



State Governments at Risk: More than Technology



**Commonwealth of Virginia
Information Security Conference**

Richmond, Virginia
April 7, 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.





States fiscally stable; budgets to grow slowly at roughly 4% in 2016.
CIOs still seeking IT operational **cost savings**, driving consolidation

Cybersecurity threats! New risks, organizing for success, funding not commensurate with risks, talent crisis

Ongoing Transition: Changing the owner-operator business model - systems-centric *to* technology as a service

Continuing IT **workforce** retirements, skills gap, recruiting challenges, talent management. Reforms are needed

Investments in **cloud services**, mobile, data analytics

Alternative **sourcing** options, IT procurement challenges, agile approaches

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



Top Ten: Priority Technologies, Applications and Tools for 2016



1. **Security Enhancement Tools:** continuous diagnostics & mitigation (CDM), digital forensics
2. Cloud Solutions: software as a service
3. Legacy Application Modernization/Renovation
4. Data Management: master client index/master data management, information exchanges
5. Business Intelligence (BI), Business Analytics (BA): applications, big data
6. Identity and Access Management: technologies and solutions
7. Mobile Workforce: technologies and solutions
8. Virtualization: servers, desktop, storage, applications, data center
9. Networking: voice and data communications, unified
10. Document/Content/Records/E-mail Management

State Governments at Risk!

States are attractive targets – data!

More aggressive threats – organized crime, ransomware, hacktivism

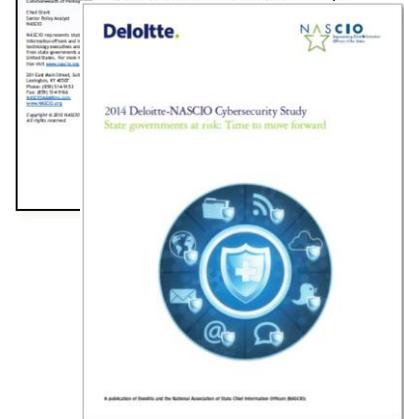
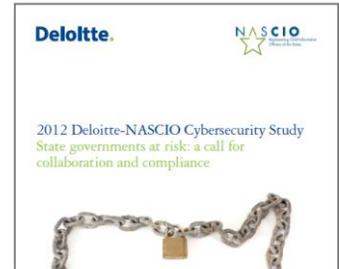
Nation state attacks

Critical infrastructure protection

Insider threats – employees, contractors

Emerging IT and data on the move

Need for continuous training, awareness



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

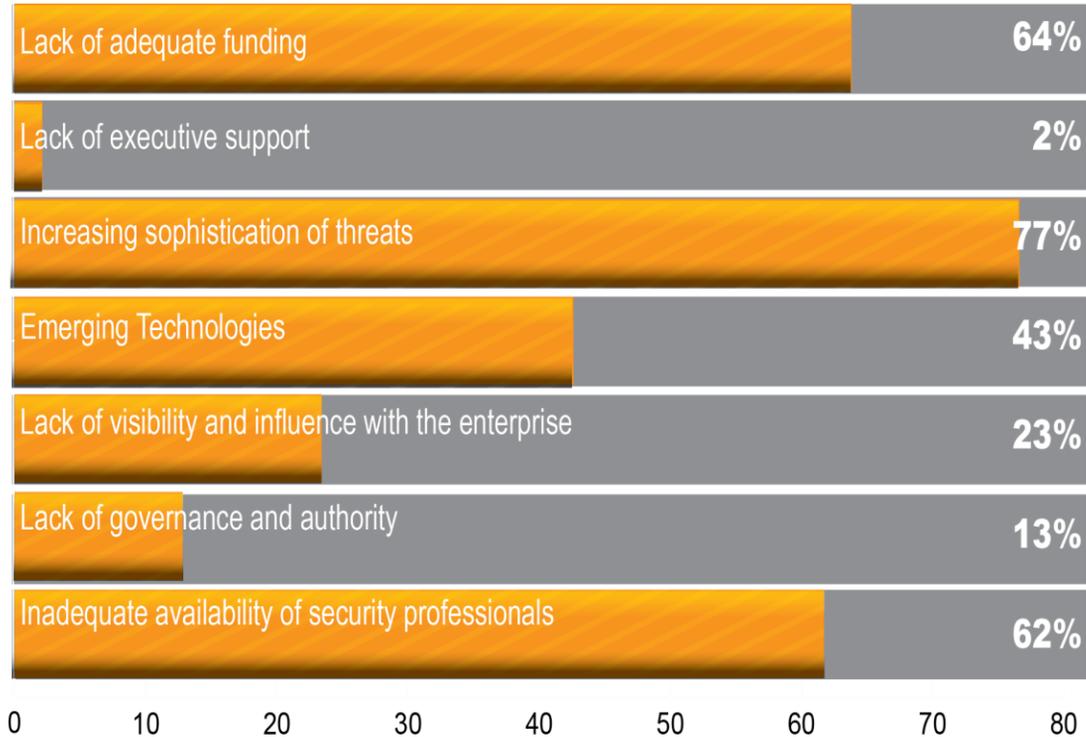
Foreign state-sponsored espionage

Third-party contractors and managed services

Cybersecurity Risks in the States

State CIOs and Cybersecurity

What major barriers does your state face in addressing cybersecurity?



State Governments at Risk: *Time to move forward*

October 2014



#StatesAtRisk

Key Themes from the 2014 Study



Maturing role of the CISO

Budget-strategy disconnect

Cyber complexity challenge

Talent crisis

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

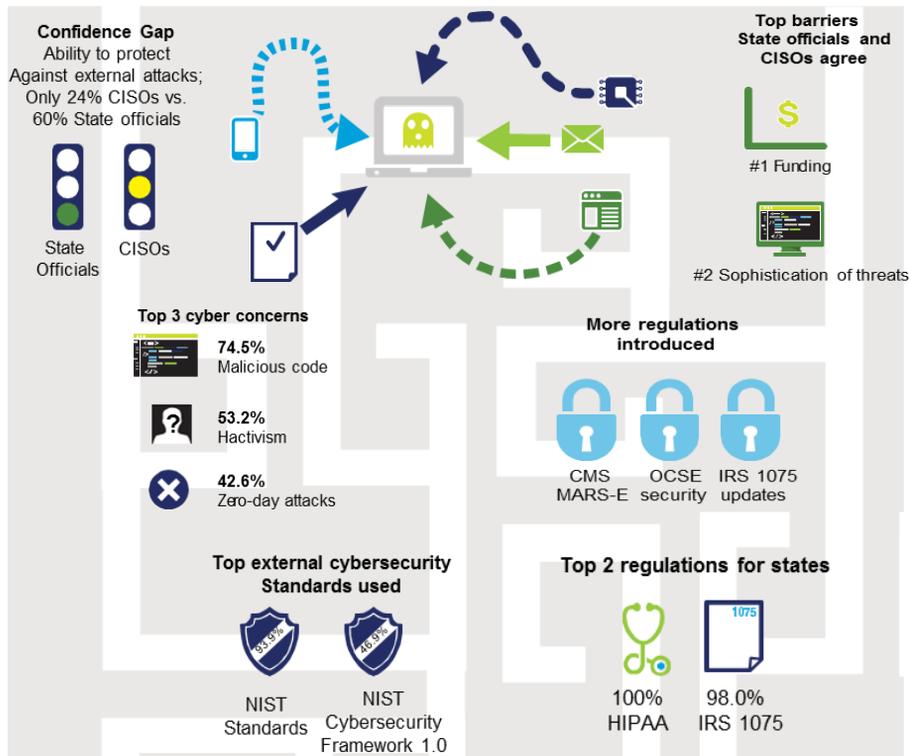
Senior Executive commitment is there, but funding still insufficient



65.3%

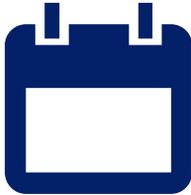
Cyber Complexity Challenge

- 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

Top challenge is staffing



Salary
9 out of 10 CISOs

Competencies have increased, training has improved

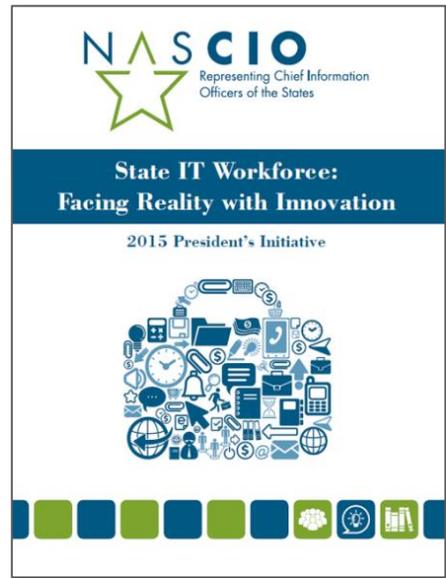
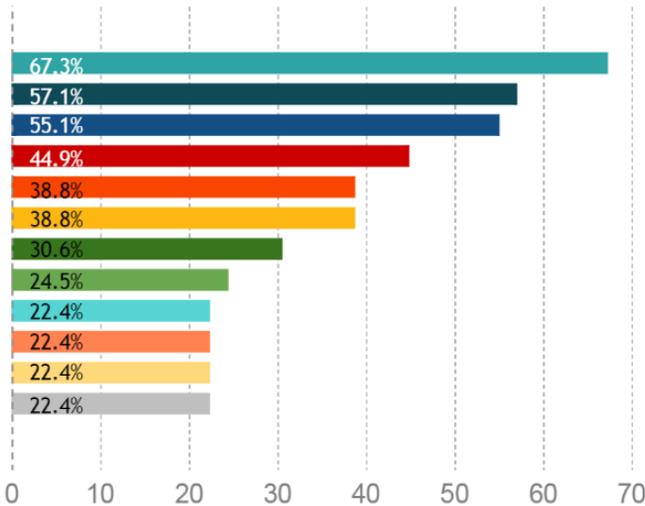


7 out of 10 states agree

Inadequate availability of cybersecurity professionals



Barrier #3
59%



What skills and disciplines present the greatest challenges in attracting and retaining IT employees?

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



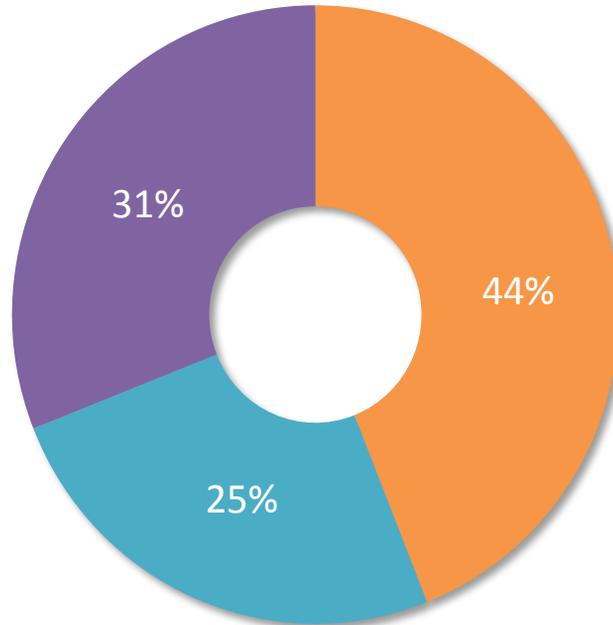
Business Risk:

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

U.S. Benchmark Data: Root Causes of a Data Breach



■ Malicious or criminal attacks

■ System Glitch

■ Human Error

Who's Responsible for Protecting State Data?

- Chief Information Officers
- Information Security Officers
- Agency Leaders
- Data Owners
- Employees
- Human Resources
- Legal Departments
- Third Party Contractors
- Elected officials



Cybersecurity involves more than *just* IT – it's a team sport.

Protecting critical assets and data is a core responsibility of the state and an investment in risk management.



A black rearview mirror is mounted on a silver metal stem. The mirror's surface is white and contains black text. The background is a light blue sky with a dark blue, textured mesh pattern at the top, likely representing the car's interior roof.

**Unfortunately state officials are often
looking at their data breach in a rear
view mirror. *After the incident...***

What Do We Know? Patterns of Success



Enterprise Leadership
and Governance



Statewide
Cybersecurity
Framework & Controls



Cybersecurity: A Team
Sport



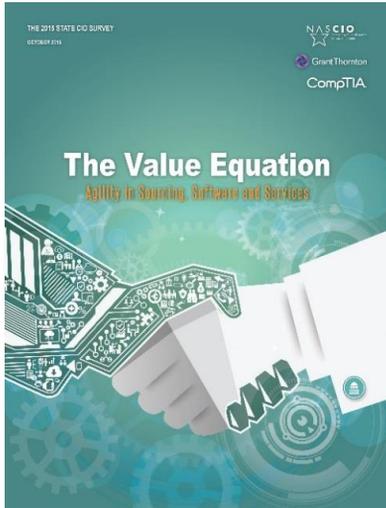
Know the Risks, Assess
the Risks, Measure



Communicating the
Risks: Training



Invest: Deploy Security
Technologies

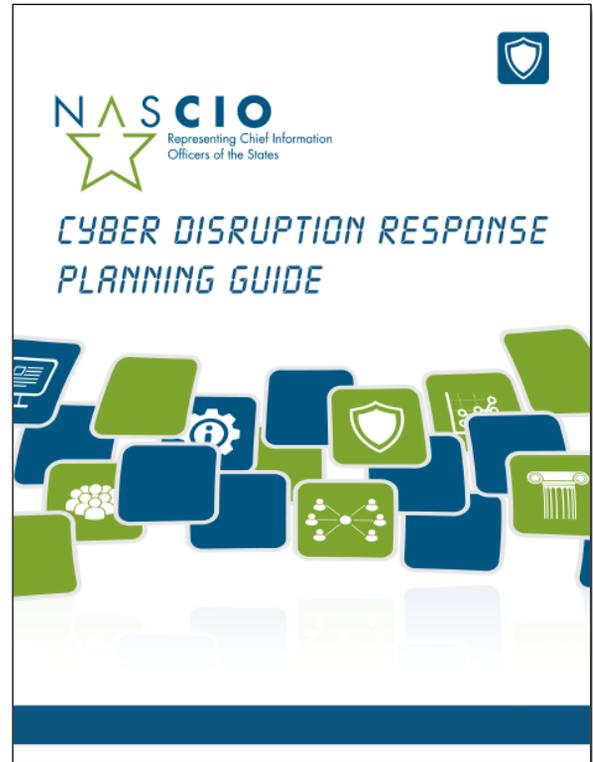


Characterize the current status of the cybersecurity program and environment in state government.

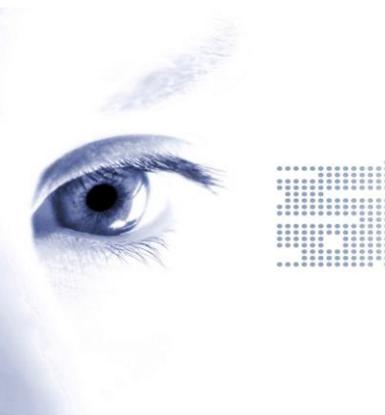
	2015	2014	2013
Adopted a cybersecurity framework based on national standards and guidelines	80%	80%	78%
Acquired and implemented continuous vulnerability monitoring capabilities	80%	78%	78%
Developed security awareness training for workers and contractors	87%	80%	78%
Established trusted partnerships for information sharing and response	80%	69%	75%
Created a culture of information security in your state government	74%	75%	73%
Adopted a cybersecurity strategic plan	74%	61%	61%
Documented the effectiveness of your cybersecurity program with metrics and testing	52%	45%	47%
Developed a cybersecurity disruption response plan	52%	51%	45%
Obtained cyber insurance	20%	n/a	n/a

Call to Action: Cyber Disruption Planning

“State governments and the critical infrastructure within the state are at risk from a cybersecurity attack that could disrupt the normal operations of government and impact citizens. “



Looking Forward...Action Needed



States must organize for success – think enterprise

Threat information sharing is essential

Focus on detection and response planning

Invest in continuous awareness and training

Collaborate on a cyber disruption plan

Talent pipeline: advocate for cybersecurity degrees

Track technologies and threats – IoT, UAS, BWC

Crisis communication...you will be breached

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?



Follow Us

 @NASCIO

 /NASCIOMedia

 /NASCIOMedia

 National Association of State
Chief Information Officers
(NASCIO)

Doug Robinson
NASCIO Executive Director

drobinson@NASCIO.org
www.nascio.org
[@nascio](https://www.linkedin.com/company/nascio)

#StatesAtRisk