2014 Information Security Survey

Personal Security Practices of the CAO

1. Do you forward your government email to your personal email account?

- Yes
- No

2. When is the last time you changed your Enterprise password?

- Within the last 60 days
- Within the last 90 days
- Within the past year
- Within the past two years
- Never

3. Do you know how your government's current security posture relates to industry best standards such as the NIST Cybersecurity Framework or SANS Critical Security Controls?

- Yes
- No

2014 Information Security Survey

Security Human Resources

4. Does your jurisdiction have a full-time employee whose tasking is Information Technology (IT) Security (CISO or CSO)?

- Yes
- No
- Do not wish to disclose

5. Does your jurisdiction have a full-time employee whose tasking is Cyber Physical Security (CPS)?

- Yes
- No
- Do not wish to disclose

6. Does your jurisdiction have a full-time employee whose tasking is Records Management (CRMO)?

- Yes
- No
- Do not wish to disclose

7. Does your jurisdiction have a full-time employee who is tasked with Network Security engineering (Firewall / Network Access Control/Routers/Switches, etc.)?

- Yes
- No
- Do not wish to disclose

8. If you do not have full-time IT security employee (ISO, CISO, engineer), who is tasked with IT security?

- [ ] Police Chief
- [ ] CIO
- [ ] Network Engineer
- [ ] Active Directory Administrator
- [ ] Schools Server Administrator
- [ ] Help Desk Technician
- [ ] Do not wish to disclose

9. If you do not have a full-time employee tasked with CP security who is tasked with this responsibility?

- ○ CISO
- ○ CSO
- ○ CIO
- ○ Controls System Engineer
- ○ Do not wish to disclose

10. How important is it for your jurisdiction to recruit and retain cyber security professionals? Importance rank 1-5 with 5 being very important.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

2014 Information Security Survey

Security Financial Resources

11. What is the per constituent cost of your current IT Security practice (include salaries, network HDWR, SaaS, MSSP, etc.).

12. Do you fund annual IT Security training for the IT Security Staff?

- Yes
- No
- Do not wish to disclose

13. What percentage of your annual IT budget is spent for IT Security?

14. Please estimate the amount of IT security spending as a percentage of annual discretionary spending for your government. Example, $7M discretionary spending for 2004 when IT security spending for that year was $100,000 would yield a result equal to .0014%

2004	
2005	
2006	
2007	
2008	
2009	
2010	
2011	
2012	
2013	
2014	

15. Is your IT department funded for annual Third Party IT Security risk assessment?

- Yes
- No
- Do not wish to disclose

16. Does your organization have Data Breach Insurance?

- Yes
- No
- Do not wish to disclose

17. If you answered yes to the previous question, what is the coverage value:

- $100,00 or Less
- $100,00 - $500,000
- $500,000 - $1,000,000
- $1,000,000 - $5,000,000
- $5,000,000 - $10,000,000
- $10,000,000 or more
- Question does not apply to me

18. Would your jurisdiction participate in a State Grant Program that would provide a one-time match 'new' IT/CP investments up to a maximum of $250,000 for your jurisdiction if you had to commit to sustaining that infrastructure for five years?

- Yes
- No
- Do not wish to answer

2014 Information Security Survey

Security Best Practices

19. Are your Anti-virus End-Point-Security updates current? (within two weeks of issuance)

- ○ Yes
- ○ No
- ○ Do not wish to disclose

20. Are the security updates on your Operating Systems current and up to date? (within two weeks of issuance)

- ○ Yes
- ○ No
- ○ Do not wish to disclose

21. Select which IT security capabilities are currently available with your Enterprise Network

- ☐ Data Base Encryption (SSNs, PII, etc.)
- ☐ Data encryption at rest
- ☐ Dual-factor Authentication
- ☐ VPN/TLS transmissions
- ☐ Automated data retention and disposition
- ☐ Date Loss Prevention
- ☐ Application Firewall
- ☐ Mobile Device Management
- ☐ Email Encryption
- ☐ Web Security Appliance
- ☐ Network Access Control with Device Remote Access Posture Assessment
- ☐ Intrusion Detection
- ☐ Security Incident Event Manager
- ☐ Do not wish to disclose

22. How do you proactively detect and analyze invalid user access and/or anomalies in applications and network traffic?

- [ ] SIEM
- [ ] IDS
- [ ] IPS
- [ ] Do not wish to disclose

23. Has your government moved 'retention' obligated records to the CLOUD?

- ○ Yes
- ○ No
- ○ Do not wish to disclose

24. If yes to the previous questions, is your government using the Government Grade CLOUD service or something less secure?

- ○ Yes
- ○ No
- ○ Do not wish to disclose

25. Do you require your IT/CP security personnel to provision never expire passwords for select individuals (agency heads, elected officials, etc.).

- ○ Yes
- ○ No
- ○ Do not wish to disclose

26. Has your government eliminated the use of Social Security Numbers as employee tracking numbers?

- ○ Yes
- ○ No
- ○ Plan to remove in the next year
- ○ Plan to remove in the next five years
- ○ Do not wish to disclose

27. Does your jurisdiction Procurement Office utilize contract language that requires vendors and contractors to confirm the use of Cyber Security Best Practices with regard to storing or handling government sensitive data?

- Yes
- No
- Do not wish to respond

28. Does your government Procurement Office utilize contract language that holds the vendor or contractor liable for data breach and or data corruption due to neglect and failure to sustain Cyber Security Best Practices in their operations?

- Yes
- No
- Do not wish to disclose

29. Does the Treasurer and Commissioner of Revenue in your jurisdiction store Constituent Personal Identifiable Information (credit card / bank account/ SSN) in clear text (not encrypted)?

- Yes
- No
- Do not wish to disclose

30. Does your new employee orientation include employee awareness training for IT/CP Security?

- Yes
- No
- Do not wish to disclose

31. Does your new employee orientation include employee awareness training for Records Management?

- Yes
- No
- Do not wish to disclose

32. Do you know if Operational Technologies for Cyber Physical Systems are in place within your jurisdiction (traffic light controls, water pumping controls, fire suppressant controls, etc)?

- Yes
- No
- Do not wish to disclose

33. Do you have Cyber Physical Systems (SCADA, HVAC, etc.) secured in your jurisdiction?

- Yes
- No
- Do not wish to disclose

2014 Information Security Survey

Security Organization

34. Do you have a centralized or de-centralized IT and Security organization?

- Centralized
- Decentralized
- Do not wish to disclose

35. Does your IT Security organization have access to senior management for Risk notification etc?

- Yes
- No
- Do not wish to disclose

36. Does your IT Security organization have authority to mitigate risks against your Enterprise without prior authorization from senior management if malicious activity is detected?

- Yes
- No
- Do not wish to disclose

37. Does your IT Security organization have compliance authority in your Enterprise Network without senior management approval?

- Yes
- No
- Do not wish to disclose

2014 Information Security Survey

Security Policy, Processes and Training

38. Please select what policies your organization has in place:

- [ ] IT Security Acceptable Use Policy for employees and contractors
- [ ] Architecture Review Process
- [ ] System Development Life Cycle
- [ ] Records/Data retention Policy
- [ ] GPS tracking of smart phone policy
- [ ] GPS vehicle tracking policy
- [ ] BYOD Policy
- [ ] HIPAA compliance Policy
- [ ] Do not wish to disclose

39. Do all employees receive annual IT Security training (online or classroom training)?

- ○ Yes
- ○ No
- ○ Do not wish to disclose

40. Do all employees receive annual Records Management training (online or classroom training)?

- ○ Yes
- ○ No
- ○ Do not wish to disclose

41. Does your government maintain an internal web presence where employee can go to learn about Cyber Security Best Practices, Threats, Risk, etc.?

- ○ Yes
- ○ No
- ○ Do not wish to disclose

42. Does your organization have a data retention and classification policy?

- ○ Yes
- ○ No
- ○ Do not wish to disclose

43. Do you believe your jurisdiction is compliant with State and Federal data retention policy?

- Yes
- No
- Do not wish to disclose

2014 Information Security Survey

Public School System IT Security

44. Is your jurisdiction's IT department also responsible for School Systems or are they separate entities?

- Yes
- No
- Do not wish to disclose

45. Do your schools and government share the same computer Domain?

- Yes
- No
- Do not wish to disclose
- N/A

46. Does your School System have an IT employee who reports to the jurisdiction CISO?

- Yes
- No
- Do not wish to disclose

47. What would you estimate is the average timer per incident to remediate malware or botnet for your School System?

- 4 hours
- 24 hours
- 48 hours
- 72 hours
- Over a week
- Do not wish to disclose

48. Does your School System provide after hours and/or weekend coverage in the event of a Cyber incident?

- Yes
- No
- Do not wish to disclose

49. Does the School System in your jurisdiction have annual IT Security audits and is your government aware of the results of those audits?

- Yes
- No
- Do not wish to disclose

50. Would you support a Governor's executive order that requires Publicly Funded Schools to follow Cyber Security Guidelines and Best Practices provided by the State Secretary of Technology or would you prefer to have those guidelines provided by your local jurisdiction's Chief Information Security Officer (CISO)?

- Yes from State Technology Secretary
- Yes from jurisdiction CISO
- No
- Do no wish to disclose

Public Safety and IT Forensics

51. Does your jurisdiction have an established Police Dept Information Technology Forensics (PDITF) dept. or team?

- Yes
- No
- Do not wish to disclose

52. If your jurisdiction does have an PDITF, do employee rotations apply those positions?

- Yes
- No
- N/A
- Do not wish to disclose

53. Would you support excluding PDITF positions from employee rotations to promote better skill retention and development in support of improved effectiveness?

- Yes
- No
- Do not wish to disclose