Deloitte. Insights

NASCIO Representing Chief Information Officers of the States

2018 Deloitte-NASCIO Cybersecurity Study

States at risk: Bold plays for change

A JOINT REPORT FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

Highlights from the 2018 Deloitte-NASCIO Cyber Study

November 13, 2018

NASCIO Representing Chief Information Officers of the States

Speakers

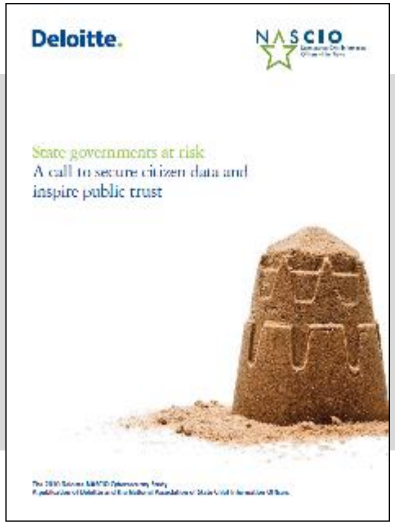
Debbi Blyth
CISO,
State of Colorado

Srini Subramanian
Principal, Deloitte Risk &
Financial Advisory,
Deloitte & Touche LLP

Doug Robinson
Executive Director,
NASCIO

Timeline of the Deloitte – NASCIO Cybersecurity Study States at Risk

2010



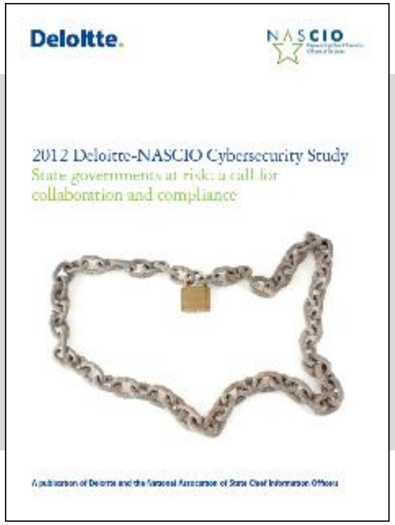
Deloitte.

State governments at risk
A call to secure citizen data and inspire public trust

The 2010 Deloitte-NASCIO Cybersecurity Study
A publication of Deloitte and the National Association of State Chief Information Officers

A call to secure citizen data and inspire trust

2012



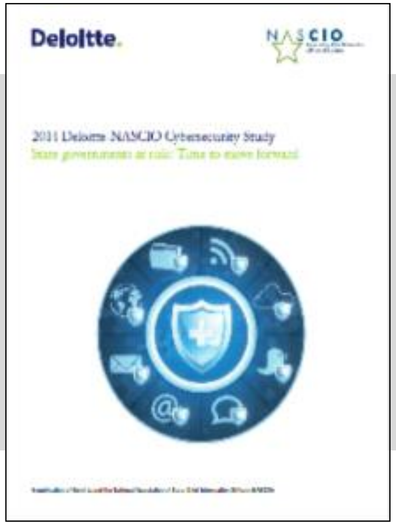
Deloitte.

2012 Deloitte-NASCIO Cybersecurity Study
State governments at risk: a call for collaboration and compliance

A publication of Deloitte and the National Association of State Chief Information Officers

A call for collaboration and compliance

2014

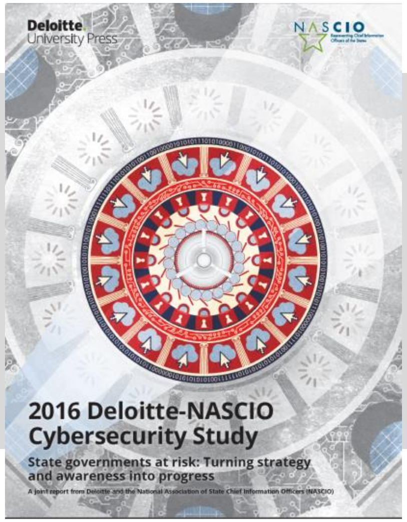


Deloitte.

2014 Deloitte-NASCIO Cybersecurity Study
State governments at risk: Time to move forward

Time to move forward

2016



Deloitte.
University Press

2016 Deloitte-NASCIO Cybersecurity Study
State governments at risk: Turning strategy and awareness into progress
A joint report from Deloitte and the National Association of State Chief Information Officers (NASCIO)

Turning strategy and awareness into progress

2018

Deloitte.
Insights

2018 Deloitte-NASCIO Cybersecurity Study
States at risk: Bold plays for change
A JOINT REPORT FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

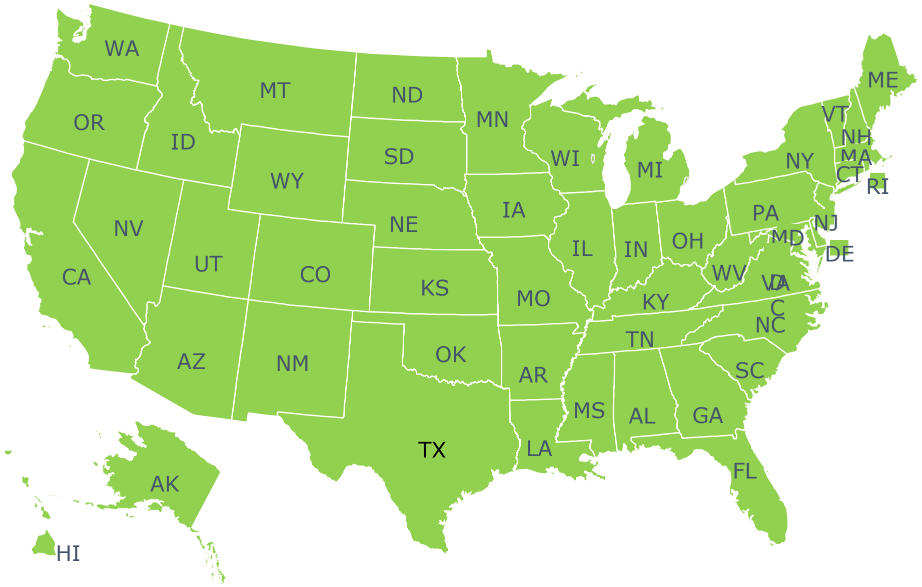
Bold plays for change

States at Risk

Chief Information Security Officer (CISO) Survey Profile

- US state enterprise-level CISOs, with additional input from agency CISOs and security staff members within state governments.

- CISO participants answered 56 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs.



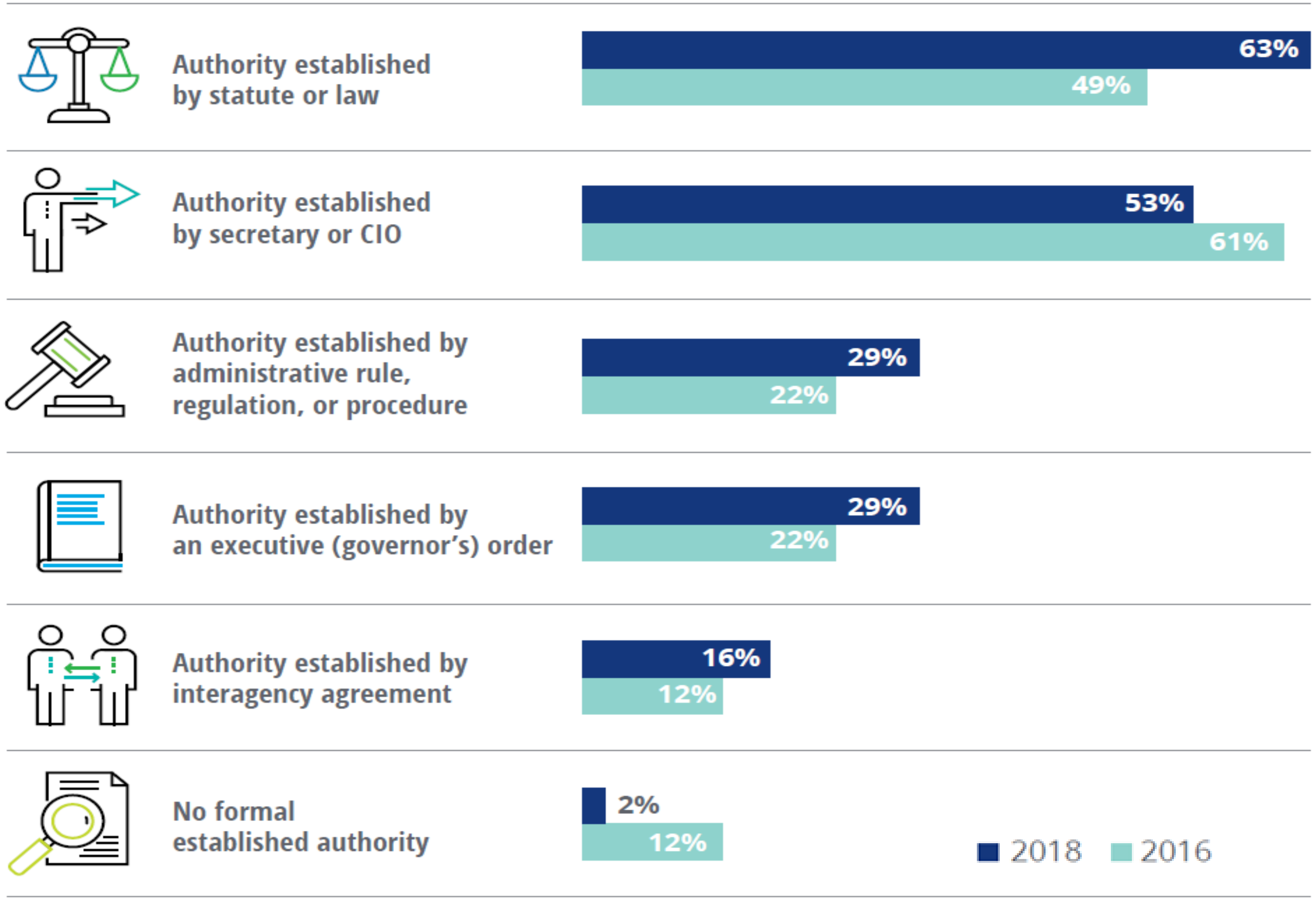
- Survey responses were received from all the **50** states.

Agenda

- Overview - CISOs have an executive platform
- Persistent challenges remain
- **Bold Plays** - States need bold actions to accelerate change
- Detailed data chart samples

CISOs have an executive leadership platform

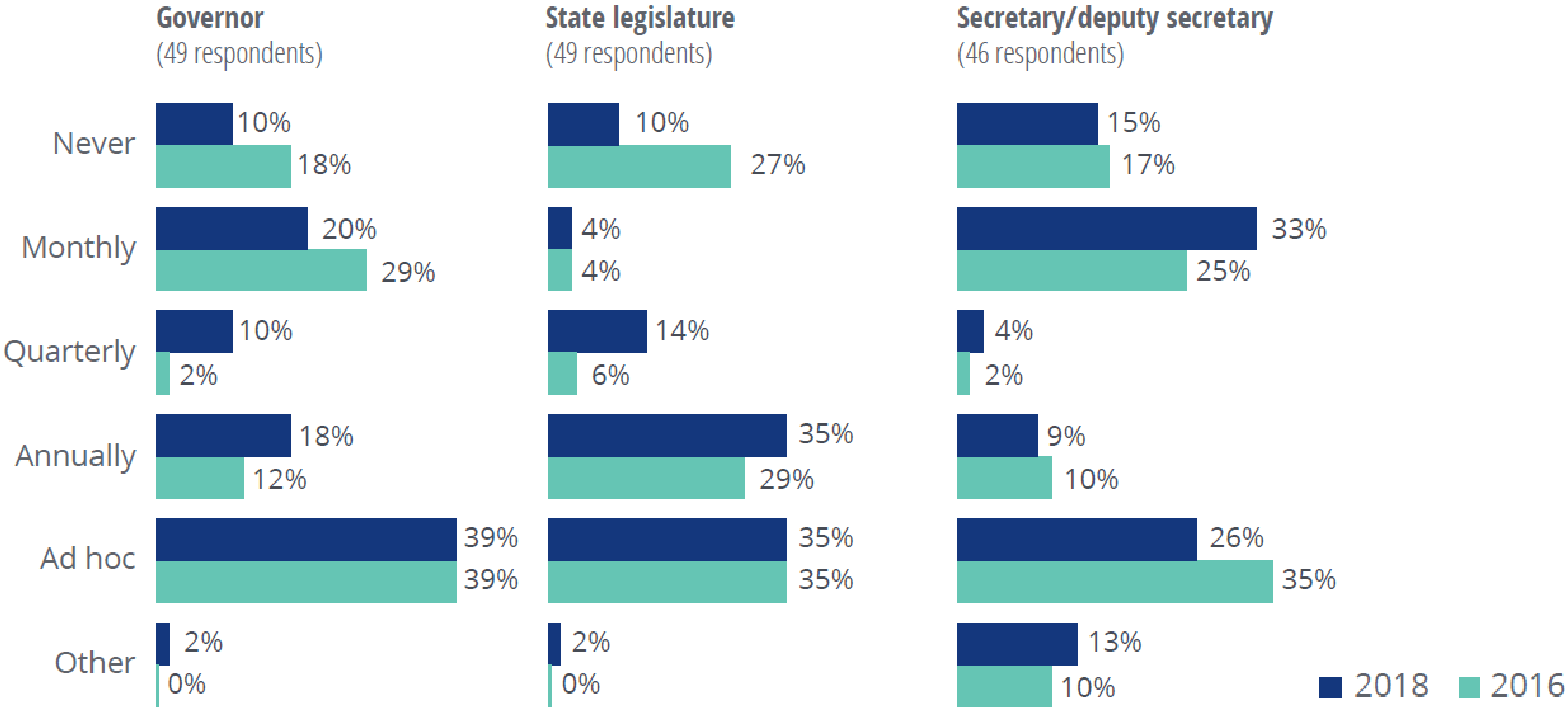
CISO role is firmly established, increasingly through legislation



Survey question: What mechanism establishes your state's CISO or equivalent position's authority over the other organizational entities for which it has responsibility? (49 respondents)

CISOs have an executive leadership platform

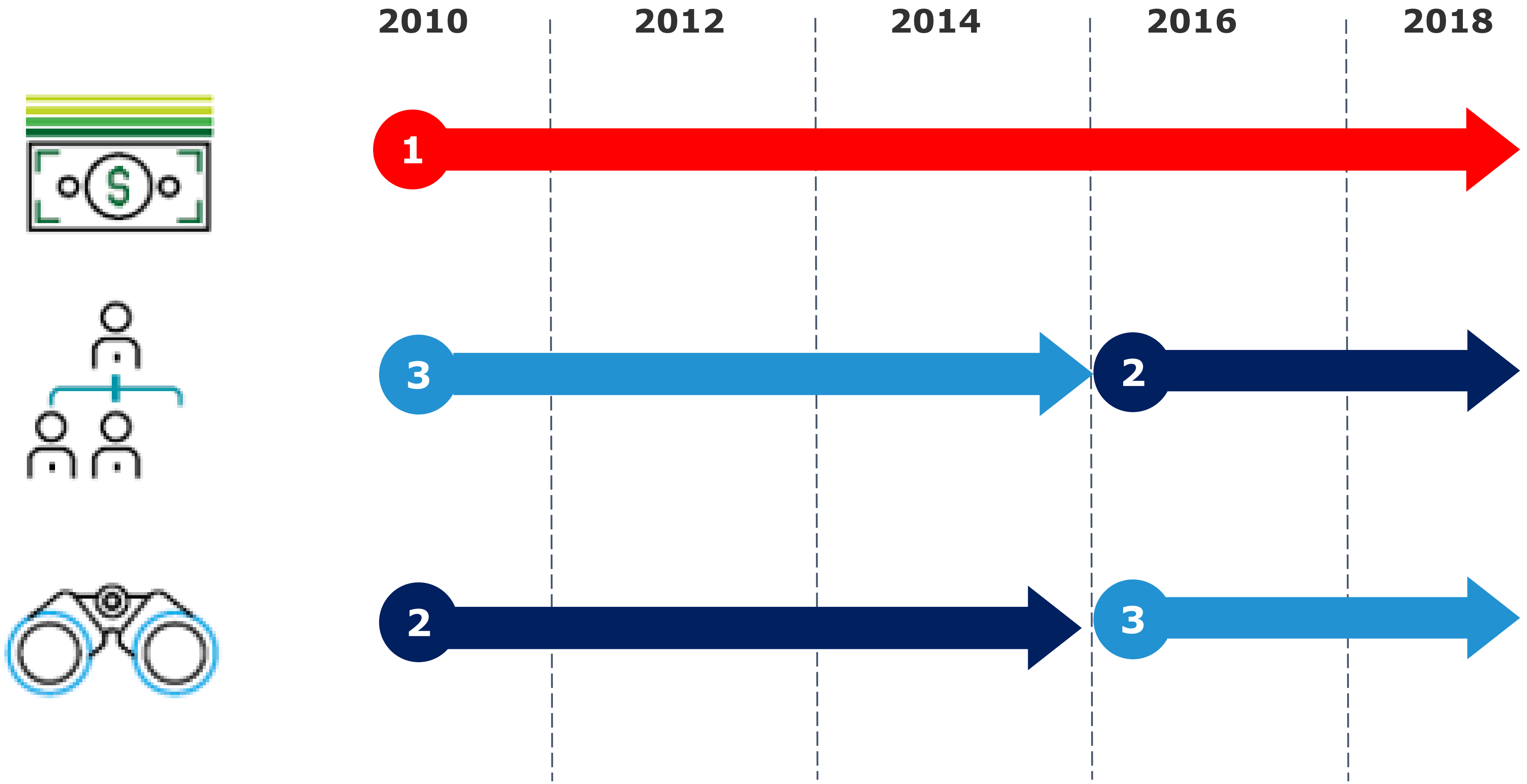
CISOs are improving reporting cadence to state leadership



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

However, top challenges remain

Budget, talent, and threats top three since 2010



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

CISOs have an executive leadership platform

Yet, top challenges persist

Deloitte.
Insights

NASCIO
Representing Chief Information
Officers of the States

2018 Deloitte-NASCIO
Cybersecurity Study

States at risk: Bold plays for change

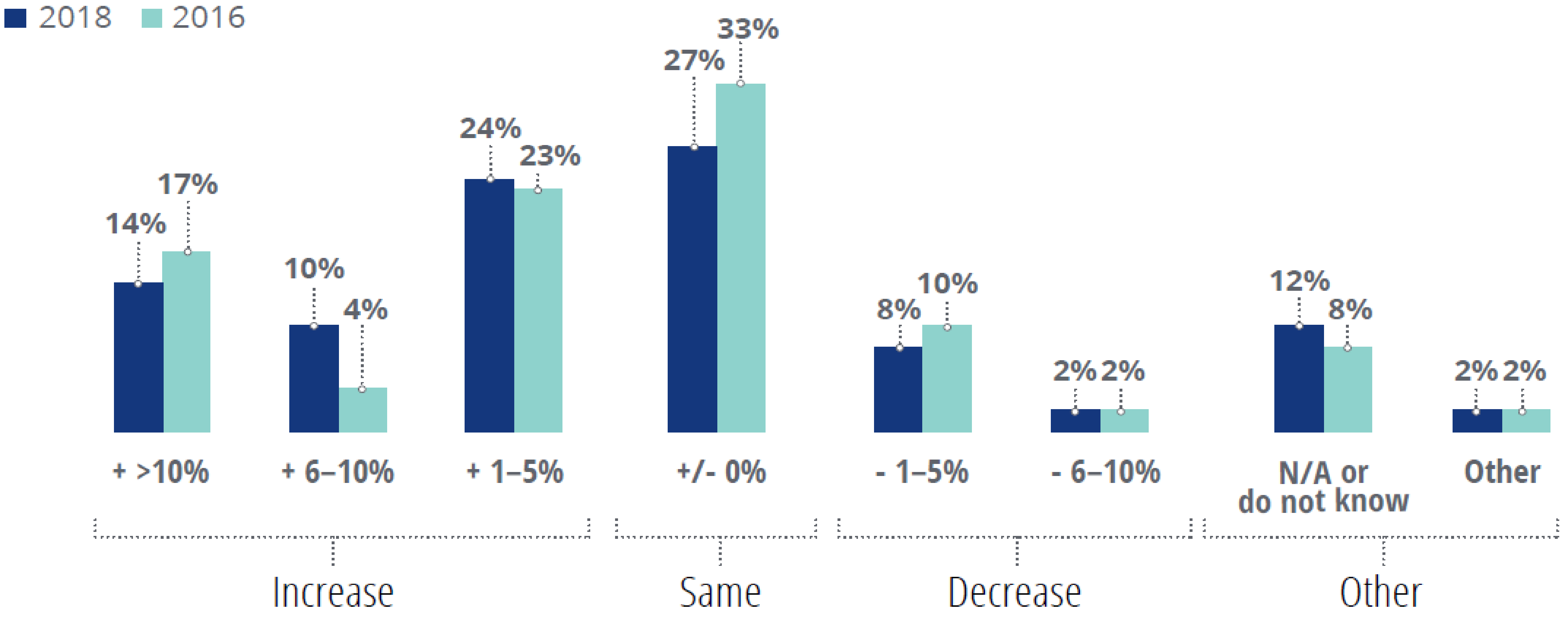
A JOINT REPORT FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

Bold Plays

States need bold actions to accelerate change

Budget challenge

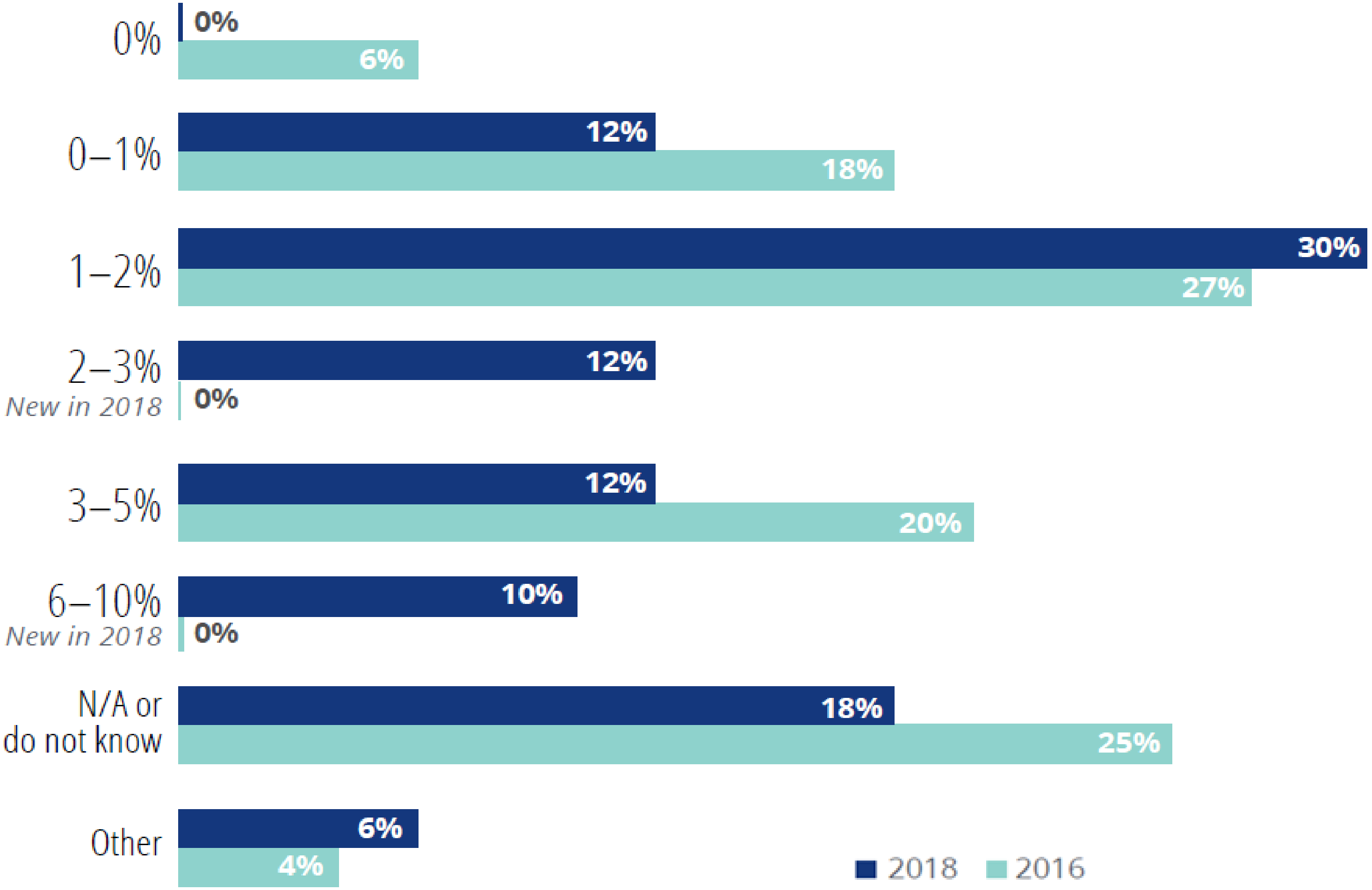
Cybersecurity budgets are growing, but very slowly



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

Budget challenge

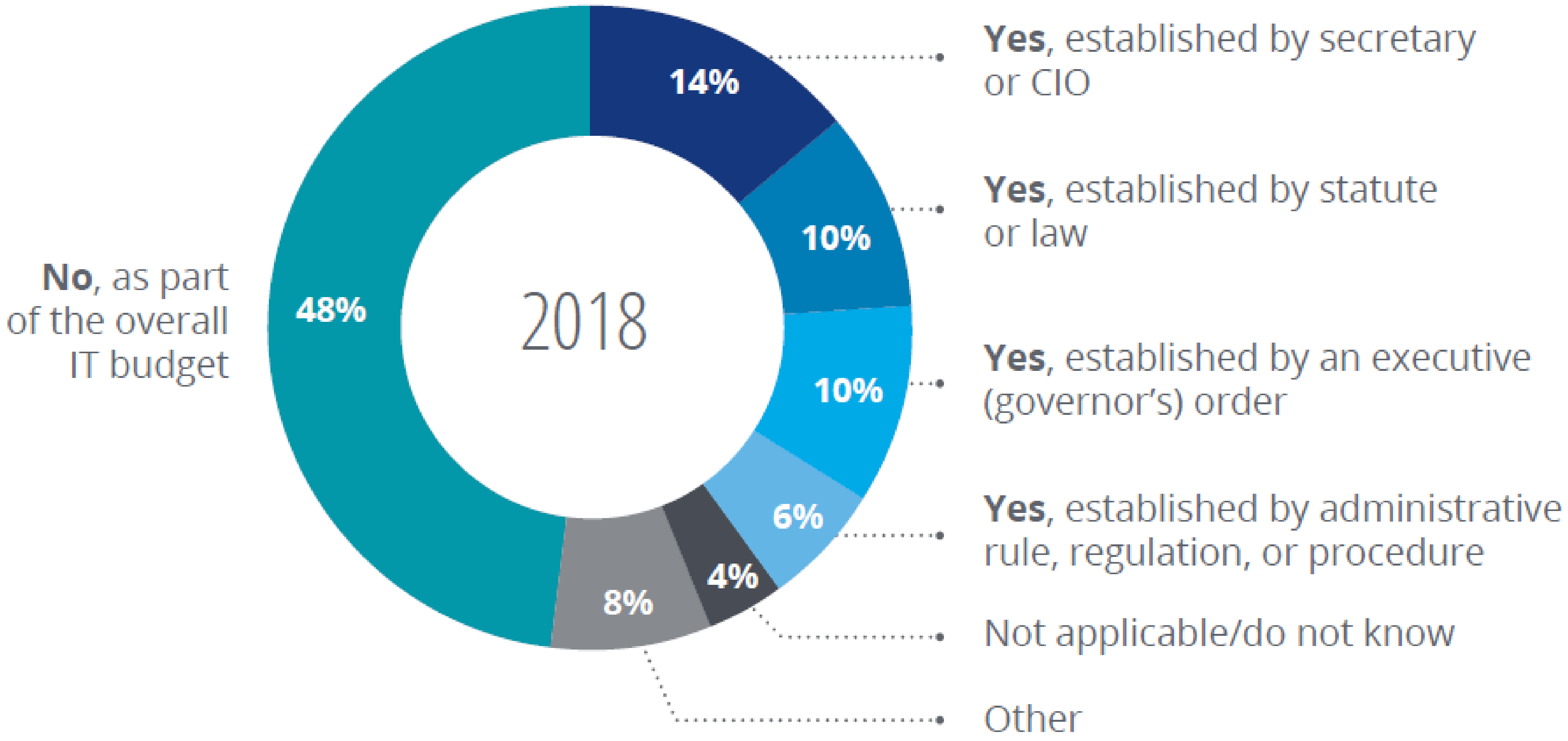
Most states only spend 0-3% of their IT budget on cybersecurity



Survey question: What percent of your state's enterprise IT budget is allocated to enterprise cybersecurity? (all executive branch agencies) (50 respondents)

Budget challenge

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



Survey question: Does your state have a cybersecurity budget line item? (50 respondents)

Budget challenge

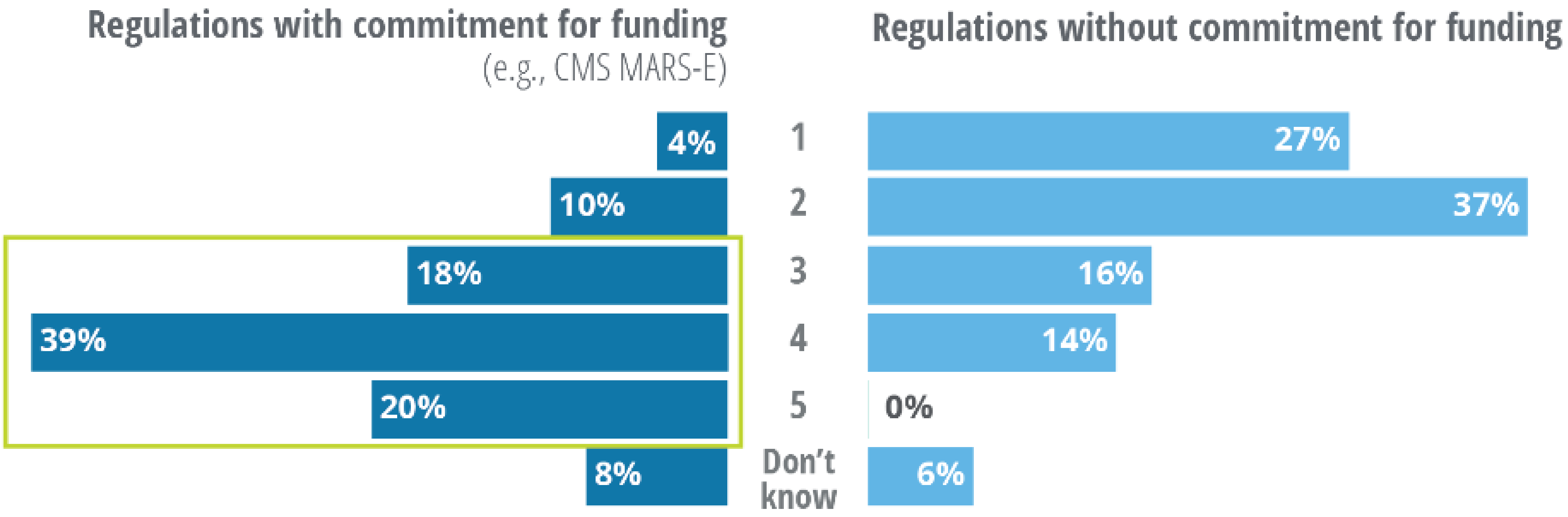
Federal agencies have dedicated cyber budget, and are (arguably) better funded

Federal agencies' cybersecurity budget as a percentage of total IT budget and year-over-year growth

		2017	2018	2019
Department of Transportation	Percentage of IT budget	4.48%	5.10%	5.63%
	Year-over-year increase	N/A	13.76%	10.54%
Health and Human Services	Percentage of IT budget	5.45%	5.44%	6.44%
	Year-over-year increase	N/A	-0.15%	18.5%
Social Security	Percentage of IT budget	8.59%	10.94%	11.4%
	Year-over-year increase	N/A	27.34%	4.21%
Treasury	Percentage of IT budget	10.78%	11.67%	10.82%
	Year-over-year increase	N/A	8.17%	-7.23%
Justice	Percentage of IT budget	27.08%	25.24%	25.07%
	Year-over-year increase	N/A	-6.79%	-0.67%

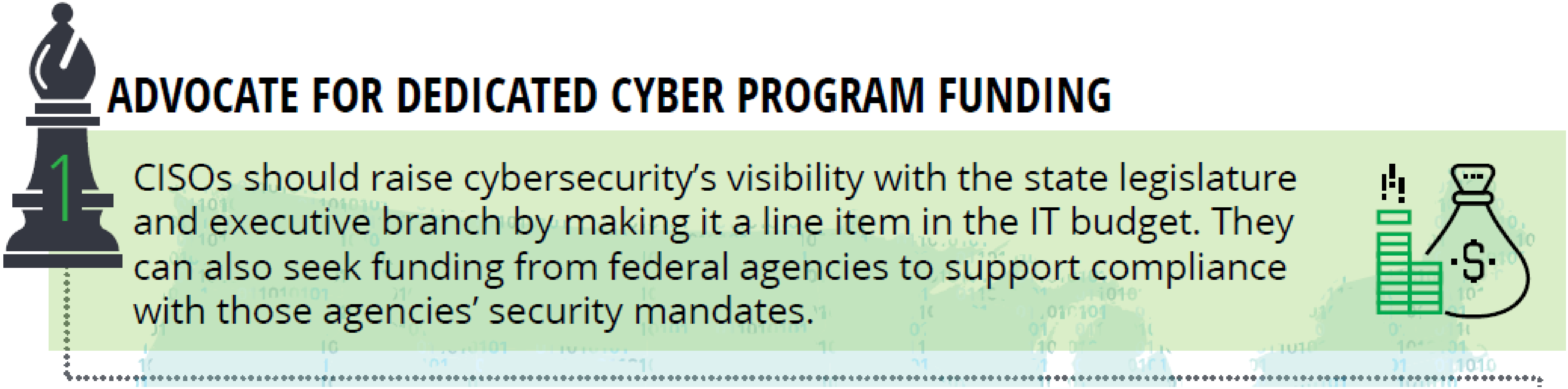
Budget challenge

Cybersecurity initiatives can be more effective with funding commitment



Survey question: How effective are applicable federal and state cybersecurity regulations at improving your state's cybersecurity posture and reducing risk? (1 = least effective, 5 = most effective) (49 respondents)

Bold Play #1:
Advocate for dedicated cyber program funding



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.

Top cybersecurity initiatives

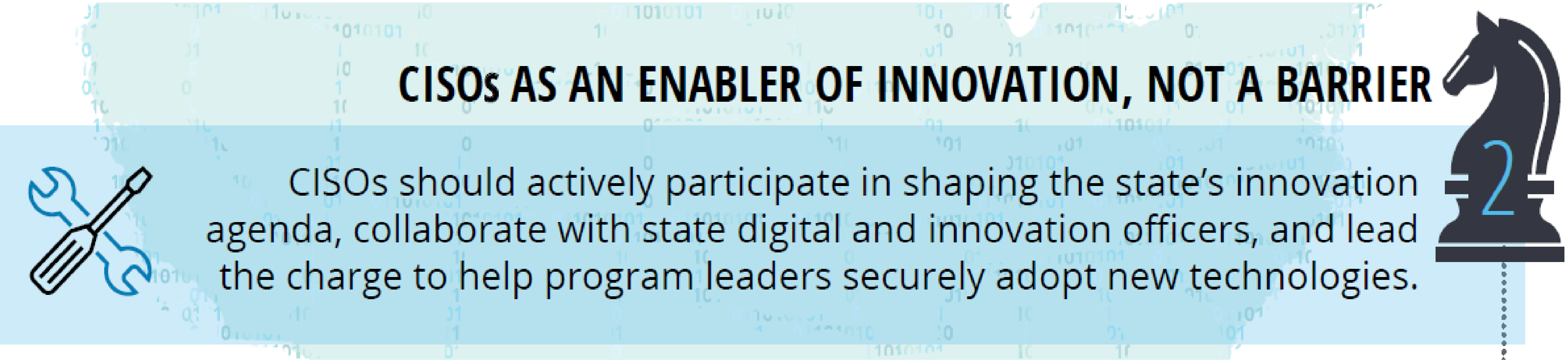
Innovation initiatives like AI, IOT, BlockChain, and Smart Government not on radar

36%	Risk assessment
36%	Metrics to measure and report effectiveness
36%	Training and awareness
34%	Cybersecurity strategy
30%	Cloud platform and solutions security

Citizen digital identity	6%
Robotics/automation/AI	4%
Internet of Things (IoT)	4%
BlockChain	0%
Smart Government	0%

Survey question: Identify your state's top five cybersecurity initiatives for 2018/2019. (50 respondents)

Bold Play#2:
CISOs as an enabler of innovation

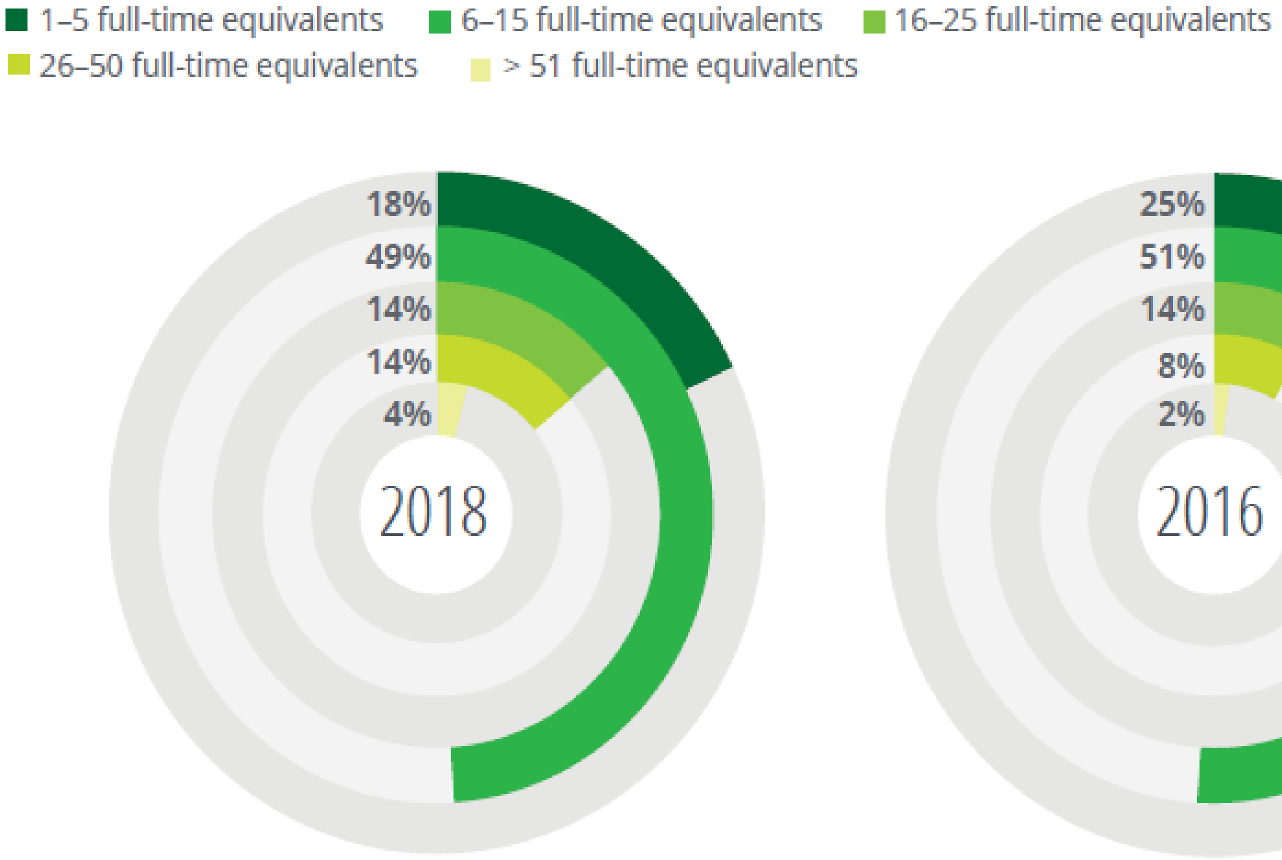


CISOs AS AN ENABLER OF INNOVATION, NOT A BARRIER

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.

Talent crisis

Most enterprise cybersecurity team consists of only 6-15 FTEs



1–5 FTE average

2010 state cyber FTE professionals

→

6–15 FTE average

2018 state cyber FTE professionals

Compared to

>100 FTE average

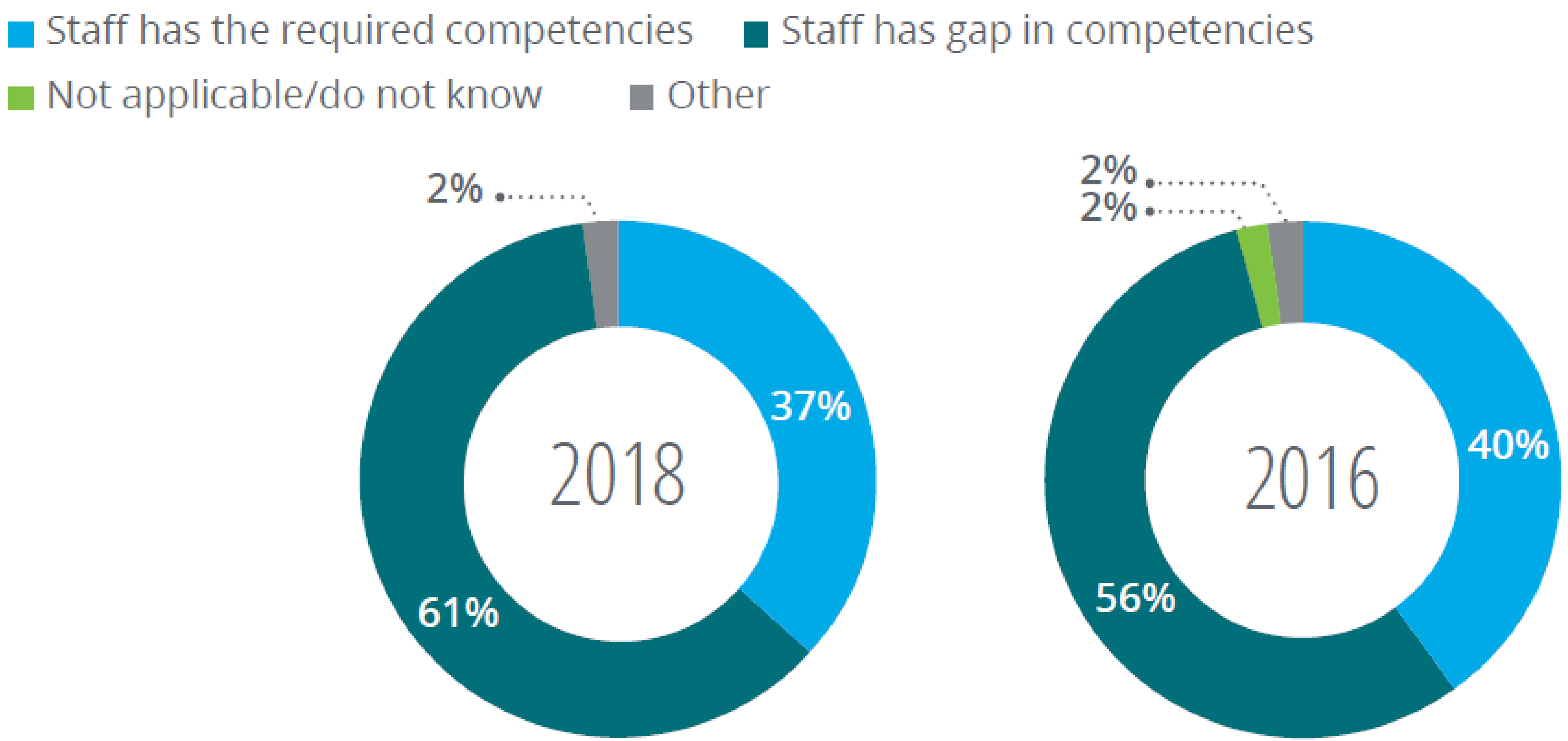
2010 financial services* cyber FTE professionals

Survey question: How many dedicated cybersecurity professionals does your enterprise security office employ? (49 respondents)

* Financial services institutions similar in size to an average state.

Talent crisis

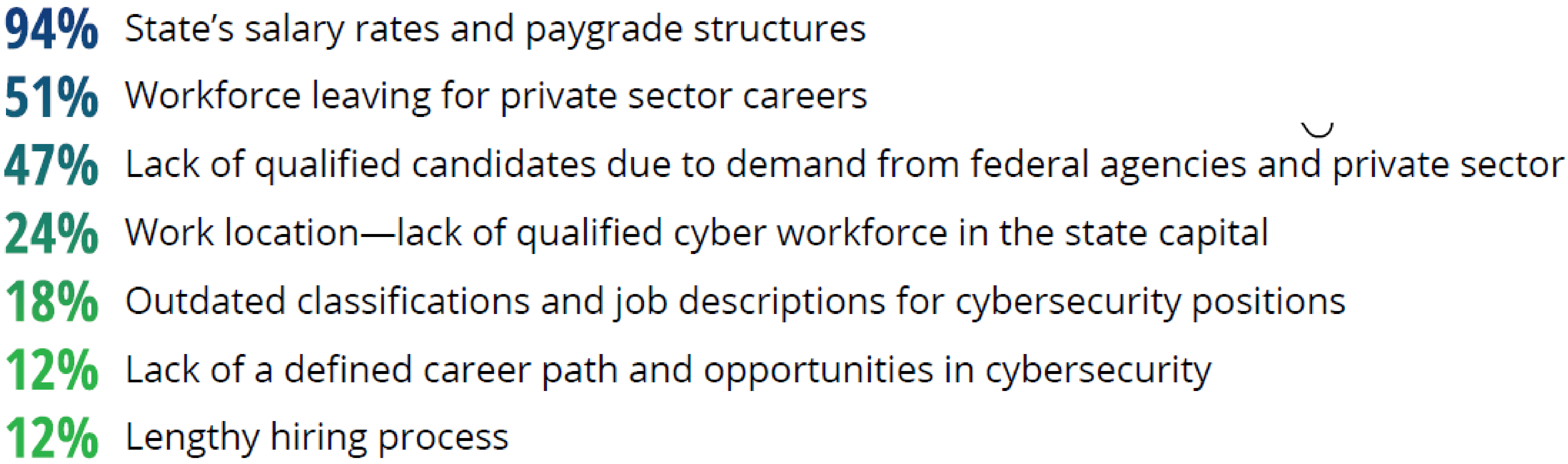
Thirty state CISOs acknowledge they face a cyber competency gap



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)

Talent crisis

Top barriers to hiring, developing and retaining cyber talent

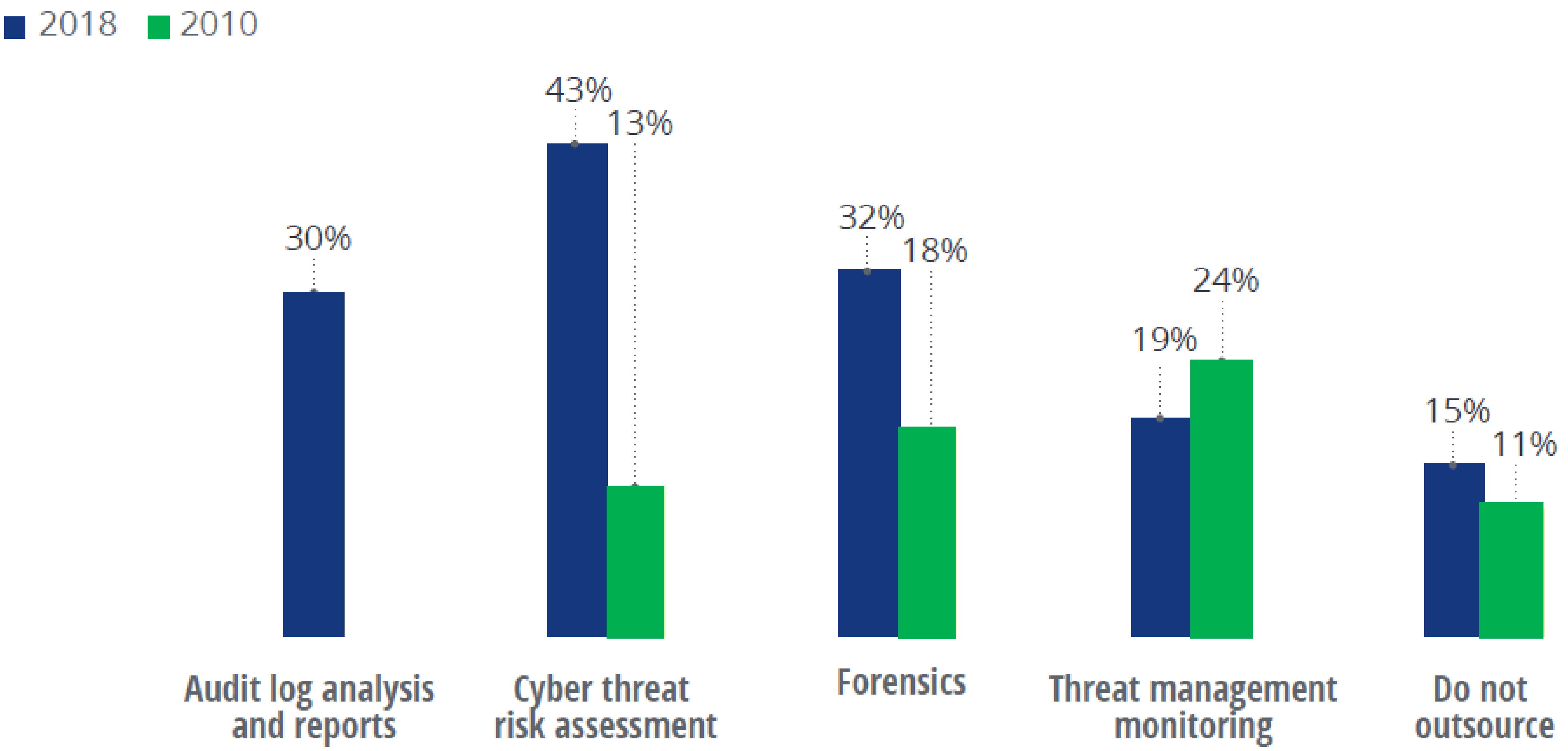


94%	State's salary rates and paygrade structures
51%	Workforce leaving for private sector careers
47%	Lack of qualified candidates due to demand from federal agencies and private sector
24%	Work location—lack of qualified cyber workforce in the state capital
18%	Outdated classifications and job descriptions 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)

Talent crisis

While outsourcing has increased for certain functions, more than half of US states have yet to outsource many of them



Survey question: Select the cybersecurity functions that your state outsources. (47 respondents)

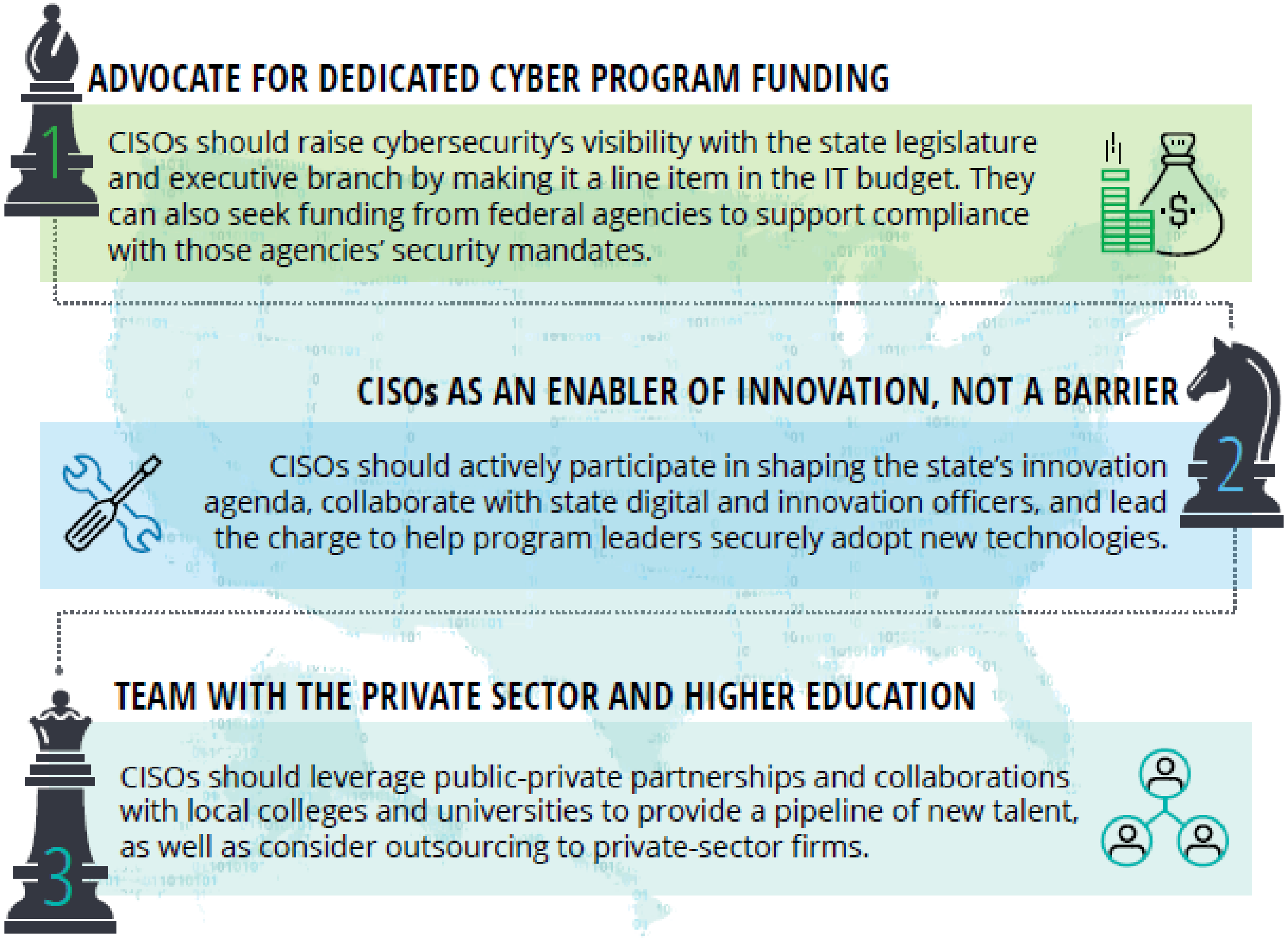
Bold Play#3:
Team with the Private Sector and Higher Education

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.

Bold Plays for Change

Summary



ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING

1

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.

CISOs AS AN ENABLER OF INNOVATION, NOT A BARRIER

2

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.

TEAM WITH THE PRIVATE SECTOR AND HIGHER EDUCATION

3

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.

Deloitte. Insights

NASCIO Representing Chief Information Officers of the States

2018 Deloitte-NASCIO Cybersecurity Study

States at risk: Bold plays for change

A JOINT REPORT FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

Security threats

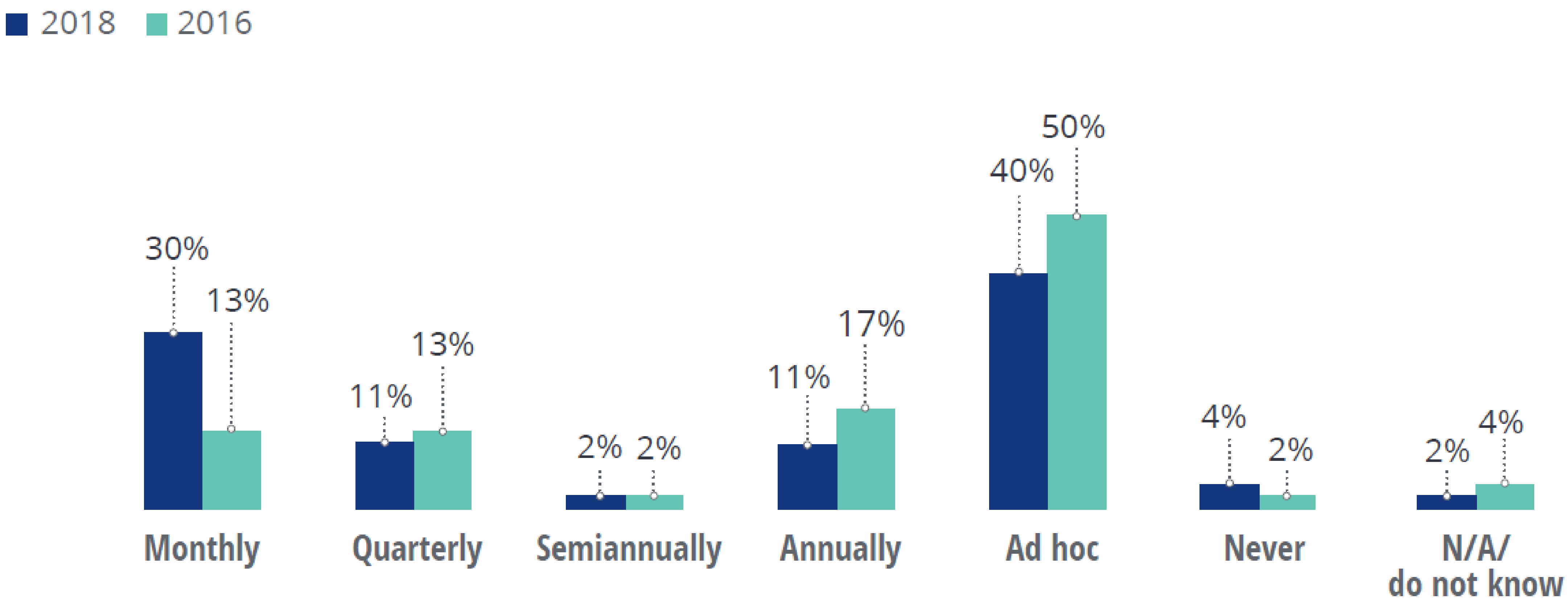
Web applications and malicious code are the leading sources of security breaches

	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

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

Security threats

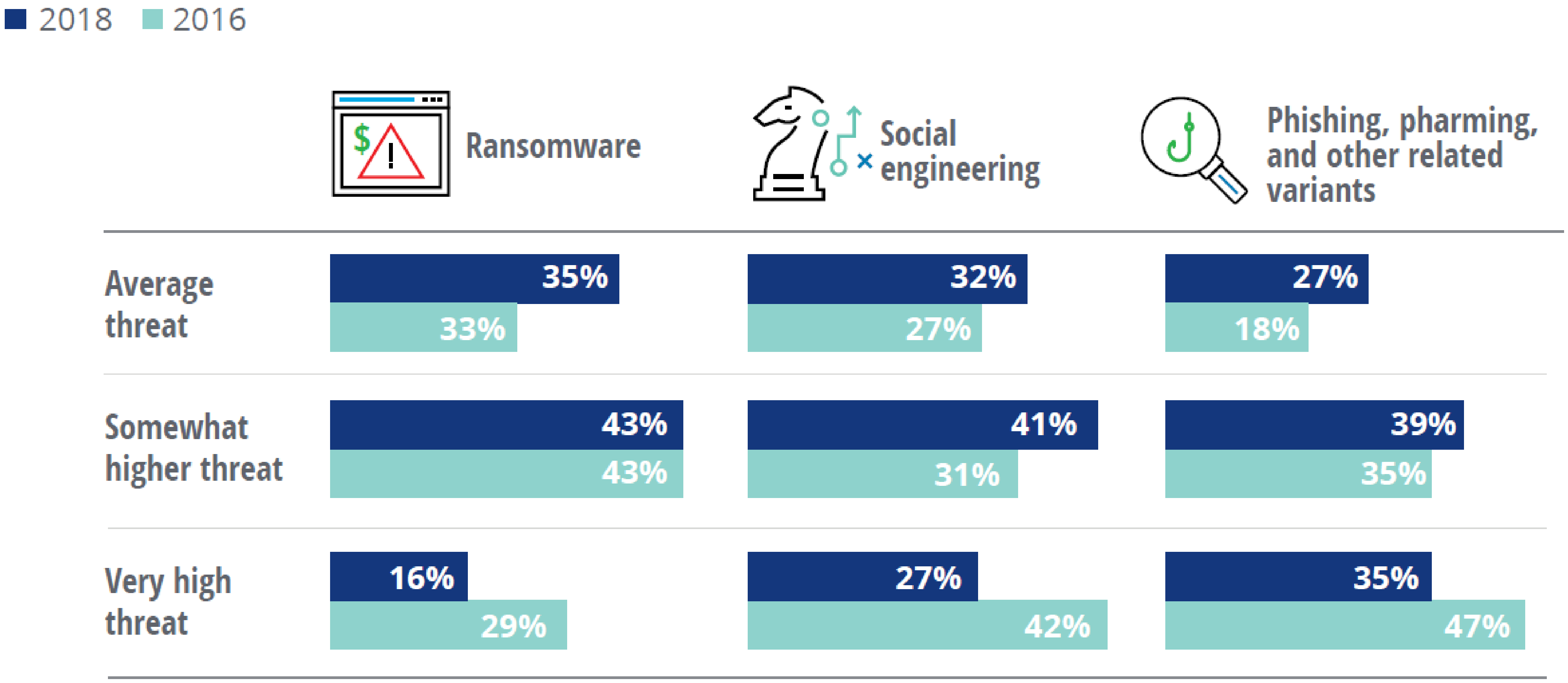
States have improved the frequency of application security testing



Survey question: How often does your state perform application security vulnerability testing and code review? (47 respondents)

Security threats

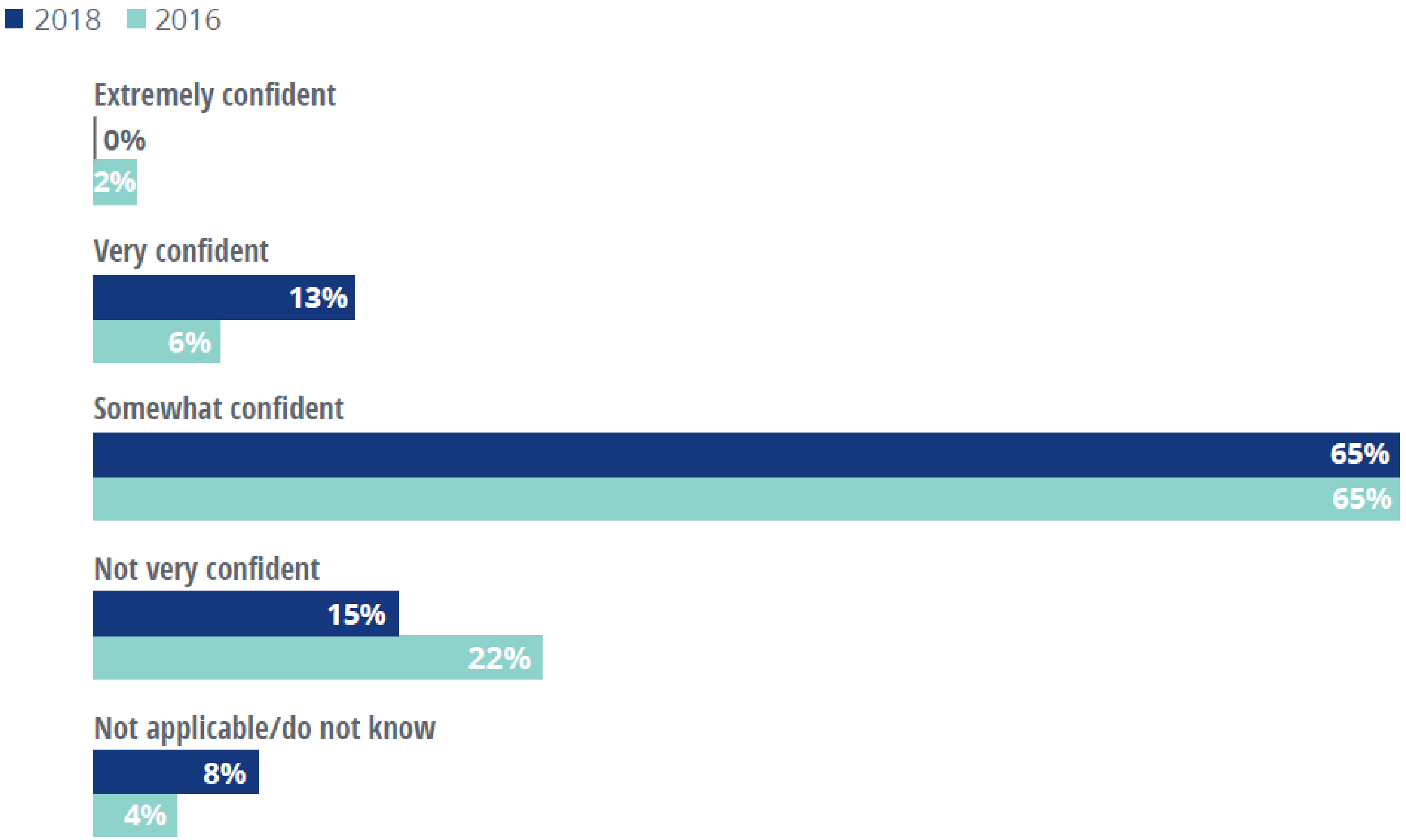
Ransomware, social engineering, and phishing are the top cyber threats for states



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

Confidence in third parties

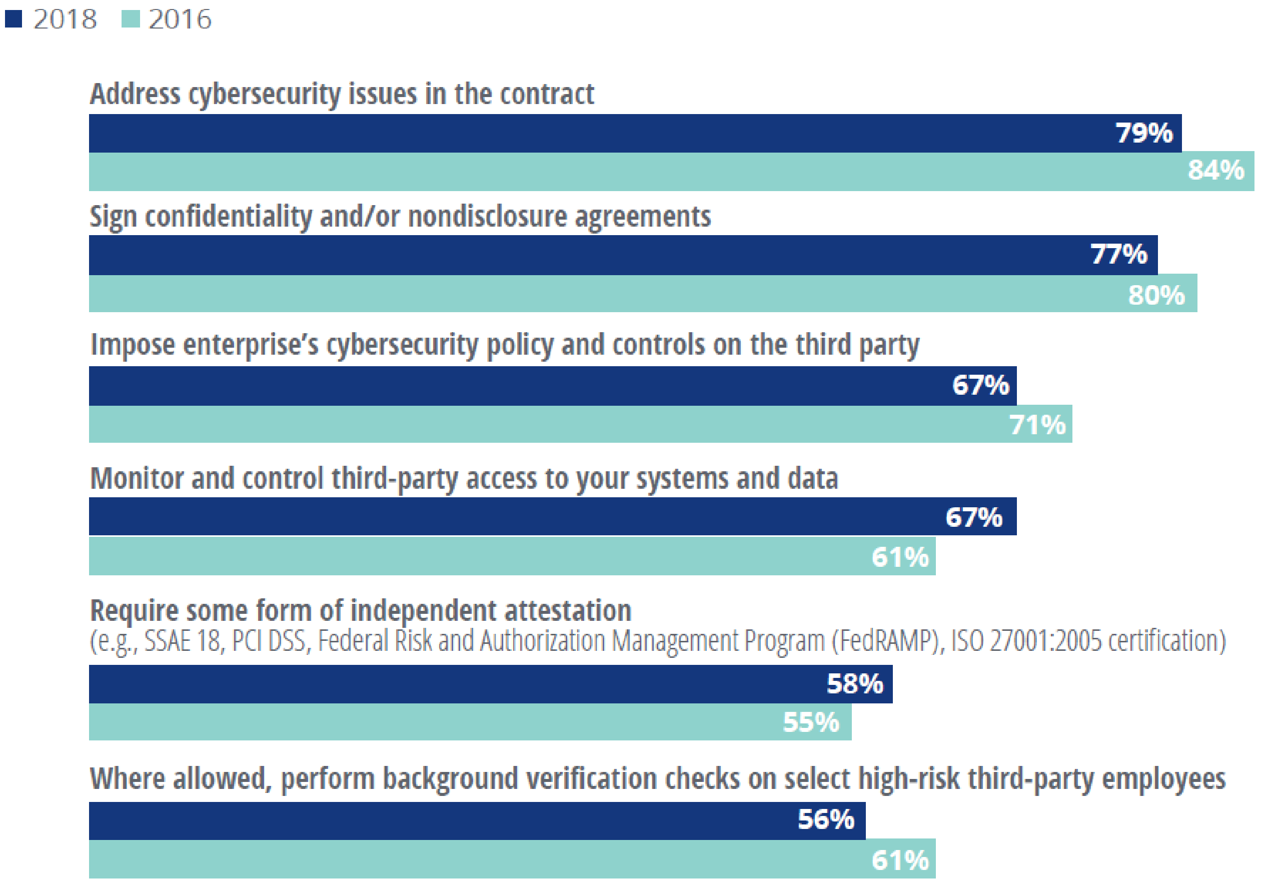
The majority of CISOs say that they are "somewhat confident" in their third parties' cybersecurity practices



Survey question: How confident are you in the cybersecurity practices of your third parties (contractors, service providers, business partners)? (48 respondents)

Confidence in third parties

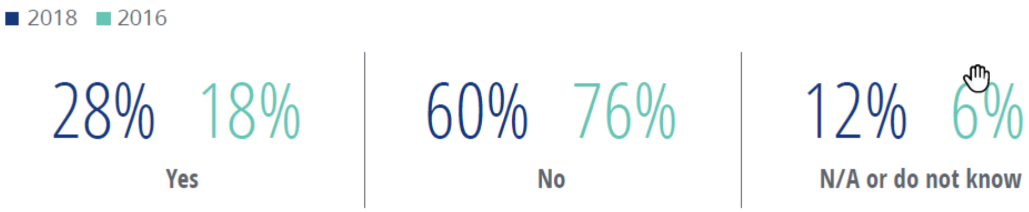
CISOs’ top options for managing the adequacy of third-party cybersecurity practices include contractual cybersecurity requirements and confidentiality/nondisclosure agreements



Survey question: How does your state manage the adequacy of third-party (contractor, service provider, business partner) cybersecurity practices? (48 respondents)

Privacy

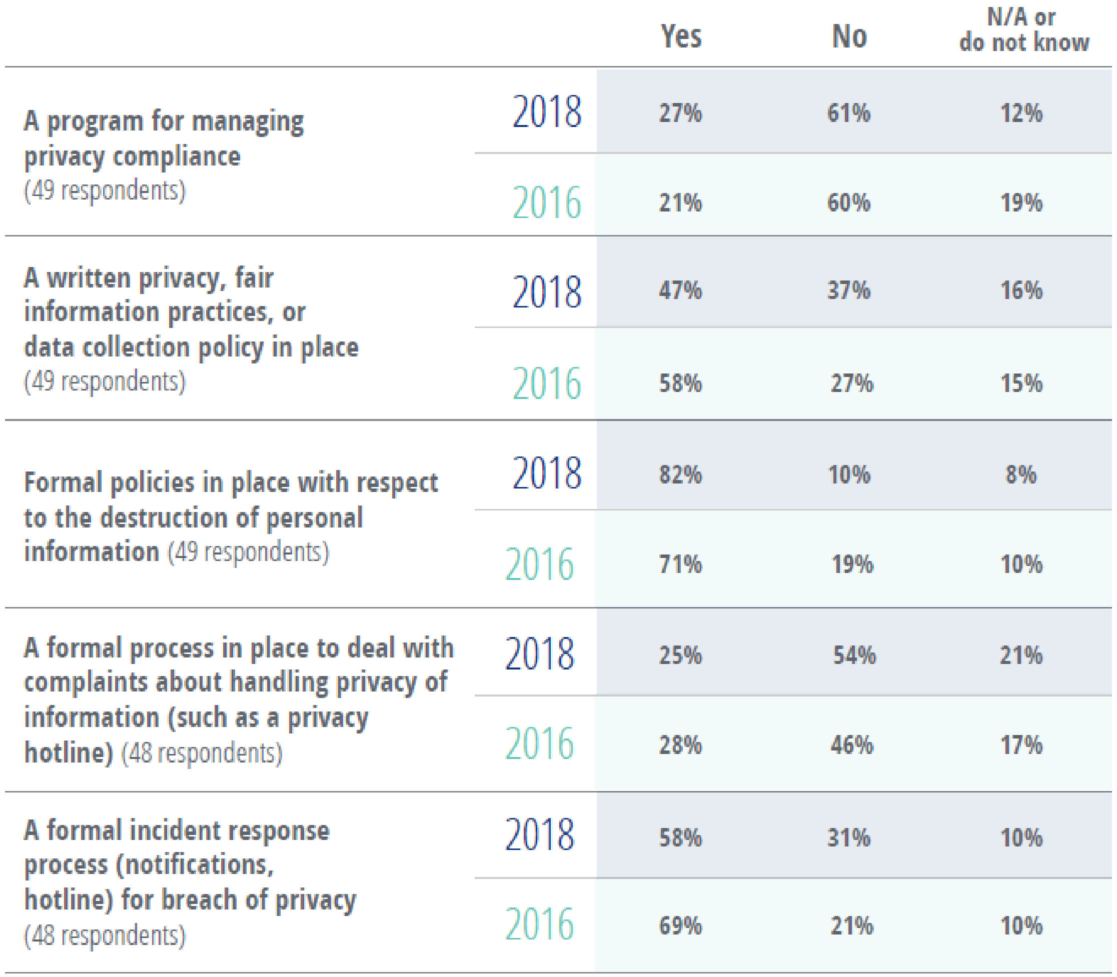
Only 14 states have a chief privacy officer; most states lack an enterprise program



■ 2018 ■ 2016

	2018	2016
Yes	28%	18%
No	60%	76%
N/A or do not know	12%	6%

Does your state have an enterprise-level chief privacy officer? (50 respondents)

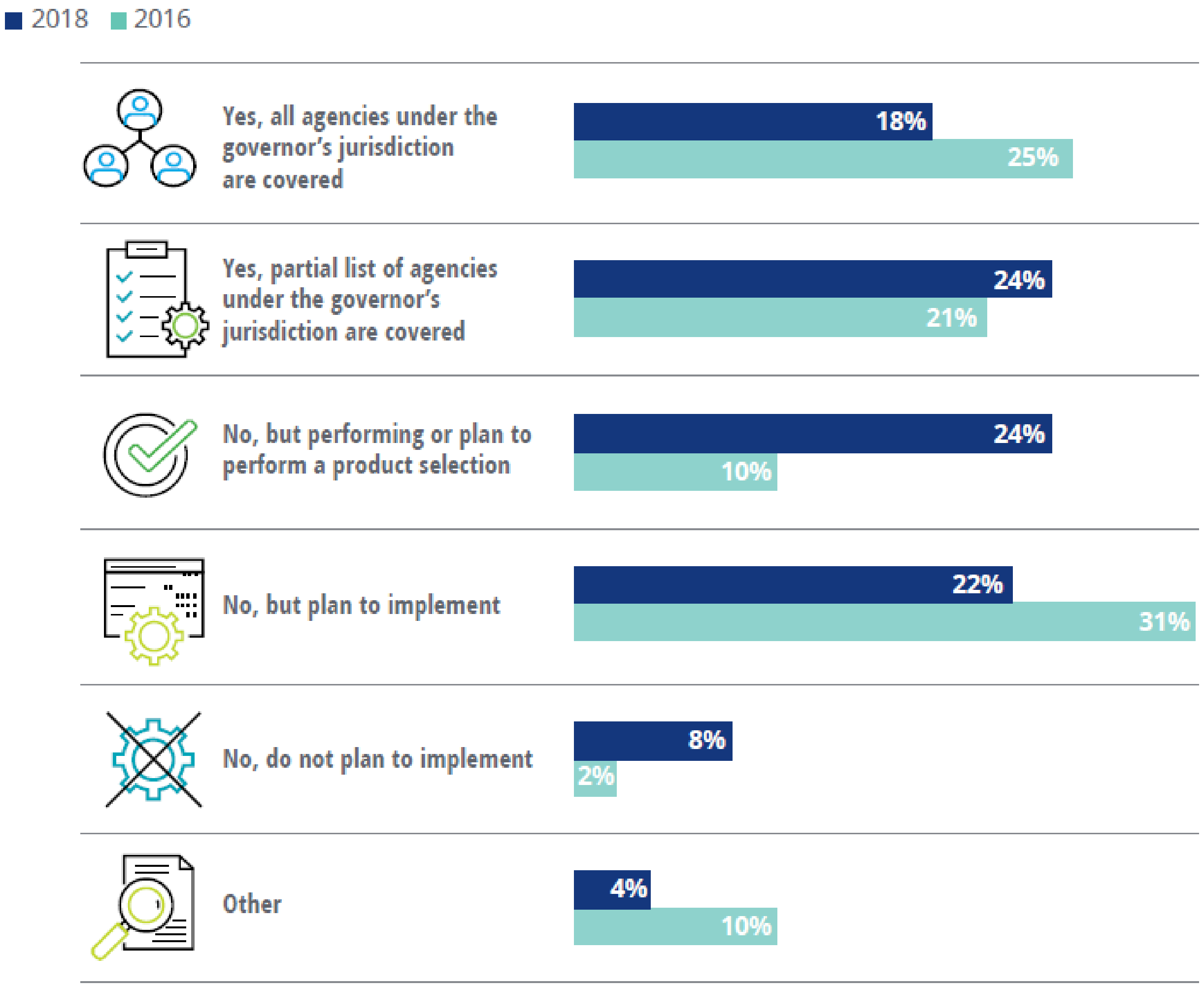


		Yes	No	N/A or do not know
A program for managing privacy compliance (49 respondents)	2018	27%	61%	12%
	2016	21%	60%	19%
A written privacy, fair information practices, or data collection policy in place (49 respondents)	2018	47%	37%	16%
	2016	58%	27%	15%
Formal policies in place with respect to the destruction of personal information (49 respondents)	2018	82%	10%	8%
	2016	71%	19%	10%
A formal process in place to deal with complaints about handling privacy of information (such as a privacy hotline) (48 respondents)	2018	25%	54%	21%
	2016	28%	46%	17%
A formal incident response process (notifications, hotline) for breach of privacy (48 respondents)	2018	58%	31%	10%
	2016	69%	21%	10%

Survey question: Does your state have the following?

Identity Access Management (IAM)

Only 21 states have an enterprise IAM solution



Survey question: Does your state provide an enterprise wide IAM solution? (50 respondents)

About Deloitte

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte’s cyber risk services help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation, and performance objectives through proactive management of the associated cyber risks. Deloitte provides advisory, implementation, and managed cybersecurity services to help our government clients lead the way with a collaborative threat intelligence strategy. Deloitte’s demonstrated approach and methodology help our clients better align security investments with risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to deliver services in the face of cyber incidents.

The Deloitte Center for Government Insights produces groundbreaking research to help government solve its most complex problems. Through forums and immersive workshops, we engage with public officials on a journey of positive transformation, crystallizing insights to help them understand trends, overcome constraints, and expand the limits of what is possible.

For more information, visit www.deloitte.com or read about the Deloitte Center for Government Insights at www.deloitte.com/us/center-for-government-insights.

About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories, and District of Columbia. NASCIO’s mission is to foster government excellence through quality business practices, information management, and technology policy. NASCIO provides state CIOs and state 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. From national conferences to peer networking, research, publications, briefings, and government affairs, NASCIO is the premier network and resource for state CIOs.

For more information, visit www.nascio.org

Questions?

Deloitte.
Insights

NASCIO
Representing Chief Information Officers of the States

2018 Deloitte-NASCIO Cybersecurity Study

States at risk: Bold plays for change

A JOINT REPORT FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

NASCIO.org/stateofcyber

NASCIO
Representing Chief Information Officers of the States

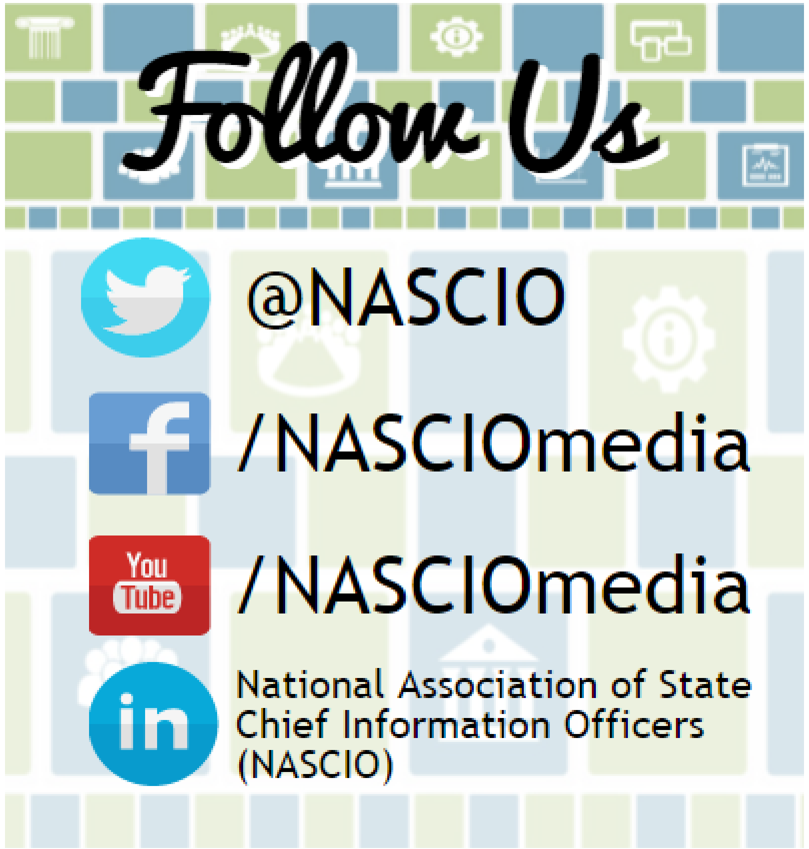
Contact Information

Debbi Blyth
Chief Information Security Officer
State of Colorado
deborah.blyth@state.co.us

Doug Robinson
Executive Director,
NASCIO
drobinson@nascio.org

Srini Subramanian
Principal, Deloitte Risk & Financial Advisory,
Deloitte & Touche LLP
ssubramanian@deloitte.com

Meredith Ward
Senior Policy Analyst,
NASCIO
mward@nascio.org



Follow Us

@NASCIO

/NASCIOmedia

/NASCIOmedia

National Association of State Chief Information Officers (NASCIO)