State Governments at Risk: Time to Move Forward

National Conference of State Legislatures Executive Committee Meeting

Minneapolis, Minnesota

May 21, 2016

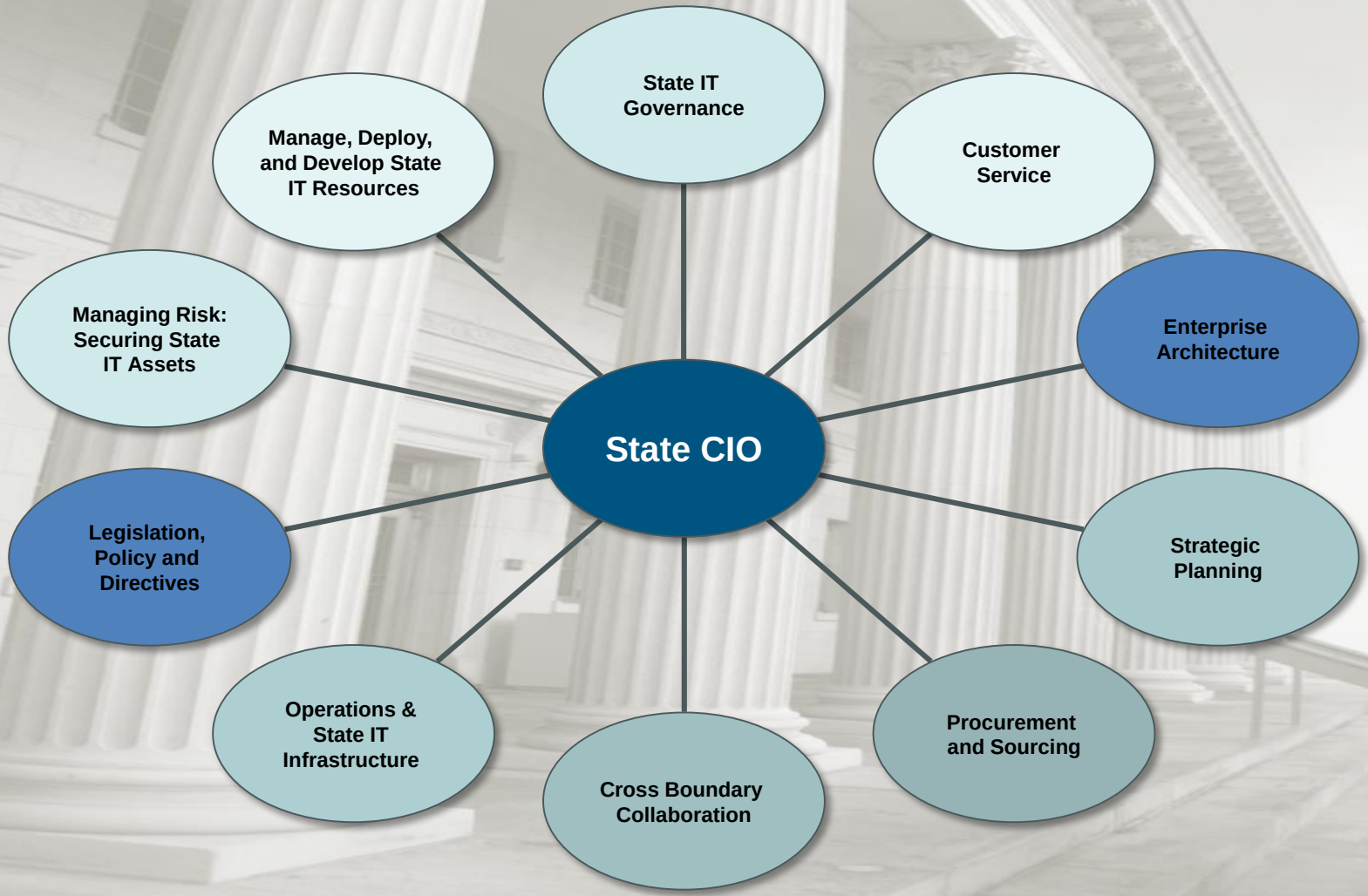
About NASCIO

- 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.

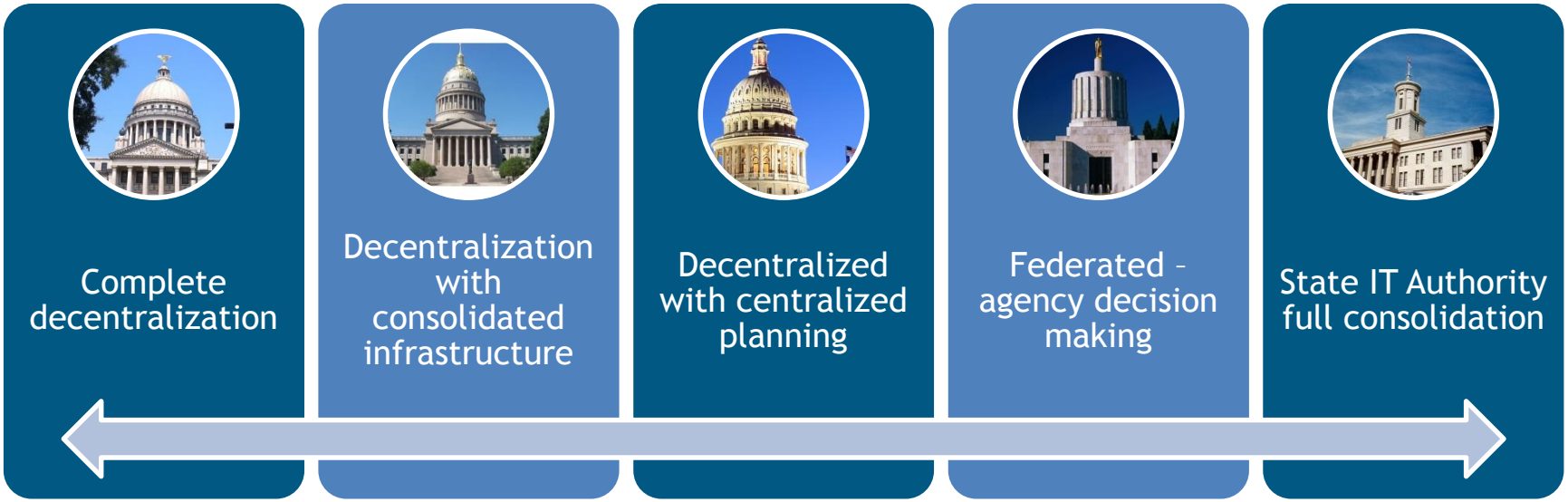
Agenda

- Chief Information Officers – Role & Authority
- Cybersecurity
- Best Practices
- Forces of Change

Multi-Faceted Role of the State CIO



How are State CIOs Organized to Meet Demands?



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.

Understanding the State CIO Landscape

Not all State IT is created equally…

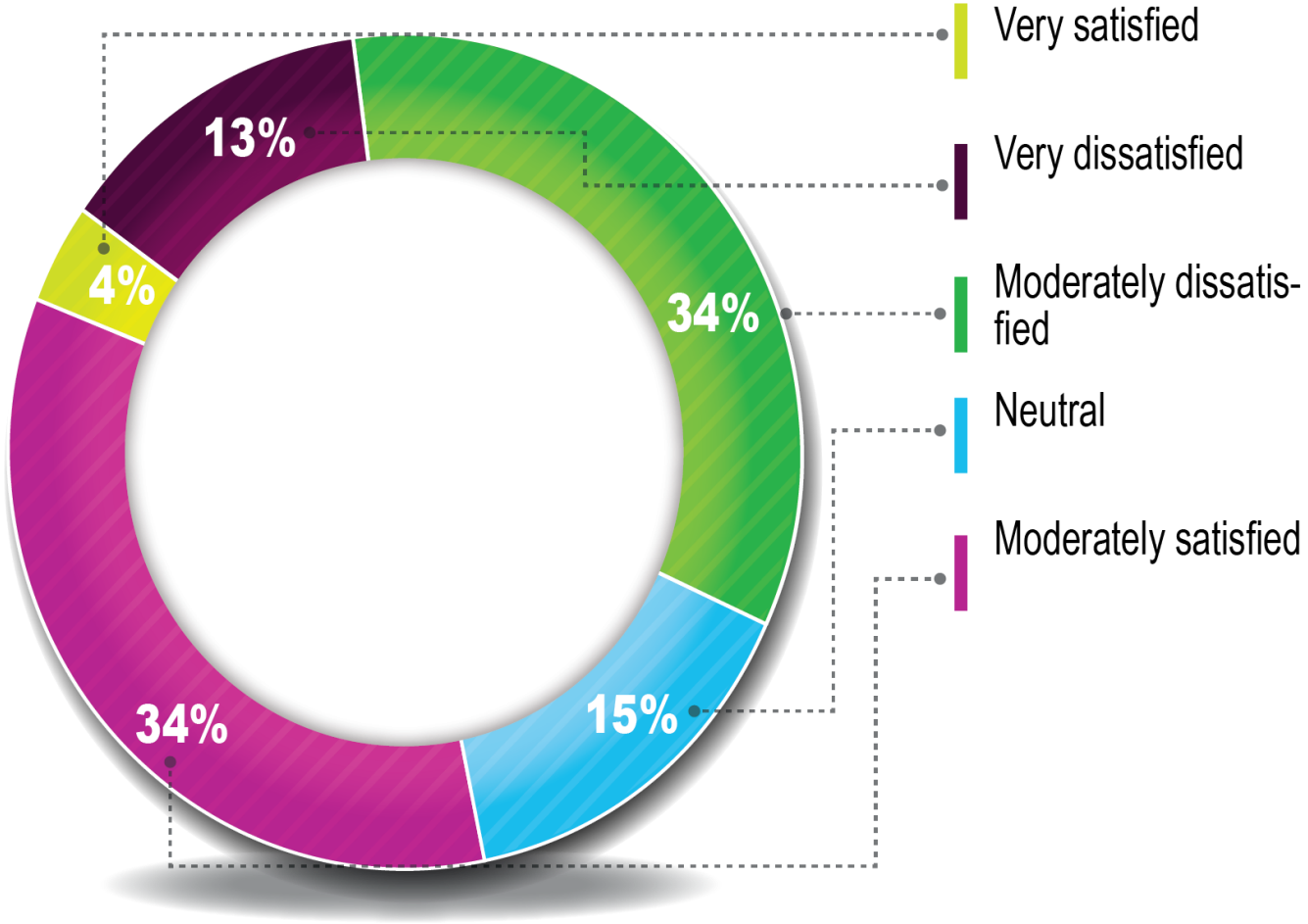
- Governor's policy agenda
- The CIO's authority
- The CIO's priorities
- Governance models
- The strategic IT plan
- State CIO business model
- Gaps: capabilities, disciplines

Service Delivery in the Next Three Years?

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

Source: The Value Equation, 2015 State CIO Survey

How satisfied are you with the current system of IT procurement in your state?



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 Leaving Performance Bonds at the Door).

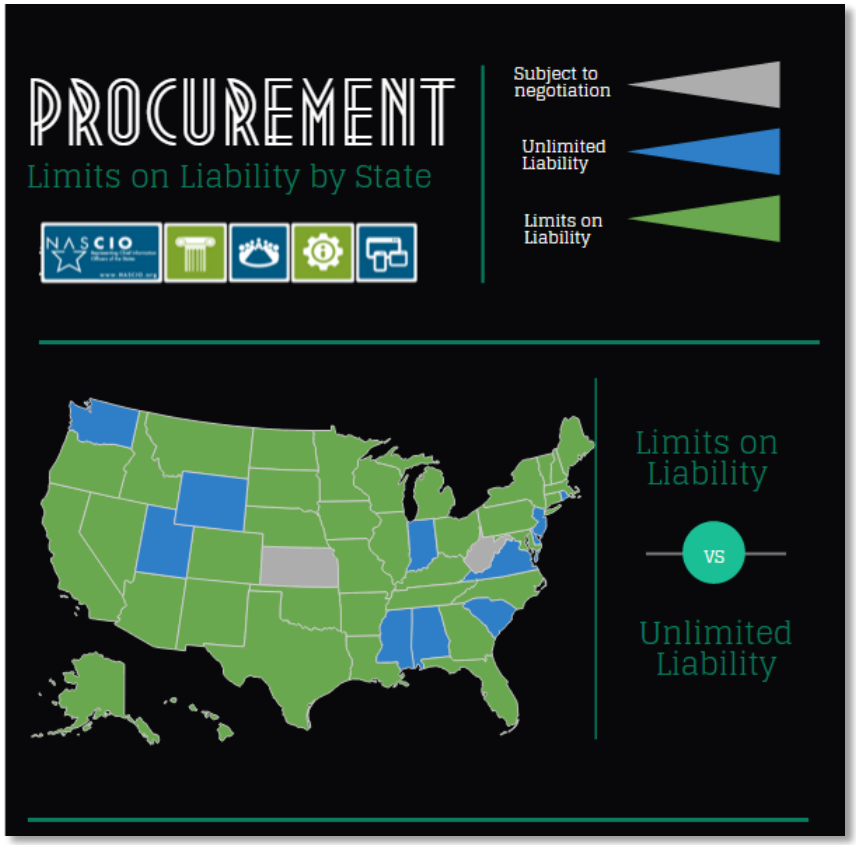
Leverage enterprise architecture for improved IT procurement
The procurement process should be adjusted to recognize and align with enterprise IT strategies, architecture and standards based acquisitions (see NASCIO publication Leveraging Enterprise Architecture for Improved IT Procurement).

Improve the Negotiations Process
Implement rules for using competitive negotiations to facilitate "give-and-take" between buyer and seller (see LJIS 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

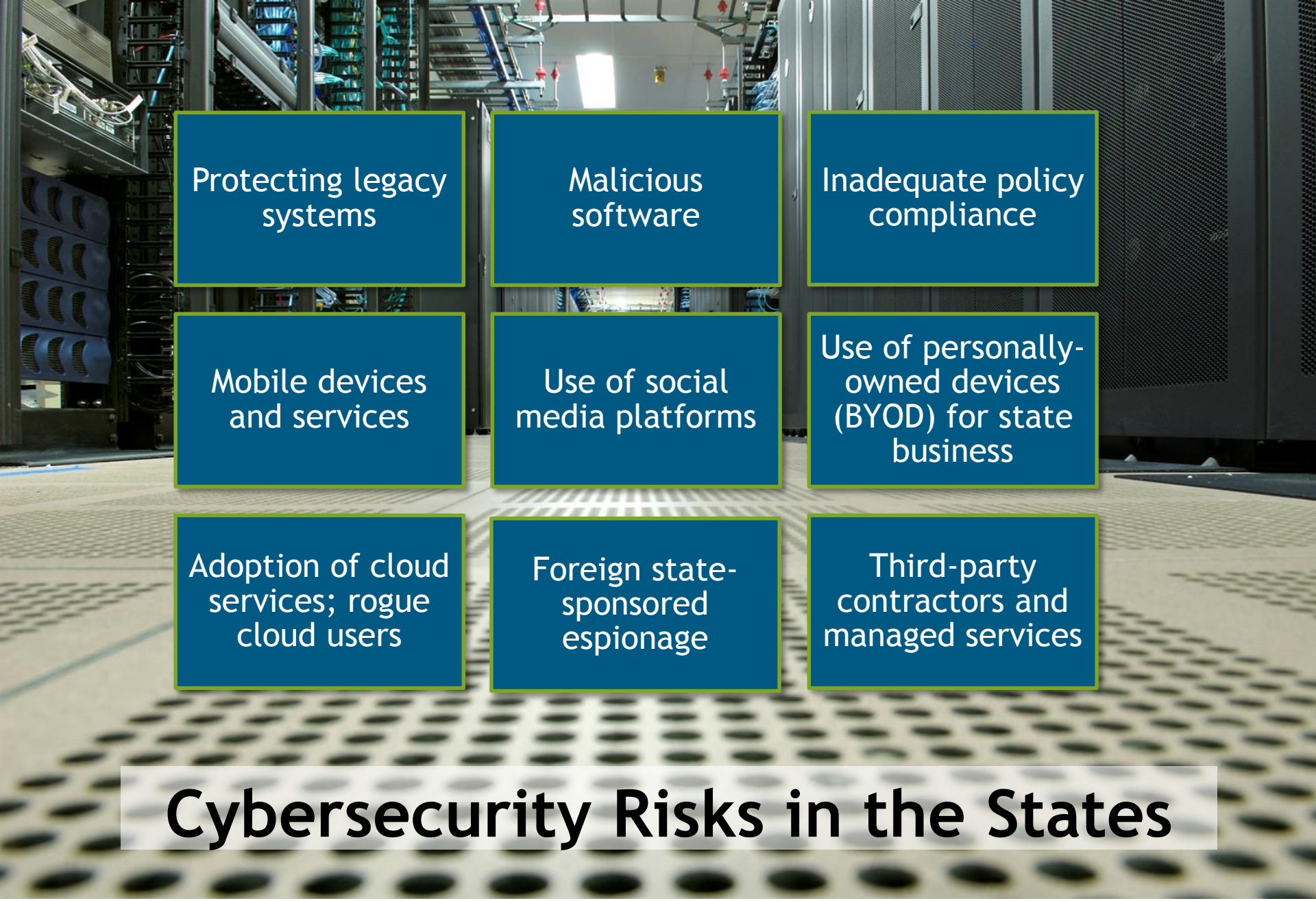
NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States.



Top Ten: State CIO Priorities for 2016

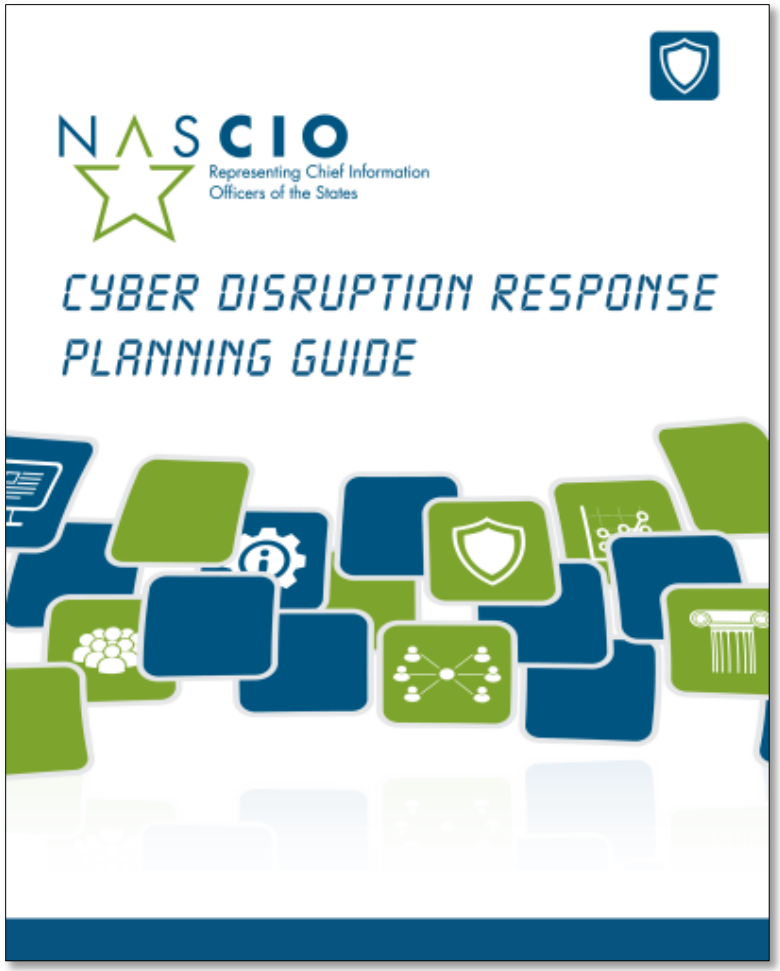
1. Security
2. Cloud Services
3. Consolidation/Optimization
4. Business Intelligence & Data Analytics
5. Legacy Modernization
6. Enterprise Vision and Roadmap for IT
7. Budget and Cost Control
8. Human Resources/Talent Management
9. Agile and Incremental Software Delivery
10. Disaster Recovery/Business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

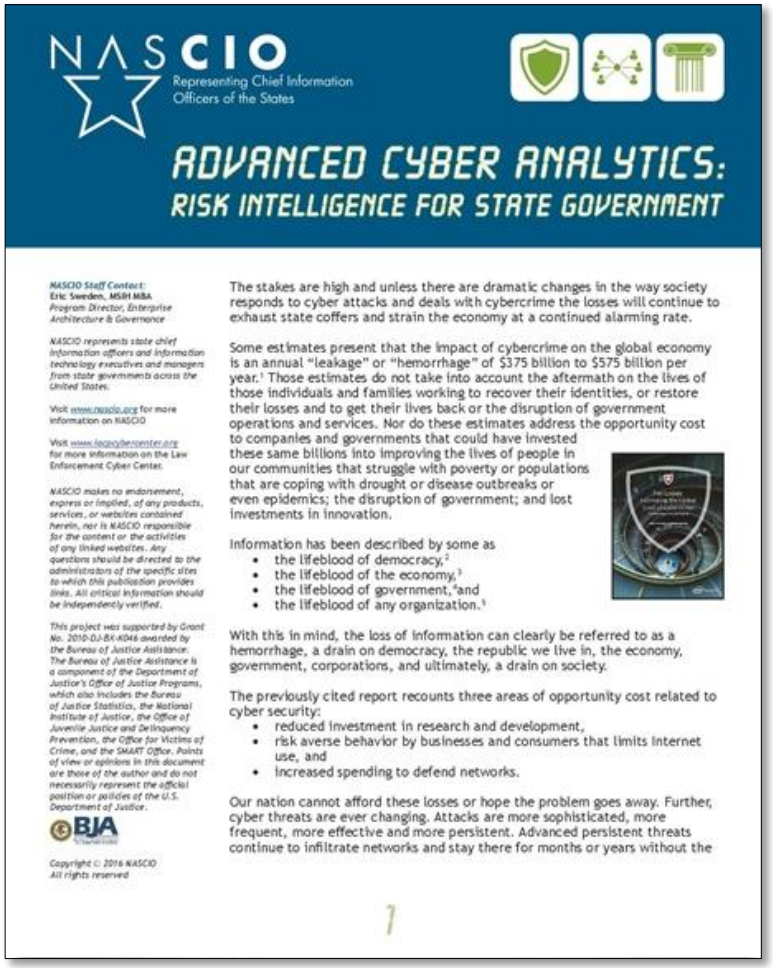
Source: NASCIO State CIO Ballot, November 2015



Cybersecurity Risks in the States

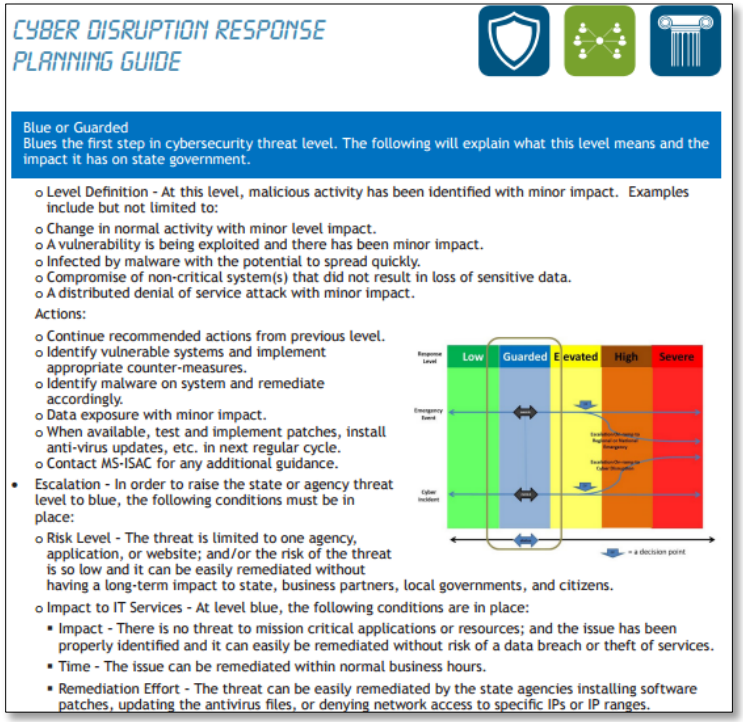
New Reports from NASCIO





Cyber Disruption Planning Guide

The ultimate outcome sought through NASCIO's Cyber Disruption Response Planning initiative is the eventual development of state government ***resiliency****.*

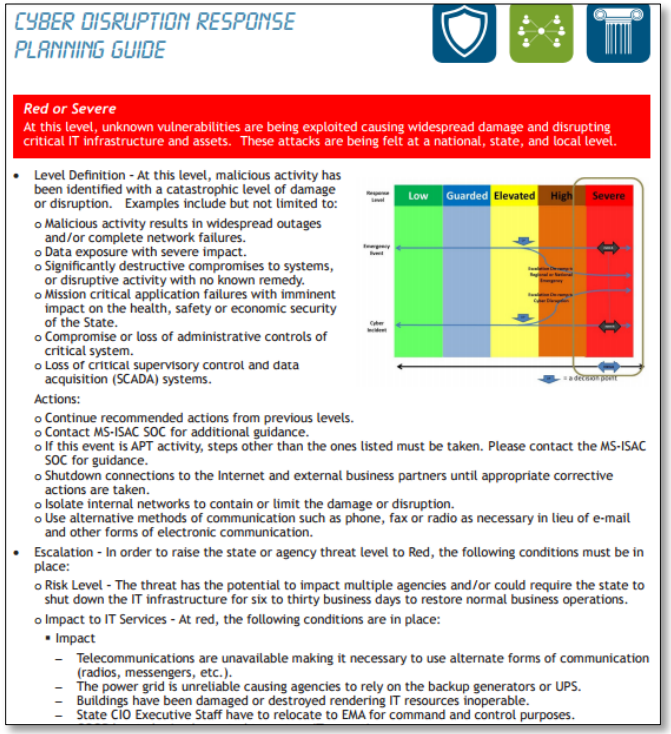


CYBER DISRUPTION RESPONSE PLANNING GUIDE

Blue or Guarded
Blues the first step in cybersecurity threat level. The following will explain what this level means and the impact it has on state government.

- Level Definition - At this level, malicious activity has been identified with minor impact. Examples include but not limited to:
  - Change in normal activity with minor level impact.
  - A vulnerability is being exploited and there has been minor impact.
  - Infected by malware with the potential to spread quickly.
  - Compromise of non-critical system(s) that did not result in loss of sensitive data.
  - A distributed denial of service attack with minor impact.

  Actions:
  - Continue recommended actions from previous level.
  - Identify vulnerable systems and implement appropriate counter-measures.
  - Identify malware on system and remediate accordingly.
  - Data exposure with minor impact.
  - When available, test and implement patches, install anti-virus updates, etc. in next regular cycle.
  - Contact MS-ISAC for any additional guidance.
- Escalation - In order to raise the state or agency threat level to blue, the following conditions must be in place:
  - Risk Level - The threat is limited to one agency, application, or website; and/or the risk of the threat is so low and it can be easily remediated without having a long-term impact to state, business partners, local governments, and citizens.
  - Impact to IT Services - At level blue, the following conditions are in place:
    - Impact - There is no threat to mission critical applications or resources; and the issue has been properly identified and it can easily be remediated without risk of a data breach or theft of services.
    - Time - The issue can be remediated within normal business hours.
    - Remediation Effort - The threat can be easily remediated by the state agencies installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges.



CYBER DISRUPTION RESPONSE PLANNING GUIDE

Red or Severe
At this level, unknown vulnerabilities are being exploited causing widespread damage and disrupting critical IT infrastructure and assets. These attacks are being felt at a national, state, and local level.

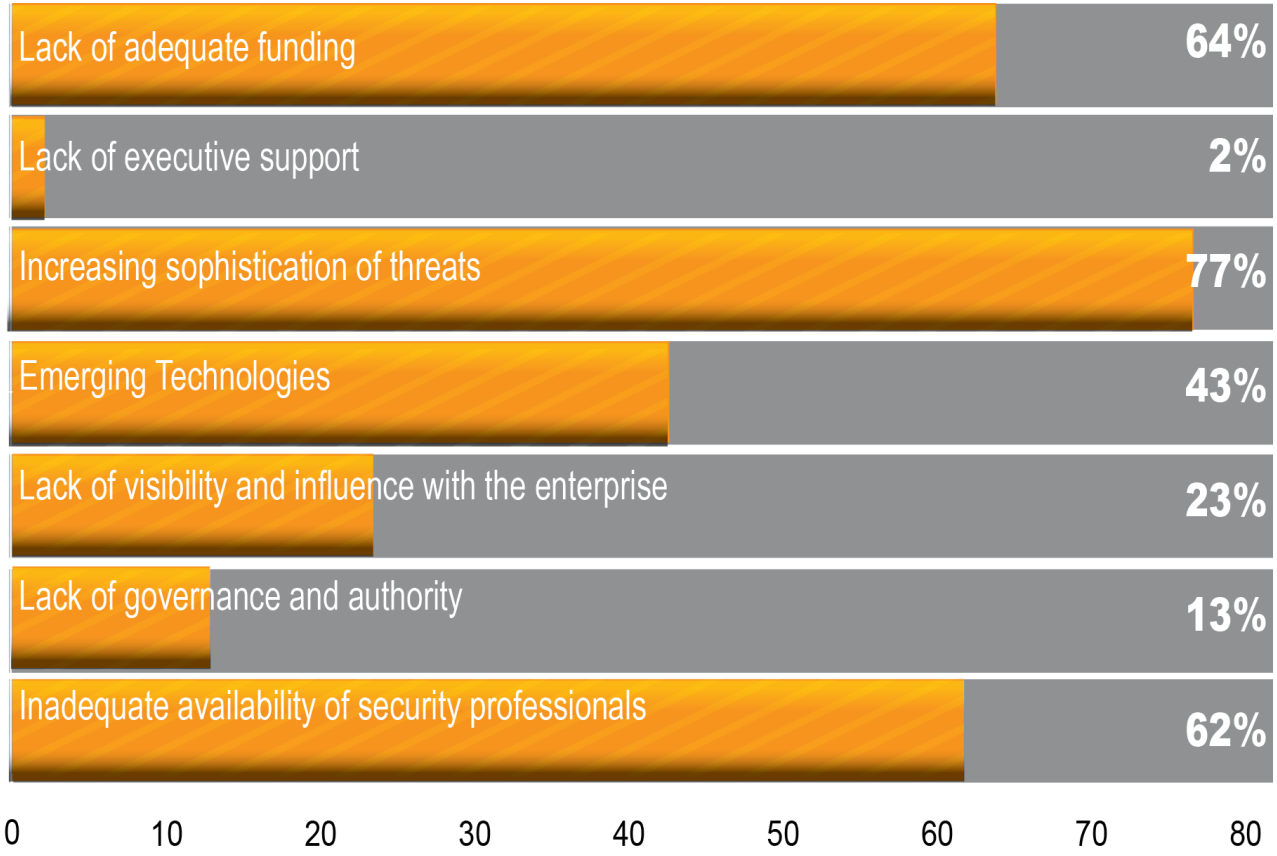
- Level Definition - At this level, malicious activity has been identified with a catastrophic level of damage or disruption. Examples include but not limited to:
  - Malicious activity results in widespread outages and/or complete network failures.
  - Data exposure with severe impact.
  - Significantly destructive compromises to systems, or disruptive activity with no known remedy.
  - Mission critical application failures with imminent impact on the health, safety or economic security of the State.
  - Compromise or loss of administrative controls of critical system.
  - Loss of critical supervisory control and data acquisition (SCADA) systems.

  Actions:
  - Continue recommended actions from previous levels.
  - Contact MS-ISAC SOC for additional guidance.
  - If this event is APT activity, steps other than the ones listed must be taken. Please contact the MS-ISAC SOC for guidance.
  - Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
  - Isolate internal networks to contain or limit the damage or disruption.
  - Use alternative methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.
- Escalation - In order to raise the state or agency threat level to Red, the following conditions must be in place:
  - Risk Level - The threat has the potential to impact multiple agencies and/or could require the state to shut down the IT infrastructure for six to thirty business days to restore normal business operations.
  - Impact to IT Services - At red, the following conditions are in place:
    - Impact
      - Telecommunications are unavailable making it necessary to use alternate forms of communication (radios, messengers, etc.).
      - The power grid is unreliable causing agencies to rely on the backup generators or UPS.
      - Buildings have been damaged or destroyed rendering IT resources inoperable.
      - State CIO Executive Staff have to relocate to EMA for command and control purposes.

NASCIO

State CIOs and Cybersecurity

What major barriers does your state face in addressing cybersecurity?



Source: The Value Equation, 2015 State CIO Survey

Key Themes from the 2014 Study

2014 Deloitte-NASCIO Cybersecurity Study

Budget-Strategy Disconnect

Funding is still the #1 barrier to effective cybersecurity

Lack of sufficient funding

Security allocation as part of IT budget remains unchanged

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

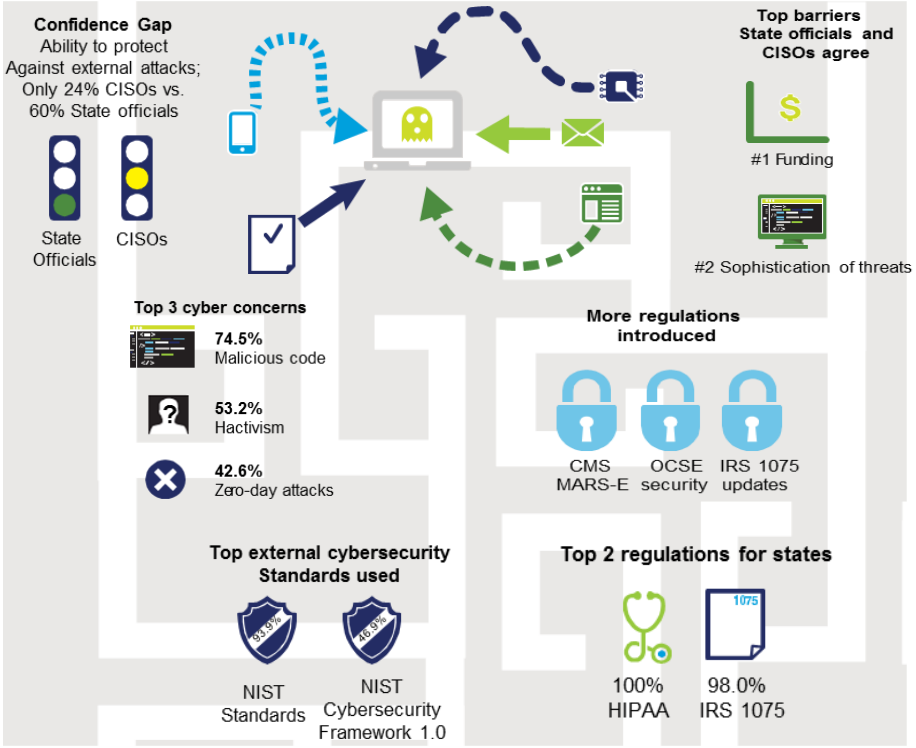
Senior Executive commitment is there, but funding still insufficient

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



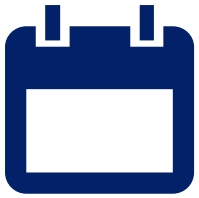
2014 Deloitte-NASCIO Cybersecurity Study

Talent Crisis

Top challenge is staffing

Salary
9 out of 10 CISOs

FTE counts are increasing



49% 6 to 15 FTEs

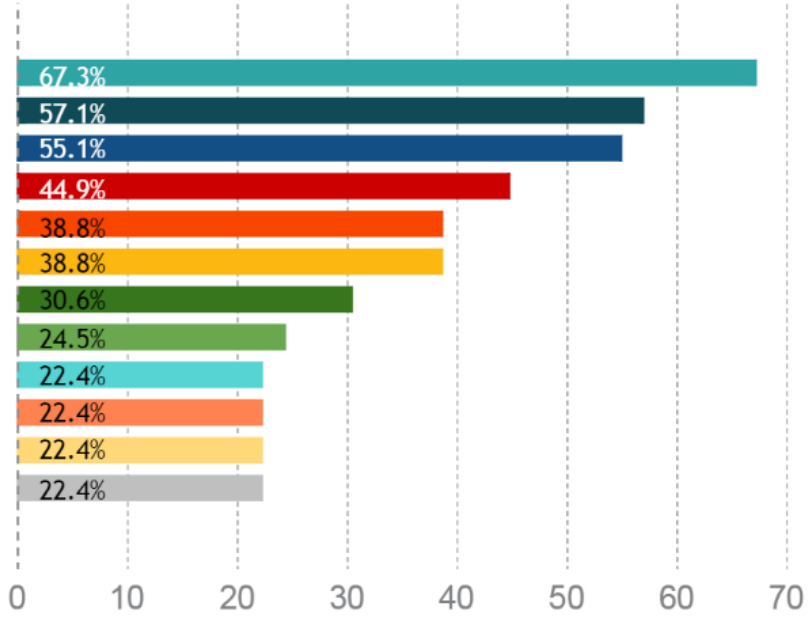
Competencies have increased, training has improved

7 out of 10
states agree

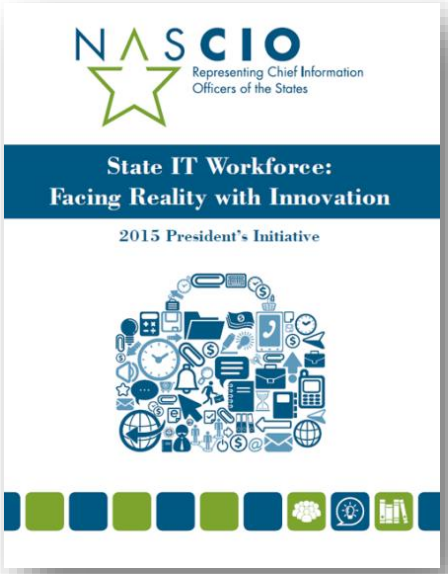
Inadequate availability of cybersecurity professionals

Barrier #3
59%

2014 Deloitte-NASCIO Cybersecurity Study



- Security
- Application Development, Programming & Support
- Architecture
- Business Intelligence/Data Analytics/Big Data
- Mainframe/Legacy Support
- Project Management
- Cloud Platforms & Services
- Networking Support
- Contract Management
- Mobile Applications & Device Management
- Analysis & Design
- Infrastructure Support



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

Sources: "Rapid7 Report: Data Breaches in the Government Sector." Rapid7. September 6, 2012.
2014 Cost of Data Breach Study, Ponemon Institute, Navigant Breach report, March 2014

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

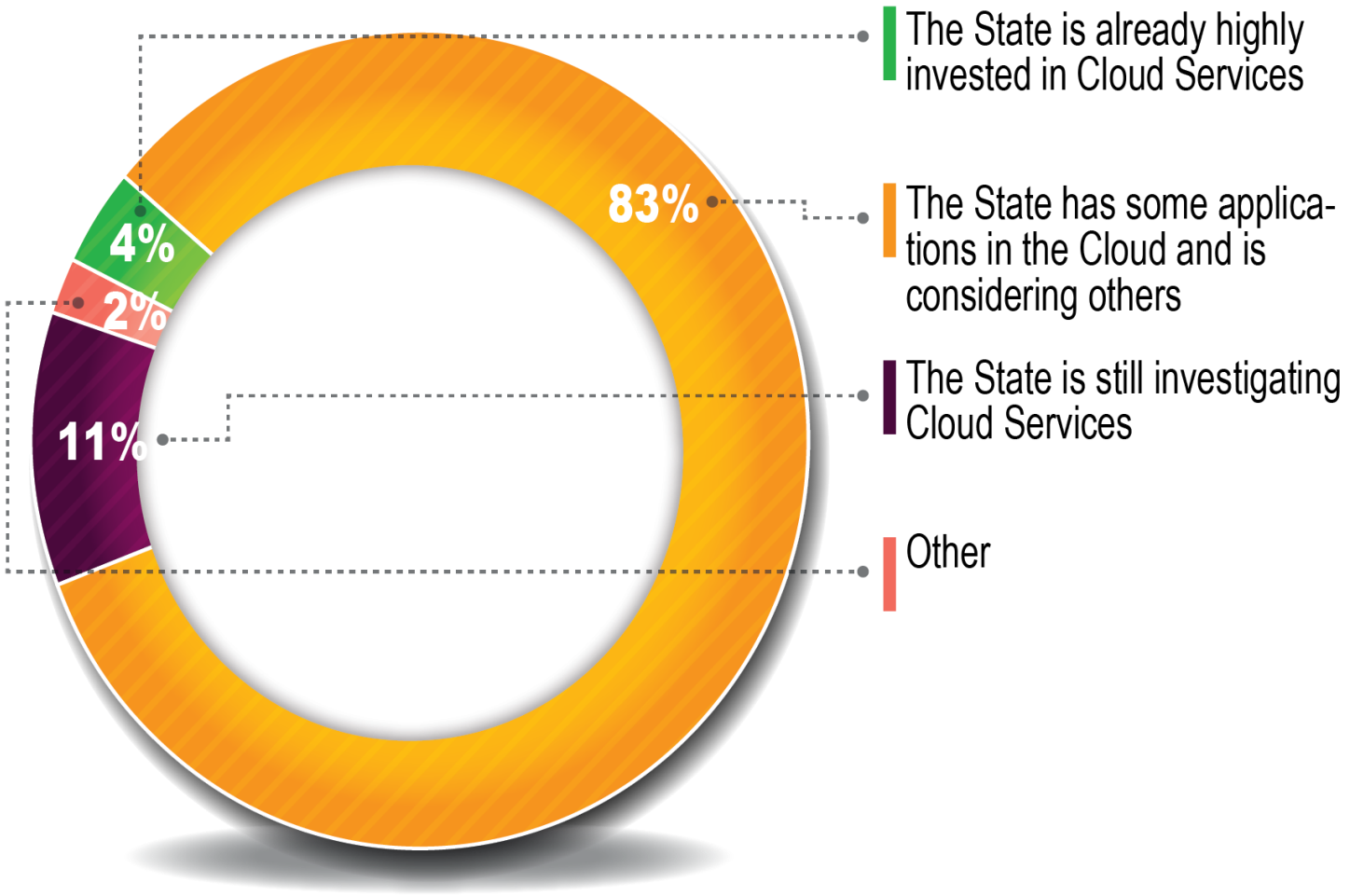
1. Service models and sourcing options
2. Adoption of cloud services
3. Power of data
4. Changing state IT workforce

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?

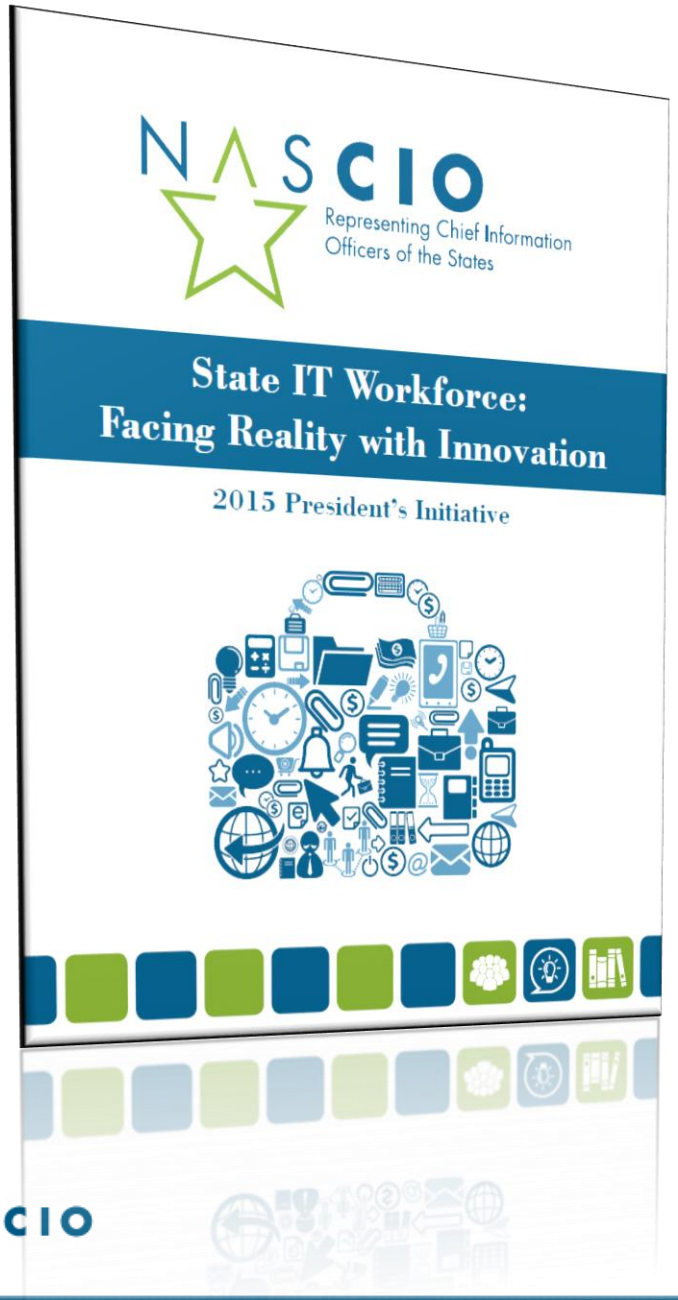


Source: The Value Equation, 2015 State CIO Survey

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