States at Risk: Bold Plays for Change

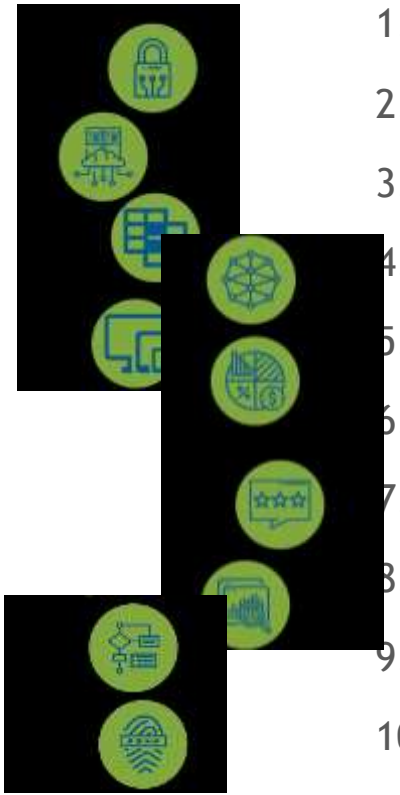
NCSL Task Force on Cybersecurity
January 18, 2019

Doug Robinson, NASCIO Executive Director
@NASCIO

NASCIO
Representing Chief Information Officers of the States

STATE CIO TOP 10 PRIORITIES

2019 Strategies, Management & Process Solutions



1. Security and Risk Management
2. Cloud Services
3. Consolidation/Optimization
4. Digital Government
5. Broadband/Wireless Connectivity
6. Budget, Cost Control, Fiscal Management
7. Customer Relationship Management
8. Data Management and Analytics
9. Enterprise IT Governance
10. Identity and Access Management

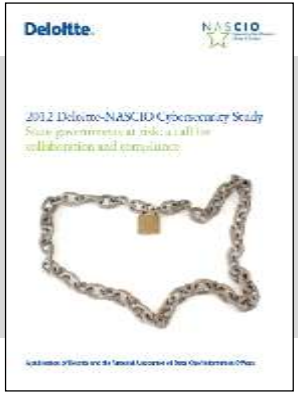
Source: NASCIO State CIO Ballot, November 2018

Timeline of the Deloitte – NASCIO Cybersecurity Study *States at Risk*

2010

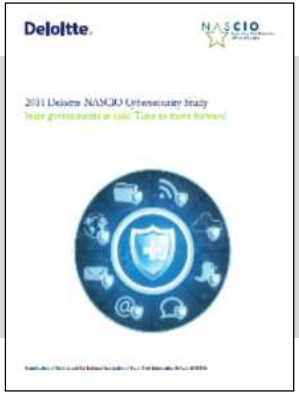
A call to secure citizen data and inspire trust

2012



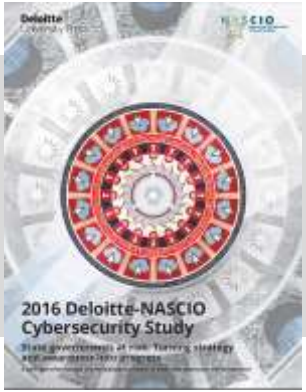
A call for collaboration and compliance

2014



Time to move forward

2016



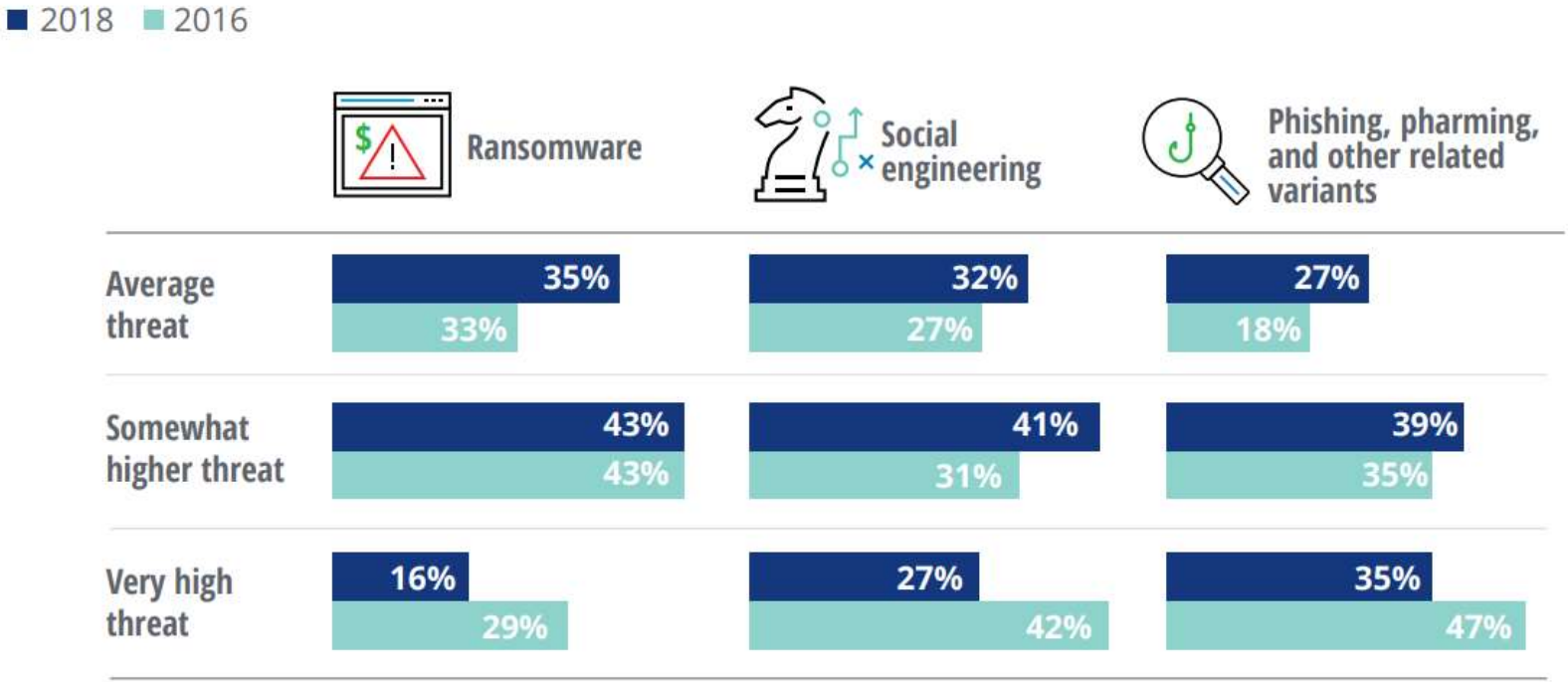
Turning strategy and awareness into progress

2018

Bold plays for change

Ransomware, social engineering, and phishing are the top cyber threats for states

Please choose the prevalence of the following cyber threats in your state for the next year. (49 respondents)



Source: 2018 Deloitte-NASCIO Cybersecurity Study

Web applications and malicious code are the leading sources of security breaches

In terms of security breaches over the past 12 months, which of the following applies to your state?





	Web applications	Malicious code (e.g., viruses/worms/ spyware/malware/ ransomware)	My state has not been breached	Electronic attack (e.g., hacker)	Physical attack (e.g., stolen computer systems)
Respondents	30	28	19	16	14
External	24	17	8	15	6
Internal	2	8	6	0	8
Business partner/ vendor	4	3	5	1	0

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Cybersecurity Maturity in the States is Improving…

Risk based strategies are being adopted

Expanded focus from operational to strategic

Expect continued progress in 2019

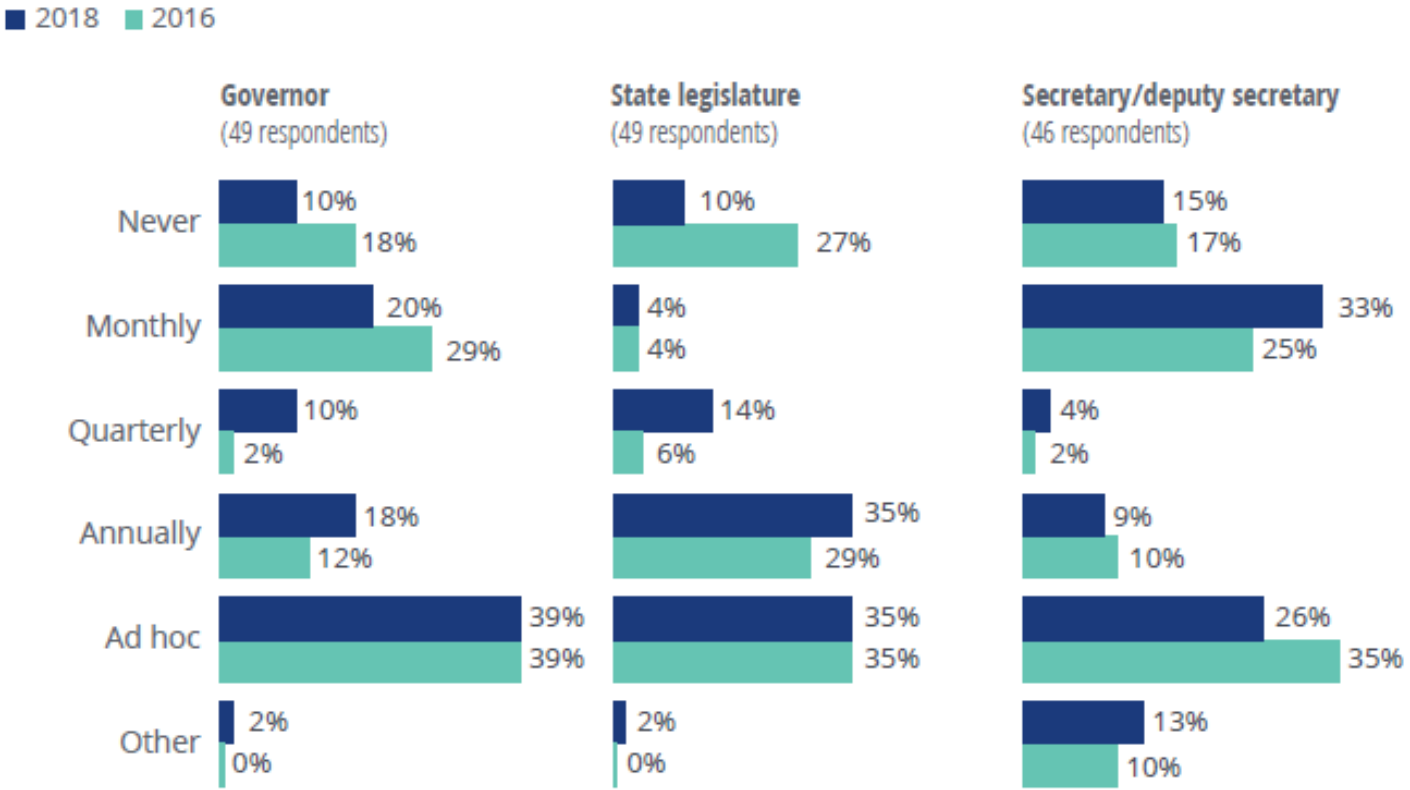
Characterize the current status of the cybersecurity program and environment in state government.

	2013	2015	2017	2018
Developed security awareness training for workers and contractors	78%	87%	88%	98%
Adopted a cybersecurity framework based on national standards and guidelines	78%	80%	95%	94%
Established trusted partnerships for information sharing and response	75%	80%	83%	92%
Adopted a cybersecurity strategic plan	61%	74%	83%	85%
Acquired and implemented continuous vulnerability monitoring capabilities	78%	80%	79%	81%
Created a culture of information security in your state government	73%	74%	83%	79%
Developed a cybersecurity disruption response plan	45%	52%	69%	69%
Documented the effectiveness of your cybersecurity program with metrics and testing	47%	52%	57%	63%
Using analytical tools, AI, machine learning, etc. to manage cybersecurity programs	n/a	n/a	n/a	44%
Obtained cyber insurance	n/a	20%	38%	42%

Source: NASCIO 2018 State CIO Survey

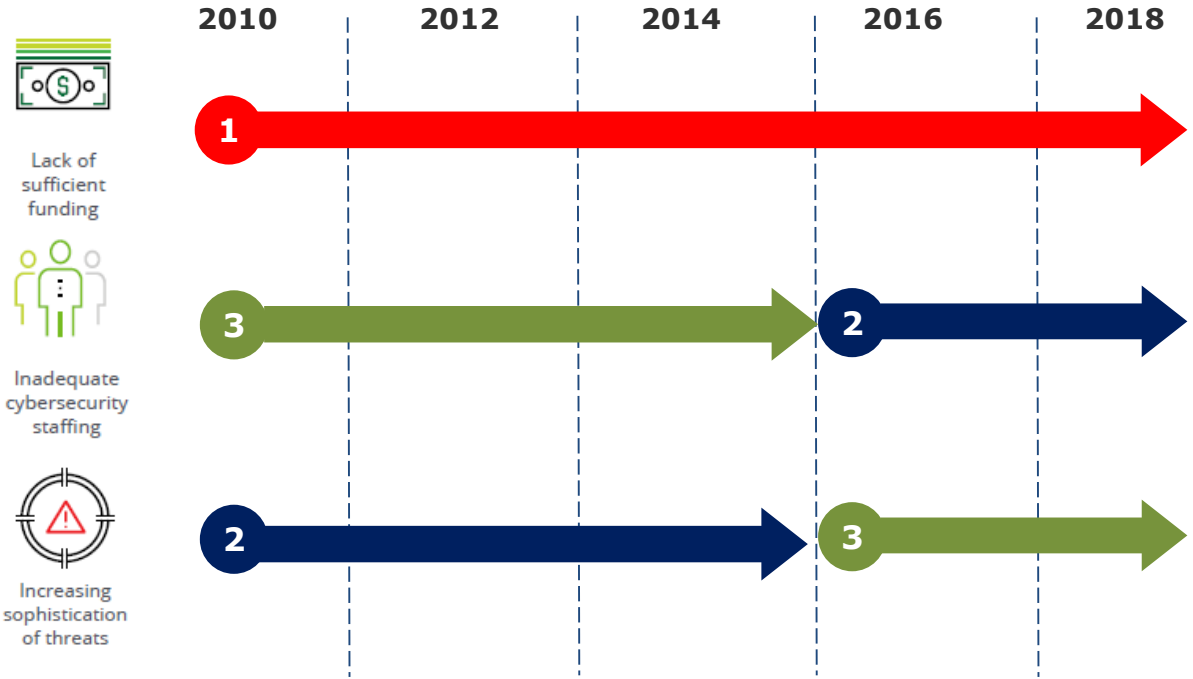
CISOs have established a frequent reporting cadence to state leadership

To what extent are you required to provide reports on cybersecurity status or posture of the enterprise to the following positions?



However persistent challenges remain…

Budget, talent, and threats top three since 2010



Survey question: Identify the top barriers that your state faces in addressing cybersecurity challenges.

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Budget and Staffing Remain Top Barriers to Effective Cybersecurity

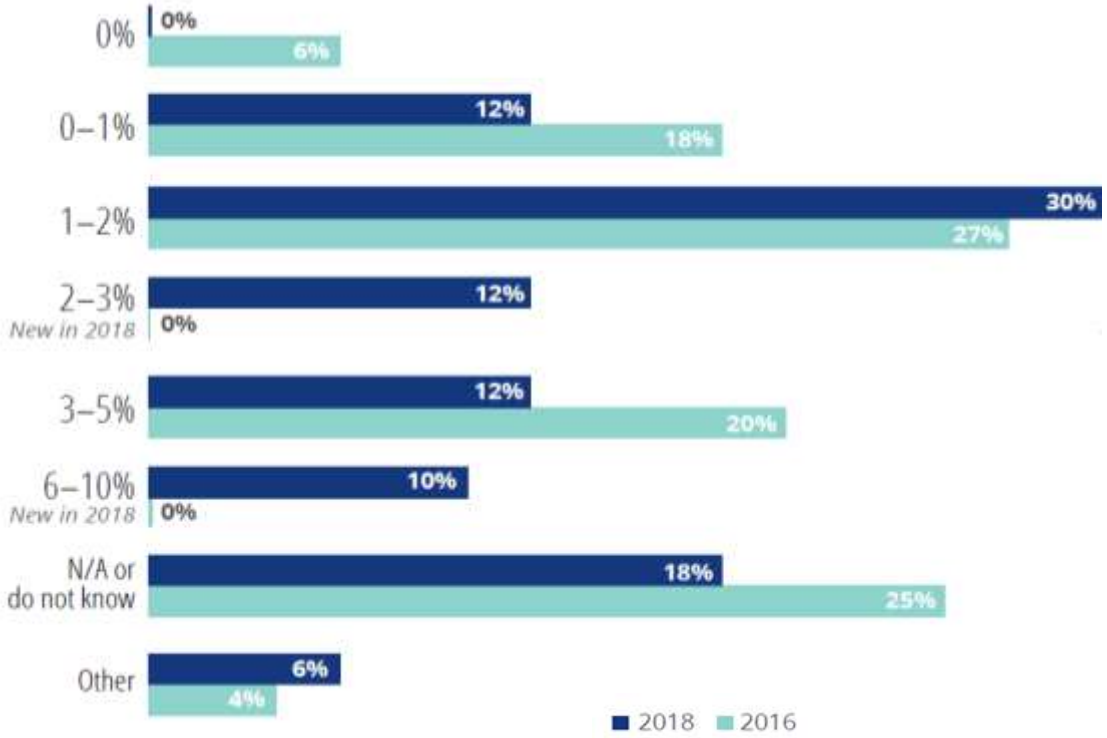
State CIOs say…

State CISOs say…

NASCIO

Budget Challenge

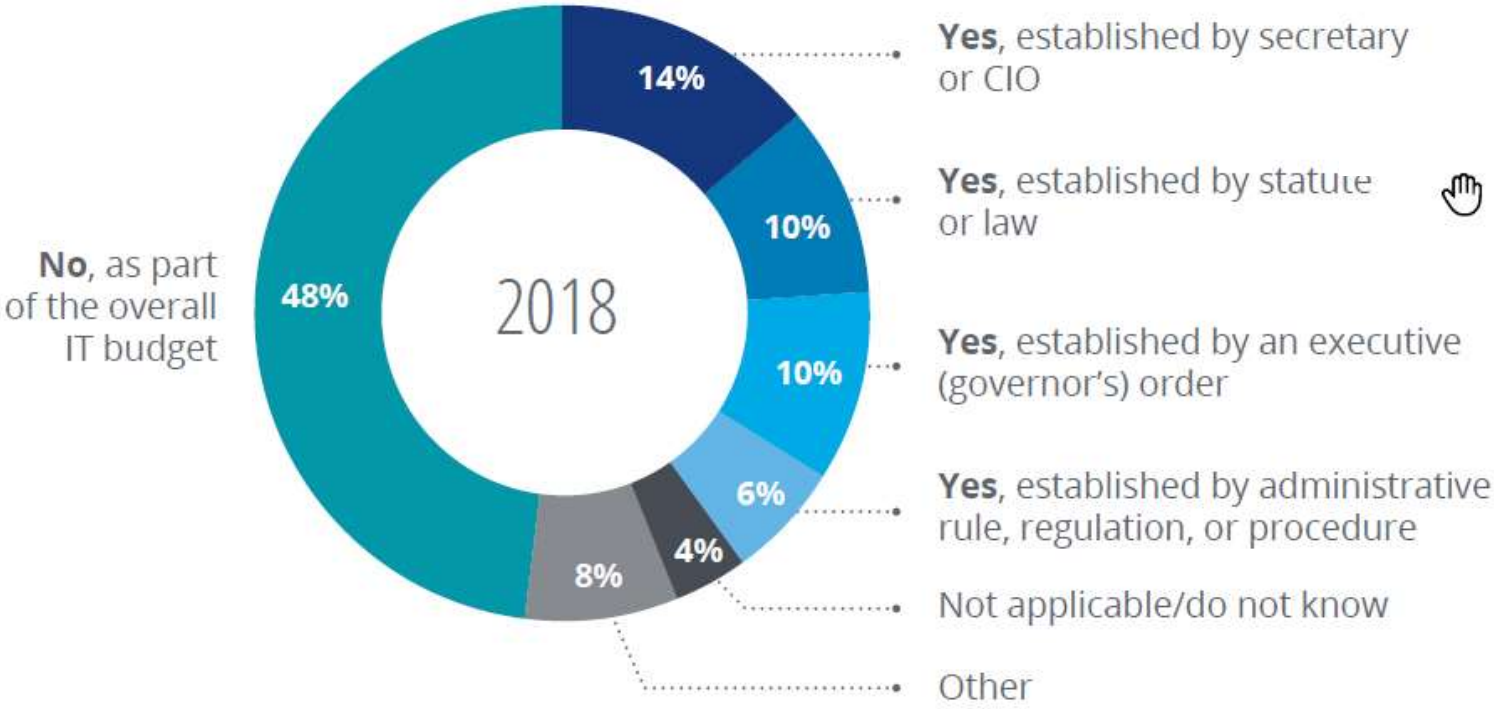
Most states only spend 0-3% of their IT budget on cybersecurity



Survey question: What percent of your state's enterprise IT budget is allocated to enterprise cybersecurity? (all executive branch agencies)

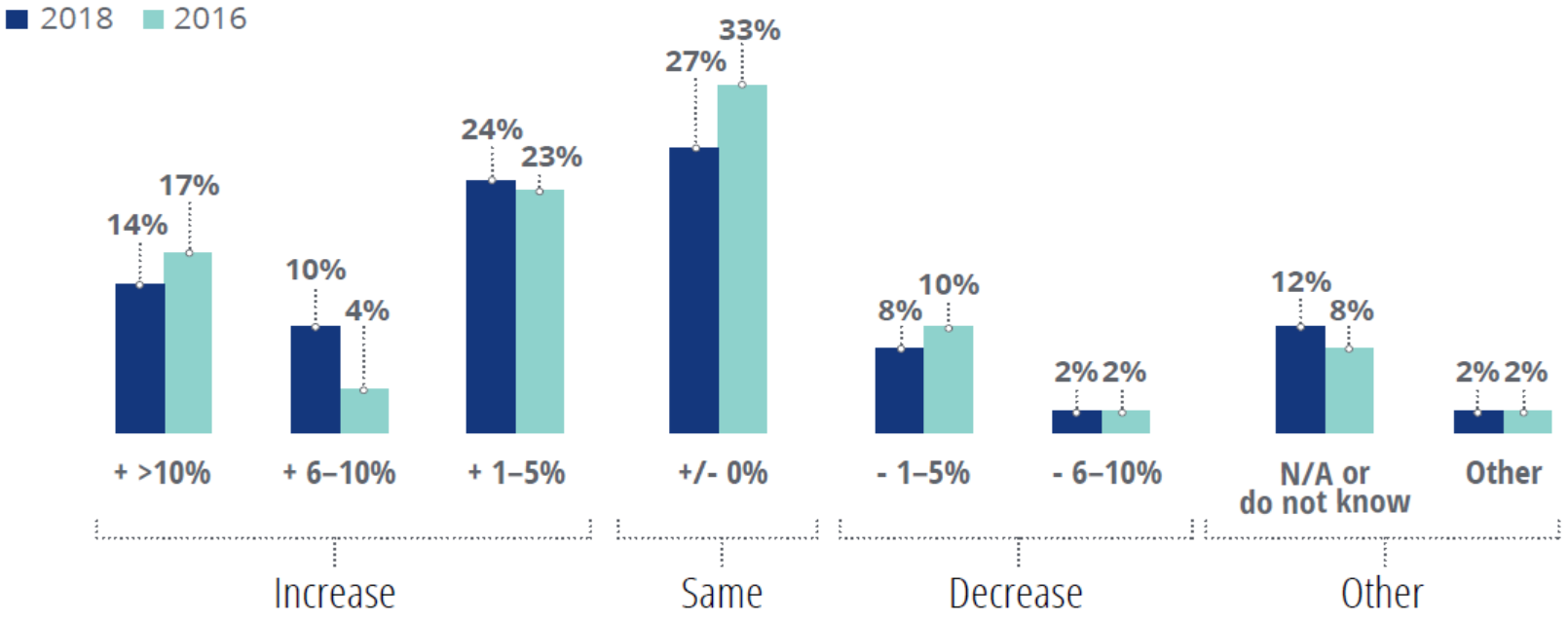
Budget Challenge

Almost half the states do not have a separate budget line item for cybersecurity



Budget Challenge

Cybersecurity budgets are growing, but very slowly

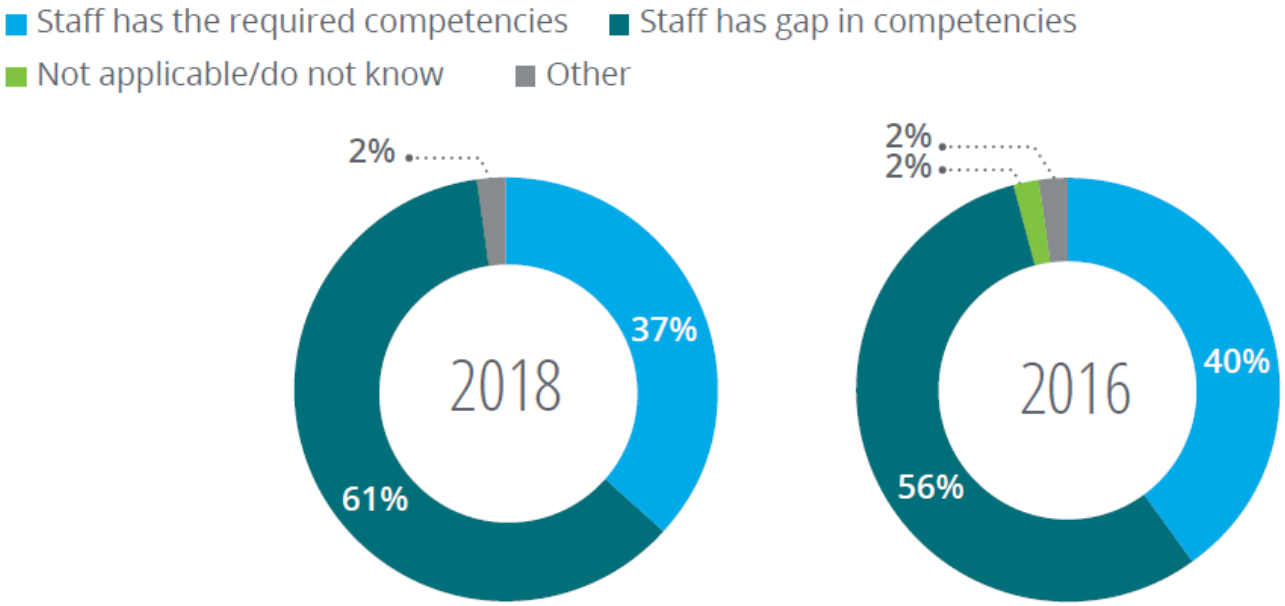


Survey question: Characterize the year-over-year trending in your state's cybersecurity budget for years 2016 and 2017. (49 respondents)

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Talent Crisis

Thirty state CISOs acknowledge they face a cyber competency gap



Survey question: Do your internal cybersecurity professionals have the required competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements? (49 respondents)

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Talent crisis

Top barriers to hiring, developing and retaining cyber talent

94% State's salary rates and paygrade structures

51% Workforce leaving for private sector careers

47% Lack of qualified candidates due to demand from federal agencies and private sector

24% Work location—lack of qualified cyber workforce in the state capital

18% Outdated classifications and job descriptions for cybersecurity positions

12% Lack of a defined career path and opportunities in cybersecurity

12% Lengthy hiring process

Survey question: What are the top three human resource factors that negatively impact your ability to develop, support, and maintain the cybersecurity workforce within your state? (49 respondents)

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Three Bold Plays for Change

1 ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING

CISOs should raise cybersecurity's visibility with the state legislature and executive branch by making it a line item in the IT budget. They can also seek funding from federal agencies to support compliance with those agencies' security mandates.

2 CISOs AS AN ENABLER OF INNOVATION, NOT A BARRIER

CISOs should actively participate in shaping the state's innovation agenda, collaborate with state digital and innovation officers, and lead the charge to help program leaders securely adopt new technologies.

3 TEAM WITH THE PRIVATE SECTOR AND HIGHER EDUCATION

CISOs should leverage public-private partnerships and collaborations with local colleges and universities to provide a pipeline of new talent, as well as consider outsourcing to private-sector firms.