

**Deloitte.**

**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

---

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

# 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<sup>1</sup>

*Governor O'Malley, Chair*

*Governor Sandoval, Vice Chair*



## *Governor O'Malley and Governor Snyder to Lead NGA Resource Center on Cybersecurity<sup>2</sup>*

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

<sup>1</sup> <http://www.c-spanvideo.org/program/311076-3>

<sup>2</sup> [http://www.nga.org/cms/home/news-room/news-releases/page\\_2012/col2-content/governors-omalley-and-snyder-to.html](http://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html)

# About the Study

**Deloitte.**



2012 Deloitte-NASCIO Cybersecurity Study  
State governments at risk: a call for  
collaboration and compliance



A publication of Deloitte and the National Association of State Chief Information Officers

# How Deloitte and National Association of State Chief Information Officers (NASCIO) Conducted This Survey<sup>4</sup>

## Objectives

- Assess status of state enterprise cybersecurity programs – compare with 2010 Deloitte-NASCIO Cybersecurity Study and Deloitte Touche Tohmatsu Limited (DTTL)'s 2012 Global Financial Services Industry (GFSI) security survey.
- 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)<sup>5</sup>.
- Provide state leadership with insights to help them make informed, strategic cybersecurity decisions; assess awareness level with an expanded business survey respondents.

## Survey Execution

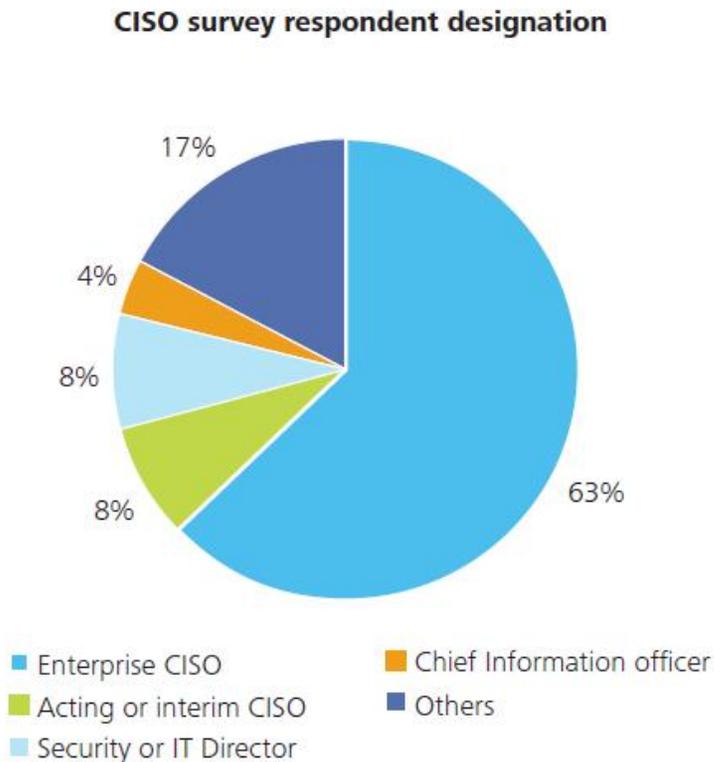
- Deloitte leveraged its global security surveys, and the 2010 Deloitte - NASCIO Study in developing the survey questions.
- A state CISO survey advisory council, consisting of the members of the NASCIO and Security & Privacy committee helped further refine survey questions.
- Respondents used an on-line tool to complete the survey during a four week period in July/August 2012.

<sup>4</sup> [2012 Deloitte-NASCIO Cybersecurity Study 10192012.pdf](#)

<sup>5</sup> [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.



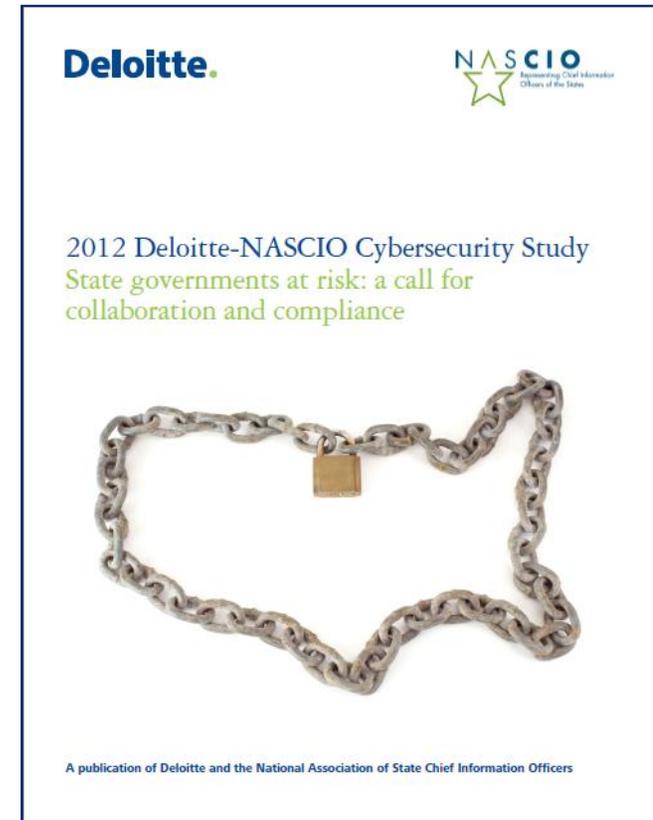
63 state officials answered a shorter survey of 17 questions to provide insight into states business stakeholders' perspectives. The participant affiliations included the following associations:

- 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

- 2012 Deloitte –NASCIO Cybersecurity Study – Available in print and electronic format – Downloadable from [www.nascio.org](http://www.nascio.org) and [www.deloitte.com](http://www.deloitte.com).
- One confidential benchmark report for every state CISO respondent – comparing their individual survey responses with the aggregated survey results.



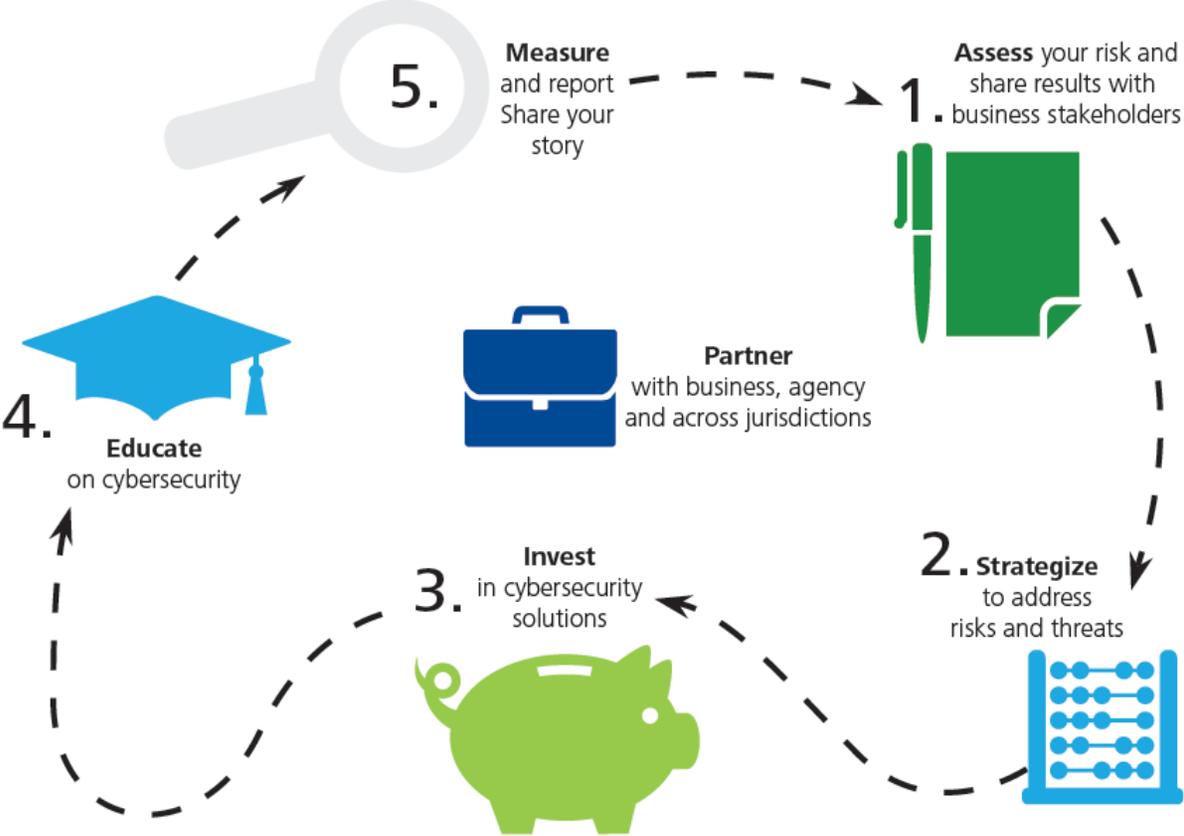
**Report :** [State Governments at risk: A call for collaboration and compliance](#)

# Learning from the Study

# The Study Echoes the Need for Collaboration and Compliance

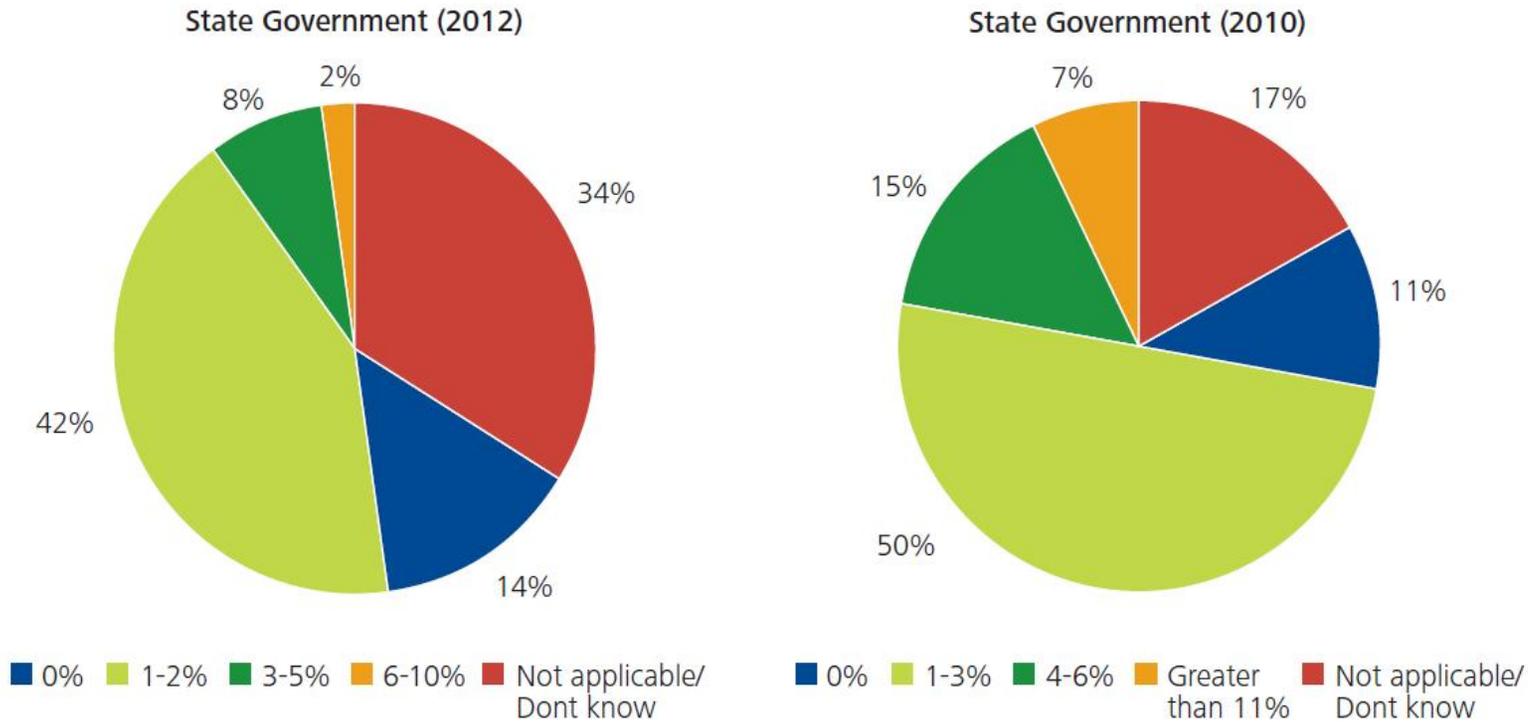
**Summary**

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



# 1. Cybersecurity Budget Allocation (2012 vs. 2010)

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

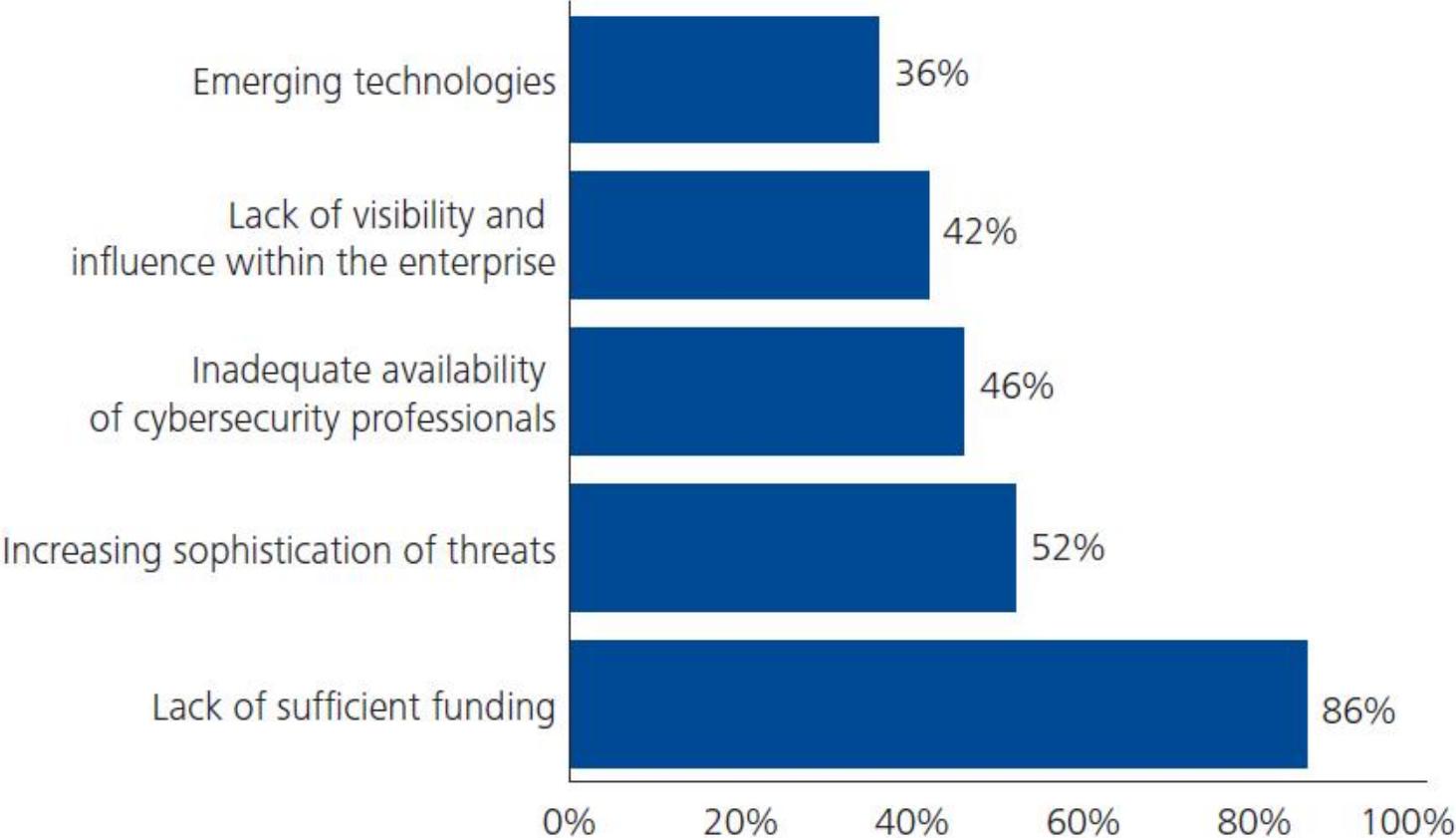


The budget discussion is complicated by the fact that most CISOs' budgets are only a portion of the total security spend across the enterprise.

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

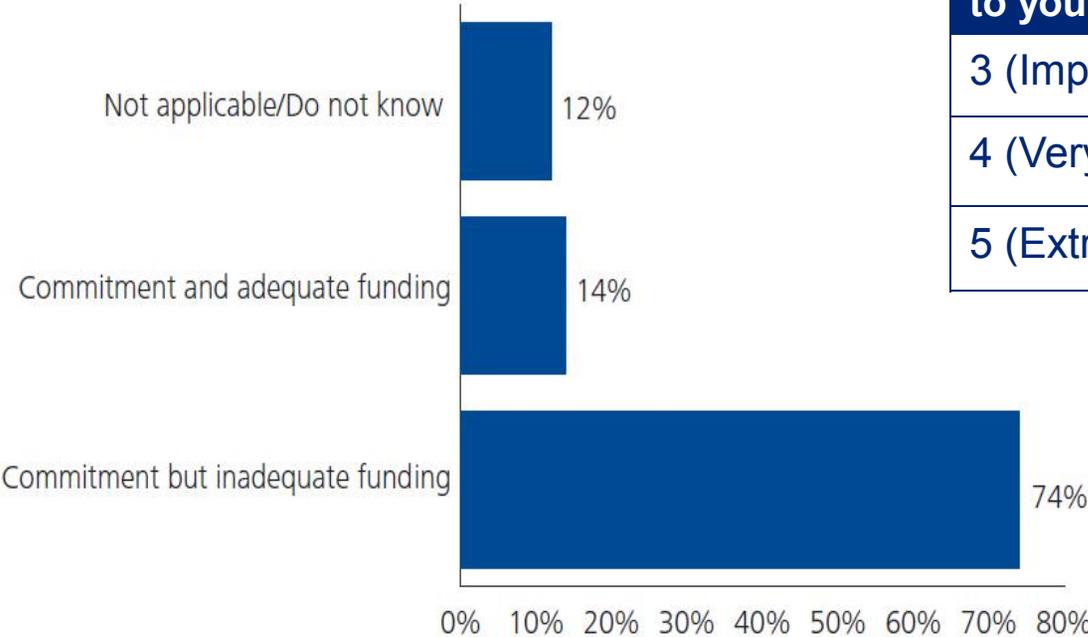
Q20. What major barriers does your state face in addressing cybersecurity?



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?



**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

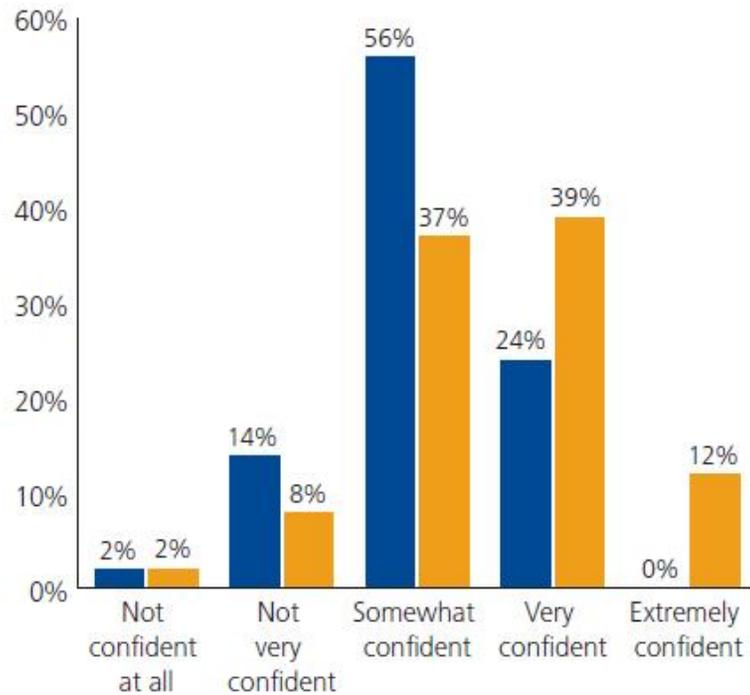
Q15. Do your internal cybersecurity professionals have the required competencies to handle existing and foreseeable cybersecurity requirements?	2010	2012
Closing the gaps by outsourcing the affected areas	9%	12%
Staff has large gaps in competencies	17%	24%
Closing the gaps through staff augmentation	22%	28%
Staff has all the required competencies	25%	32%
Closing the gaps through adequate training to staff for developing required competencies	35%	50%
	<b>2012 Deloitte-NASCIO Cybersecurity Study</b>	<b>2012 DTTL GFSI Security Study (large organizations)</b>
<b>Dedicated cybersecurity professionals</b>	50% have 1-5 Full Time Equivalent (FTEs)	<b>47% have &gt;100 FTEs</b>

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

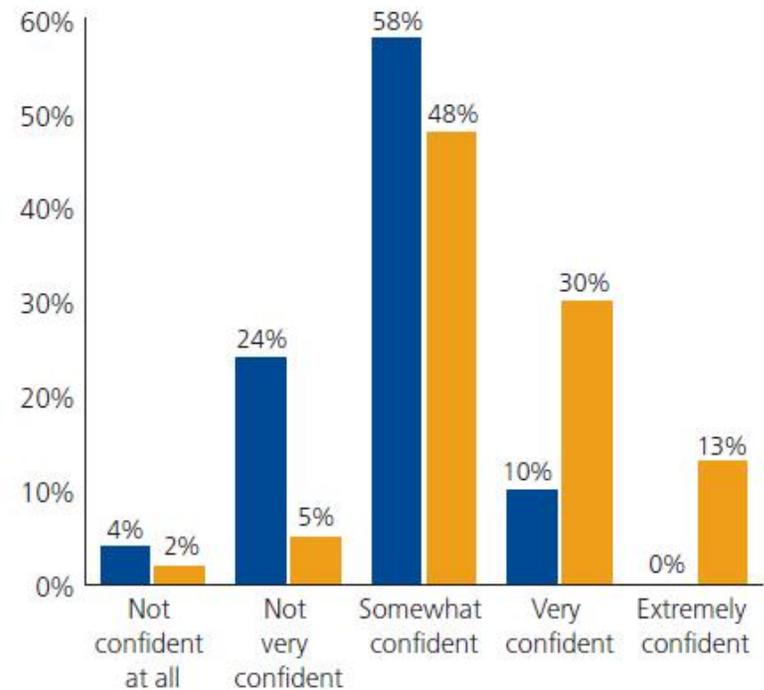
Q33. Indicate your level of confidence that your state's information assets are protected from threats.

Threats originating externally



■ CISO ■ State officials

Threats originating internally



■ CISO ■ State officials

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.

## 6. The Changing Face of External Breaches (2010 vs. 2012)

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

	2010	2012	Change
Malicious software	68%	58%	↓
Web	55%	30%	↓
Hackers	45%	30%	↓
Physical attack, such as stolen laptop	36%	20%	↓
Foreign state-sponsored espionage	6%	12%	↑
External financial fraud	4%	12%	↑

Emerging cybercrime and state-sponsored threats will require a strong response from states.

# Summary of Key Findings



# 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.

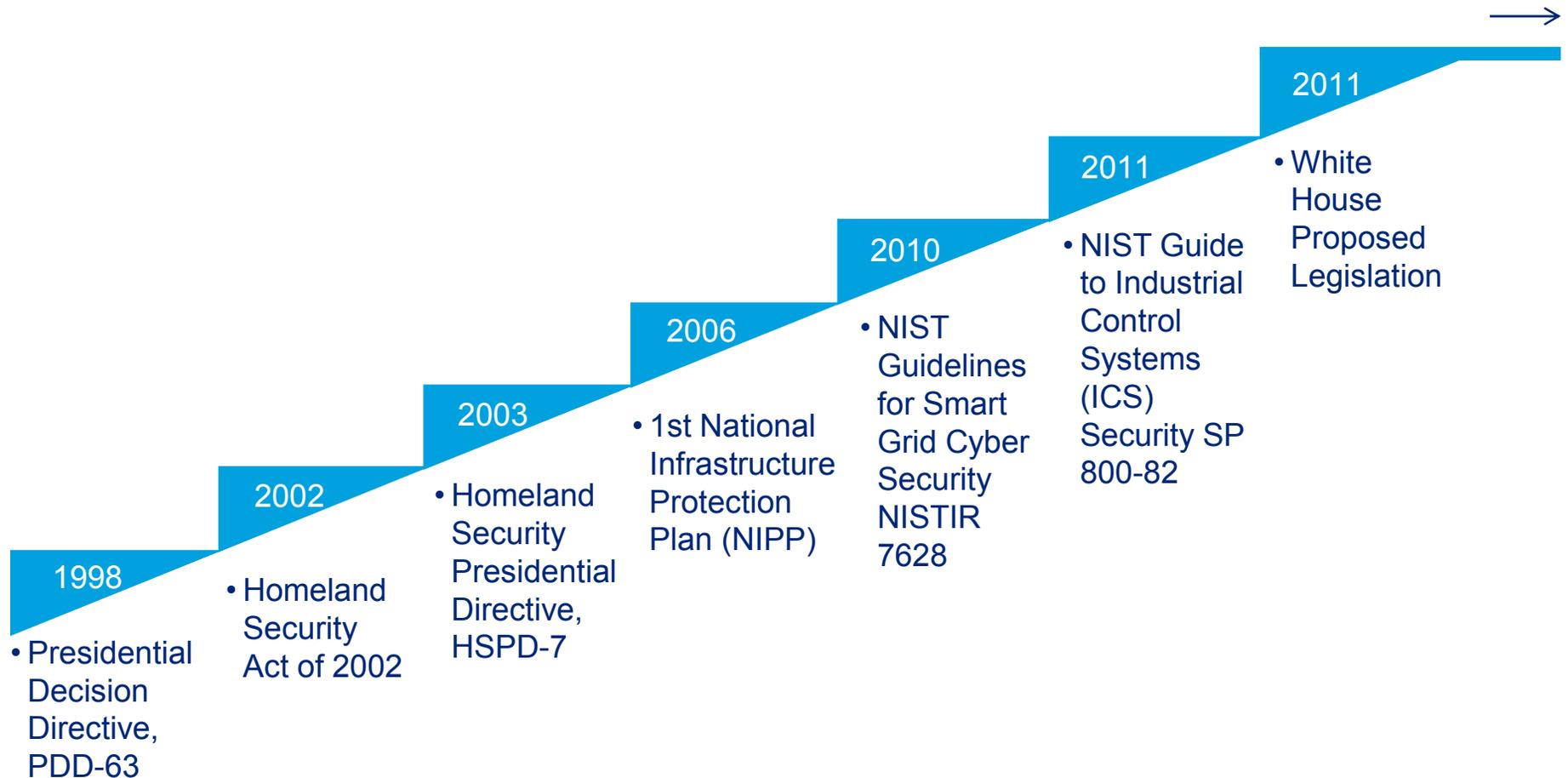
President's Critical  
Infrastructure Cybersecurity  
Executive Order  
State Impact

# State of the Union - President Obama's Plan on Cybersecurity<sup>6</sup>



<sup>6</sup> <http://www.whitehouse.gov/photos-and-video/video/2013/02/12/2013-state-union-address-0>

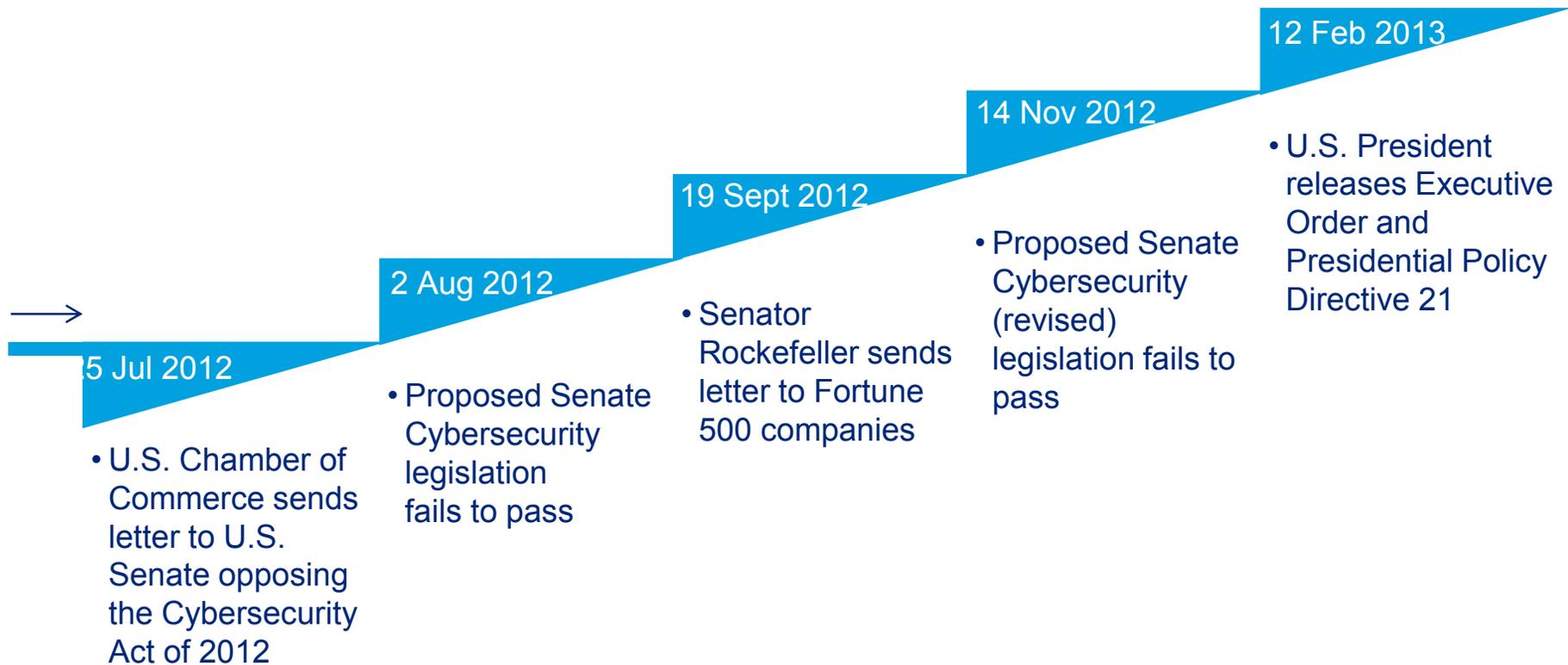
# How we got here: A look back at the evolving legislative and regulatory framework...



**“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

## ...culminating in a call to action

- Key milestones in 2012 and 2013



**“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

<b>Information sharing</b>	<ul style="list-style-type: none"><li>• Opens up information-sharing program to other sectors</li><li>• Requires Federal government information-sharing programs with private sector</li></ul>
<b>Privacy</b>	<ul style="list-style-type: none"><li>• Mandates strong privacy and civil liberties protections</li><li>• Directs regular assessments of agency activities</li></ul>
<b>Cybersecurity standards</b>	<ul style="list-style-type: none"><li>• Requires development of a Cybersecurity Framework</li><li>• Develops voluntary critical infrastructure cybersecurity program and adoption incentives</li><li>• Identifies regulatory gaps</li></ul>
<b>Critical infrastructure review</b>	<ul style="list-style-type: none"><li>• Identifies critical infrastructure at greatest risk</li><li>• Changes the definition of critical infrastructure</li></ul>

# Cybersecurity of Critical Infrastructure - timeline

		Near-term	Mid-term	Long-term
		< 150 days	150-240 days	1 year from now
<b>Federal Sector</b>		<ul style="list-style-type: none"> <li>• Broaden information sharing process and assess privacy risks (120 days)</li> <li>• Review and comment on Cybersecurity framework</li> <li>• Establish voluntary program to support framework adoption (120 days)</li> </ul>	<ul style="list-style-type: none"> <li>• Identify critical infrastructure at greatest risk</li> <li>• Develop a preliminary Framework (240 days)</li> <li>• Look for funding and budget opportunities to implement Cybersecurity Framework</li> </ul>	<ul style="list-style-type: none"> <li>• Issue final framework (1 year)</li> <li>• Report program participation and privacy risks (annually)</li> </ul>
<b>State sector</b>		<ul style="list-style-type: none"> <li>• <i>Partner to shape development of a cybersecurity framework</i></li> <li>• <i>Dialogue on information sharing</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Identification of agencies as “critical infrastructure”</i></li> <li>• <i>Identify Cybersecurity framework leader</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Adopt the Cybersecurity framework</i></li> </ul>

# Questions

**Contact:**  
Srini Subramanian  
Principal  
[ssubramanian@deloitte.com](mailto:ssubramanian@deloitte.com)  
(717) 651-6277





**[www.deloitte.com](http://www.deloitte.com)**

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