



States at Risk: Cybersecurity Priorities and Trends

Vermont General Assembly
House Committee on Energy and Technology
April 6, 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; **crisis with cybersecurity positions**

Focus on digital government services: user centric design, improved customer experience, **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

Human factor – employees, contractors

Election security - disinformation

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

STATE CIO TOP 10 ENTERPRISE RISKS






2022 Priority State Enterprise Risks



www.nascio.org

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



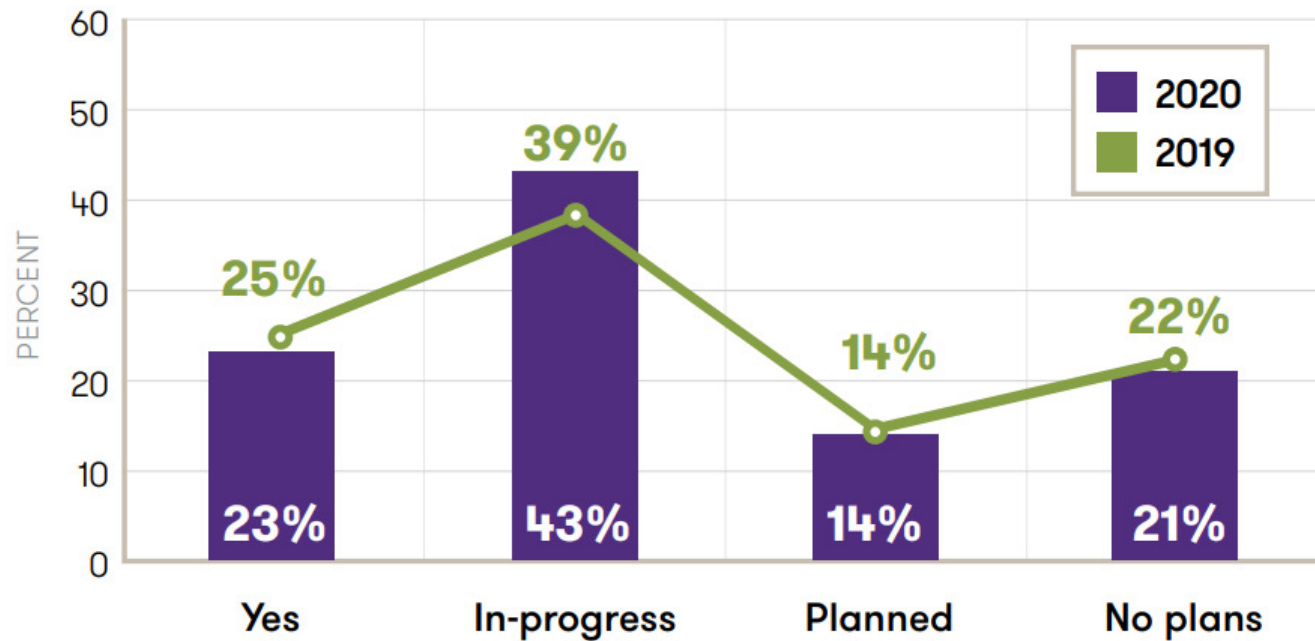
Characterize the current status of the cybersecurity program and environment in state government.

Developed security awareness training for workers and contractors	96%
Acquired and implemented continuous vulnerability monitoring capabilities	89%
Established trusted partnerships for information sharing and response	89%
Adopted a cybersecurity framework, based on national standards and guidelines (based on NIST)	80%
Created a culture of information security in your state government	77%
Developed a cybersecurity disruption response plan	66%
Adopted a cybersecurity strategic plan	66%
Obtained cyber insurance	55%
Documented the effectiveness of your cybersecurity program with metrics and testing	52%
Used analytical tools, AI, machine learning, etc. to manage cyber security program	41%

Assessing Cybersecurity Maturity

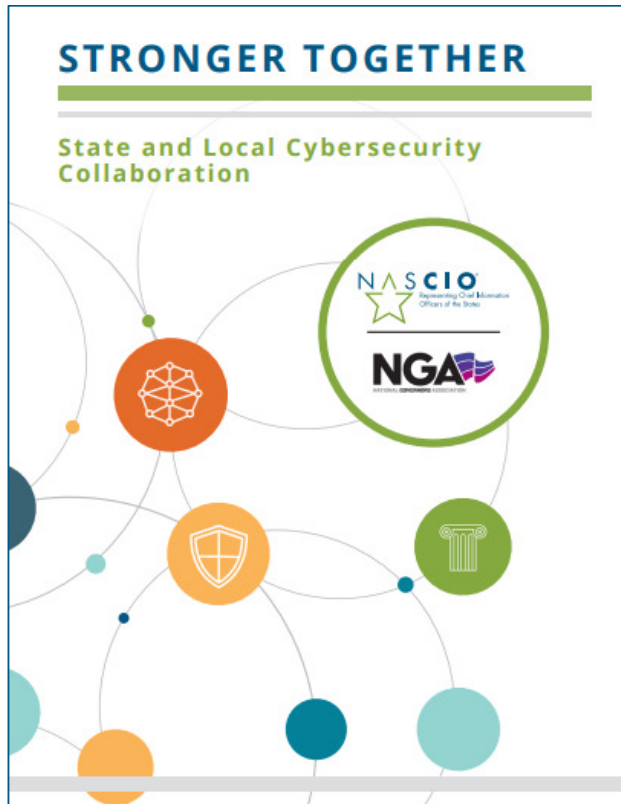


Has your state adopted a whole-of-state approach to cybersecurity with collaboration among state agencies, local governments, utilities, private companies, universities, healthcare and others?



©2020 Grant Thornton Public Sector LLC. All rights reserved.

Action is Needed Now



- 1) **At the very minimum states should be building relationships with local governments.**
 - Work through state municipal leagues and county associations, with emphasis on local information technology associations.
- 2) **States should raise awareness of existing services being offered to local governments.**
 - Hold cyber summits
 - Educate stakeholders
- 3) **States should be exploring cost savings that can be achieved through including local governments in service contracts.**
 - Consult local governments during the contract planning process solicitation
 - Provide a conduit for discussions about pooling resources among shared risk pools at the local level

States Supporting Local Governments

Local representation on governance bodies

Access to state contracts and services

Cybersecurity awareness training

Partners in table-top exercises

Vulnerability assessments

Cyber crisis response teams



Centralized Operating Model Reduces Risk

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

Advantages of a centralized structure

- 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.



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

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)

83%

Adoption/expansion
of enterprise identity and
access management solutions

69%

Continuous enterprise
cybersecurity assessment

67%

Endpoint detection

67%

Introducing or expanding
a zero trust framework

63%

Increased due diligence
with vendors and
third-party providers

60%

Improved
anti-fraud capabilities
and services

56%

Cybersecurity
awareness training

50%

Increased use
of behavioral analytics

State Cyber Issues to Watch

Talent crisis: recruitment, retention, compensation

More centralized operating model for cybersecurity

Increasing threats with expanded digital services

Whole-of-state cybersecurity resilience

Supply chain compromises; considering SBOM

Support and partnerships with local governments

