Protection of Data at Attorneys General Offices: A Strategic Imperative

NAAG Southern Region Meeting
April 5, 2017

Doug Robinson, Executive Director
National Association of State Chief Information Officers (NASCIO)
States are high value targets – data!

More aggressive and changing threats – organized crime, ransomware, hacktivism

Nation state attacks

Critical infrastructure protection

Insider threats – employees, contractors, third parties

Emerging IT and data on the move

Need for standard approaches and methods
Cybersecurity Risks in the States

- Protecting legacy systems
- Malicious software
- Not organized and mature to be successful
- Mobile devices and services
- Use of social media platforms
- Use of personally-owned devices (BYOD) for state business
- Adoption of cloud services; rogue cloud users
- Foreign state-sponsored espionage
- Third-party contractors and managed services
One of the major factors unique to government is the inherent openness that is expected of government at all levels. This has created the challenge of balancing that expectation of openness and transparency with the need to protect the privacy of personal or sensitive data.
State Governments at Risk:
Turning strategy and awareness into progress
### Emerging trends

#### Top cyber threats across state government

<table>
<thead>
<tr>
<th>Threat</th>
<th>Somewhat higher threat</th>
<th>Very high threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing, pharming, and other related variants</td>
<td>35%</td>
<td>47%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>31%</td>
<td>42%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>43%</td>
<td>29%</td>
</tr>
<tr>
<td>Increasing sophistication and proliferation of threats (e.g., viruses, worms, and malware)</td>
<td>51%</td>
<td>14%</td>
</tr>
<tr>
<td>Exploits of vulnerabilities from unsecured code</td>
<td>45%</td>
<td>8%</td>
</tr>
</tbody>
</table>
63 percent of confirmed data breaches involve using weak, default or stolen passwords

‘Miscellaneous errors’ take the No. 1 spot for security incidents - humans!

Basic defenses continue to be sorely lacking in many organizations
“Humans are the most vulnerable point of any information system, Mr. Wynne said, adding that the vast majority of cyberattacks use social engineering, such as phishing, to trick employees into taking actions detrimental to the company. “The education aspect is a critical component because it increases employee resilience to social engineering,” he said.
Figure 8. What are the top 5 security threats that affect your organization?
Four responses permitted

- Negligent insiders: Federal 44%, State & Local 40%
- Zero-day attacks: Federal 36%, State & Local 38%
- Third-party or contractor mistakes: Federal 36%, State & Local 35%
- Failure to patch known vulnerabilities: Federal 34%, State & Local 43%
- Nation-state attackers: Federal 16%, State & Local 30%

Who’s Responsible for Protecting State Data?

- Chief Information Officers
- Information Security Officers
- Agency Leaders
- Data Owners
- Employees
- Human Resources
- Legal Departments
- Third Party Contractors
- Elected Officials
Cybersecurity involves more than just IT – it’s a team sport.

Protecting data is a core responsibility of state government entities and an investment in risk management.

It’s a complex ecosystem that requires a roadmap.
Adopt a risk-based cybersecurity framework to protect data

Use the NIST Cybersecurity Framework as a guide. Includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Asset Management</td>
<td>ID.AM</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>ID.BE</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>ID.GV</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>ID.RA</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
</tr>
<tr>
<td>Protect</td>
<td>Access Control</td>
<td>PR.AC</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
<td>PR.AT</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>PR.DS</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures</td>
<td>PR.IP</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>PR.MA</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>PR.PT</td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events</td>
<td>DE.AE</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>DE.CM</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>DE.DP</td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning</td>
<td>RS.RP</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RS.CO</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>RS.AN</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>RS.MI</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RS.IM</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
<td>RC.RP</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RC.IM</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RC.CO</td>
</tr>
</tbody>
</table>
In the **Identify** function is a category called Risk Assessment. The goal of a risk assessment is for an organization to understand “the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.” As set out by NIST, use the following six steps:

1. Identify and Document Asset Vulnerabilities
2. Identify and Document Internal and External Threats
3. Acquire Threat and Vulnerability Information from External Sources
4. Identify Potential Business Impacts and Likelihoods
5. Determine Enterprise Risk by Reviewing Threats, Vulnerabilities, Likelihoods and Impacts
6. Identify and Prioritize Risk Responses
The Cyberthreat to Government That's Lurking in the Shadows

Many public employees use unsanctioned software on work computers. It poses serious security risks.

BY TOD NEWCOMBE | APRIL 2017
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

PR.AT-2: Privileged users understand roles & responsibilities

PR.DS-1: Data-at-rest is protected

PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved tools

PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality
### CIS 20 Critical Controls: Focus on Top 5

1. **CSC 1:** Inventory of Authorized and Unauthorized Devices
2. **CSC 2:** Inventory of Authorized and Unauthorized Software
3. **CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.
4. **CSC 4:** Continuous Vulnerability Assessment and Remediation
5. **CSC 5:** Controlled Use of Administrative Privileges

Source: Center for Internet Security, Critical Controls v 6.1, 2017
Use a Risk-Based Strategy and Take Action

1. Develop a strategy to protect data. Use the NIST Cybersecurity Framework as a roadmap.
2. Conduct a risk assessment and allocate resources accordingly. Where is your data? How would you classify the data in terms of risk?
3. Implement continuous vulnerability and threat mitigation practices.
4. Limit data collection, control access, consider data loss prevention.
5. Create a culture of risk awareness. Educate and test employees.