Security vs Compliance and SANS
Securing the Utility (STU) Training and Awareness

By: Chris Humphreys
CEO/Director

www.TheAnfieldGroup.com   |   info@TheAnfieldGroup.com   |   904.347.7657
Overview

- The Security Vs. Compliance Dilemma
- Strategic Solutions
- Training/Awareness
The Security Vs. Compliance Dilemma

Question: “Shouldn’t I be secure if I’m compliant with the NERC CIP Standards?”
The Security Vs. Compliance Dilemma

- Often Completely siloed departments within utilities
- Little to no coordination except 3-6 months prior to an audit or 2 weeks prior to self-certification- way too late!
- Budget and Resourcing allocations are not coordinated between departments
The Security Vs. Compliance Dilemma

- Millions of dollars being spent on Compliance and not Security
- What is the ROI for having a compliance assessment done when the standards will be outdated in 6-12 months?
- How many FTEs does your organization exhaust tracking administrative documentation for demonstrating compliance instead of focusing on security and reliability?
In this model, Compliance serves as a byproduct of sound security best practices.
Strategic Solutions

- Security-based Controls that satisfy multiple regulatory frameworks
  
  - Example: A Risk-Based Assessment approach that satisfies Sox, NERC, and SANS Top 20 Critical Controls
    
    - CCA Identification - NERC
    
    - Objective Settings/Event Identification - SOX
    
    - Inventory of Authorized and Unauthorized Devices and Software - SANS 20 Critical Controls
    
    - The Compliance burden becomes far more sustainable
Training and Awareness

- Continues to be a major challenge for most utilities

- CIP-004 “Personnel and Training” is one of the highest violated NERC Standards

- Knowledge Transfer is not happening between compliance and security divisions

- Training is inadequate and out of date
Training and Awareness

- Partnered with the SANS Institute (www.sans.org)

- Authoring the SANS Securing the Utility Curriculum
  - Launches February 2013 at SANS SCADA Orlando Florida

- Leveraging the NERC CIP Standards as a base, the course will provide the student the knowledge needed to be secure and compliant

  - Six Video Modules, 5-8 minutes each
    1. Overview of NERC and FERC
    2. Introduction to the NERC CIP Standards
    3. Identification and Proper Use of Critical Cyber Assets
    4. Physical Access Controls to Critical Cyber Assets
    5. Electronic Access Controls to Physical Cyber Assets
    6. Recovery of Critical Cyber Assets following a Cyber Security Incident
Questions?

Chris Humphreys, CEO/Director
The Anfield Group
429 Manchester Lane  •  Austin, TX  78737  •  904.347.7657
chumphreys@theanfieldgroup.com  •  www.theanfieldgroup.com
Follow us on Twitter @InfoAnfield

Monday, February 11, 13