CHALLENGES FACING INDUSTRIAL INFRASTRUCTURE

Skills Gap
- Dearth of qualified personnel
- Achieving productivity goals
- Lack of staffing to expand operations

Vulnerability
- Security is an After Thought
- Aging Industrial Control Systems and Protocols
- Lack of proper policies and procedures
- Evolving Industrial Security Standards

Inflexibility
- Low Adoption of Risk Management Processes
- Shadow/Stealth IT
- Lack of tools to manage Infrastructure
- Too Much Data, Lack of Actionable Information

IT/OT Convergence
- Lack of comprehensive Asset Inventory
- Integration of new technologies
- Integrate: customer demand, supply chain and industrial processes
Industrial Security Trends
Established Industrial Security Standards

- International Electrotechnical Commission
  - IEC-62443 (Formerly ISA-99), Industrial Automation and Control Systems (IACS) Security
  - Zones and Conduits
    - Defense-in-Depth
    - Segmentation, IDMZ

- National Institute of Standards and Technology
  - NIST 800-82, Industrial Control System (ICS) Security
  - Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover
    - Defense-in-Depth
    - Segmentation, IDMZ

- Department of Homeland Security / The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - Recommended Practices, Secure Network Architecture
    - Defense-in-Depth
    - Segmentation, IDMZ

- Department of Homeland Security / Idaho National Lab
  - DHS INL/EXT-06-11478
    - Defense-in-Depth
    - Segmentation, IDMZ
Reference Architectures
Converged Plantwide Ethernet (CPwE)

- Tested, validated and documented Reference Architectures
  - Tested for performance, availability, repeatability, scalability and security
  - Comprised of a collection of Cisco and Rockwell Automation Validated Designs
- Built on technology and industry standards
  - “Future-ready” network design
- Content relevant to both OT and IT Engineers
  - OT – Operational Technology
    - Industrial Control Systems
- Deliverables
  - Tested and Validated Reference Architectures
    - Deploy Firewalls Within a CPwE Architecture – Dec. 31, 2016
  - Industrial Network and Security Whitepapers
A HOLISTIC APPROACH TO INDUSTRIAL INFRASTRUCTURE SECURITY

**BEFORE**
- Identify & Protect
  - Asset Inventory Services
  - Qualified Patch Management Services
  - Vuln / Risk Assessments And Program Development
  - ICS Security Zone and Mitigation Deployment

**DURING**
- Detect
  - Real-Time Threat Detection Services
  - Remote Monitoring and Administration Services

**AFTER**
- Respond & Recover
  - Backup and Recovery Solutions
  - Incident Handling and Response
  - Incident Response and Disaster Recovery Planning Services

BUILD A SECURE, ROBUST, FUTURE-READY NETWORK FOR YOUR CONNECTED ENTERPRISE

ACCELERATE IMPLEMENTATION AND REMOVE ONGOING SUPPORT BURDEN

Improve Asset Utilization with Remote Monitoring and Administration or Pre-Engineered Infrastructure
Building a Roadmap
Directions to your Digital Transformation

“A roadmap is the governing document that dictates specifically how technology will support the business strategy and help drive businesses priorities over the next 3-5 years”

A roadmap addresses the traditional approach of providing point solutions that create pockets of value that tend to resist integration with the neighboring value-chain functions.

Roadmap Characteristics

- Defines Strategy with a list of business priorities
- Defines OT/IT Goals with a potential timeline
- Has executive level support and buy-in
- Has Consensus in the business
- Has Actionable Projects with owners, value, cost, and payback

Source: CIO 2015