States at Risk: Cybersecurity Threats, Laws, and Access to Public Information

2019 National FOI Summit
April 12, 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.

22 new governors in 2018; 25 state CIO transitions in the last twelve months. 15 CIO transitions in 2019 to date

More focus on cybersecurity governance, risk frameworks, infrastructure protection, investments, cyber workforce crisis

CIO as broker business model: evolution from owner-operator to more managed services and multi-sourcing initiatives

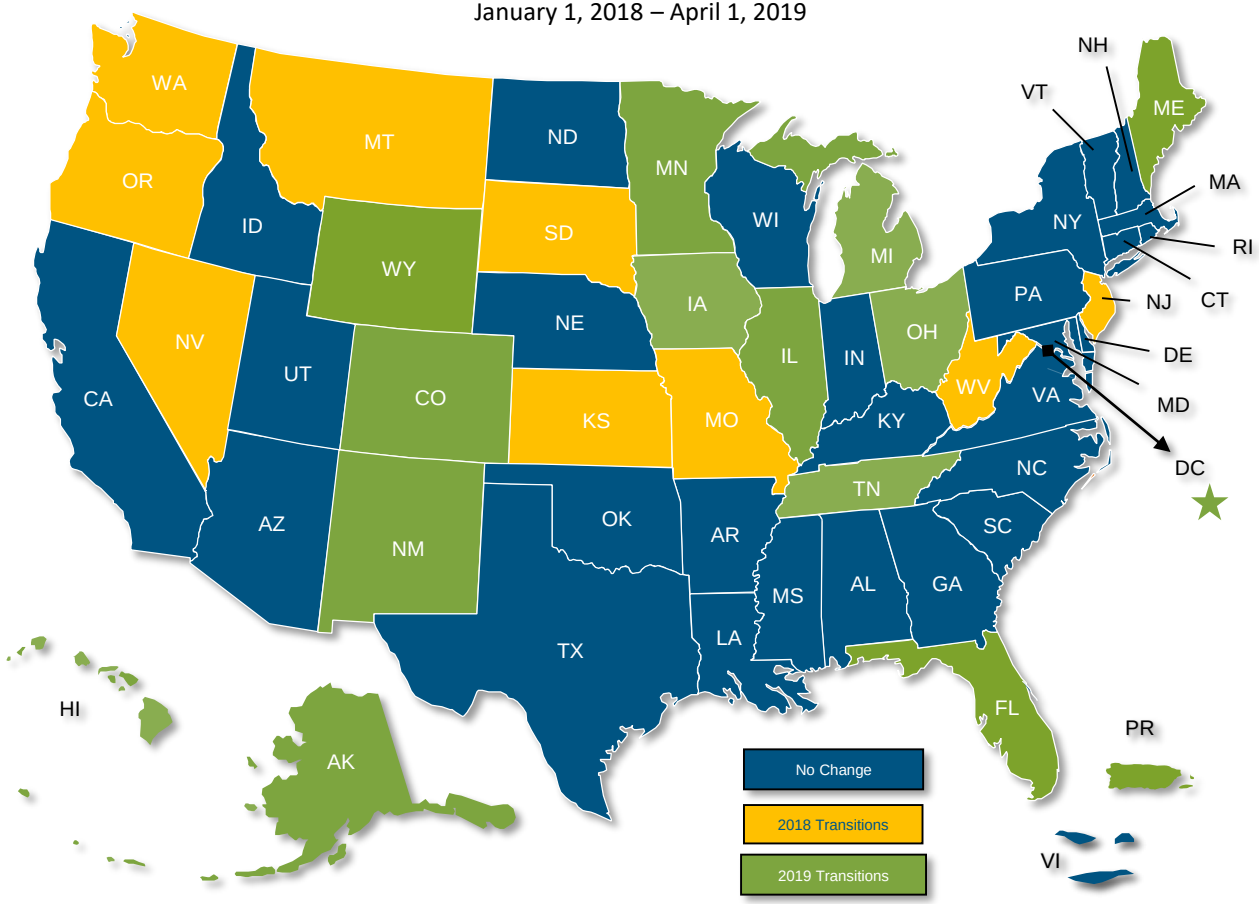
Digital government: user centric design, citizen IAM

Interest and use of AI and RPA slowly grows as state roadmaps are created and benefits are realized

State IT organization transition continues: more consolidation, hybrid models and unification initiatives

State CIO Transitions 2018-19

January 1, 2018 – April 1, 2019

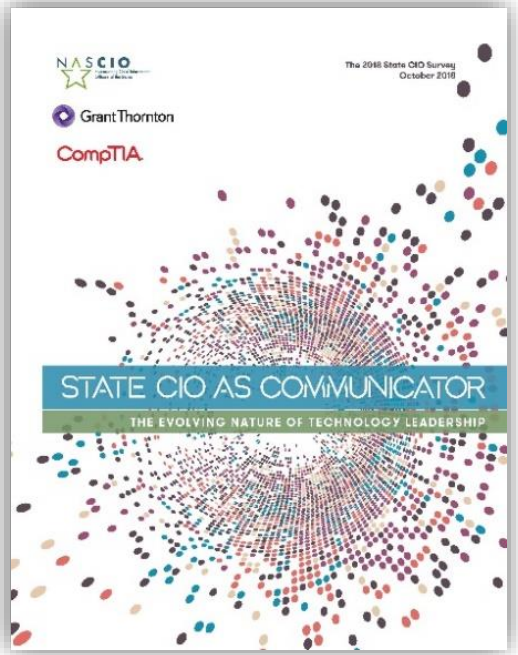


STATE CIO TOP 10 PRIORITIES

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



What would you consider your top priorities/ goals as a CIO?

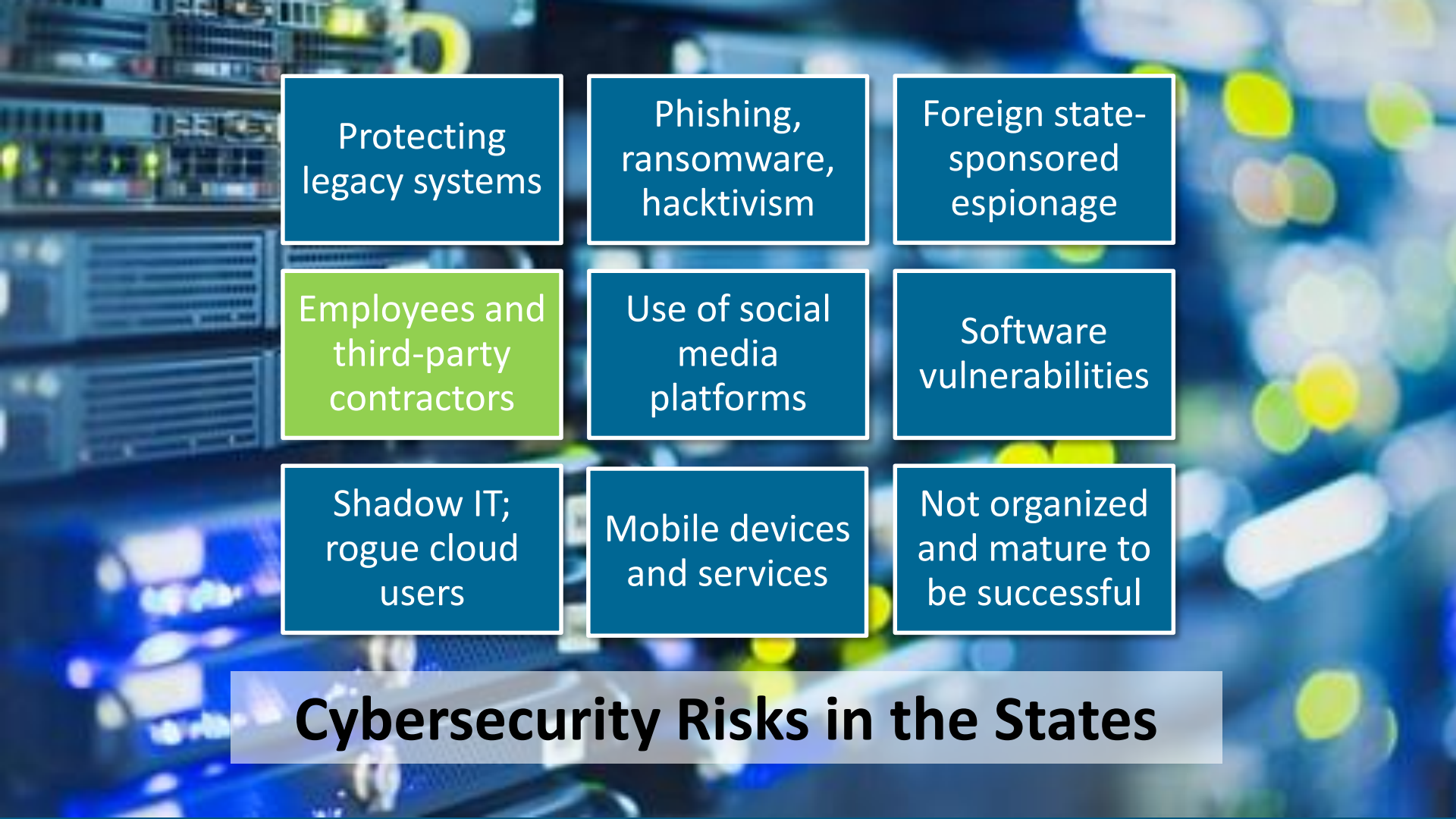
64% Ensure IT systems comply with security and regulatory requirements

60% Improve IT relationships with the business

58% Create and drive IT strategy that aligns to overall state objectives

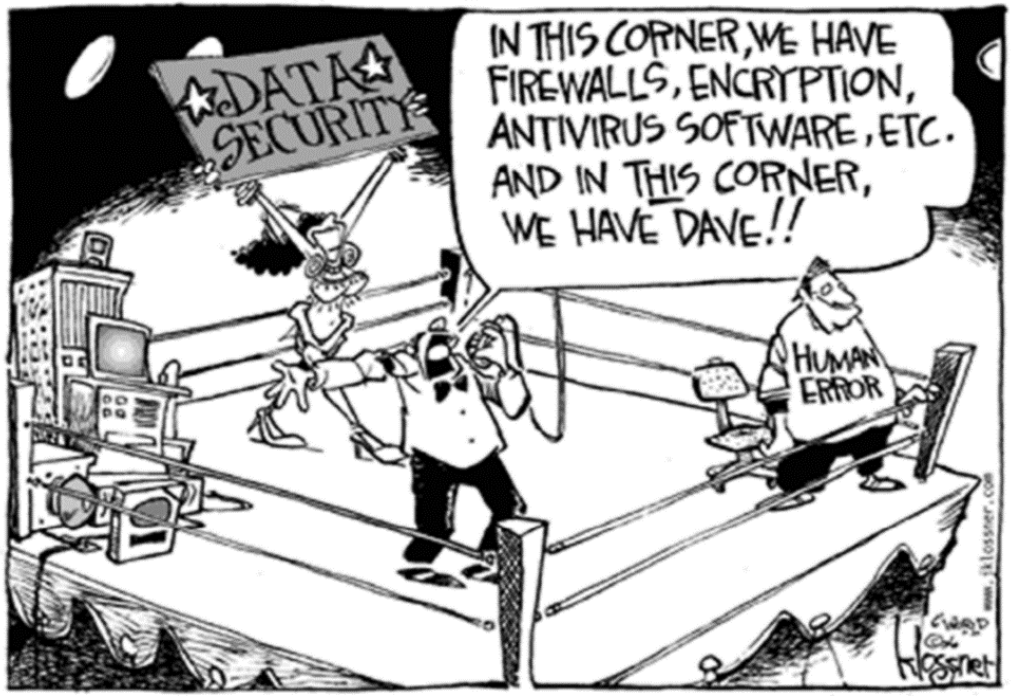
48% Improve IT governance

40% Improve portfolio management and project delivery metrics



Cybersecurity Risks in the States

Humans…


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

What Do States Care About?

State Business Risk

- Life, Health and Safety
- Delivering Services to Citizens
- Delivering Services to Employees

Financial Risk

- Lost Revenue
- Fraud and Theft
- Breach Costs

Privacy & Confidentiality Risk

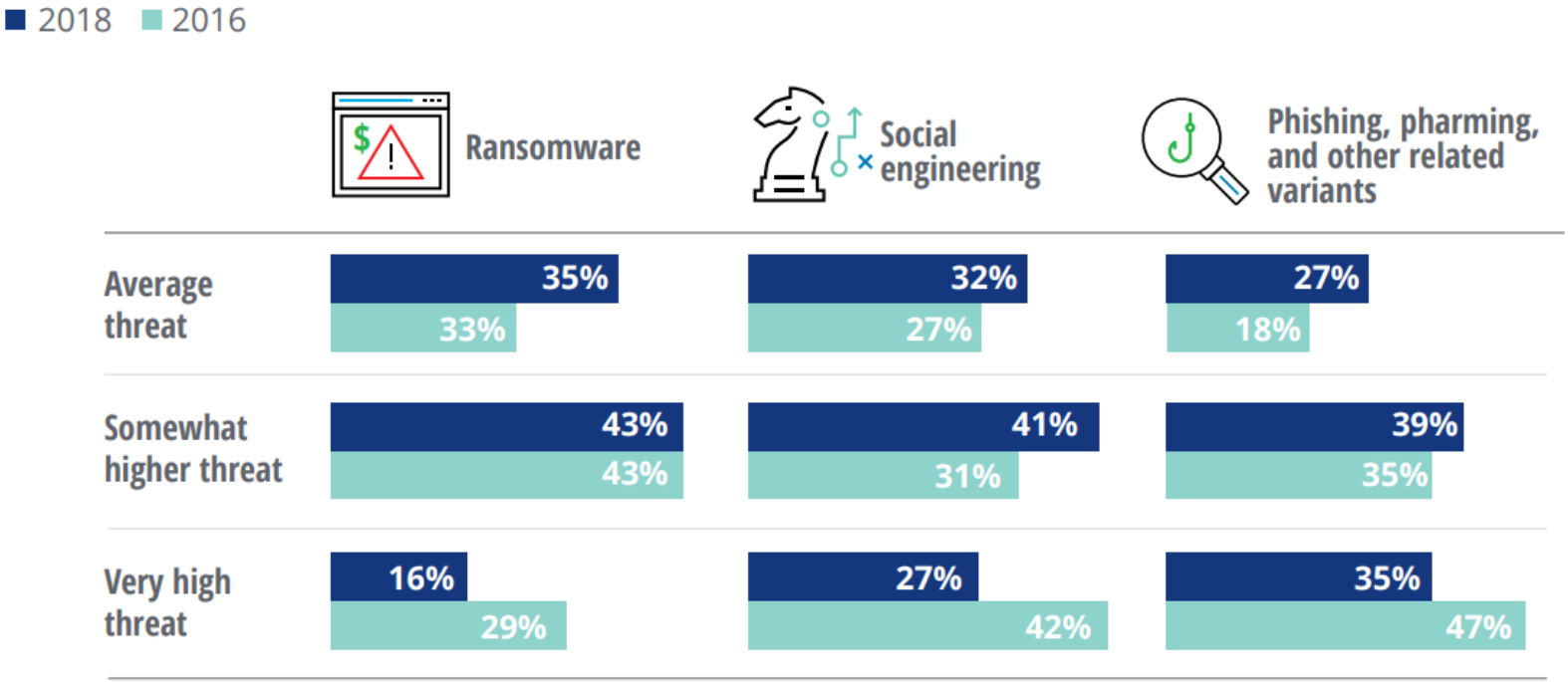
- Personal Information – Identify Theft (PII)
- Confidential Information

Reputational/Political Risk

- Elected Officials
- Agency Directors
- Program Managers

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

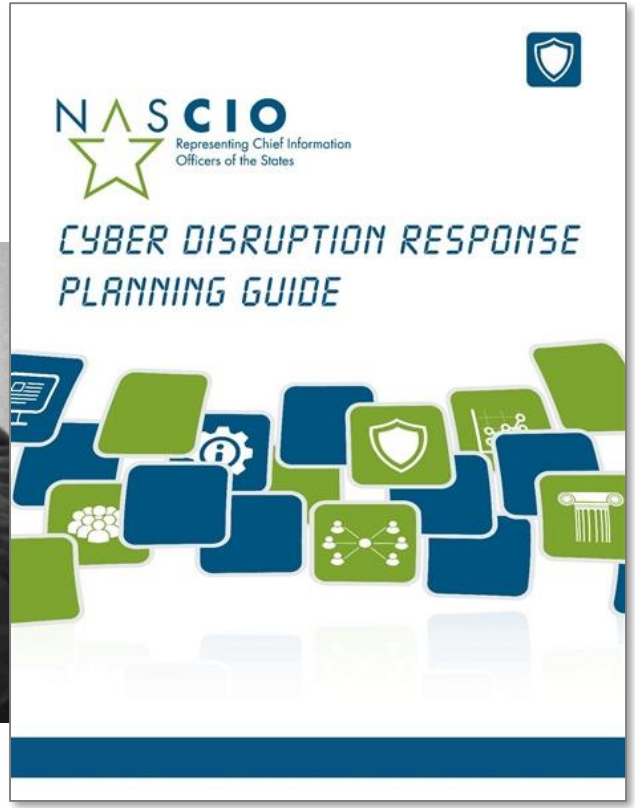
Please choose the prevalence of the following cyber threats in your state for the next year. (49 respondents)



Source: 2018 Deloitte-NASCIO Cybersecurity Study

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. "



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

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

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



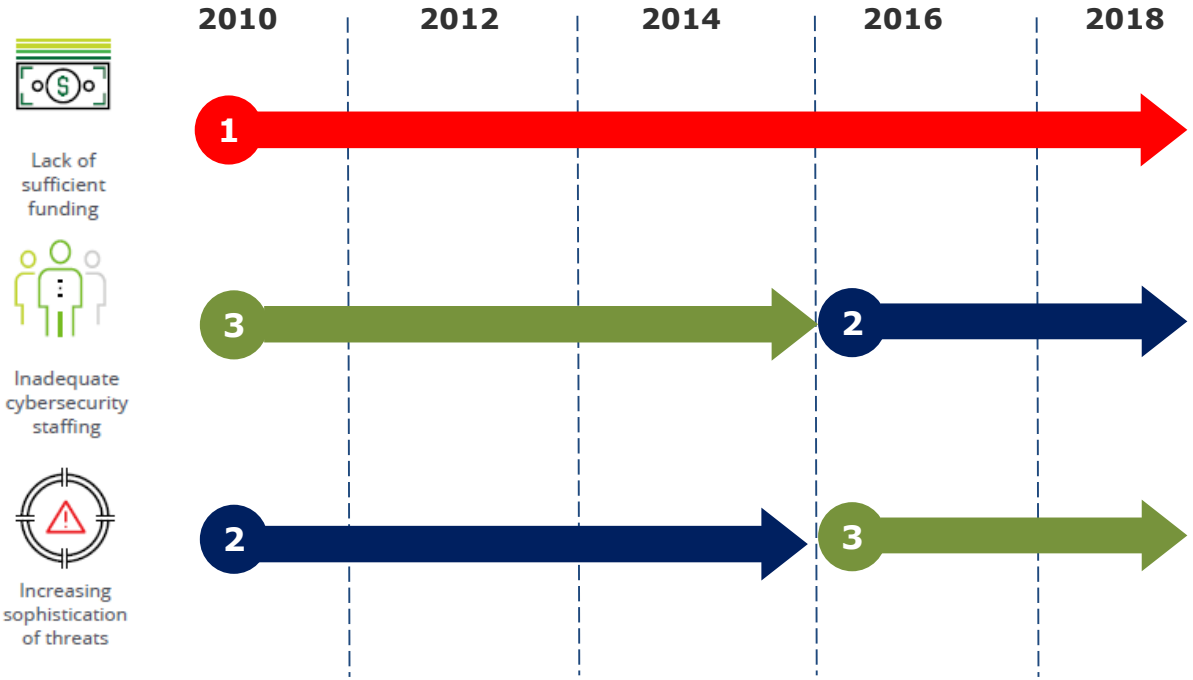


	Web applications	Malicious code (e.g., viruses/worms/ spyware/malware/ ransomware)	My state has not been breached	Electronic attack (e.g., hacker)	Physical attack (e.g., stolen computer systems)
Respondents	30	28	19	16	14
External	24	17	8	15	6
Internal	2	8	6	0	8
Business partner/ vendor	4	3	5	1	0

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

Three Bold Plays for Change

1 ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING

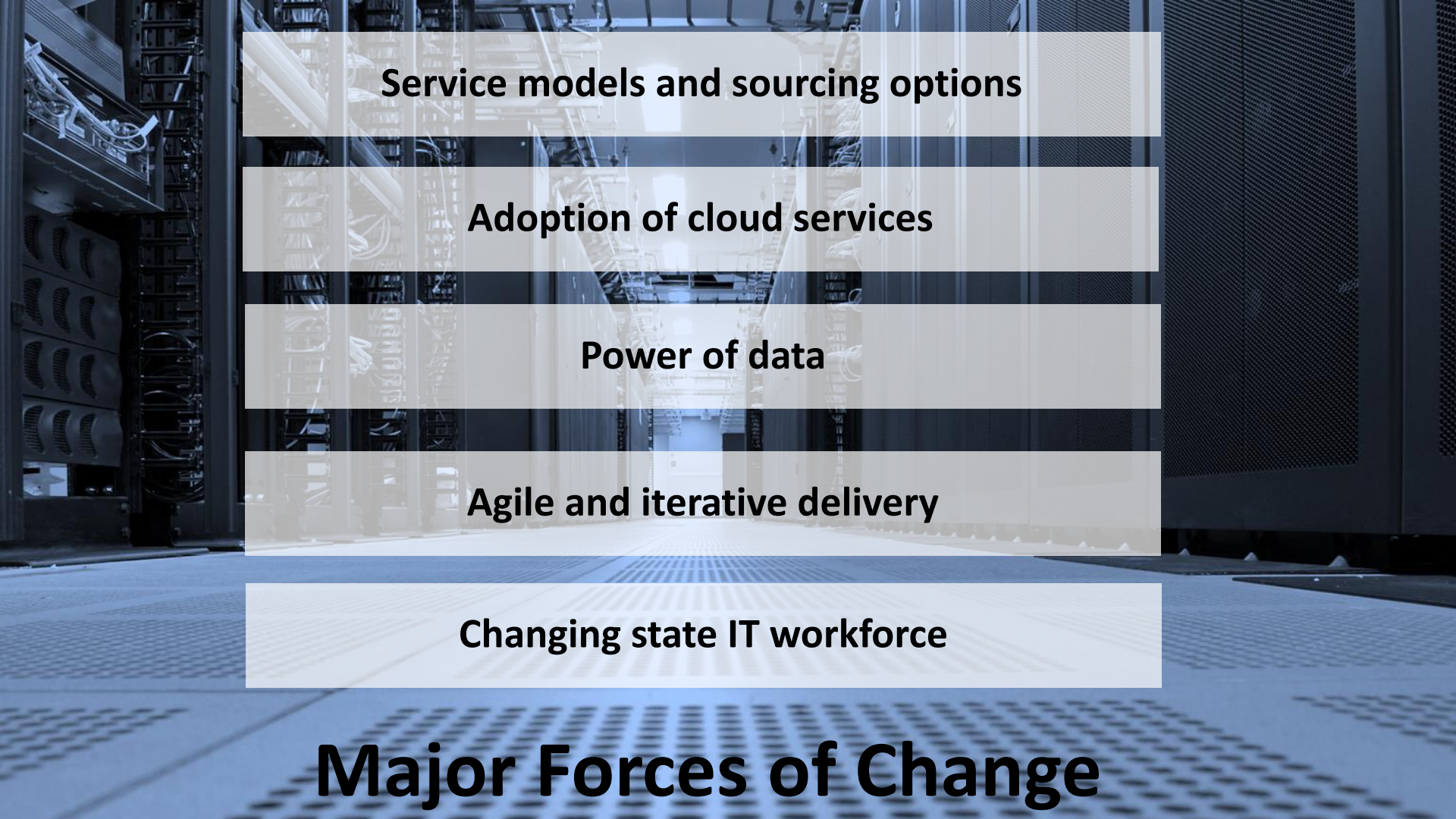
CISOs should raise cybersecurity's visibility with the state legislature and executive branch by making it a line item in the IT budget. They can also seek funding from federal agencies to support compliance with those agencies' security mandates.

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.



Major Forces of Change

How does your state CIO organization plan to deliver or obtain IT services over the next three years (e.g., server and platform administration, backup, storage, software and hardware maintenance, network management and service desk management)?

	Introduce	*Maintain*	*Expand*	*Downsize*
State-owned-and-operated data center(s)	0%	35%	14%	52%
Outsourcing service model	15%	26%	57%	2%
Managed services model	10%	23%	65%	2%
IT shared services model	0%	22%	75%	2%
"As-a-service" models (e.g. SaaS, PaaS, IaaS, etc.)	14%	12%	75%	0%
State IT staff	0%	69%	10%	22%

Evolving Business Model: CIO as Broker

Forces of Change: Why Cloud?

- Cost savings and efficiency
- Flexibility and scalability
- Rapid provisioning
- Measured service
- Better data and applications security
- Shift from capital spend to operating spend
- Reduced IT staffing and costs

This transition is disruptive to the traditional notions of state IT. It has serious implications for service delivery, state budgeting, procurement, legal, business processes, data protection, project and portfolio management.

Does your organization have a strategy to migrate legacy applications to the cloud?

41%	Yes, cloud migration strategy in place
37%	No, but cloud migration strategy in development
22%	No cloud migration strategy planned

NASCIO Representing Chief Information Officers of the States

Grant Thornton

CompTIA

Are you planning to move to an off-premise Mainframe-as-a-Service solution in the next 2-3 years?

18%	Yes, already complete
20%	Yes, planned
27%	Yes, considering
29%	No
6%	Unsure

Source: NASCIO 2018 State CIO Survey

- State government is in the information business and data is its lifeblood
- Public services create information in the form of records, increasingly in electronic formats
- States continue to struggle with new challenges presented by a growing portfolio of electronic records and digital content that must be preserved
- Electronic records require attention to ensure they are preserved and accessible as they are more complex to preserve than paper records

The volume and complexity of electronic government records continues to increase at an exponential rate. 19 states now use a commercial SaaS-cloud solution for digital preservation.

1693% growth in state and territorial electronic records between 2006-2016

445% growth in electronic versus paper records in state and territorial archives

1371.1TB of electronic government records held by states and territorial archives

All states have security measures in place to protect data and systems

At least 27 states have statutory provisions in public records laws that expressly exempt from disclosure information in government technology systems that involve security information.

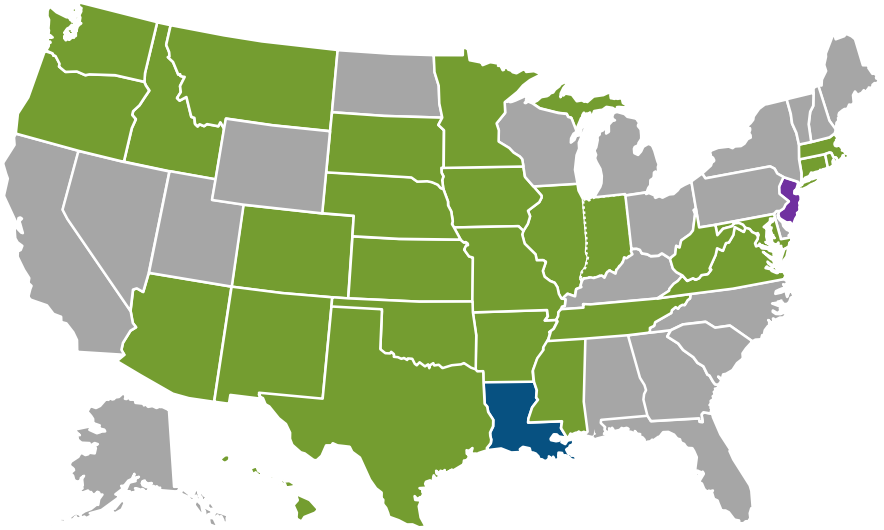
Categories of Record Exemptions for Information Technology Systems

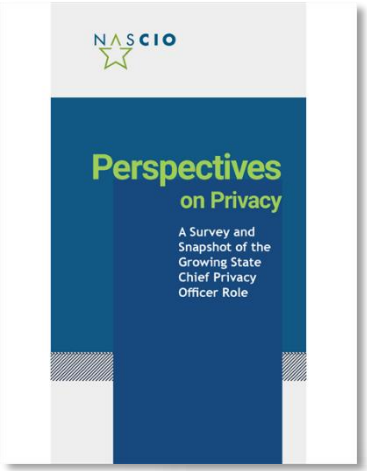
- Cybersecurity systems, procedures, IT infrastructure (19)
- IT systems in context of homeland security, anti-terrorism (5)
- Critical infrastructure – energy, telecommunications
- Elections security

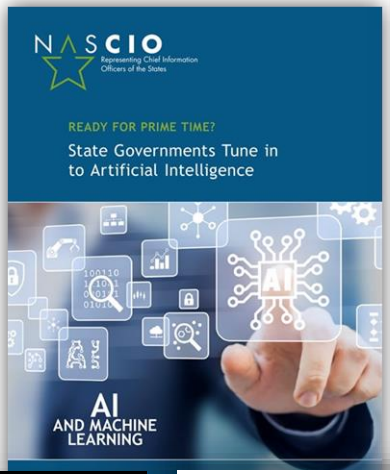
Source: NCSL, April 2019

Contractor Monitoring Software Legislation

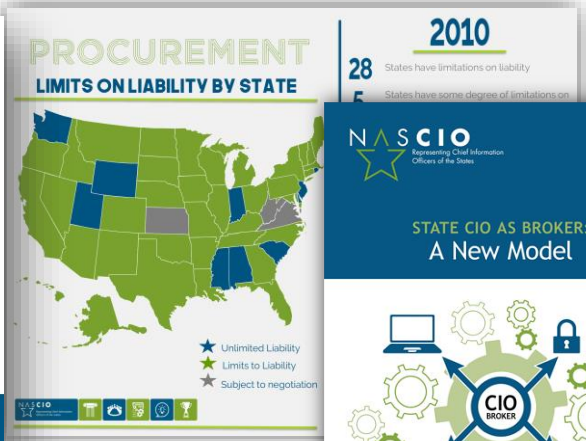
"NASCIO opposes state legislation which would mandate contractor monitoring software because of the significant risks to citizen privacy and federal regulatory compliance concerns it could create. While NASCIO certainly supports contractor productivity, cost efficiency and successful project outcomes, legislation of this nature could introduce unnecessary risks to citizen data by essentially transferring ownership of private citizen data to a third party." February 21, 2019




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

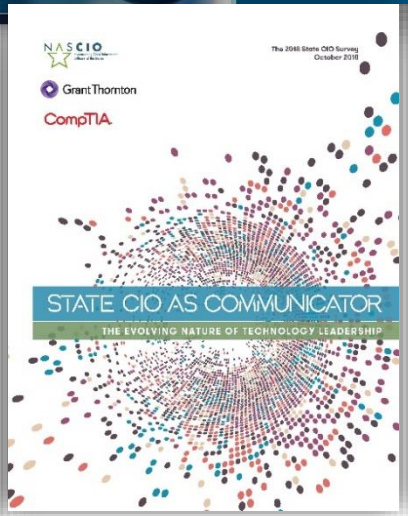

NASCIO
Representing Chief Information Officers of the States
READY FOR PRIME TIME?
State Governments Tune in to Artificial Intelligence
AI
AND MACHINE LEARNING

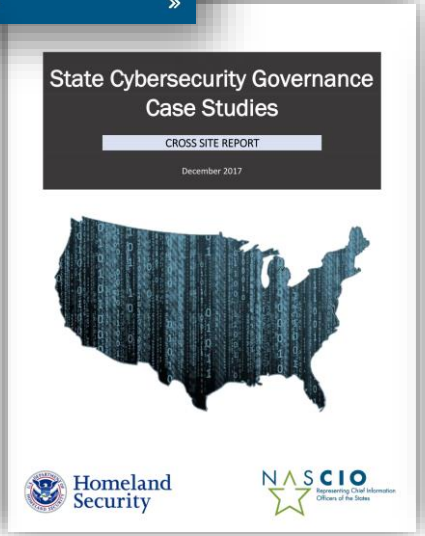

STATE ARCHIVING IN THE DIGITAL ERA
A Playbook for the Preservation of Electronic Records
October
2018
NASCIO
CoSA

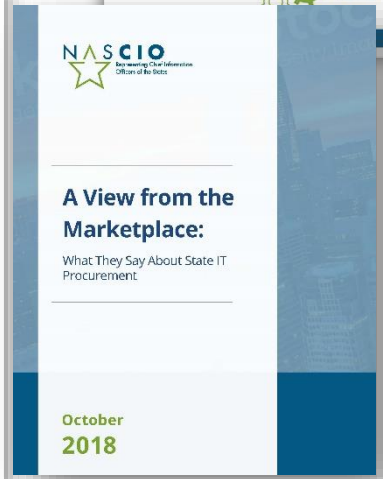

PROCUREMENT
LIMITS ON LIABILITY BY STATE
2010
28 States have limitations on liability
Unlimited Liability
Limits to Liability
Subject to negotiation

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