State Governments at Risk: Time to Move Forward

National Conference of State Legislatures Executive Committee Meeting
Minneapolis, Minnesota
May 21, 2016
About NASCIO

- National association representing state chief information officers and information technology executives from the states, territories and D.C.

- Founded in 1969

- NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.
Agenda

- Chief Information Officers - Role & Authority
- Cybersecurity
- Best Practices
- Forces of Change
Multi-Faceted Role of the State CIO

- Manage, Deploy, and Develop State IT Resources
- State IT Governance
- Customer Service
- Enterprise Architecture
- Strategic Planning
- Procurement and Sourcing
- Cross Boundary Collaboration
- Operations & State IT Infrastructure
- Legislation, Policy and Directives
- Managing Risk: Securing State IT Assets

State CIO
How are State CIOs Organized to Meet Demands?

- Complete decentralization
- Decentralization with consolidated infrastructure
- Decentralized with centralized planning
- Federated - agency decision making
- State IT Authority full consolidation

States approach IT governance with different strategies, business drivers and models. There are variations on these themes depending on state finances, political will and the ability to absorb change.
Not all State IT is created equally...

- Governor’s policy agenda
- The CIO’s authority
- The CIO’s priorities
- Governance models
- The strategic IT plan
- State CIO business model
- Gaps: capabilities, disciplines
## Service Delivery in the Next Three Years?

<table>
<thead>
<tr>
<th>How does your state CIO organization plan to deliver or obtain IT services over the next three years?</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand existing IT shared services model</td>
<td>62%</td>
</tr>
<tr>
<td>Outsource business applications through a Software-as-a-Service model</td>
<td>55%</td>
</tr>
<tr>
<td>Expand existing managed services model</td>
<td>53%</td>
</tr>
<tr>
<td>Downsize state-owned-and-operated data center(s)</td>
<td>49%</td>
</tr>
<tr>
<td>Expand outsourcing</td>
<td>43%</td>
</tr>
<tr>
<td>Introduce a managed services model</td>
<td>26%</td>
</tr>
<tr>
<td>In-source some operations that currently are outsourced</td>
<td>17%</td>
</tr>
<tr>
<td>Introduce outsourcing as a new service model</td>
<td>15%</td>
</tr>
<tr>
<td>Maintain the status quo</td>
<td>13%</td>
</tr>
<tr>
<td>Introduce an IT shared services model</td>
<td>6%</td>
</tr>
<tr>
<td>Build new data centers</td>
<td>2%</td>
</tr>
<tr>
<td>Increase state IT staff</td>
<td>2%</td>
</tr>
</tbody>
</table>

Source: The Value Equation, 2015 State CIO Survey
How satisfied are you with the current system of IT procurement in your state?

- 34% Very satisfied
- 13% Very dissatisfied
- 34% Moderately dissatisfied
- 15% Neutral
- 4% Moderately satisfied

Source: The Value Equation, 2015 State CIO Survey
Call To Action: Recommendations for Improved State IT Procurement

The state information technology (IT) community has long called for improvements in IT procurement processes and practices and state chief information officers (CIOs) are consistently dissatisfied with the state IT procurement process.

In the 2015 state CIO survey, The Value Equation, roughly one-half (47%) of state CIOs expressed negative outlooks on IT procurement processes.

Because of this consistent level of dissatisfaction, NASCIO is advocating for procurement reform by issuing the following call to action to states. NASCIO recommends that states:

- Remove unlimited liability clauses in state terms and conditions
  - As of 2016, 36 states have eliminated unlimited liability (www.nascio.org/LOL).

- Introduce more flexible terms and conditions
  - As technology options continue to evolve, states must adopt flexible and agile terms and conditions (see Center for Digital Government’s Best Practice Guide for Cloud and As-A-Service Procurements).

- Don’t require performance bonds from vendors
  - In order for states to lower costs and create a competitive procurement pool, states need to consider finding ways of leveraging existing protections and adjusting performance bond requirements if necessary (see NASCIO publication Leverage Performance Bonds at the Door).

- Leverage enterprise architecture for improved IT procurement
  - The procurement process should be adjusted to recognize and align with enterprise IT strategies, architecture and standards based acquisitions (see NASCIO publication Leverage Enterprise Architecture for Improved IT Procurement).

- Improve the Negotiations Process
  - Implement rules for using competitive negotiations to facilitate “give-and-take” between buyer and seller (see UIIS Institute document Strategies for Procurement Innovation and Reform).

For more information and resources, please visit www.nascio.org/procurement

NASCIO Procurement Contact:
Meredith Ward, Senior Policy Analyst
mward@nascio.org

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States.

Copyright © 2015 NASCIO All Rights Reserved www.nascio.org 201 East Main Street, Suite 1405 Lexington, KY 40507
Top Ten: State CIO Priorities for 2016

1. Security
2. Cloud Services
3. Consolidation/Optimization
4. Business Intelligence & Data Analytics
5. Legacy Modernization
6. Enterprise Vision and Roadmap for IT
7. Budget and Cost Control
8. Human Resources/Talent Management
9. Agile and Incremental Software Delivery
10. Disaster Recovery/Business Continuity

Source: NASCIO State CIO Ballot, November 2015
Cybersecurity Risks in the States

- Protecting legacy systems
- Malicious software
- Inadequate policy compliance
- Mobile devices and services
- Use of social media platforms
- Use of personally-owned devices (BYOD) for state business
- Adoption of cloud services; rogue cloud users
- Foreign state-sponsored espionage
- Third-party contractors and managed services
New Reports from NASCIO

The stakes are high and unless there are dramatic changes in the way society responds to cyber attacks and deals with cybercrime the losses will continue to exhaust state coffers and strain the economy at a continued alarming rate.

Some estimates present that the impact of cybercrime on the global economy is an annual "leakage" or "hemorrhage" of $175 billion to $445 billion per year. These estimates do not take into account the aftermath on the lives of those individuals and families working to recover their identities, or restore their losses and to get their lives back or the disruption of government operations and services. Nor do these estimates address the opportunity cost to companies and governments that could have invested these same billions into improving the lives of people in our communities that struggle with poverty or populations that are coping with drought or disease outbreaks or even epidemics; the disruption of government; and lost investments in innovation.

Information has been described by some as:
- the lifeline of democracy;
- the lifeline of the economy;
- the lifeline of government; and
- the lifeline of any organization.

With this in mind, the loss of information can clearly be referred to as a hemorrhage, a drain on democracy, the republic we live in, the economy, government, corporations, and ultimately, a drain on society.

The previously cited report recounts three areas of opportunity cost related to cyber security:
- reduced investment in research and development,
- risk averse behavior by businesses and consumers that limits Internet use, and
- increased spending to defend networks.

Our nation cannot afford these losses or hope the problem goes away. Further, cyber threats are ever changing. Attacks are more sophisticated, more frequent, more effective and more persistent. Advanced persistent threats continue to infiltrate networks and stay there for months or years without the...
The ultimate outcome sought through NASCIO’s Cyber Disruption Response Planning initiative is the eventual development of state government resiliency.
# State CIOs and Cybersecurity

What major barriers does your state face in addressing cybersecurity?

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of adequate funding</td>
<td>64%</td>
</tr>
<tr>
<td>Lack of executive support</td>
<td>2%</td>
</tr>
<tr>
<td>Increasing sophistication of threats</td>
<td>77%</td>
</tr>
<tr>
<td>Emerging Technologies</td>
<td>43%</td>
</tr>
<tr>
<td>Lack of visibility and influence with the enterprise</td>
<td>23%</td>
</tr>
<tr>
<td>Lack of governance and authority</td>
<td>13%</td>
</tr>
<tr>
<td>Inadequate availability of security professionals</td>
<td>62%</td>
</tr>
</tbody>
</table>

Source: The Value Equation, 2015 State CIO Survey
Key Themes from the 2014 Study

Maturing role of the CISO
Budget-strategy disconnect
Cyber complexity challenge
Talent crisis

2014 Deloitte-NASCIO Cybersecurity Study
Budget-Strategy Disconnect

Funding is still the #1 barrier to effective cybersecurity

Security allocation as part of IT budget remains unchanged

46.8% of states have only 1-2% of IT budget for cybersecurity

Lack of sufficient funding

Senior Executive commitment is there, but funding still insufficient

65.3%

2014 Deloitte-NASCIO Cybersecurity Study
Cyber Complexity Challenge

- Sophistication and sheer range of cyber threats continue to evolve
- Regulatory complexity is growing
- Complex and mostly federated state government environment poses governing challenges
- CISOs and business leaders are not on the same page regarding the states’ abilities to protect against an attack
Talent Crisis

FTE counts are increasing

49% 6 to 15 FTEs

Competencies have increased, training has improved

7 out of 10 states agree

Top challenge is staffing

Salary
9 out of 10 CISOs

Inadequate availability of cybersecurity professionals

Barrier #3 59%
What skills and disciplines present the greatest challenges in attracting and retaining IT employees?

Source: NASCIO State IT Workforce: Facing Reality with Innovation, April 2015
By the Numbers: Consequences For States

- Government agencies have lost more than **94 111.5 million** records of citizens since 2009
- Average number of days between discovery and disclosure: **58**
- Average cost per breached record in US: **$201**
- Average cost per breach: **$5.8 million**

What Do We Know? Patterns of Success

- Enterprise Leadership and Governance
- Statewide Cybersecurity Framework & Controls
- Cybersecurity: A Team Sport
- Know the Risks, Assess the Risks, Measure
- Communicating the Risks: Training
- Invest: Deploy Security Technologies
NASCIO’s Cybersecurity Call to Action

Key Questions for State Leaders

- Does your state government support a “culture of information security” with a governance structure of state leadership and all key stakeholders?
- Has your state conducted a risk assessment? Is data classified by risk? Are security metrics available?
- Has your state implemented an enterprise cybersecurity framework that includes policies, control objectives, practices, standards, and compliance? Is the NIST Cybersecurity Framework a foundation?
- Has your state invested in enterprise solutions that provide continuous cyber threat detection, mitigation and vulnerability management? Has the state deployed advanced cyber threat analytics?
- Have state employees and contractors been trained for their roles and responsibilities in protecting the state’s assets?
- Does your state have a cyber disruption response plan? A crisis communication plan focused on cybersecurity incidents?
The Forces of Change

1. Service models and sourcing options
2. Adoption of cloud services
3. Power of data
4. Changing state IT workforce
Top Ten: State CIO Priorities for 2016

1. Security
2. Cloud Services
3. Consolidation/Optimization
4. Business Intelligence & Data Analytics
5. Legacy Modernization
6. Enterprise Vision and Roadmap for IT
7. Budget and Cost Control
8. Human Resources/Talent Management
9. Agile and Incremental Software Delivery
10. Disaster Recovery/Business Continuity

Source: NASCIO State CIO Ballot, November 2015
What is your State's status regarding Cloud Services?

- 83% The State is already highly invested in Cloud Services
- 11% The State is still investigating Cloud Services
- 4% The State has some applications in the Cloud and is considering others
- 2% Other

Source: The Value Equation, 2015 State CIO Survey
Forces of Change: Why Cloud?

- Cost savings and efficiency
- Flexibility and scalability
- Rapid provisioning
- Measured service
- Better data security?
- Shift from capital spend to operating spend
- Reduced IT staffing and administration costs

This transition is disruptive to the traditional notions of state IT. It has serious implications for state budgeting, procurement, legal, business processes, project and portfolio management.
Nearly 92 percent of states say salary rates and pay grade structures present a challenge in attracting and retaining IT talent.

86 percent of states are having difficulty recruiting new employees to fill vacant IT positions.
• 46 percent of states report that it is taking 3 to 5 months to fill senior level IT positions

A shortage of qualified candidates for state IT positions is hindering 66 percent of states from achieving strategic IT initiatives

Security is the skill that presents the greatest challenge in attracting and retaining IT employees
Yejin Cooke
Director of Government Affairs

ycooke@NASCIO.org
www.nascio.org
@nascio