The Deloitte-NASCIO Cybersecurity Study
Insights from 2010 - 2016

August 21, 2018
Srini Subramanian
State Government Sector Leader
Deloitte

Erik Avakian
CISO
Pennsylvania

Michael Roling
CISO
Missouri

Meredith Ward
Senior Policy Analyst
NASCIO

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
Key findings

- **2010**: Governance; strategy; budget; internal, external threats and creating a cyber mindset; security of third party providers

- **2012**: Cybersecurity budget-strategy connection; cyber authority and governance; preparedness for emerging threats; compliance—a lever for CISO leadership

- **2014**: Maturing role of the CISO; continuing budget-strategy disconnect; cyber complexity challenge; talent crisis

- **2016**: Governor-level awareness is on the rise; cybersecurity is becoming part of the fabric of government operations; a formal strategy and better communications lead to greater command of resources.

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
The growth of the CISO role
100% of states now have an enterprise-level CISO with associated cyber risk management authority

Percent of states with a CISO role

- 2006: 83%
- 2010: 92%
- 2012: 96%
- 2014: 98%
- 2016: 100%

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
**Full-time Employees (FTEs)**
Dedicated cybersecurity professionals employed by the state’s enterprise security office

- **2010**: 47% with 1 to 5
- **2012**: 50% with 1 to 5
- **2014**: 49% with 6 to 15
- **2016**: 51% with 6 to 15
- **2018**: 49% with 6 to 15

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
State of cyber workforce in 2016

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: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
State of cyber workforce in 2018

Top negative impact:

State’s salary rates and pay grade structures
Documented security strategy

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.

Percentage of states with a formal, documented cybersecurity strategy

- **2010**: 55%
- **2012**: 46%
- **2014**: 55%
- **2016**: 67%

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
Reporting/briefing

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

- **2010**: Reporting was to agency leadership, CIO’s. No governors.
- **2012**: 19.1% reporting to governor annual; 23.4% reporting legislature annually
- **2014**: 39.6% reporting to governor on ad hoc basis; 40.4% reporting to legislature ad hoc
- **2016**: 40% reporting to governor on ad hoc; 29% monthly
- **2018**: nearly 30% briefing governors on a monthly basis

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
Barriers

Top barriers in addressing cybersecurity challenges

- Emerging technologies (2010, 2012)
IT budget allocated to information security

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

- **2010**: Majority: 1-3% of budget
- **2012**: Majority: 1-3% of budget
- **2014**: Majority: 1-2% of budget
- **2016**: Majority: 1-2% of budget; 20% said 3-5%

Budget allocation has made some improvement, but continues to remain a top challenge

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
Chief privacy officer (CPO)

Percentage of state’s with a defined CPO role

- **2010**: 18% of states had one
- **2012**: 18%
- **2014**: 29.2%
- **2016**: 18%
- **2018**: 28%

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
Confidence in third parties

CISOs’ confidence in cybersecurity practices followed by third parties

- **2010**: 69% said somewhat confident; 23% said 3rd party security capabilities and controls are unknown
- **2012**: 74% somewhat confident
- **2014**: 81.3% somewhat confident
- **2016**: 65% somewhat confident

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
## Top outsourced cybersecurity functions

### Which functions do states outsource?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>24% threat monitoring</td>
<td>40% threat management and monitoring</td>
<td>39% forensics/legal support</td>
<td>54% cyber threat risk assessments</td>
</tr>
<tr>
<td></td>
<td>11% vulnerability management</td>
<td>20% security technology services</td>
<td>37% threat monitoring</td>
<td>44% forensics/legal support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>37% risk assessments</td>
<td>35% cyber threat mgmt. &amp; monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>18% vulnerability management</td>
<td>27% vulnerability management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>18% security tech. services</td>
<td>23% audit log analysis &amp; reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>18% audit log analysis &amp; reports</td>
<td></td>
</tr>
</tbody>
</table>

Source: Deloitte-NASCI Cybersecurity Studies, 2010-2016
## Top outsourced cybersecurity functions

<table>
<thead>
<tr>
<th>Outsourced Functions</th>
<th>2016</th>
<th>2014</th>
<th>2012</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber threat risk assessments</td>
<td>54%</td>
<td>37%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Forensics/legal support</td>
<td>44%</td>
<td>39%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Cyber threat management and monitoring services</td>
<td>35%</td>
<td>37%</td>
<td>40%</td>
<td>24%</td>
</tr>
<tr>
<td>Vulnerability management</td>
<td>27%</td>
<td>18%</td>
<td>-</td>
<td>11%</td>
</tr>
<tr>
<td>Audit log analysis and reports</td>
<td>23%</td>
<td>18%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Security technology services</td>
<td>-</td>
<td>18%</td>
<td>20%</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
### Top five cybersecurity initiatives by study

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection</td>
<td>Risk assessments</td>
<td>Risk assessments</td>
<td>Training and awareness</td>
</tr>
<tr>
<td>Information security risk assessments</td>
<td>Training and awareness</td>
<td>Training and awareness</td>
<td>Continuous monitoring/SOC</td>
</tr>
<tr>
<td>Information security training and awareness</td>
<td>Data protection</td>
<td>Data protection</td>
<td>Strategy</td>
</tr>
<tr>
<td>Application security</td>
<td>Strategy</td>
<td>Continuous monitoring/SO</td>
<td>Governance</td>
</tr>
<tr>
<td>Security infrastructure improvement</td>
<td>Governance</td>
<td>Incident response</td>
<td>Operationalizing cybersecurity</td>
</tr>
</tbody>
</table>

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
Top cybersecurity initiatives 2018

Risk assessments

Metrics to measure and report effectiveness

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016
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.

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