2020 Deloitte-NASCIO Cybersecurity Study
States at Risk: The Cybersecurity Imperative in Uncertain Times

Meredith Ward

12.3.2020
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
2020: The cybersecurity imperative in uncertain times
All 50 States and D.C. Participated
COVID-19 Challenged Continuity and Amplified Gaps

The pandemic widened cyber challenges: budget, talent, threats and the need for partnerships

Top barriers to overcome cybersecurity challenges

1. Lack of sufficient cybersecurity budget
2. Inadequate cybersecurity staffing
3. Legacy infrastructure and solutions to support emerging threats
4. Lack of dedicated cybersecurity budget
5. Inadequate availability of cybersecurity professionals
Connecting the Cyber Dots Across State, Local and Higher Education

Collaboration with local governments and public higher education is critical to managing increasingly complex cyber risk within state borders.

56% of CISOs are not very confident and 35% of CISOs are only somewhat confident in the cybersecurity practices of their local governments.

Only 28% of states reported that they had collaborated extensively with local governments as part of their state’s security program during the past year, with 65% reporting limited collaboration.
Centralized Operating Model Reduces Risk

A centralized structure helps CISOs position cyber in a way that improves agility, effectiveness, and efficiencies.

1. A centralized model should help to increase adoption of essential enterprise security services.

2. States have an opportunity to leverage federal funding for implementing and delivering cybersecurity services in a shared model to benefit all agencies.

3. The ability to manage a centralized cybersecurity budget is likely to help evaluate the overall cyber posture.

4. Cross-training and upskilling can also be simplified and more easily scaled, providing more career growth opportunities for cyber staff.
Identity & Access Management (IAM)

<table>
<thead>
<tr>
<th>IAM moves up in enterprise priority</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2018</td>
</tr>
<tr>
<td>Risk assessments</td>
<td>1</td>
</tr>
<tr>
<td>Enterprise identity and access management</td>
<td>11</td>
</tr>
<tr>
<td>Cybersecurity strategy</td>
<td>4</td>
</tr>
<tr>
<td>Operationalizing cybersecurity</td>
<td>13</td>
</tr>
<tr>
<td>Metrics to measure and report effectiveness</td>
<td>1</td>
</tr>
</tbody>
</table>

Top barriers to adopt enterprise IAM

01 Complexity of integrating with legacy systems (65%)
02 Competing or higher-priority initiatives (46%)
02 Decentralized environment of the state (46%)
Cyberthreats

30 states said financial fraud was a leading cause of breaches in the past year compared to 10 states in 2018.

Leading causes of breaches continue to be from external sources: malicious code (68%), web applications from external sources (81%), and “hacktivism” (86%), which is on the rise.
Budget

Only a few states reported an increase in the cybersecurity budget since 2018.

**2018 vs. 2020**

- **Increase of 1-5%**: 24% to 35%
- **Increase of 6-10%**: 10% to 6%
- **Increase of >10%**: 14% to 16%

**Top five areas covered in the cybersecurity budget**

- **86%** Audit logging and security information and event monitoring
- **84%** Security operations center
- **76%** Cybersecurity strategy and road map
- **76%** Threat intelligence and analytics
- **76%** Compliance and risk management

**2020 vs. 2018**

- Don't know, N/A: -16%
- Other: +18%
- appropriations: +4%
- Chargeback: +6%
- Hybrid of chargeback/appropriations: +10%

Cyber funding charge back versus appropriations

NASCIO
Representing Chief Information Officers of the States
www.nascio.org/stateofcyber
mward@nascio.org