North Dakota
Information Technology Department

New Deputy CIO / Director of Operations

Dan Sipes, CPA, CISA

26 Year State Employee

10 Years with State Auditor's Office – Information Systems Audit Manager

16 Years with ITD – Director of Administration (Accounting / Security)

IT Committee Security Update

- Security Focus at ITD
  - ITD continues to focus on expanding security awareness and improving the security posture for the state network and computing resources.
- Escalation of Attacks
- Increasing Number of Audits
- Recent Steps Taken by ITD
- Future impact

Attacks continue to escalate

- Utah Department of Health – March 2012
  - 780,000 residents had PII, health data or social security numbers compromised.
- South Carolina Dept of Revenue – August 2012
  - August 2012 a spear phishing attack compromised user credentials resulting in 44 compromised systems and exported 75 GB of encrypted and unencrypted data.
- Websites of Washington Post, CNN and Time – August 2013
  - Syrian Electronic Army uses phishing to gain access
- Google/Facebook/Yahoo/Twitter – December 2013
  - Over 2 million login credentials and passwords were stolen and posted online using malware on personal computers.

Increasing Number of Audits

- During the last year ITD has been subject to numerous audits
  - State Auditor Security Audit - ManTech Audit (2)
  - State Auditor Service Organization Control Report – pending
  - Federal Audits (4)
  - Federal Reviews (2)
  - PCI Review (1)
- Overall audits are a good thing. However the current risk that ITD must manage is spending too much time on lower level audit issues rather than primary security risk areas.
- "Security by Compliance" is not the desired state. We need to fear the attacker rather than fear the auditor.

Recent/Current Security Initiatives

- Expanding Intrusion Detection/Intrusion Prevention solutions at various locations on the network.
- Implementation of Security Information and Event Management solution.
- Implementation of Multi-Factor Authentication solution.
- Initiation of the Security Application Scanning process (AppScan).
- Initiation of Formal Risk Assessment Process.
- Implementation of encryption of data at rest solution.
- ITD Security Framework 2.0 (mapped to NIST 800-53).

Security Impact

- Security is a trade-off – we often must give something to get an improvement in perceived security posture:
  - Time, Money, Convenience, Capabilities, Liberties
  - We must continue to evaluate "Risk" and determine if the trade-off is worth risk we are mitigating.
- Forecasting an increase in the number of resources ITD is committing towards security – time, staffing, solutions.
- When possible ITD is attempting to make security changes "transparent" to its customers, however some changes may bring an impact.
- We appreciate the cooperation we receive from state agencies as we continue to improve our security posture.

ITD Security Framework

- Security Functions
  - Identify (Assess) Protect (Prevent)

    Detect Respond

    Recover
- Security Areas
  - Network Security Host Security

    Application Security User Security

- Effective security applies all five functions across all four security areas.