Industrial Control System Security Assessment

ICS Security Is Your Responsibility

Industrial Control Systems (ICS) are designed to provide high availability to support 24/7 production systems, but often have very little or no security protection mechanisms to deter potential cyber threats. In many cases the implementation of multiple project upgrades, expansions, and inter-changing multiple system engineers has left numerous vulnerabilities open for assailants.

The ability to proactively protect a production system from potential threats requires a thorough understanding of the system vulnerabilities to clearly define the level of associated risk to develop an effective security plan.
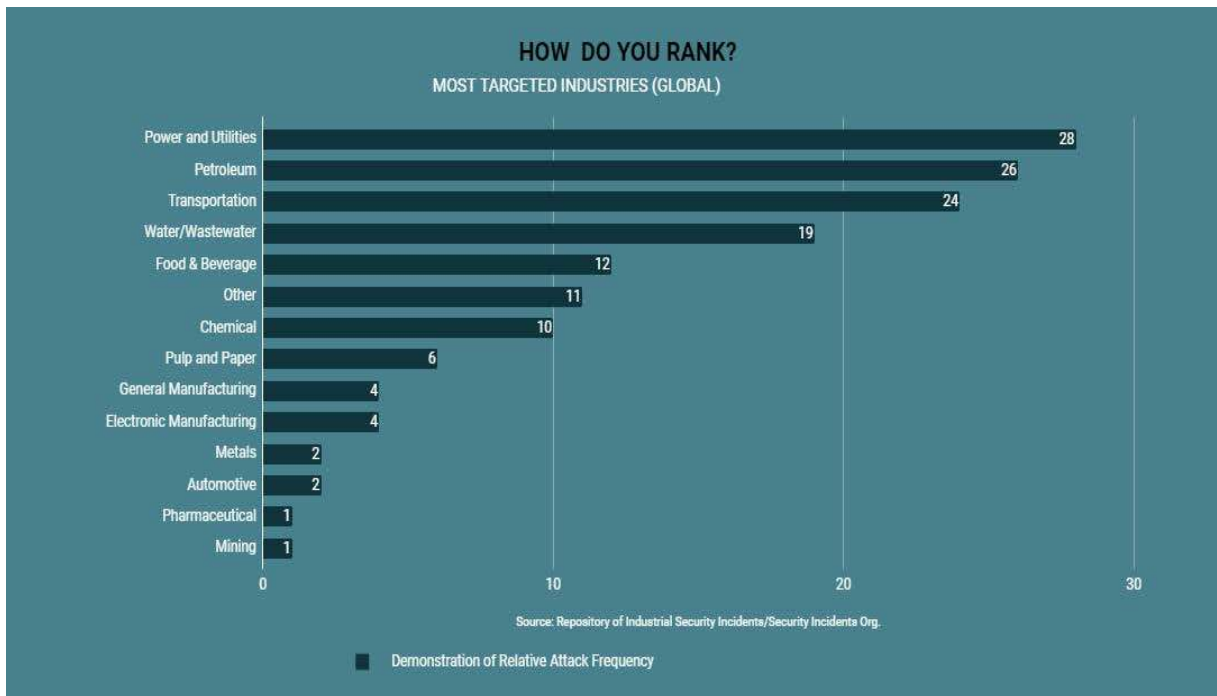
The Escalating Threat

According to the U.S. Department of Homeland Security Industrial Control System Cyber Emergency Response Team (ICS-CERT), the amount of cyber-attacks on ICS is at an all-time high. The level of sophistication of organized attacks are unprecedented and are exploiting critical infrastructure on a daily basis.

Any type of malicious penetration to an ICS network risks the loss of production, environmental release, equipment damage, and/or compromise of human safety. **These threats are real, continually escalating, and should be considered a priority for asset owners.**

cross

HOW DO YOU RANK?
MOST TARGETED INDUSTRIES (GLOBAL)

- Power and Utilities — 28
- Petroleum — 26
- Transportation — 24
- Water/Wastewater — 19
- Food & Beverage — 12
- Other — 11
- Chemical — 10
- Pulp and Paper — 6
- General Manufacturing — 4
- Electronic Manufacturing — 4
- Metals — 2
- Automotive — 2
- Pharmaceutical — 1
- Mining — 1

Source: Repository of Industrial Security Incidents/Security Incidents Org.

■ Demonstration of Relative Attack Frequency

Asessment Benefits

- Identify system vulnerabilities
- Define all ICS connectivity
- Define an ICS road map for growth and expansion
- Develop a comprehensive security and training plan over the entire lifecycle of the ICS
- Create remediation strategies to minimize impact in case of a security attack
- Create a cybersecurity culture to ensure a conscious effort to protect assets

Deliverables

- ICS Security & Vulnerability Asessment
- ICS Security Standard, Policy, & Procedures
- Mitigation & Recovery Planning
- Education & Training
- ICS Critical Infrastructure Compliance with Industry Standards & Practices

The Cross Company Advantage

Cross Company has in-depth knowledge of industrial security from our extensive ICS development, system migration experience, and detailed network design practices developed over the past two decades of business.

The Cross Company Cyber Assessment analysis includes an evaluation of ICS architecture, analysis of network traffic, and invasive scanning to identify potential vulnerabilities. A physical evaluation will be performed to identify the accessibility of devices, network, and/or interfaces. Finally, the data and analysis shall be reviewed and identified within the existing vendor lifecycle to determine potential risks and/or considerations for continued operational support.

The ICS security management plan encompasses multiple layers of protection to ensure production systems remain safe and available. This comprehensive assessment solution includes both internal and external vulnerabilities and provides a roadmap to meet the overall system lifecycle objectives.

cross

Process Control Integration
www.crossisg.com
850 Discovery Lane | Knoxville, TN 37932
Phone. 865.671.7700 | Fax. 865.671.1920

Corporate Office
www.crossco.com
4400 Piedmont Parkway | Greensboro, NC 27410
Phone. 336.856.6000 | Fax. 336.856.6999