STATE CIO TOP 10 PRIORITIES

Priority Strategies, Management Processes and Solutions for 2023

01 Cybersecurity and Risk Management
02 Digital Government / Digital Services
03 Workforce
04 Legacy Modernization
05 Identity and Access Management
06 Cloud Services
07 Consolidation/ Optimization
08 Data and Information Management
09 Broadband/ Wireless Connectivity
10 Customer Relationship Management
Please characterize the current status of the cybersecurity program and environment in your state. (Select all that apply)

<table>
<thead>
<tr>
<th>Provided Cybersecurity Awareness Training for Workers and Contractors</th>
<th>2023</th>
<th>2020</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developed cybersecurity awareness training for workers and contractors</td>
<td>98%</td>
<td>96%</td>
<td>92%</td>
</tr>
<tr>
<td>Established trusted partnerships for information sharing and response</td>
<td>92%</td>
<td>89%</td>
<td>82%</td>
</tr>
<tr>
<td>Acquired and implemented continuous vulnerability monitoring capabilities</td>
<td>90%</td>
<td>89%</td>
<td>86%</td>
</tr>
<tr>
<td>Adopted the NIST Cybersecurity Framework</td>
<td>84%</td>
<td>80%</td>
<td>N/A</td>
</tr>
<tr>
<td>Required multi-factor authentication for executive branch agencies</td>
<td>84%</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Created a culture of information security in your state government</td>
<td>82%</td>
<td>77%</td>
<td>80%</td>
</tr>
<tr>
<td>Developed a cybersecurity disruption response plan</td>
<td>80%</td>
<td>66%</td>
<td>61%</td>
</tr>
<tr>
<td>Adopted a cybersecurity strategic plan</td>
<td>76%</td>
<td>66%</td>
<td>74%</td>
</tr>
<tr>
<td>Required .gov domain for executive branch agencies</td>
<td>71%</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Documented the effectiveness of your cybersecurity program with metrics and testing</td>
<td>57%</td>
<td>52%</td>
<td>55%</td>
</tr>
<tr>
<td>Obtained commercial cybersecurity insurance</td>
<td>53%</td>
<td>55%</td>
<td>47%</td>
</tr>
<tr>
<td>Used analytical tools, AI, machine learning and similar approaches to manage cybersecurity program</td>
<td>51%</td>
<td>41%</td>
<td>49%</td>
</tr>
<tr>
<td>Adopted a self-insured model for cybersecurity</td>
<td>33%</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Designed and implemented an antifraud strategy</td>
<td>18%</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Source: 2023 State CIO Survey
Has the CIO organization received supplemental funding for the current fiscal year? (Select all that apply)

- **45%** Cybersecurity funding
- **33%** Other, one-time capital investment
- **29%** Technology modernization fund
- **22%** We did not receive supplemental funding for this fiscal year
- **12%** One-time operating investment
- **8%** Innovation fund

Source: 2023 State CIO Survey
Concerning continuity of government, what is your top cybersecurity risk today?

1. Ransomware attack
2. Agency use of shadow IT solutions or products
3. Human error
4. Compromises to the software supply chain
5. Phishing / business email compromise

Source: 2023 State CIO Survey
If your state has banned a specific foreign-made technology, application platform or software, which category is banned? (select all that apply)

- Social media apps
- Telecommunications/networking
- Video platforms
- Computers
- Generative AI
- Robotic process automation (RPA)

Source: 2023 State CIO Survey
Which emerging IT area will be the most impactful in the next three to five years?

- Generative AI: 53%
- AI / machine learning: 20%
- Robotic process automation: 8%
- Low code / no code: 6%
- Mass personalization / citizen personas: 6%
- Other: 4%

Source: 2023 State CIO Survey
States are allowed to provide services to localities, rather than direct funding and the majority of states are adopting the shared services approach.

Just under ten percent of states are only providing direct funding to local governments with no shared services.

The five most common services offered are training, endpoint detection, risk assessments, support for .gov migration and adoption of multi-factor authentication.

While some initial benefits of the SLCGP have already been observed, such as improved coordination between state and local governments on cybersecurity, many respondents raised concerns over how any progress made can be sustained beyond its four-year life cycle.