

# Smart Grid Security

Security Risk Planning

Presented by:  
**DOUG POWELL**  
Thursday, January 19<sup>th</sup>, 2012  
EDIST Conference  
Markham, ON

---

---

---

---

---

---

---

---

## THE "DUMB OLD GRID"

- ▶ What was at risk
- ▶ How was it protected
- ▶ SCADA and Control Systems Issues

Copyright Doug Powell - No Re-use Without Permission

---

---

---

---

---

---

---

---

## "SMART GRID" - A DEFINITION

- ▶ What has changed
- ▶ What is at risk
- ▶ SCADA and Control Systems interfaces

---

---

---

---

---

---

---

---

**SECURING THE NEW GRID  
-MANAGING RIKS-**

**SECURITY-BY-DESIGN:**

Defense in Depth- An expanded definition

1. A multi-layered approach to standards definition
2. A multi-layered approach to assessment and validation
3. A multi-layered approach to security solutions

---

---

---

---

---

---

---

---

**DEFINING STANDARDS  
-GOVERNANCE-**

- ▶ Begin with what we know
  - ISO 2700 Policy Set
  - NERC CIP critical cyber asset protection
  - NISTIR 7628 Framework for Smart Grid Security
  - Now, fill in the blanks
- ▶ Assemble a team of experts
- ▶ Create a Framework Document
- ▶ Establish an Architectural Design Council
- ▶ Provide Security & Privacy Oversight to a central office

---

---

---

---

---

---

---

---

**FRAMEWORK CONTENT  
-COMPLIANCE-**

- ▶ All government regulations and laws, applicable
- ▶ All BCH Policy and Standards Applicable
- ▶ All ISO 27000, NERC CIP and NISTIR 7628 content
- ▶ Additional Standards and Best Practices to complete the Framework
- ▶ Review by company SME's and Responsible Managers
- ▶ Review and Approval by Design Council and Director/VP Level Management
- ▶ Define Smart Grid Architecture according to the Framework
- ▶ AN ONGOING PROCESS OF REVIEW AND REVISION ACROSS SIX RELEASES

---

---

---

---

---

---

---

---

### “SMART GRID” – STANDARDS – COMPLIANCE & REGULATION –

- ▶ A quick word about security standards
  - NERC CIP in the “dumb grid”
  - Clamoring for something new
- ▶ Do regulatory standards work?
- ▶ Self-regulation through comprehensive standards
- ▶ Working groups

---

---

---

---

---

---

---

---

### SECURITY BY DESIGN – RISK MANAGEMENT –

- ▶ FIVE LEVELS OF ASSESSMENT TO VALIDATE THE SOLUTION
  1. Modulo Risk Assessment (GRC)
  2. 3<sup>rd</sup> party Vulnerability Assessment
  3. Security Delivery Team Assessment (Framework)
  4. Privacy Impact Assessments (Provincial Regulation)
  5. 3<sup>rd</sup> Party Ethical Hacking (Penetration Testing)

---

---

---

---

---

---

---

---

### GRC RISK ASSESSMENT – MODULO

**Why Modulo:**

1. We were able to add relevant standards sets for assessment (NISTIR 7628, NERC CIP)
2. Automated process reduced assessment time
3. Question sets were easy to administer for interviews and data collection
4. Question sets were comprehensive, scalable and could be segmented for multiple person responses
5. Results were collated and aggregated according to our criteria
6. Risk rating was according to our criteria
7. Business group owners were identified and managed within the software
8. Prioritization and reporting was automated according to our criteria and standards
9. Executive level reporting was easily extracted
10. Management level reporting was comprehensive but not overwhelming and was configurable to the type of report we wanted
11. Modulo became a defects tracking and management system that allows subsequent assessments to be layered on to previous assessment data for ongoing, cumulative tracking
12. Treatment is managed from the application
13. Modulo can be used as a repository for other assessments we run such as vulnerability scans, penetration testing, etc.

---

---

---

---

---

---

---

---

**RISK ASSESSMENT HIGHLIGHTS**  
Security & Privacy planning requires effective standards  
↓  
Applying standards effectively requires effective assessment and validation work  
↓  
Risk Assessment is the foundation of all security planning  
↓  
Risk treatment requires expert application

---

---

---

---

---

---

---

---

**IN SUMMARY**

3 Starting Points:

1. Those who do not assess risk comprehensively are creating risk.
2. Smart Grid is a complex machine. Smart Grid security needs to address that complexity through:
  - A comprehensive Risk Management Approach
  - A multi-layered solution set
  - Defense In Depth
3. GRC risk management is extremely important to Smart Grid
  - IT Governance across the utility is not only necessary, it is extremely critical to the sustainment of Smart Grid security
  - Enterprise IT Risk Management is not a one time thing!
  - Compliance to your own Standards Framework is a much healthier approach than complying with Regulation

---

---

---

---

---

---

---

---

**THANK YOU!**

**QUESTIONS?**

Doug Powell  
Manager, Security, Privacy & Safety (SM)  
BC Hydro

doug.powell@bchydro.com  
778-452-6676

---

---

---

---

---

---

---

---