**CYBER BREAKOUT**

20 were in attendance

1. Procedure versus EC – Maintenance Procedure to allow patches, version updates, graphic displays. (Duke). Bounding Technical Requirements. What is the entry point WO versus other (e.g IT Techs service ticket).
2. Efficiencies – Configuration Settings, 2 processes Design/Cyber. INPO Database – inconsistencies but attempting to correct. There are other COTS software to trend network performance. SQA documents in your Document Management System as Controlled Documents and the introduction of Digital Master Data Sheets (DMDSs).
3. Challenges – Roles and Responsibilities. IT or I&C or Design Engineering who owns it? Ultimately Design Engineering is the design authority. Emergent digital issues that may arise off hours, the Plant General Manager (PGM) makes the call in an emergency and follow-up with documentation within 24 hours. Cyber Security restraints on WO/EC that would flag when you would need a cyber review or oversight during the implementation. CGS sends deliberate email notifications
4. Tie to the Equipment Data Base (EDB) – What level of software (business versus plant).Include equipment tags for software and the identification of the operating system? Version control, Critical Digital Asset, Vulnerabilities. Compatibility.
5. Patch Management – See 1 above.
6. Roles and Responsibilities – Org Chart, where they sit versus report too. Division of Responsibilities (DOR), create a template. Dedicated cyber role. Who has authority of the plan (Design Engineering does). Expand the team to be successful.
7. EC Lessons learned – Don’t order equipment without a digital review. Use of your cyber tools. Create a design spec to bound margin on power, heat load and weight, location restrictions (e.g. sensitive equipment)
8. Wireless and Monitoring – Build an infrastructure. Consider having a vendor perform an Electro Magnetic Capability (EMC) study in the plant to determine acceptable locations. On-going monitoring such as; Automated fire watch, use of cameras, robotics in hi-rad areas to monitor steam leaks, drones (CGS used a drone to video reactor building siding where it was discovered loose hardware was causing degradation of the siding). Business network versus plant network. Use of scalable devices for hardware and software expansion to support increasing workloads on the network and PCs.
9. Technical Assessment Method (TAM) – Industry initiative that provides a consistent process, efficiencies on changing out equipment.

07/30/19 morning news - 100 million Capital One customer data stolen (13 years worth), SSNs, credit reports – Seattle woman arrested yesterday. She’s a former Amazon software engineer employee. Misconfigured Firewall breach.