States at Risk: Cybersecurity Priorities and Trends

OSU Digital Solutions Gallery
April 21, 2022

Doug Robinson, Executive Director
@NASCIO
Fiscal impact of pandemic: increased state revenues and spending - increased IT spending? Impact of ARPA and IIJA funding for state IT? **$1B State and Local Cybersecurity Improvement Grant** funds - $200M in FY2022

State IT organization transition continues: CIO as broker business model, evolution from owner-operator to more managed services, outsourcing and multi-supplier initiatives

Elevated cyber threats during pandemic, nation state and criminal attacks, more focus on enterprise cybersecurity models, whole-of-state collaboration, ransomware mitigation, zero trust framework

5R challenges of state IT workforce: recruitment, retention, reskilling, retirements, resignations - a **crisis with cybersecurity positions**

Focus on digital government services: user centric design, improved customer experience, **enhanced security**, automation, citizen identity management
State Governments at Risk!

- States are attractive targets – constant attack
- More aggressive threats, more intensity, ransomware
- Nation state threats, organized crime
- Critical infrastructure impact: disruption and resiliency
- Human factor – employees, contractors
- Election security - disinformation

Representing Chief Information Officers of the States
STATE CIO TOP 10 PRIORITIES
2022 Strategies, Policy Issues and Management Processes

1. Cybersecurity and Risk Management
   - #1 for nine consecutive years. On the top ten list since 2006

2. Digital Government/Digital Services
   - Steadily moving up the list. Pandemic impact

3. Broadband/Wireless Connectivity
   - #4 in 2021 - on/off list for a decade. Pandemic impact

4. Cloud Services
   - Major force of change. In top three since 2013

5. Legacy modernization
   - Pandemic impact! On the list since 2011

6. Identity and Access Management
   - New to the list in 2021. Enables digital services

7. Workforce
   - A continuing priority. Back on the list

8. Enterprise Architecture: governance
   - New to the list in 2022

9. Data and Information Management
   - On the list since 2016

10. Consolidation/Optimization
    - CIO priority each year. Frequently #1 since 2007

NASCIO
Representing Chief Information Officers of the States
Cybersecurity involves more than just IT – it’s a business risk.

Protecting data and infrastructure is a core responsibility of state government leaders and an investment in risk management and resiliency.

It’s a complex ecosystem that requires governance and regular communication on risk.
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.
Challenges

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
Budget and Spending

Average cybersecurity spend in 2020 (percentage of IT budget)
- 1–3% Most state governments
- 16.3% Federal agencies*
- 10.9% Financial institutions

*Federal civilian agencies under the CFO Act of 1990.

Only a few states reported a budget increase since 2018

2018 vs. 2020

- Increase of 1–5%
  - 24% in 2018, 35% in 2020
- Increase of 6–10%
  - 10% in 2018, 6% in 2020
- Increase of >10%
  - 14% in 2018, 16% in 2020

The number of states that receive funding through the overall IT budget increased from 48% in 2018 to 57% in 2020.
Assessing Cybersecurity Maturity

| Characterize the current status of the cybersecurity program and environment in state government. | 96% |
| Developed security awareness training for workers and contractors | 89% |
| Acquired and implemented continuous vulnerability monitoring capabilities | 89% |
| Established trusted partnerships for information sharing and response | 80% |
| Adopted a cybersecurity framework, based on national standards and guidelines (based on NIST) | 77% |
| Created a culture of information security in your state government | 66% |
| Developed a cybersecurity disruption response plan | 66% |
| Adopted a cybersecurity strategic plan | 55% |
| Obtained cyber insurance | 52% |
| Documented the effectiveness of your cybersecurity program with metrics and testing | 41% |
| Used analytical tools, AI, machine learning, etc. to manage cybersecurity program |
Has your state adopted a whole-of-state approach to cybersecurity with collaboration among state agencies, local governments, utilities, private companies, universities, healthcare and others?

<table>
<thead>
<tr>
<th>Status</th>
<th>2020</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>25%</td>
<td>23%</td>
</tr>
<tr>
<td>In-progress</td>
<td>43%</td>
<td>-</td>
</tr>
<tr>
<td>Planned</td>
<td>14%</td>
<td>-</td>
</tr>
<tr>
<td>No plans</td>
<td>22%</td>
<td>21%</td>
</tr>
</tbody>
</table>
What Do We Know? Patterns of Success

- Enterprise Leadership and Governance
- Statewide Cybersecurity Framework & Controls
- Cybersecurity Culture: A Team Sport
- Know the Risks, Assess the Risks and Measure Progress
- Communicating the Risks: Awareness
- Invest: Operations and Security Technologies
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.
Based on the impact of the COVID-19 pandemic, what cybersecurity initiatives will receive more attention in the next 2-3 years? (select all that apply)

- Adoption/expansion of enterprise identity and access management solutions: 83%
- Continuous enterprise cybersecurity assessment: 69%
- Endpoint detection: 67%
- Introducing or expanding a zero trust framework: 67%
- Increased due diligence with vendors and third-party providers: 63%
- Improved anti-fraud capabilities and services: 60%
- Cybersecurity awareness training: 56%
- Increased use of behavioral analytics: 50%
# State Cyber Trends to Watch

- Talent crisis: recruitment, retention, compensation
- More centralized operating model for cybersecurity
- Increasing threats with expanded digital services
- Whole-of-state cybersecurity resiliency
- Supply chain compromises; considering SBOM
- Support and partnerships with local governments