Welcome to the

Deloitte-NASCIO Cybersecurity Webinar

Reviewing the results and recommendations of the third biennial Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Time to Move Forward

www.nascio.org/DeloitteNASCIO2014CybersecurityStudy/

#StatesAtRisk

Tuesday, December 16, 2014 2:00-3:00pm ET

You are welcome to join in “Listen Only” mode or by telephone. If you joined audio via telephone, please enter the code provided by Adobe Connect to match your name and number. All attendees will be muted.

During the webinar, please ask questions by typing in the chat box.

Deloitte.

NASCIO Representing Chief Information Officers of the States

State Governments at Risk:
Time to move forward

December 16, 2014

www.nascio.org/DeloitteNASCIO2014CybersecurityStudy/

#StatesAtRisk #NASCIO #deloittegov

Today's Agenda

Introductions

About the 2014 Deloitte-NASCIO Cybersecurity Study and participation

Discuss study findings

Questions

Our Speakers Today

Stu Davis
CIO, State of Ohio and NASCIO President

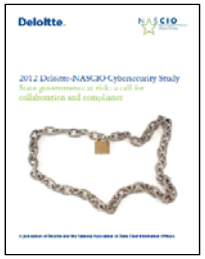
Srini Subramanian
State Sector Risk Advisory Leader
Deloitte & Touche LLP

Doug Robinson
Executive Director
NASCIO

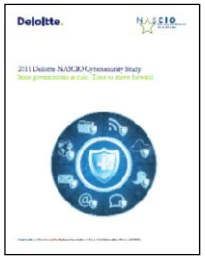
Mike Wyatt
State Sector Cyber Risk
Program Services Leader
Deloitte & Touche LLP

The 2014 Deloitte-NASCIO Cybersecurity Study

2010



2012



2014

Third biennial study

The study is based on surveys and comparisons, and offers suggestions to:

- Provide state leadership with insights and identify trends to help states set informed and strategic cybersecurity direction
- Assess elected and appointed business leader input with a state officials survey
- Compare responses from CISOs and state officials, along with relevant results from the 2010 and 2012 studies

An outstanding response and result

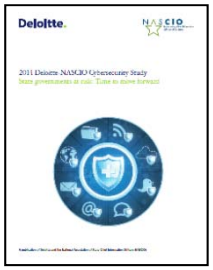
State CISO Survey: 49 state CISOs responded to an online survey containing 58 questions

State Officials Survey: 186 elected and appointed officials from 14 affiliated organizations answered 14 questions:

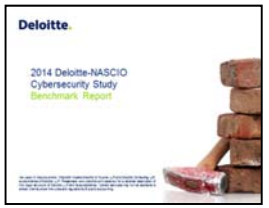
1. National Association of State Auditors, Controllers & Treasurers (NASACT)
2. National Association of Attorneys General (NAAG)
3. National Association of Secretaries of State (NASS)
4. National Association of State Personnel Executives (NASPE)
5. National Association of State Chief Administrators (NASCA)
6. National Association of State Budget Officers (NASBO)
7. National Association of State Procurement Officials (NASPO)
8. American Association of Motor Vehicle Administrators (AAMVA)
9. National Association of Medicaid Directors (NAMD)
10. National Emergency Management Association (NEMA)
11. Adjutant General Association of the United States (AGAUS)
12. Governors Homeland Security Advisors Council (GHSAC)
13. Federation of Tax Administrators (FTA)
14. International Association of Chiefs of Police (IACP) – Division of State & Provincial Police (S&P)

Results

1. Cybersecurity Study



2. Benchmark Report



Findings from the study

Key themes from the study

- Maturing role of the CISO
- Budget-strategy disconnect
- Cyber complexity challenge
- Talent crisis

I. Maturing role of the CISO

Maturing role of the CISO

The CISO role is gaining legitimacy

98.0%
Of states have a CISO

89.8%
CISOs report to CIOs

49.0%
CISO authority established by statue or law

55.1%
CISO authority established by secretary or CIO

Maturing role of the CISO

39.6%
Governors

Communication to business leaders is mostly ad hoc

25.0%
Secretary/
deputy secretary

40.4%
State legislature

43.8%
Business stakeholders

98.0%
Of states have a CISO

89.8%
CISO report to CIO

49.0%
CISO authority established by statue or law

55.1%
CISO authority established by secretary or CIO

Maturing role of the CISO

Top CISO function have standardized

100%
Awareness and training

100%
Strategy and planning

95.9%
Risk assessment and management

98.0%
Incident management

98.0%
Governance (architecture, policies, and standards)

98.0%
Of states have a CISO

89.8%
CISO report to CIO

49.0%
CISO authority established by statue or law

55.1%
CISO authority established by secretary or CIO

Moving forward…

Role and Governance

- **Governance, Risk and Compliance:** CISOs could continue to manage the strategic, risk management, and regulatory/compliance functions
- **Privacy:** Enterprise-level privacy officers can help determine which data needs to be protected and why
- **Security technology and operations**: A security executive could manage technical and operational aspects of security

II. Budget-strategy disconnect

Budget-strategy disconnect

Cybersecurity budgets are increasing year over year

Percentage of CISO respondents

2012 2014

Additional funding sources are helping with the increase

47.9%
U.S. Department of Homeland Security

32.7%
Business/program stakeholders

Budget-strategy disconnect

Funding is still the #1 barrier to effective cybersecurity

Lack of sufficient funding

Security allocation as part of IT budget remains unchanged

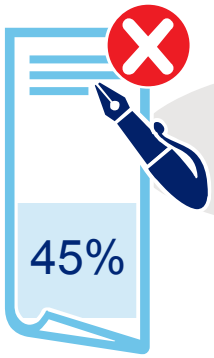
46.8% of states have only 1-2% of IT budget for cybersecurity

Senior Executive commitment is there, but funding still insufficient

65.3%

Budget-strategy disconnect

Approved strategies are still largely missing



Absence of approved strategy

Absence of business-aligned metrics

47.9%

Majority of CISOs continue to work on establishing business-aligned metrics

Moving forward…

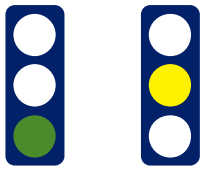
Strategize & achieve appropriate funding

- Communicate and collaborate with legislators and state business/program leadership to build a business case for security as a line item in the budget
- Effectively collaborate with agency-level program and business leaders to get cybersecurity included in program budgets
- Work with CIOs to:
  - Allocate a reasonable percentage of new business and technology initiatives for cybersecurity
  - Identify creative ways to include cybersecurity as a critical part of enterprise data center consolidation initiatives

III. Cyber complexity challenge

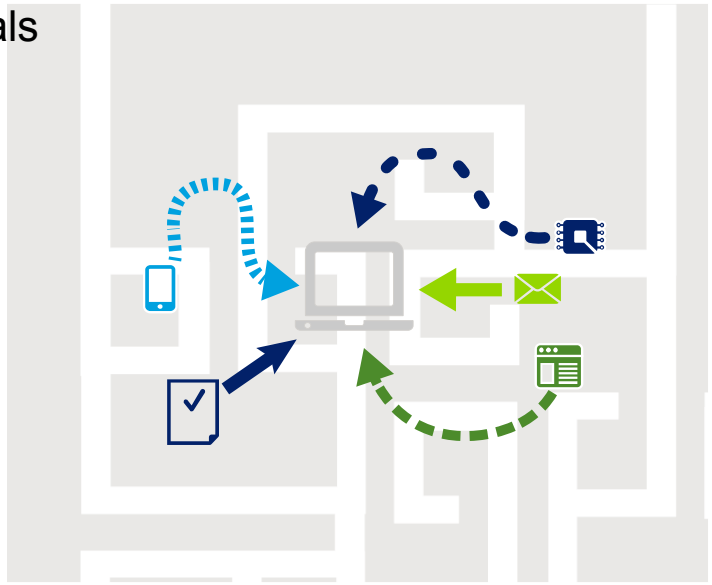
Cyber complexity challenge

Confidence Gap
Ability to protect against external attacks;
Only 24% CISOs vs.60% State officials



State officials

CISOs



Top barriers
State officials and CISOs agree

#1 Funding

#2 Sophistication of threats

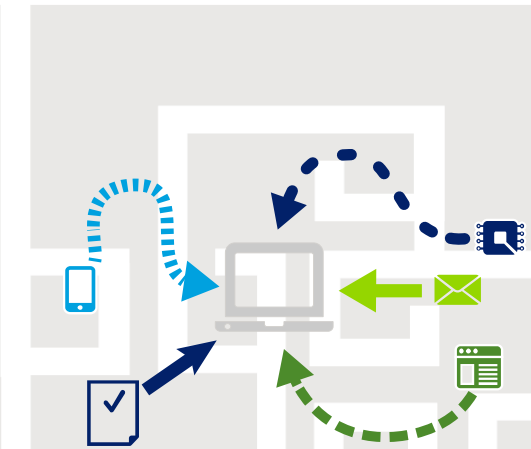
Cyber complexity challenge

Top 3 cyber concerns

74.5% Malicious code

53.2% Hactivism

42.6% Zero-day attacks



Top external cybersecurity standards used

93.9% NIST standards

46.9% NIST Cybersecurity Framework 1.0

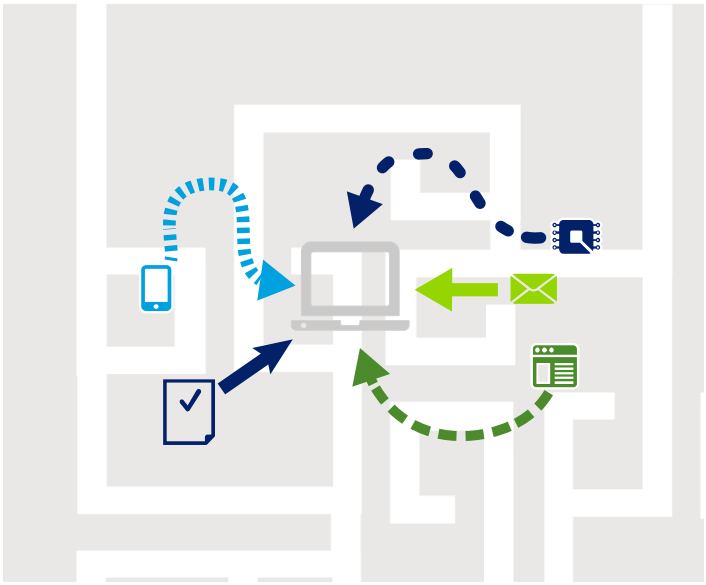
Cyber complexity challenge

Top 2 regulations for states

100%
HIPAA

1075

98.0%
IRS 1075



More regulations introduced

CMS MARS-E

OCSE security

IRS 1075 updates

Moving forward…

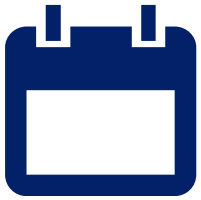
Unravel the complexity

- Use both increasing regulatory requirements and audit findings to gain the attention of business and agency/program leaders
- Clearly communicate the nature and severity of cyber risks and impacts to business stakeholders, agency/program leaders and legislative leaders
- State cybersecurity approach needs to evolve – can't rely on protection or securing efforts alone

IV. Talent crisis

Talent crisis

FTE counts are increasing



49% 6 to 15 FTEs

Competencies have increased, training has improved

7 out of 10 states agree

Inadequate availability of cybersecurity professionals

Barrier #3
59%

Talent crisis

Top challenge is staffing

Salary
9 out of 10 CISOs

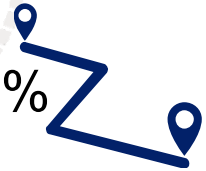
Collaboration needed with HR to define cybersecurity career path

25%

States with appropriate job descriptions documented by HR

Leading challenge in workforce development

67.3%



CISOs choose "Lack of a defined cybersecurity career path"

Talent crisis

Top three actions to improve workforce

57.1% Non-salary benefit

46.9% Cross-train IT workforce

42.9% University relations

Top functions outsourced

38.8% Forensics/ legal support

36.7% Threat risk assessments

36.7% Threat management and monitoring services

NICE framework

35.4% CISOs are reviewing

Moving forward…

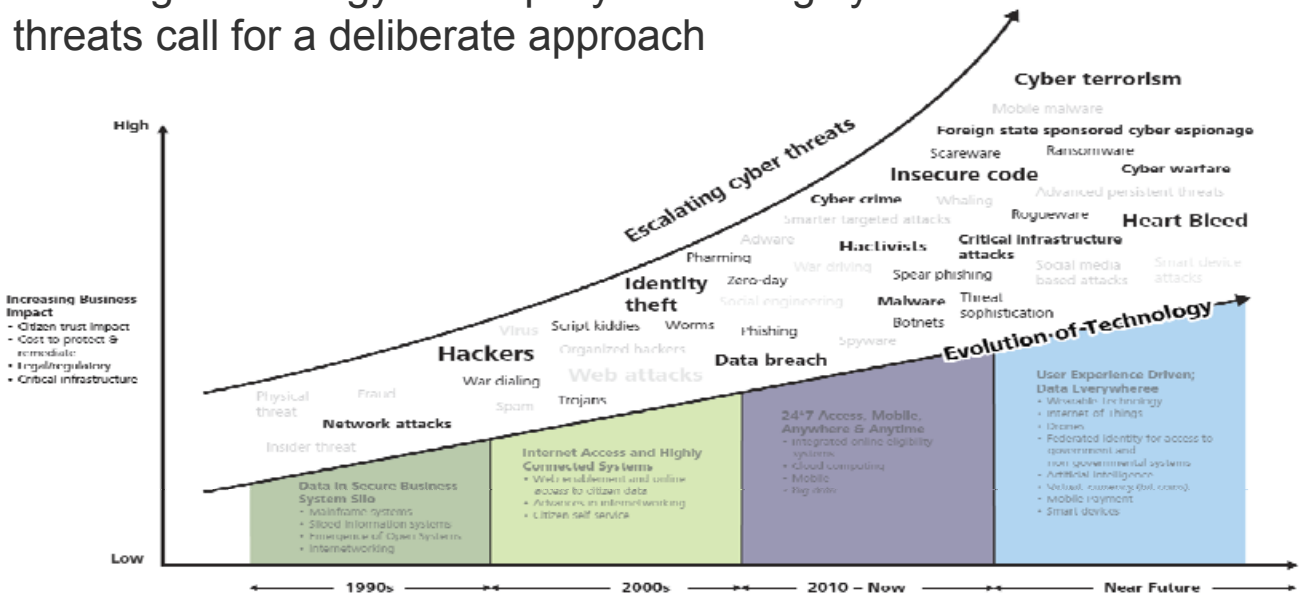
Get creative & gain on talent

- Attracting Millennials is a whole new ballgame: Millennial are likely to be an important source of talent in the cybersecurity arena
- Partner with Human Resources: States need a career development path for cybersecurity talent
- Partner with private sector to supplement cybersecurity teams: CISOs should provide training to their staff to effectively manage teams that may include members from third parties

Time to move forward

Cybersecurity should become an enterprise business imperative

Evolving technology and rapidly escalating cyber threats call for a deliberate approach



Questions

Deloitte.

About Deloitte

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see 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.

Deloitte’s Cyber Risk Services help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation and performance objectives through proactive management of the associated cyber risks. Deloitte’s practitioners provide advisory, implementation, and managed services to help transform legacy IT security programs into proactive *Secure.Vigilant.Resilient.* cyber risk programs that better align security investments with risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to thrive in the face of cyber incidents.

For more information visit www.deloitte.com.

Other questions?

Please send additional questions to
Meredith Ward at mward@nascio.org.

www.nascio.org/DeloitteNASCIO2014CybersecurityStudy/
#StatesAtRisk #NASCIO #deloittegov