The Urgent Need for Critical Infrastructure Cybersecurity

"Every organization – large and small – must be prepared to respond to disruptive cyber activity."
— *CISA Shields Up warning*

ICS + IT=

EXTREME EFFICIENCIES + **NEW CYBERSECURITY THREATS**

New connections require new protections for Industrial Control Systems (ICS). Prioritize action with the **Power of 5.**

5 THREATS TO CRITICAL INFRASTRUCTURE

- EMPLOYEE PHISHING
- NATION-STATE ATTACKS
- RANSOMWARE
- INSIDER THREATS
- ADVANCED PERSISTENT THREATS

5 PROTECTIONS TO DEPLOY ASAP

- SEGMENT NETWORKS, ESPECIALLY BETWEEN IT & OT
- ADD CONTINUOUS THREAT MONITORING
- CREATE & PRACTICE AN INCIDENT RESPONSE PLAN
- AUDIT NETWORK INVENTORY FREQUENTLY
- ASSESS RISKS & VULNERABILITIES

5 CYBERSECURITY FOCUS AREAS

IDENTIFY
Review risks impacting cybersecurity. Expose every item connected to networks. Perform penetration testing to reveal hidden vulnerabilities. Plant-floor assets | Controllers | Laptops | Mobile devices | IoT sensors | Security cameras | USBs | Supply chain

PROTECT
Using insights gained in the Identify step, architect appropriate security controls. Network segmentation | Multi-factor authentication | IDMZ deployment | Secure ICS Protocols | Firewalls | Patching | Zero Trust policies | Employee awareness training

DETECT
Gain real-time visibility into how, when, and where others are accessing or manipulating assets. 24/7 threat monitoring | Malware detection | Vulnerability scanning | Impact assessment | Daily asset inventories | Alerts and advisories

RESPOND
Implement an incident response plan to stop breaches from expanding infection and damage. Incident response | Containment | Mitigation | Communication planning | Tabletop exercises

RECOVER
Put a plan in place to quickly regain normal operations after an incident, shortening the recovery cycle and minimizing impact. Backup planning | Restoration | Investigation and analysis | Resilience planning

5 REGIONAL / INTERNATIONAL CYBERSECURITY FRAMEWORKS

Australia
The Critical Infrastructure Centre **(CIC) Compliance Strategy** offers recommendations for Critical Infrastructure owners/operators.

European Union
The Network and Information Security (NIS) Directive **(EU 2016/1148)** is the EU's first EU-wide cybersecurity legislation.

Germany
Plattform Industrie 4.0 is used to secure and expand Germany's robust manufacturing sector.

United Kingdom
The National Cybersecurity Center (NCSC) issued its **OT Security Design Principles** in 2020.

Global
The International Society of Automation (ISA) **ISA/IEC-62443** standard specifies security capabilities for control system components.

5 FACTS ABOUT $1B+ IN U.S. CYBERSECURITY GRANTS

- The bipartisan Infrastructure Investment and Jobs Act (IIJA) was signed into law in November 2021.
- It authorizes $1.2 trillion in funding and set aside billions of dollars for state and local governments.
- New grants offer opportunities to upgrade Critical Infrastructure cybersecurity for everything from vulnerability assessments, to malware analysis or threat detection.
- To be eligible for a grant, state or local agencies must submit a cybersecurity plan to the Department of Homeland Security (DHS), detailing technical capabilities and protocols for detecting and responding to cyberattacks.
- Rockwell Automation offers cybersecurity assessment and planning services to help you obtain necessary grant funding.

5 NEXT STEPS TO TAKE

Rockwell Automation: Securing what the world relies on.

- Talk to a **Rockwell Automation OT Cybersecurity expert**
- Take the **Cybersecurity Preparedness Assessment**
- View our action plan on **How to Win a Critical Infrastructure Cybersecurity Grant** in the U.S.
- Learn **How a Canadian Water Utility Company Improved Cybersecurity and Operational Resilience**
- Discover the ultimate **Guide to Critical Infrastructure Cybersecurity**

Rockwell Automation

Publication GMSN-SP019A-EN-P-September 2022 |