Business Services

TMI

LaSalle

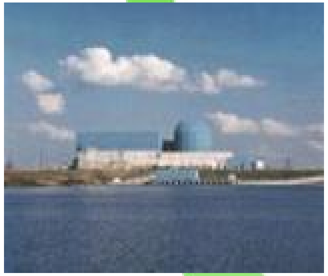
Oyster Creek

Balancing security, business requirements and company IT standards for PPC systems

Presented by:
Kevin Rumbaugh
Lead Analyst IT
Exelon

1/2009

Dresden



Clinton

Quad Cities

Outline

- ✓ Introduction
- ✓ Internal IT review of PPC system
- ✓ Actions from IT review of PPC system
- ✓ Best practices
- ✓ NEI-04-04 Cyber Security

Introduction to Exelon R*TIME use

- ✓ R*TIME PPCs in use or being implemented for use at 9 of 17 Exelon reactor units
- ✓ Installations at four more units currently under consideration
- ✓ PMAX to be installed at all 10 nuclear sites (17 units)
- ✓ Mix of Windows and UNIX based PPC servers
- ✓ Operator display stations are Windows based

Audit of Dresden PPC system

- ✓ Exelon IT internal audit of Dresden PPC system for compliance with IT process/procedures conducted in 2007
- ✓ Audit was not initiated by an event, but the system was just chosen for review
- ✓ System had been installed focusing on Nuclear procedures/processes not IT procedures
- ✓ IT procedures/processes generally center more on business use systems not plant equipment
- ✓ This was NOT an NEI-04-04 cyber security audit
- ✓ Did not look extensive at network boundaries or connections, focused mainly on the computer system vulnerabilities and compliance to IT standards
- ✓ System was reviewed in regards to disaster recovery, operating security, and application security, for example.

IT Audit findings

- ✓ Unneeded services running on systems, that might pose a risk, but whose removal would have no negative affect
- ✓ No automatic password aging
- ✓ Disaster recovery plan not updated
- ✓ No use of ‘secondary’ location for disaster recovery
- ✓ ‘Least access’ privilege not implemented
- ✓ Accessing systems using ‘clear text’ protocols
- ✓ Guest logins remaining on some systems
- ✓ OS Audit policies not enabled
- ✓ Standard system account names still in use
- ✓ Systems not auto locking to screen savers with password protection

IT response to audit findings

- ✓ Reviewed recommended changes with Scientech
- ✓ Generated exception approval documentation for changes not implemented because the R*TIME system required them
- ✓ Tested changes on lab systems before implementation on the production system
- ✓ For password management decided on a manual/process approach instead of forcing changes that might end up locking out someone that needs access
- ✓ Took exception to requiring systems in the control room to auto screen lock
- ✓ Implemented system to allow PCs that are part of the PPC network to be able to run and update their anti-virus signature files
- ✓ Not practical to have a secondary location for the redundant PPC to better satisfy disaster recovery desires

IT actions for Dresden system

- ✓ Had to plan for implementing changes to production system since system was already installed and operating at the plant
- ✓ Implemented changes on the Dresden simulator PPC system
- ✓ Worked with site personnel to schedule and implement changes onto each plant unit’s PPC system
- ✓ Performed basic functionality testing on the system after changes were implemented
- ✓ Monitored system to ensure no adverse affects were found
- ✓ Not desirable to make these changes to a production system, but there was no choice

IT actions for Clinton system

- ✓ By the time the action plan for Dresden had been developed, the Clinton PPC system was just about to start FAT testing
- ✓ Decided to wait until after FAT, but before SAT to implement audit finding changes on Clinton system
- ✓ Changes implemented after equipment was onsite at Clinton and staged for installation
- ✓ System monitored for adverse affects
- ✓ SAT testing was performed on the system
- ✓ Most changes were implemented between FAT and SAT, some were not completed until during SAT due to scheduling issues
- ✓ Better time to make the changes, but not the best time

IT actions for Quad system

- ✓ Exelon real-time IT implemented majority of changes to systems while still staged in Idaho Falls
- ✓ Changes were implemented well before FAT and before much of the development work on site specific apps was done
- ✓ System was FAT tested with most changes in place
- ✓ A few changes were identified as items that would be done on site at Quad Cities before SAT testing
- ✓ Much better way to make these kinds of changes, i.e. before FAT testing
- ✓ Will be implementing anti-virus scanning for all PCs that make up the PPC system

Anti Virus configuration

- ✓ We were able to tap into the existing company standard anti-virus infrastructure to reduce costs and overall support needed
- ✓ Configured ‘parent anti-virus’ servers behind the PPC firewalls that can update from the corporate infrastructure
- ✓ Corporate IT built an ‘install package’ that we can then use on PCs in the PPC network that installs and configures the client on each PC
- ✓ We allow the PCs to automatically update the anti-virus signature files
- ✓ Scans run weekly in the middle of the night and have not had reports of affects on the usability of the PCs because of the scans, but would be cautious of doing so on ‘older’ PCs due to system load

Experiences/Best Practices

- ✓ Keep in mind any company specific IT related processes that you might be held to, not just nuclear processes and identify them early on
- ✓ Perform a more comprehensive review and engagement with corporate IT governance early in the project
- ✓ Discuss with Scientech any IT specific changes that may be required to the system and plan for them from the project start
- ✓ Implement the changes before FAT testing so that the consequences of any of the changes would be found and less likely to cause any production issues
- ✓ Consider the business impact of a change, document the risk and have the nuclear business unit accept that risk if the change would adversely affect the use of the system
- ✓ Implement changes on lab systems before production systems

NEI-04-04 Cyber Security

- ✓ Implementing Exelon Nuclear NEI-04-04 Cyber security program currently
- ✓ Very focused on the ‘boundaries’ between networks and what crosses those boundaries
- ✓ We had previously connected several Level 4 (i.e. control systems to R*TIME PPCs to aggregate data into the PPCs) and those connections will require cyber security remediation
- ✓ R*TIME systems single TCP port access for R*TIME data viewer ‘good’ from a security standpoint
- ✓ Going to require changes to remote administration of the systems
- ✓ Not able to go into too many details

Questions

- ✓ Questions ????
- ✓ Contact information
  - Kevin Rumbaugh
  - Kevin.rumbaugh@exeloncorp.com
  - **630-657-4748**