John Byers

Presentation to the
Joint Committee on
Information Technology
(Information Security)

December 18, 2012

Information Security Audits

ITEM 1

Do selected states agencies have an adequate security management process to assess, manage, and monitor IT risks

Information Security Audits

ITEM 2

Do selected state agencies adequately control passwords?

Information Security Audits

ITEM 3

Do selected state agencies provide adequate security awareness training to all staff?

Information Security Audits

ITEM 4

Do selected state agencies adequately patch servers and workstations?

Information Security Audits

ITEM 5

Do selected state agencies adequately secure network access points?

Information Security Audits

ITEM 6

Do selected state agencies adequately inventory and track IT hardware?

Information Security Audits

ITEM 7

Do selected state agencies have adequate policies and procedures for continuing operations in the event of an emergency?

Improvements and Enhancements

- Wireless
  - KS-Open
  - May 2013 (KS-GOV)
- Desktop Anti-Virus/DLP Solution
  - Sophos end point protection solution
    - Anti-Virus
    - Malware

Improvements and Enhancements

- Sophos – End point solution
  - Host Intrusion Detection
  - Data Loss Prevention (Centrally Managed)
- Intrusion Detection Protection (Sourcefire Solution)
  - Gateway SolutionIntrusion Detection Protection (Sourcefire Solution)
  - Gateway Solution

Security Centralization

- With over ninety agencies, boards and commissions the ability to manage security is dependent on establishment of State-wide standards that are measured, repeatable and universally applied.

Dedicated Security Staff

- Ten years ago a Professional Security person might be someone who provided User creation, today with the challenges faced by various organizations looking to disrupt services and undermine government functions a security professional is no longer doing user creation, but overseeing the fundamentals and processes to ensure the necessary safeguard are applied and following in the creation process.

Dedicated Security Staff

- Identity Access Management IAM with automated workflows has replaced the manual processes. That user creation person has become the person who helps and assist in the identification of rolls and responsibilities for the automation process. The State lacks a IAM system which would provide for greater accountability and security.

Information Security Funding

- Decentralization has contributed to the lack of funding of Information Security or the funding figures have been buried in the agencies budgets making it impossible to figure what expenditures are for security and what is used elsewhere.

Information Security Funding

- Information Security needs to have dedicated funding. The funding should be based on a outside assessment. The recommendations would be to use Gartner to conduct.

Risk and Vulnerability Assessment

- Without a dedicated professional security staff the basic fundamentals of security Risk and Vulnerability assessment is lacking. This is more than some automated scanner scanning for system vulnerabilities.

Risk and Vulnerability Assessment

- This requires a security person to conduct a risk assessment on our agencies, board and commissions annually. These assessments will identify shortfalls in security and allow for the growth of the State's overall Cyber-Security program.

Log Management and Security Incident and Event Management (SIEM)

- Various federal standards require Log Management and Security Event Monitor and Alerting. These services are lacking for the State. Over the next year it is our desire to find a solution and begin the process of providing these services.

Log Management

- Log Management is a requirement for several of the programs that the State administers. HIPAA, IRS, PII and others require these services for Sensitive data to ensure that any potential issue with security is address early and does not escalate into a major situation. South Carolina recent issues point to the real need for a log management SIEM solution for the State.

Log Management

- Without Log Management and Security Incident Event Monitoring we run a real risk of placing ourselves in a similar situation as South Carolina and other organizations.

Information Technology Standardization

- Standardization of Technology across the agencies, boards and commissions not only reduces expenses but improves overall security. The efforts are ongoing to standardize on hardware and software this we believe will over time improve effectiveness and security through gained infrastructure standardization.

Closing

- The Goal of Cyber-Security is to become part of the overall organizational culture. A recent government finding stated that by the year 2020 we will have a shortfall of 4 to 5 million security professionals.
- I believe one of our goals is to find away for Kansas to become one of the places that those security professional are trained. To do so the State must set it's goal as being a leader in a State government committed to Cyber-Security.

Contact Information

John Byers
CISO
Landon State Office Building
900 SW Jackson St, Suite 751-S
Topeka, KS 66612

Office: 785.296.8434

Conclusions

- Any questions...?