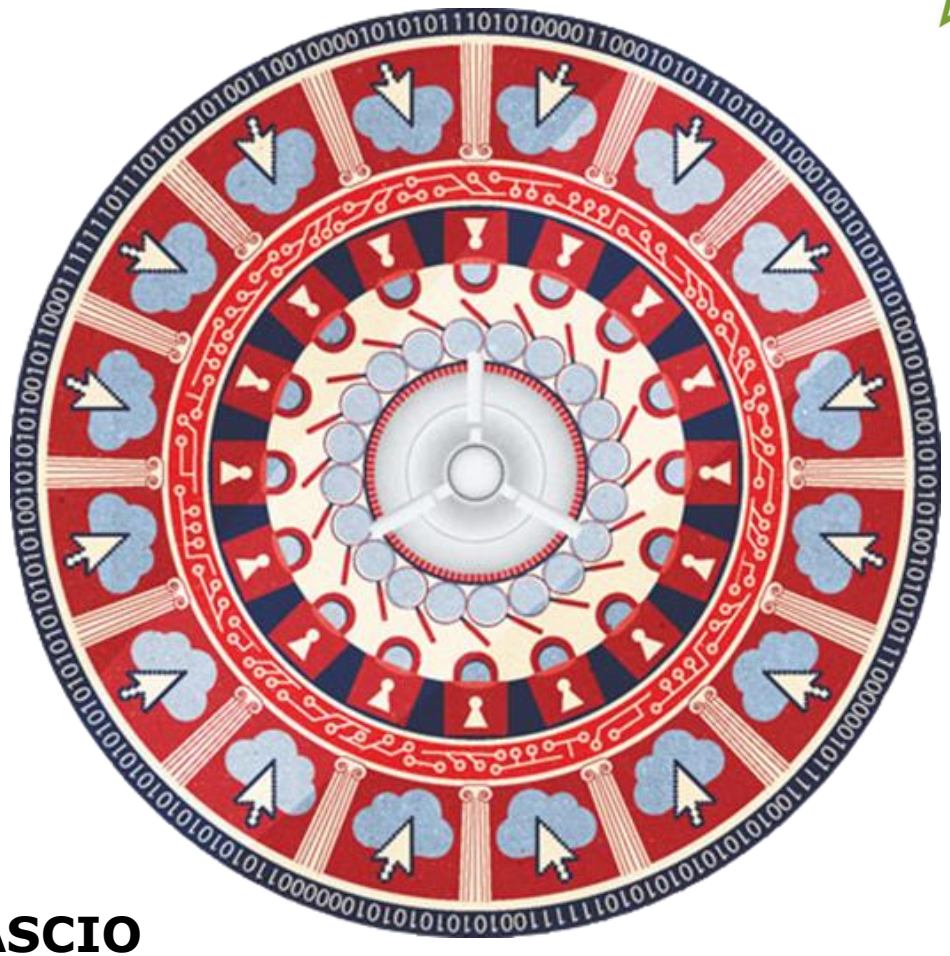
Deloitte.

NASCIO
Representing Chief Information Officers of the States



The Deloitte-NASCIO Cybersecurity Study Insights from 2010 - 2016

August 21, 2018

Srini Subramanian
State Government Sector Leader
Deloitte

Erik Avakian
CISO
Pennsylvania

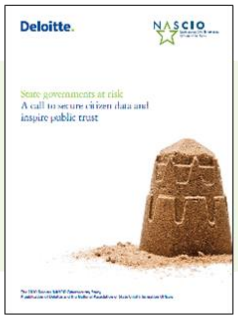
Michael Roling
CISO
Missouri

Meredith Ward
Senior Policy Analyst
NASCIO

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

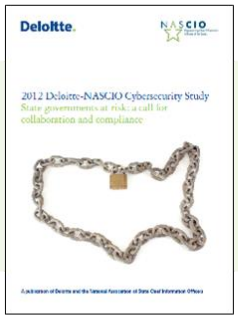
Key findings

2010



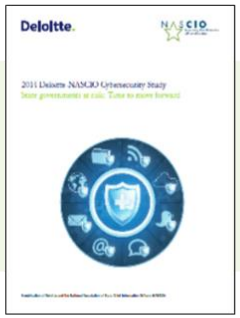
A call to secure citizen data and inspire trust

2012



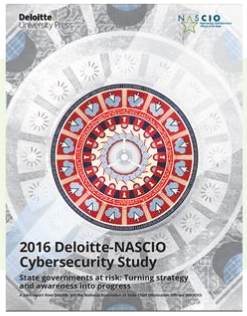
A call for collaboration and compliance

2014



Time to move forward

2016



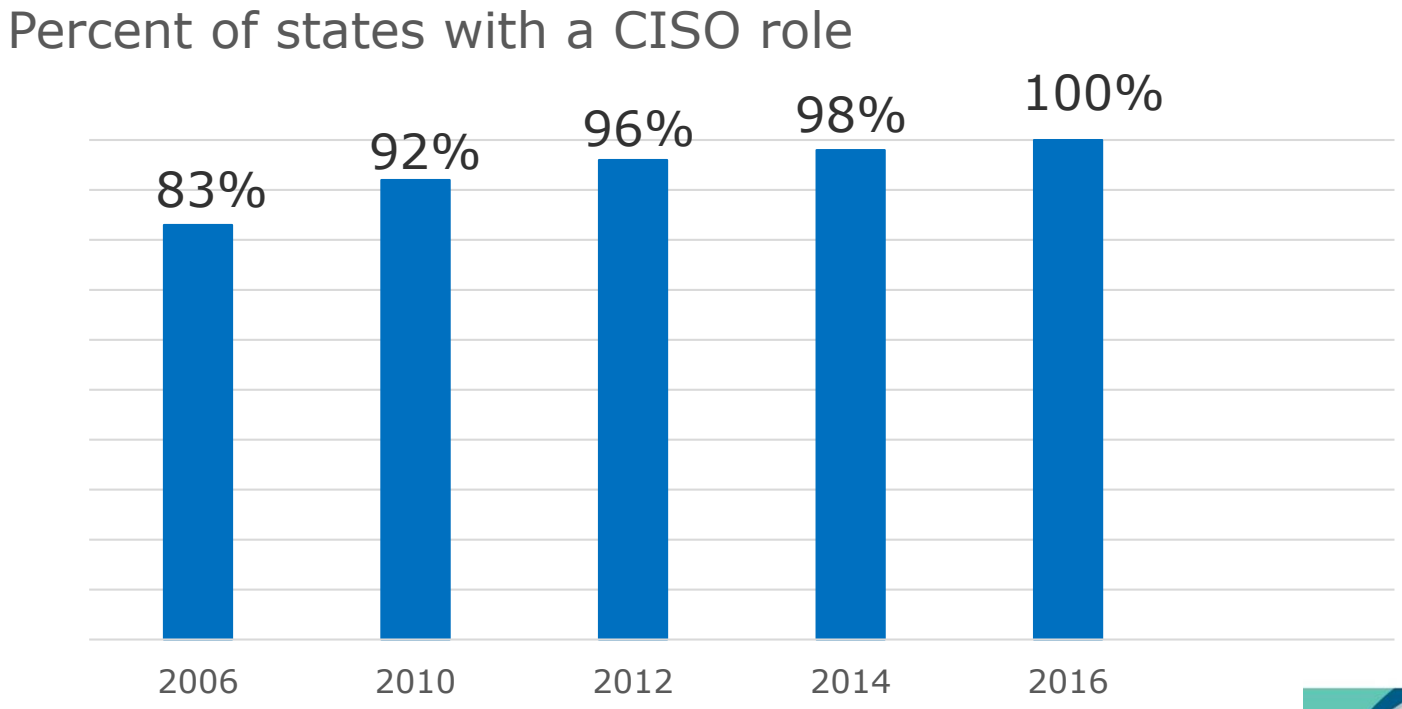
Turning strategy and awareness into progress

- **2010**: Governance; strategy; budget; internal, external threats and creating a cyber mindset; security of third party providers
- **2012**: Cybersecurity budget-strategy connection; cyber authority and governance; preparedness for emerging threats; compliance—a lever for CISO leadership
- **2014**: Maturing role of the CISO; continuing budget-strategy disconnect; cyber complexity challenge; talent crisis
- **2016**: Governor-level awareness is on the rise; cybersecurity is becoming part of the fabric of government operations; a formal strategy and better communications lead to greater command of resources.

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

The growth of the CISO role

100% of states now have an enterprise-level CISO with associated cyber risk management authority



Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Full-time Employees (FTEs)

Dedicated cybersecurity professionals employed by the state's enterprise security office

- **2010**: 47% with 1 to 5
- **2012**: 50% with 1 to 5
- **2014**: 49% with 6 to 15
- **2016**: 51% with 6 to 15
- **2018**: 49% with 6 to 15

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

State of cyber workforce in 2016

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

96%

State's salary rates and pay grade structures

59%

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

47%

Workforce leaving for private sector

*New in 2016

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

State of cyber workforce in 2018

Top negative impact:

State's salary rates and pay grade structures

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Documented security strategy

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

Percentage of states with a formal, documented cybersecurity strategy

- **2010**: 55%
- **2012**: 46%
- **2014**: 55%
- **2016**: 67%

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Reporting/briefing

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

- **2010**: Reporting was to agency leadership, CIO's. No governors.
- **2012**: 19.1% reporting to governor annual; 23.4% reporting legislature annually
- **2014**: 39.6% reporting to governor on ad hoc basis; 40.4% reporting to legislature ad hoc
- **2016**: 40% reporting to governor on ad hoc; 29% monthly
- **2018**: nearly 30% briefing governors on a monthly basis

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Barriers

Top barriers in addressing cybersecurity challenges

- Lack of sufficient funding (2010, 2012, 2014, 2016)
- Inadequate availability of cyber professionals (2010, 2012, 2014, 2016)
- Increasing sophistication of threats (2010, 2012, 2014, 2016)
- Lack of visibility and influence within enterprise (2010, 2012, 2014, 2016)
- Lack of documented processes (2010, 2014, 2016)
- Emerging technologies (2010, 2012)

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

IT budget allocated to information security

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

- **2010**: Majority: 1-3% of budget
- **2012**: Majority: 1-3% of budget
- **2014**: Majority: 1-2% of budget
- **2016**: Majority: 1-2% of budget; 20% said 3-5%

Budget allocation has made some improvement, but continues to remain a top challenge

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Chief privacy officer (CPO)

Percentage of state's with a defined CPO role

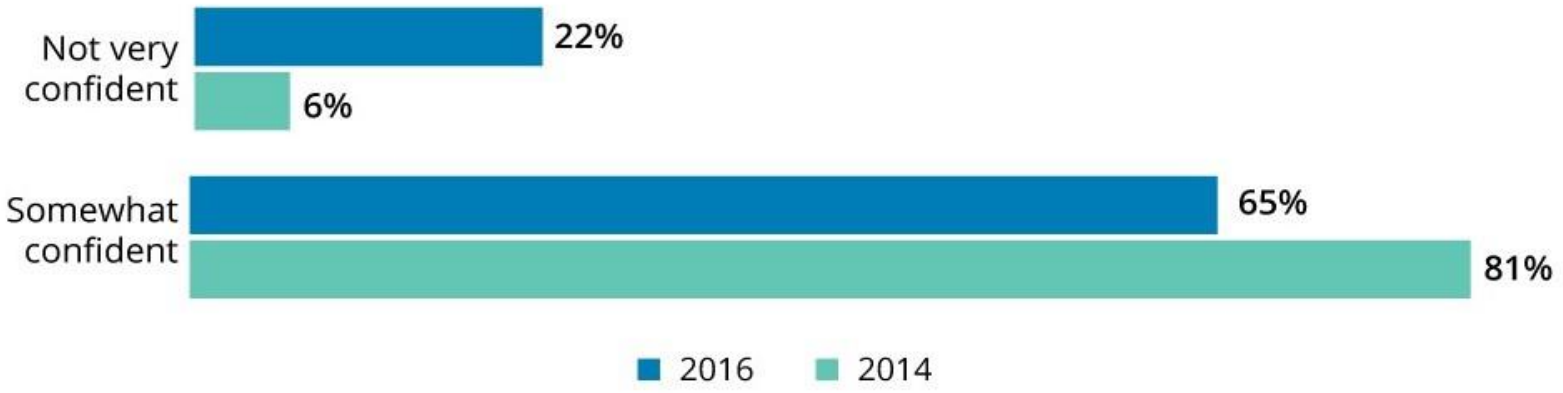
- **2010**: 18% of states had one
- **2012**: 18%
- **2014**: 29.2%
- **2016**: 18%
- **2018**: 28%

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Confidence in third parties

CISOs' confidence in cybersecurity practices followed by third parties

- **2010**: 69% said somewhat confident; 23% said 3rd party security capabilities and controls are unknown
- **2012**: 74% somewhat confident
- **2014**: 81.3% somewhat confident
- **2016**: 65% somewhat confident



Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Top outsourced cybersecurity functions

Which functions do states outsource?

2010	2012	2014	2016
24% threat monitoring **11%** vulnerability management	**40%** threat management and monitoring **20%** security technology services	**39%** forensics/ legal support **37%** threat monitoring **37%** risk assessments **18%** vulnerability management **18%** security tech. services **18%** audit log analysis & reports	**54%** cyber threat risk assessments **44%** forensics/ legal support **35%** cyber threat mgmt. & monitoring **27%** vulnerability management **23%** audit log analysis & reports

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Top outsourced cybersecurity functions

Outsourced Functions	2016	2014	2012	2010
Cyber threat risk assessments	54%	37%	-	-
Forensics/legal support	44%	39%	-	-
Cyber threat management and monitoring services	35%	37%	40%	24%
Vulnerability management	27%	18%	-	11%
Audit log analysis and reports	23%	18%	-	-
Security technology services	-	18%	20%	-

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Top five cybersecurity initiatives by study

2010	2012	2014	2016
• Data protection • Information security risk assessments • Information security training and awareness • Application security • Security infrastructure improvement	• Risk assessments • Training and awareness • Data protection • Strategy • Governance	• Risk assessments • Training and awareness • Data protection • Continuous monitoring/SO • Incident response	• Training and awareness • Continuous monitoring/ SOC • Strategy • Governance • Operationalizing cybersecurity

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

Top cybersecurity initiatives 2018

Risk assessments

Metrics to measure and report effectiveness

Source: Deloitte-NASCIO Cybersecurity Studies, 2010-2016

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.