States at Risk: Bold Plays for Change

NCSL Task Force on Cybersecurity
January 18, 2019

Doug Robinson, NASCIO Executive Director
@NASCIO
STATE CIO TOP 10 PRIORITIES
2019 Strategies, Management & Process Solutions

1. Security and Risk Management
2. Cloud Services
3. Consolidation/Optimization
4. Digital Government
5. Broadband/Wireless Connectivity
6. Budget, Cost Control, Fiscal Management
7. Customer Relationship Management
8. Data Management and Analytics
9. Enterprise IT Governance
10. Identity and Access Management

Source: NASCIO State CIO Ballot, November 2018
Timeline of the Deloitte - NASCIO Cybersecurity Study

States 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

2018

Bold plays for change
Ransomware, social engineering, and phishing are the top cyber threats for states

Please choose the prevalence of the following cyber threats in your state for the next year. (49 respondents)

<table>
<thead>
<tr>
<th>Threat Level</th>
<th>2018</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Threat</td>
<td>35%</td>
<td>32%</td>
</tr>
<tr>
<td>Somewhat Higher</td>
<td>43%</td>
<td>41%</td>
</tr>
<tr>
<td>Very High</td>
<td>16%</td>
<td>27%</td>
</tr>
</tbody>
</table>

Source: 2018 Deloitte-NASCIO Cybersecurity Study
**Web applications and malicious code are the leading sources of security breaches**

In terms of security breaches over the past 12 months, which of the following applies to your state?

<table>
<thead>
<tr>
<th>Source</th>
<th>Respondents</th>
<th>Web applications</th>
<th>Malicious code (e.g., viruses/worms/spyware/malware/ransomware)</th>
<th>My state has not been breached</th>
<th>Electronic attack (e.g., hacker)</th>
<th>Physical attack (e.g., stolen computer systems)</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>30</td>
<td>24</td>
<td>17</td>
<td>8</td>
<td>15</td>
<td>6</td>
</tr>
<tr>
<td>Internal</td>
<td>2</td>
<td>2</td>
<td>8</td>
<td>6</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Business partner/vendor</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: 2018 Deloitte-NASCIO Cybersecurity Study
Cybersecurity Maturity in the States is Improving...

<table>
<thead>
<tr>
<th>Characterize the current status of the cybersecurity program and environment in state government.</th>
<th>2013</th>
<th>2015</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developed security awareness training for workers and contractors</td>
<td>78%</td>
<td>87%</td>
<td>88%</td>
<td>98%</td>
</tr>
<tr>
<td>Adopted a cybersecurity framework based on national standards and guidelines</td>
<td>78%</td>
<td>80%</td>
<td>95%</td>
<td>94%</td>
</tr>
<tr>
<td>Established trusted partnerships for information sharing and response</td>
<td>75%</td>
<td>80%</td>
<td>83%</td>
<td>92%</td>
</tr>
<tr>
<td>Adopted a cybersecurity strategic plan</td>
<td>61%</td>
<td>74%</td>
<td>83%</td>
<td>85%</td>
</tr>
<tr>
<td>Acquired and implemented continuous vulnerability monitoring capabilities</td>
<td>78%</td>
<td>80%</td>
<td>79%</td>
<td>81%</td>
</tr>
<tr>
<td>Created a culture of information security in your state government</td>
<td>73%</td>
<td>74%</td>
<td>83%</td>
<td>79%</td>
</tr>
<tr>
<td>Developed a cybersecurity disruption response plan</td>
<td>45%</td>
<td>52%</td>
<td>69%</td>
<td>69%</td>
</tr>
<tr>
<td>Documented the effectiveness of your cybersecurity program with metrics and testing</td>
<td>47%</td>
<td>52%</td>
<td>57%</td>
<td>63%</td>
</tr>
<tr>
<td>Using analytical tools, AI, machine learning, etc. to manage cybersecurity programs</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>44%</td>
</tr>
<tr>
<td>Obtained cyber insurance</td>
<td>n/a</td>
<td>20%</td>
<td>38%</td>
<td>42%</td>
</tr>
</tbody>
</table>

Source: NASCIO 2018 State CIO Survey

Risk based strategies are being adopted

Expanded focus from operational to strategic

Expect continued progress in 2019
CISOs have established a frequent reporting cadence to state leadership

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

- **Governor** (49 respondents)
  - Never: 18% (2016), 10% (2018)
  - Monthly: 29% (2016), 20% (2018)
  - Quarterly: 12% (2016), 10% (2018)
  - Annually: 29% (2016), 18% (2018)
  - Other: 0% (2016), 2% (2018)

- **State legislature** (49 respondents)
  - Monthly: 4% (2016), 4% (2018)
  - Quarterly: 6% (2016), 14% (2018)
  - Annually: 29% (2016), 35% (2018)
  - Ad hoc: 35% (2016), 35% (2018)
  - Other: 0% (2016), 2% (2018)

- **Secretary/deputy secretary** (46 respondents)
  - Never: 17% (2016), 15% (2018)
  - Monthly: 25% (2016), 4% (2018)
  - Quarterly: 10% (2016), 4% (2018)
  - Annually: 33% (2016), 9% (2018)
  - Ad hoc: 35% (2016), 10% (2018)
  - Other: 10% (2016), 13% (2018)
However persistent challenges remain...

Budget, talent, and threats top three since 2010

Survey question: Identify the top barriers that your state faces in addressing cybersecurity challenges.

Source: 2018 Deloitte-NASCIO Cybersecurity Study
### Budget and Staffing Remain Top Barriers to Effective Cybersecurity

**State CIOs say...**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of sufficient resources</td>
<td>82%</td>
</tr>
<tr>
<td>Inadequate cybersecurity</td>
<td>71%</td>
</tr>
<tr>
<td>Staffing</td>
<td>47%</td>
</tr>
<tr>
<td>Cloud Services</td>
<td>43%</td>
</tr>
<tr>
<td>Security Policies</td>
<td>31%</td>
</tr>
<tr>
<td>Access Management</td>
<td>31%</td>
</tr>
</tbody>
</table>

**State CISOs say...**

- **52%** Lack of sufficient cybersecurity budget
- **50%** Inadequate cybersecurity staffing
- **48%** Increasing sophistication of threats

*Source: NASCIO*
Survey question: What percent of your state’s enterprise IT budget is allocated to enterprise cybersecurity? (all executive branch agencies)

Budget Challenge
Most states only spend 0-3% of their IT budget on cybersecurity

- 0%: 6% (2016), N/A or do not know: 18% (2018), Other: 6% (2018)
- 0-1%: 12% (2018), 12% (2016), 18% (2018)
- 1-2%: 27% (2018), 30% (2016)
- 2-3%: 12% (2018), New in 2018: 0% (2016)
- 3-5%: 12% (2018)
- 6-10%: 10% (2018), New in 2018: 0% (2016)
- N/A or do not know: 18% (2018), 25% (2016)

Budget Challenge

Almost half the states do not have a separate budget line item for cybersecurity.
Survey question: Characterize the year-over-year trending in your state's cybersecurity budget for years 2016 and 2017. (49 respondents)

Source: 2018 Deloitte-NASCIO Cybersecurity Study
Talent Crisis
Thirty state CISOs acknowledge they face a cyber competency gap

Survey question: Do your internal cybersecurity professionals have the required competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements? (49 respondents)

Source: 2018 Deloitte-NASCIO Cybersecurity Study
Talent crisis

Top barriers to hiring, developing and retaining cyber talent

94% State’s salary rates and paygrade structures
51% Workforce leaving for private sector careers
47% Lack of qualified candidates due to demand from federal agencies and private sector
24% Work location—lack of qualified cyber workforce in the state capital
18% Outdated classifications and job descriptions for cybersecurity positions
12% Lack of a defined career path and opportunities in cybersecurity
12% Lengthy hiring process

Survey question: What are the top three human resource factors that negatively impact your ability to develop, support, and maintain the cybersecurity workforce within your state? (49 respondents)

Source: 2018 Deloitte-NASCIO Cybersecurity Study
Three Bold Plays for Change

1. Advocate for Dedicated Cyber Program Funding
   CISOs should raise cybersecurity’s visibility with the state legislature and executive branch by making it a line item in the IT budget. They can also seek funding from federal agencies to support compliance with those agencies’ security mandates.

2. CISOs as an Enabler of Innovation, Not a Barrier
   CISOs should actively participate in shaping the state’s innovation agenda, collaborate with state digital and innovation officers, and lead the charge to help program leaders securely adopt new technologies.

3. Team with the Private Sector and Higher Education
   CISOs should leverage public-private partnerships and collaborations with local colleges and universities to provide a pipeline of new talent, as well as consider outsourcing to private-sector firms.