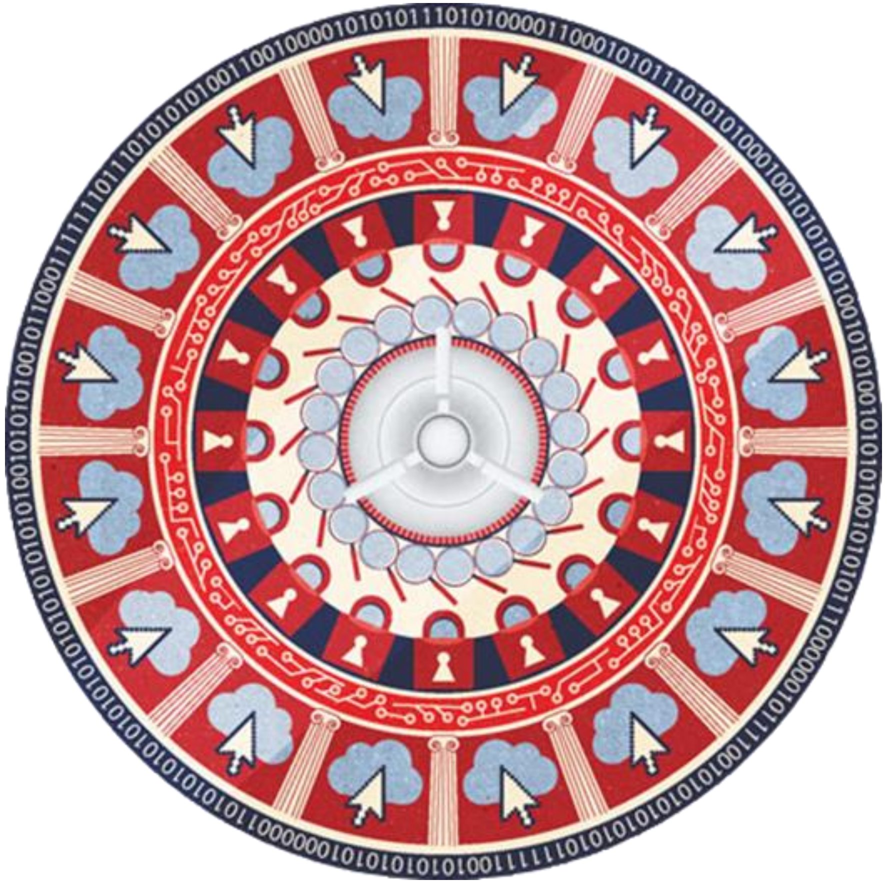
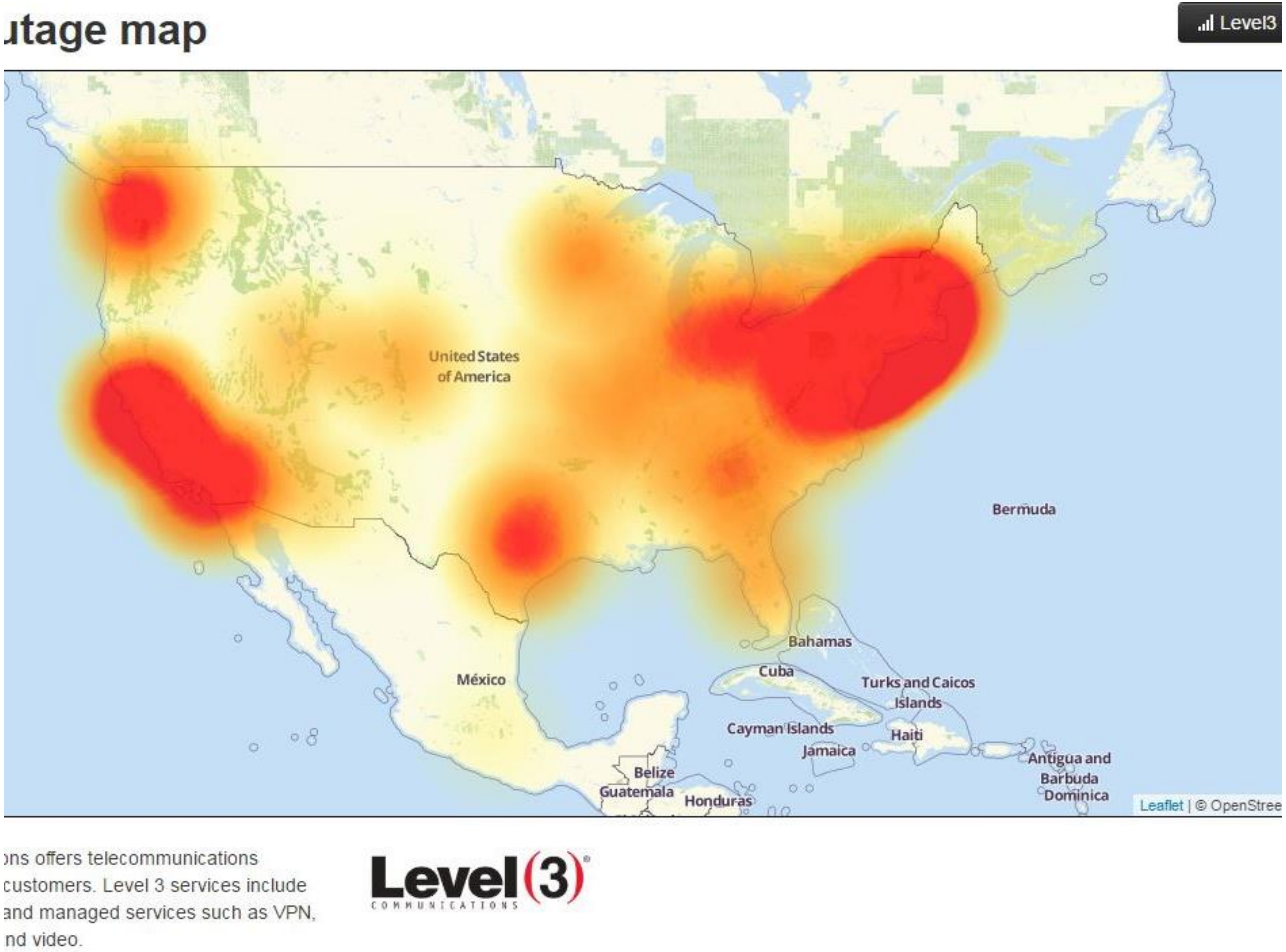
Joint NASCIO-NCSL Cybersecurity Webinar



NASCIO
Representing Chief Information Officers of the States

NCSL
National Conference of State Legislatures



utage map

ons offers telecommunications
customers. Level 3 services include
and managed services such as VPN,
nd video.

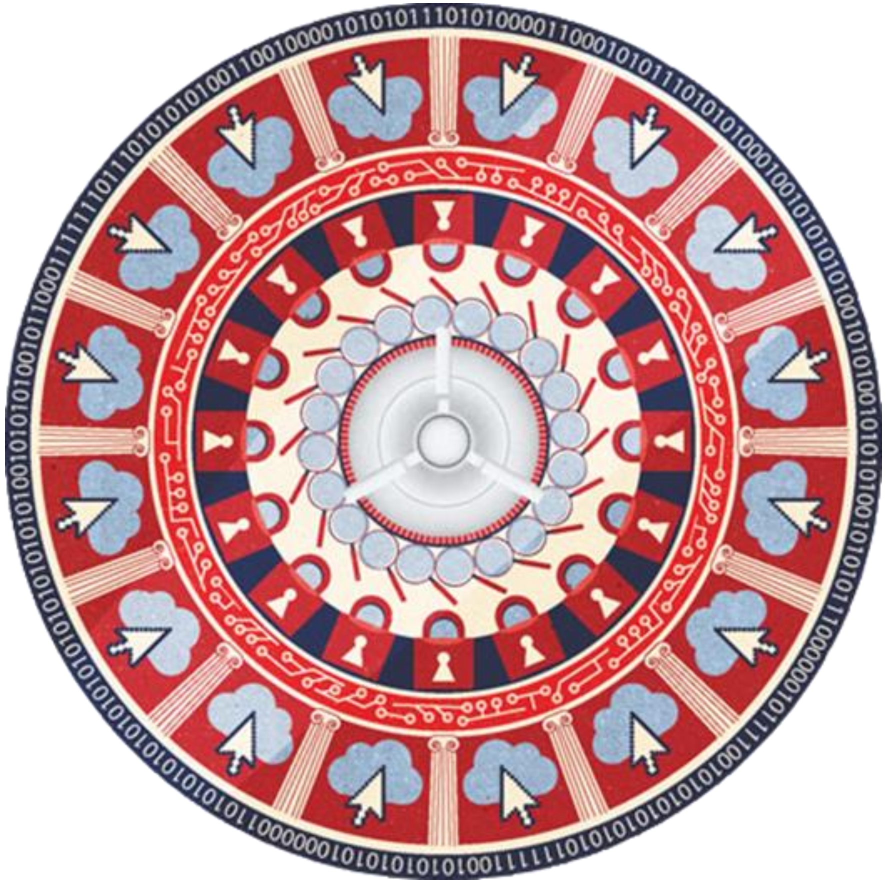
Deloitte.

NASCIO Representing Chief Information Officers of the States

NCSL National Conference of State Legislatures

State Governments at Risk:

Turning strategy and awareness into progress



National Conference of State Legislatures
Task Force on Cybersecurity
October 21, 2016

Today’s Speakers

Assemblymember Jacqui Irwin

State of California

Co-chair, NCSL Task Force On Cybersecurity

Doug Robinson

Executive Director

National Association of State Chief Information Officers (NASCIO)

Srini Subramanian

State Government Sector Leader – Deloitte Advisory

Principal, Deloitte & Touche LLP

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

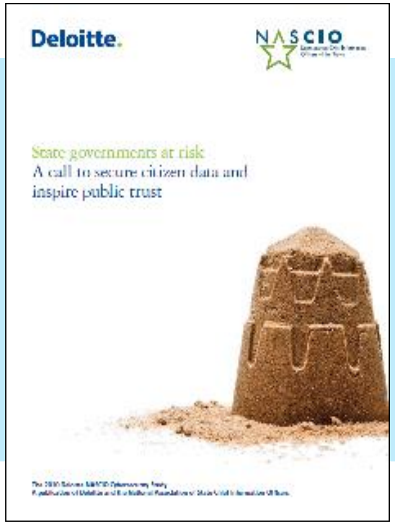
Agenda

- 2016 cybersecurity survey
- Study results: three key takeaways
- Strategy and governance
- Budget and funding
- Talent
- Emerging trends

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Timeline of state governments at risk

2010

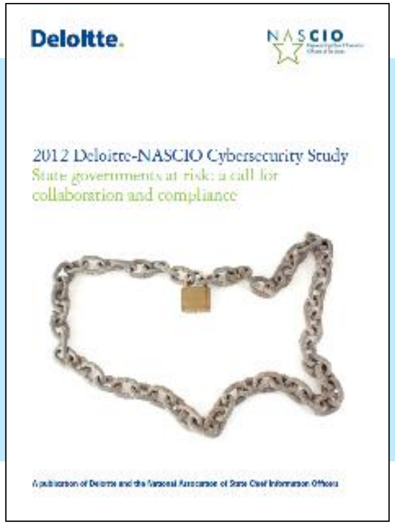


Deloitte. NASCIO

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

A call to secure citizen data and inspire trust

2012



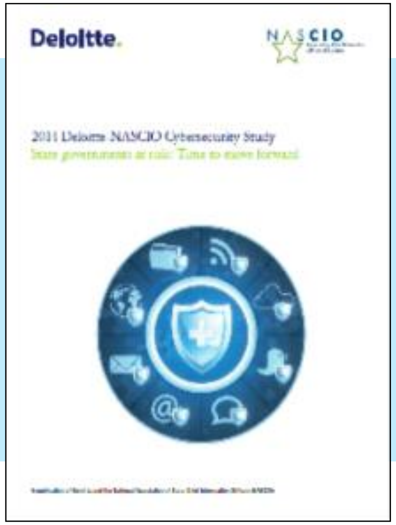
Deloitte. NASCIO

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

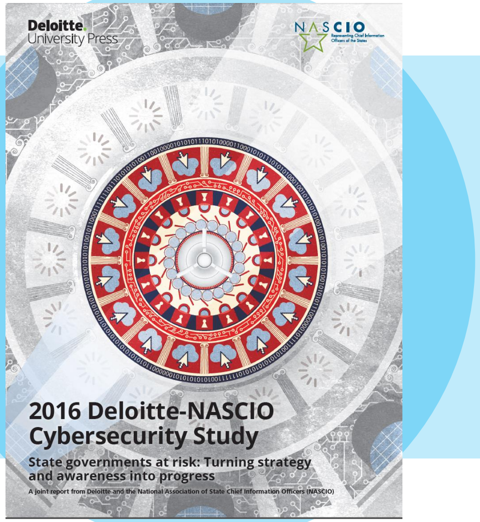


Deloitte. NASCIO

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

Time to move forward

2016



Deloitte University Press NASCIO

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

#StateofCyber

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

State Governments at Risk

2016 survey respondents

CISO survey profile

CISO participants answered **59** questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Responses from **49 states and territories**.

State official profile

96 state business and elected officials answered **15** questions, providing valuable insight into state business stakeholder perspectives. **12** associations participated

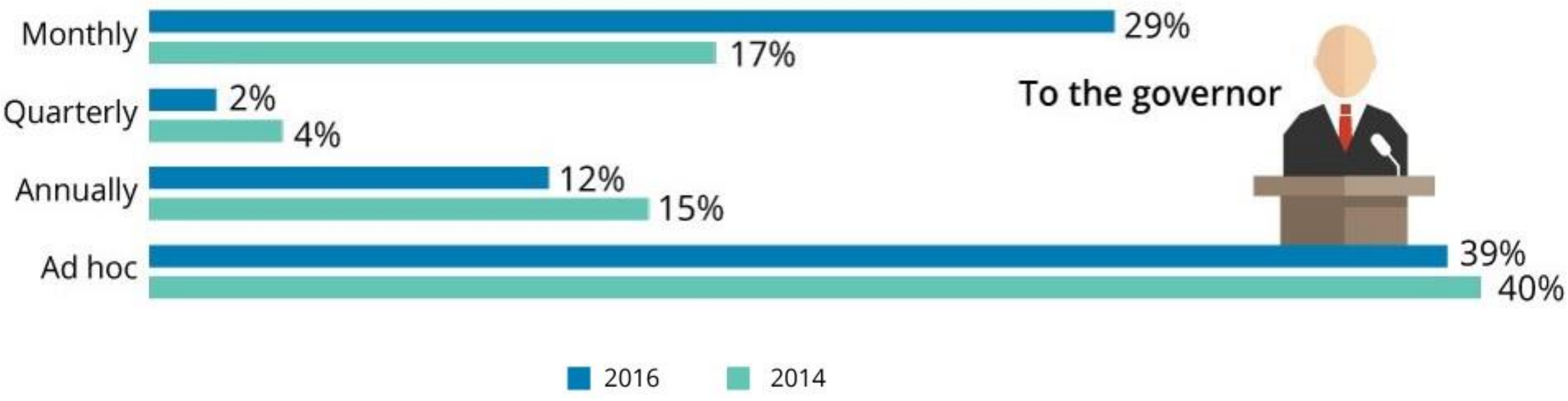
Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

Key takeaways

#1: Governor-level awareness is on the rise

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

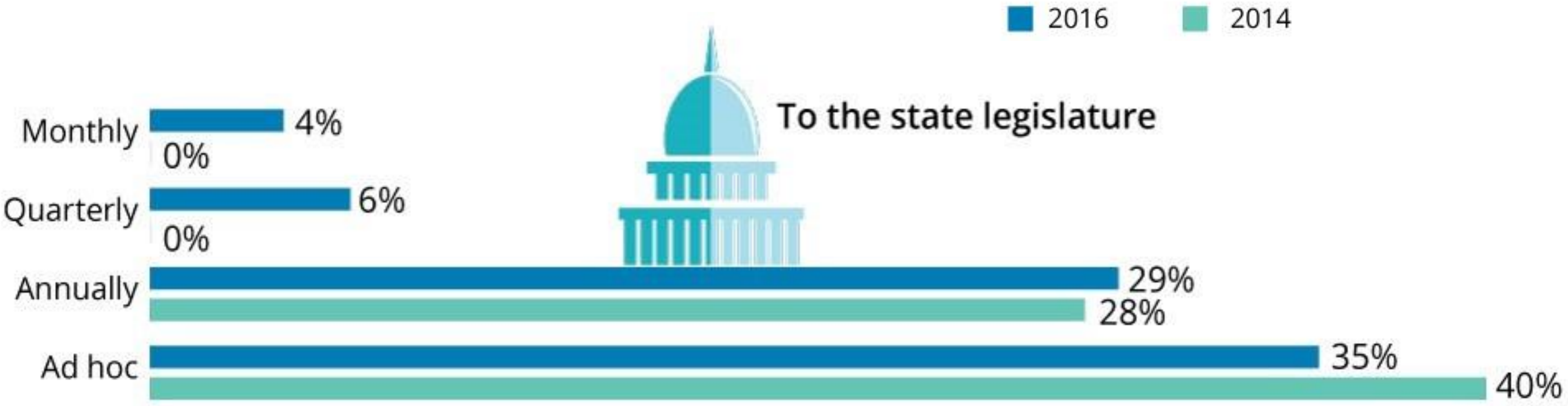


Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#1: Governor-level awareness is on the rise

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



State cyber legislation: most state laws only cover data breach notification

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

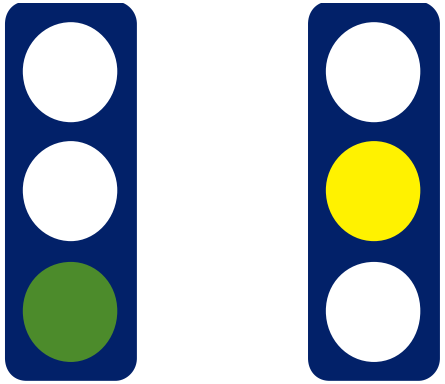
Key takeaways

#1: Governor-level awareness is on the rise

How confident are you in your state's ability in managing cyber risk?

Confidence Gap

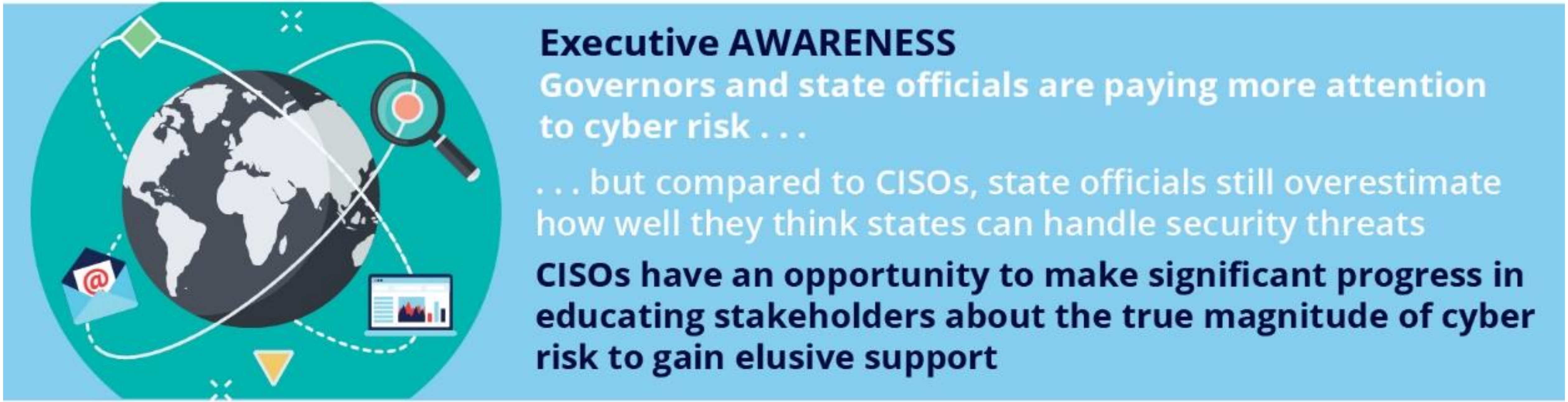
Confidence in ability to protect against external attacks:
Only **27%** CISOs
vs
66% State officials



Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#1: Governor-level awareness is on the rise



Executive AWARENESS

Governors and state officials are paying more attention to cyber risk . . .

. . . but compared to CISOs, state officials still overestimate how well they think states can handle security threats

CISOs have an opportunity to make significant progress in educating stakeholders about the true magnitude of cyber risk to gain elusive support

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#2: Cybersecurity is becoming part of the fabric of government operations

Top five cybersecurity initiatives for 2016

39%
Training and awareness

37%
Monitoring/ security operations centers (SOCs)

29%
Strategy

29%
Governance (e.g., roles, reporting structures, and directives)

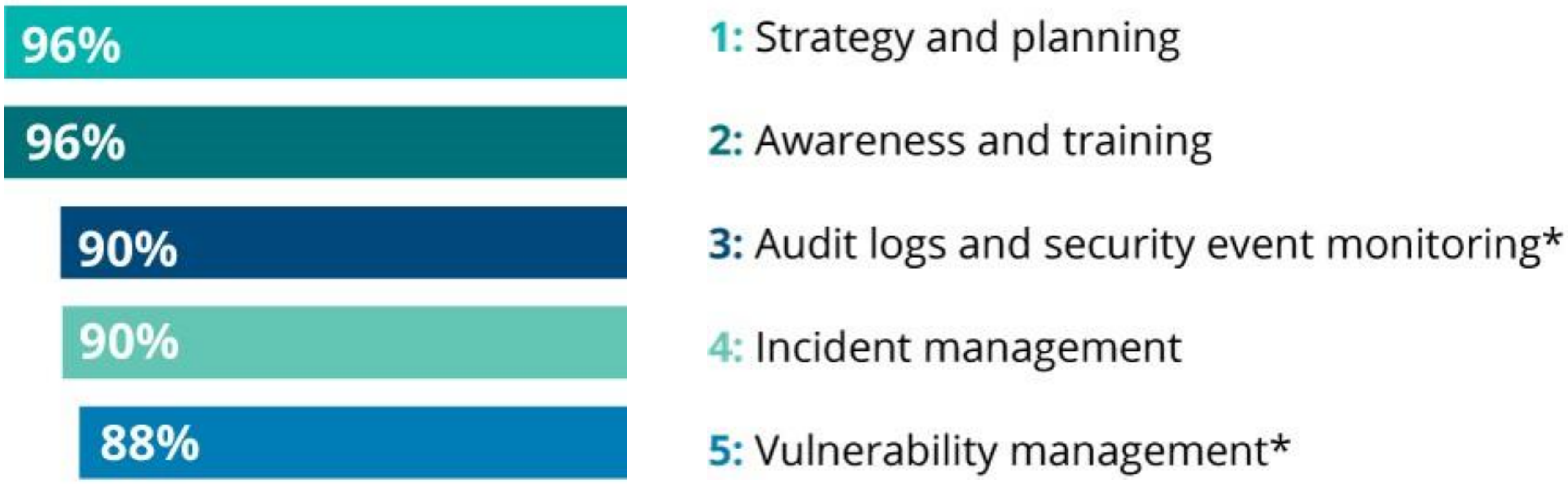
29%
Operationalizing cybersecurity

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#2: Cybersecurity is becoming part of the fabric of government operations

Top five functions within the scope of the CISO role



Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#2: Cybersecurity is becoming part of the fabric of government operations

Operational INTEGRATION

Cybersecurity is becoming part of the fabric of government operations . . .

. . . but the largely federated model of governance makes it challenging for the CISO to exercise influence and authority across the enterprise

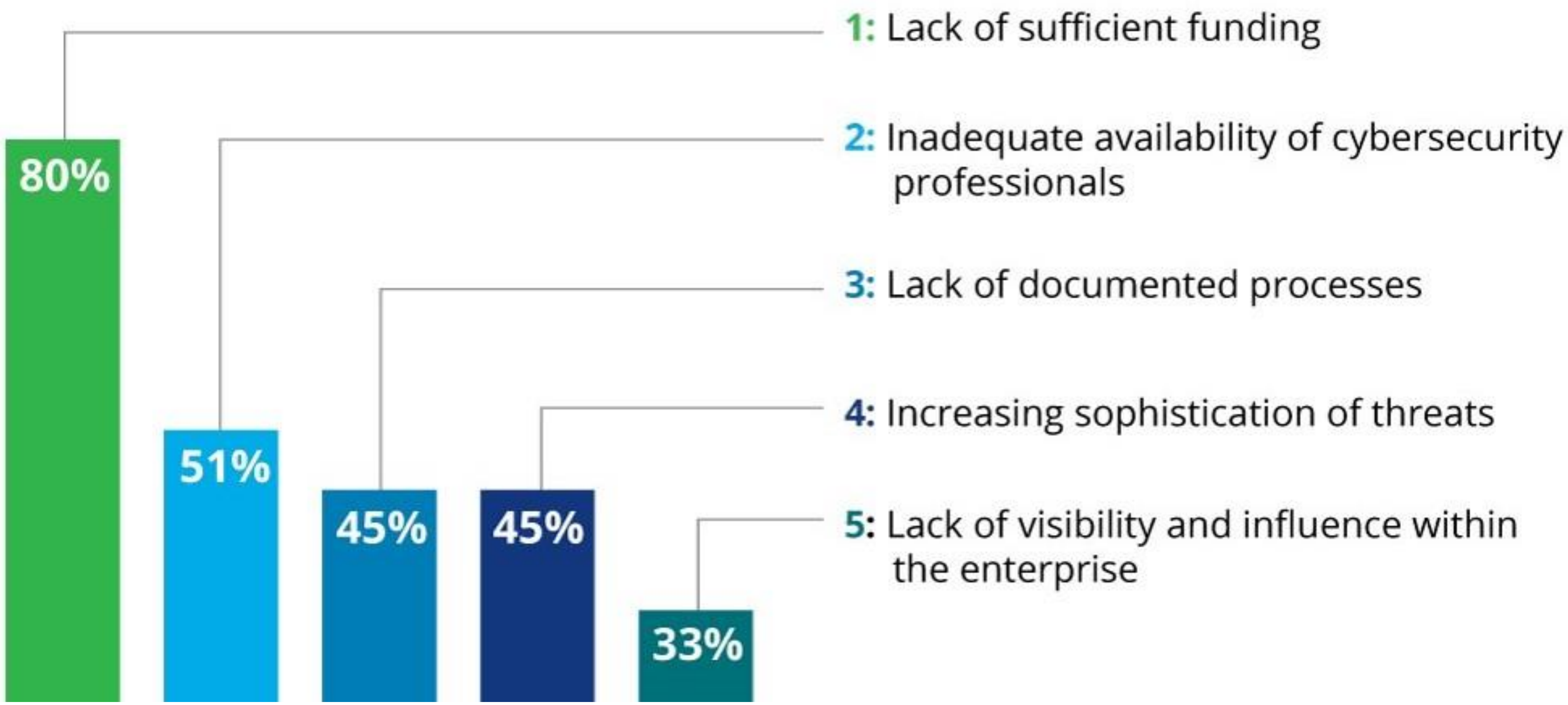
Effective collaboration across agencies, legislators, and federal partners is key to effective cyber risk management

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#3: A formal strategy can lead to more resources

Top five barriers in addressing cybersecurity challenges

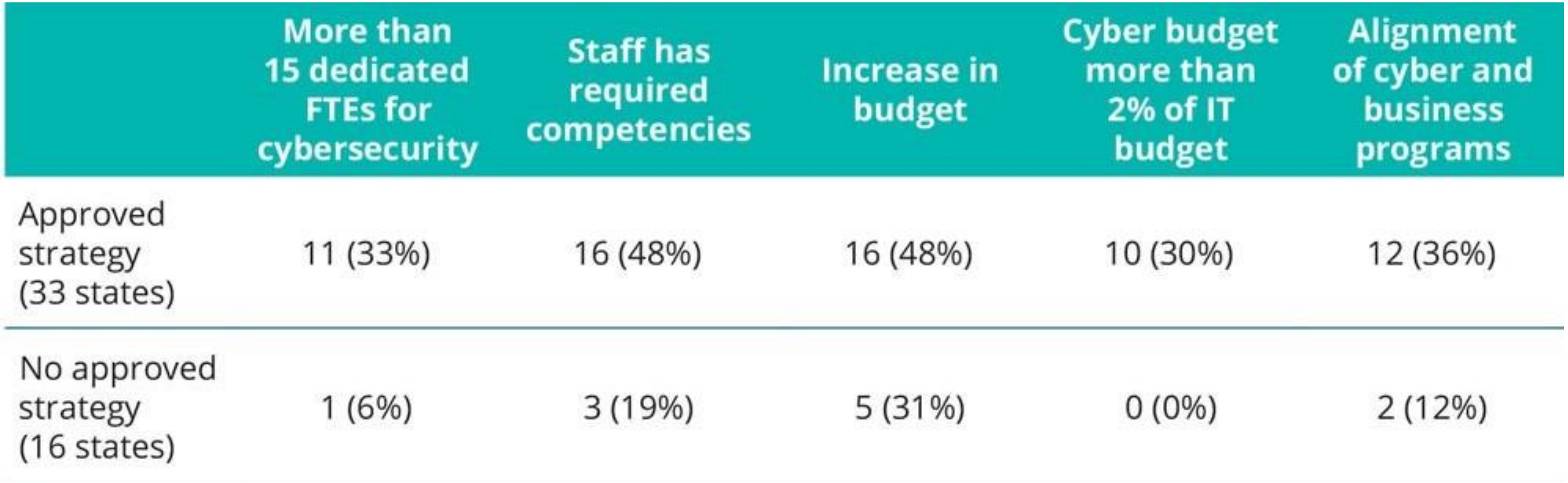


Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#3: A formal strategy can lead to more resources

Intersection of approved strategy and resources



	More than 15 dedicated FTEs for cybersecurity	Staff has required competencies	Increase in budget	Cyber budget more than 2% of IT budget	Alignment of cyber and business programs
Approved strategy (33 states)	11 (33%)	16 (48%)	16 (48%)	10 (30%)	12 (36%)
No approved strategy (16 states)	1 (6%)	3 (19%)	5 (31%)	0 (0%)	2 (12%)

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Key takeaways

#3: A formal strategy can lead to more resources

Formal STRATEGY

The top challenges of lack of funding and finding talent for cybersecurity continue at the same intensity . . .

. . . but CISOs with a formal, approved cybersecurity strategy are more likely to secure funding and talent

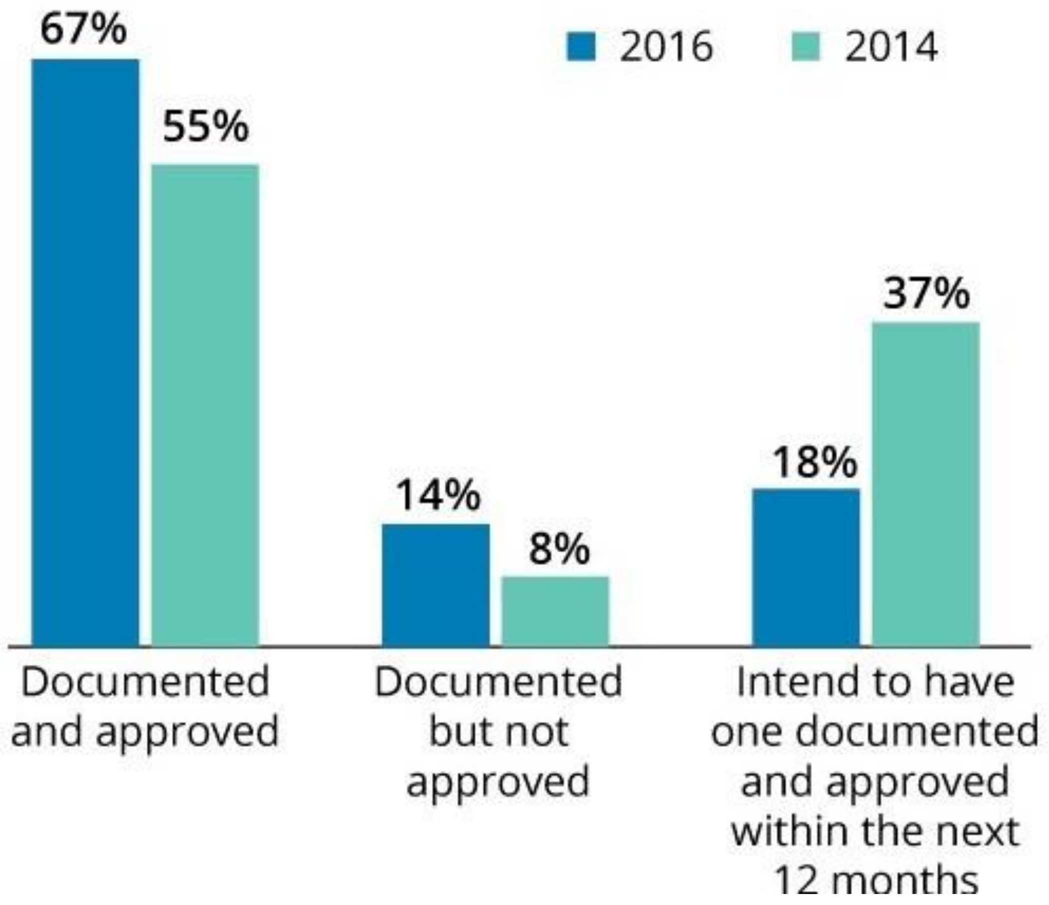
CISOs should formalize their cybersecurity strategy and communicate its urgency to the stakeholders who need to approve it

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Strategy and governance

Strategy and governance

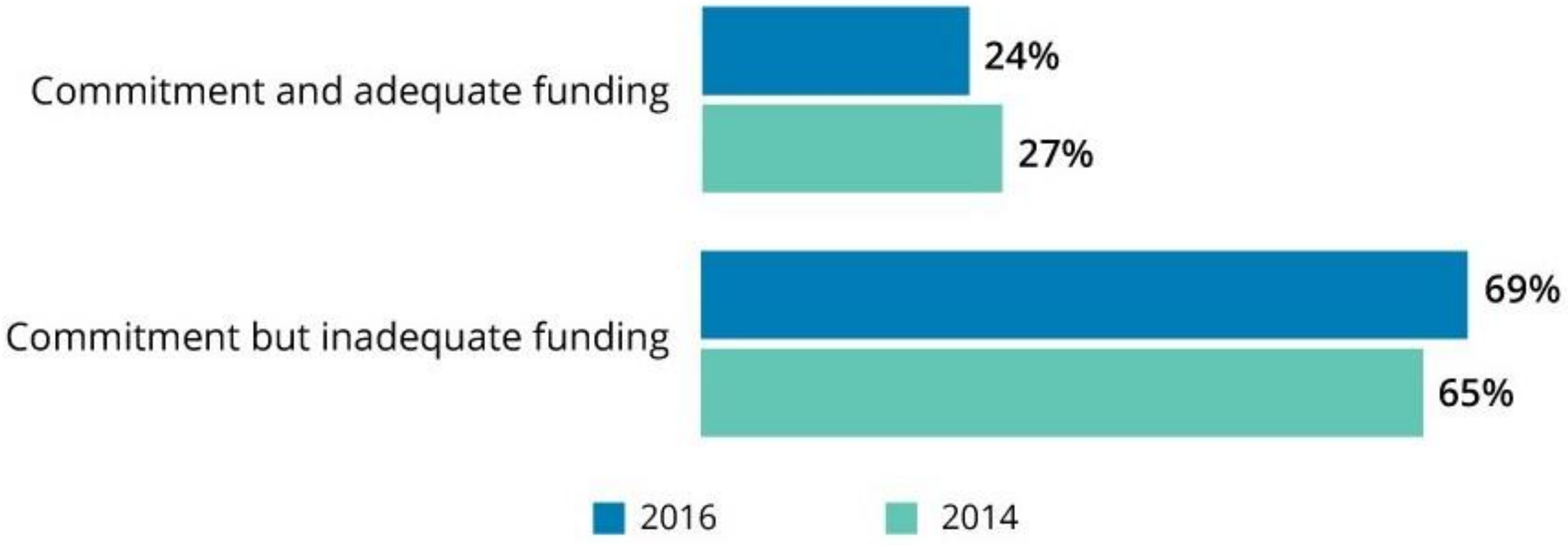
State's progress in maintaining cybersecurity strategy



Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Strategy and governance

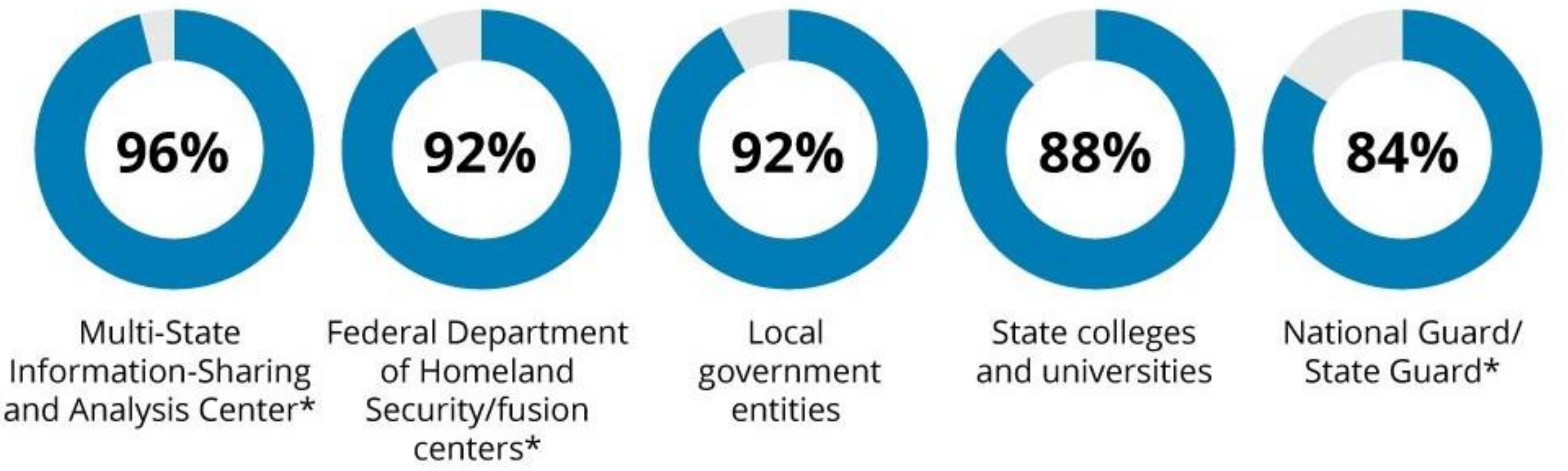
Senior executive support (governor’s office, agency secretary, or CIO) for security projects to effectively address regulatory or legal requirements



Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Strategy and governance

Collaboration trends as part of the states' cybersecurity program

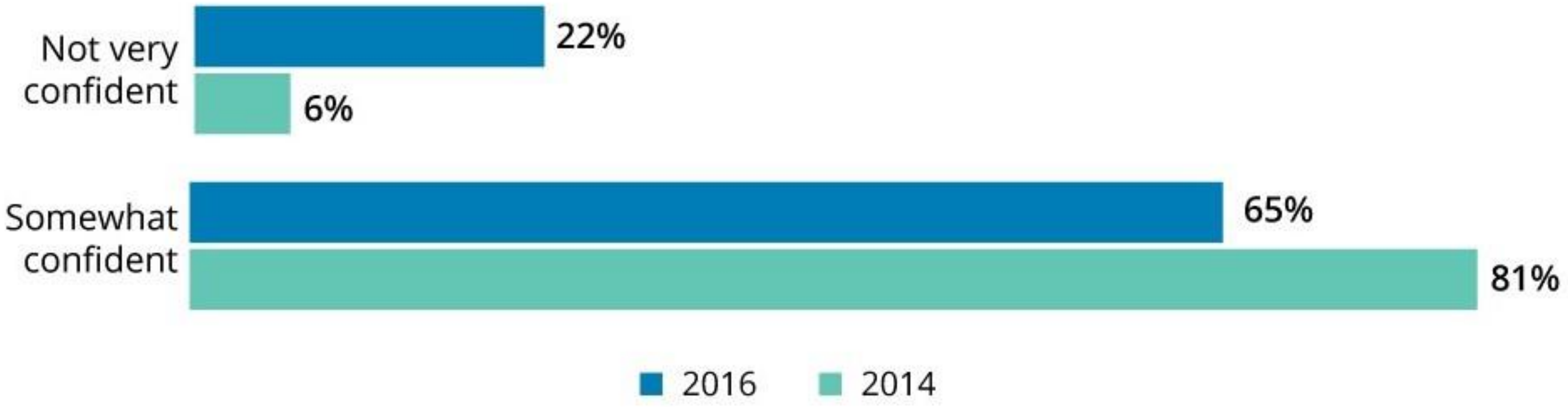


*New in 2016

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Strategy and governance

CISOs’ confidence levels in cybersecurity practice followed by third parties (contractors, service providers, business partners)

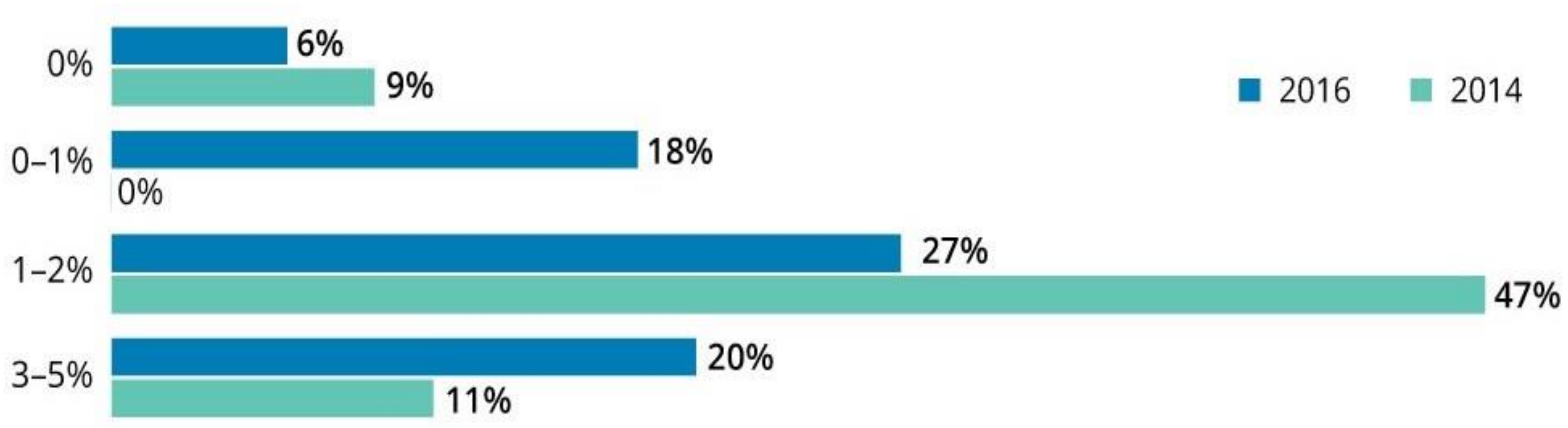


Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Budget & funding

Budget remains top challenge

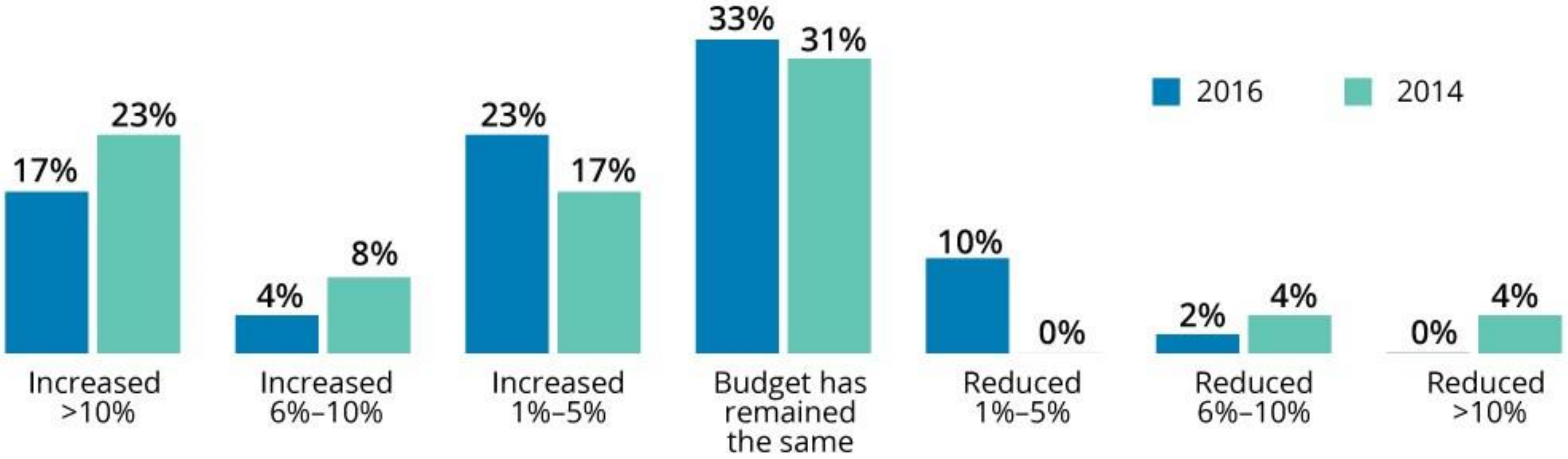
Percentage of state's cybersecurity allocation as part of overall IT budget



Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Budget remains top challenge

Year-over-year trending of the state cybersecurity budget 2014-2016

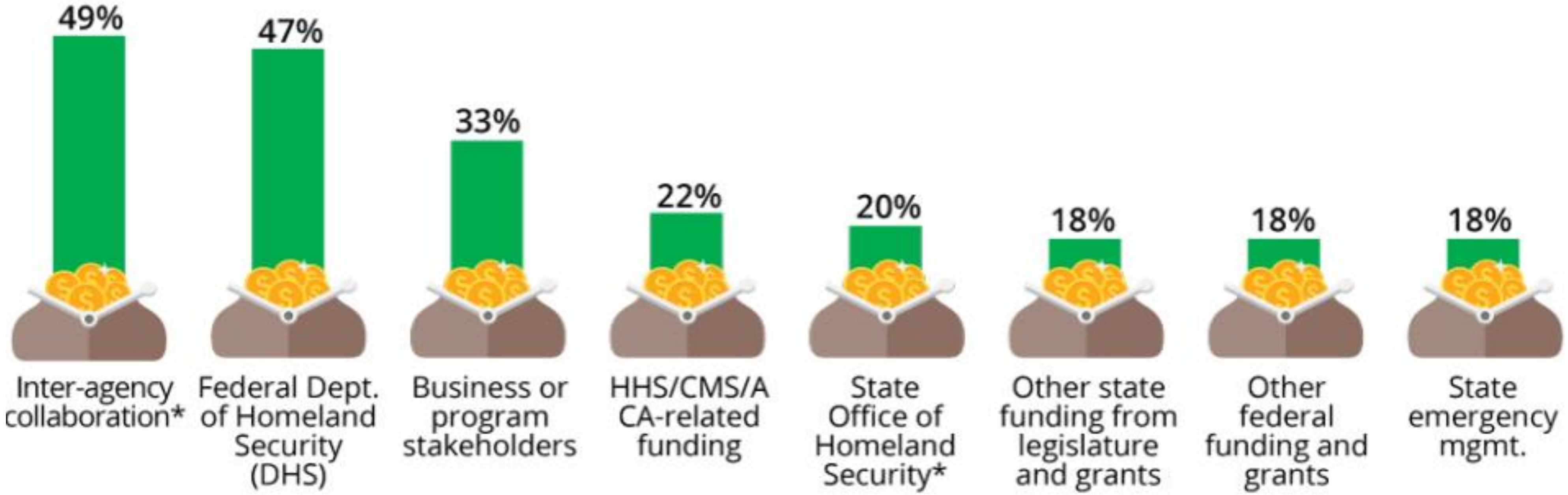


#StateofCyber

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Budget remains top challenge

Additional funding sources for cybersecurity initiatives



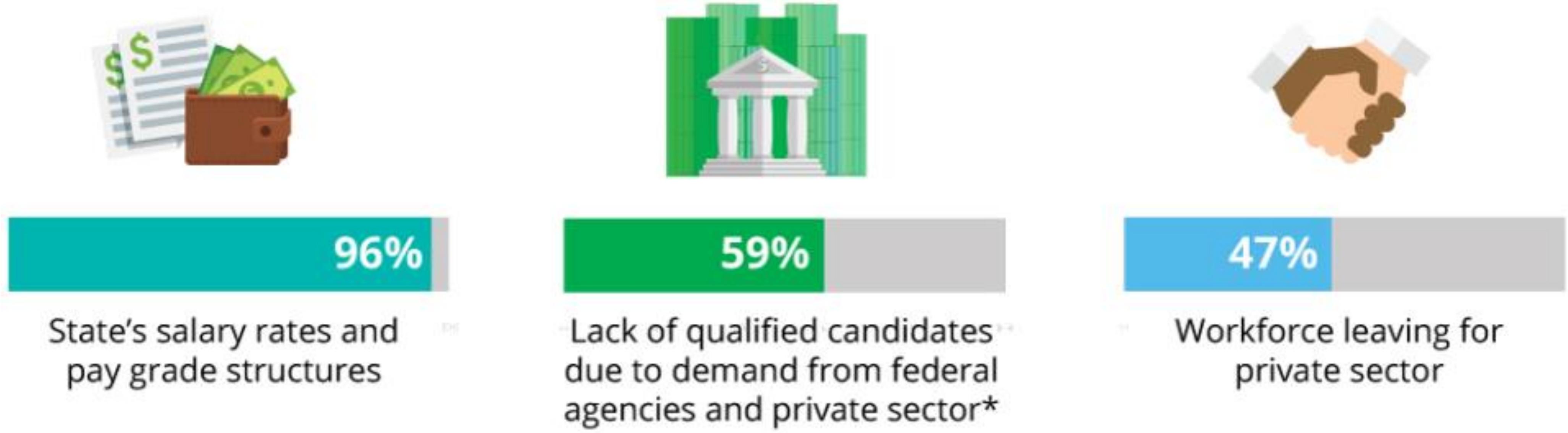
*New in 2016

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Talent

Talent crisis continues

Top three human resources factors that negatively impact the CISO's ability to develop, support, and maintain cybersecurity workforce

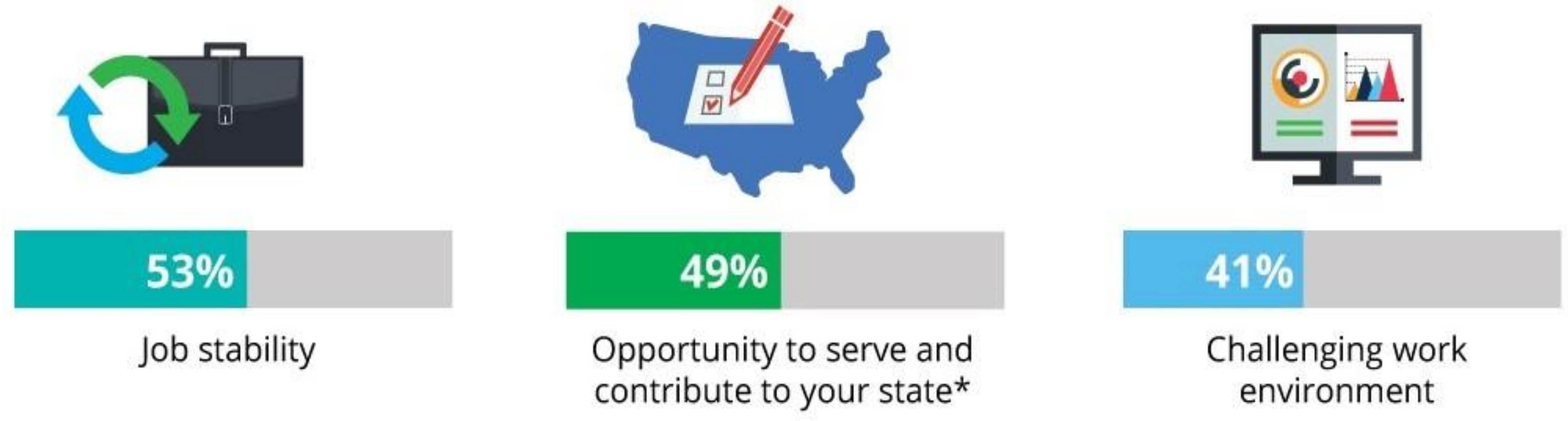


*New in 2016

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Talent crisis continues

Top three factors that CISOs employ to attract and retain cybersecurity talent

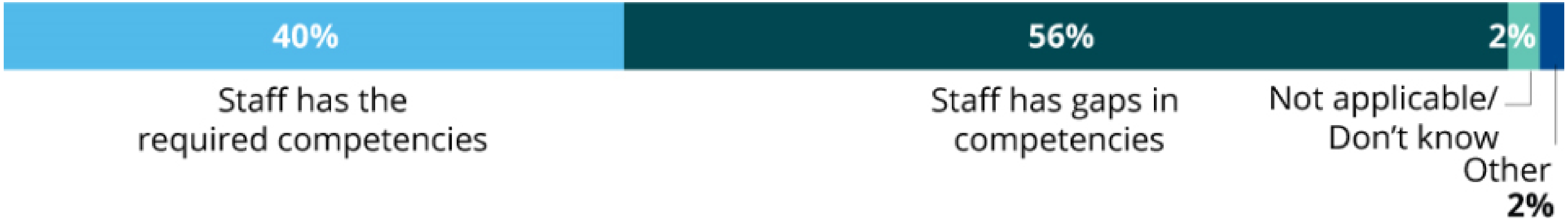


Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Talent crisis continues

State internal cybersecurity professional competencies

(i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements

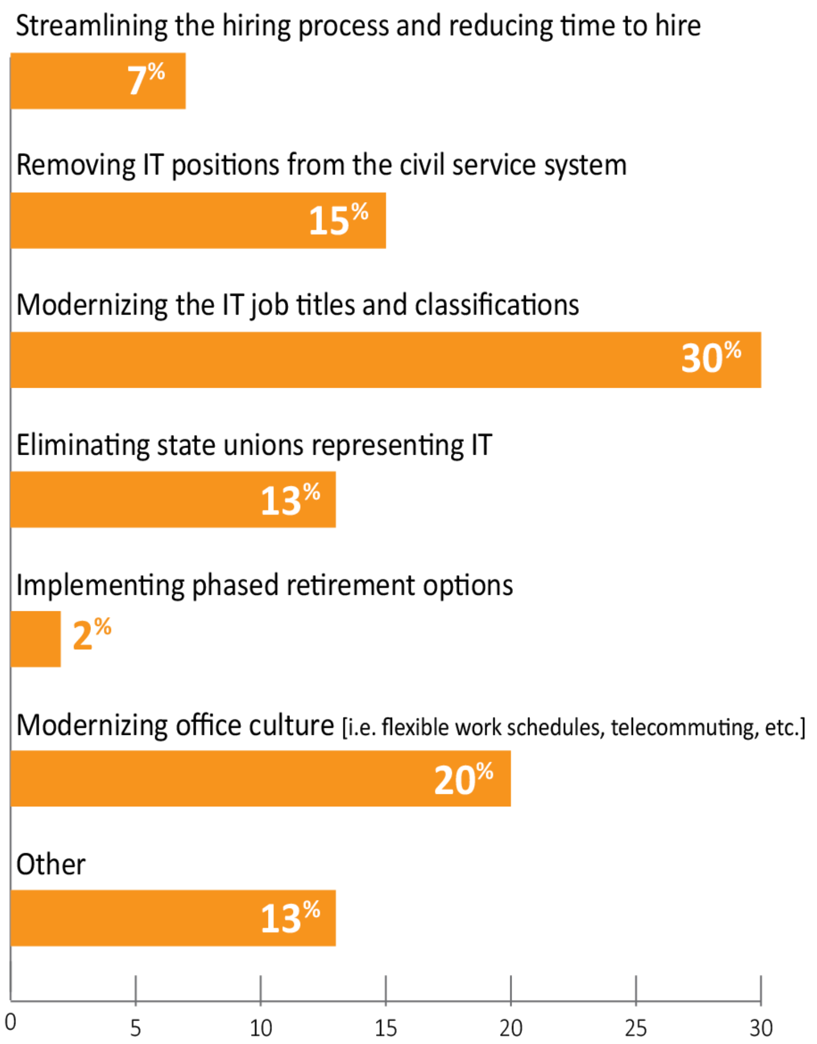


Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Talent crisis continues

What innovative/out-of-the-box strategies and tactics has your state used in attracting and retaining a highly qualified IT workforce?	
Promoting non-salary benefits like greater stability and diversity of experience	**75%**
Call to public service	**64%**
Public/private internships	**39%**
Sponsoring community awareness events (i.e. hackathons, robot build events, speaking at STEM schools)	**35%**
Building "talent networks"	**31%**
Emphasizing location (i.e. working in state capital)	**29%**

What single personnel reform could be implemented that would be the most impactful in reforming your state IT workforce?

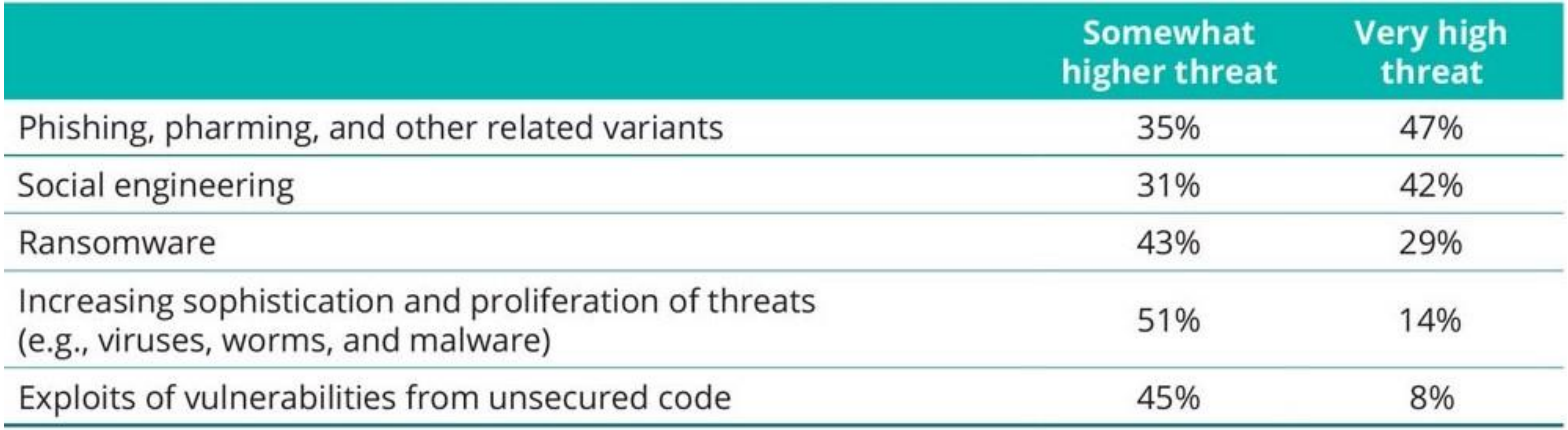


Source: 2016 NASCIO State CIO Survey

Emerging trends

Emerging trends

Top cyber threats across state government

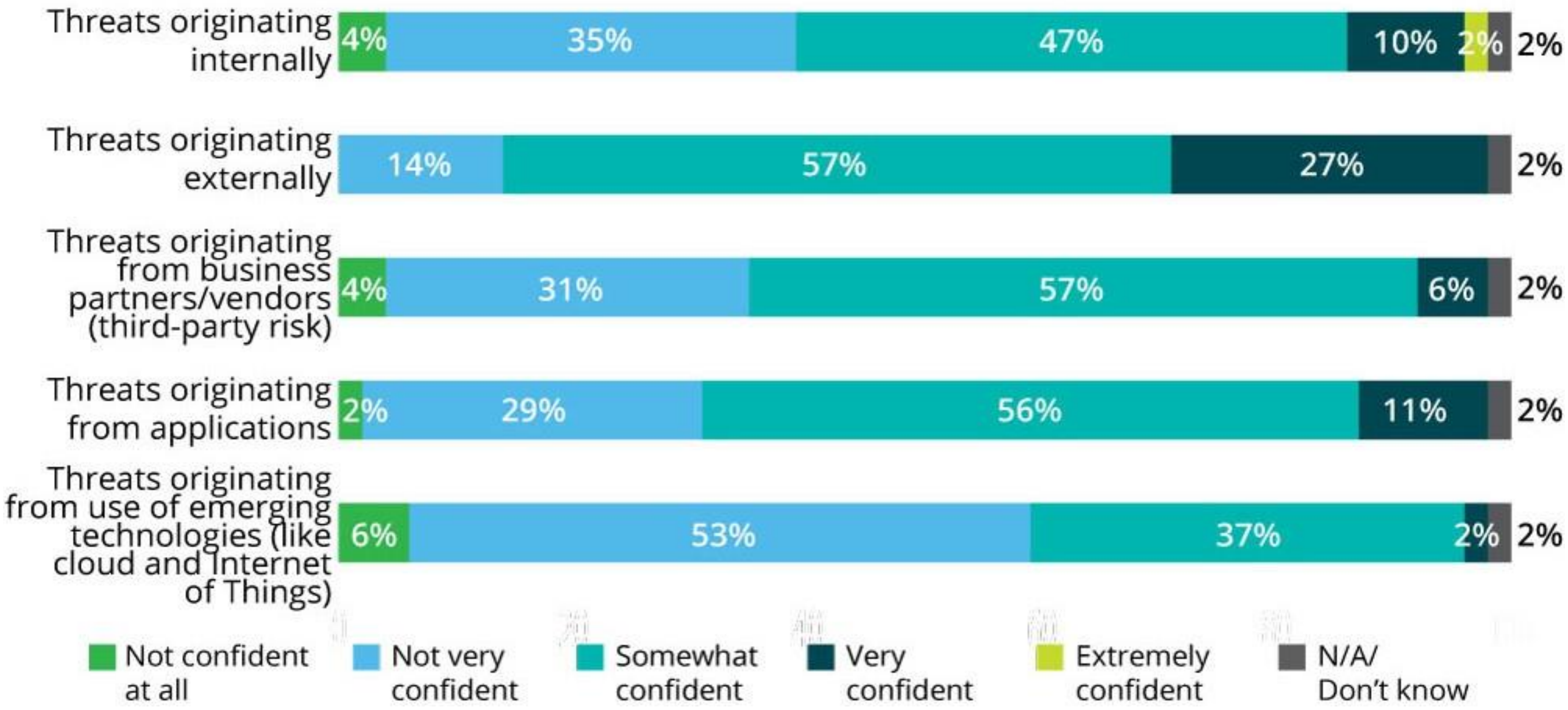


	Somewhat higher threat	Very high threat
Phishing, pharming, and other related variants	35%	47%
Social engineering	31%	42%
Ransomware	43%	29%
Increasing sophistication and proliferation of threats (e.g., viruses, worms, and malware)	51%	14%
Exploits of vulnerabilities from unsecured code	45%	8%

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Emerging trends

CISOs’ confidence levels in protecting their state’s information assets cyber threats

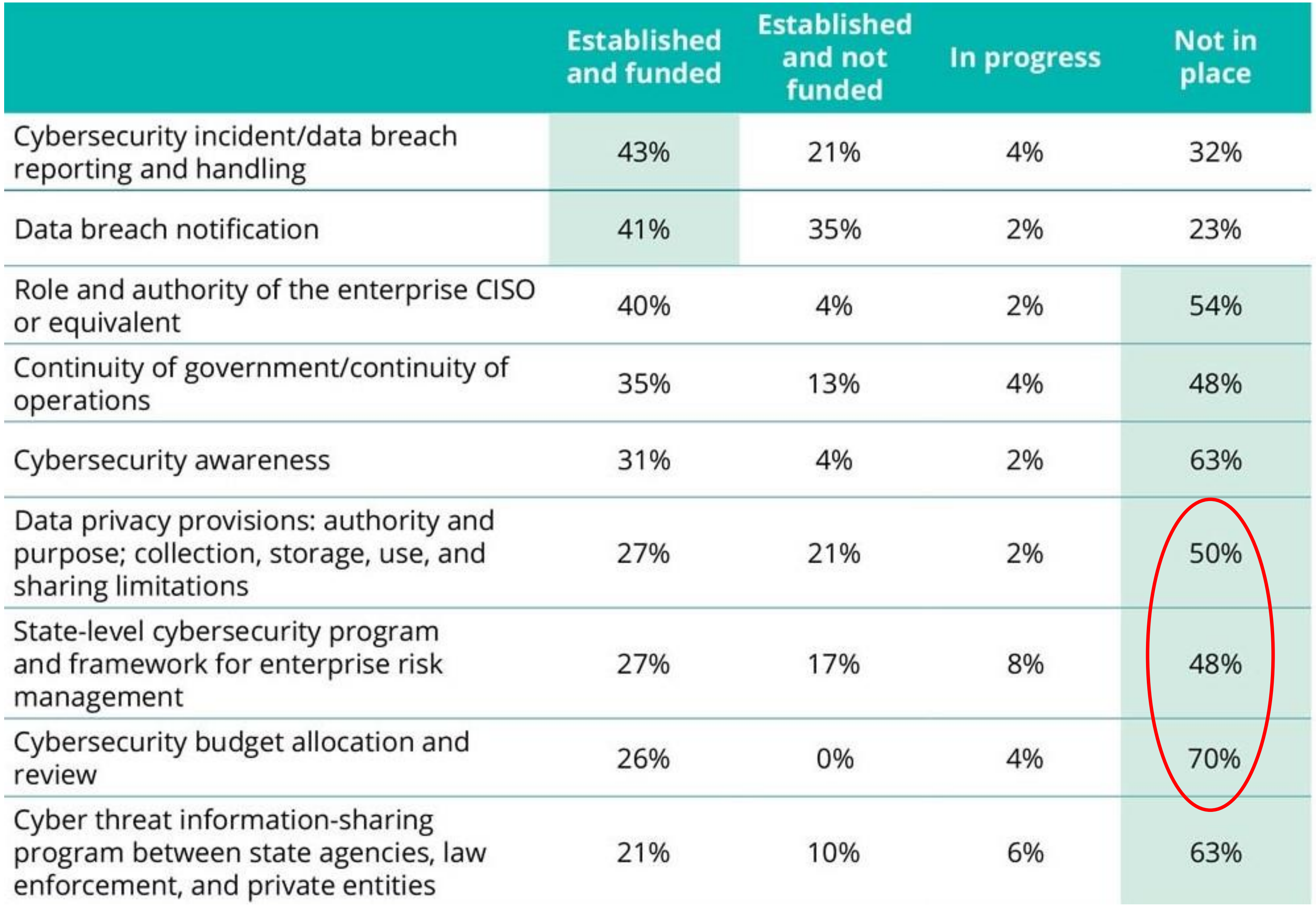


Source: The 2016 Deloitte-NASCIO Cybersecurity Study

#StateofCyber

Emerging trends

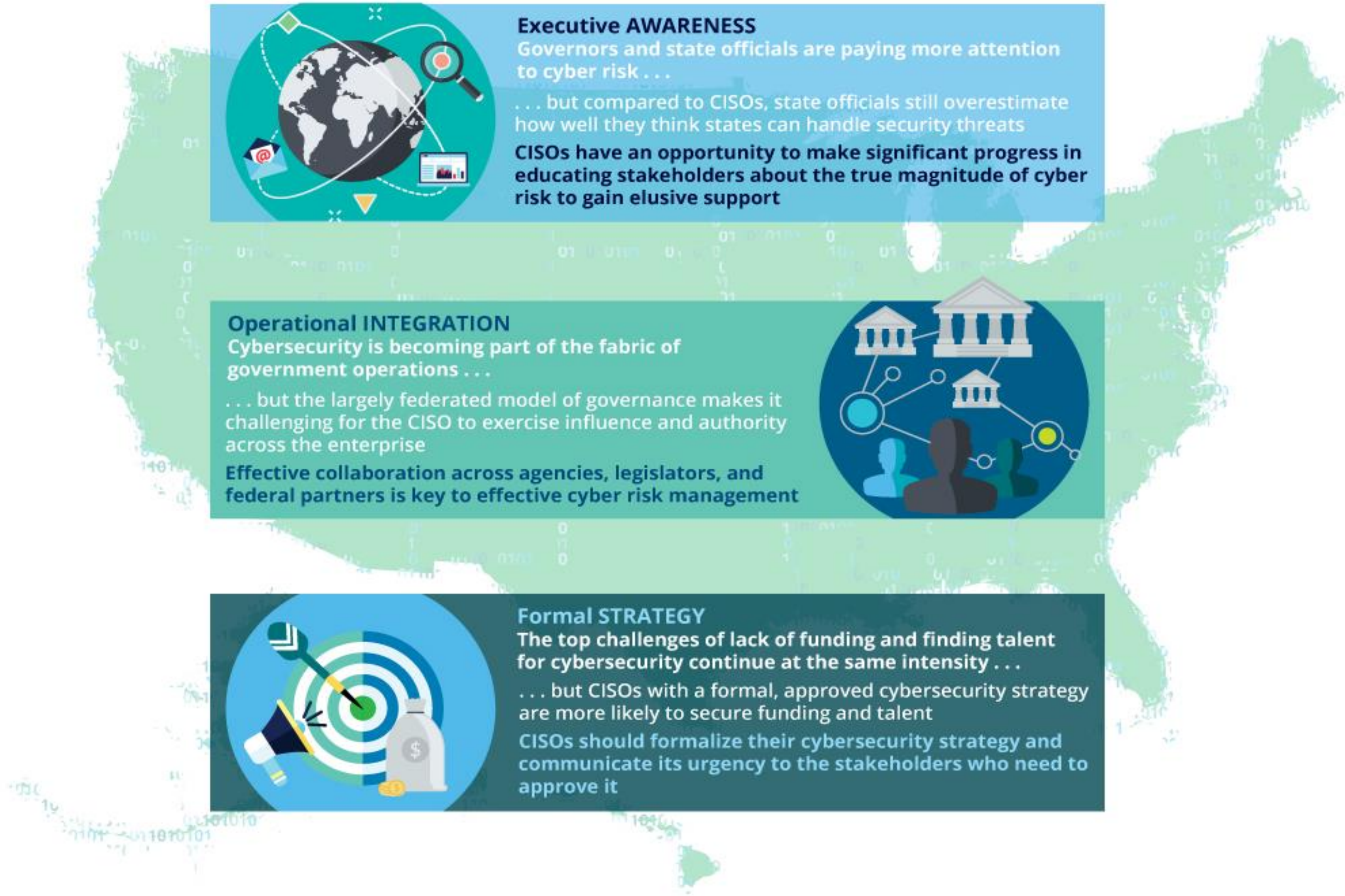
Provisions of states' cyber legislation/statutes



	Established and funded	Established and not funded	In progress	Not in place
Cybersecurity incident/data breach reporting and handling	43%	21%	4%	32%
Data breach notification	41%	35%	2%	23%
Role and authority of the enterprise CISO or equivalent	40%	4%	2%	54%
Continuity of government/continuity of operations	35%	13%	4%	48%
Cybersecurity awareness	31%	4%	2%	63%
Data privacy provisions: authority and purpose; collection, storage, use, and sharing limitations	27%	21%	2%	50%
State-level cybersecurity program and framework for enterprise risk management	27%	17%	8%	48%
Cybersecurity budget allocation and review	26%	0%	4%	70%
Cyber threat information-sharing program between state agencies, law enforcement, and private entities	21%	10%	6%	63%

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Moving forward



Executive AWARENESS

Governors and state officials are paying more attention to cyber risk . . .

. . . but compared to CISOs, state officials still overestimate how well they think states can handle security threats

CISOs have an opportunity to make significant progress in educating stakeholders about the true magnitude of cyber risk to gain elusive support

Operational INTEGRATION

Cybersecurity is becoming part of the fabric of government operations . . .

. . . but the largely federated model of governance makes it challenging for the CISO to exercise influence and authority across the enterprise

Effective collaboration across agencies, legislators, and federal partners is key to effective cyber risk management

Formal STRATEGY

The top challenges of lack of funding and finding talent for cybersecurity continue at the same intensity . . .

. . . but CISOs with a formal, approved cybersecurity strategy are more likely to secure funding and talent

CISOs should formalize their cybersecurity strategy and communicate its urgency to the stakeholders who need to approve it

Source: The 2016 Deloitte-NASCIO Cybersecurity Study

Deloitte.

NASCIO Representing Chief Information Officers of the States

NCSL National Conference of State Legislatures

State Governments at Risk:

Turning strategy and awareness into progress

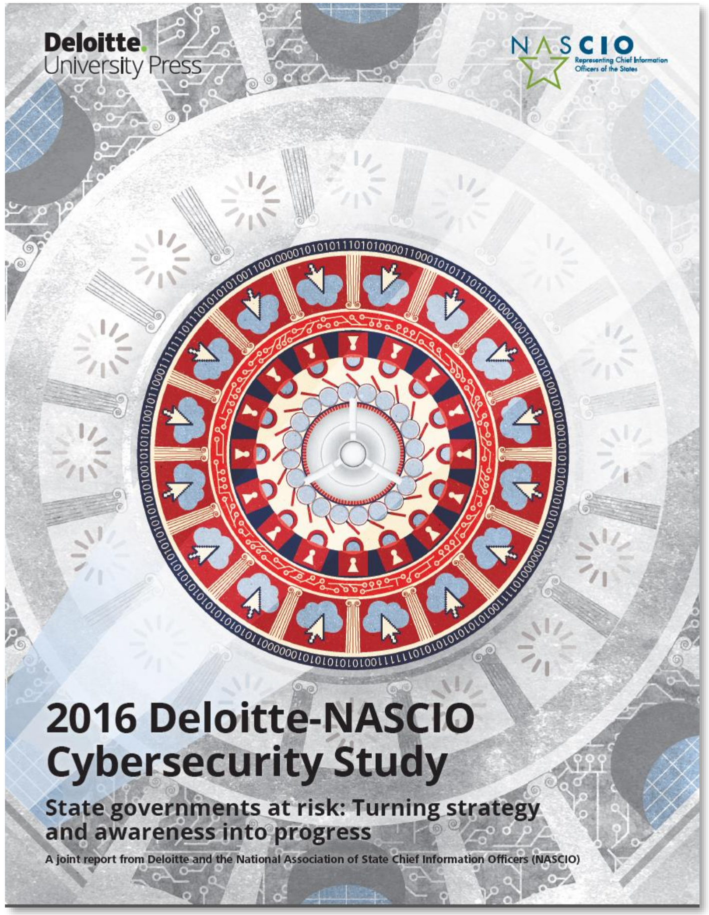
Available for download at www.nascio.org/stateofcyber

Video from 2016 NASCIO Annual Conference session available at https://youtu.be/9DXoATWFbE4

Contacts:

Doug Robinson – drobinson@NASCIO.org

Srini Subramanian - ssubramanian@deloitte.com



Deloitte. University Press

NASCIO Representing Chief Information Officers of the States

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)

Deloitte.

NASCIO Representing Chief Information Officers of the States

About NASCIO
The National Association of State Chief Information Officers is the premier network and resource for state CIOs and a leading advocate for technology policy at all levels of government. NASCIO represents state chief information officers and information technology executives from the states, territories, and the District of Columbia. For more information about NASCIO visit www.nascio.org.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this presentation contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

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