PSEG Nuclear Cyber Security Supply Chain Guidance

Developed by:

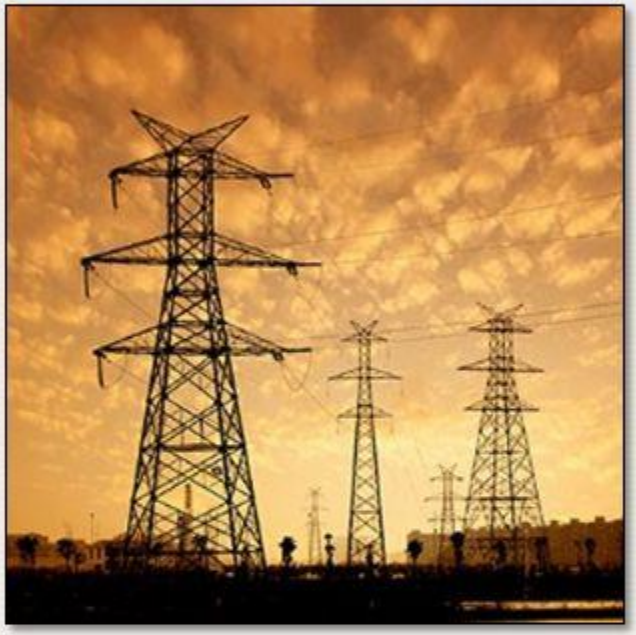
Jim Shank – PSEG Site IT Manager & Cyber Security Program Manager

Presented at Rapid 2018 by:

Bob Tilton- Director Procurement PSEG Power

PSEG Nuclear LLC

Targeted Attack – Ukraine Power Grid



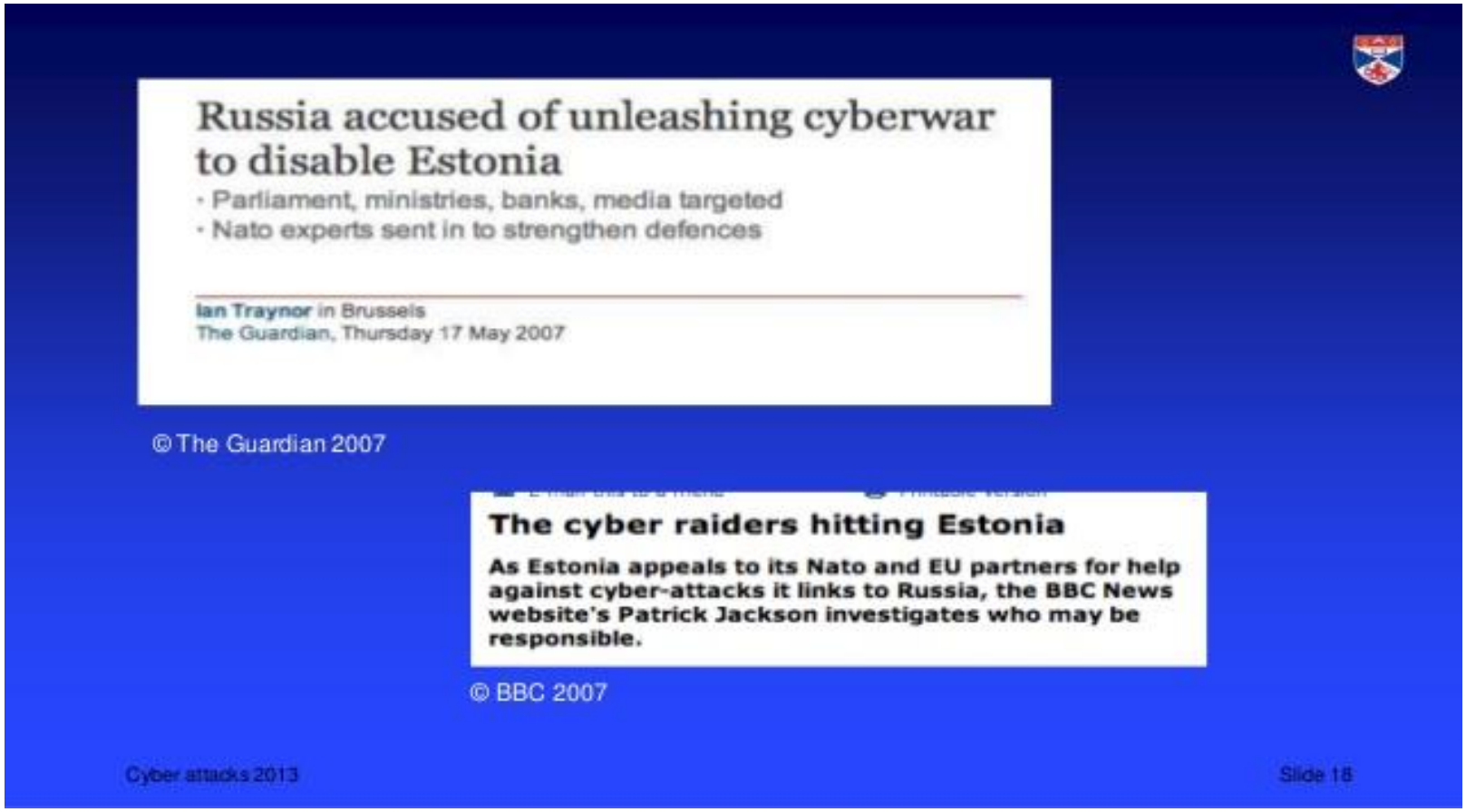
Cyber-Attack Against Ukrainian Critical Infrastructure

December 23, 2015 – Ukraine

Cyber Attack causes power outages at 3 regional electric power distribution companies (Oblenergos) impacting approximately 225,000.

- Coordinated attack (30 minutes attack window)
- malicious remote operation of the breakers (not malware)
- Call centres hit with denial of service attack
- Selected deletion of computer files on affected machines
- BlackEnergy malware identified on the machines
- Initial infection through spear phishing emails with malicious Microsoft Office attachments.

IAEA


Russia accused of unleashing cyberwar to disable Estonia
· Parliament, ministries, banks, media targeted
· Nato experts sent in to strengthen defences
Ian Traynor in Brussels
The Guardian, Thursday 17 May 2007
© The Guardian 2007
The cyber raiders hitting Estonia
As Estonia appeals to its Nato and EU partners for help against cyber-attacks it links to Russia, the BBC News website's Patrick Jackson investigates who may be responsible.
© BBC 2007
Cyber attacks 2013
Slide 18

Goals & Objectives

Goal: Share information regarding how peer Licensees can address the NEI 08-09 Rev. 6 "Cyber Security Plan for Nuclear Power Reactors" Appendix E11 family of System and Services Acquisition cyber security control requirements

Objectives:

- *Share PSEG's implementing model for the Appendix E11 cyber security controls*
- *Identify and define roles and processes*
- *Discuss key concepts and encourage the use of a generic procurement specification for upgrade and replacement projects*
- *Share lessons learned from application of this approach*

Purpose

What problem are we attempting to solve?

The purpose of system and services acquisition controls is to establish and maintain supply chain protections to minimize the introduction of malware and security vulnerabilities associated with the procurement of CDA products and services.

How should we do this?

Develop and implement a standard process that encourages vendor adoption and support for designing required cyber security controls into critical digital assets

PSEG's Internal Cyber Security Supply Chain Integration Model

Information Technology

IT-AA-505 "Cyber Security Control Implementation Strategy

Design Engineering

CC-AA-300-1002, "Procurement Classifications Guidelines"

Supply Chain Procurement

SM-AA-404-1000, "Nuclear Procurement of Materials and Services"

PSEG Nuclear LLC

Information Technology (IT)

Information Technology (IT) has the following roles:

- Owns and manages the PSEG Cyber Security Program
- Identifies Critical Systems and Critical Digital Assets (CDAs)
- IT-AA-505 “Cyber Security Control Implementation Strategy” documents how PSEG is addressing the Appendix E11 Supply Chain cyber security controls
- Collaborates with Engineering to define the cyber security scope for digital plant modifications
- Collaborates with Procurement to identify cyber security requirements that need to be included in Purchase Orders

Design Engineering

Design Engineering has the following roles:

- Supports Cyber Security Program compliance
- Assists with identifying critical digital assets (CDAs) in SAP equipment database
- CC-AA-300-1002, “Procurement Classifications Guidelines” documents need to identify cyber security requirements for assets classified as CDAs
- Collaborates with IT to implement cyber security scope into design change packages for digital plant modifications
- Collaborates with Procurement to ensure cyber security requirements for plant modification are included in Purchase Orders

Procurement Engineering

Procurement Engineering has the following roles:

- Supports Cyber Security Program compliance
- Ensures procurement requirements are invoked and referenced in PO for items identified as critical digital assets (CDAs)
- SM-AA-400-1001, "Procurement Classifications Guidelines" establishes vendor requirement to deliver products free from known malware and compliant with applicable cyber security control requirements
- Collaborates with IT and/or Engineering to address vendor comments/feedback regarding applicable cyber security control requirements

NEI 08-09 R6 App E11 New Supply Chain Term

Trusted Distribution Paths (an NEI 08-09 R6 term):

- **Defined in SM-AA-400-1001 as a Supplier that certifies their CDA goods and services comply with applicable PSEG cyber security specification requirements and that delivered products are free of known security flaws and malicious content (malware)**
- **The intent here is to ensure the integrity of the Suppliers and the materials delivered through the Supply Chain; there are many methods and tools available to do this**
  - Vendor validation and audit practices
  - Secure design and development practices
  - Tamper packaging/protections

NEI 08-09 R6 App E11 Recommendation

PSEG Nuclear generic purchase specification H-5-SEC-KGS-0217, "Digital Technology Systems Critical Digital Asset Cyber Security Specification"

- **Identifies NEI 08-09 R6 cyber security control requirements applicable to devices classified as CDAs**
- **Requirements can be tailored based upon device capability and functionality**
- **Factory and site acceptance testing to ensure security proper device performance when required**
- **Several commercial Nuclear Suppliers have seen and provided feedback on the PSEG cyber security specification for CDA procurement activities**

Lessons Learned – Hope Creek (HC) PRNM Project

Power Range Neutron Monitoring (PRNM) System Replacement

- PRNM is part of the HC safety-related Neutron Monitoring plant system
- Project replaces existing analog PRNM hardware with GE digital NUMAC hardware and application software
- NUMAC hardware was classified as NEI 13-10 direct-impact, Class B.2 CDA
- GE was provided Rev. 0 of the PSEG Cyber Security specification and provided a detailed response for each security control
- This exchange allowed the Licensee to collaborate with GNF to identify how best to address each security control requirement.

Lessons Learned – Salem BEACON Project

Best Estimate Analysis of Core Operations Nuclear (BEACON) System Replacement

- BEACON is part of the Salem Important-to-Safety Plant Computer system
- Project replaces existing BEACON workstations with Westinghouse's new hardware and application software
- BEACON hardware classified as NEI 13-10 indirect-impact computer system
- Westinghouse (WEC) was provided requirements consistent with Rev. 1 of the PSEG Cyber Security specification which required addressing the NI 08-09 R6 D1.4, D1.17 and D1.19 security controls
- WEC has agreed to modify their proposed solution to implement a white-listing software product on their qualified BEACON platform.

Summary & Conclusion

Licensees are required to address the NEI 08-09 R6 Appendix E11 cyber security controls. PSEG is addressing the Appendix E11 cyber security controls via the following:

1. IT/Engineering/Procurement process integration that focuses on identifying CDA procurement activities.

2. Ensuring CDA procurements invoke applicable cyber security control requirements in the PO. The use of a generic Cyber Security Specification that documents applicable Supplier cyber security control requirements for the procurement of CDA products and services is recommended.

When properly invoked and complied with these steps provide reasonable assurance Supplier-delivered CDA products are free of known security vulnerabilities and malicious code. Licensee calibration, configuration, testing and malware scanning aid to ensure CDA products are malware-free before being placed into service.

Questions

APPENDIX

NEI 08-09 Supply Chain Requirements

- **SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**

This security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates:

A formal, documented, system and services acquisition policy that addresses the following:

- The purpose of the security program as it relates to protecting the organization's personnel and assets;
- The scope of the security program as it applies to the organizational staff and third-party contractors;
- The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments.

A formal, documented procedure to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

- **SUPPLY CHAIN PROTECTION**

This security control protects against supply chain threats by employing the following measures to protect against supply chain threats and to maintain the integrity of the CDAs that are acquired:

- Establishment of trusted distribution paths,
- Validation of vendors, and
- Requirement of tamper proof products or tamper evident seals on acquired products.

- **TRUSTWORTHINESS**

This security control requires that CDAs meet defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

NEI 08-09 Supply Chain Requirements

- **INTEGRATION OF SECURITY CAPABILITIES**

This security control documents and implements a program to ensure that new acquisitions incorporate security controls based on the following:

- Being cognizant of evolving cyber security threats and vulnerabilities;
- Being cognizant of advancements in cyber security protective strategies and security controls; and
- Conducting analyses of the effects advancements could have on the security, safety and operation of the nuclear critical assets, systems, CDAs and networks at their facility.

- **DEVELOPER SECURITY TESTING**

This security control requires system developers/integrators of acquired CDAs create a security test and evaluation plan, implement the plan, and document the results such that:

- The products are delivered to meet specified security requirements, and
- The delivered product is free from known testable vulnerabilities and known malicious code.
- This security control also requires the plan and results be reviewed and approved by the licensee.

- **LICENSEE TESTING**

This security control:

- Requires testing (e.g., off-line on a comparable CDA) of security devices and software to ensure that they do not compromise the CDA or interconnected CDAs operation prior to installation, and
- Deploys security controls and flaw remediation measures based on reliable and credible sources of risk information.
-
- This security control also requires audits of CDAs, to provide high level of assurance that the safety, security, and emergency preparedness function are protected from a cyber attack to validate the following items:
- Security controls present during system validation testing are still installed and operating in the production system,
- CDAs are free from known security compromises and continue to provide information on the nature and extent of compromises should they occur, and
- Management of change program is being followed with an audit trail of reviews and approvals for changes.

PSEG Procurememnt Specification Example

PSEG Requirements (doc # S-4-CN-CDS-0507, rev 0)		Compliance for ADFWCS	
NEI Control #	Requirement	Code	Westinghouse ADFWCS Cyber Security Response
	5.1 Overview		
	5.1.2 Vendors shall provide documentation detailing how their product addresses each requirement of this specification. References to vendor manual numbers and page numbers should be provided.	CL	References to applicable vendor documents will be provided in some instances, due to the fact that the majority of these are system configuration items they will not be listed in the manual.
	5.1.3 The Company must approve all exceptions to this specification.	N/A	
	5.1.4 In situations where the vendor is unable to apply/implement the security controls as defined and documented in this specification, the vendor may use alternative controls and document the justification for the use of alternative controls or countermeasures that include any of the following: - A design that aids with physically restricting access to the CDA - A design that provides monitoring and recording physical access to the CDA to detect and respond to intrusions in a timely manner	CL	WEC has identified the following controls that will use the physical Alternative Controls listed. 5.4.18.3, 5.5.4.1, 5.5.4.2
	5.1.5 Vendors are required to provide with their bid details regarding the use of any alternate controls and any exceptions to the requirements of this specification.	I	N/A
	5.2 Account Management		
	5.2.1 Account Management		
D.1.2C	5.2.1.1 The vendor shall design devices with end-user configurable accounts that can be tailored to assigned job functions within defined system functionality.	C	Ovation implements domain-based role-based access for the Windows drops using Active Directory. Ovation Security Manager provides a front end to manage users, computers, and group policy objects. User roles include administrator, operator, and engineer at a minimum. Access to privileged functions and applications in the operating system and Ovation is defined by these roles.
D.1.2E	5.2.1.2 The vendor shall employ automated mechanisms to support device account management functions and enable the device to automatically: - Terminate temporary, guest, and emergency accounts based on an administrator defined frequency - Disable inactive accounts based on an administrator defined frequency - Create and protect audit records for account creation, deletion, and modification - Document and notify system administrators of all account creation, deletion, and modification activities so that system administrators are aware of any account modifications and can investigate potential cyber attacks in a timely manner	C	Ovation implements domain-level role-based user access through Active Directory and Ovation Security Manager. Ovation Security Manager is used to terminate or disable applicable accounts. Active Directory will also be configured to audit user account activity as required. This activity is logged in the Windows Event Log of the Domain Controller. COMPANY will provide the SIEM and Westinghouse will ensure that the ADFCS and other OSC components delivered with this project will be able to connect to the COMPANY provided SIEM. Westinghouse CS Services for configuring the SIEM for the ADFCS are outside the scope of this Contract.
	5.2.2 Access Enforcement		
D.1.3B	5.2.2.1 The vendor design shall support assigning user rights and privileges within defined system functionality and user authorization.	C	Ovation uses Domain based user access. These controls will be implemented at the domain level.