You May Be Compliant But Are You Secure?

Scott Neifert, Manager CISS CIP Security & Compliance, Exelon
Richard Jones, VP of Grid Security, BRIDGE Energy Group

January 14, 2016

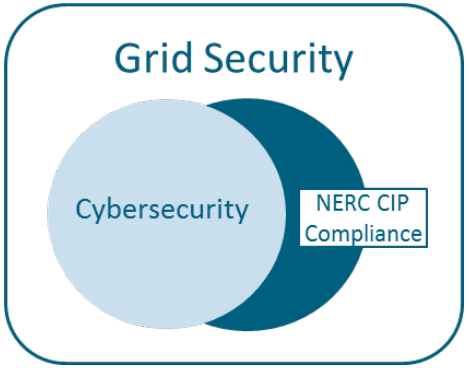
Agenda

1. Introductions – 5 Minutes - Moderator
2. Exelon Security and Compliance – 10 Minutes Scott
3. Exelon Focus on Cybersecurity for NERC Compliance – 15 Minutes Scott
4. Cybersecurity Fundamentals – 5 Minutes Richard
5. Cybersecurity & Compliance Health Check – 5 Minutes Richard
6. Final Thoughts – 10 Minutes Scott then Richard Final Slide
7. Questions – 10 Minutes

Introductions

Why This Webinar

- Improve Compliance and Security Posture
  - Enhancing Elements of Your Grid Security Program
  - Mitigating Vulnerabilities and Risks to Your Protected Stuff
  - Improving Your Compliance Measures and Actions
- Concern That the US is One Breach Away



Forbes / Security

JAN 4, 2016 @ 12:15 PM 7,766 VIEWS

Ukraine Claims Hackers Caused Christmas Power Outage

Exelon Security and Compliance

Scope of Service

Exelon Corporation

- Holding company for 4 NERC CIP Jurisdictional Transmission and Generation Entities
  - PECO, BG&E, ComEd and Exelon Generation
- NERC CIP Assets in 2 Regions MPCC and RF
- More than 4000 v5 NERC CIP Assets

Impacted Systems and Networks

SITUATION:

- Multiple Utilities with different processes and technologies
  - Different Business and Compliance Profiles
  - Multiple SCADA Vendors
  - IED Vendors of all genres and forms

Exelon Solution

Exelon IT/OT Working Definitions

- **IT Cyber Assets:** Control Center Cyber Assets that exist in CIP Control Centers or are Cyber Assets that support Control Center assets.
- **OT Cyber Assets**: Cyber Assets that exist in the substations and are supported by the reliability organizations.

Exelon Focus

Cybersecurity for NERC Compliance

Exelon Diligence - Focus

- Exelon reviewed several frameworks for focusing their efforts around cybersecurity and compliance requirements
  - NIST: Framework for Improving Critical Infrastructure Cybersecurity (EO 16636)
    - Voluntary framework to supplement existing risk management and cybersecurity capabilities
  - DOE: ES-C2M2- Maturity Model, Evaluation Tool and DOE facilitated self-evaluations
  - NERC CIP Guidance and Technical Basis
- Determined that the best focus would be the use of the NERC CIP Guidance and Technical Basis as they focus on each requirement and provide guidance on the Mandated not Voluntary Requirements

Example: Systems Security Management

R4.2 NERC Guidance and Technical Basis – Consider the Following Alert Types

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts of a policy
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

Exelon NERC Cybersecurity Paradigm

- CIP Version 3
  - Rigid minimalist requirements, meet the requirements as written

- CIP Version 5 Skipped Grades
  - Determine what items are important (risk) and develop a security program around the high risk items.

Utilities Can Do The Right Thing

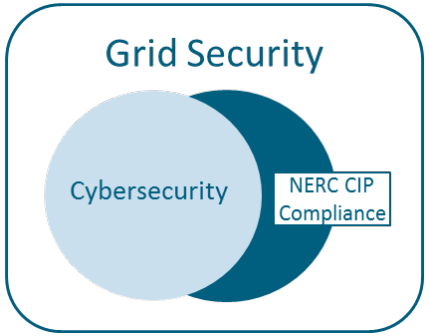
- Golden Opportunity For Utilities To Shine

  ALTHOUGH

  - CIP Standards are bare minimum AND
  - NERC Guideline and Technical Basis Provides Good Guidance
    - This is Not Enough to Secure the Utility
    - Utilities Must Do More

Examples: Doing The Right Things

- Example 1: Successful Authentication
  - Smart view based on the Risk
    - Good on Relays; Bad on Domain Controllers
- Example 2: Active Vulnerability Assessment
  - Step 1: Meet the 3 Year Compliance Requirement
  - Step 2: Automate where feasible and do Yearly



Cybersecurity Fundamentals (BRIDGE)

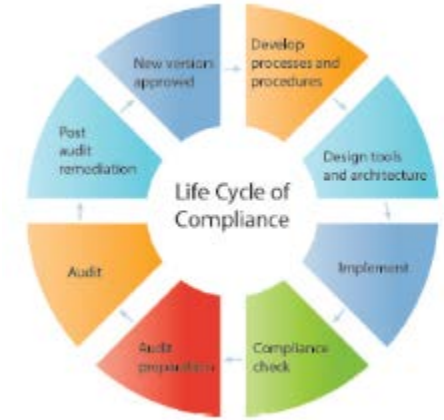
Process and Technology Stack

BRIDGE: Grid Security

Grid Security

- Advise
- Deliver
- Support

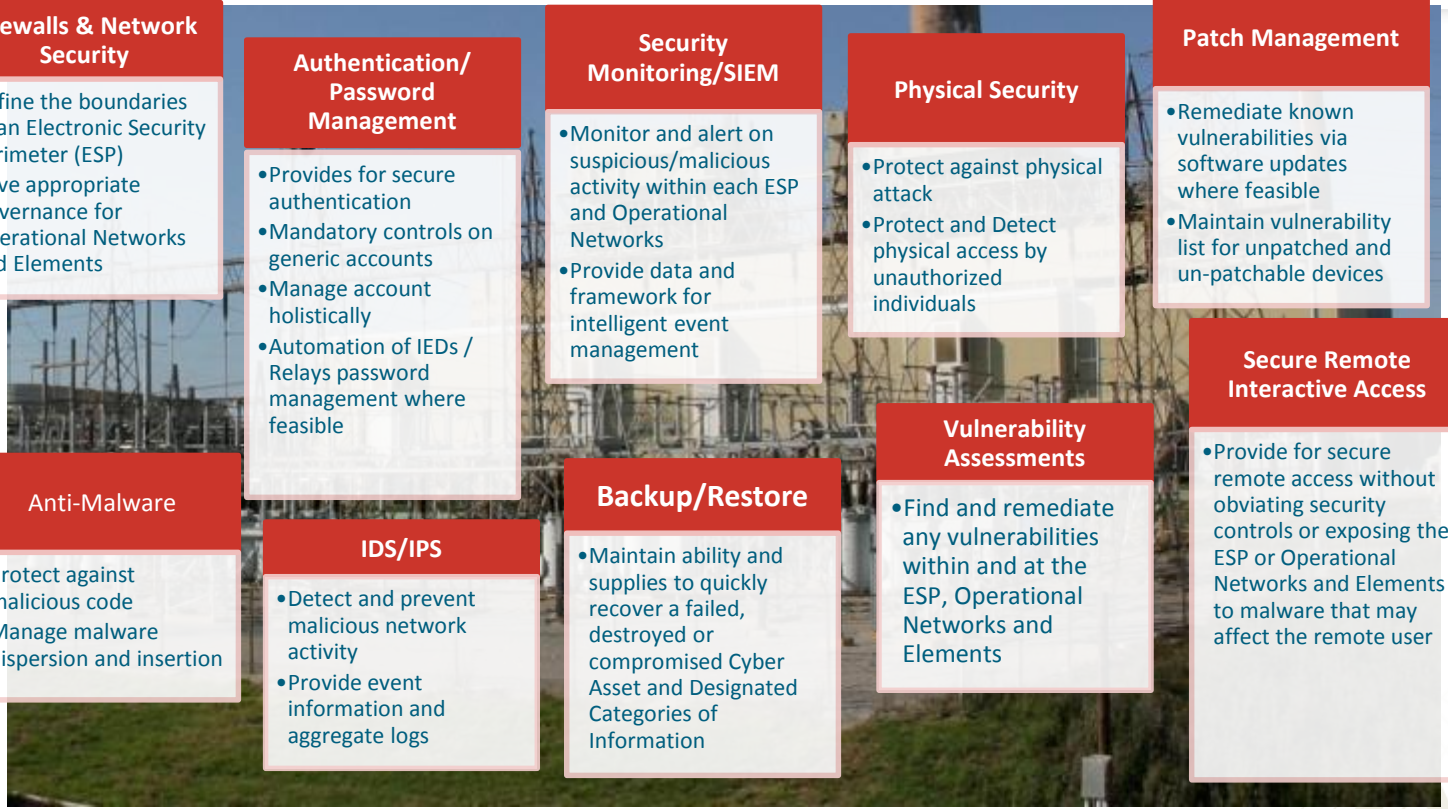
NERC CIP Compliance



Cybersecurity

Governance	Security Operations and Monitoring	Risk and Threat Assessment / Management
Asset and Configuration Management	**Protected Assets**	Capability Monitoring and Self-Assessment
Incident / Event Management	Forensics and Investigations	Risk and Threat Mitigations (Projects)

Technical Controls



Firewalls & Network Security

- Define the boundaries of an Electronic Security Perimeter (ESP)
- Have appropriate Governance for Operational Networks and Elements

Authentication/ Password Management

- Provides for secure authentication
- Mandatory controls on generic accounts
- Manage account holistically
- Automation of IEDs / Relays password management where feasible

Security Monitoring/SIEM

- Monitor and alert on suspicious/malicious activity within each ESP and Operational Networks
- Provide data and framework for intelligent event management

Physical Security

- Protect against physical attack
- Protect and Detect physical access by unauthorized individuals

Patch Management

- Remediate known vulnerabilities via software updates where feasible
- Maintain vulnerability list for unpatched and un-patchable devices

Secure Remote Interactive Access

- Provide for secure remote access without obviating security controls or exposing the ESP or Operational Networks and Elements to malware that may affect the remote user

Anti-Malware

- Protect against malicious code
- Manage malware dispersion and insertion

IDS/IPS

- Detect and prevent malicious network activity
- Provide event information and aggregate logs

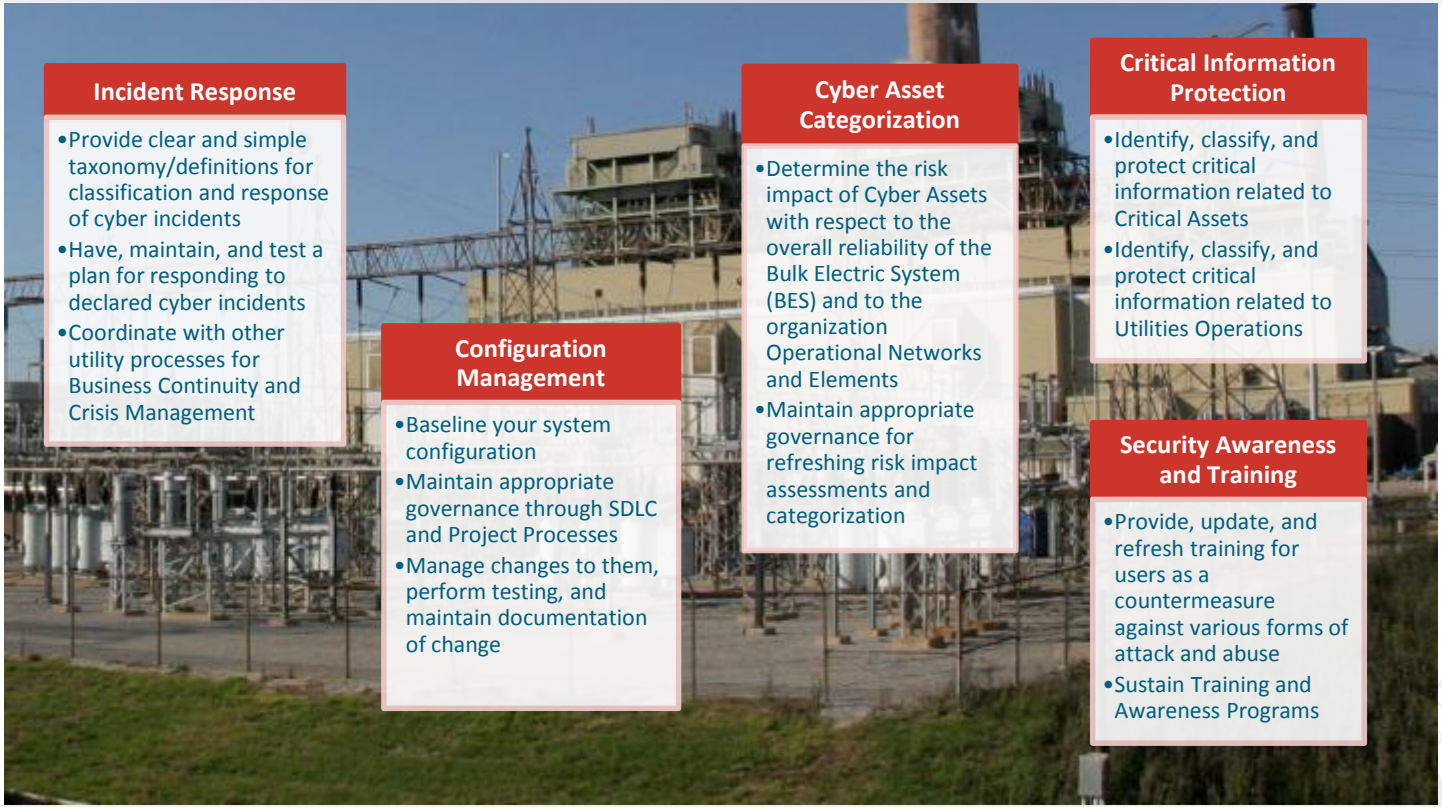
Backup/Restore

- Maintain ability and supplies to quickly recover a failed, destroyed or compromised Cyber Asset and Designated Categories of Information

Vulnerability Assessments

- Find and remediate any vulnerabilities within and at the ESP, Operational Networks and Elements

Procedural Controls



Incident Response

- Provide clear and simple taxonomy/definitions for classification and response of cyber incidents
- Have, maintain, and test a plan for responding to declared cyber incidents
- Coordinate with other utility processes for Business Continuity and Crisis Management

Configuration Management

- Baseline your system configuration
- Maintain appropriate governance through SDLC and Project Processes
- Manage changes to them, perform testing, and maintain documentation of change

Cyber Asset Categorization

- Determine the risk impact of Cyber Assets with respect to the overall reliability of the Bulk Electric System (BES) and to the organization Operational Networks and Elements
- Maintain appropriate governance for refreshing risk impact assessments and categorization

Critical Information Protection

- Identify, classify, and protect critical information related to Critical Assets
- Identify, classify, and protect critical information related to Utilities Operations

Security Awareness and Training

- Provide, update, and refresh training for users as a countermeasure against various forms of attack and abuse
- Sustain Training and Awareness Programs

Cybersecurity and Compliance

Health Check

Health Check

Task 1 — Collect Data

- NERC CIP Version 5 Requirements checklist
- Compliance Cutover Planning
- Operational Process Readiness
- Operations Awareness and Training
- Cybersecurity Tools and Process Stack
- Cybersecurity Posture and Testing

Task 2 — Analyze and Plan

- Review and corroborate compliance findings with key stakeholders
- Review and corroborate cybersecurity findings with key stakeholders
- Review project status with project teams
- Document gaps, issues and concerns
- Develop remediation options

Task 3 — Report

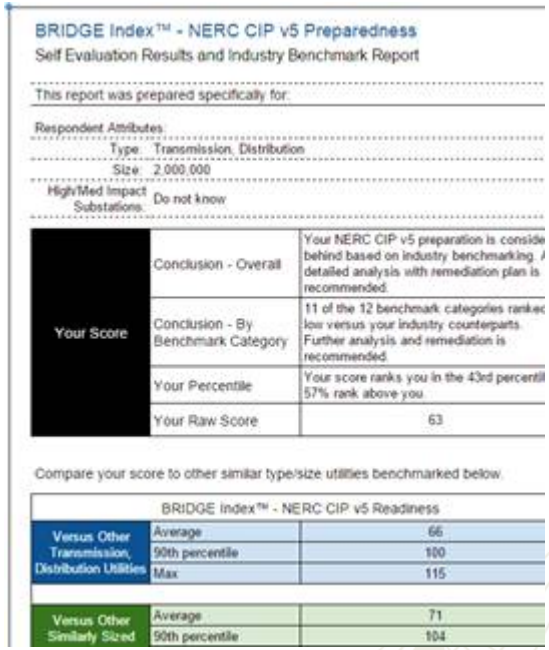
- Present findings to Key Management
- Select Remediation Options
- Finalize Remediation Plan/Report

Final Thoughts

What Have We Forgotten?

Are You Ready for April 1, 2016?

- List of remaining vulnerabilities and mitigation plans for
  - Substation IEDs / relays
    - Patch Management
    - Account Management
    - Ports and Services
  - SCADA, EMS and Other Impacted ICS
  - Are your mitigation plans confirmed with vendor timelines and your operational schedule
    - Will they stand up to scrutiny
- List of work-arounds and fixes that will need to be updated
  - Consideration of re-use / modification for low impact facilities and systems
  - Consideration of delayed technology deployments
- Go-live inventory of substation IEDs and Relays
- Your plans for a Mock-Audit/Health Check or Self-Assessment



BRIDGE Index™ - NERC CIP v5 Preparedness

Self Evaluation Results and Industry Benchmark Report

This report was prepared specifically for:

Respondent Attributes

Type: Transmission, Distribution

Size: 2,000,000

High/Med Impact Substations: Do not know

Your Score	Conclusion - Overall	Your NERC CIP v5 preparation is conside behind based on industry benchmarking. A detailed analysis with remediation plan is recommended
	Conclusion - By Benchmark Category	11 of the 12 benchmark categories ranke low versus your industry counterparts. Further analysis and remediation is recommended
	Your Percentile	Your score ranks you in the 43rd percentil 57% rank above you
	Your Raw Score	63

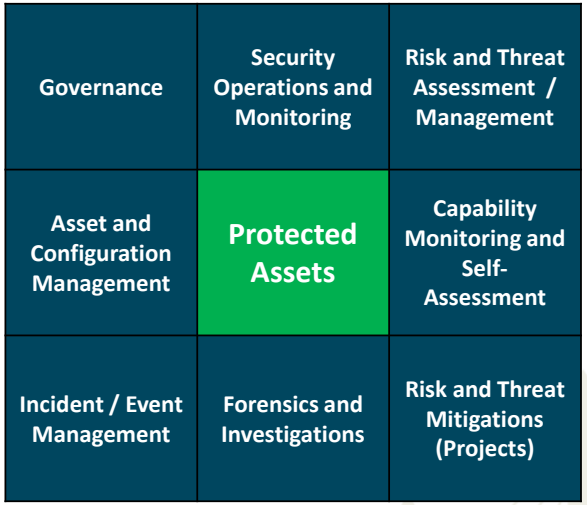
Compare your score to other similar type/size utilities benchmarked below

BRIDGE Index™ - NERC CIP v5 Readiness		
Versus Other Transmission, Distribution Utilities	Average	66
	90th percentile	100
	Max	115
Versus Other Similarly Sized	Average	71
	90th percentile	104

After April 1, 2016

Continue Evolving Compliance Elements into the Cybersecurity Program

- Confirming / evolving solutions and technology stack
- Unwrapping workarounds and temporary fixes
- Continuation of education and training and awareness staff
- Continuous improvement of program focus
- Plans Must Be Solid For Sustaining Compliance
  - 2016 and 2017 Budgets Are Fixed
  - Deployment of security / compliance solutions to Low Facilities by April 2017
  - Understanding NERC CIP Version 6 and 7



Questions

Scott Neifert

Manager CIP Security & Compliance, Exelon

410-470-1898

Richard Jones

Vice President Grid Security

BRIDGE Energy Group

Info@bridgeenergygroup.com

508-281-7133