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

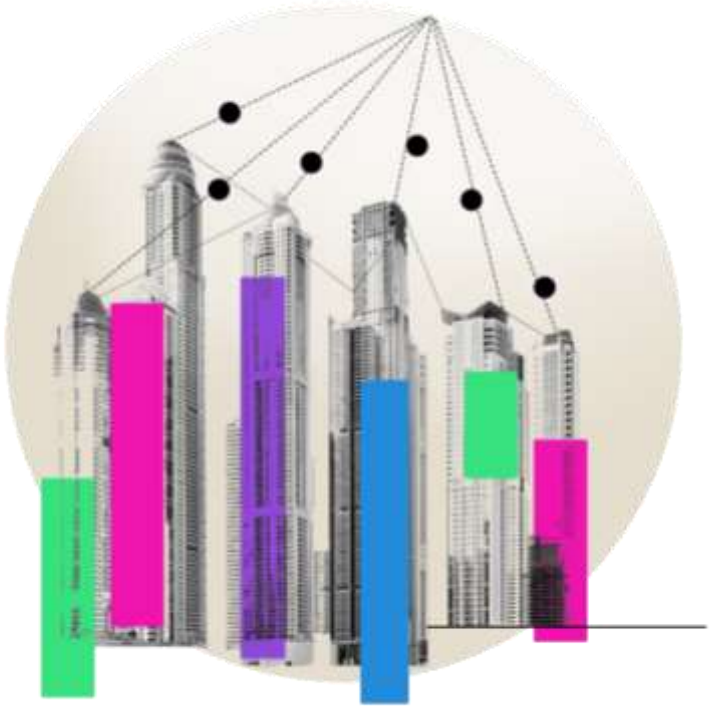
1 Cybersecurity and Risk Management	#1 for nine consecutive years. On the top ten list since 2006
2 Digital Government/Digital Services	Steadily moving up the list. Pandemic impact
3 Broadband/Wireless Connectivity	#4 in 2021 - on/off list for a decade. Pandemic impact
4 Cloud Services	Major force of 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

Deloitte.

NASCIO

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)

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

2010

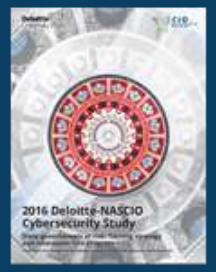
A call to secure citizen data and inspire trust

2012

A call for collaboration and compliance

2014

Time to move forward



2016

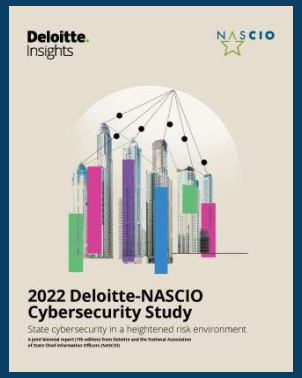
Turning strategy and awareness into progress

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

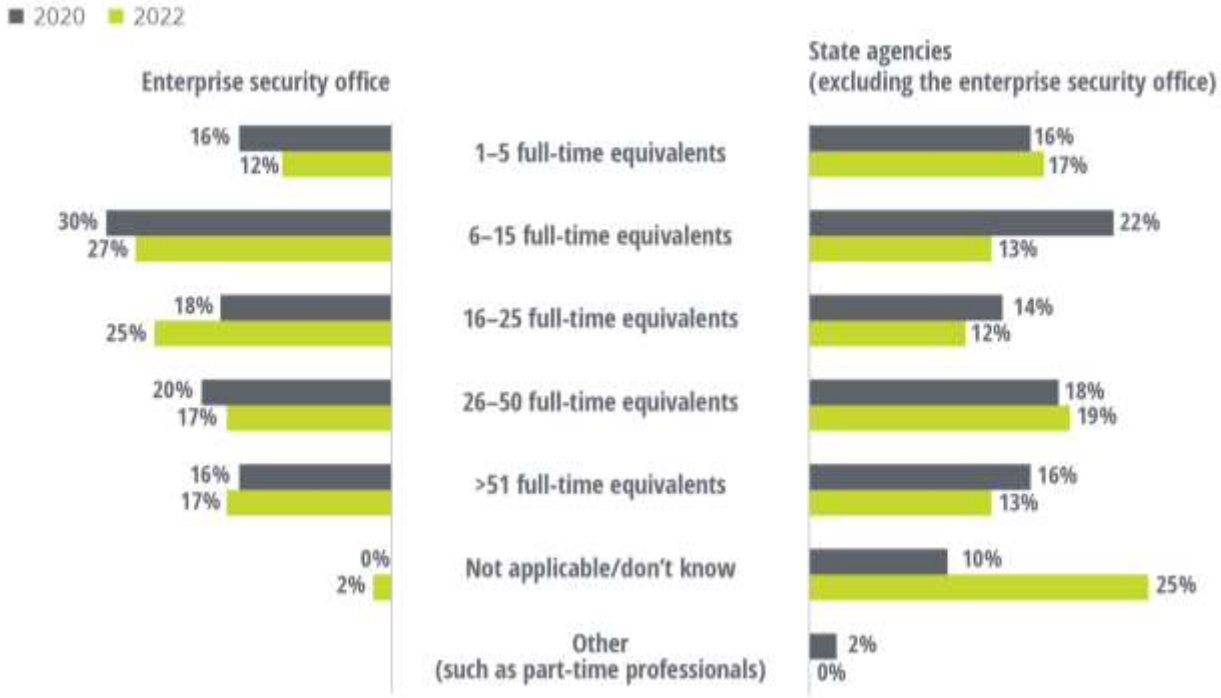
Cyber talent a top barrier for state CISOs

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

2020	2022
01 Lack of sufficient cybersecurity budget (46%)	**01** Legacy infrastructure and solutions to support emerging threats (52%)
02 Inadequate cybersecurity staffing (42%)	**02** Inadequate availability of cybersecurity professionals (50%)
03 Legacy infrastructure and solutions to support emerging threats (34%)	**03** Inadequate cybersecurity staffing (46%)
04 Inadequate availability of cybersecurity professionals (28%)	**04** Decentralized IT and security infrastructure and operations (38%)
05 Lack of dedicated cybersecurity budget (28%)	**05** Increasing sophistication of threats (29%)

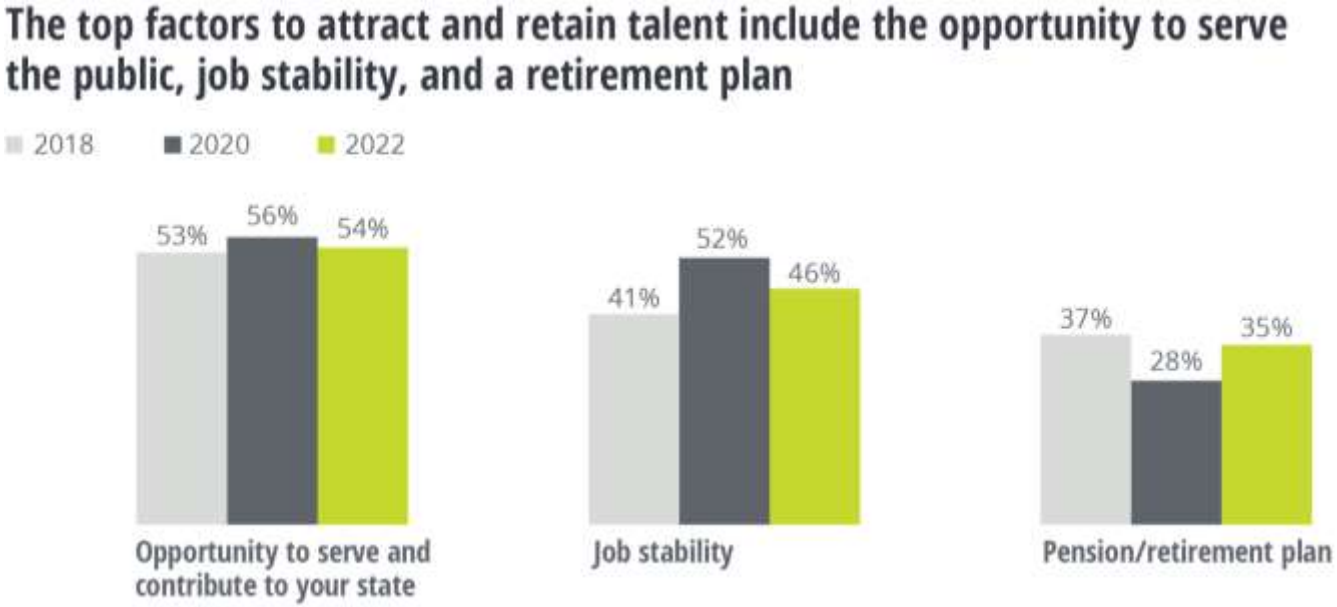
State cybersecurity professionals' headcount not seeing an increase and it takes a long time to acquire cyber talent

Head counts for state cybersecurity professionals haven't changed much since 2020



The time taken to hire talent is delaying the process and putting states at a disadvantage

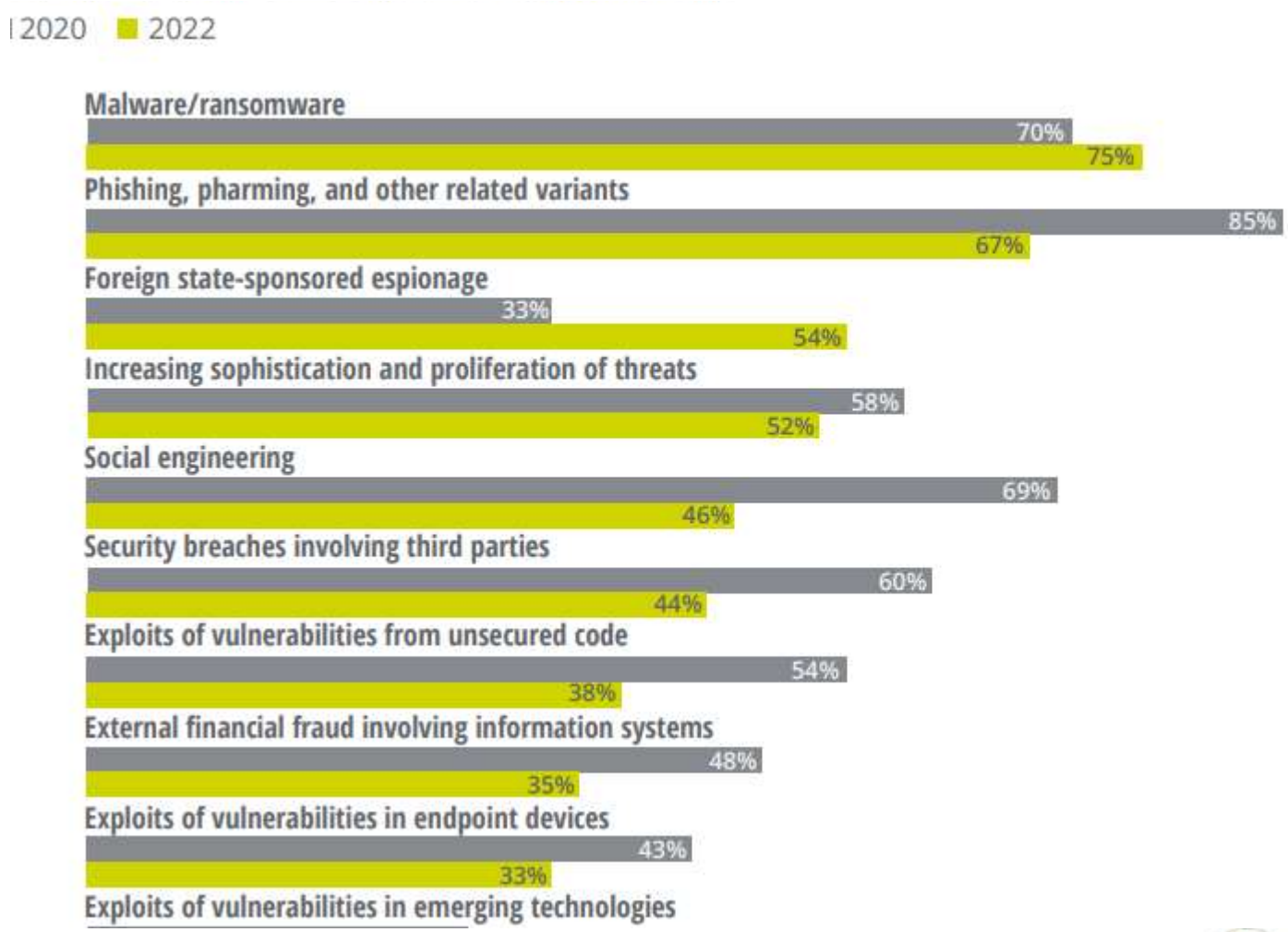
Are states appealing to the new generation of tech workers?



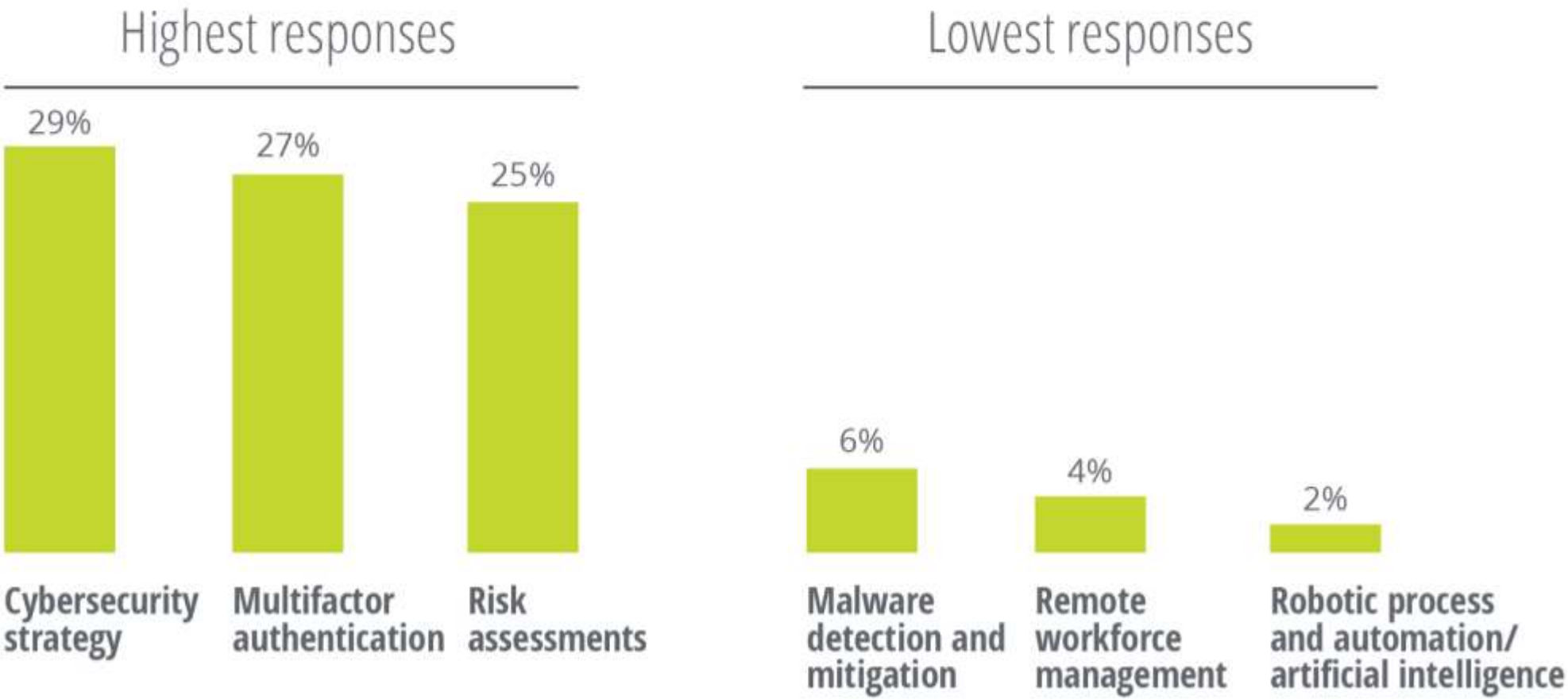
Insights on Cybersecurity Threats

- 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

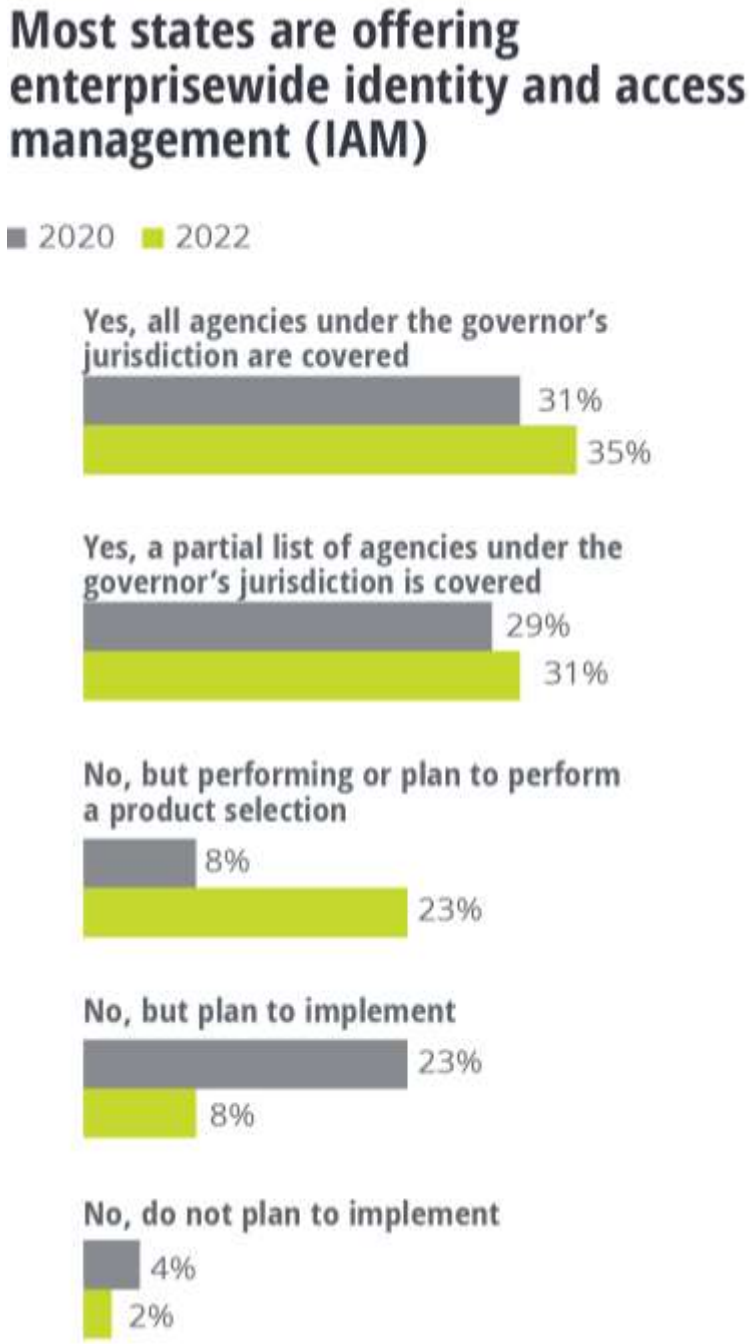
How much of a threat do each of the following cyberthreats pose to your state? (Very high and somewhat higher threat combined)



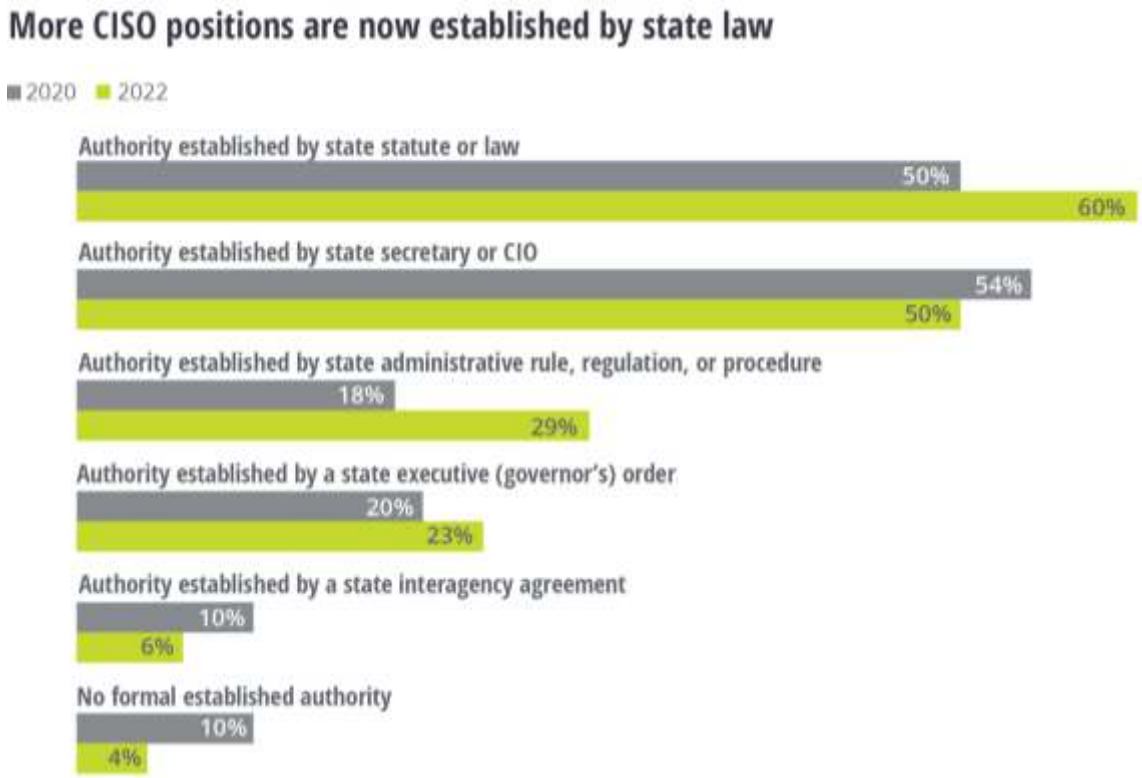
Majority of states focused on cyber strategy, multifactor authentication, and risk assessments as upcoming initiatives

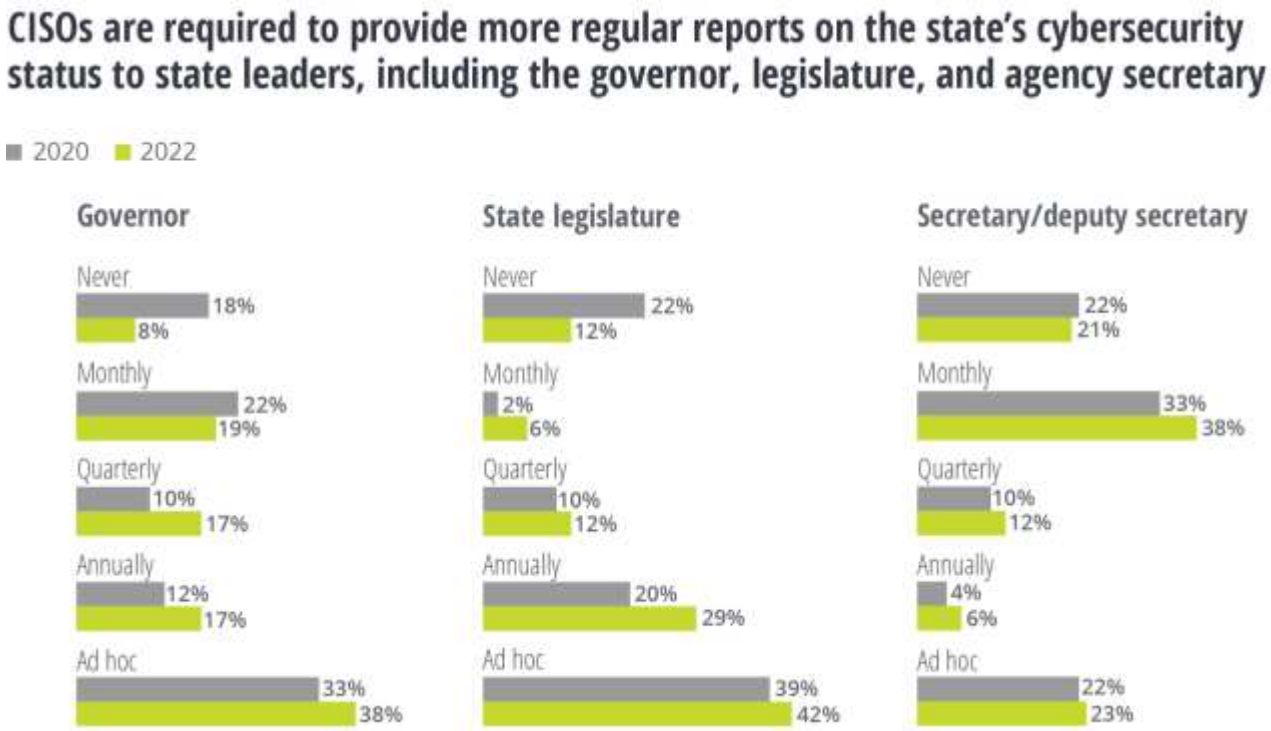


Identity Access Management (IAM)



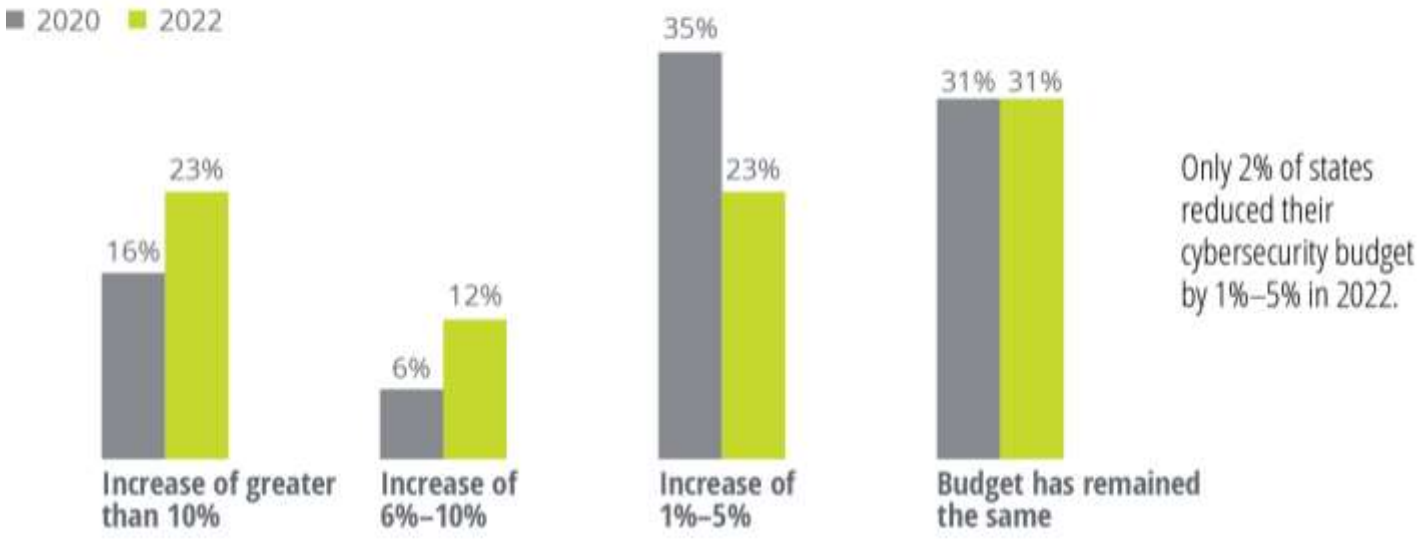
State level CISO role is maturing – more visibility and increased executive reporting



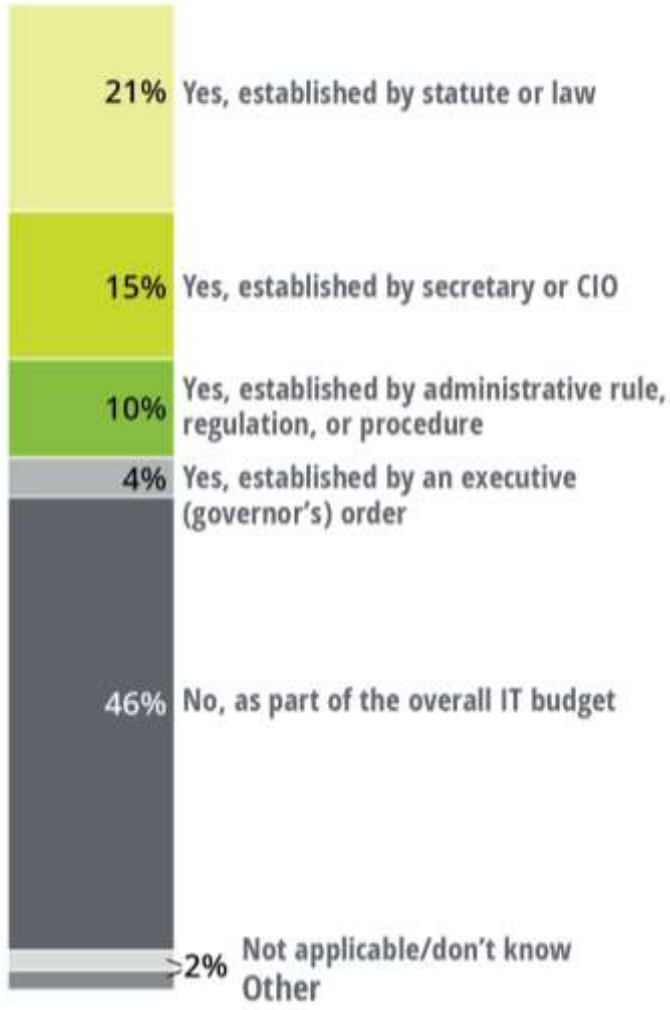


A firm financial footing sets a lasting foundation

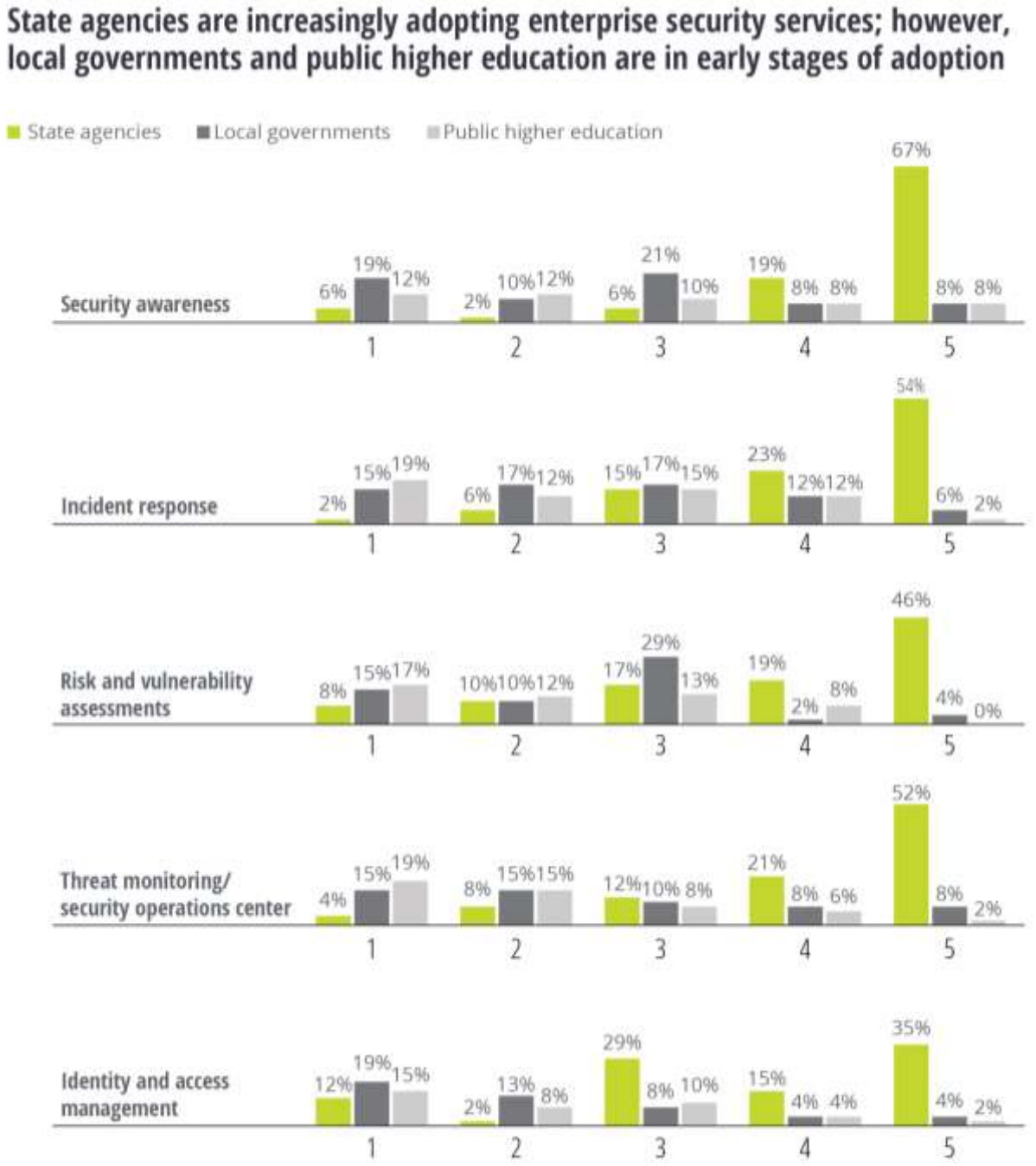
Thirty states reported increases to their cybersecurity budget over the past year



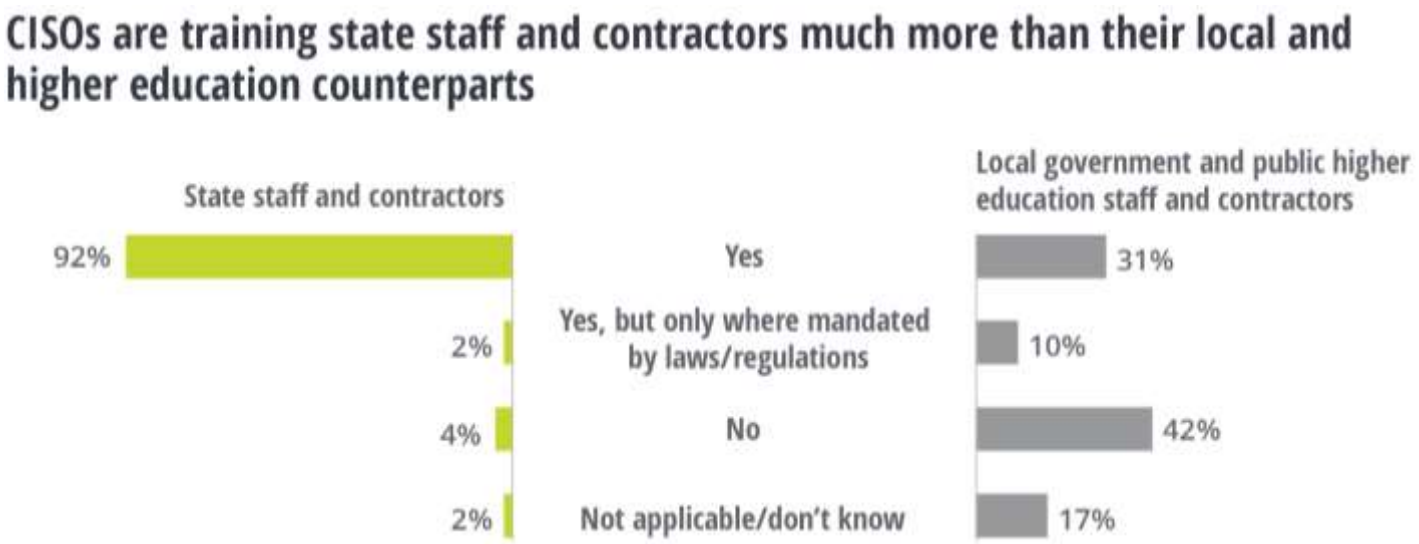
Most states have a dedicated budget line item for cybersecurity

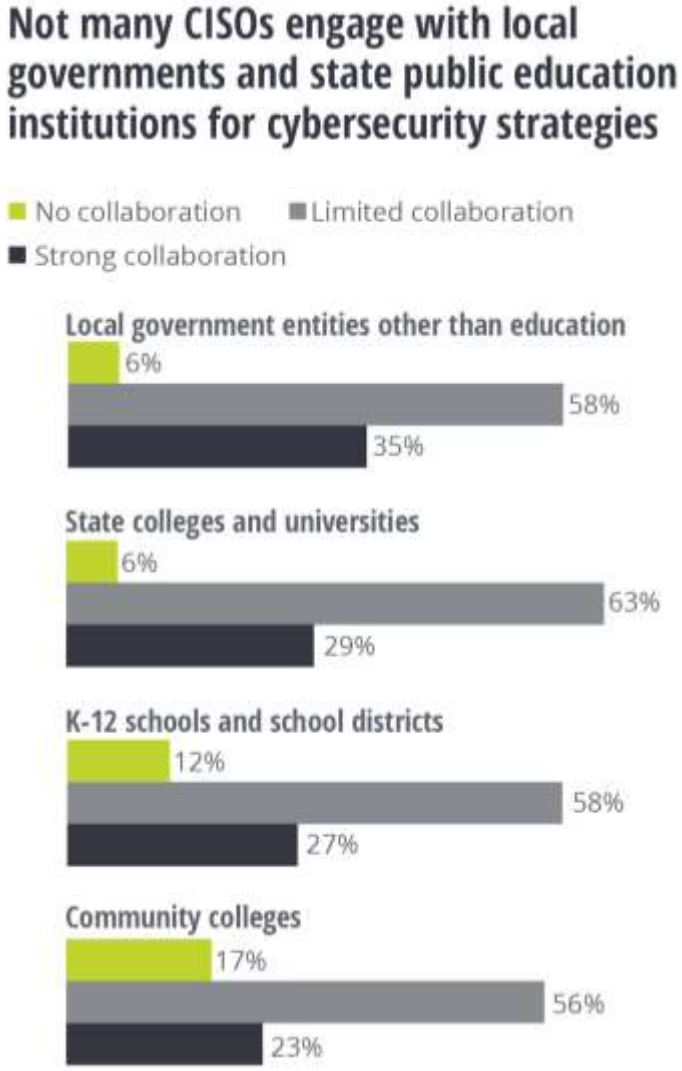


State agencies are increasingly adopting enterprise security services



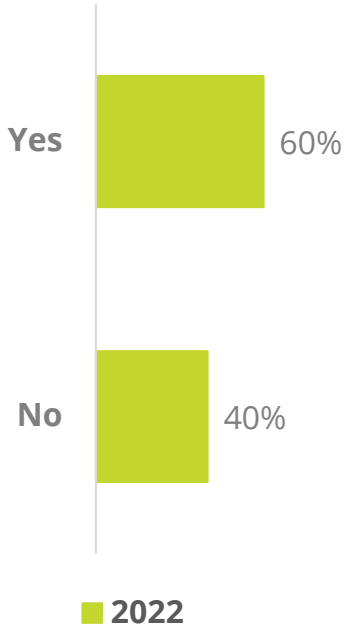
Embracing the entire state: Tighter collaboration with local governments and public higher education provides greater security across the state



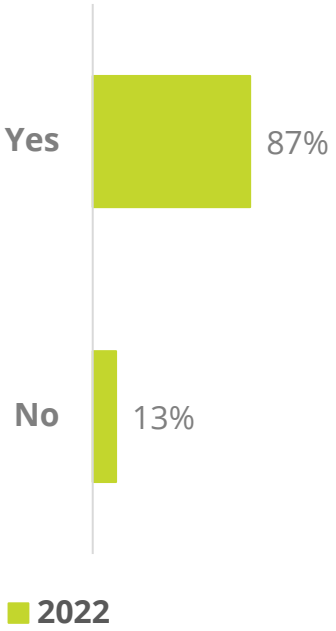


Cyber Insurance

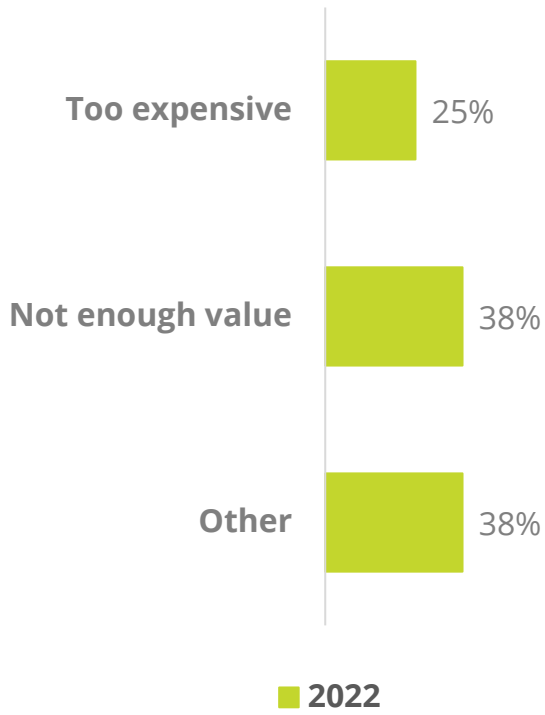
States with cyber insurance



Plans to renew cyber insurance

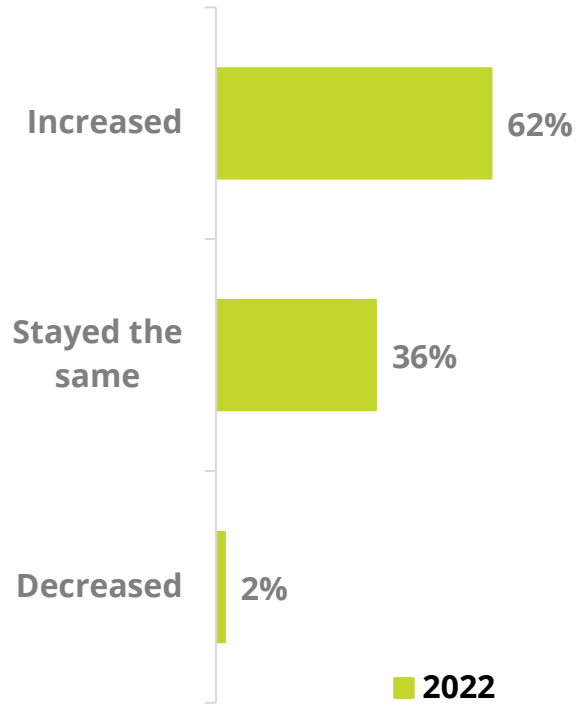


Challenges with cyber insurance

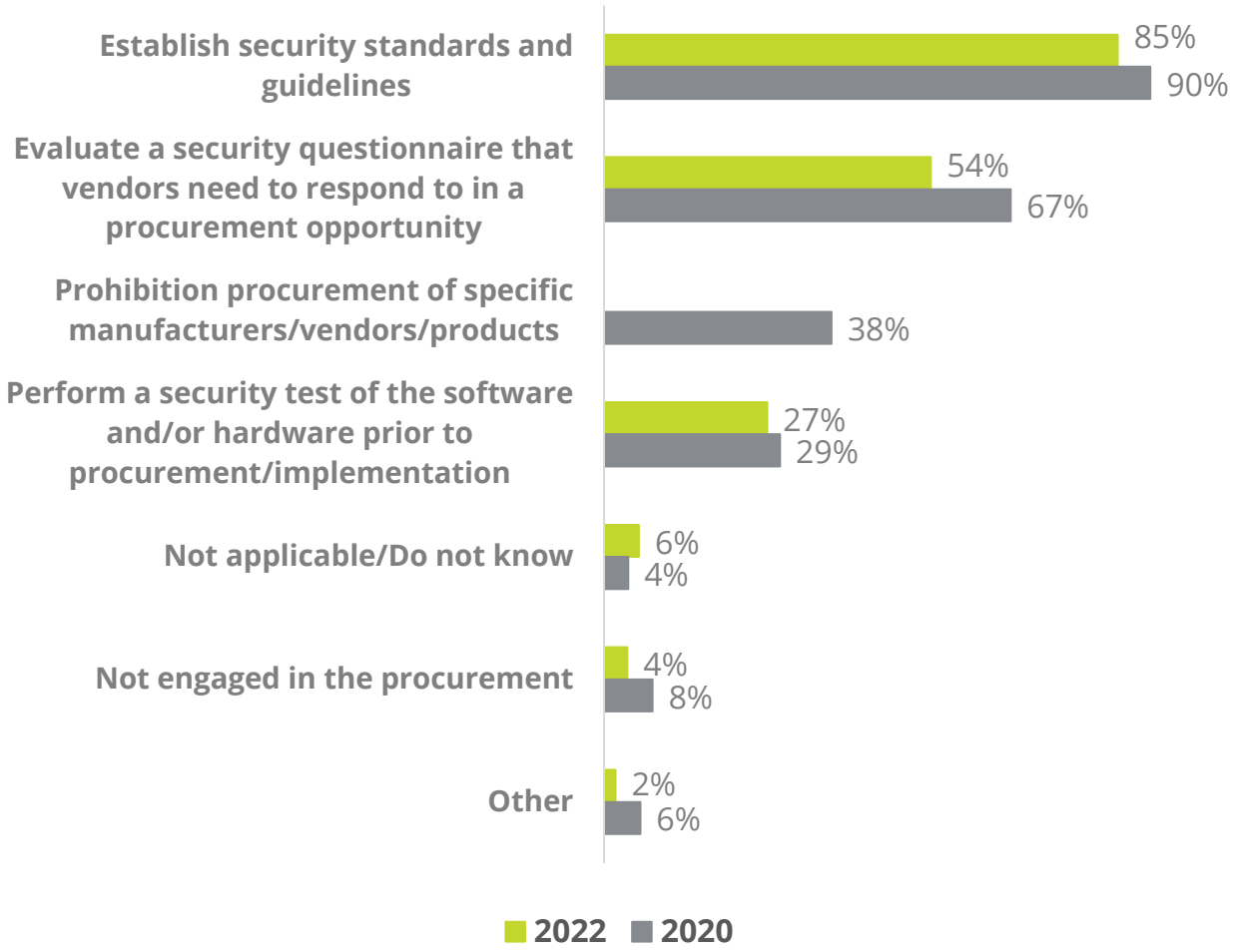


Supply Chain

CISO involvement level in procurement process



CISO Role in procurement process



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