5 Ways State and Local IT Leaders Can Drive Change in Their Organizations

On Nov. 15, 2022, funding for the State and Local Cybersecurity Grant Program (SLCGP) closed. The program promises $1 billion allocated to state, local, tribal and territorial governments over four years for shoring up cyber defenses, an action that is welcomed by many as cyber threat actors increasingly seek to disrupt state and local operations. In fact, between 2013 and 2018, nearly every state and territory reported experiencing cyberattacks, a number that has no doubt grown in recent years as attackers take advantage of changing IT environments and an increase in remote workers.

For malicious threat actors, stealing state and local data is big business. A recent report from The Conversation found that data stolen from organizations often finds its way onto the dark web, where the information sells for hundreds of thousands of dollars.

Many chief information officers understand the gravity of the situation, but this bears repeating: SLCGP funding is a once-in-a-lifetime opportunity to shore up cyber defenses. With this in mind, gaining employee buy-in will be of critical importance in helping CIOs with one of their most significant challenges: Driving organizational change.

So what can state and local IT leaders do to drive change management? Here's 5 tips to get started:

1 Establish Governance Surrounding Your Data and Information

Before starting down the path of change management, CIOs — alongside their security and technology counterparts — should look at drafting strong governance surrounding agency data and information systems. Without strong guidance or support from leadership, agencies may end up spending money on duplicate systems — therefore creating shadow IT — or exposing the company to potential security risks due to mismanagement of government information.

To drive change within state and local government requires the centralization of information. Here are four actions you can take today, to start building a strong governance plan according to the Office of Management and Budget's Federal Data Strategy:

- Appoint employees to an internal Data Governance Committee
- Map out the mission and vision of data within your organization
- Assess data maturity levels and record areas for improvement
- Build data architecture guidelines

Key Takeaway: Create governance and collaboration across departments surrounding your agency's security.

2 Look at Acquiring Industry Solutions to Increase Visibility Into Data & Assets

Driving change management requires a comprehensive understanding of workflows, processes and tools at play within your organization. To effectively drive change, IT leaders should look for solutions that help them consolidate.

"Our biggest challenge was inventory management. We didn't have a good sense of what or how many devices we had or where they were — let alone the software or amount of memory that was running on them. We were concerned that we were wasting money on licenses and devices that weren't being used," says Ryan Murray, deputy director for the State of Arizona's Department of Homeland Security.

According to Murray, utilizing an automated inventory management solution for hardware and software helped the State of Arizona's DHS gain the visibility they needed into their technology stack. Coupled with a strong governance framework, the DHS was able to successfully shore up its defenses and protect state data from malicious actors.

Key Takeaway: Search for solutions that provide visibility into your tech stack.

> **"Visibility is king, and we now have visibility that we never had before," says Ryan Murray, deputy director for the State of Arizona's Department of Homeland Security.**

3 Conduct a Workforce Assessment

Another crucial part of change management requires leaders to sit down with key stakeholders to understand their pain points. What parts of their job are tedious? What tasks are too complex or time-consuming? For the City of Bend, Oregon, these questions helped them pinpoint a significant issue: Employees were spending hundreds of hours gathering information and verifying information through inspections.

According to a case study from the Atlas, "[The City of Bend's] existing process was cumbersome and time-consuming, and ultimately left their program running an entire month behind when compared to what was happening in the field. One program manager was performing 500+ inspections per year, which took up the majority of her time."

By conducting a workforce analysis, the City of Bend found that this problem extended outside the initial scope of one individual and was a widespread problem within the organization. With this knowledge in hand, the City sought to onboard an automated solution that would help alleviate employees' burden when managing data.

Key Takeaway: Conduct a workforce assessment. Knowing your key stakeholders' pain points is crucial when building a use case. SLED leaders can leverage use cases to gain employee buy-in.

4 Establish a Digital Transformation "Dream Team"

In a recent article titled "State Chief Information Officers are Handling More Than Just Tech," Bill Lucia, executive editor for Route Fifty, explores the emergence of the State CIO as the "enterprise strategist." Although state and local leaders are increasingly relied upon to solve some of the biggest challenges facing the government, this is not a problem that has to be faced alone.

IT leaders should look to establish a "dream team" of employees and key stakeholders passionate about transformation. Establishing a task force of motivated employees alongside top-down governance can help leaders organically drive change. Your grassroots champions can source feedback and help act as that bridge between governance and action.

Key Takeaway: Establish a "digital transformation" dream team — this should consist of employees who are passionate about the product and can drive change within their teams and departments.

5 Connect with Industry Leaders

With malicious threat actors seeking to disrupt, deny and disable local government, now is the time to reach out to industry leaders. For Jennifer Pittman-Leeper, Whole of State Strategist and customer engagement manager for Tanium, collaboration is crucial.

Key Takeaway: Reach out to industry partners to set up collaborative partnerships.

> **"The only reason that ransomware and cyberattacks work is because we're keeping our mouths shut — we aren't communicating. In a whole-of- state model, if you only look within the confines of your state border, you're missing out on a lot of great ideas and solutions," explains JPL. "Partner with everyone and really find and identify vendors that are ready to listen to your challenges and work on them with you to achieve some of your goals."**

Learn more about how Tanium can help your organization drive digital transformation.

LEARN MORE

TANIUM