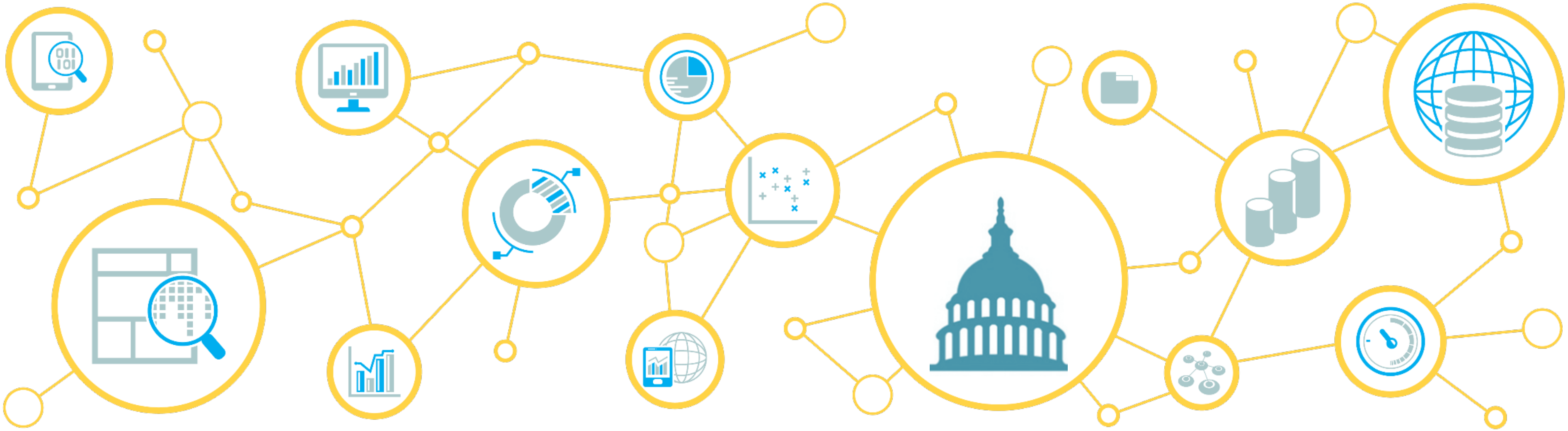


State Governments at Risk: State CIOs and Cybersecurity

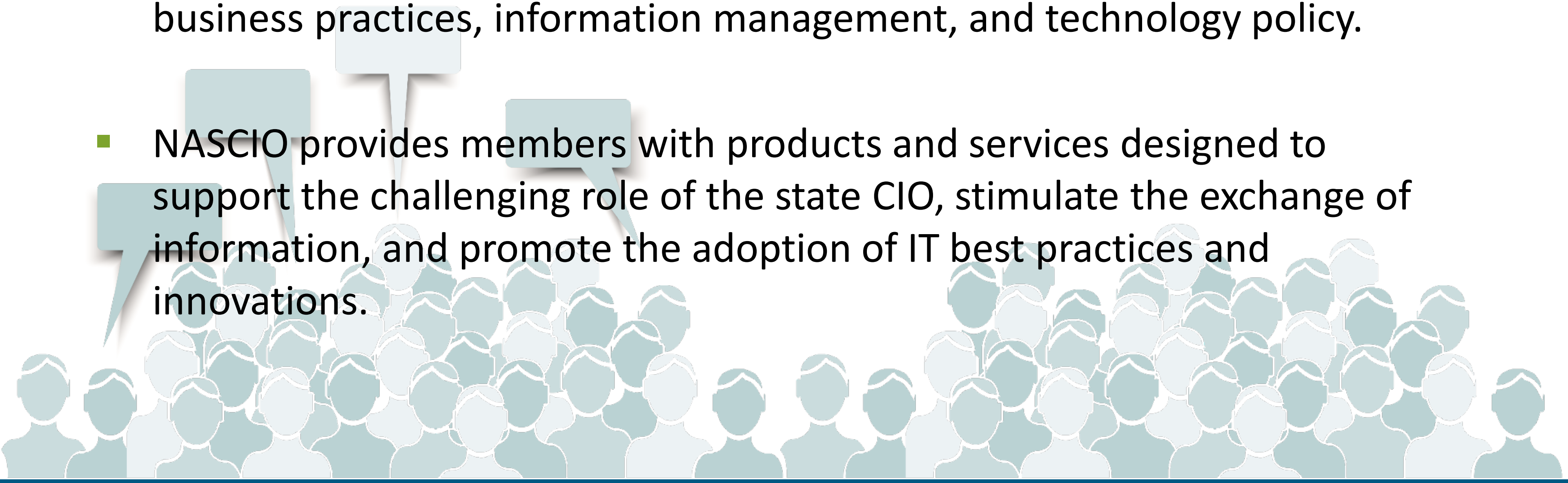
GOVERNMENT, TECHNOLOGY AND SECURITY COMMITTEE
KANSAS HOUSE OF REPRESENTATIVES
January 31, 2018 - 9:00 am
Eric Sweden, Program Director, NASCIO

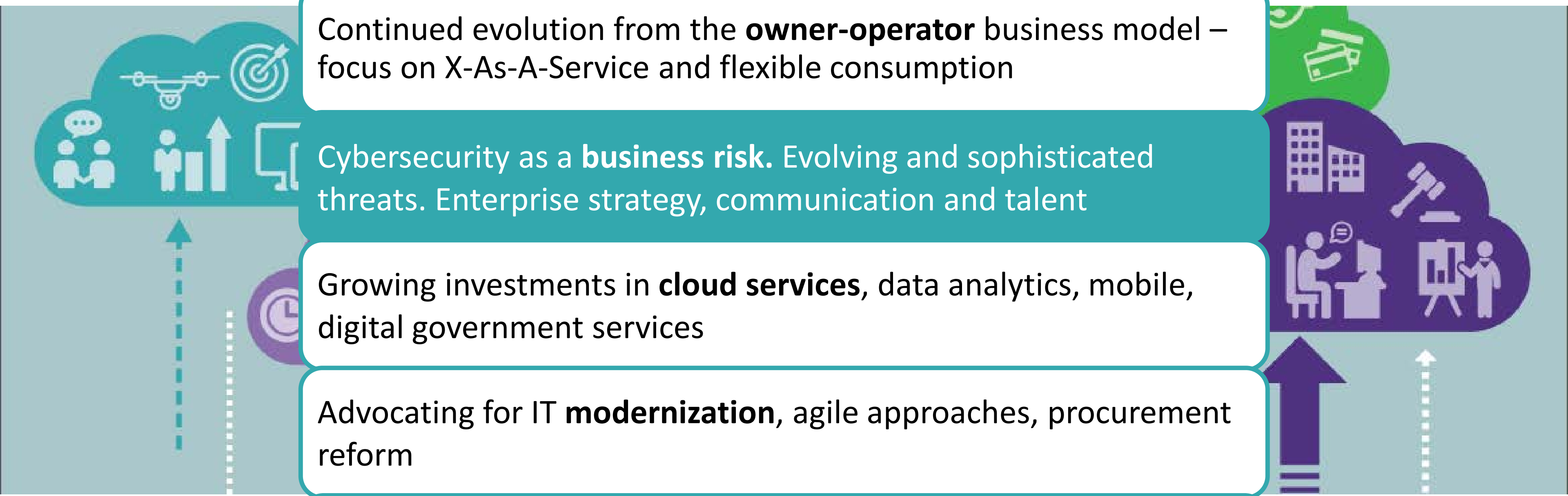
About NASCIO

- National association representing state chief information officers and information technology executives from the states, territories and D.C.

- NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.

- NASCIO provides 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.





Budgets for FY 2018 remain cautious. CIOs pressured to find **cost savings,** driving consolidation, optimization strategies

Continued evolution from the **owner-operator** business model – focus on X-As-A-Service and flexible consumption

Cybersecurity as a **business risk.** Evolving and sophisticated threats. Enterprise strategy, communication and talent

Growing investments in **cloud services**, data analytics, mobile, digital government services

Advocating for IT **modernization**, agile approaches, procurement reform

Continuing IT **workforce challenges:** retirements, skills gap, recruiting, talent management, workplace innovation

State Governments at Risk!

States are attractive targets – data!

More aggressive threats – organized crime, phishing, ransomware, hacktivism

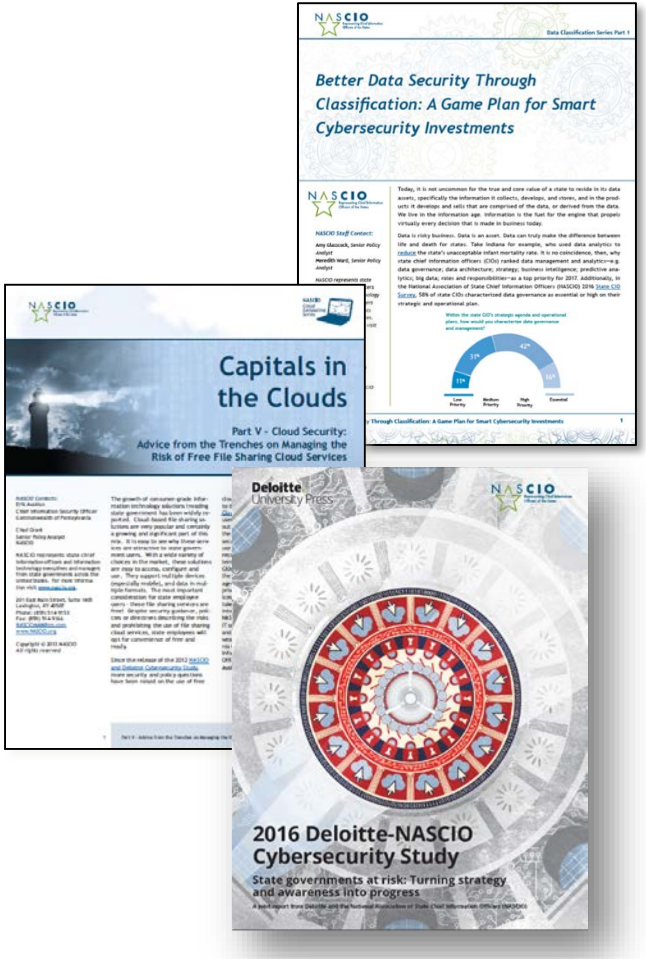
Nation state threats, attacks

Critical infrastructure protection: disruption

Human factor – employees, contractors

Data and services on the move: cloud and mobile

Need for continuous training, awareness



Data Classification Series Part 1

Better Data Security Through Classification: A Game Plan for Smart Cybersecurity Investments

NASCIO Staff Contact:

Amy Glasscock, Senior Policy Analyst

Meredith Ward, Senior Policy Analyst

NASCIO represents state

Today, it is not uncommon for the true and core value of a state to reside in its data assets, specifically the information it collects, develops, and stores, and in the products it develops and sells that are comprised of the data, or derived from the data. We live in the information age. Information is the fuel for the engine that propels virtually every decision that is made in business today.

Data is risky business. Data is an asset. Data can truly make the difference between life and death for states. Take Indiana for example, who used data analytics to reduce the state's unacceptable infant mortality rate. It is no coincidence, then, why state chief information officers (CIOs) ranked data management and analytics—e.g. data governance; data architecture; strategy; business intelligence; predictive analytics; big data; roles and responsibilities—as a top priority for 2017. Additionally, in the National Association of State Chief Information Officers (NASCIO) 2016 State CIO Survey, 58% of state CIOs characterized data governance as essential or high on their strategic and operational plan.

Within the state CIO's strategic agenda and operational plans, how would you characterize data governance and management?

y Through Classification: A Game Plan for Smart Cybersecurity Investments 1

NASCIO Cloud Computing Series

Capitals in the Clouds

Part V - Cloud Security: Advice from the Trenches on Managing the Risk of Free File Sharing Cloud Services

NASCIO Contacts:
Erik Avakian
Chief Information Security Officer
Commonwealth of Pennsylvania

Chad Grant
Senior Policy Analyst
NASCIO

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
NASCIO@AMRms.com
www.NASCIO.org

Copyright © 2013 NASCIO
All rights reserved

The growth of consumer-grade information technology solutions invading state government has been widely reported. Cloud-based file sharing solutions are very popular and certainly a growing and significant part of this mix. It is easy to see why these services are attractive to state government users. With a wide variety of choices in the market, these solutions are easy to access, configure and use. They support multiple devices (especially mobile), and data in multiple formats. The most important consideration for state employee users - these file sharing services are free! Despite security guidance, policies or directives describing the risks and prohibiting the use of file sharing cloud services, state employees will opt for convenience of free and ready.

Since the release of the 2012 NASCIO and Deloitte Cybersecurity Study, more security and policy questions have been raised on the use of free

7 Part V - Advice from the Trenches on Managing the

Deloitte. University Press

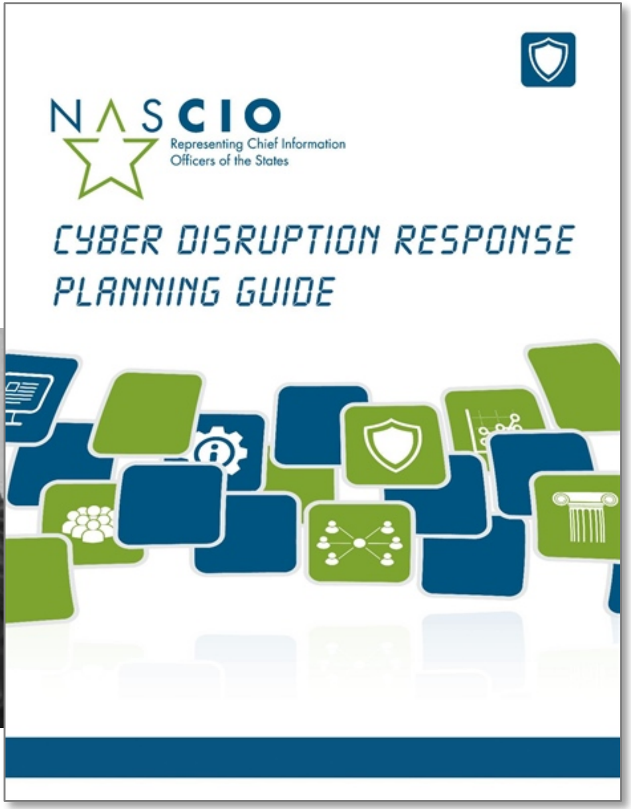
2016 Deloitte-NASCIO Cybersecurity Study

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)

Cyber Disruption: Impacting State Services

“State governments and the critical infrastructure within the state are at risk from a cybersecurity attack that could disrupt the normal operations of government and impact citizens. “



NASCIO Representing Chief Information Officers of the States

CYBER DISRUPTION RESPONSE PLANNING GUIDE

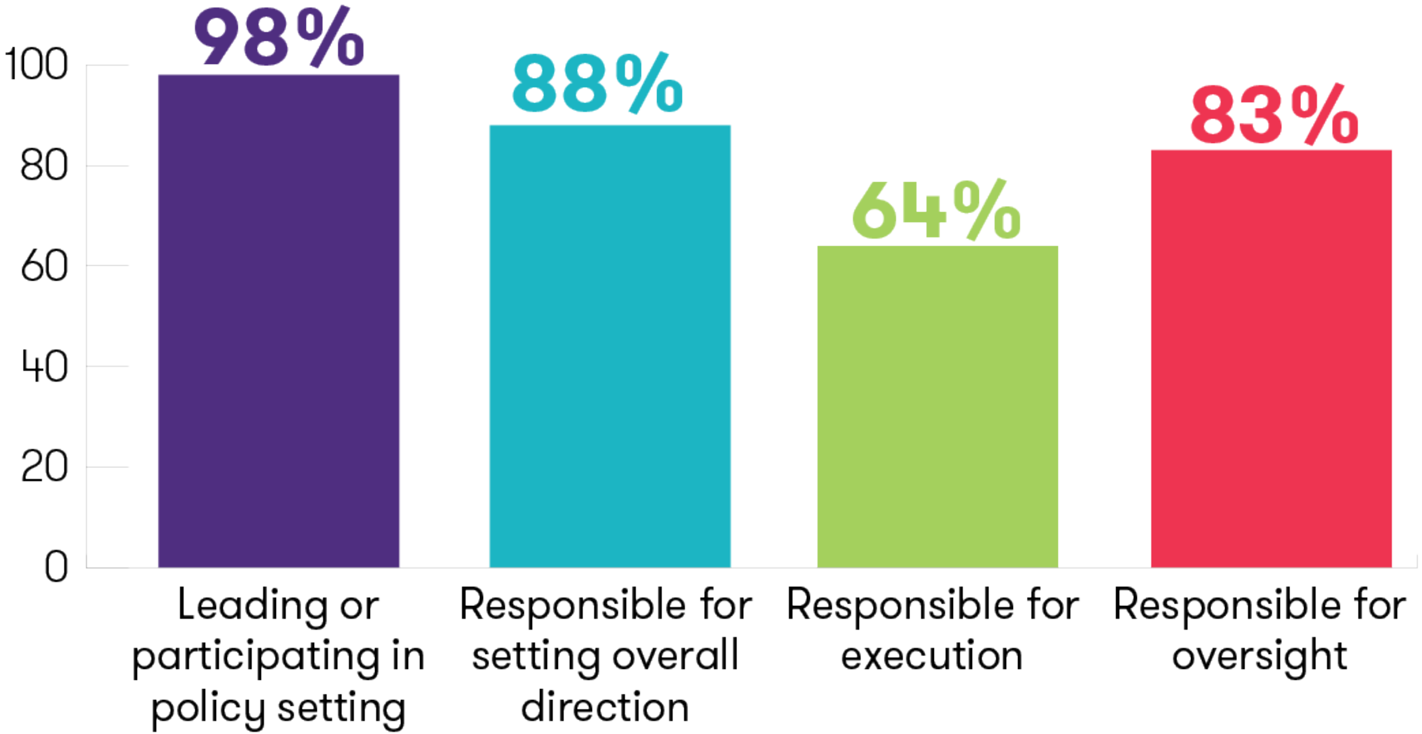
Source: NASCIO. This project was supported by Grant No. 2010-DJ-BX-K046 awarded by the Bureau of Justice Assistance.

Top Ten: State CIO Priorities for 2018

1. Security
2. Cloud Services
3. Consolidation/Optimization
4. Digital Government
5. Budget and Cost Control
6. Shared Services
7. Broadband/Wireless Connectivity
8. Data Management and Analytics
9. Enterprise IT Governance
10. Agile and Incremental Software Delivery

Source: NASCIO State CIO Ballot, November 2017

What is the current role of your CIO organization in administering the statewide cybersecurity program?



Source: NASCIO 2017 State CIO Survey

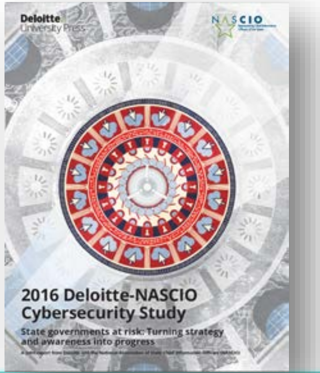
Cybersecurity involves more than *just* IT – it's a business risk.

Protecting data and infrastructure is a core responsibility of state government entities and an investment in risk management.

It's a complex ecosystem that requires a roadmap.

Emerging trends

Top cyber threats across state government

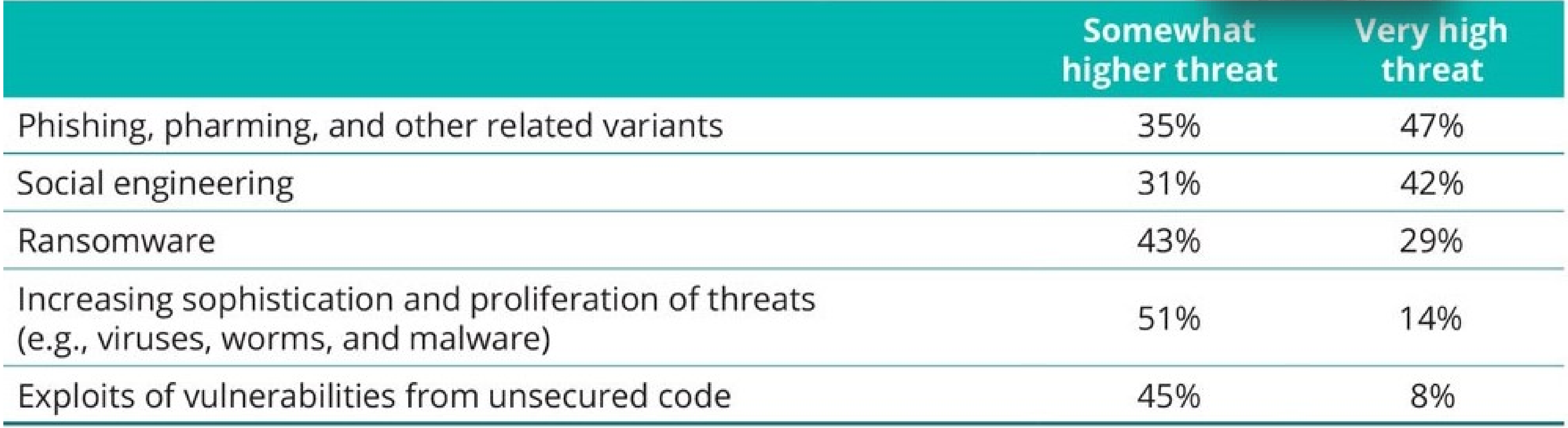


Deloitte
University Press

NASCIO

2016 Deloitte-NASCIO Cybersecurity Study

State governments at risk: Turning strategy and awareness into progress



	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%

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

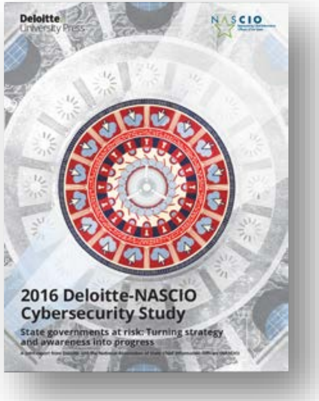
CISOs have an opportunity to make significant progress in educating stakeholders about the true magnitude of cyber risk to gain elusive support

NASCIO

Source: Deloitte-NASCIO 2016 Cybersecurity Study

Key takeaways

#1: Governor-level awareness is on the rise



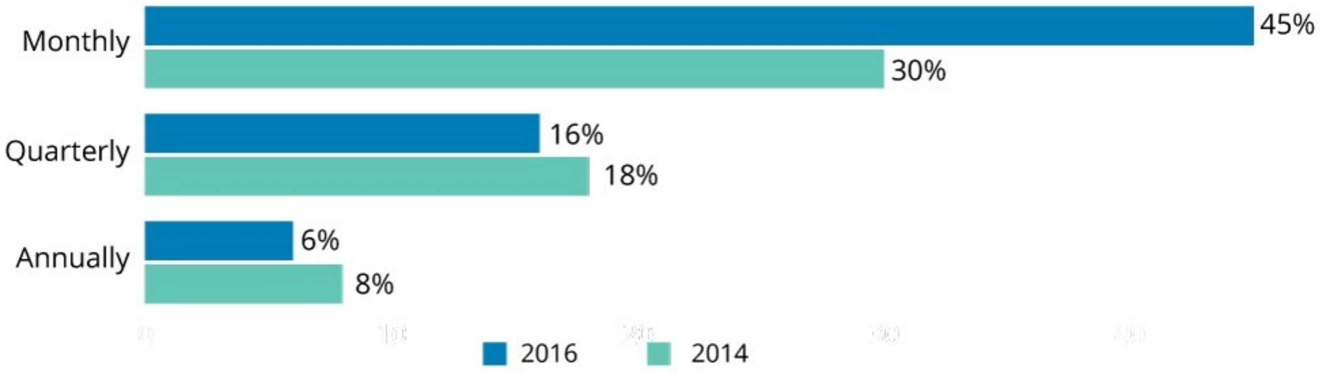
Deloitte University Press

NASCIO

2016 Deloitte-NASCIO Cybersecurity Study

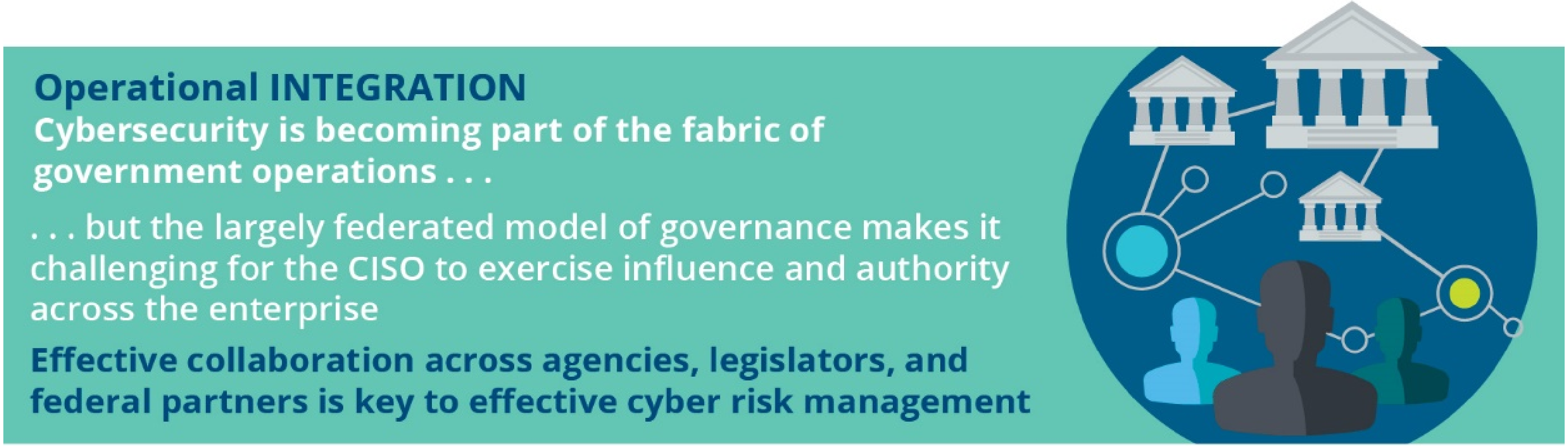
State governments at risk: Turning strategy and awareness into progress

How often is the topic of cybersecurity presented or discussed at your agency/office executive leadership meetings?



Key takeaways

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



Operational INTEGRATION

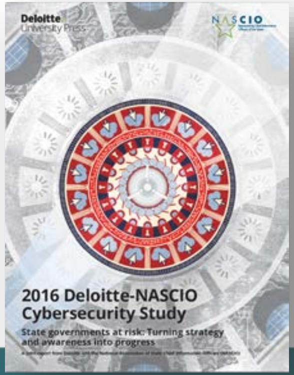
Cybersecurity is becoming part of the fabric of government operations . . .

. . . 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

Key takeaways

#3: A formal strategy can lead to more resources



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)

Formal STRATEGY

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

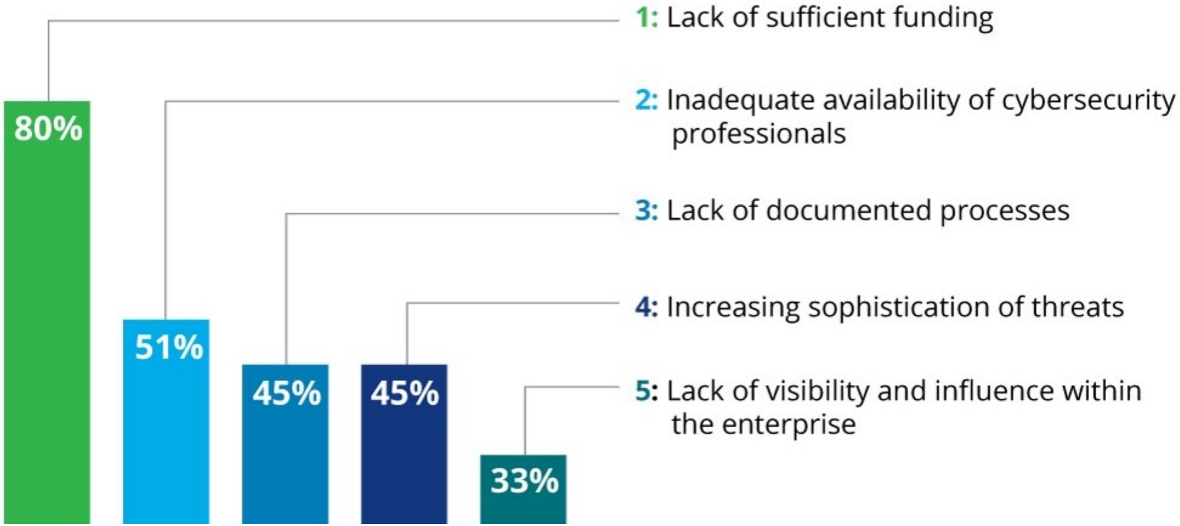
. . . but CISOs with a formal, approved cybersecurity strategy are more likely to secure funding and talent

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

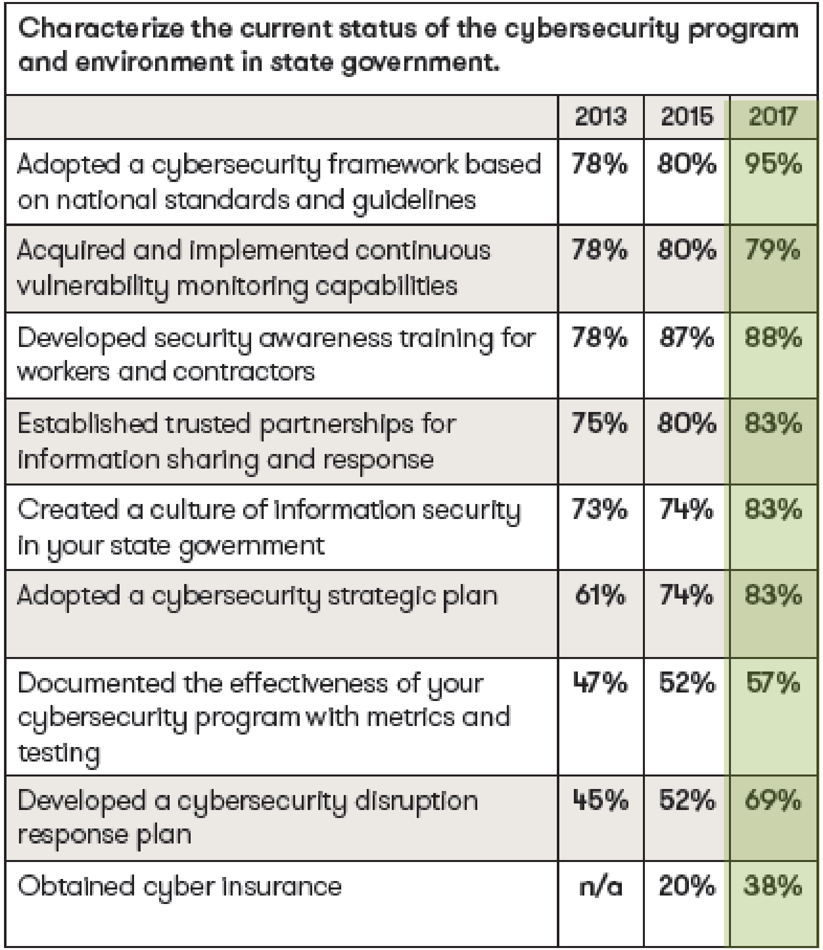
Key takeaways

#3: A formal strategy can lead to more resources

Top five barriers in addressing cybersecurity challenges



Cybersecurity Maturity in the States is Improving



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

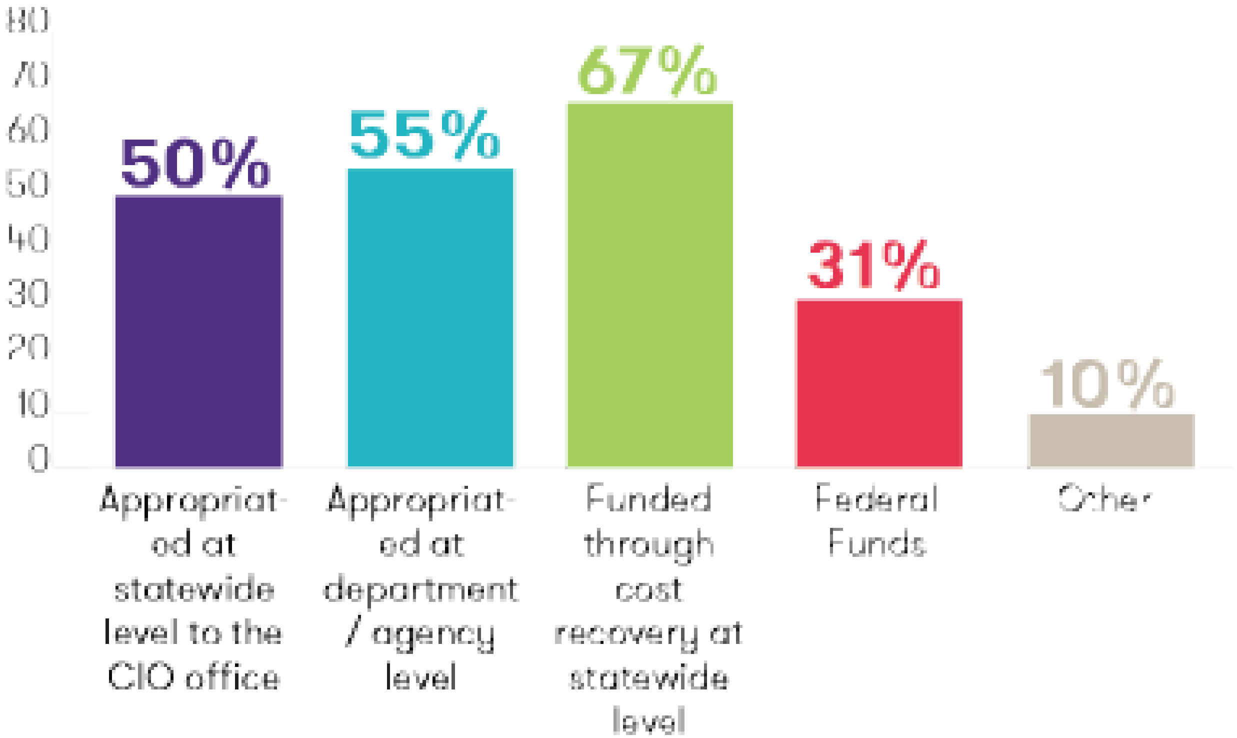
	2013	2015	2017
Adopted a cybersecurity framework based on national standards and guidelines	78%	80%	95%
Acquired and implemented continuous vulnerability monitoring capabilities	78%	80%	79%
Developed security awareness training for workers and contractors	78%	87%	88%
Established trusted partnerships for information sharing and response	75%	80%	83%
Created a culture of information security in your state government	73%	74%	83%
Adopted a cybersecurity strategic plan	61%	74%	83%
Documented the effectiveness of your cybersecurity program with metrics and testing	47%	52%	57%
Developed a cybersecurity disruption response plan	45%	52%	69%
Obtained cyber insurance	n/a	20%	38%

Risk Based Strategies are Being Adopted

Source: NASCIO 2017 State CIO Survey

NASCIO

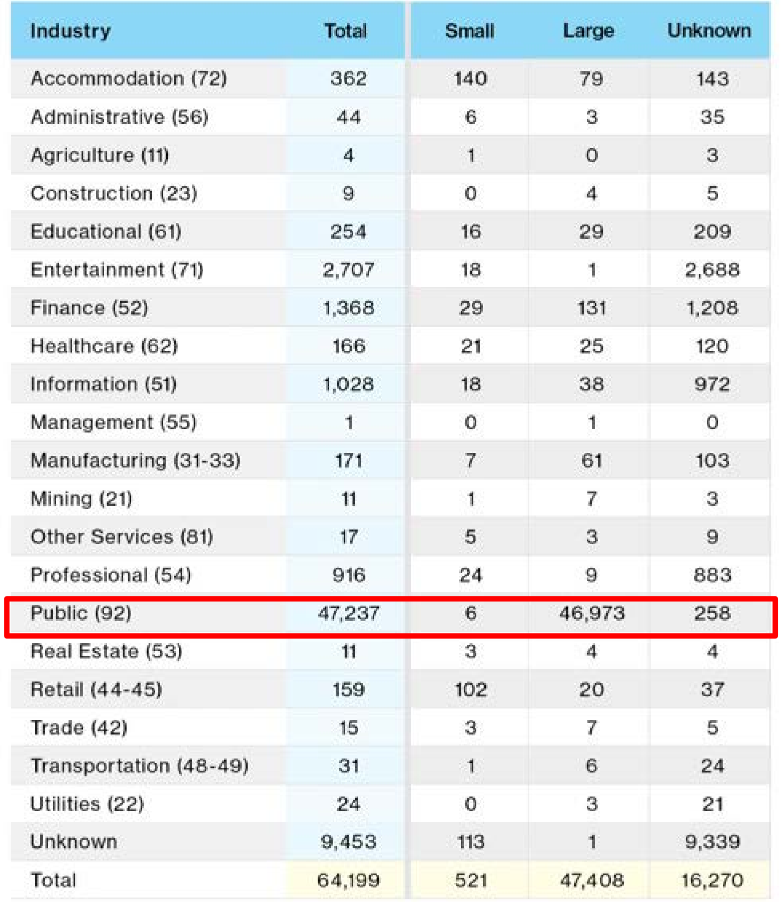
How is cybersecurity currently funded for your state?



Source: NASCIO 2017 State CIO Survey

The Human Factor

Number of security incidents by victim industry and organization size, 2015 dataset.



Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	159	102	20	37
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

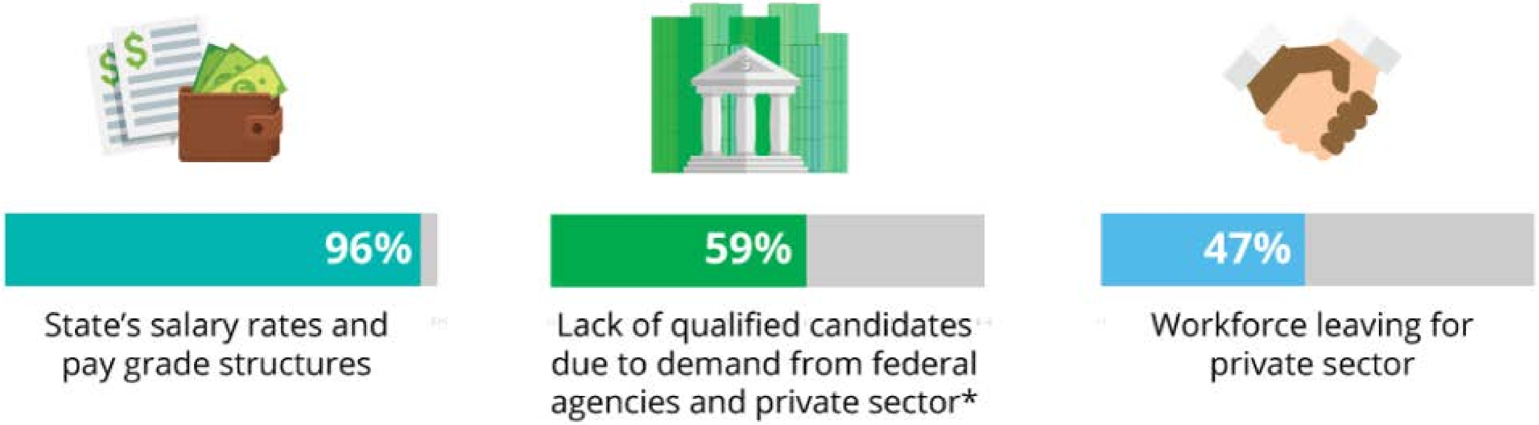
Source: *Verizon 2016 Data Breach Investigations Report*

- 63 percent of confirmed data breaches involve using weak, default or stolen passwords
- **‘Miscellaneous errors’ take the No. 1 spot for security incidents - humans!**
- Basic defenses continue to be sorely lacking in many organizations

The Talent Crisis

Talent crisis continues

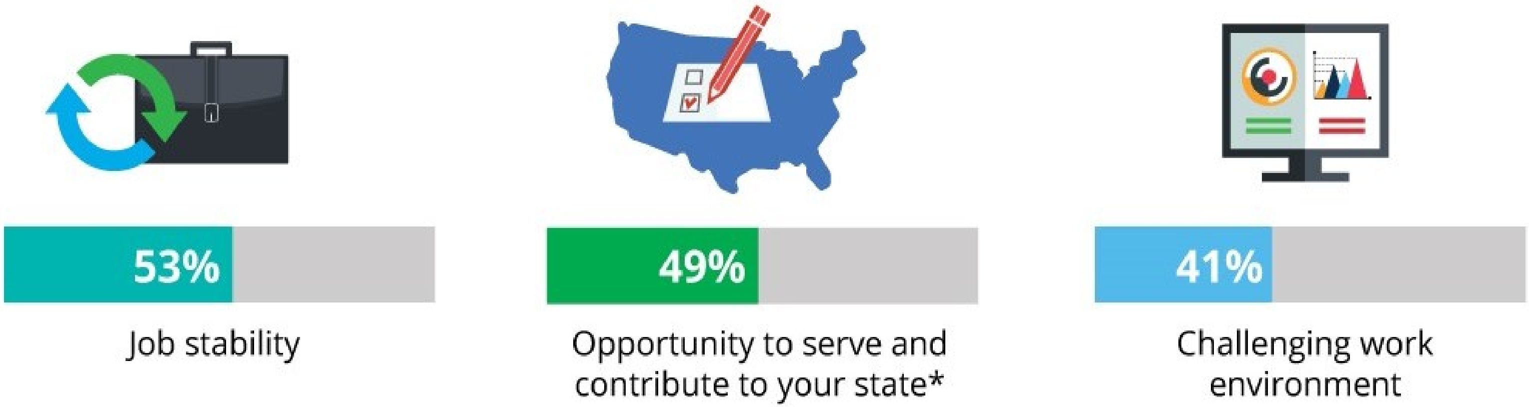
Top three human resources factors that negatively impact the CISO's ability to develop, support, and maintain cybersecurity workforce



*New in 2016

Talent crisis continues

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



What Do We Know? Patterns of Success

- Enterprise Leadership and Governance
- Statewide Cybersecurity Framework & Controls
- Cybersecurity Culture: A Team Sport
- Know the Risks, Assess the Risks, Measure
- Communicating the Risks: Training
- Invest: Deploy Security Technologies

NASCIO's Cybersecurity Call to Action
Key Questions for State Leaders

- Does your state government support a "culture of information security" with a governance structure of state leadership and all key stakeholders?
- Has your state conducted a risk assessment? Is data classified by risk? Critical infrastructure reviewed? Are security metrics available?
- Has your state implemented an enterprise cybersecurity framework that includes policies, control objectives, practices, standards, and compliance? Is the NIST Cybersecurity Framework a foundation?
- Has your state invested in enterprise solutions that provide continuous cyber threat detection, mitigation and vulnerability management? Has the state deployed advanced cyber threat analytics?
- Have state employees and contractors been trained for their roles and responsibilities in protecting the state's assets?
- Does your state have a cyber disruption response plan? A crisis communication plan focused on cybersecurity incidents?