Cybersecurity Engineering for Rail

June 12, 2017

Justin K. Smith, CISSP

Rockwell Collins

Building trust every day

Common Trends

Three of the most painful cybersecurity trends we find in rail.

Cybersecurity Trends in Rail

- Legacy systems. We all have and for some reason, we can't seem to get rid of them.
- Strong enterprise defenses; weak industrial control defenses.
- No holistic approach to cybersecurity. Reactive to events, and limited proactive monitoring.

Legacy Systems

- Limited to no patching
- Insecure implementations
- Reactive maintenance

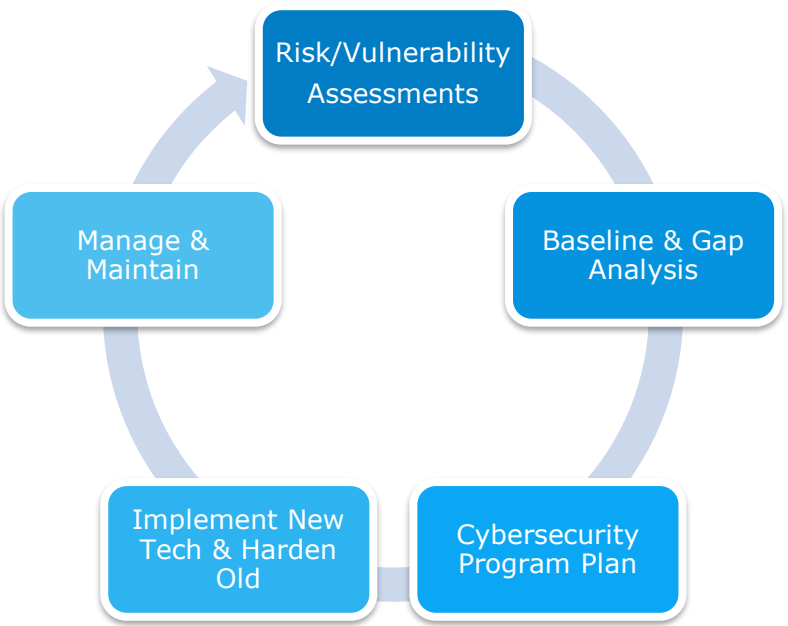
Weak ICS Defenses

- Is it *really* disconnected?
- Direct connections to the internet
- Limited vulnerability management

Cybersecurity Culture

- "We know it's insecure"
- "Security through obscurity"
- "If it's not broken, don't try to fix it"

Cybersecurity Trends in Rail



- There are many challenges facing rail; but they can be solved by strategically assessing your infrastructure.
- With better cooperation between enterprise, operations, engineering and etc. you can rope in your vulnerabilities.
- Independent, third-party assessments are critical.

