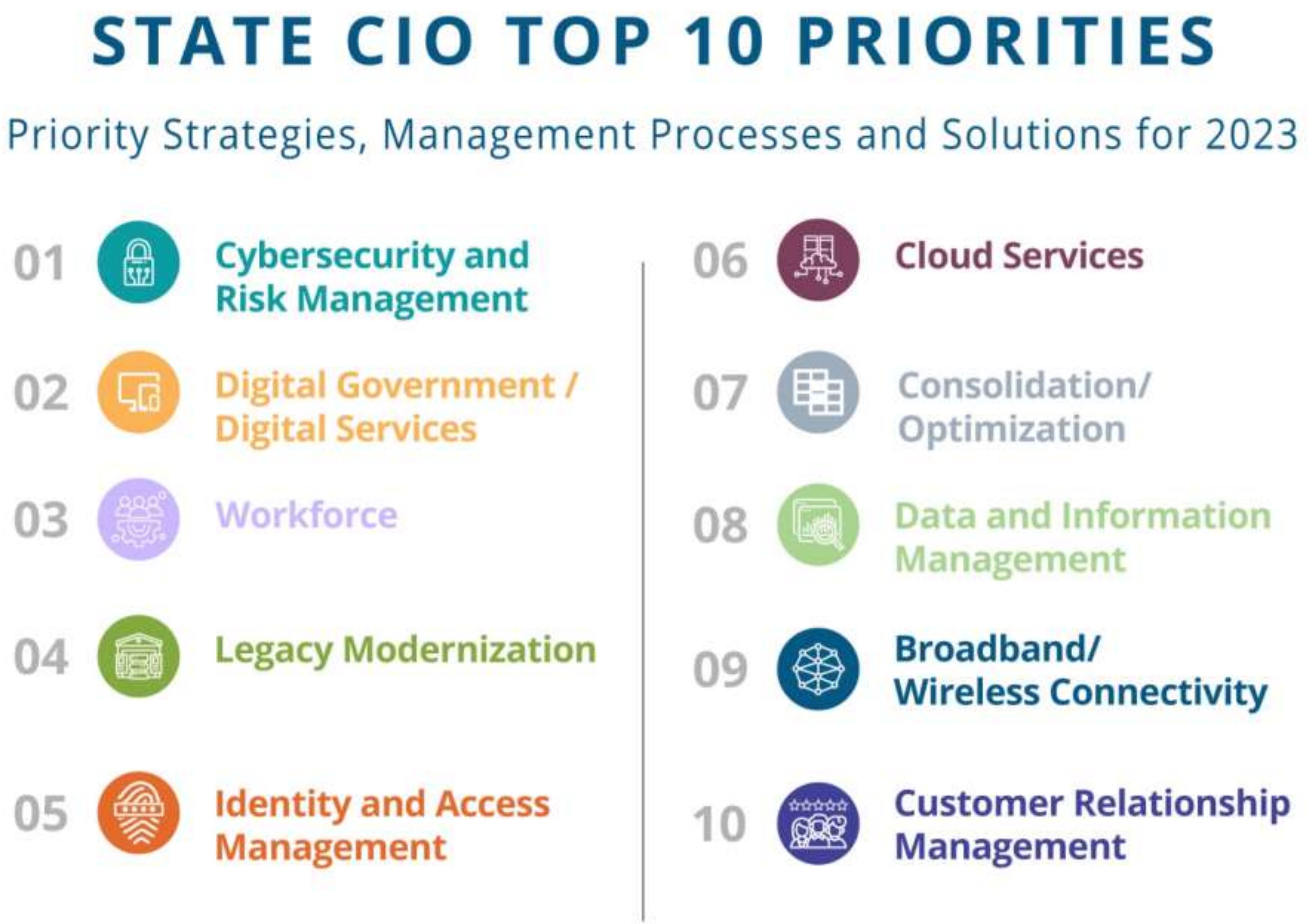


STATE CIO TOP 10 PRIORITIES

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

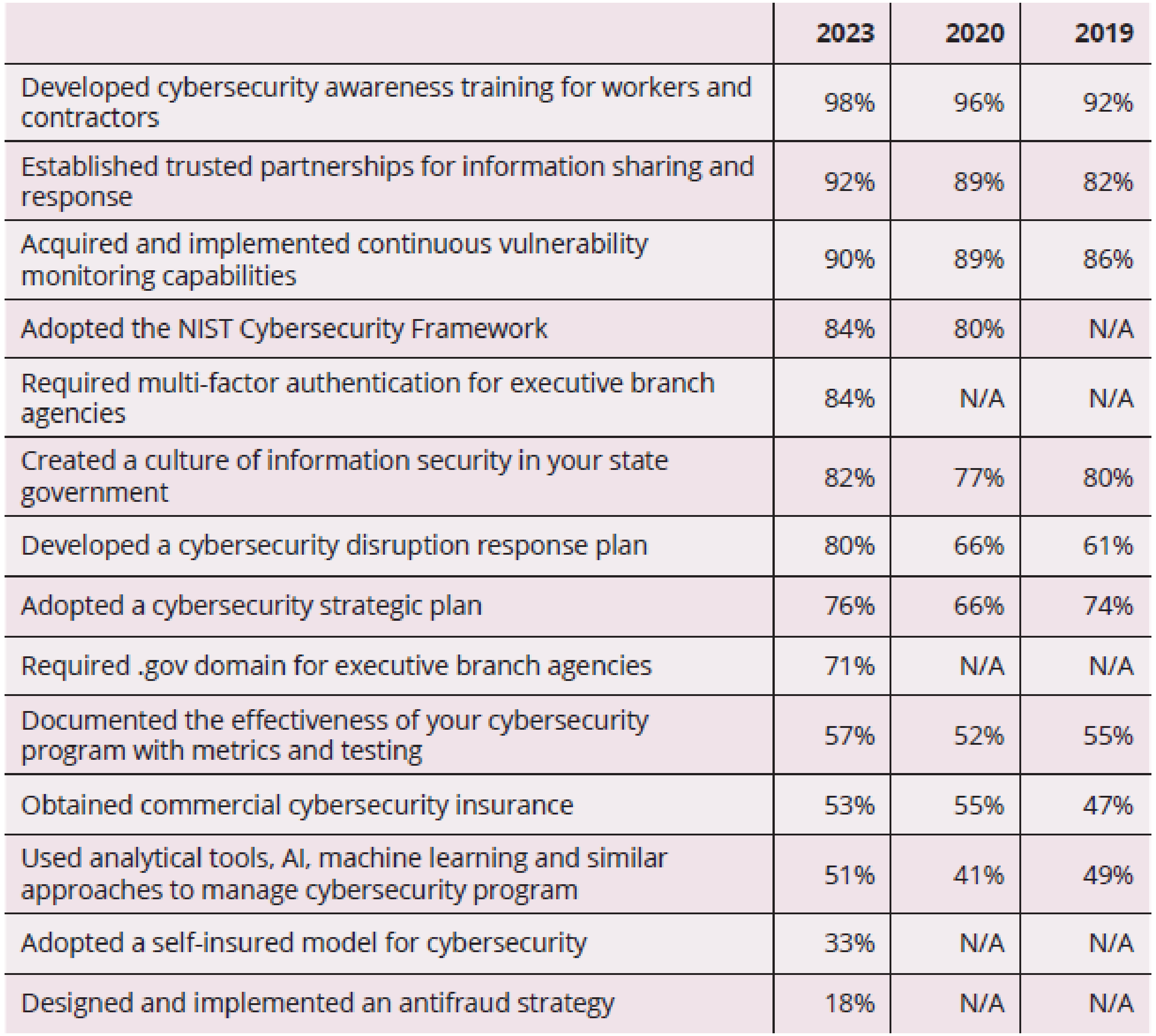
07 Consolidation/ Optimization

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)



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

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

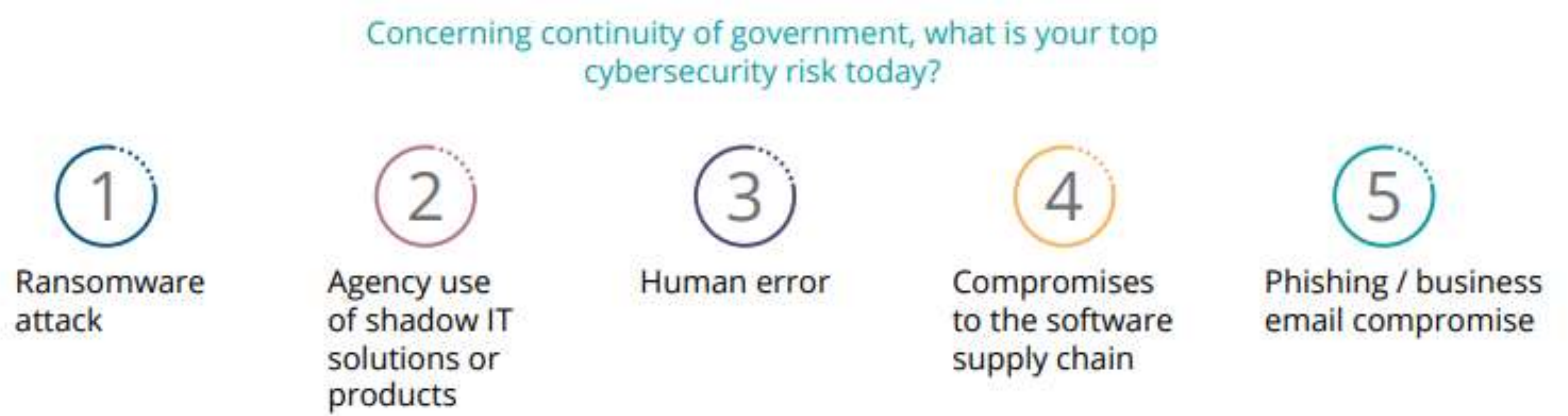
22%
We did not receive supplemental funding for this fiscal year

12%
One-time operating investment

8%
Innovation fund

NASCIO
Representing Chief Information Officers of the States

Source: 2023 State CIO Survey

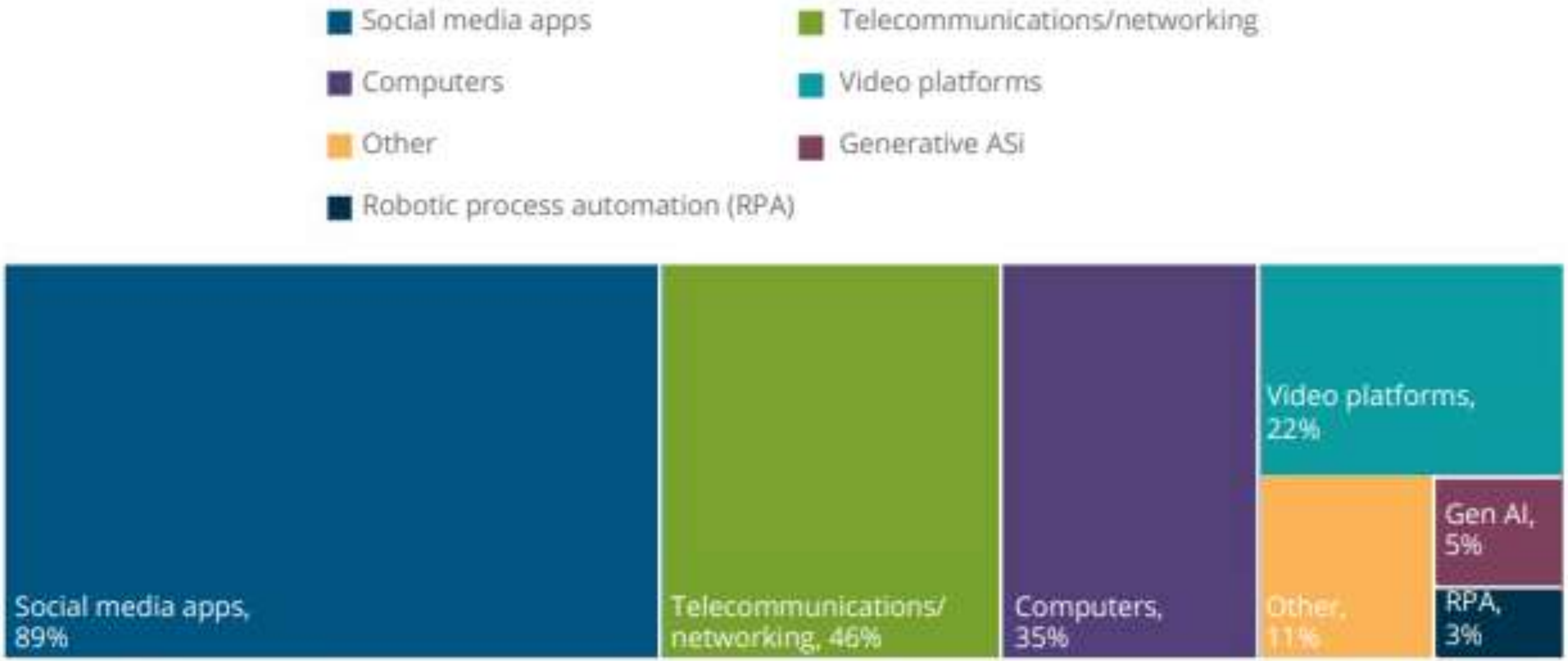


Concerning continuity of government, what is your top cybersecurity risk today?

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

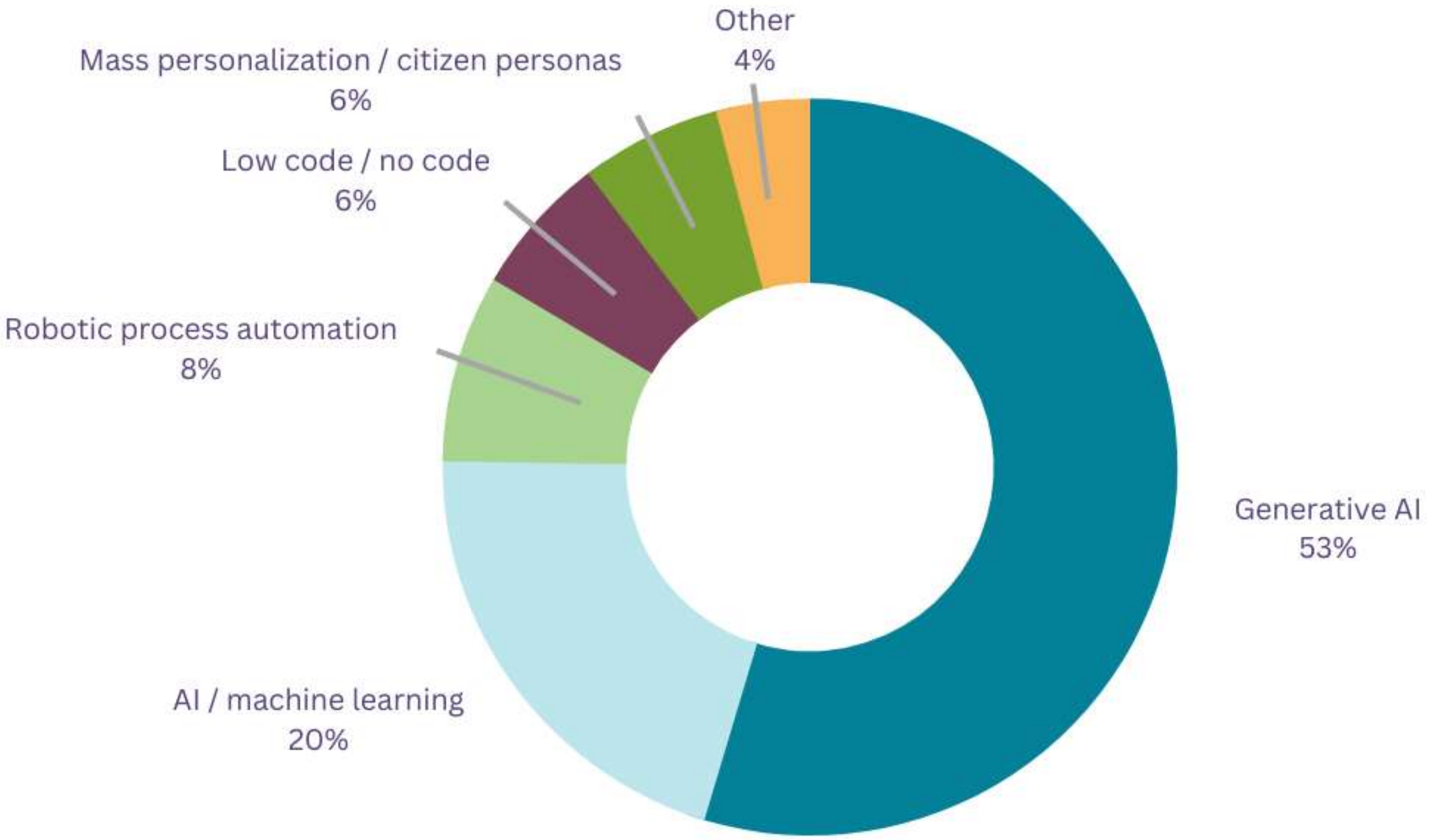
Source: 2023 State CIO Survey

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



Source: 2023 State CIO Survey

Which emerging IT area will be the most impactful in the next three to five years?



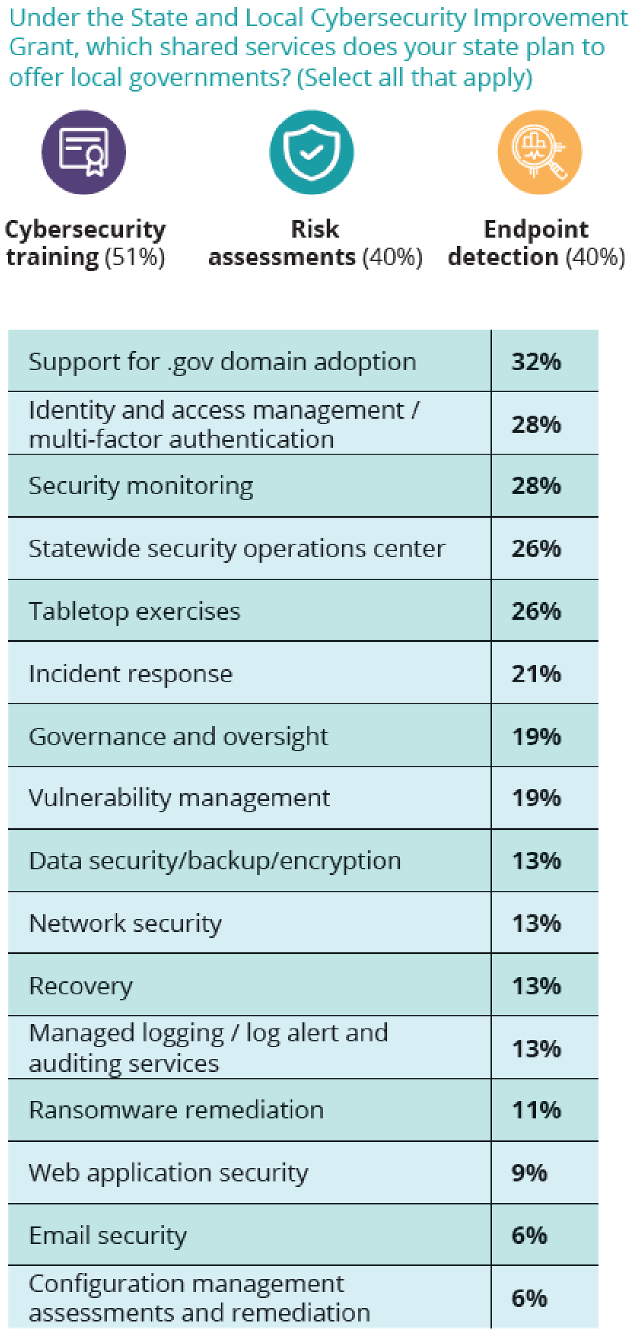
NASCIO
Representing Chief Information Officers of the States

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.



Under the State and Local Cybersecurity Improvement Grant, which shared services does your state plan to offer local governments? (Select all that apply)

Cybersecurity training (51%)

Risk assessments (40%)

Endpoint detection (40%)

Support for .gov domain adoption	**32%**
Identity and access management / multi-factor authentication	**28%**
Security monitoring	**28%**
Statewide security operations center	**26%**
Tabletop exercises	**26%**
Incident response	**21%**
Governance and oversight	**19%**
Vulnerability management	**19%**
Data security/backup/encryption	**13%**
Network security	**13%**
Recovery	**13%**
Managed logging / log alert and auditing services	**13%**
Ransomware remediation	**11%**
Web application security	**9%**
Email security	**6%**
Configuration management assessments and remediation	**6%**

Source: 2023 State CIO Survey

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.