Cyber Security Presentation

1. **Cybersecurity is a growing priority for federal and state government. It is a growing and pervasive problem**

   From January 1, 2009 to May 31, 2012, there have been 268 breach incidents in government agencies with more than 94 million records containing personally identifiable information (PII) exposed.

   The Department of Homeland Security (The U.S. Computer Emergency Readiness Team (US-CERT)) reported an over 650-percent increase in the number of cyber incidents reported by federal agencies over a five-year period, from 5,503 in FY 2006, to 41,776 in FY 2010.

   The average cost per breached record is $194.00

   The average cost of a data breach for an organization is $5.5 million (page 15 NASCIO Survey)

   External Threats

   New threats are emerging. We are seeing a decline in traditional attacks such as physical attacks (stealing a laptop) or attacking web sites and in increase in the following:

   - Foreign state sponsored attacks increase from 6% to 12%
   - External financial fraud increase from 4% to 12%

   Hackers are more sophisticated and aggressive; they are after data they can turn into money. Some hackers – called hacktivists – are motivated by a political or social cause and desire to make political statements. Their techniques are very sophisticated and use new, rapidly changing technologies.

   At the Federal level:

   The Government Accountability Office (GAO) recently reported that 18 out of 24 major federal agencies in the United States reported inadequate information security controls for reporting.

   In October, FBI Director Robert Mueller said that “cyber security may well become our highest priority in the years to come.”

   Defense Secretary Leon Panetta - In a recent speech warned that America’s enemies are taking aim at the systems that run everything, from the electrical grid to transportation systems to the nation’s financial infrastructure, and he said that although the U.S. military is trying to get ready for a worst-case scenario, the rest of the government and the private sector must get moving now.

2. Cybersecurity in other states

A. Most states have a more centralized model of IT and Cyber Security Management

96% of states have a Chief Information Security Officer (CISO) now in place; however most CISOs do not have statewide authority to set policy, procedure and a security framework for agencies

- 56% have authority over the executive branch agencies
- 14% have statewide authority over legislative, executive and judicial government agencies
- 12% their own agency only (SC would fall here)
- 18% other

Most state CISOs operate in a federated environment (distributed) where IT and security resources are spread across various state agencies and departments

California as an example passed a law in 2010 that required each state agency to hire an Information Security Officer. The ISO reports CISO and establishes a structure for the governance and management of security.

Michigan created a new organization – the Cybersecurity and Infrastructure Protection (CIP) - and appointed an enterprise Chief Security Officer.

State CISOs are responsible for:

- Cyber security planning and strategy
- Information Sharing
- Incident management
- Cyber security governance (polices/procedures, architecture)
- Awareness and Training
- Program Measurement and reporting
- Cyber security monitoring
- Risk assessment and management
- Compliance and monitoring
- Vulnerability Management

B. Challenges are the same

Top 5 barriers to address Cyber security:

- Funding – 86%
- Increase sophistication of threats – 52%
- Inadequate availability of cybersecurity professionals – 46%
- Lack of visibility and influence within the enterprise (state) – 42%
- Emerging technologies – 36%

As you can see , the challenge for a state CISO and his staff is to protect against more sophisticated attacks, support users with new enabling technologies (like mobile phones, pads, cloud technologies) while competing for tight budget dollars

Budget/Funding

- Cyber security budgets average 1 -2 % of overall IT budget
- 17% of states don't know – which is in itself a big problem

Staffing

- 50% report a staff of few than 5 employees
- 38% report 6 to 15

Key comparison - States vs. Financial industry

Security budget has increased	14%	> 60%
Year-over-year trending	4% report an increase of 1-5%	39% report an increase of 1-5%
Dedicated security professionals	50% have 1-5 FTEs	47% have >100 FTEs

More state CISOs are turning to outsourcing and staff augmentation to close the skill sets they lack

- Outsourcing has grown by 3% (9% to 12%) between 2010 and 2012
- Staff Augmentation has grown from 22% to 28% in the same time period

In Delaware, every state organization is required to designate one to three Information Security Officers (ISOs) who are responsible for security matters. A commitment was made by the state to provide the training and tools these employees would need. They created a 2 year ISO certification program so that employees could develop and demonstrate the skill necessary to perform their job duties.

Important Note: Given the decentralized federated and distributed models of governance, most state CISOs do not have insight into agency level regulatory and audit findings

A recently completed survey of all state CIOs and CISOs: (50 CISOs responded) and a number of state officials across the country (63 state officials responded) show:

- Only 14% of state CISOs feel that they have appropriate executive commitment and adequate funding
- 70% of state CISOs have reported a breach
- Only 24% of state CISOs feel confident in ability to protect state assets
- Only 32% of state CISOs feel that staff have the required cyber security competency
- 86% of state CISOs indicate "Lack of sufficient funding" is the key barrier to address cyber security

82% of CISOs feel that Phishing is the top cyber security threat

C. Other state priorities are similar to ours

Top five initiatives for CISOs

- Risk Assessments 52%
- Training and awareness 46%
- Data protection 44%
- Cybersecurity strategy 44%
- Governance 42%

These are also high priority items for SC as we look to establish a statewide security program

3. Recommendations – What the State Security Experts say

1. Manage security at the statewide level – CISOs should have authority (within a federated model) to create policies, processes and a security framework for all agencies to use. Create an enterprise governance model and give CISOs the authority to set standards and create policy
2. Work Together. Create a shared services model and competency centers to facilitate sharing of resources
    a. Given the fact that security professionals are in high demand and the high costs associated with technologies, products and operations, states should strive to share technology and people.
    b. Underutilized, skilled employees in one agency or in the central office can be shared across the enterprise
    c. Agencies can specialize in a certain discipline, such as identity management, and share their knowledge with other agencies
    d. For example, a state health agency like HHS may receive federal funds to develop critical identity access management (IAM). These technologies and practices can be leveraged across the state
3. Governance should be extended to third party providers as well. Many state agencies use third party providers (vendors) to deliver products/services or help mange critical functions. Some of these vendors have access to state PII and sensitive state data. Need to review and audit their compliance with state security policies and regulations.
4. Use new and emerging technologies as a means to review and improve security measures and practices. Cloud solutions and mobile solutions are examples.
5. Agencies are subject to a number of different regulatory requirements depending on the type of personal data they manage. Their compliance requirements and audit findings should be reported to state business leaders (Governor, Legislators, elected officials – not just agency personnel) CISOs should guide agencies in meeting these regulatory standards by establishing a statewide security framework.
6. Name a statewide Privacy Officer – Privacy officers determine what data needs to be protected. CISOs determine how to protect this information