CSO PERSPECTIVES

Regaining Control & Preparing for the Future

Securely Embracing BYOD and the Demands of Mobile Data

Topics

- Emergence of BYOD @AIC
- Regaining our Security Footing
- Building a Secure Future
- Wish List & Future Considerations

AIC Overview

- Publically held P&C company
- Insuring over 16M households
- Principally US Based
- Approx 40,000 agents & staff
- Approx 43,000 FTE's and partners

Technical Landscape

- Approximately 100,000 managed end points
  - Disk Encryption
  - AV & HIPS
  - Controlled MSD access
- DLP implemented on egress points
- Mixed population of mobile devices
- Centralized security, procurement, privacy & other corporate functions

Emergence of BYOD

- 2001 Agency Owned Technology direction established
- 2009 BYOD for Employees
- Initiator: Expense Reduction
- Witnessed natural evolution to phone & tablet form factors

BYOD Controls (what we thought)

- Strategy was focused almost exclusively on PC form factor
- Predominately leveraged Citrix technology
  - Consolidate data/ systems to data center
- Implemented controls to limit ability to remove data
- Increased monitoring of egress traffic

Uncontrolled Growth (what actually happened)

- Surge in (personal) iPhone devices, declining BES clients
- Emergence of Android tablets & handhelds
- C-Suite pressure to adopt new technology
- WiFi “hotspot” service developed
- Our implementation of tactical controls loosing operational viability

Turning Point

- Adoption of BYOD declining; clients demanding off-line data access
  - Assumption of near constant WiFi proving false
- Current state assessment of mobile access demonstrated inefficient, non sustainable controls
- Re-calculating compute offerings for thin-client/ client-less services
- Incorporating security into architectural requirements

Establishing our Foothold

- Decline in BYOD enrollment provided opportunity
- Executive focus/awareness on information security
- Maintained tactical IT controls to curb growth
- Leveraged mature architectural and procurement processes to establish control

Current State

- Investigating Mobile data security offerings for handheld devices (phones, tablets).
  - Intend to deploy in 2012
- Understanding client demand for cloud and mobile use cases
  - Creating comprehensive strategy for data management on non-managed devices
- Enhancing DLP capabilities

Building a Secure Future

- Anticipate expanded field use cases, in particular claims management.
- Windows 8 will likely increase the extent of data replication and introduce new challenges
- Assume demise of corporate assets, set focus on data management

Building a Secure Future

- More accurately predict and monitor for shifts in the utilization or innovation of mobile apps
- Think through use cases and the ramifications of instituting controls
- Understand our legal limits & obligations relative to mobile data and access.

Wish List

- Ability to securely manage data across multiple mobile device types –regardless of form factor
- Ability to create & manage of off-line data repositories
- Field specific DLP controls (PII, PHI, etc)
- Enhance ActiveSync controls in preparation for Windows8

Wish List

- Enhanced e-discovery & forensic capabilities
- Ability to (easily) integrate with existing Identity & Access Management tools
- Geographic awareness

Thank you

Jeffrey Wright
jeff.wright@allstate.com