Three Questions State and Local Governments Should Answer Now About Identity Security

Jeff Kidwell and Mike Giordano

The American Rescue Plan, a $1.9 trillion economic stimulus package that became law in March of 2021, includes a $350 billion lifeline for state, local and tribal governments[1]. Governments have considerable leeway in how they apply the funding, which is available for costs incurred by the end of 2024[2]. Qualified expenses may extend to modernizing IT in several broad categories, such as public health and initiatives to address negative economic impacts from the COVID-19 pandemic.

The flexibility of the Coronavirus State and Local Recovery Funds means that states and localities have an extraordinary opportunity to transform their IT operations, workforce mobility and the services they offer constituents. As agencies weigh their digital options, a key concern is how to bolster the security around access to systems and files. The sooner IT and security leaders develop a roadmap for identity security, the smoother the overall transformation journey can be — and the greater the chances of claiming reimbursement before that 2024 deadline.

To get started, here are three important questions to answer.

1 Where are the organization's IT assets?

State, local and education (SLED) agencies gather vast amounts of sensitive data, from taxpayers' financial information to confidential documents filed with the courts. Although the data is a byproduct of the normal course of government business, many agencies recognize its value and put it to work in preventing crime, improving public health, providing personalized services to citizens and more.

What's not so obvious is where all this sensitive data is located. Typically, it's scattered across disparate systems and sequestered into functional silos. There it can stay out

[1] "Coronavirus State and Local Fiscal Recovery Funds," U.S. Department of the Treasury, https://home.treasury.gov/policy-issues/coronavirus/assistance-for-state-local-and-tribal-governments/state-and-local-fiscal-recovery-funds.

[2] "Coronavirus State and Local Fiscal Recovery Funds: Frequently Asked Questions," U.S. Department of the Treasury, June 10, 2021, https://home.treasury.gov/system/files/136/SLFRPFAQ.pdf.

of sight of the broader organization, often due to concerns about legal and regulatory compliance. Adding to the complexity, much of the data isn't even in databases — think emails, photographs, CAD diagrams and other unstructured documents.

The systems themselves could be outside of the IT division's purview. Shadow IT, or the use of unsanctioned IT resources, is a growing phenomenon due to the ready availability of subscription-based cloud solutions. Because these resources are excluded from oversight, they're more vulnerable to a data breach.

What To Do Now

Visit the departments and offices in your organization to find out where they store their documents and the kind of data they contain. Then, with this inventory in hand, apply data analytics to identify sensitive information and map the connections between data sources. This can help you decide what processes and solutions to use in protecting personal identifiable information (PII).

2 Who has access to these assets?

State and local governments provide numerous services for citizens in need.Delivering these services can involve employees, contractors and third-party providers accessing sensitive information, which agencies have the duty to protect. Sometimes organizations have to act fast to give access in times of emergency. There are real-world reasons for giving employees, contractors and other users immediate access to applications and platforms, but they need to be balanced with the concerns of exposing PII, over-provisioning a user and inadvertently exposing departments to future cybersecurity attacks.

Then there are aging infrastructures coupled with shifting internal departmental processes, which can create inconsistencies in the application of identity access management policies. An example of this is the sharp surge in unemployment applications during the COVID-19-related economic crisis. Policy guidance on unemployment relief (who could receive it and how long) was constantly changing, forcing state and local governments to amend user access with minimal identity management oversight.

The challenge comes in when contractors or employees change roles or leave the organization altogether. Keeping track of all these identities — and manually maintaining the appropriate permissions — can become an overwhelming effort. When users retain access to highly valuable assets and information long after they should, it creates a data security issue for the organization and could expose the PII of the constituents they serve.

What To Do Now

Use an activity monitoring software tool to see who's accessing sensitive data and PII. Compare that with the last time their access was reviewed. This way, you can narrow the field of users whose entitlements may need to be decommissioned or removed.

3 What are SLED users doing with that access?

State agencies typically have one organization that brings users onto the systems and another that maintains the system's infrastructure. On top of that, counties may be doing their own hiring and giving the new hires access to the state agency's platforms and applications. When all these groups get out of synch, the agency's Active Directory services — which connect users to the resources they need to do their work — can quickly become a convoluted security brew that exposes the organization to cybersecurity threats.

A similar situation can exist across user environments and systems. Over the last decade, state and local governments have evolved from a homogenous corporate network to a hybrid environment of on-premises, cloud and mobile computing — each of which may have a different set of identity access management protocols.

With more applications and platforms to manage, state and local governments have limited visibility into what users are doing with the access they have. That — paired with the lack of a uniform process to onboard and offboard users — can obscure the actions users are taking when they access systems that contain sensitive data, which leaves the organization open to an unauthorized disclosure. In 2019, unauthorized access amounted to 40% of the most common types of data breach attacks.[3]

What To Do Now

Use your activity monitoring tool to identify the top users of each resource. After verifying them, collaborate with them to develop a set of protocols governing the appropriate use of that resource and bring those protocols into your review processes.

[3] Lance Whitney, "Data breaches cost US companies more than $1.2 trillion last year," TechRepublic, June 3, 2020, https://www.techrepublic.com/article/data-breaches-cost-us-companies-more-than-1-2-trillion-last-year/

Putting the plan together

For state and local jurisdictions, IT historically has followed a distributed model. That is, the department of transportation may get funding for one type of platform, the department of health and human services for another and so on. The Coronavirus State and Local Recovery Funds are different because they offer the chance to build an identity security program horizontally across different departments.

Meanwhile, the pandemic revealed numerous disconnects in how state and local government implement identity access management protocols. Between these security gaps and the overarching security challenges that can occur with over-provisioning, IT leaders in state and local government face a complex issue that needs to be remediated before the next disaster strikes. To prevent a security breach or cyberattack, SLED entities should define an identity governance process and establish rules of engagement for managing complex identities. By asking these three questions — **where are the organization's IT assets, who has access to these assets, and what are SLED users doing with that access** — state and local governments can build out an identity security remediation plan. That in turn serves as the first step to an identity security program that supports the organization's mission while continuously reducing the complexity of manual provisioning.

ABOUT SAILPOINT

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.

SP1967-2107