INTERACTIVE SPONSORS

Deloitte.

Hewlett Packard Enterprise

Are You Smarter than a State CISO?

INTERACTIVE SPONSORS

Deloitte.

Hewlett Packard Enterprise

1. How many states have an enterprise CISO position or equivalent?

7%	A. Less than half
20%	B. Just over half
67%	C. About two-thirds
7%	D. 100%

Source: 2015 NASCIO State CISO Toolkit

2. What is the average tenure for a state CISO?

0%	A. 6 months
31%	B. 24 months
69%	C. 39 months
0%	D. 60 months

Source: 2015 NASCIO State CISO Toolkit

3. What did state CISOs rank as the top two most important leadership traits or attributes for their position?

7%	A. Facilitator and motivator
87%	B. Strategist and communicator
7%	C. Negotiator and coordinator
0%	D. Technologist and operator

Source: 2015 NASCIO State CISO Toolkit

4. What did state CISOs report as the leading barrier to battling cyber threats?

0%	A. Lack of enterprise communication
73%	B. Insufficient funding
0%	C. Lack of organizational structure
27%	D. Lack of training for state employees

Source: 2014 Deloitte-NASCIO Cybersecurity Study

5. Behind insufficient funding, what two barriers did CISOs sight most frequently as barriers to battling cyber threats?

14%	A.	Lack of communication AND training for state employees
0%	B.	Lack of centralization AND organizational control
86%	C.	Increase in sophistication of threats AND shortage of qualified cybersecurity professionals
0%	D.	Legacy systems AND infrastructure unable to detect threats

Source: 2014 Deloitte-NASCIO Cybersecurity Study

6. Which colleague did state CISOs say having a strong relationship with was important to their success?

93%	A.	State CIO
0%	B.	State Privacy Officer
0%	C.	Their mother
7%	D.	Governor

Source: 2015 NASCIO State CISO Toolkit

7. A Chief Information Security Officer's message should be:

0%	A.	IT will fix it
100%	B.	Security is everyone's responsibility
0%	C.	Don't worry, be happy

8. Who is the primary source of cybersecurity information for state legislators and their staff?

33%	A.	Chief Information Officer
7%	B.	Chief Information Security Officer
0%	C.	Advocacy groups
53%	D.	Media reports
7%	E.	Vendors

Question Provided By: e.Republic Source: Governing Institute Research

9. What percentage of state legislators and staff know that their state has a Cyber Emergency Incident Response Plan?

40%	A.	7%
47%	B.	15%
13%	C.	28%
0%	D.	42%
0%	E.	63%

Question Provided By: e.Republic Source: Governing Institute Research

10. Who do most legislators and staff believe is responsible for enterprise cybersecurity strategy development?

67%	A.	CIO
0%	B.	CTO
7%	C.	Agency head or designee
0%	D.	CISO
27%	E.	Unsure

Question Provided By: e.Republic Source: Governing Institute Research

11. Why is state government a bigger cybersecurity threat than the federal government?

7%	A.	Lack of budgetary resources
0%	B.	Weaker security team posture
0%	C.	Lack of skilled professionals
0%	D.	Failure to patch known vulnerabilities
93%	E.	All of the above

Question Provided By: Symantec Source: Ponemon Institute

12. What percentage of polled technology and policy experts predict a major cyberattack causing widespread harm by 2025?

0%	A.	14%
0%	B.	26%
20%	C.	61%
80%	D.	87%

Question Adapted From: Govloop article
Source: Pew Research Center

13. According to US-CERT, how many breaches of federal computers occurred in 2013?

7%	A.	12,894
27%	B.	25,462
53%	C.	46,605
13%	D.	89,214

Question Adapted From: Govloop article

14. What is the average cost per lost or breached record for government agencies?

0%	A.	$1
13%	B.	$97
67%	C.	$194
20%	D.	$261

Source: Ponemon Institute

15. Approximately how many identities were exposed in 2015?

0%	A.	10
0%	B.	100
0%	C.	1000
27%	D.	1,000,000
73%	E.	200,000,000

Question Provided By: Symantec

16. In a Stanford University Study, what percentage of insider threat cases involved employees whose behavior was flagged by supervisors as suspicious, but was not followed-up on by the organization?

7%	A.	25%
47%	B.	46%
33%	C.	74%
7%	D.	82%
7%	E.	97%

Source: Sailpoint 2016 Market Pulse Survey

17. What percentage of employees would sell their work password?

53%	A. 6%
7%	B. 17%
7%	C. 27%
33%	D. 31%

Source: Sailpoint 2016 Market Pulse Survey

18. Which of these Gmail passwords is most secure?

0%	A. 12345
7%	B. N@SCIO16
40%	C. DougR@N@SCIO2016!
40%	D. 12345 + (a free text message # sent to smartphone)
13%	E. C and D are both equally secure

Question Provided By: Security Mentor

19. Which of the following is a good cyber-hygiene practice?

0% A. Write down passwords and hide them in your office.

100% B. Encrypt sensitive data before putting on portable media (CD, DVD, Flash Drive, external hard drive).

0% C. Leave sensitive information exposed on your desk, in unlocked file drawers, or written on whiteboards.

0% D. Use the same complicated password for everything.

Question Provided By: Security Mentor

20. Which of the following is a non-technical way to gain access to secure information?

0%	A.	Behavioral analysis
13%	B.	Old-fashioned bribery
87%	C.	Social engineering
0%	D.	Flattering the systems administrator

21. What is the most commonly used subject line in phishing emails?

0%	A.	Mail delivery failure
87%	B.	Your account needs attention
0%	C.	Invitation to connect on LinkedIn
13%	D.	You may already be a winner

Source: McAfee

22. Which age group is the most likely to be the victims of cybercrime?

20%	A. Generation Z (under age 18)
7%	B. Millennials (age 18-33)
13%	C. Gen-X (age 34-49)
60%	D. Boomers (age 50-68)

Source: Norton Cyber Crime Report

23. How many new pieces of malware are detected each day?

0%	A.	100
20%	B.	1500
13%	C.	1,005,000
47%	D.	1,179,000
20%	E.	5,000,000

Question Provided By: Symantec

24. What is the generic malware name given to the recent cyber threats used to extort cash from hospitals?

0%	A.	Encryptionlocker
7%	B.	Ransomlocker
0%	C.	Extortionware
93%	D.	Ransomware
0%	E.	Ransomlocker

Question Provided By: Security Mentor

25. Between 2005 – 2013, 930 million data records were breached. 80% of these breaches could have been prevented by which security solution?

0%	A. Next gen firewalls
8%	B. AntiVirus/AntiMalware
85%	C. Multi-factor authentication
8%	D. Stronger passwords

Question Provided By: Symantec

26. How do the majority of organizations learn they've been breached?

7%	A. Internal employees or tools
93%	B. Notification by an external source
0%	C. Jeff Bridges' character in Tron

Question Provided By: FireEye
Source: M-Trends Report

27. The median time it took an organization to discover a compromise was 56 days when discovered internally. How many days did it take to discover when the organization learned of the breach through an ***outside*** entity?

27%	A.	40
0%	B.	114
67%	C.	246
7%	D.	320

Question Provided By: FireEye - Source: M-Trends Report

28. What is the recommended risk management-based cybersecurity process?

80%	a)	Evaluate → Improve → Develop → Re-evaluate
0%	b)	Listen → Learn → Hope → Pray
20%	c)	Evaluate → Improve → Develop → Maintain

Question Provided By: CGI
Source: Governing-CGI Guide to Cybersecurity

29. Which of the following is NOT in the top 5 CIS Critical Security Controls v6.0?

20% A. Inventory of authorized and unauthorized software

27% B. Controlled use of administrative privileges

33% C. Intrusion prevention and detection

20% D. Continuous vulnerability assessment and remediation

Question Provided By: Tripwire

30. What percentage of files uploaded by agencies to the cloud contain sensitive data (personal, payment, health or confidential data)?

0%	A.	0%
0%	B.	3.6%
27%	C.	14.3%
73%	D.	44.9%

Question Provided By: Skyhigh
Source: Skyhigh Cloud Adoption Risk Report