TIPS & TACTICS
CONTROL SYSTEM CYBERSECURITY

NIST CYBER

Quick steps you can take *now* to PROTECT your control system:

1 PUT SOMEONE IN CHARGE

Designate one or more people to lead your control system cybersecurity efforts.

2 KNOW WHAT YOU HAVE

Document which types of computer and control system assets you have, how each asset is used, and determine the most critical assets. Check for and remove unauthorized assets.

3 ESTABLISH CYBERSECURITY RELATIONSHIPS

Join your sector-specific cybersecurity communities and establish relationships with vendors and integrators who can help you with recommended cybersecurity practices.

4 CHANGE DEFAULT PASSWORDS

Check your assets for default passwords, and change any you find to new, hard-to-guess passwords. Do not display passwords in plain sight.

5 PROTECT ASSETS FROM TAMPERING

Keep critical assets physically secured and keep the keys of control system assets like Programmable Logic Controllers (PLCs) and safety systems in the "Run" position at all times unless they are being actively programmed.

Additional steps to MANAGE your control system cybersecurity risk:

1 TRAINING & AWARENESS

Train control system users on their cybersecurity responsibilities and to look for things out of the ordinary, which may be evidence of a cybersecurity incident.

2 MANAGE USER CREDENTIALS & ACCESS

Check who has on-site or remote access to your systems, and revoke access that isn't needed. Immediately disable accounts and revoke IDs when someone leaves the organization.

3 RESTRICT ACCESS TO THE CONTROL SYSTEM NETWORK & NETWORK ACTIVITY

Implement a layered network topology with a Demilitarized Zone (DMZ) to restrict access to control system networks. Restrict control system access to only users that require it. Consider requiring two-factor authentication for remote access instead of only a password.

4 MANAGE CYBERSECURITY VULNERABILITIES

Keep your assets up-to-date and fully patched. Prioritize patching of "PC" machines used in Human-Machine Interfaces (HMIs), database servers, and engineering workstations. Disable unused ports and services. Implement anti-virus/anti-malware/anti-phishing technologies where feasible to prevent, detect, and mitigate malware including ransomware.

5 IMPLEMENT APPLICATION CONTROL

The static nature of some control system assets, such as database servers, HMIs, and engineering workstations, make them ideal candidates to run application control solutions.

6 PREPARE TO RECOVER FROM A CYBERSECURITY INCIDENT

Develop and implement an incident recovery plan. Plan, implement, and test a system and data backup and restoration strategy.

7 IMPLEMENT & PERFORM CONTINUOUS MONITORING

Continuously monitor system boundaries and ingress and egress traffic. Be aware of relevant cybersecurity threats and vulnerabilities by using free resources like those available from NIST and the Cybersecurity & Infrastructure Security Agency (CISA).

NIST National Institute of Standards and Technology
U.S. Department of Commerce