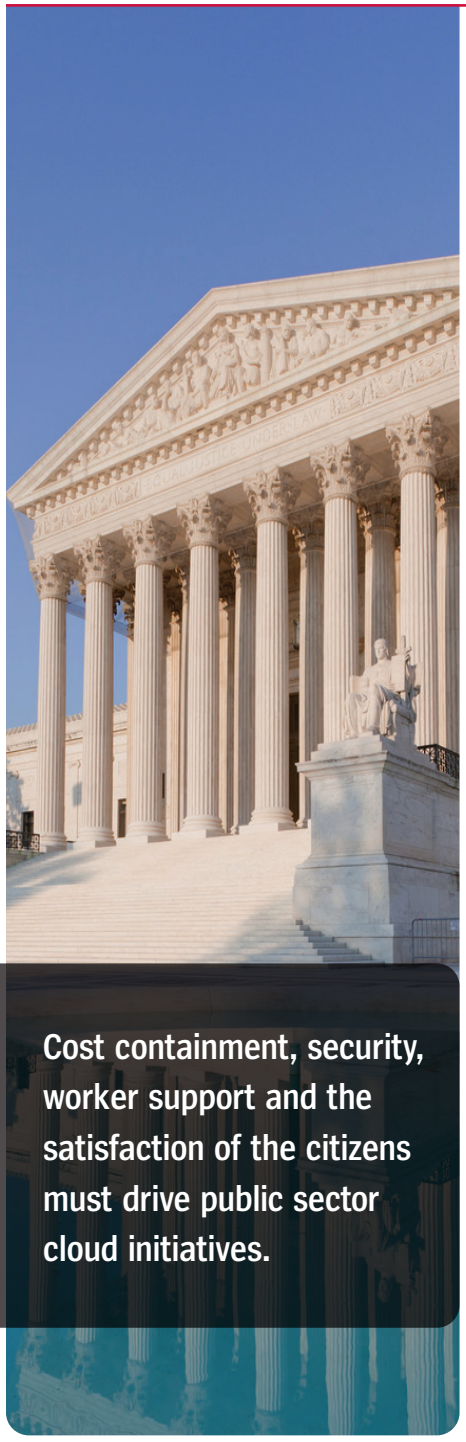
UNISYS | Securing Your Tomorrow®

Four Ways Cloud Can Meet the Most Pressing Public Sector Needs

By Shawn Kingsberry



Cost containment, security, worker support and the satisfaction of the citizens must drive public sector cloud initiatives.

As government agencies grapple with the pressures of tight budgets, cyber threats, skilled worker shortages, and citizen expectations, they can find ready value in an effective cloud adoption strategy.

Public sector CIOs and their IT teams can take credit for how swiftly and responsibly their organizations made widespread remote work manageable and secure in 2020 – in large part by moving as much computing power to the cloud as possible. Despite the challenges – legacy systems unsuited for remote work and contingency plans that failed to anticipate the emptying out of offices – by and large government agencies fulfilled their respective missions in the new and uncertain environment.

Now, as the pandemic wanes, many are redoubling their improvement efforts that inevitably lead to cloud services. The National Association of State CIOs (NASCIO) lists "cloud services" as #3 on its list of CIO Top 10 Priorities for 2021. In its annual survey, NASCIO queried its members about their cloud strategy. The responses underscored this priority:

- 41% of respondents have a cloud-first strategy for new applications.
- Another 17% have instituted or are in the process of instituting infrastructure-as-a-service.

But, as one state IT executive stated, "It's a mistake to think that 'cloud' is our focus – it's not. Our focus is on fixing problems so we can fulfill our mission – deliver the value the agency exists to provide. 'Cloud' just happens to be shorthand for the myriad technological improvements that we have deployed and will continue to deploy, if and only if they serve the particular needs of a particular agency."

And what are those needs? They vary by public sector organization, of course, but there are four major categories of prime importance to public sector CIOs.

1. Cost Containment

Cost containment is an ever-present obligation. Government CIOs are continually challenged to cut costs and do more with less. And now, after many months of unexpected but necessary spending on all the investments required to weather the pandemic (remote access infrastructure, laptops for newly remote workers, new collaboration options, added security for the expanded attack surface, contact center improvements, etc.), they are bound to have smaller budgets than otherwise anticipated. The Wall Street Journal reported that states could see a $434 billion shortfall, per Moody's Analytics.

On top of that, states will continue to be beset with new mandates, sometimes funded and often unfunded. Regardless, they still must execute the planned strategy – along with the mandates.

Cloud reduces the attack surface and leverages enormous storage and processing power to identify security threats.

Moving to the cloud comes with a price. But it also enables significant cost containment: reduced costs of licensing, hardware, labor and maintenance, CAPEX to OPEX paying only for the compute power needed, improved productivity, and software, compliance, and specialized skills all provided by the vendor.

2. Security

While health worries consumed much of the populace, public sector CIOs were equally consumed by security concerns. Acutely aware that their rush to provision employees with access from home (or the local coffee shop) was simultaneously a sudden, unplanned expansion of their attack surface, they had no choice but to redirect their cybersecurity professionals to focus on new vulnerabilities at the expense of planned support for new business applications/business.

The focus on cybersecurity was well warranted, as hackers and fraudsters took advantage of the pandemic-driven chaos to launch attacks around the world. Per Comparitech, U.S. government organizations experienced 79 separate ransomware attacks in 2020, "potentially impacting 71 million people and costing an estimated $18.88 billion in downtime and recovery costs."

Despite important security improvements in the public sector, security remains an ever-present priority for several reasons: the ongoing prevalence of remote workers as potentially vulnerable targets, the dearth of cybersecurity skills in the face of enormous demand, and the increased prevalence of IoT devices as a result of 5G. Yet, according to NASCIO, "Nearly half of all US states do not have a dedicated cybersecurity budget line item; most state cybersecurity budgets are between 0-3% of their overall IT budget, compared with an average of more than 10% in the private sector."

Unisys and other security experts were routinely tapped to assess whether agencies' protection was sufficient for the new, remote environment and the rising onslaught of penetration attempts throughout the pandemic. Invariably, new vulnerabilities would be discovered – and in some cases, previously undetected breaches.

Fortunately, cloud offers extensive security advantages, including integrating security and compliance, reducing the total attack surface that the organization's security experts need to protect, and leveraging enormous storage and processing power to identify security threats.

3. Worker Support

Government agencies have a fundamental challenge when it comes to tech workers: There are simply not enough skilled workers to go around, and they compete for the best candidates against private sector organizations who can outbid them. In addition, the median age of the state government workforce has been rising for years, disproportionately employing workers who are nearing retirement. Not only will that leave agencies shorthanded, overloading the remaining workers, but the retirees will take with them the institutional knowledge of the numerous legacy systems that younger workers are unable to support.

For government to work – to effectively serve the taxpayers who support it – employees need to be supported, and increasingly that means digital workers. The digital spike at the onset of the pandemic shone a bright light on the technology-related obstacles government employees face. One study found that 85% of government tech professionals surveyed claimed to be unable to deliver adequate services because of outdated IT systems – not surprisingly, given the magnitude of the change. Before the pandemic, less than 5% of staff worked remotely. After its onset, more than half of workers were remote in 35 states, while nine states had more than 90% remote, and thus had constrained access to normal support.

Because cloud computing can significantly improve worker productivity, government organizations that prioritize transformation can offset the severe attrition they experience, relieve workloads, and deploy their skilled workers to mission-critical activities.

One state reported its five main difficulties to be: 1) not having telework policies in place, 2) failing to accommodate non-essential employees whose work could not be done remotely, 3) numerous technology challenges reported by 83.6% of the state's agency leaders and 47.2% of its employees, 4) insufficient guidance for supervisors on managing remote teams and tracking productivity, and 5) difficulty maintaining productivity.

Because cloud computing can significantly improve worker productivity, government organizations that prioritize transformation can offset the severe attrition they experience, relieve workloads, and deploy their skilled workers to mission-critical activities. The increase in cloud security options also means that more and more workers, even those in highly sensitive positions, can perform much of their work remotely – thus enabling agencies to recruit from a wider pool.

4. Citizen Satisfaction

Citizens are people, and people are fickle. What astonishes and thrills them one day strikes them as nothing more than technology table stakes the next day. One moment they are thrilled to see they can update their auto registration online. Halfway through they are annoyed that the website doesn't already know their license number and autofill it for them.

As the pandemic pushed private sector companies to ever-greater accommodation of remote interactions, citizen expectations rose accordingly. With little exaggeration, it can be said that citizens now expect to interact with government agencies with the same ease and confidence that they interact with Netflix. Not surprisingly, they are frequently disappointed because cost pressures and skill shortages constrain governments from investing in improvements. But make no mistake, those that can deliver a better citizen experience will have a demonstrable competitive advantage when it comes to recruiting employees and businesses.

Shifting workloads to the cloud can free up employees to focus on improvements to the citizen experience. It can reduce departmental silos and bottlenecks and eliminate the excessive paperwork that otherwise complicates service delivery and frustrate citizens.

When a large U.S. state government's technology arm engaged Unisys to improve the overall quality and speed of services to agencies and citizens *and* do so at a better price point, they achieved their goals through a variety of technology advances: single sign-on for a better end-user experience, moving to a data consumption model for lower costs, faster infrastructure deployment (months to hours), better security, and the ability to rapidly offer new and innovative services to citizens.

Conclusion

Cloud adoption is bound to be in the future for virtually every public sector organization. As CIOs and other leaders assess the transformation journey that will best serve their overall strategy, each must weigh the relative value and timing of using cloud computing to contain costs, secure assets, and improve worker and citizen experience. Making those strategic and high-impact decisions can be substantially facilitated by understanding the experiences of other organizations, both public and private.

Shawn Kingsberry
Shawn is Vice President of Digital Government and Citizen Services for Unisys, is a recognized expert in driving digital government transformation by guiding public sector consumers to adopt cloud computing, data analytics and other digital government platforms.

For more information visit www.unisys.com

06/21 21-0278