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

2019 National FOI Summit
April 12, 2019

Doug Robinson, NASCIO Executive 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.
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

- Protecting legacy systems
- Phishing, ransomware, hacktivism
- Foreign state-sponsored espionage
- Mobile devices and services
- Software vulnerabilities
- Not organized and mature to be successful
- Employees and third-party contractors
- Use of social media platforms
- Shadow IT; rogue cloud users
- Foreign state-sponsored espionage

Cybersecurity Risks in the States
Humans...
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
“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?

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

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

- Adoption of cloud services
- Power of data
- Service models and sourcing options
- Agile and iterative delivery
- Changing state IT workforce
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)?

<table>
<thead>
<tr>
<th>Service Model</th>
<th>Introduce</th>
<th>Maintain</th>
<th>Expand</th>
<th>Downsize</th>
</tr>
</thead>
<tbody>
<tr>
<td>State-owned-and-operated data center(s)</td>
<td>0%</td>
<td>35%</td>
<td>14%</td>
<td>52%</td>
</tr>
<tr>
<td>Outsourcing service model</td>
<td>15%</td>
<td>26%</td>
<td>57%</td>
<td>2%</td>
</tr>
<tr>
<td>Managed services model</td>
<td>10%</td>
<td>23%</td>
<td>65%</td>
<td>2%</td>
</tr>
<tr>
<td>IT shared services model</td>
<td>0%</td>
<td>22%</td>
<td>75%</td>
<td>2%</td>
</tr>
<tr>
<td>“As-a-service” models (e.g. SaaS, PaaS, IaaS, etc.)</td>
<td>14%</td>
<td>12%</td>
<td>75%</td>
<td>0%</td>
</tr>
<tr>
<td>State IT staff</td>
<td>0%</td>
<td>69%</td>
<td>10%</td>
<td>22%</td>
</tr>
</tbody>
</table>

Evolving Business Model: CIO as Broker

Source: 2018 NASCIO SURVEY | State CIO as a Communicator
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.

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
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
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

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity systems, procedures, IT infrastructure</td>
<td>19</td>
</tr>
<tr>
<td>IT systems in context of homeland security, anti-terrorism</td>
<td>5</td>
</tr>
<tr>
<td>Critical infrastructure – energy, telecommunications</td>
<td></td>
</tr>
<tr>
<td>Elections security</td>
<td></td>
</tr>
</tbody>
</table>

Source: NCSL, April 2019
“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