The Future State: IT Trends, Priorities and Perspectives

CSG South Policy Masterclass
September 29, 2022

Doug Robinson, Executive Director
@NASCIO
About NASCIO

- National association representing state chief information officers and information technology executives from the states, territories and D.C.

- NASCIO's mission is to foster government excellence through quality business practices, information management, and technology.

- NASCIO provides members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information, and promote the adoption of IT best practices and innovations.
Increased state revenues = increased IT spending? Federal $1B State and Local Cybersecurity Improvement Grant funds - $200M in FY2022

Focus on digital government services: improved citizen experience, citizen-centric design, security, automation, citizen identity management

Elevated cyber threats, nation state and criminal attacks, benefits fraud; focus on whole-of-state cybersecurity resilience, growth in chief privacy officers

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

**Forces of Change**: cloud migration, X-as-a-Service, prioritizing IT and application modernization, accelerated deployment; addressing technical debt is difficult

36 gubernatorial elections in 2022. Impact of transitions on leadership continuity?
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.
Rank top five business processes, practices, or investment changes that you believe will continue after the COVID-19 pandemic.

1. Increased attention on digital government services / citizen experience
2. Increased priority and investment in legacy modernization
3. Investments in broadband expansion / adoption
4. Expanded work from home / remote work options
5. Expanded use of collaboration platforms / remote meetings

#1 in 2021
#3 in 2020
#5 in 2021
#5 in 2020
#3 in 2021
#4 in 2020
#2 in 2021
#1 in 2020
#4 in 2021
#2 in 2020
How is the CIO organization moving to deliver services to agencies within the next two years?

- **56%**: Consolidation of infrastructure
- **54%**: Centralization of IT project management and oversight under the CIO organization
- **48%**: Consolidation of services (e.g., help desk, training etc.)
- **38%**: Consolidation of applications
- **31%**: Responsibility for technology procurement within the CIO organization
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%
What strategies and tactics has your state used in attracting and retaining a highly qualified IT workforce?

<table>
<thead>
<tr>
<th>Strategy</th>
<th>2022</th>
<th>2019</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promoting non-salary benefits like greater stability and diversity of experience</td>
<td>76%</td>
<td>73%</td>
<td>71%</td>
</tr>
<tr>
<td>Expanding flexible / remote work</td>
<td>73%</td>
<td>N / A</td>
<td>N / A</td>
</tr>
<tr>
<td>Building talent pipelines (e.g., partnering with local colleges / universities / technical schools)</td>
<td>71%</td>
<td>44%</td>
<td>29%</td>
</tr>
<tr>
<td>Call to public service</td>
<td>65%</td>
<td>67%</td>
<td>71%</td>
</tr>
<tr>
<td>Modifying job pre-requisites (e.g. education requirements)</td>
<td>57%</td>
<td>N / A</td>
<td>N / A</td>
</tr>
</tbody>
</table>
Besides increased compensation, what **single** action should be implemented that would be the most impactful in recruiting and retaining the future IT workforce in your state?

<table>
<thead>
<tr>
<th>Action</th>
<th>2022</th>
<th>2019</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reskilling current employees to meet modern IT demands</td>
<td>35%</td>
<td>25%</td>
<td>N / A</td>
</tr>
<tr>
<td>Aligning IT job titles, classifications and descriptions more closely to the private sector</td>
<td>31%</td>
<td>33%</td>
<td>31%</td>
</tr>
<tr>
<td>Increasing remote work options</td>
<td>18%</td>
<td>N / A</td>
<td>N / A</td>
</tr>
<tr>
<td>Expanding flexible work schedules</td>
<td>8%</td>
<td>N / A</td>
<td>N / A</td>
</tr>
<tr>
<td>Streamlining the hiring process and reducing time to hire</td>
<td>6%</td>
<td>14%</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>N / A</td>
<td>N / A</td>
</tr>
</tbody>
</table>
What major challenges do you face in meeting demand for digital services?

- Workforce skills and capability constraints to deliver/implement digital services: 63%
- Lack of organizational agility/flexibility: 43%
- Lack of adequate funding and budget to balance immediate public needs with future critical investment: 43%
- Data and information quality requirements and digitization complexity constraints: 41%
- Lack of internal willingness to take risks or embrace innovation: 37%
- Inability to envision and operationalize new ways of providing government services: 35%
- Lack of trust in shared digital solution provisioning, coordination and effective support for digital solution offerings: 31%
- Citizen expectations exceed organizational capabilities: 22%
- Lack of strategy and vision to implement: 22%
Promoted an agile organization to rapidly deploy solutions and create a continuous feedback loop for improvements

Encouraged experimentation and innovation to increase the speed to market to bring solutions to internal and external users

Used technology for a personalized citizen experience

Integrated design thinking and human-centered design concepts in the problem-solving and prioritization process

Created a dedicated digital services team

Created center of excellence / innovation

Deployed automation and AI to uncover user needs

Appointed a chief digital officer

Which digital services approaches and solutions has the CIO organization adopted and incorporated into enterprise-wide practice?
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.
48. How much of a threat do each of the following cyberthreats in the coming fiscal year 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>67%</td>
<td>85%</td>
</tr>
<tr>
<td>Foreign state-sponsored espionage</td>
<td>33%</td>
<td>54%</td>
</tr>
<tr>
<td>Increasing sophistication and proliferation of threats</td>
<td>52%</td>
<td>58%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>46%</td>
<td>69%</td>
</tr>
<tr>
<td>Security breaches involving third parties</td>
<td>44%</td>
<td>60%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities from unsecured code</td>
<td>28%</td>
<td>54%</td>
</tr>
<tr>
<td>External financial fraud involving information systems</td>
<td>35%</td>
<td>48%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities in endpoint devices</td>
<td>33%</td>
<td>43%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities in emerging technologies</td>
<td>27%</td>
<td>31%</td>
</tr>
</tbody>
</table>
CISOs identified their top barriers to addressing cybersecurity challenges

Q33. Identify the top five barriers that you believe your state faces to address cybersecurity challenges.

- **Legacy infrastructure and solutions to support emerging threats**
  - 2020: 34%
  - 2022: 52%

- **Inadequate availability of cybersecurity professionals**
  - 2020: 28%
  - 2022: 50%

- **Inadequate cybersecurity staffing**
  - 2020: 42%
  - 2022: 46%

- **Decentralized IT and security infrastructure and operations**
  - 2020: 20%
  - 2022: 38%

- **Increasing sophistication of threats**
  - 2020: 22%
  - 2022: 29%

Sources: 2022 Deloitte-NASCIO Cybersecurity Study and 2020 Deloitte-NASCIO Cybersecurity Study.
Insights on Cybersecurity Workforce

- Inadequate availability of cybersecurity professionals and staff remains among the top five barriers to progress.

- Despite CISOs’ growing responsibilities and the increasing sophistication of technology and threats, headcounts for state cybersecurity professionals remain about the same as 2020.

- Over 60 percent of state CISOs report gaps in competencies among their staff.

- Outsourcing is on the rise especially within the security operations center (SOC).
Only 25% of states allow talent to work remotely within their state

27. Identify the top three talent management practices followed by your state to attract and retain state cybersecurity workforce.

- 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%
- Recruit former military personnel: 15%
- Promote the location of government jobs: 13%
State Cyber Trends to Watch

Talent crisis: recruitment, retention, compensation

More centralized operating model for cybersecurity

Adopting whole-of-state cybersecurity resilience

Expanding attack surface – services, remote work

Software supply chain risks

Support and partnerships with local governments
Is identity, credential and access management part of a statewide digital strategy?

<table>
<thead>
<tr>
<th></th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>80%</td>
<td></td>
</tr>
<tr>
<td>Being considered</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>2%</td>
<td></td>
</tr>
</tbody>
</table>

Please characterize the status of your citizen digital identity initiative 2022 vs 2021.

<table>
<thead>
<tr>
<th></th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partially implemented</td>
<td>40%</td>
<td>49%</td>
</tr>
<tr>
<td>Planned</td>
<td>36%</td>
<td>27%</td>
</tr>
<tr>
<td>No plans to implement</td>
<td>20%</td>
<td>18%</td>
</tr>
<tr>
<td>Fully implemented</td>
<td>4%</td>
<td>6%</td>
</tr>
</tbody>
</table>

What is the status of digital / mobile driver’s licenses in your state 2022 vs 2021?

<table>
<thead>
<tr>
<th></th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planned</td>
<td>31%</td>
<td>27%</td>
</tr>
<tr>
<td>No plans to implement</td>
<td>25%</td>
<td>46%</td>
</tr>
<tr>
<td>Under development</td>
<td>20%</td>
<td>6%</td>
</tr>
<tr>
<td>Fully implemented and available to citizens</td>
<td>12%</td>
<td>10%</td>
</tr>
<tr>
<td>Pilot underway</td>
<td>12%</td>
<td>10%</td>
</tr>
</tbody>
</table>
APPLICATION PORTFOLIOS IN NEED OF MODERNIZATION

48% of the State Respondents Indicated a Majority of their Applications Need Modernization.

Respondents selected a percentage (in segments of 10%) in regards to applications needing modernization.
THE APPLICATION MODERNIZATION JOURNEY

State Respondents Selected All Options That Applied

Primary Drivers To Modernize Applications

- Older, Risky Code: 37
- Do Not Meet Business Need: 30
- Action Prioritized By Agency: 29
- Cybersecurity Risk: 29
- Technical Debt: 27
- Citizen Services: 23
- Statute Or Regulatory Requirement: 21
- Leverage SaaS Offerings: 20
- Workforce Changes: 14
- Cloud Microservices: 12
- Transition To OPEX Funding Model: 8
- Vacate Data Center: 8
- Remote Workforce Requirements: 6
- Other: 4
TOP CHALLENGES FOR APPLICATION MODERNIZATION INITIATIVES

1. Funding
2. Dedicating Staff Time
3. Large Legacy Systems
4. Significant Business Process Redesign
5. Agency Resistance to Change
6. Lack of Enterprise Insight
7. Procurement
8. Technical Know How
9. Shadow IT
10. Maintaining Current Enterprise Architecture
11. Cybersecurity

Experienced by 10 or More of Survey Respondents
What are your top three priorities in driving your cloud strategy forward?

<table>
<thead>
<tr>
<th>Priority</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability/Flexibility</td>
<td>78%</td>
</tr>
<tr>
<td>Security</td>
<td>57%</td>
</tr>
<tr>
<td>Investment optimization</td>
<td>43%</td>
</tr>
<tr>
<td>Disaster recovery/Risk management</td>
<td>41%</td>
</tr>
<tr>
<td>Application rationalization</td>
<td>27%</td>
</tr>
<tr>
<td>Staff training</td>
<td>20%</td>
</tr>
<tr>
<td>Mobility</td>
<td>10%</td>
</tr>
<tr>
<td>Extending catalog of cloud services</td>
<td>10%</td>
</tr>
<tr>
<td>Procurement reform to terms and conditions</td>
<td>4%</td>
</tr>
</tbody>
</table>
What emerging IT area will be most impactful in the next 3-5 years?

1. Low-code/no-code
2. Artificial intelligence (AI)/Machine learning
3. Mass personalization/citizen personas
4. Robotic process automation (RPA)
5. Internet of things (IoT)
6. Remote work technology
Looking to the Future

Future of the IT workforce: sustaining the remote work environment? Recruitment/retention/resignation, adaptation, skills transformation

Growing cloud adoption, SaaS, data center migration, off-premise solutions

Huge investments in broadband; more granular mapping data for better decisions; addressing affordability issues

Increasing use of data analytics to support policy decisions

Pressure to improve program integrity: identity verification, anti-fraud solutions, data sharing

State chief privacy officer role is growing and evolving