Building a Cybersecurity Culture: Tips and Tricks

Public Power Cybersecurity Summit
November 13, 2018 | Austin, TX

Randy Black, CIO and IT Manager, Norwich Public Utilities
RandyBlack@NPUMail.com

Joshua Cox, Sr. System Admin., City of Westerville Electric Div
Joshua.Cox@Westerville.org

Christopher Kelley, PMP, VP, Beam Reach Consulting Group
CKelley@BeamReachGroup.com
Norwich Public Utilities

- Est. 1904 - Electric, Natural Gas, Water, & Wastewater
- City of 40,000
- 21,000 electric customers
  - 2,200 Commercial
- 3 Substations
- 40 MW of generation
  - plus, 10 MW of community Solar
- Our mission is to make Norwich a better place to live, work, and do business
Westerville Electric Division

- Est. 1898
- 17,000+ total customers
  - 2,100+ business customers
- Full AMI deployment
- Reliable Public Power Provider (RP3)
- 6 substations, 27 feeders
Beam Reach Consulting Group

• Strategic planning, project management support for energy infrastructure and resilience programs
• Staff have supported over 75 electric grid projects across the US
• Program management for energy infrastructure programs > $7.9 billion
• APPA Associate Member, WOSB
Overview

• Public Power Cybersecurity Roadmap
• What is change management and why is it important for cybersecurity improvement?
• Stories from public power
• Moderated discussion
Public Power
Cybersecurity Roadmap

- Clear actions and outputs for small- to med-public power utilities
- Focused on priority pathways

Driven by Cybersecurity Roadmap Advisory Council
Informed by industry

Public Power cybersecurity Roadmap bridges the gap between assessment and action.
(Organizational) Change Management for Security

- Structured approach
- Impacts teams, individuals, organizations
- Current state → Desired future state
Why is Change Management So Important?

- Impact on people is often overlooked
- People are what make your organization work

20% of employees willing to sell passwords to a third party*

Trap: The value of technology improvements are self-evident

*SailPoint Market Pulse Survey (2016)
Change Management Challenges for Cybersecurity Adoption

• Security is the enemy of productivity!
• Cybersecurity has never been an issue for us before.
• We are a small utility in a small town. We’re not on the radar screen.
• We can’t afford it!
• I already have 3 day jobs. How do I have time for one more?
Public Power Cybersecurity Roadmap Advisory Council

Designed approach to cybersecurity maturity implementation

- Establish management buy-in
  - Security program
  - Budget and resources
- Assess the need and set the vision
- Prioritize and treat cybersecurity maturity like a project
- Develop successful employee training
- Establish data/metrics for security program
Models

GE Model for Change

• “Why” before the “how”
• Vision for the new state outline what the change achieves
• Strong senior leadership support
• Mobilize the workforce by engaging staff in planning and definition of new process
• Measure success
• Maintain consistency

Prosci’s ADKAR®

• Awareness of the need for change
• Desire to support the change
• Knowledge of how to change
• Ability to demonstrate skills and behaviors
• Reinforcement to make the change stick

Identify a model that works for your organization… and be prepared to change it!
Engagement is the key

• Stakeholder identification
• Create clear measures for the change
• Identify and arm change sponsors and change agents
• Staff support via honest solution-seeking

Change Management Resources

• Select a methodology that works for your organization
• Figure out who will effect the change and who will be affected
• Create a change and engagement plan
• Generate ideas from staff and act on them
• Celebrate your champions and change agents
• Measure and reinforce the change
Case Study: Segregation of Electric SCADA at NPU

• Due to the NERC/CIP Standards Changes, we needed to segregate the electric SCADA from the “Corporate” LAN

• In conjunction with that activity, we needed to validate that all “active” users were still truly required to access the SCADA system
  o Deleted those users and notified them that they were losing access due to regulatory requirements. No push back was received
  o Also implemented process to delete users as they leave the utility or take on other roles that no longer require the SCADA access

• System now runs inside a secluded Electronic Security Perimeter (and a revised/enhanced Physical Security Perimeter)

• Operations staff have also since contracted with the SCADA vendor to manage antivirus protection and system backups within the ESP
Case Study: Other SCADA at NPU

• Currently performing quarterly updates of operating system software (not SCADA software)
• In process of upgrading all other SCADA systems to current release
• Included in that activity is a review of the current user base
• Also implementing (mandated) Antivirus Protection and automated system backup tools for each device as its being upgraded to the new SCADA version
  o Thus ensuring all systems work seamlessly without conflict day 1 (explain)
Case Study: Financial / CIS adoption at Westerville

• The task at hand was to implement a new Financial and CIS system.
  ○ Phased approach
• We organized a core team from various parts of the organization (cross-functional).
• Engaged all employees, defined current business processes, discussed the “to-be”, and maintained communication throughout the project.
• Financial system went live July 2016 and CIS on December 2016.
Moderated Discussion

Josh Cox
Senior System Administrator

Randy Black
CIO and IT Manager
Questions?