Security & Risk Management:

MODERNIZING IT INFRASTRUCTURE FOR BETTER PROTECTION

PRESSURE TO DELIVER FASTER, BETTER AND MORE economical government services is driving IT modernization across state and local government. But new research from the Center for Digital Government (CDG) indicates that CIOs are approaching modernization with growing emphasis on value.

CDG surveyed 126 state and local IT leaders in March 2017 to determine their perspectives and priorities relating to technology, procurement and planning. Respondents said "budget, cost control and fiscal management" dominate their attention, discussions and strategic planning activities nearly across the board. This thought leadership paper explores how to approach security and risk management in an environment where value and fiscal responsibility are paramount.

Stories about cybersecurity threats against governments are commonplace. Some of these threats result from lapses in data handling policies or IT governance and oversight. In other cases, they're more sinister.

Like their private sector counterparts, government agencies have experienced incidents ranging from accidental release of sensitive data to devastating phishing attacks. In some cases, these incidents have compromised personal information for millions of citizens, disrupted crucial operations and cost agencies millions of dollars for remediation.

In the modern digital economy, state and local agencies share a growing amount of data with citizens and business partners. But information systems deployed years or decades ago weren't designed with today's threats in mind. More systems than ever are network or Internet connected. And state and local IT leaders also must ensure that newer technologies — like cloud and mobile devices — offer the data protection that governments need.

Given those realities, perhaps it's not surprising that security and risk management are key priorities for CDG survey respondents. Security ranked second only to budget and cost control as a current focus of attention and strategic planning. What's more, respondents don't foresee their commitment to security changing anytime soon — 37 percent say they expect future engagement and attention to be directed toward this priority.

Within security and risk management, mobile, cloud technology, platforms and servers were called out as needing increased investment. This indicates CIOs understand the future capabilities necessary to increase data security, but they need access to larger budgets or the ability to shift current allocations to facilitate their organizations' digital transformations. In fact, 31 percent of those surveyed said improving security and reducing risk was their greatest challenge — again, second only to budget, cost control and fiscal management.

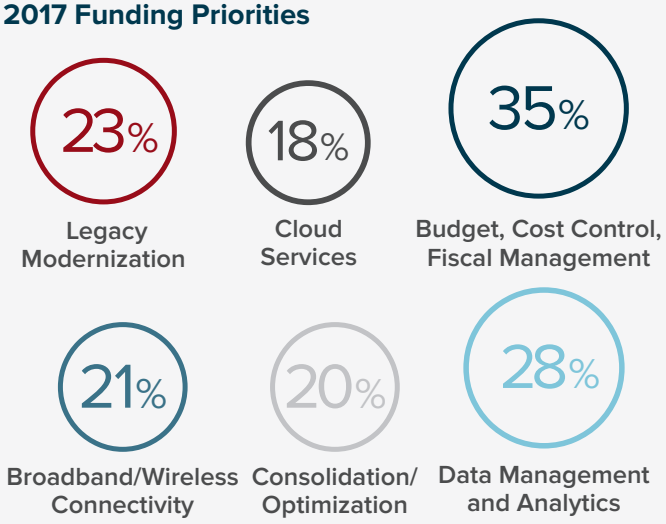
To adequately manage risk in today's dynamic threat environment, security must be built into every aspect of IT. Some states may have the internal capability to assess the risk posed to their current systems and to combat today's cybersecurity threats — but most don't. To have comprehensive security throughout their IT infrastructure, states need to start with a secure foundation and operating system and keep security in mind throughout the software development life cycle.

Commercially supported open source solutions can help states achieve this goal. Protecting against sophisticated

security threats requires a modern operating system that can adapt to new challenges and be customized to meet the public sector's unique needs. Linux, an open source operating system,[1] can serve as the foundation for the public sector's modern IT infrastructure, providing the resiliency governments need and the value CIOs demand.

Security and Risk Management: A Top Priority for State and Local CIOs

2017 Funding Priorities



Security and Risk Management

Top Investment Priorities within Security and Risk Management

48%	Mobile
44%	Cloud
41%	Platforms/Servers
41%	Storage
17%	Automation/Outsourcing
17%	Virtualization

Why Open Can Be More Secure

Protecting data is one thing, but remaining transparent doesn't compromise security — it enhances it, because the best minds across the private and public sector can work together to solve the problem.

"The things that keep me awake at night are the things I don't know about," Jon Dolan, chief information security officer of Oregon State University recently told *Government Technology.* "It's the things that I have no idea are out there that the hackers know that I don't, that are going to cause us problems on our security operation front."[2]

This same concern likely keeps other CIOs' minds reeling. Commercially supported open source solutions provide greater transparency and more responsiveness to quickly address issues when they arise, which is critical for state and local governments in the event of a security breach that could affect millions of citizens. For instance, Red Hat's annual Product Security Risk Report provides information about vulnerabilities and how they were addressed by the company.[3] This type of support is one reason why it's important to choose commercially supported open source solutions, rather than free versions that can introduce risk.

The CDG survey indicates local and state IT leaders are rightly concerned about security and risk management, but to address this technology priority they need not only to have a willingness to increase investment in this area, but also must adopt solutions that are more flexible, open and collaborative — which may seem counterintuitive.

Commercially supported open source software, however, can have distinct security advantages over proprietary software because it is developed and refined collaboratively by user communities. This open collaboration enables teams to proactively identify weaknesses and create more secure environments than they would have been able to achieve working in silos. As IT security challenges continue to evolve and more threats arise, adopting this approach is critical to help state and local CIOs build a secure, modern IT infrastructure. »

1. https://www.redhat.com/en/files/resources/en-rhel-7-server-datasheet-12182617.pdf
2. http://www.govtech.com/security/Is-Open-Source-Software-More-Secure.html
3. https://www.redhat.com/en/resources/2016-product-security-risk-report

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. The Center conducts e.Republic's annual Digital Cities and Counties Surveys; the biennial Digital States Survey; and a wide range of custom research projects. **www.centerdigitalgov.com**

For: redhat.

State and local government agencies demand performance, transparency, and value—exactly what Red Hat offers. As the standard for Linux in governments worldwide, our cloud, virtualization, storage and platform solutions bring freedom and collaboration to the public sector. Bring the power of open source to your agency. We are a part of a larger community working together to drive innovation. Learn more at: **www.redhat.com/government**