States at Risk:
State Cybersecurity in a Heightened Risk Environment

NCSL Task Force on Cybersecurity and Privacy Work Group

December 5, 2022

Doug Robinson, Executive Director
@NASCIO
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
2022 Deloitte-NASCIO Cybersecurity Study
State cybersecurity in a heightened risk environment

A joint biennial report (7th edition) from Deloitte and the National Association of State Chief Information Officers (NASCIO)
Representing Chief Information Officers of the States

States at risk: A look across the evolution of cybersecurity in state government

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

2022
State cybersecurity in a heightened risk environment
About the 2022 respondents

Chief Information Security Officer (CISO) Survey Profile

• Enterprise-level CISO participants, or equivalents, answered 66 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs.

• Survey responses were received from 53 states and territories
## Cyber talent a top barrier for state CISOs

Inadequate availability of cybersecurity professionals is among the top five barriers that CISOs cite.

<table>
<thead>
<tr>
<th>2020</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>01</strong> Lack of sufficient cybersecurity budget (46%)</td>
<td><strong>01</strong> Legacy infrastructure and solutions to support emerging threats (52%)</td>
</tr>
<tr>
<td><strong>02</strong> Inadequate cybersecurity staffing (42%)</td>
<td><strong>02</strong> Inadequate availability of cybersecurity professionals (50%)</td>
</tr>
<tr>
<td><strong>03</strong> Legacy infrastructure and solutions to support emerging threats (34%)</td>
<td><strong>03</strong> Inadequate cybersecurity staffing (46%)</td>
</tr>
<tr>
<td><strong>04</strong> Inadequate availability of cybersecurity professionals (28%)</td>
<td><strong>04</strong> Decentralized IT and security infrastructure and operations (38%)</td>
</tr>
<tr>
<td><strong>05</strong> Lack of dedicated cybersecurity budget (28%)</td>
<td><strong>05</strong> Increasing sophistication of threats (29%)</td>
</tr>
</tbody>
</table>

NASCIO
Representing Chief Information Officers of the States
State cybersecurity professionals’ headcount not seeing an increase and it takes a long time to acquire cyber talent
Are states appealing to the new generation of tech workers?

The top factors to attract and retain talent include the opportunity to serve the public, job stability, and a retirement plan.

- Opportunity to serve and contribute to your state: 53% (2018), 56% (2020), 54% (2022)
- Job stability: 41% (2018), 52% (2020), 46% (2022)
- Pension/retirement plan: 37% (2018), 28% (2020), 35% (2022)

Only 25% of states reported offering remote work as a way to attract cybersecurity talent.

- Highlight greater stability, with less nonvoluntary turnover than in the private sector: 40%
- Promote nonsalary benefits: 37%
- Cross-train and develop state IT workforce: 33%
- Cybersecurity internship programs: 31%
- Active use of social media: 27%
- Flexible work location/remote within the state: 25%
- Relationship with state universities and faculty: 17%
Insights on Cybersecurity Threats

- CISOs continue to be **fairly confident** that states are protected against various threats, including those that may arise from remote work arrangements.

- Malware and phishing rank as the top threats, foreign state-sponsored espionage has risen significantly, and third parties and social engineering have declined in threat levels.

- In the past 12 months, the three leading causes of cyber incidents involve web applications, malicious code and **financial fraud**.

- On the rise are incidents involving foreign state-sponsored espionage, zero-day attacks, electronic/hacker attacks, and cloud platforms and solutions.
How much of a threat do each of the following cyberthreats pose to your state? (Very high and somewhat higher threat combined)

<table>
<thead>
<tr>
<th>Threat</th>
<th>2020</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware/ransomware</td>
<td>70%</td>
<td>75%</td>
</tr>
<tr>
<td>Phishing, pharming, and other related variants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foreign state-sponsored espionage</td>
<td>67%</td>
<td>85%</td>
</tr>
<tr>
<td>Increasing sophistication and proliferation of threats</td>
<td>54%</td>
<td></td>
</tr>
<tr>
<td>Social engineering</td>
<td></td>
<td>58%</td>
</tr>
<tr>
<td>Security breaches involving third parties</td>
<td></td>
<td>69%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities from unsecured code</td>
<td>44%</td>
<td>60%</td>
</tr>
<tr>
<td>External financial fraud involving information systems</td>
<td></td>
<td>48%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities in endpoint devices</td>
<td></td>
<td>43%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities in emerging technologies</td>
<td></td>
<td>33%</td>
</tr>
</tbody>
</table>
Majority of states focused on cyber strategy, multifactor authentication, and risk assessments as upcoming initiatives

<table>
<thead>
<tr>
<th>Highest responses</th>
<th>Lowest responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity strategy</td>
<td>Malware detection and mitigation</td>
</tr>
<tr>
<td>29%</td>
<td>6%</td>
</tr>
<tr>
<td>Multifactor authentication</td>
<td>Remote workforce management</td>
</tr>
<tr>
<td>27%</td>
<td>4%</td>
</tr>
<tr>
<td>Risk assessments</td>
<td>Robotic process and automation/artificial intelligence</td>
</tr>
<tr>
<td>25%</td>
<td>2%</td>
</tr>
</tbody>
</table>
Identity Access Management (IAM)
State level CISO role is maturing – more visibility and increased executive reporting

More CISO positions are now established by state law

<table>
<thead>
<tr>
<th>Authority established by state statute or law</th>
<th>2020</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority established by state secretary or CIO</td>
<td>54%</td>
<td>50%</td>
</tr>
<tr>
<td>Authority established by state administrative rule, regulation, or procedure</td>
<td>18%</td>
<td>29%</td>
</tr>
<tr>
<td>Authority established by a state executive (governor’s) order</td>
<td>20%</td>
<td>23%</td>
</tr>
<tr>
<td>Authority established by a state interagency agreement</td>
<td>10%</td>
<td>6%</td>
</tr>
<tr>
<td>No formal established authority</td>
<td>4%</td>
<td>10%</td>
</tr>
</tbody>
</table>

CISOs are required to provide more regular reports on the state’s cybersecurity status to state leaders, including the governor, legislature, and agency secretary

<table>
<thead>
<tr>
<th>Governor</th>
<th>State legislature</th>
<th>Secretary/deputy secretary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Monthly</td>
<td>Monthly</td>
<td>Monthly</td>
</tr>
<tr>
<td>Quarterly</td>
<td>Quarterly</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Annually</td>
<td>Annually</td>
<td>Annually</td>
</tr>
<tr>
<td>Ad hoc</td>
<td>Ad hoc</td>
<td>Ad hoc</td>
</tr>
</tbody>
</table>

NASCIO
Representing Chief Information Officers of the States
A firm financial footing sets a lasting foundation

Thirty states reported increases to their cybersecurity budget over the past year

- 21% Yes, established by statute or law
- 15% Yes, established by secretary or CIO
- 10% Yes, established by administrative rule, regulation, or procedure
- 4% Yes, established by an executive (governor's) order
- 46% No, as part of the overall IT budget
- 2% Not applicable/don't know

Only 2% of states reduced their cybersecurity budget by 1%–5% in 2022.
State agencies are increasingly adopting enterprise security services
Embracing the entire state: Tighter collaboration with local governments and public higher education provides greater security across the state.
Cyber Insurance

States with cyber insurance:
- Yes: 60%
- No: 40%

Plans to renew cyber insurance:
- Yes: 87%
- No: 13%

Challenges with cyber insurance:
- Too expensive: 25%
- Not enough value: 38%
- Other: 38%
Supply Chain

CISO involvement level in procurement process

- Increased: 62%
- Stayed the same: 36%
- Decreased: 2%

CISO Role in procurement process

- Establish security standards and guidelines:
  - 85%
- Evaluate a security questionnaire that vendors need to respond to in a procurement opportunity:
  - 54%
- Prohibition procurement of specific manufacturers/vendors/products:
  - 38%
- Perform a security test of the software and/or hardware prior to procurement/implementation:
  - 27%
- Not applicable/Do not know:
  - 6% in 2022, 4% in 2020
- Not engaged in the procurement:
  - 4% in 2022, 8% in 2020
- Other:
  - 2% in 2022, 6% in 2020

2022 vs. 2020
State Cyber Trends to Watch

- Talent crisis: recruitment, retention, compensation
- Adopting whole-of-state cybersecurity resilience
- More centralized operating model for cybersecurity
- Expanding attack surface – services, remote work
- Software supply chain risks
- Support and partnerships with local governments
Resource Center at NASCIO.org