2012 Deloitte-NASCIO Cybersecurity Study
State Governments at Risk: A Call for Collaboration and Compliance

Highlights from 2013 President’s Executive Order

Srini Subramanian, Principal, Deloitte & Touche LLP
Thomas D. Smith, Chief Information Security Officer, ITS Enterprise Information Security Office
Agenda

State Cyber Threat Landscape

About the Deloitte-NASCIO Cybersecurity Study

Learning from the Study

President’s Cybersecurity Critical Infrastructure Executive Order
State Cyber Threat Landscape
State Governments Are a Target

• States have the most comprehensive information about citizens; for this reason, organized cyber criminals have targeted government and higher education agencies for the past few years.

  – Data loss from government impacts citizen trust and has the potential to impact state business by affecting citizen services, revenue collections, or unplanned spending

• In recent months, there has been an increase in high-profile cyber attacks from loose-knit, politically-motivated groups operating globally.

  – These groups are distinct from more well established cyber criminal organizations, in both organizational structure (ad-hoc vs. top-down) and motivation (“hacktivism” vs. monetary gain).

• Recent developments have elevated Cybersecurity to a Governor level issue.
Highlights from the National Governors Association (NGA)

NGA Health and Homeland Security Committee\(^1\)

**Governor O’Malley, Chair**

**Governor Sandoval, Vice Chair**

**Governor O’Malley and Governor Snyder to Lead NGA Resource Center on Cybersecurity\(^2\)**

• Create a “National Policy Council for State Cybersecurity” that will provide policy recommendations for state governors

\(^1\) [http://www.c-spanvideo.org/program/311076-3](http://www.c-spanvideo.org/program/311076-3)

About the Study
How Deloitte and National Association of State Chief Information Officers (NASCIO) Conducted This Survey

Objectives


• Identify additional trends:
  • In emerging areas such as mobile and cloud security.
  • For Chief Information Security Officers (CISOs) assess the maturity level of security services – using the services taxonomy brief published by NASCIO (Nov 2011).

• Provide state leadership with insights to help them make informed, strategic cybersecurity decisions; assess awareness level with an expanded business survey respondents.

Survey Execution

• Deloitte leveraged its global security surveys, and the 2010 Deloitte - NASCIO Study in developing the survey questions.

• A state CISO survey advisory council, consisting of the members of the NASCIO and Security & Privacy committee helped further refine survey questions.

• Respondents used an on-line tool to complete the survey during a four week period in July/August 2012.

---

4 2012 Deloitte-NASCIO Cybersecurity Study 10192012.pdf
5 The Heart of the Matter: A Core Services Taxonomy for State IT Security Programs, NASCIO, Nov 2011
Impressive Survey Response

48 state and two territory CISOs (or equivalents) responded to the CISO version of the survey, which consisted of 64 questions.

63 state officials answered a shorter survey of 17 questions to provide insight into states business stakeholders' perspectives. The participant affiliations included the following associations:

- National Association of State Auditors, Controllers and Treasurers (NASACT).
- National Association of Attorneys General (NAAG).
- National Association of Secretaries of State (NASS).
- National Association of State Personnel Executives (NASPE).
- National Association of State Chief Administrators (NASCA).
Survey Results and Timeline

Survey results


• One confidential benchmark report for every state CISO respondent – comparing their individual survey responses with the aggregated survey results.

Report: State Governments at risk: A call for collaboration and compliance
Learning from the Study
The Study Echoes the Need for Collaboration and Compliance

Summary
1. Cybersecurity challenges persist – no change from 2010 Survey
2. People change but results have not.
3. State officials acknowledge the importance of security.

Q30. What percentage of your state’s overall IT budget is allocated to cybersecurity?

The budget discussion is complicated by the fact that most CISOs’ budgets are only a portion of the total security spend across the enterprise.

A small portion of the overall IT budget is devoted to cybersecurity - most state security budgets are in the 1-2% range.
2. Top Five Barriers faced in addressing Cybersecurity

Q20. What major barriers does your state face in addressing cybersecurity?

- Emerging technologies: 36%
- Lack of visibility and influence within the enterprise: 42%
- Inadequate availability of cybersecurity professionals: 46%
- Increasing sophistication of threats: 52%
- Lack of sufficient funding: 86%

Insufficient resources against growing sophistication of threats and emerging technologies make the need to raise stakeholder awareness to gain their support and funding the more critical.
3. Senior Executive Support for Security Projects to Address Legal/Regulatory Requirements

Q24. Which of the following best describes the state of senior executive support for security projects to effectively address regulatory or legal requirements?

- Not applicable/Do not know: 12%
- Commitment and adequate funding: 14%
- Commitment but inadequate funding: 74%

Q5 (State Officials). On a scale of 1 to 5, please indicate how you consider the importance of information security to your state Government?

- 3 (Important): 7%
- 4 (Very Important): 11%
- 5 (Extremely Important): 81%

74% of CISO respondents have executive commitment—but that has not translated into adequate funding.
### 4. Internal Cybersecurity Professionals Competency

<table>
<thead>
<tr>
<th>Q15. Do your internal cybersecurity professionals have the required competencies to handle existing and foreseeable cybersecurity requirements?</th>
<th>2010</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closing the gaps by outsourcing the affected areas</td>
<td>9%</td>
<td>12%</td>
</tr>
<tr>
<td>Staff has large gaps in competencies</td>
<td>17%</td>
<td>24%</td>
</tr>
<tr>
<td>Closing the gaps through staff augmentation</td>
<td>22%</td>
<td>28%</td>
</tr>
<tr>
<td>Staff has all the required competencies</td>
<td>25%</td>
<td>32%</td>
</tr>
<tr>
<td>Closing the gaps through adequate training to staff for developing required competencies</td>
<td>35%</td>
<td>50%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2012 Deloitte-NASCIO Cybersecurity Study</th>
<th>2012 DTTL GFSI Security Study (large organizations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated cybersecurity professionals</td>
<td>50% have 1-5 Full Time Equivalents (FTEs)</td>
</tr>
</tbody>
</table>

The evolution of cybersecurity governance, combined with a strategy to promote collaboration and shared services, will help CISOs find ways to do more with existing cybersecurity resources across the enterprise.
5. Confidence Level of Agency/Office’s Measures to Protect Information Assets from Threats

Q33. Indicate your level of confidence that your state’s information assets are protected from threats.

Majority of the State Officials’ survey respondents are very confident or extremely confident in the State’s measures to protect information assets against threats originating internally.

Q35. In terms of external security breaches over the past 12 months, which of the following apply to your state?

<table>
<thead>
<tr>
<th></th>
<th>2010</th>
<th>2012</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious software</td>
<td>68%</td>
<td>58%</td>
<td>↓</td>
</tr>
<tr>
<td>Web</td>
<td>55%</td>
<td>30%</td>
<td>↓</td>
</tr>
<tr>
<td>Hackers</td>
<td>45%</td>
<td>30%</td>
<td>↓</td>
</tr>
<tr>
<td>Physical attack, such as stolen laptop</td>
<td>36%</td>
<td>20%</td>
<td>↓</td>
</tr>
<tr>
<td>Foreign state-sponsored espionage</td>
<td>6%</td>
<td>12%</td>
<td>↑</td>
</tr>
<tr>
<td>External financial fraud</td>
<td>4%</td>
<td>12%</td>
<td>↑</td>
</tr>
</tbody>
</table>

Emerging cybercrime and state-sponsored threats will require a strong response from states.
Summary of Key Findings

Cybersecurity budget – strategy connection
CISOs should communicate strategies & report on risks, progress, and results to build business stakeholder advocacy for cybersecurity initiatives. Shared services and competency centers are a must.

Preparedness for emerging threats
Emerging threats equal emerging opportunities: Mobile, Cloud, Big Data are security enabling opportunities that also help build stronger business stakeholder support.

Cybersecurity authority and governance
CISOs need to evolve their role to be effective in a largely federated model.
- Skillset gap and security function outsourcing.
- Improve security management of third party service providers.

Compliance—a lever for CISO leadership
Regulatory compliance and audit findings can be used to as tools to better communicate risks to business stakeholders.
A Call for Action
Call for Action – Checklist of considerations

- Assess and communicate security risks.
- Better articulate risks and audit findings with business stakeholders.
- Explore creative paths to improve cybersecurity effectiveness within states’ current federated governance models.
- Focus on audit and continuous monitoring of third-party compliance.
- Raise stakeholder awareness to combat accidental data breaches.
- Aggressively explore alternative funding sources including collaboration with other entities.
- Make better security an enabler of the use of emerging technologies.
President’s Critical Infrastructure Cybersecurity Executive Order
State Impact
State of the Union - President Obama’s Plan on Cybersecurity\textsuperscript{6}

\textsuperscript{6} http://www.whitehouse.gov/photos-and-video/video/2013/02/12/2013-state-union-address-0
How we got here: A look back at the evolving legislative and regulatory framework…

“Given the magnitude of the threat and the gaps in the government’s ability to respond, we cannot afford to delay action on this critical legislation.”
— Senate Majority Leader Harry Reid, November 2011
In all my years on the Homeland Security Committee, I cannot think of another issue where the vulnerability is greater and we’ve done less.”
— Senator Susan Collins, November 2012
## Points to know about the new Cybersecurity Executive Order

| Information sharing | • Opens up information-sharing program to other sectors  
|                     | • Requires Federal government information-sharing programs with private sector  
| Privacy             | • Mandates strong privacy and civil liberties protections  
|                     | • Directs regular assessments of agency activities  
| Cybersecurity standards | • Requires development of a Cybersecurity Framework  
|                     | • Develops voluntary critical infrastructure cybersecurity program and adoption incentives  
|                     | • Identifies regulatory gaps  
| Critical infrastructure review | • Identifies critical infrastructure at greatest risk  
|                     | • Changes the definition of critical infrastructure  

## Cybersecurity of Critical Infrastructure - timeline

<table>
<thead>
<tr>
<th></th>
<th>Near-term</th>
<th>Mid-term</th>
<th>Long-term</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State sector</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Partner to shape development of a cybersecurity framework</td>
<td>• Identification of agencies as “critical infrastructure”</td>
<td>• Adopt the Cybersecurity framework</td>
</tr>
<tr>
<td></td>
<td>• Dialogue on information sharing</td>
<td>• Identify Cybersecurity framework leader</td>
<td></td>
</tr>
<tr>
<td><strong>Federal Sector</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Broaden information sharing process and assess privacy risks (120 days)</td>
<td>• Identify critical infrastructure at greatest risk</td>
<td>• Issue final framework (1 year)</td>
</tr>
<tr>
<td></td>
<td>• Review and comment on Cybersecurity framework</td>
<td>• Develop a preliminary Framework (240 days)</td>
<td>• Report program participation and privacy risks (annually)</td>
</tr>
<tr>
<td></td>
<td>• Establish voluntary program to support framework adoption (120 days)</td>
<td>• Look for funding and budget opportunities to implement Cybersecurity Framework</td>
<td></td>
</tr>
</tbody>
</table>
Questions

Contact:
Srini Subramanian
Principal
ssubramanian@deloitte.com
(717) 651-6277
Deloitte's approximately 182,000 professionals are committed to becoming the standard of excellence.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

In addition, this presentation contains the results of a survey conducted in part by Deloitte. The information obtained during the survey was taken “as is” and was not validated or confirmed by Deloitte.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

Copyright © 2013 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited