BELDEN
SENDING ALL THE RIGHT SIGNALS

The Industrial Cyber Blind Spots

Connectivity and data expose new operational risks to industrial process integrity and human safety. Can we see and quantify these risks to keep our plants operational?

Issue 1:

Sprawl of Network-connected, Data-enabled Equipment

Digitization means connectivity and data. As ever more industrial devices are being connected to networks, data from every device can be transformed into a treasure chest of valuable information to optimize the process. With connectivity, however, comes new concerns. Connectivity opens previously air-gapped or physically isolated control networks to the world of cyberthreats, where potentially damaging impacts to brand reputation, human safety, operational productivity and product quality can occur.

Cyber events impact the bottom line. What does a minute of downtime cost? What would be the financial impact if yields are impacted or a recall has to be issued?

Issue 2:

Incomplete Visibility of Connected Devices on the Plant Floor

Having visibility into your manufacturing environment is the first step toward a cyber-secure environment. How can something be secured if you do not know it exists on the network and how it's communicating?

Would you have the ability to recognize when a cybersecurity event has impacted your operation around product quality or productivity?

Issue 3:

Process Control Integrity and Resilience View

- How do you know if your process is running as intended?
- How do you know if a controller mode just changed?
- How do you know if the recently updated engineering workstation is configured correctly against your own internal build specification or cybersecurity framework?

77% of companies surveyed believe their organization is likely to become the target of a cybersecurity incident involving their industrial control networks.

64% of cybersecurity incidents in 2018 were caused by conventional malware attacks.

Be certain.
Belden.

Manage by Fact, Not Hope

What would it cost if your entire production facility had to be shut down for an hour, a day… or a week? Operational shutdown of the plant for any amount of time is not an option.

Insight 1:

Achieve Complete Visibility from Field I/O to Enterprise IT

There cannot be any surprises, at any level. Vulnerabilities, rogue assets, communication changes, controller mode/configuration changes, firmware updates, asset inventory, and suspicious/malicious behavior—complete visibility must be maintained to meet throughput and quality metrics.

- Translate raw data into actionable information
- Identify and quickly recover from cyber events
- Minimize down time

Insight 2:

Implement Protective Controls

Focus on the following controls that reduce the most risk and have the greatest impact:

- Network Segmentation
  - Between Enterprise IT and Industrial control network
  - Between cells/zones
- Device Configuration (Secure and Accurate Configuration)
  - Standards based: IEC 62443, NIST SP 800-82, American Water Works Association, NERC CIP, NEI 08-09, and many others
  - Applicable for HMIs, engineering workstations, switches, routers, firewalls, controllers, etc.

Do not let IT targeted ransomware adversely affect cycle times and yield

Insight 3:

Perform Continuous Monitoring

How do you know all is operating as it should, or that an impending cyber event is about to negatively impact safety, productivity or quality? This should not be a mystery.

Control what you can control:

- Network design
- Monitor device configurations
- Cyber event recovery time

You cannot control:

- # of ICS vulnerabilities
- If you are a target for malicious behavior
- Insider threats

Tripwire and Belden deliver solutions that transform raw data into actionable information.
Our solutions are flexible and can scale to met your operational and safety needs.
It's easy to get started with a small pilot that is non-impactful to your process.

Call your Belden or Tripwire sales representative to schedule a demonstration.
Or visit our websites at www.Belden.com and www.Tripwire.com.

Belden US 1-855-400-9071
Belden EMEA +49 (0)7127 14 1809
Belden APAC +65 6879 9800

Tripwire US 1-503-276-7500
Tripwire EMEA +44 (0) 16 2877 5850
Tripwire APAC+65 6879 9839

TRIPWIRE-INDUSTRIAL-CYBER-BLIND-SPOTS-FLYER_SF_INET_TRW_0419_ENG

Be certain.
Belden.