Joint NASCIO-NCSL Cybersecurity Webinar
State Governments at Risk:
Turning strategy and awareness into progress

National Conference of State Legislatures
Task Force on Cybersecurity
October 21, 2016
Today’s Speakers

Assemblymember Jacqui Irwin
State of California
Co-chair, NCSL Task Force On Cybersecurity

Doug Robinson
Executive Director
National Association of State Chief Information Officers (NASCIO)

Srini Subramanian
State Government Sector Leader – Deloitte Advisory
Principal, Deloitte & Touche LLP
Agenda

- 2016 cybersecurity survey
- Study results: three key takeaways
- Strategy and governance
- Budget and funding
- Talent
- Emerging trends
Timeline of state governments at risk

2010
A call to secure citizen data and inspire trust

2012
A call for collaboration and compliance

2014
Time to move forward

2016
Turning strategy and awareness into progress

#StateofCyber
State Governments at Risk
2016 survey respondents

CISO survey profile
CISO participants answered 59 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Responses from 49 states and territories.

State official profile
96 state business and elected officials answered 15 questions, providing valuable insight into state business stakeholder perspectives. 12 associations participated
Key takeaways
Key takeaways

#1: Governor-level awareness is on the rise

To what extent are you required to provide reports on cybersecurity status or posture of the enterprise?

- Monthly: 29% (2016), 17% (2014)
- Quarterly: 2% (2016), 4% (2014)
- Annually: 12% (2016), 15% (2014)
- Ad hoc: 39% (2016), 40% (2014)

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Key takeaways

#1: Governor-level awareness is on the rise

To what extent are you required to provide reports on cybersecurity status or posture of the enterprise?

State cyber legislation: most state laws only cover data breach notification

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Key takeaways

#1: Governor-level awareness is on the rise

How confident are you in your state’s ability in managing cyber risk?

Confidence Gap

Confidence in ability to protect against external attacks:
Only 27% CISOs
vs
66% State officials

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Key takeaways

#1: Governor-level awareness is on the rise

Executive AWARENESS
Governors and state officials are paying more attention to cyber risk . . .

. . . but compared to CISOs, state officials still overestimate how well they think states can handle security threats

CISOs have an opportunity to make significant progress in educating stakeholders about the true magnitude of cyber risk to gain elusive support
Key takeaways

#2: Cybersecurity is becoming part of the fabric of government operations

Top five cybersecurity initiatives for 2016

- **39%** Training and awareness
- **37%** Monitoring/security operations centers (SOCs)
- **29%** Strategy
- **29%** Governance (e.g., roles, reporting structures, and directives)
- **29%** Operationalizing cybersecurity

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
# Key takeaways

#2: Cybersecurity is becoming part of the fabric of government operations

## Top five functions within the scope of the CISO role

<table>
<thead>
<tr>
<th>Function</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Strategy and planning</td>
<td>96%</td>
</tr>
<tr>
<td>2: Awareness and training</td>
<td>96%</td>
</tr>
<tr>
<td>3: Audit logs and security event monitoring*</td>
<td>90%</td>
</tr>
<tr>
<td>4: Incident management</td>
<td>90%</td>
</tr>
<tr>
<td>5: Vulnerability management*</td>
<td>88%</td>
</tr>
</tbody>
</table>

* indicates a change from previous years.
Key takeaways

#2: Cybersecurity is becoming part of the fabric of government operations

Operational INTEGRATION
Cybersecurity is becoming part of the fabric of government operations...

...but the largely federated model of governance makes it challenging for the CISO to exercise influence and authority across the enterprise

Effective collaboration across agencies, legislators, and federal partners is key to effective cyber risk management
Key takeaways

#3: A formal strategy can lead to more resources

Top five barriers in addressing cybersecurity challenges

1: Lack of sufficient funding
2: Inadequate availability of cybersecurity professionals
3: Lack of documented processes
4: Increasing sophistication of threats
5: Lack of visibility and influence within the enterprise
## Key takeaways

### #3: A formal strategy can lead to more resources

Intersection of approved strategy and resources

<table>
<thead>
<tr>
<th>Approved strategy (33 states)</th>
<th>More than 15 dedicated FTEs for cybersecurity</th>
<th>Staff has required competencies</th>
<th>Increase in budget</th>
<th>Cyber budget more than 2% of IT budget</th>
<th>Alignment of cyber and business programs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11 (33%)</td>
<td>16 (48%)</td>
<td>16 (48%)</td>
<td>10 (30%)</td>
<td>12 (36%)</td>
</tr>
<tr>
<td>No approved strategy (16 states)</td>
<td>1 (6%)</td>
<td>3 (19%)</td>
<td>5 (31%)</td>
<td>0 (0%)</td>
<td>2 (12%)</td>
</tr>
</tbody>
</table>

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
# Key takeaways

### #3: A formal strategy can lead to more resources

**Formal STRATEGY**
The top challenges of lack of funding and finding talent for cybersecurity continue at the same intensity . . .

. . . but CISOs with a formal, approved cybersecurity strategy are more likely to secure funding and talent.

CISOs should formalize their cybersecurity strategy and communicate its urgency to the stakeholders who need to approve it.
Strategy and governance
Strategy and governance

State’s progress in maintaining cybersecurity strategy

<table>
<thead>
<tr>
<th>Category</th>
<th>2016</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documented and approved</td>
<td>67%</td>
<td>55%</td>
</tr>
<tr>
<td>Documented but not approved</td>
<td>14%</td>
<td>8%</td>
</tr>
<tr>
<td>Intend to have one documented and approved within the next 12 months</td>
<td>18%</td>
<td>37%</td>
</tr>
</tbody>
</table>
Strategy and governance

Senior executive support (governor’s office, agency secretary, or CIO) for security projects to effectively address regulatory or legal requirements

- Commitment and adequate funding:
  - 2016: 24%
  - 2014: 27%
- Commitment but inadequate funding:
  - 2016: 69%
  - 2014: 65%
Strategy and governance

Collaboration trends as part of the states’ cybersecurity program

- Multi-State Information-Sharing and Analysis Center*: 96%
- Federal Department of Homeland Security/fusion centers*: 92%
- Local government entities: 92%
- State colleges and universities: 88%
- National Guard/State Guard*: 84%

*New in 2016

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Strategy and governance

CISOs’ confidence levels in cybersecurity practice followed by third parties (contractors, service providers, business partners)

- Not very confident: 22% in 2016, 6% in 2014
- Somewhat confident: 65% in 2016, 81% in 2014

#StateofCyber
Budget & funding
Budget remains top challenge

Percentage of state’s cybersecurity allocation as part of overall IT budget

- 0%: 6% (2016), 9% (2014)
- 0-1%: 0% (2016), 18% (2014)
- 1-2%: 27% (2016), 47% (2014)
- 3-5%: 20% (2016), 11% (2014)
Budget remains top challenge

Year-over-year trending of the state cybersecurity budget 2014-2016

- Increased >10%: 2016 - 23%, 2014 - 17%
- Increased 6%-10%: 2016 - 8%, 2014 - 4%
- Increased 1%-5%: 2016 - 17%, 2014 - 23%
- Budget remained the same: 2016 - 33%, 2014 - 31%
- Reduced 1%-5%: 2016 - 0%, 2014 - 10%
- Reduced 6%-10%: 2016 - 0%, 2014 - 2%
- Reduced >10%: 2016 - 4%, 2014 - 4%

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Budget remains top challenge

Additional funding sources for cybersecurity initiatives

- Inter-agency collaboration*
- Federal Dept. of Homeland Security (DHS)
- Business or program stakeholders
- HHS/CMS/ACA-related funding
- State Office of Homeland Security*
- Other state funding from legislature and grants
- Other federal funding and grants
- State emergency mgmt.

*New in 2016
Talent
Talent crisis continues

Top three human resources factors that negatively impact the CISO’s ability to develop, support, and maintain cybersecurity workforce

- State's salary rates and pay grade structures: 96%
- Lack of qualified candidates due to demand from federal agencies and private sector: 59%
- Workforce leaving for private sector: 47%

*New in 2016

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Talent crisis continues

Top three factors that CISOs employ to attract and retain cybersecurity talent

- Job stability: 53%
- Opportunity to serve and contribute to your state*: 49%
- Challenging work environment: 41%

#StateofCyber

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Talent crisis continues

State internal cybersecurity professional competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements

- 40% Staff has the required competencies
- 56% Staff has gaps in competencies
- 2% Not applicable/Don’t know
- 2% Other

#StateofCyber Source: The 2016 Deloitte-NASCIO Cybersecurity Study
## Talent crisis continues

### What innovative/out-of-the-box strategies and tactics has your state used in attracting and retaining a highly qualified IT workforce?

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promoting non-salary benefits like greater stability and diversity of experience</td>
<td>75%</td>
</tr>
<tr>
<td>Call to public service</td>
<td>64%</td>
</tr>
<tr>
<td>Public/private internships</td>
<td>39%</td>
</tr>
<tr>
<td>Sponsoring community awareness events (i.e. hackathons, robot build events, speaking at STEM schools)</td>
<td>35%</td>
</tr>
<tr>
<td>Building &quot;talent networks&quot;</td>
<td>31%</td>
</tr>
<tr>
<td>Emphasizing location (i.e. working in state capital)</td>
<td>29%</td>
</tr>
</tbody>
</table>

### What single personnel reform could be implemented that would be the most impactful in reforming your state IT workforce?

- **Streamlining the hiring process and reducing time to hire**: 7%
- **Removing IT positions from the civil service system**: 15%
- **Modernizing the IT job titles and classifications**: 30%
- **Eliminating state unions representing IT**: 13%
- **Implementing phased retirement options**: 2%
- **Modernizing office culture [i.e. flexible work schedules, telecommuting, etc.]**: 20%
- **Other**: 13%

Source: 2016 NASCIO State CIO Survey
Emerging trends
## Emerging trends

### Top cyber threats across state government

<table>
<thead>
<tr>
<th>Threat</th>
<th>Somewhat higher threat</th>
<th>Very high threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing, pharming, and other related variants</td>
<td>35%</td>
<td>47%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>31%</td>
<td>42%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>43%</td>
<td>29%</td>
</tr>
<tr>
<td>Increasing sophistication and proliferation of threats (e.g., viruses, worms, and malware)</td>
<td>51%</td>
<td>14%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities from unsecured code</td>
<td>45%</td>
<td>8%</td>
</tr>
</tbody>
</table>
Emerging trends

CISOs’ confidence levels in protecting their state’s information assets cyber threats

- Threats originating internally: 4% Not confident at all, 35% Not very confident, 47% Somewhat confident, 10% Very confident, 2% Extremely confident, 2% N/A/Don't know
- Threats originating externally: 14% Not confident at all, 57% Not very confident, 27% Somewhat confident, 2% Very confident, 2% Extremely confident
- Threats originating from business partners/vendors (third-party risk): 4% Not confident at all, 31% Not very confident, 57% Somewhat confident, 6% Very confident, 2% Extremely confident
- Threats originating from applications: 2% Not confident at all, 29% Not very confident, 56% Somewhat confident, 11% Very confident, 2% Extremely confident
- Threats originating from use of emerging technologies (like cloud and Internet of Things): 6% Not confident at all, 53% Not very confident, 37% Somewhat confident, 2% Very confident, 2% Extremely confident

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
# Emerging trends

## Provisions of states’ cyber legislation/statutes

<table>
<thead>
<tr>
<th>Provision</th>
<th>Established and funded</th>
<th>Established and not funded</th>
<th>In progress</th>
<th>Not in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity incident/data breach reporting and handling</td>
<td>43%</td>
<td>21%</td>
<td>4%</td>
<td>32%</td>
</tr>
<tr>
<td>Data breach notification</td>
<td>41%</td>
<td>35%</td>
<td>2%</td>
<td>23%</td>
</tr>
<tr>
<td>Role and authority of the enterprise CISO or equivalent</td>
<td>40%</td>
<td>4%</td>
<td>2%</td>
<td>54%</td>
</tr>
<tr>
<td>Continuity of government/continuity of operations</td>
<td>35%</td>
<td>13%</td>
<td>4%</td>
<td>48%</td>
</tr>
<tr>
<td>Cybersecurity awareness</td>
<td>31%</td>
<td>4%</td>
<td>2%</td>
<td>63%</td>
</tr>
<tr>
<td>Data privacy provisions: authority and purpose; collection, storage, use, and sharing limitations</td>
<td>27%</td>
<td>21%</td>
<td>2%</td>
<td>50%</td>
</tr>
<tr>
<td>State-level cybersecurity program and framework for enterprise risk management</td>
<td>27%</td>
<td>17%</td>
<td>8%</td>
<td>48%</td>
</tr>
<tr>
<td>Cybersecurity budget allocation and review</td>
<td>26%</td>
<td>0%</td>
<td>4%</td>
<td>70%</td>
</tr>
<tr>
<td>Cyber threat information-sharing program between state agencies, law enforcement, and private entities</td>
<td>21%</td>
<td>10%</td>
<td>6%</td>
<td>63%</td>
</tr>
</tbody>
</table>

Source: The 2016 Deloitte-NASCIO Cybersecurity Study
Moving forward

Executive AWARENESS
Governors and state officials are paying more attention to cyber risk . . .
. . . but compared to CISOs, state officials still overestimate how well they think states can handle security threats.
CISOs have an opportunity to make significant progress in educating stakeholders about the true magnitude of cyber risk to gain elusive support.

Operational INTEGRATION
Cybersecurity is becoming part of the fabric of government operations . . .
. . . but the largely federated model of governance makes it challenging for the CISO to exercise influence and authority across the enterprise.
Effective collaboration across agencies, legislators, and federal partners is key to effective cyber risk management.

Formal STRATEGY
The top challenges of lack of funding and finding talent for cybersecurity continue at the same intensity . . .
. . . but CISOs with a formal, approved cybersecurity strategy are more likely to secure funding and talent.
CISOs should formalize their cybersecurity strategy and communicate its urgency to the stakeholders who need to approve it.

#StateofCyber
State Governments at Risk:
Turning strategy and awareness into progress

Available for download at www.nascio.org/stateofcyber
Video from 2016 NASCIO Annual Conference session available at https://youtu.be/9DXoATWFbE4

Contacts:
Doug Robinson – drobinson@NASCIO.org
Srini Subramanian - ssubramanian@deloitte.com
About NASCIO
The National Association of State Chief Information Officers is the premier network and resource for state CIOs and a leading advocate for technology policy at all levels of government. NASCIO represents state chief information officers and information technology executives from the states, territories, and the District of Columbia. For more information about NASCIO visit [www.nascio.org](http://www.nascio.org).

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this presentation contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken “as is” and was not validated or confirmed by Deloitte.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte