LESSONS LEARNED IN SMART GRID CYBER SECURITY

Lynda McGhie CISSP, CISM, CGEIT
Quanta Technology
Executive Advisor Smart Grid Cyber Security and Critical Infrastructure Protection
lmcghie@quanta-technology.com

QUANTA TECHNOLOGY

Agenda

- Smart Grid Cyber Security Challenges
- IT OT Traditional Integration Challenges
- More Interconnectivity, Distribution and Access Points
- Cyber Security Vs. Compliance
- Smart Grid Vendor Management Challenges
- Software Assurance
- Other Observations
- Positive directions - things are changing

QUANTA TECHNOLOGY

Smart Grid Cyber Security Issues and Challenges

- System complexity is growing through expanding interconnectivity of systems and the extension of the electronic perimeter to new grid components and participants
  - Increasingly distributed assets (AMI, HAN)
- Lots of legacy investments that need to be secured along side newer, unproven technologies
  - Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures
- Operations and control networks previously thought to be inherently protected through private networks, serial connections and proprietary protocols are increasingly more vulnerable as networks are connected

QUANTA TECHNOLOGY

Smart Grid Cyber Security Issues and Challenges

- SCADA vulnerabilities and malware (Vendor access, USBs, disgruntled employees)
- Aurora Project proves that control networks can be penetrated
- Cyber threats are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures
- Threat, vulnerability, incidents and mitigation information sharing is insufficient among government and industry

QUANTA TECHNOLOGY

Smart Grid Cyber Security Issues and Challenges

- Increasing concern for privacy issues
- Weak business case for cyber security investment by industry
- Regulatory uncertainty in energy sector cyber security
- DOE SGIG investments
  - Provided a boost to cyber security awareness and enhancement, but what is next?
- Business drivers to change traditional IT / OT boundaries

QUANTA TECHNOLOGY

IT OT Integration Challenges

- Typically do not work together
- OT views the corporate network as vulnerable and resources inadequate
- OT networks and systems have different performance and reliability requirements
- Differing security architectures and risk management goals
- OT legacy systems challenging to support, upgrade and integrate
- Multiple support systems that do not integrate or interoperate – change management, ticketing , tracking and reporting, configuration management, patch management, audit and monitoring

QUANTA TECHNOLOGY

New Technology Challenges Traditional Approaches

- More Interconnectivity, distribution and access points
- Mobile devices
- Wireless network security
- Encryption and authentication
- Distributed key management
  - Need a secure network for key management
- Integrated and active monitoring

QUANTA TECHNOLOGY

Cyber Security Vs. Compliance

- Culture of compliance, culture of security – Compatible goals?
- Many utilities didn't have a centralized security function prior to NERC CIP
  - Security modeled after NERC CIP – Process not technology oriented
- Risk management and security governance programs are not in place
- Getting management's attention and building the business case for cyber security after NERC CIP

QUANTA TECHNOLOGY

Smart Grid Vendor Management Challenges

- Without skilled resources, many utilities rely on vendors to configure device security
  - Vendors do not know utilities cyber security requirements and do not configure to implement a defined policy or integrated architecture
  - No linkage from vendor to vendor – Defense in depth?
- Vendors ship products with little or no security turned on by default
- Rush to bring products to market without testing to ensure that they actually work as advertised or integrate
- Utilities typically don't have test environments and rely on vendors to test
- Technology and standards continue to evolve
- Vendors won't share system certifications or provide proof of testing

QUANTA TECHNOLOGY

Software Assurance

- Secure software development
  - Integrated systems testing
  - Testing code from third-party vendors
  - Code testing
- Vendor mergers and use of third-parties
  - Built in backdoors for troubleshooting
- Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations

QUANTA TECHNOLOGY

Other Smart Grid Deployment Observations

- Smart grids inherent goal to provide consumers with more information to make informed decisions regarding energy consumption
  - But what about concerns for the protection and sharing of usage information and privacy information?
- Loss of traditional physical security perimeters with more distributed assets requiring physical and logical security to work together
- Aging infrastructure – many legacy smart grid assets are not being upgraded or patched
- Outsourced hardware and software support – many partners
- Anti-virus problem still not solved – integrated solutions and management
- Current cyber security skill set and ability to recruit
- Incident Management continues to evolve and integrate

QUANTA TECHNOLOGY

Positive Directions – Things are Changing

- Beginning to see a risk management Vs. pure compliance approach to security within the utilities
- Government, vendors, research and universities and utilities are working together
- Practical, business-oriented metrics and measurement mechanisms are being developed and used
  - Increased visibility and understanding of current state and challenges, and to facilitate prioritization
- Beginning to describe security requirements and incidents in language more accessible to management and more aligned with core utility values and business drivers, including safety and reliability
- More attention to Operational-side issues

QUANTA TECHNOLOGY