The Pathway to Modern Government:
How the Public Sector Can Build Constituent Trust

Trust isn't given, it is earned. But with every headline about a new data breach or ransomware attack, the public's faith that government can protect their data is at risk. Constituents want more digital services with their information unified across government systems so they don't have to repeatedly provide the same information. They want a seamless, efficient experience and they want their data to be secure throughout the process. Modernization can empower government agencies to meet their constituents' expectations while securely expanding their digital footprint.

Current Barriers to Constituent Trust

Several factors affect constituents' faith that governments will keep their data safe, but none more so than a security incident.

"What impacts trust for citizens is, frankly, when there's a breach. Even a very small breach with very little information that becomes inconsequential for citizens amplifies their lack of trust with government and their data," says Kathy Cruz, director of government cybersecurity at KPMG, a leading professional services firm that works with governments to transform their operations and service delivery models.

Some constituents also don't completely understand how governments will use their data, even though many municipalities have policies on their websites regarding privacy and compliance. Legacy technologies, data silos, and limited automation can lead to cumbersome government interactions with constituents and make government data collection and deployment processes seem opaque.

However, modernizing their technology infrastructure, business processes, and user interfaces can help governments deliver a more seamless and transparent experience. Modernization can position governments to create unified constituent profiles across departments, be more agile, and deliver more responsive service, especially during times of crisis when constituents rely on these organizations the most.

How to Build Greater Trust in Government with Modernization

Modernization can help governments build trust in four critical ways: improving their data center operations, enabling a development security operations (DevSecOps) approach, bringing IT and the business closer together, and facilitating vendor management to reduce third-party security risks.

Improving data center operations

Outdated programming languages and unsupported or unpatched hardware and software solutions present barriers to modernization and increase governments' security vulnerabilities in today's relentless threat environment. By extension, this undermines constituents' faith that government agencies can effectively protect their data.

A modern data center, whether in a public, private, or hybrid cloud, makes it easier for agencies to scale their compute resources as their business needs change. It also improves uptime, availability, reliability, and critical application performance. Governments can provide a secure digital constituent and employee experience because a modern data center allows them to onboard the latest security automation technologies that increase enterprise visibility and facilitate unified management of IT assets.

"As government entities implement their vision for modern government by enhancing the citizen experience, modernizing their support functions, re-inventing operations, and building stakeholder and citizen trust, the modern data center is now front and center in this transformation," Cruz says. "With data on-premises and in multiple clouds and increased reliance on third parties, it's never been more important to ensure citizens can trust that the personal data they share with government is protected to the highest standards."

In addition to the security advantages a modern data center provides, it improves collaboration across departments and with external business partners, including technology vendors and strategic consulting partners.

Data silos often hamper enterprise visibility and make it difficult for government organizations to access meaningful intelligence that can drive better decisions, but modernization can break down these silos and foster greater interagency and enterprise collaboration.

As governments try to determine how to put public dollars to highest and best use to deliver maximum impact, a modern data center can reduce their IT burdens and expand their IT capacity, freeing technical teams to focus on innovations and everyday improvements that enhance the constituent experience.

Enabling a DevSecOps approach

Modernization can also foster greater collaboration among development, security, and operations teams.

A DevOps approach makes security integral to the development process and improves application, device, and infrastructure performance — and by extension, governments' resilience. This approach allows governments to be nimble because security is integrated from the very beginning of the project lifecycle, rather than at the end where this consideration can add time and costs to technology projects and delay delivery.

"In today's environment, citizens want things delivered digitally, so government needs to be nimble," Cruz says. "In the DevSecOps model, you're incorporating security from initiation of the project through delivery of the project and delivery of the solution, so it's much more efficient."

> **"Trust has to be built into the business imperative and into the business mission. It can't be something that IT or the security organization handles."**
>
> *- Kathy Cruz, Director of Government Cybersecurity, KPMG*

Bringing IT and the business closer together

Governments have had to contend not just with data silos, but organizational silos. While the enterprise as a whole may have an overarching mission, every department also has its own goals and objectives that feed into this broader mission.

However, with governments onboarding an array of cloud services and digital solutions, it's imperative for IT and the business to work more collaboratively to mature their organization's risk management program. This new joint risk responsibility means IT and the business must work together to collectively understand their organization's risk appetite, including what level of data loss the organization is willing to accept, what high-priority assets they must protect, and in what type of computing environment they will store certain organizational data.

IT and the business also must collaborate to build a security-minded culture within their organizations. Security must be organic within an organization's ecosystem, rather than a separate program. This means building cyber-awareness among employees year-round — and not just with an annual security training exercise. It also means educating employees, enabling them with the right knowledge and tools, and consistently enforcing compliance with internal governance policies to make sure everyone is a key stakeholder in protecting the organization's data.

Facilitating vendor management to reduce third-party security risks

Modernization can give government agencies the tools and capabilities they need to minimize their internal and external risks from third-party vendors.

Due to hybrid work and a growing number of digital applications, the attack surface has expanded. More applications are connecting to agency networks and governments need greater visibility into the potential risks they pose. Therefore, to build greater trust, agencies must implement a robust third-party risk management strategy.

As part of this strategy, agencies should verify and measure their vendor's security program throughout the contract lifecycle — not just at the beginning of an engagement. They should classify each vendor's risk level based on the system and data access they require and services they provide. They also must conduct regular independent audits to validate cloud services and ongoing vulnerability assessments with their external partners to ensure they have implemented robust security measures.

It's important for governments to understand the third-party vendor risk isn't static. Managing this part of their security program will require constant attention.

"We've arrived at the day where governments have to ensure their partners have good security practices and measures in place and that they're being verified," Cruz says. "It's one thing to put them in contractually, but in a five-year contract how do you know that during year two something hasn't unintentionally gone wrong? There has to be not only the contractual terms, but ways to verify and measure security throughout the life of the contract."

The Trust Factor in Modern Government

Trust isn't given, but rather earned. In government, this is especially true.

It only takes one security incident to compromise constituents' trust that governments will keep their data safe. But agencies can significantly reduce the likelihood of these events by modernizing their data center operations, embracing a DevSecOps approach, fine-tuning their internal collaborative processes, and better managing third-party risks. Employing all these strategies will empower agencies to adopt more proactive security measures and bring their organization together to better serve constituents.

"Trust has to be built into the business imperative and into the business mission," Cruz says. "It can't be something that IT or the security organization handles. Building trust and sustaining trust has to be everyone's mission."

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from KPMG.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: KPMG

For more than 100 years, KPMG LLP has assisted governments, higher education, research and not-for-profit organizations through sector-specific audit, tax and advisory services. Today, we help these organizations adapt to new environments by working with them modernize their business models, leverage data, increase operational efficiencies and ensure greater transparency.

IMAGE PROVIDED BY SHUTTERSTOCK.COM