. By taking a holistic governance-based approach to identity — looking at authentication, authorization, administration,

[9] https://statetechmagazine.com/article/2017/03/what-it-means-deal-outdated-it-infrastructure

[10] Ibid

analysis and audit — agencies can close many of their most easily exploited holes while keeping costs low, reducing burden on shrinking IT security staffs, and extending the lifecycle of legacy IT infrastructure.

Properly implemented, a governance-based approach enables state IT officials to answer many critical questions around effectively managing access to sensitive content, including:

- How are state employees' credentials provisioned?
- How are state employees authorized to access data and resources?
- How are access request approvals themselves audited?
- What is your approach to access certification and attestation?
- How are those authorizations managed and updated within state and local government agencies as employees' roles or attributes change?
- How is access to privileged systems provisioned and managed?
- Are Privileged Account Management (PAM) solutions tightly integrated with the rest of the identity management stack?
- Are firm controls in place to prevent the creation of new "phantom" accounts?
- How is access revoked when someone leaves a state or local government agency, ensuring that "orphan" accounts do not persist?
- With a blended workforce of employees and contractors, how are access and privilege consistently managed through a unified approach?

Identity governance solutions can assign employee risk profiles and automatically flag privilege escalation requests to deter improper access to networks. Identity governance limits the extent to which identity offers a vector of attack within a network by controlling user access privileges across multiple systems and ensuring that negligent and disgruntled insiders are unable to access — and therefore leak or compromise — information outside their purview. A strong identity governance solution will also generate risk scores for all users based on their combined entitlements and historical performance. Furthermore, identity governance can and should extend beyond systems and applications. A robust identity governance solution applies the same capabilities to data files wherever the content resides, whether on premises or in the cloud.

BENEFITS OF IDENTITY GOVERNANCE TO STATE AND LOCAL GOVERNMENT

Identity governance solutions gather technical identity data scattered across multiple enterprise systems and consolidate the information into a centralized business information repository, which can be aggregated and scaled at no additional cost. This capability enables infrastructure managers to extend the lives of legacy IT systems and connect them with modern systems deployed in this new era of digital transformation. The consolidation of identity data across legacy and modern IT infrastructure is a key benefit for state and local government CIOs and CISOs who've inherited decades old systems in the face of cloud and software-defined perimeter modernization trends.

Identity governance solutions also accommodate the low cybersecurity talent pool by catering to a less technical user population. Beyond automating the once-manual provisioning process, governance platforms increasingly offer user interfaces designed specifically for business users to request and manage user lifecycle events. Whereas legacy provisioning tools were designed for use by IT administrators, identity governance solutions offer a business-friendly user interface that reduces burden on IT staffs by involving a broader set of business users in identity management processes such as access requests, privilege escalation approvals and access certifications.

As a software solution, governance platforms also comply with the recent trend toward state-level operational expenditures over capital expenditures. State-level organizations have become increasingly allergic to spending millions of dollars on single projects requiring multi-year implementation lifecycles[11]. Because governments designate operational expenditure dollars annually, software solutions have become a more prudent investment.

A properly-configured governance platform can not only ameliorate the core cost, labor and infrastructure challenges associated with implementing cybersecurity solutions at the state and local levels, but can also reduce cybersecurity exposure and drive various operational, compliance and risk management benefits. As a scalable and easily-updatable software solution capable of ingesting the various data sets managed at the state and local levels, identity governance platforms offer promising cybersecurity solutions for state and local government agencies.

STATE AND LOCAL COMPLIANCE OBLIGATIONS

Responsive to both the critical citizen-facing responsibilities of state and local government agencies and the challenges they face in executing on those responsibilities, government authorities impose a diverse set of compliance requirements to ensure the privacy and security of this information, including IRS Publication 1075; the Health Insurance Portability and Accountability Act (HIPAA); the Health Information Technology for Economic and Clinical Health Act (HITECH); and the Payment Card Industry Data Security Standard (PCI DSS).

IRS Publication 1075

The IRS Office of Safeguards manages IRS Publication 1075—Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns, which mandates government adherence to certain cybersecurity and physical security controls for the protection of federal tax information (FTI). IRS 1075 compliance requirements intend to maintain the integrity of the tax system, protect the privacy of citizens' personal identifiable information, enhance security and streamline the coordination of all levels of government in the tax revenue process. One major aspect of IRS Publication 1075 is the appropriate management of access control to information systems containing FTI.

Similar to many government compliance guidelines, IRS 1075's security controls are based on the NIST Special Publication (SP) 800-53 for government information systems.

[11] The Chertoff Group regularly conducts interviews with senior state and Federal-level cybersecurity leaders. Some information shared in this paper reflects insights gathered from this network of experts.

Adherence to NIST 800-53 makes up an essential part of full IRS 1075 compliance. Of the main Security Control Families contained within NIST SP 800-53 (captured in the below table), a proper identity governance platform will address those highlighted:

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

These requirements assume a level of understanding among state and local officials of the risks surrounding their organization(s) and the security controls in place to protect their information systems. Identity solutions rooted in governance deliver this needed transparency. Given that most of business risk related to user access can be tied to a very small percentage of the user population, compliance with NIST SP 800-53, and by extension, IRS Publication 1075, requires identifying that small percentage and focusing on it. Unlike provisioning solutions, which view identity at the account level, governance solutions look at entitlements, giving organizations the ability to quantitatively assess which users and applications represent the greatest threat for noncompliance in a particular organization. This type of risk-based approach also gives organizations the ability to measure their risk over time and demonstrate that controls are working and reducing compliance exposure.

Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)

Like other government and healthcare entities, state and local governments are required to adhere to regulatory guidelines set forth by HIPAA and HITECH if they handle patients' protected health information (PHI). State- and local-level HIPAA compliance and citizen privacy protection has become even more important with the expansion of Medicare and Medicaid because of the Affordable Care Act. State healthcare agencies have faced increased scrutiny, particularly due to the value of citizen PII contained in their records.

Public healthcare agencies face significant challenges in achieving two core HIPAA compliance requirements:

- Implement technical security measures to guard against unauthorized access to PHI that is being transmitted over an electronic communications network; and
- Implement policies and procedures for authorizing access to PHI that are consistence with the Privacy Rule.

These challenges include disparate repositories of identity information, documenting access policies, demonstrating Meaningful Use for employees' individual access rights, and conducting manual processes for periodic access reviews. With an identity governance solution installed, public agencies can consolidate identity repositories into a single authoritative source, and automate and streamline the process of reviewing access privilege across its workforce. In addition, identity governance solutions can define the policies surrounding that access to ensure full audit and HIPAA compliance. Identity governance solutions should also provide an identity risk score to all users that provide context to a state's overall risk management posture.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

Similar to HIPAA and HITECH, the Payment Card Industry Data Security Standard (PCI DSS) requires the implementation of strong access control measures among other security controls to protect cardholder data. PCI DSS has 12 main requirements and identity governance solutions can help organizations, including state and local agencies, to secure cardholder data with the following bolded actions.

NO.	REQUIREMENT
1	Install and maintain a firewall configuration to protect cardholder data.
2	Do not use vendor-supplied defaults for system passwords and other security parameters.
3	Protect stored cardholder data.
4	Encrypt transmission of cardholder data across open, public networks.
5	Protect all systems against malware and regularly update antivirus software or programs.
6	Develop and maintain secure systems and applications.
7	Restrict access to cardholder data by business need-to-know.
8	Identify and authenticate access to system components.
9	Restrict physical access to cardholder data.
10	Track and monitor all access to network resources and cardholder data.
11	Regularly test security systems and processes.
12	Maintain a policy that addresses information security for all personnel.

Through standalone capabilities and integrations with single sign-on, multifactor authentication and privilege management solutions, identity governance solutions can ensure appropriate password management, authentication and authorization mechanisms for regular and privileged users. In addition, identity governance can provide a centralized interface and repository for administrators to manage user privileges and identify any improper access credentials, conducting periodic access reviews and audits as necessary. Finally, identity governance can implement strong identity management policies at the intersection of other security, IT and human resource policies for full compliance coverage.

CONCLUSION

In the face of a rapidly-evolving threat landscape, significant budgetary restrictions, talent shortages, aging and outdated IT infrastructure, and compliance obligations, state and local government leaders must prioritize implementation of an identity management strategy rooted in governance. Identity governance solutions, through the prism of the "Five As" — authentication, authorization, administration, analysis and audit — can extend the lifecycle of legacy IT systems by consolidating identity data, automating provisioning capabilities to relieve overburdened IT security staffs, and scaling to increase security, ease compliance and enable business processes. As cyber threats to state and local governments continue to proliferate, CIOs and CISOs should embrace governance-based, identity-centric security strategy.

ABOUT THE CHERTOFF GROUP

The Chertoff Group is a premier global advisory firm focused on security and risk management. Founded in 2009, The Chertoff Group helps clients grow and secure their enterprise through business strategy, mergers and acquisitions, and risk management security services.

With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantage. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations.

Headquartered in Washington D.C., The Chertoff Group also maintains offices in Menlo Park and New York City. For more information about The Chertoff Group, visit www.chertoffgroup.com.

ABOUT SAILPOINT

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

SailPoint: The Power of Identity™