# State Governments at Risk: Cybersecurity Update

## Vermont General Assembly
## Joint Information Technology Oversight Committee

**August 23, 2019**

**Doug Robinson, NASCIO Executive Director**
**@NASCIO**

NASCIO
Representing Chief Information Officers of the States

# About NASCIO

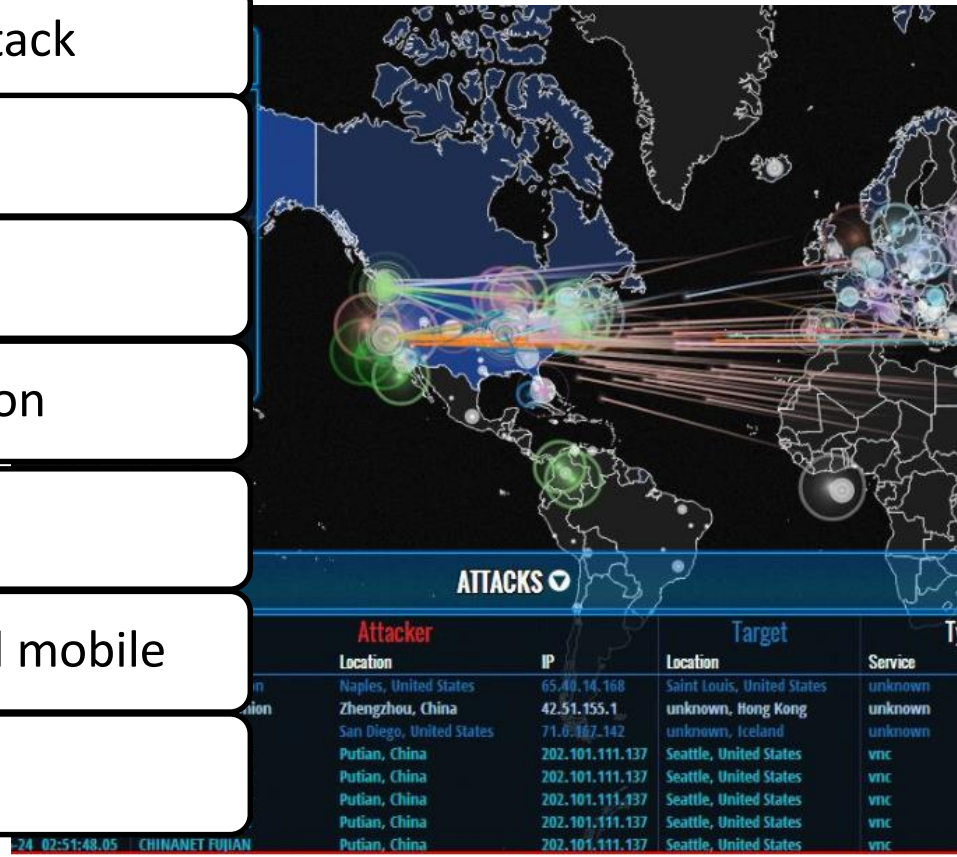
- National association representing state chief information officers and information technology executives from the states, territories and D.C.

- 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.

# State Governments at Risk!

- States are attractive targets – constant attack
- More aggressive threats, more intensity
- Nation state threats, organized crime
- Critical infrastructure protection: disruption
- Human factor – employees, contractors
- Data and services on the move: cloud and mobile
- Elections security!




NASCIO

# Ransomware Attacks Are Testing Resolve of Cities Across America


A handwritten sign posted near City Hall in Baltimore after some of the government's computer systems were hacked in May. The city, which did not pay a ransom of about $76,000, has spent more than $5.3 million to recover from the attack.
Stephanie Keith/Reuters

By Manny Fernandez, David E. Sanger and Marina Trahan Martinez

Aug. 22, 2019, 5:00 a.m. ET

# By the Numbers: Government Risk

| | |
|---|---|
| **75%** | Hacks perpetrated by external actors in the government sector |
| **94%** | Email is the primary point of entry |
| **2.5X** | Public breaches are more likely to go undiscovered for years |
| **#1** | Government holds the top spot for both incidents and breaches |

# What's the Current Situation?


- Critical life, health and safety systems must be available
  - Public Safety
  - Crucial Services to Citizens
- States hold billions of confidential records
  - Personally Identifiable Information (PII)
  - Personal Health Information (PHI)
  - Intelligence
  - Other Confidential
- Information integrity must be maintained
- Must be able to withstand and recover

# 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 governance and regular communication on risk.

# STATE CIO TOP 10 PRIORITIES

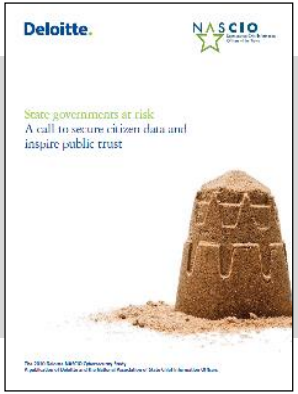
## 2019 Strategies, Management & Process Solutions

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

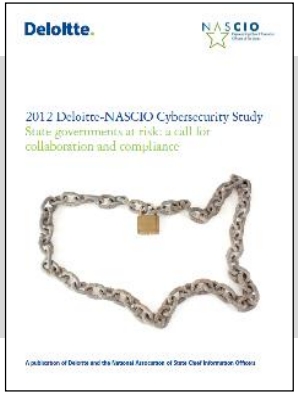
# Timeline of the Deloitte – NASCIO Cybersecurity Study
## *States at Risk*

**2010**



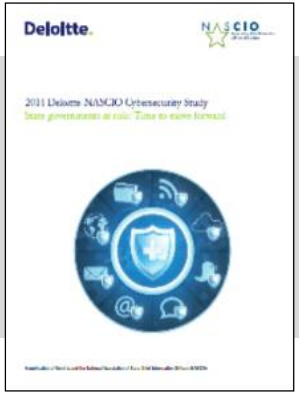

**A call to secure citizen data and inspire trust**

**2012**



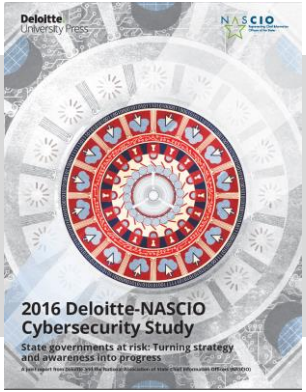

**A call for collaboration and compliance**

**2014**




**Time to move forward**

**2016**



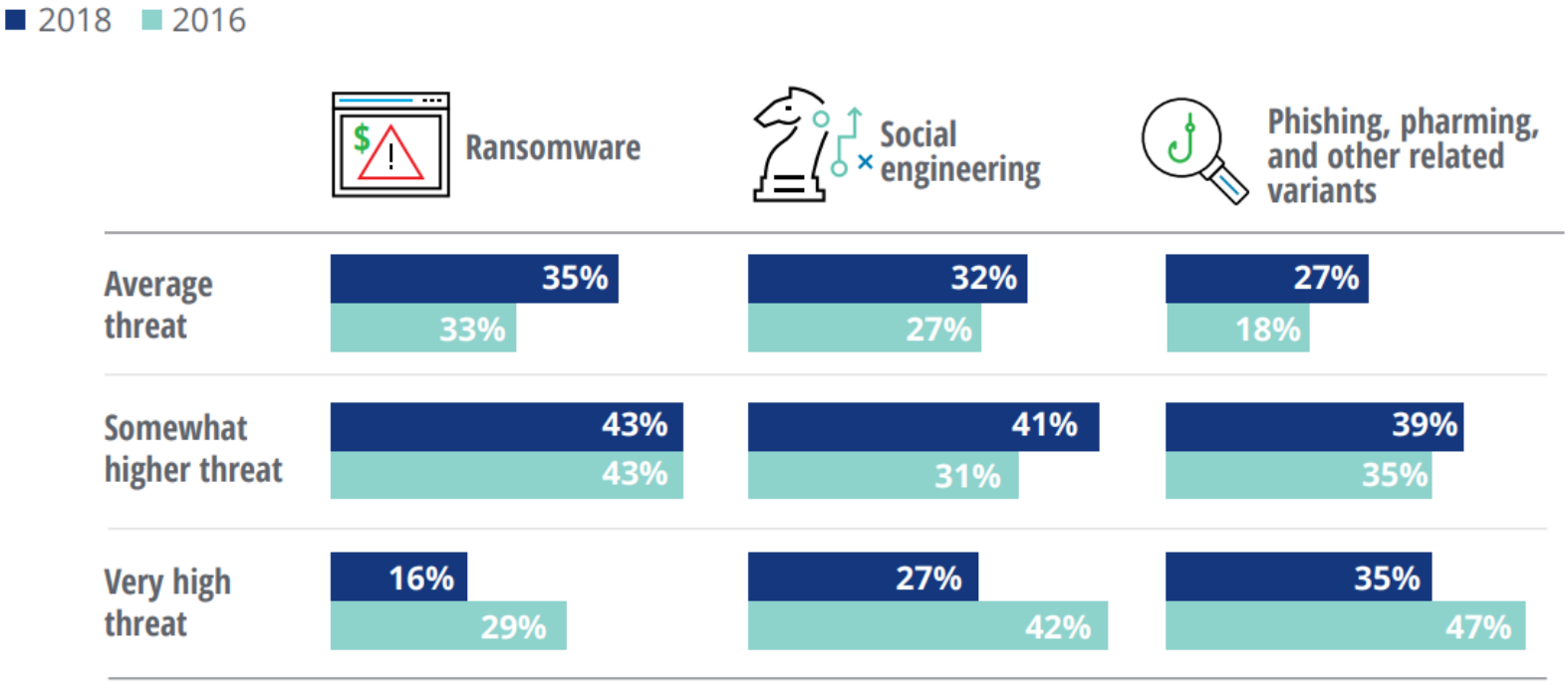

**Turning strategy and awareness into progress**

**2018**


**Bold plays for change**

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

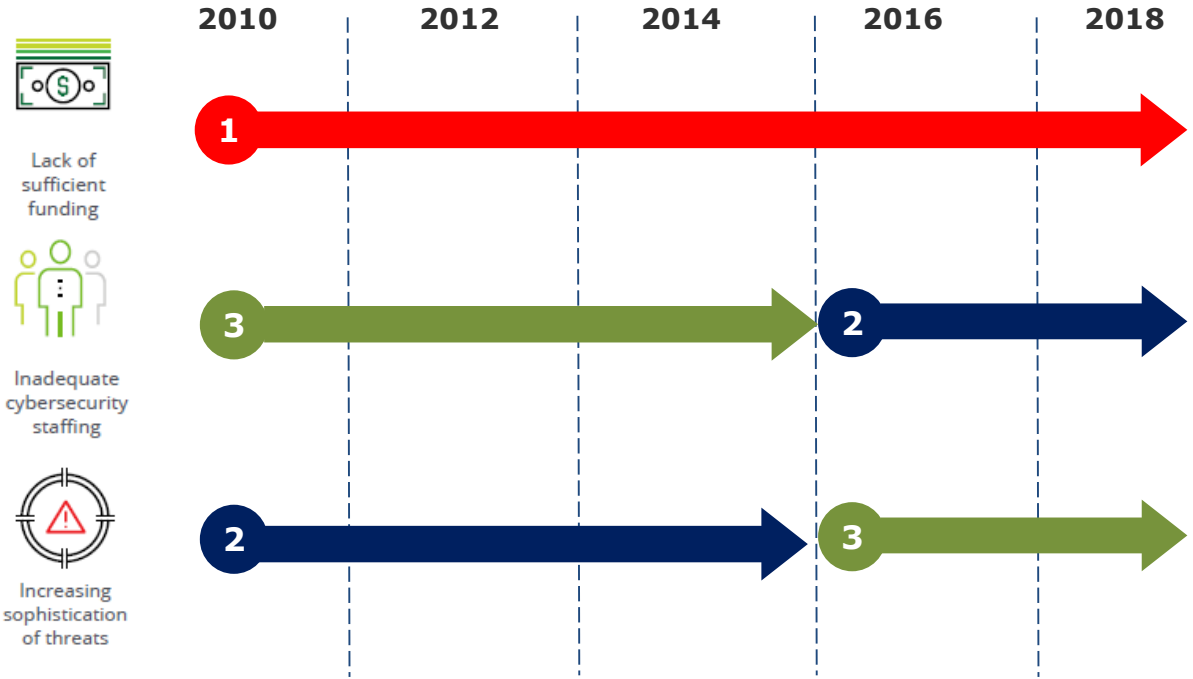
Please choose the prevalence of the following cyber threats in your state for the next year. (49 respondents)




Source: 2018 Deloitte-NASCIO Cybersecurity Study

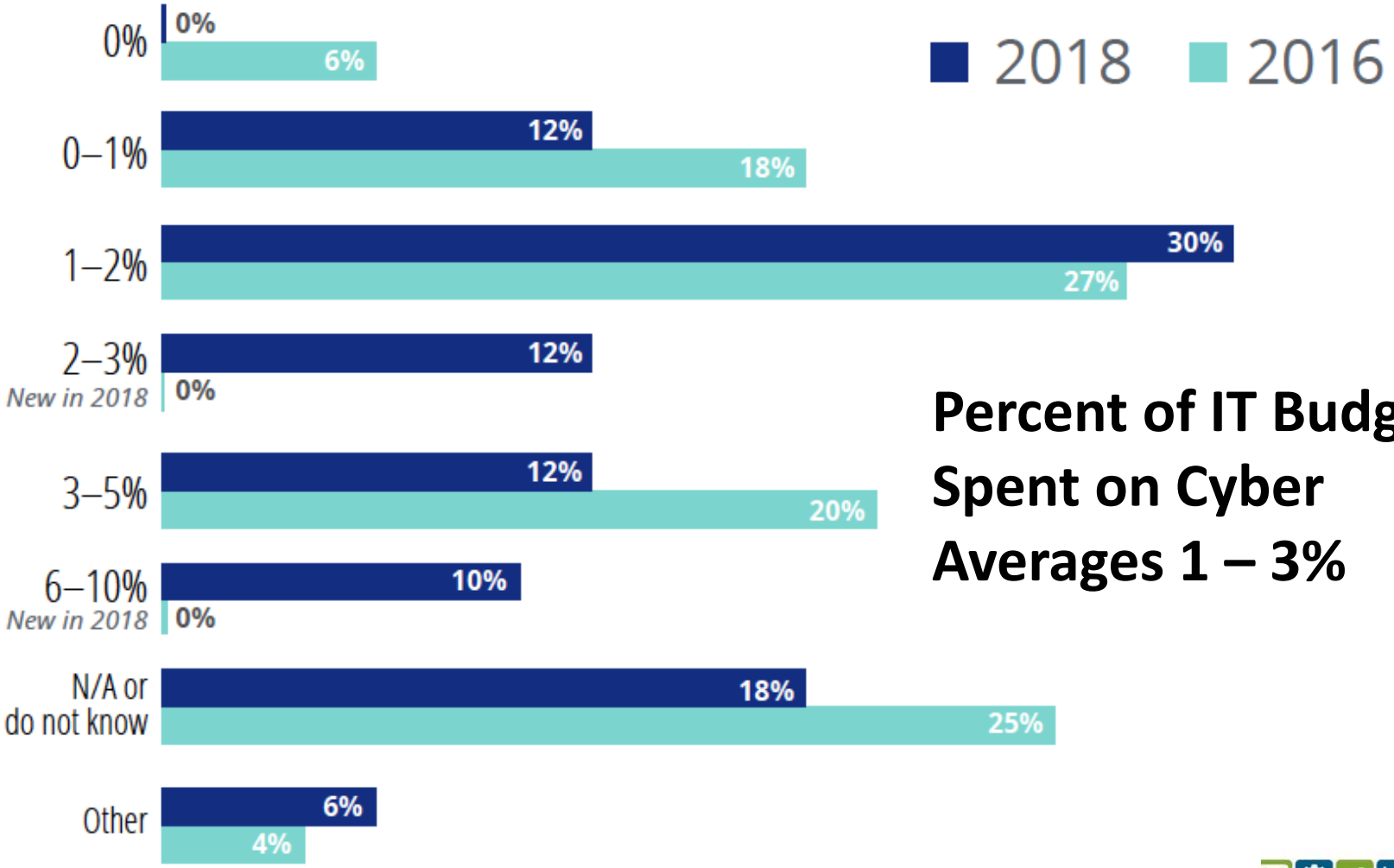
# Persistent challenges remain…

## Budget, talent, and threats top three since 2010




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

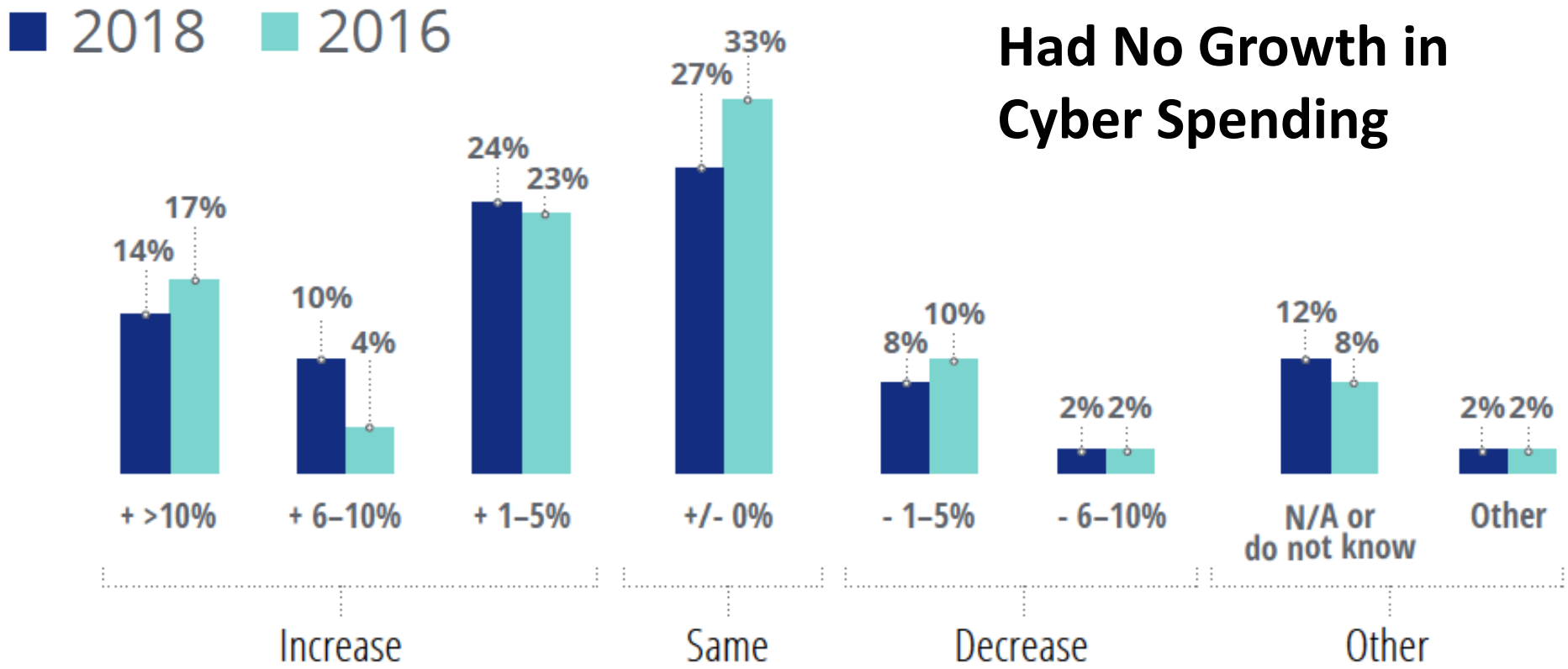
Source: 2018 Deloitte-NASCIO Cybersecurity Study



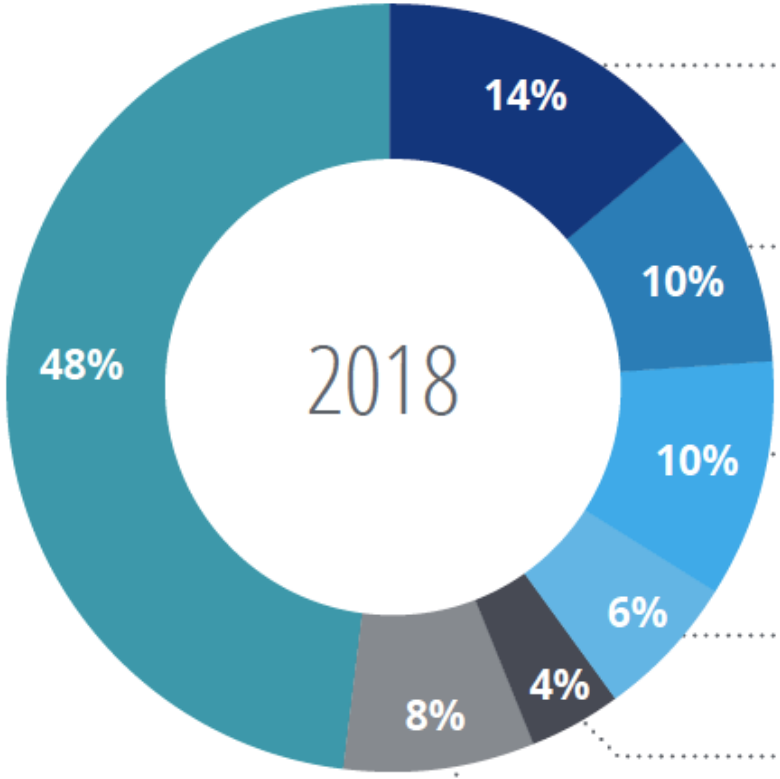

**Percent of IT Budget Spent on Cyber Averages 1 – 3%**

NASCIO

# 51% Percent of States Had No Growth in Cyber Spending



# 48% Percent of States Have No Dedicated Cyber Budget




**Yes**, established by secretary or CIO

**Yes**, established by statute or law

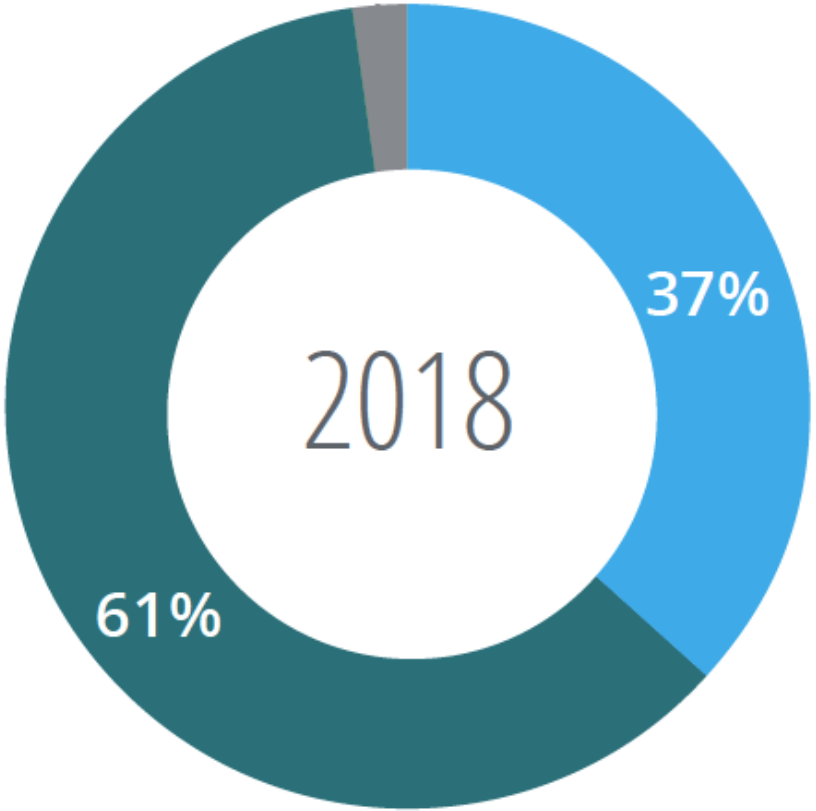
**Yes**, established by an executive (governor's) order

**Yes**, established by administrative rule, regulation, or procedure

Not applicable/do not know

Other

**No**, as part of the overall IT budget




**61% of State CISOs Say That They Lack the Collective Competency to Manage Cyber Risks**

# 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)

# 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.

# Cybersecurity maturity in the states is improving

**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

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

**88%** Leading or participating in policy setting

**88%** Responsible for setting overall direction

**76%** Responsible for execution

**86%** Responsible for oversight

**4%** Not CIO responsibility

NASCIO Representing Chief Information Officers of the States

Grant Thornton

CompTIA

# What major barriers does your state face in addressing cybersecurity?

**82%** Increasing sophistication of threats

**71%** Inability to attract and retain top-tier security and privacy talent

**47%** Lack of adequate funding

**43%** Inadequate availability of security professionals

**31%** Emerging technologies

**31%** Lack of support from business stakeholders

**29%** Lack of visibility and influence within the enterprise

**22%** Lack of legislative support

**18%** Lack of governance and authority

**12%** Inadequate competence of security professionals

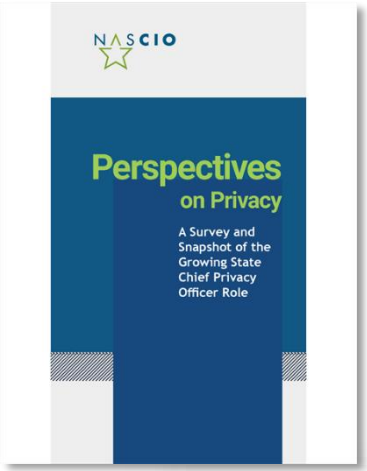
**8%** Lack of executive support

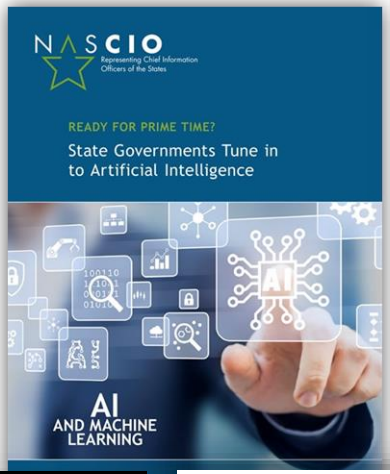
# What Do We Know? Patterns of Success

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

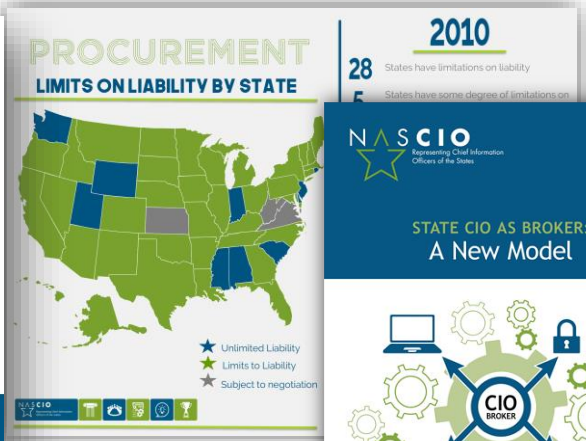
# NASCIO's Cybersecurity Call to Action
# Key Questions for State Leaders

- 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?


NASCIO
Perspectives
on Privacy
A Survey and Snapshot of the Growing State Chief Privacy Officer Role

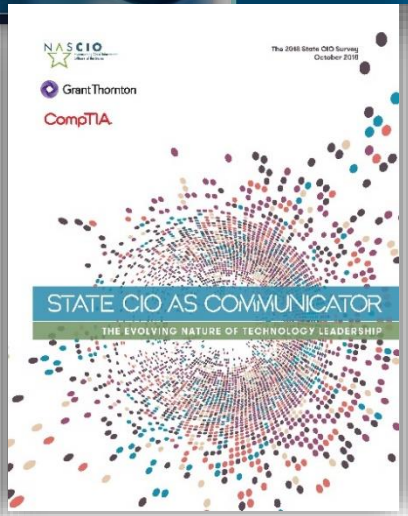

NASCIO
Representing Chief Information Officers of the States
READY FOR PRIME TIME?
State Governments Tune in to Artificial Intelligence
AI
AND MACHINE LEARNING

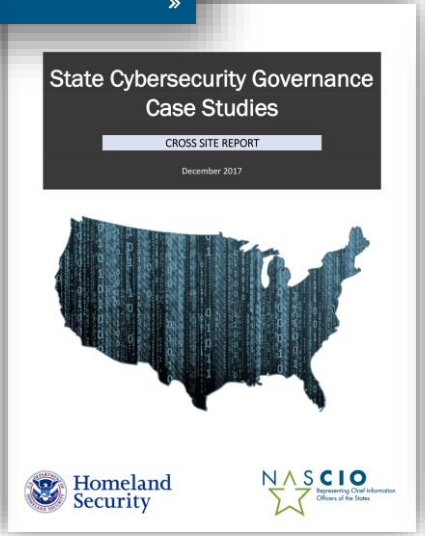

STATE ARCHIVING IN THE DIGITAL ERA
A Playbook for the Preservation of Electronic Records
October
2018
NASCIO
CoSA

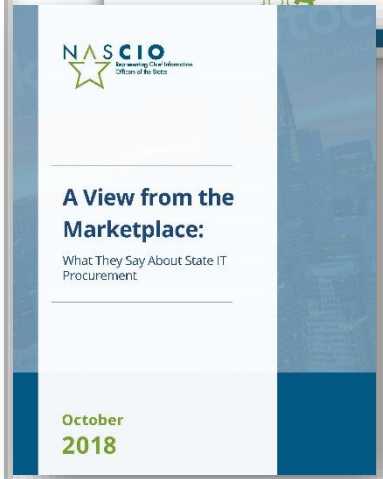

PROCUREMENT
LIMITS ON LIABILITY BY STATE
2010
28 States have limitations on liability
Unlimited Liability
Limits to Liability
Subject to negotiation


NASCIO
Representing Chief Information Officers of the States
STATE CIO AS BROKER:
A New Model
CIO
BROKER


Deloitte.
Insights
NASCIO
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
Grant Thornton
CompTIA
The 2018 State CIO Survey
October 2018
STATE CIO AS COMMUNICATOR
THE EVOLVING NATURE OF TECHNOLOGY LEADERSHIP


State Cybersecurity Governance Case Studies
CROSS SITE REPORT
December 2017
Homeland Security
NASCIO
Representing Chief Information Officers of the States


NASCIO
Representing Chief Information Officers of the States
A View from the Marketplace:
What They Say About State IT Procurement
October
2018

NASCIO