Industrial Cybersecurity Checklist

Use this checklist to verify your operational technology and industrial cybersecurity posture, in compliance with NERC CIP, NIST CSF, UL2900, ISO 27001 & applicable data protection laws.

1. Physical Security

- ❑ Control Access to Facilities: Implement strict access controls to sensitive areas, using key cards, biometrics, and surveillance systems.
- ❑ Monitor and Secure Entry Points: Ensure that all entry and exit points are monitored with cameras and equipped with alarm systems.
- ❑ Visitor Management: Maintain a detailed log of all visitors, including their purpose of visit and access level granted. Issue visitor badges and escort them when necessary.
- ❑ Physical Barriers: Install physical barriers like fences, gates, and security doors to prevent unauthorized access.
- ❑ Regular Security Audits: Conduct regular security audits and risk assessments to identify and mitigate physical security vulnerabilities.

2. Operational Technology (OT) Security

- ❑ Network Segmentation: Separate OT networks from IT networks to limit the spread of malware and unauthorized access.
- ❑ Access Controls: Implement role-based access controls and ensure that only authorized personnel have access to OT systems.
- ❑ Patch Management: Regularly update and patch all OT systems to protect against known vulnerabilities.
- ❑ Monitoring and Logging: Continuously monitor OT systems for suspicious activity and maintain detailed logs for forensic analysis.
- ❑ Incident Response Plan: Develop and test an OT-specific incident response plan that includes steps for containment, eradication, and recovery.

3. Industrial Cybersecurity

- ❑ Risk Assessment: Conduct regular risk assessments to identify and address cybersecurity threats to industrial control systems (ICS).

- ❑ Security Policies and Procedures: Develop and enforce comprehensive security policies and procedures in line with NIST CSF, PCI DSS, and ISO 27001.
- ❑ Employee Training: Provide ongoing cybersecurity training to employees, focusing on the unique threats to industrial environments.
- ❑ Backup and Recovery: Ensure that critical data and configurations are regularly backed up and can be quickly restored in the event of a cyber incident.
- ❑ Vulnerability Management: Implement a robust vulnerability management program to continuously identify, assess, and remediate security weaknesses.

Remember these Key Attack Vectors for Industrial Cybersecurity

- Multifactor Authentication (MFA): Require MFA for all critical systems and remote access points to enhance security.
- Encryption: Use encryption to protect sensitive data both at rest and in transit.
- Third-Party Risk Management: Assess and manage the cybersecurity risks posed by third-party vendors and contractors.
- Incident Reporting: Establish clear procedures for reporting cybersecurity incidents internally and to relevant authorities.
- Continuous Improvement: Regularly review and update cybersecurity practices to adapt to evolving threats and compliance requirements.

These steps will help secure operational technology, physical premises, and manufacturing locations, ensuring compliance with industry standards and enhancing overall security posture.

Start Building Your ICS & OT Cyber Security Here:
https://www.industrialcybersecurity.ca/