GSA Cloud Security Case Study

Kurt Garbars
Certified Information Systems Security Professional
Senior Agency Information Security Officer
General Services Administration
June 13, 2012

Topics

- Purpose
- Reason for moving to the cloud
- Byproduct of moving to the cloud
- Google Mail
- Salesforce.com
- Fiberlink (MaaS 360)
- Cloud ATOs
- Key to successful cloud security ATO

Topics (cont)

- Google security differentiators
- Salesforce security differentiators
- Fiberlink security differentiators
- Cloud security threats
- Cloud security challenges
- GSA cloud security best practices
- Lessons Learned

Purpose

- Provide overview of GSA’s accomplishments and security challenges in implementing 3 cloud based services (i.e. SaaS) for 17,000 users
  - –Google
  - –Salesforce.com
  - –Fiberlink

Reason for moving to cloud

- Aging Infrastructure
  - Lotus Notes, Lotus Domino, Sametime and Quickr
    - Expensive to maintain
- Agility
  - Ability to quickly add functionality
    - For all 3 services
- Cost Savings
  - $3M/year for email/collaboration
  - $200K/year for Fiberlink MaaS360 power management

Byproduct of moving to the cloud

- Increased security

Google

Google Apps Cloud Core Applications	Available in Google Apps Cloud ATO Scope	Available in Google Apps for Government and CONUS
Gmail	X	X
Google Calendar	X	X
Google Drive (Documents, Spreadsheets, and Presentations)	X	X
Google Talk	X	X
Google Contacts	X	X
Google Groups	X	
Google Sites	X	
Google Video	X	

Salesforce

Salesforce.com Applications	Available in CONUS
Force.com Platform	X
CRM Applications (including Sales Cloud, Service Clould, Custom Cloud, Content, Ideas, Knowledge, and Answers)	X
Chatter	X
Force.com Platform Public Sites	X
Service Cloud Portal, Customer Portal, Partner Portal	X
Authenticated Sites	X
Sites.com	X
Visualforce coding	X

Fiberlink

- MaaS 360
  - Power Management
  - Monitoring security status of workstations/servers
  - Mobile device management for smart phones/tablets
  - Cyberscope reporting
  - Application inventory for all assets

Cloud ATOs

- GSA began discussions with a few cloud providers in June 2009
  - Based on cloud initiative by Federal CIO
  - Precursor to FedRAMP
  - Used GSA security requirements based on NIST 800-53 R3
  - Cloud providers hired independent assessors with GSA oversight
  - Google was the first to obtain ATO in July 2010
- ATOs maintained in GSA's FISMA inventory; working on FedRAMP
- ATOs can be leveraged government-wide
- Agencies still need to perform assessment on agency responsible controls and provide final ATO

Key to successful cloud security ATO

- Thorough understanding/agreement on the boundary of the cloud/scope of the assessment
- Understand the inherited controls
- Understand the vendor versus agency security control responsibilities
- Understand the security control touch points (those controls that have a shared responsibility)
- Agree upfront on all NIST 800-53 parameters, alternate implementations, key controls, and show stoppers

Google Security Differentiators

- Configuration management
- Vulnerability management
- Source code scanning
- Google for Government “cages”
- Full Disk Encryption (GAfG)
- Anti-malware and spam filtering capability
- System availability (COOP)

Salesforce.com Security Differentiators

- Apex programming language
- Source code scanning of all apps
- Configuration Management
- Agile Application development with like security
- Common development practices for entire agency
- Individual assessments of minor applications
- Weekly scans of the Application environments

Fiberlink Security Differentiators

- Monitor workstations, servers for security settings
- Control workstations, servers for security settings
  - Patching
  - Security Hardening
- USGCB compliance (i.e. old FDCC) & Cyberscope
- Quickly add security functionality for agencies
- Mobile device management for smartphones/tablets
- Perform above functions to multiple devices in any Internet connected location

Cloud Security Threats

- End user information sharing to unauthorized users
- APT attacks on agency admins/agency end users
- APT attacks on vendor admins
- Insider threat (vendor)
- Web site attacks on insecure code

Cloud Security Challenges

- Vendors not familiar with government security requirements
- Qualified assessors with cloud security expertise
- Environments that are continuously changing
- Vendors did not design system IAW NIST 800-53 security requirements
- Transparency
- Background investigations
- Location of datacenters

Cloud Security Challenges (cont)

•Auditing/Logging

•Continuous monitoring

•Trusted Internet Connection

•Direct HSPD-12 authentication

•2-factor authentication of vendor personnel

•Data leakage prevention

•Custom/specialized environments; requires atypical assessment models

GSA Cloud Security Best Practices

- Layered security authorizations for Salesforce apps
  - Platform/Gov-wide, Agency/Org, Application
- Efficient Salesforce apps ATO process to include security code scanning
- Upfront background investigation process
- Information sharing process
- Isolation of admin access
- Maintain internal control of 2 factor authentication

Lessons Learned

- Need stronger contract clauses related to security
  - Incentives/Penalties
  - FISMA Cyberscope
  - Auditing/Logging
  - Background investigations
  - Continuous monitoring
- Better process for security reviews before upgrades/enhancements

Questions