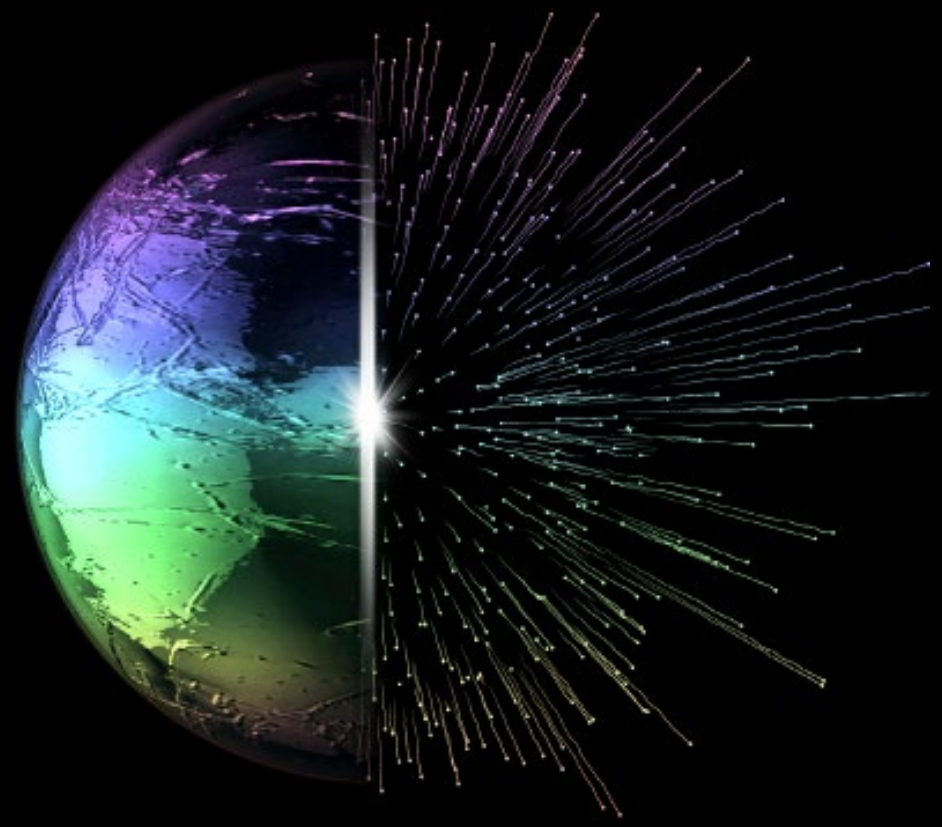
Deloitte.



Cyber risk overview for state and local government

Department of Information Resources – Internet Security Forum

March 10, 2020

Agenda

- Current cybersecurity landscape and emerging trends
- Highlights of the Deloitte/NASCIO Cybersecurity Study
- State and Local Government Cybersecurity Act
- The path forward

Current Cyber Landscape

The realm of cyber **everywhere.**

In the digital age, cyber is everywhere.
Which means cyber risk now permeates every aspect of how we live and work.

Cyber risk isn't just about IT

Cyber risk isn't just about data centers

Cyber risk isn't just about employees

Cyber is **complex.**
Cyber is **ever-changing.**
Cyber is **everywhere.**

Cyber **everywhere.**
Succeed **anywhere.**

Top threats currently facing the State and Local Governments

Destructive malware

Ransomware

IOT/connected devices

Phishing

Credential compromise

3rd party/vendors

Insider threat

Lost/stolen devices

Business email compromise (BEC)

15 seconds Time required to break into a network using automated botnets[1]

136% Percentage increase between December 2016 and May 2018 for identified global exposed losses due to BEC.[4]

#1 The cause of breaches in 2018 was the use of compromised Credentials[5]

Nearly two-thirds of all ransomware in the US have targeted state or local government[2]

2/3

11 seconds Businesses will experience ransomware attacks every 11 seconds by 2021[3]

Sources: [1] Cyber Reason https://www.cybereason.com/blog/botnets-honeypot-automation-cybersecurity [2] Statescoop article written by Benjamin Freed Aug 28, 2019 [3] Cybersecurity Ventures "Attackers use botnets to break into networks faster" 17 Apr 2018 [4] "Business E-Mail Compromise the 12 Billion Dollar Scam" FBI Internet Crime Compliant Center PSA Jul 12, 2018 [5] "2018 Data Breach Investigations Report", Verizon

Deloitte.

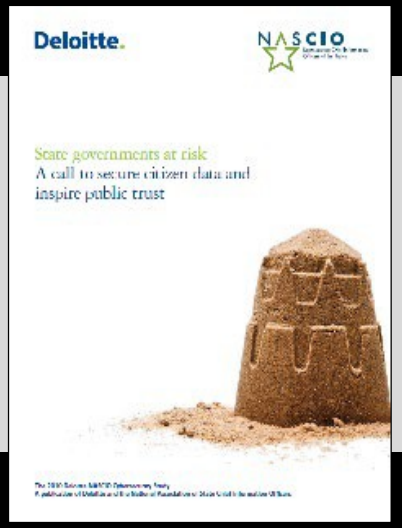
NASCIO
Representing Chief Information Officers of the States

Highlights from the 2018 Deloitte-NASCIO Cybersecurity Study

States at Risk: Bold plays for change

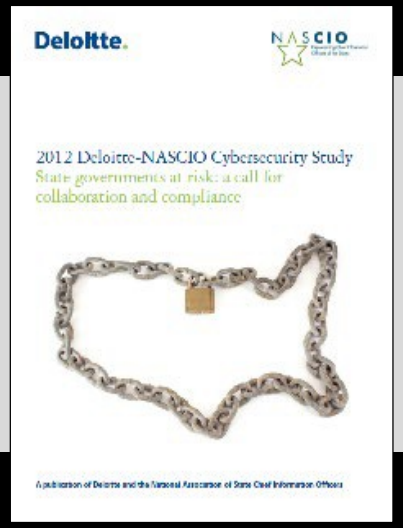
Timeline of the Deloitte – NASCIO Cybersecurity Study: States at Risk

2010



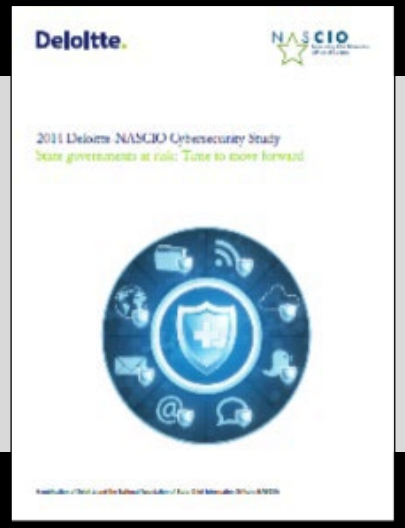
A call to secure citizen data and inspire trust

2012



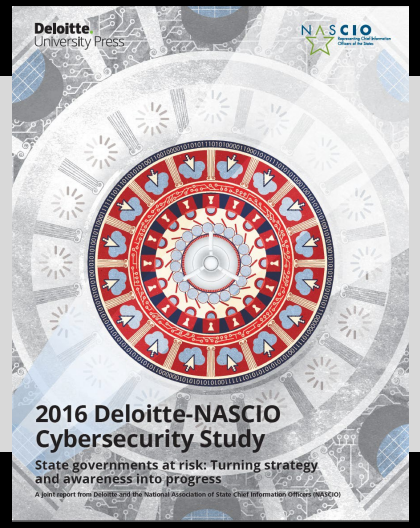
A call for collaboration and compliance

2014



Time to move forward

2016

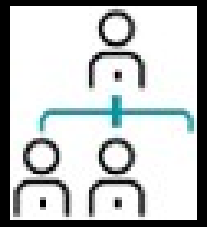


Turning strategy and awareness into progress

2018

Bold plays for change

Budget, talent, and threats remain top three challenges since 2010



Budget Challenge

- Cybersecurity budgets are growing, but very slowly
- Most states only spend 0-3% of their IT budget on cybersecurity

Talent Challenge

- Inadequate cybersecurity staffing
- State salaries, paygrades, and structure still fall behind what the private sector offers
- 6-15 state cyber FTE professionals compared with >100 cyber FTE professionals for financial services

Threats Challenge

- Increasing sophistication of threats
- Ransomware, social engineering, and phishing are the top cyber threats for states
- Web applications and malicious code are the leading sources of security breaches

The data about was obtained from surveying all 50 states as a part of the Deloitte/NASCIO study

Source: Deloitte-NASCIO Cybersecurity Study

Bold Play #1:
Advocate for dedicated cyber program funding

ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING

CISOs should raise cybersecurity's visibility with the state legislature and executive branch by making it a line item in the IT budget. They can also seek funding from federal agencies to support compliance with those agencies' security mandates.

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Bold Play#2:
CISOs as an enabler of innovation

CISOs AS AN ENABLER OF INNOVATION, NOT A BARRIER

CISOs should actively participate in shaping the state's innovation agenda, collaborate with state digital and innovation officers, and lead the charge to help program leaders securely adopt new technologies.

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Bold Play#3:
Team with the Private Sector and Higher Education

Source: 2018 Deloitte-NASCIO Cybersecurity Study

Deloitte.

US Senate has passed the State and Local Government Cybersecurity Act.

Next step is to move this to the House for passage:

- The purpose of the State and Local Cybersecurity Act, is to improve the cybersecurity posture of state, local, tribal, and territorial governments (SLTTs) through the coordination of activities with the Department of Homeland Security
- This bill will allow the Secretary to make grants to SLTTs that provide assistance and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings
- The DHS is required to provide a report to Congress one year after enactment, and every two years thereafter on the status of cybersecurity measures in each state and the largest urban areas of the United States

The Path Forward

Ideas for a path forward

- Establish or enhance a cyber governance model that transcends the typical boundary of state, agency, local, and municipalities, etc.
- View cyber with an enterprise-wide lens driven across various entities (State, local, higher education, critical infrastructure, etc.). Implement integrated services delivery model that aligns with the federal direction for funding (e.g. Security Operations Centers, Threat Intelligence, Incident Response, Training, etc.)
- Take advantage of employment and economic development opportunities with cyber being integrated

Deloitte.

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.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.