



Call to Action: Cybersecurity and the States

As new state leaders enter office they are faced with severe fiscal issues and a forecast of economic stress and slow growth for several years. In this environment, a priority that may be overlooked is the cybersecurity risks to state government. States rely on information technology to deliver state services. It is critical that new administrations transition with full awareness of the cybersecurity threat landscape, the mechanisms that states and the federal government have created to reduce risk levels, and new opportunities states have to simultaneously improve cybersecurity and service delivery. Failure to maintain the integrity of state networks and systems, protect the state's data resources and safeguard personal information will gravely undermine citizen confidence, as well as the direct ability to deliver government programs and services.

1. Know the Risks

Governors new or old know that in 2011 their administrations face unprecedented fiscal challenges and enormous pressures to reduce government expenditures while enhancing the services that good governments must provide in the 21st century. To meet these challenges, many governors are looking to information technology to transform government and reduce the cost of service delivery. They are moving as quickly as possible to implement enterprise approaches that align technology to the new business models for governing, which require economy, transparency, and accountability.

Governors also recognize that a critical requirement of this transformation is protection of the key resources vested in government information systems – the data itself. Personal information collected and maintained by governments is the lifeblood of all these efforts. Government information must be managed to minimize the risk of exposure either inadvertently, through loss to the determined attacks of outsiders, or to insiders who misuse the public trust. Citizens lack confidence in the state's ability to protect their personal information. To restore this confidence, it is critical that states demonstrate their capacity to protect the data they hold in trust.

The digital infrastructure that enables state government to both conduct business and protect federal programs administered by the states is under daily attack. This digital infrastructure includes electronic information and communications systems, and the information contained in those systems. Due to the breadth and scope of the state role in entitlement services, facilitating travel and commerce, regulatory oversight, licensing and citizen services, states gather, process, store and share extensive amounts of personal information. From cradle to grave, the states are the nexus of identity information for individuals. This makes the states prime targets for external and internal cyber threats.

As state leaders act to streamline services, consolidate IT infrastructure and perform more efficiently, they frequently turn to private sector firms to outsource services. As this happens, it is critical that appropriate protection of the information continues, and that all requirements surrounding the data are met, in terms of the identification of information that is collected, data classification, retention, and transparency. All levels of government and the private sector must work together and share responsibility to protect cyber assets and ensure appropriate mechanisms are in place for a coordinated response to and recovery from a cyber attack or other disruption.

2. Know the Landscape

Cybersecurity threats are growing in numbers, as well as severity. These threats may be characterized as:

- Constantly evolving due to rapidly emerging technologies and increasing demands on agency services
- Disruptive and profitable to organized crime and a preferred method for generating income through cybercrime activities
- Escalating internal threats as employees fail to comply with security measures, internal controls are circumvented and data becomes increasingly mobile
- Increasing demands of users to have constant access to data, which increases the need for data loss prevention capabilities and protection

One of our critical infrastructure assets, our state networks, are attacked on a daily basis. The failure to secure these networks has serious implications for national security, including continuity of government, the operations of critical infrastructure and the health, safety and general welfare of citizens. Cyber attacks have disrupted state government networks, systems and operations, and could potentially impact first-responder communications during an attack on our homeland. Homeland security and emergency preparedness initiatives must include plans for restoring networks and systems in the event of a cyber attack, terrorist event, or natural disaster. Any plan, decision, or action regarding cybersecurity must respect privacy and civil liberties.

3. Know Your Cyber Assets

State Chief Information Officers (CIO) and State Chief Information Security Officers (CISO) are the key leaders overseeing cybersecurity in your state's government. Their professional focus and commitment is to ensure the cost-effective deployment of information technology and to do so in a way in which the data assets of your state government are securely held, available to everyone with the authority to use them, and transparent and open where permitted by privacy restrictions and open government law. Information security professionals' shorthand for this function is protection of the confidentiality, integrity, and availability of government information throughout its life-cycle, the C-I-A of data protection.

While organizational models for CIO and CISO authority and functions vary somewhat from state to state, the most effective programs are those in which information security governance is part of an enterprise, government-wide approach to IT management as a whole. The governance model establishes clear lines of authority and responsibility for cybersecurity management, integrating that into the larger fabric of IT management. The most effective cybersecurity programs produce accurate assessments of the risks associated with each system the government maintains, and for the network as a whole. They assign responsibilities to security professionals directly, to IT staff, to agency managers, and to employees, who play a critical and under-appreciated role in cyber protection. The most effective programs have the further characteristic of creating a culture of security, in the interest of protecting government data.

As government moves forward in adoption of new technologies to streamline services and meet growing citizen expectations, it is critical that security mechanisms associated with those advancements be fully understood and risks reevaluated. A 2010 Deloitte-NASCIO survey of state CISOs conducted last year reflected great concern about the degree to which outsourcing and the expanded use of third party providers threatens to diminish cybersecurity controls. Means of guaranteeing continued security can be found, but it must be emphasized that progress and change that are driven by the need to reduce the cost of government service delivery must not come at the cost of increased vulnerabilities and cyber risks.

In this regard, it is also critical that governors be aware that state governments are spending less on information security than do counterparts in the private sector, as is reflected in the same Deloitte-NASCIO survey. Governors must ensure that data protection mechanisms are adequate and must be sure that they understand CIO and CISO estimates of current risk levels, from agency to agency.

4. Know Your Opportunities

One of the most significant opportunities that states have right now is that fiscal circumstances are forcing reexamination of decentralized and stovepiped computing models and adoption and reassessment of the advantages of enterprise approaches that reduce redundancies and share existing or needed IT services. Baking security into that model and fully integrating risk assessment will go a very long way to enhance the cybersecurity posture of most state governments.

State governments have the further advantage that there is currently an unprecedented recognition by federal agencies of the role that securing state systems plays in securing the larger, national enterprise. Since the tragedies of 9/11 and Katrina, there have been very significant Federal grants flowing down to states, but these have been primarily focused on funding to protect infrastructure and improve physical security. Through ongoing communication with the Federal CIO and the Department of Homeland Security, NASCIO, together with the Multi-State Information Sharing and Analysis Center (MS-ISAC) are advocating that state-level cyber programs need additional funding to close the risk gap. An important cybersecurity assessment of the states will be performed by DHS

in the fall of 2011. It is anticipated that this will document gaps and provide an important roadmap for action.

5. State Governments at Risk: Key Questions on Cybersecurity

- Is your state supporting a “culture of information security” encompassing a governance structure of state leadership and all key stakeholders?
- Has your state implemented an enterprise cybersecurity framework that includes policies, control objectives, practices, standards and compliance?
- Has your state invested in information technologies that provide continuous vulnerability management and protect against critical cyber threats on an ongoing basis?
- Are security metrics available in your state that accurately measure and report intrusion attempts, penetrations, vulnerabilities and security breaches?
- Have state employees and contractors been trained for their roles and responsibilities in protecting the state’s cyber assets?

Ultimately, meeting the cybersecurity challenge may be perceived as a balancing of risks. There are political risks to not optimizing service delivery, to continuing to operate in old service delivery models with stovepiped, agency-focused, standalone IT systems. There are risks to proceeding too quickly. There are risks of breach, exposure and embarrassment. Governors must understand the degree to which their states are under daily cyber attack, the existing frameworks that governments have created to protect the state, and the gaps in their current resources. It then becomes possible to minimize risks, right-size security investments, and ensure public confidence in government’s capacity to protect the critical infrastructure and data resources.

For more information contact:

Pamela Richardson Walker
Director of Government Affairs
National Association of State Chief Information Officers (NASCIO)
Hall of States
444 North Capitol Street NW, Suite 642
Washington, D.C. 20001-1511
P: (202) 624-8477
F: (202) 624-7745
C: (202) 215-2015
E: pwalker@AMRms.com
W: www.nascio.org