How To Implement Security Effectively Without Impacting Reliability: Lessons From the Trenches

SANS SCADA Summit
January 16th 2008
New Orleans, LA

PACIFICORP
A MIDAMERICAN ENERGY HOLDINGS COMPANY

PacifiCorp Quick Stats

- Headquarters in Portland, OR
- ~6750 Employees
- ~136,000 square miles of service area over six states
  - Oregon, Washington, California, Utah, Wyoming, Idaho
- ~1.6 million customers
- ~8,470 MW of generation
- Owned by MidAmerican Energy Holdings Company
- Made up of three sub-organizations
  - PacifiCorp Energy, Pacific Power and Rocky Mountain Power

The New EMS Challenge

- Needed to consolidate 14 legacy systems into one new system
- RFP language was unsatisfactory, but it was too late
- Vendor pulled a "bait and switch" – and some other stuff
- InfoSec clashed with Ops and vendor over everything
- InfoSec shifted perspective: seek first to understand
- Started over – first step, wag the dog
  - Factory/Site Acceptance Tests (FAT/SAT)
  - Maintenance and Support Contract
  - User Group
  - National Labs (INL NSTB)

Our CLS Cure (Chicken Little Syndrome)

- The prior message from Ops was "absolutely not!"
- The EMS implementation costs were rising – good timing
  - New ownership
  - After this much time and money, will it be secure?
- Senior Management approved an assessment
  - Performed our own internal assessment first
  - InfoSec presented a careful, phased, and financially balanced approach to Senior Management that had no FUD – just dollars and risk
  - Requested validation by a qualified external third party of our findings
- More meetings to get Ops on-board

EMS Growing Pains

- QAS is essential, but comes with interesting challenges
  - Connections to what?
  - Boundaries (both physical and electronic)
  - Hardware drift
- Patches – not just for Microsoft anymore
- Passwords, SSO/CSO and disparate technologies
- Shared accounts (need I say more?)
- Managing devices across boundaries
- Moving heaven and earth: the upgrade path

External Efforts

- A huge round of applause for the NSTB/INL for the initial effort
- The "consortium" = INL, vendor and asset owner partnership
- Another huge round of applause for the User Group
- And why not, let's even give the Vendor some kudos
- People are finally talking: SANS, E-Sec NW, S4 etc…

Lessons Learned…

- Complexity was the enemy; it was easy to hide things in chaos
- Ops really did want a secure system, but it still had to function
- Culture shift – for everyone – was the hardest part, and it still is…
- "Soft-skills" mattered more than technical skills
- Isolation/separation is best, but *very* hard to achieve
- The vendor relationships will make/break our efforts
- Some interesting new technologies can actually help (finally!)

Questions?

Patrick Miller

CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM

Sr. Security Consultant – Corporate Security and Regulatory Compliance

patrick.miller@pacificorp.com

503.813.7014