Highlights from the 2018 Deloitte-NASCIO Cyber Study

November 13, 2018
Speakers

Debbi Blyth
CISO, State of Colorado

Srini Subramanian
Principal, Deloitte Risk & Financial Advisory, Deloitte & Touche LLP

Doug Robinson
Executive Director, NASCIO
States at Risk
Chief Information Security Officer (CISO) Survey Profile

• US state enterprise-level CISOs, with additional input from agency CISOs and security staff members within state governments.

• CISO participants answered 56 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs.

• Survey responses were received from all the 50 states.
Agenda

• Overview - CISOs have an executive platform
• Persistent challenges remain
• **Bold Plays** - States need bold actions to accelerate change
• Detailed data chart samples
CISOs have an executive leadership platform

CISO role is firmly established, increasingly through legislation

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>2018</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority established by statute or law</td>
<td>63%</td>
<td>49%</td>
</tr>
<tr>
<td>Authority established by secretary or CIO</td>
<td>53%</td>
<td>61%</td>
</tr>
<tr>
<td>Authority established by administrative rule, regulation, or procedure</td>
<td>29%</td>
<td>22%</td>
</tr>
<tr>
<td>Authority established by an executive (governor’s) order</td>
<td>29%</td>
<td>22%</td>
</tr>
<tr>
<td>Authority established by interagency agreement</td>
<td>16%</td>
<td>12%</td>
</tr>
<tr>
<td>No formal established authority</td>
<td>2%</td>
<td>12%</td>
</tr>
</tbody>
</table>

Survey question: What mechanism establishes your state’s CISO or equivalent position’s authority over the other organizational entities for which it has responsibility? (49 respondents)
CISOs have an executive leadership platform

CISOs are improving reporting cadence to state leadership

Survey question: To what extent are you required to provide reports on cybersecurity status or posture of the enterprise to the following positions?
However, top challenges remain
Budget, talent, and threats top three since 2010

Survey question: Identify the top barriers that your state faces in addressing cybersecurity challenges.
CISOs have an executive leadership platform

Yet, top challenges persist
Bold Plays

States need bold actions to accelerate change
Budget challenge
Cybersecurity budgets are growing, but very slowly

Survey question: Characterize the year-over-year trending in your state's cybersecurity budget for years 2016 and 2017. (49 respondents)
Survey question: What percent of your state’s enterprise IT budget is allocated to enterprise cybersecurity? (all executive branch agencies) (50 respondents)
Budget challenge

Almost half the states do not have a separate budget line item for cybersecurity

Survey question: Does your state have a cybersecurity budget line item? (50 respondents)
**Budget challenge**

Federal agencies have dedicated cyber budget, and are (arguably) better funded

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Department of Transportation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of IT budget</td>
<td>4.48%</td>
<td>5.10%</td>
<td>5.63%</td>
</tr>
<tr>
<td>Year-over-year increase</td>
<td>N/A</td>
<td>13.76%</td>
<td>10.54%</td>
</tr>
<tr>
<td><strong>Health and Human Services</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of IT budget</td>
<td>5.45%</td>
<td>5.44%</td>
<td>6.44%</td>
</tr>
<tr>
<td>Year-over-year increase</td>
<td>N/A</td>
<td>-0.15%</td>
<td>18.5%</td>
</tr>
<tr>
<td><strong>Social Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of IT budget</td>
<td>8.59%</td>
<td>10.94%</td>
<td>11.4%</td>
</tr>
<tr>
<td>Year-over-year increase</td>
<td>N/A</td>
<td>27.34%</td>
<td>4.21%</td>
</tr>
<tr>
<td><strong>Treasury</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of IT budget</td>
<td>10.78%</td>
<td>11.67%</td>
<td>10.82%</td>
</tr>
<tr>
<td>Year-over-year increase</td>
<td>N/A</td>
<td>8.17%</td>
<td>-7.23%</td>
</tr>
<tr>
<td><strong>Justice</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of IT budget</td>
<td>27.08%</td>
<td>25.24%</td>
<td>25.07%</td>
</tr>
<tr>
<td>Year-over-year increase</td>
<td>N/A</td>
<td>-6.79%</td>
<td>-0.67%</td>
</tr>
</tbody>
</table>

Federal agencies’ cybersecurity budget as a percentage of total IT budget and year-over-year growth
Survey question: How effective are applicable federal and state cybersecurity regulations at improving your state’s cybersecurity posture and reducing risk? (1 = least effective, 5 = most effective) (49 respondents)
Bold Play #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.
Top cybersecurity initiatives
Innovation initiatives like AI, IOT, BlockChain, and Smart Government not on radar

36% Risk assessment
36% Metrics to measure and report effectiveness
36% Training and awareness
34% Cybersecurity strategy
30% Cloud platform and solutions security

Citizen digital identity 6%
Robotics/automation/AI 4%
Internet of Things (IoT) 4%
BlockChain 0%
Smart Government 0%

Survey question: Identify your state’s top five cybersecurity initiatives for 2018/2019. (50 respondents)
Bold Play#2: CISOs as an enabler of innovation

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.
Talent crisis

Most enterprise cybersecurity team consists of only 6-15 FTEs

Survey question: How many dedicated cybersecurity professionals does your enterprise security office employ? (49 respondents)
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)
### Talent crisis

#### Top barriers to hiring, developing and retaining cyber talent

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

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)
Talent crisis

While outsourcing has increased for certain functions, more than half of US states have yet to outsource many of them

Survey question: Select the cybersecurity functions that your state outsources. (47 respondents)
Bold Play#3: Team with the Private Sector and Higher Education

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.
**Bold Plays for Change**

**Summary**

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.
Security threats

Web applications and malicious code are the leading sources of security breaches

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

<table>
<thead>
<tr>
<th></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><strong>External</strong></td>
<td>24</td>
<td>17</td>
<td>8</td>
<td>15</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td><strong>Internal</strong></td>
<td>2</td>
<td>8</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td><strong>Business partner/ vendor</strong></td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Security threats

States have improved the frequency of application security testing

Survey question: How often does your state perform application security vulnerability testing and code review? (47 respondents)
Security threats

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

<table>
<thead>
<tr>
<th>Threat Level</th>
<th>2018</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average threat</strong></td>
<td>35%</td>
<td>33%</td>
</tr>
<tr>
<td><strong>Somewhat higher threat</strong></td>
<td>43%</td>
<td>43%</td>
</tr>
<tr>
<td><strong>Very high threat</strong></td>
<td>16%</td>
<td>29%</td>
</tr>
</tbody>
</table>
The majority of CISOs say that they are “somewhat confident” in their third parties’ cybersecurity practices.

Survey question: How confident are you in the cybersecurity practices of your third parties (contractors, service providers, business partners)? (48 respondents)
Confidence in third parties

CISOs’ top options for managing the adequacy of third-party cybersecurity practices include contractual cybersecurity requirements and confidentiality/nondisclosure agreements

Survey question: How does your state manage the adequacy of third-party (contractor, service provider, business partner) cybersecurity practices? (48 respondents)
Privacy

Only 14 states have a chief privacy officer; most states lack an enterprise program

Survey question: Does your state have the following?

- A program for managing privacy compliance (49 respondents)
  - 2018: Yes 27%, No 61%, N/A or do not know 12%
  - 2016: Yes 21%, No 60%, N/A or do not know 19%

- A written privacy, fair information practices, or data collection policy in place (49 respondents)
  - 2018: Yes 47%, No 37%, N/A or do not know 16%
  - 2016: Yes 58%, No 27%, N/A or do not know 15%

- Formal policies in place with respect to the destruction of personal information (49 respondents)
  - 2018: Yes 82%, No 10%, N/A or do not know 8%
  - 2016: Yes 71%, No 19%, N/A or do not know 10%

- A formal process in place to deal with complaints about handling privacy of information (such as a privacy hotline) (48 respondents)
  - 2018: Yes 25%, No 54%, N/A or do not know 21%
  - 2016: Yes 28%, No 46%, N/A or do not know 17%

- A formal incident response process (notifications, hotline) for breach of privacy (48 respondents)
  - 2018: Yes 58%, No 31%, N/A or do not know 10%
  - 2016: Yes 69%, No 21%, N/A or do not know 10%
Identity Access Management (IAM)

Only 21 states have an enterprise IAM solution

Survey question: Does your state provide an enterprise wide IAM solution? (50 respondents)
About Deloitte

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte’s cyber risk services help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation, and performance objectives through proactive management of the associated cyber risks. Deloitte provides advisory, implementation, and managed cybersecurity services to help our government clients lead the way with a collaborative threat intelligence strategy. Deloitte’s demonstrated approach and methodology help our clients better align security investments with risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to deliver services in the face of cyber incidents.

The Deloitte Center for Government Insights produces groundbreaking research to help government solve its most complex problems. Through forums and immersive workshops, we engage with public officials on a journey of positive transformation, crystallizing insights to help them understand trends, overcome constraints, and expand the limits of what is possible.

For more information, visit www.deloitte.com or read about the Deloitte Center for Government Insights at www.deloitte.com/us/center-for-government-insights.

About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories, and District of Columbia. NASCIO’s mission is to foster government excellence through quality business practices, information management, and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information, and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research, publications, briefings, and government affairs, NASCIO is the premier network and resource for state CIOs.

For more information, visit www.nascio.org
Questions?

NASCIO.org/stateofcyber
Contact Information

Debbi Blyth
Chief Information Security Officer
State of Colorado
deborah.blyth@state.co.us

Doug Robinson
Executive Director,
NASCIO
drobinson@nascio.org

Srini Subramanian
Principal, Deloitte Risk & Financial Advisory,
Deloitte & Touche LLP
ssubramanian@deloitte.com

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