B04

Securing industrial systems in a digital world

Erica Barrett
ABB

ABB

Securing industrial systems in a digital world

The threats are real

2014, Germany
Cyber attack causing physical damage to a Steel Mill.

2015, Ukraine
Cyber attack causing large blackouts to the power grid.

2016, Ukraine
Cyber attack causing larger blackouts to the power grid.

2017, Global
A ransomware, WannaCry targeted vulnerabilities in Windows systems.

The challenges are real

Workforce shortages

- ✗ Increased technology changes = new skills & skill combinations.
- ✗ Cost pressures & workforce reductions = things slip through the cracks.
- ✓ **Build collaborative teams with IT and OT staff.**
- ✓ **Look at 3rd party partners (like ABB) to deliver IT/OT expertise through managed service.**
- ✓ **Look to automation for routine security maintenance.**

Lifecycle of older products & systems

- ✗ Older systems weren't designed with cyber security in mind.
- ✗ Older systems have fewer support options and are more challenging and costly to update.
- ✗ Product lifecycles are long, and it may take time to upgrade products or systems.
- ✓ **Complete a risk assessment to evaluate systems, and prioritise remediation.**
- ✓ **Evaluate new systems to ensure they are secure by design and by default.**

Implement real baseline security measures

Identify
A cyber security risk assessment, threat intelligence & modelling can prioritise risk areas.

Protect
Implement security solutions and services ensuring the right security controls are in place.

Detect
Monitor and notify when breaches and vulnerabilities are detected.

Specialists can improve detection and reaction times.

Respond
Ensure you can respond 24hr/7d/365d and have mitigation responses in place to reduce further damage.

Recover
Have proper backup and recovery systems in place and ready to be used.

Comply
Standards and policies protect against fines & allow companies to benchmark to ensure a minimum standard.