Today, these forces of change are led by the highest priority of all CIOs—cybersecurity and risk management. Since 2013, this priority has held the number one position as voted by state CIOs in NASCIO’s annual top 10 ranking. It’s evident state governments are at risk.

Today’s headlines are filled with stories of cybersecurity incidents and their disturbing impact on both public and private sector organizations. Because of the massive amounts of personal information held in trust by state government agencies, states are attractive targets for hackers, cyber criminals and foreign entities, and in the last three years, states have experienced a significant increase in cybersecurity threats. Attacks from activist groups or “hacktivists” with a political agenda have also become more prevalent. In fact, because of the increasing severity, volume and sophistication of cyber threats, states are becoming more vulnerable to attacks.

State governments face persistent challenges in cybersecurity risk reduction because of several factors, most importantly these four key issues:

- **Inadequate Strategic Direction and Organizational Structure**
- **Constrained Security Budgets**
- **Increasing Sophistication of the Threats**
- **Lack of Cybersecurity Professionals**

In the face of these rising threats, states must organize for success with a clear and authoritative governance structure that includes all appropriate stakeholders—and not just technology leaders. Cybersecurity threats present “business” risks to the states and must be understood in this context. States should adopt a cybersecurity framework based on national standards and guidelines, including a focus on adopting critical controls for cyber defense, and should prioritize actions that will yield the best results. This will provide a roadmap for action and guide investments.

Certainly cybersecurity should be addressed as a significant risk to state governments and funded at a level commensurate with the risk. Based on NASCIO data, the percentage of IT spending on security is much lower than recommended benchmarks for comparable organizations. States should prioritize their risks and adequately invest in data protection, security tools and training. Finally, NASCIO recommends states plan for the consequences of a cyber incident or data breach with a robust recovery protocol, including a crisis communications plan.

**EVOLVING SERVICE DELIVERY MODELS**

With a focus on enterprise strategy, state CIOs preside over increased diversity in service delivery models and options for sourcing IT services. Since 2010, state CIOs have continued a steady progression toward more consolidation, optimization of technology resources, and increased use of shared services and outsourcing. One thing is clear; the conventional “owner-operator” model, where state government owns all the computer systems and infrastructure and licenses commercial software to support business applications, is declining. More than half the states now outsource at least some of their IT infrastructure and operations. NASCIO expects this trend to continue and transform the longstanding approach to IT management in state government.

This shift has been supported by the major force of change in IT—cloud computing.

Cloud computing allows organizations to pool expensive IT resources and consume needed services like a utility.

Leveraging advances in technology and the power of the internet, users pay for only what is used when it’s needed. Constrained by budgets and supported by the availability and utility of cloud services, state governments are becoming more mature in adopting this alternative approach. An attractive model delivers business software applications using Software-as-a-Service, or SaaS, over the internet, where the application and supporting infrastructure are provided by an external third party, rather than the state data center. While cloud services are certainly more flexible and agile than traditional IT service delivery, their adoption raises policy questions related to procurement, data ownership, security and legal concerns that must be addressed.

**RENEWING THE WORKFORCE**

A major concern for state CIOs continues to be the significant number of state IT employees who are eligible to retire today. The pending retirements and the challenge of recruiting new IT talent to state government is a force of change with significant impact. Some call it a crisis. Retirements present a challenge, but also an opportunity to bring new talent to the state workforce. However, 86 percent of states are having difficulty recruiting new employees to fill vacant IT positions.

The major reason?

State CIOs continue to advocate for personnel and pay reforms and have been proactive in using non-traditional and innovative approaches for recruiting. Crafting a formal marketing strategy, using social media, partnering with schools and universities, targeting veterans and tracking metrics are all essential to a successful program.

It remains to be seen if states can fill the IT pipeline and retain the talent they recruit. What’s clear is the transition to a digital government world is highly dependent on a skilled and capable state IT workforce.

**DATA IS EVERYWHERE!**

The growth of digital data and the power of analytics represent prominent forces of change in state government. As service and knowledge intensive organizations, states rely on data, but historically only a small percentage of data collected is ever analyzed for insights on citizen service delivery, improving performance and making better policy decisions. This is slowly changing, but will quickly advance if states devote more attention to data strategy, governance, stewardship and quality.

State agencies do recognize data and information are essential to improved service delivery and program integrity. They are responding to the public demand for open data and presenting more datasets in online portals and dashboards, including opening up legacy data resources.

States also are exploring new ways to support and improve the performance of programs and service delivery through better management of government data, business intelligence and data analytics. There is power in analyzing data on new trends and capabilities, however, states will need to focus on appropriate roles and responsibilities, while being attentive to security and privacy concerns.

About the Author

Doug Robinson is the executive director of the National Association of State Chief Information Officers. By Doug Robinson