These seven areas should form the backbone of your cybersecurity program.

Get Your Cybersecurity Off the Ground

IMPLEMENTING CYBERSECURITY defenses for industrial-control systems can seem intimidating. The right initial actions are crucial. Alexandre Peixoto, cybersecurity expert for the DeltaV distributed-control system from Emerson (Round Rock, TX, emerson.com), urges users to look closely at these seven key areas. They can offer a good defense-in-depth strategy in the short term:

- **Workstation hardening:** Ensure that the workstation configuration meets security policies.
- **User-account management:** Maintain unique user accounts and password-change routines.
- **Patch/security management:** Keep hardware and software up to date.
- **Physical security/perimeter protection:** Limit physical and electronic access to system networks.
- **Security monitoring/risk assessment:** Develop security policies and system-monitoring behavior.
- **Data management:** Develop guidelines for secure data creation, transmission, storage, and destruction.
- **Network security:** Ensure that system networks are properly segregated and protected.

For organizations wanting to get new cybersecurity programs off the ground fast, Peixoto recommends starting with the first three items on this list. Inexpensive to implement, they typically can be completed in-house.

—Jane Alexander, Managing Editor

Workstation hardening

Workstations are usually the entry points to isolated networks. New installations run at peak security but, over time, changes intended for temporary use, such as a remote access or use of removable media, are not reversed. These changes increase the system's attack surface, especially if the allowed remote connections aren't monitored or periodically audited.

Cybersecurity isn't a set-and-forget type of initiative. Operations should monitor and maintain all workstations using the initial configuration as a baseline. System administrators should keep records of their system's security policies and develop policy guidelines surrounding what can and cannot be changed.

Dedicated applications are available to help audit essential files and services running on each control-system workstation. These applications can be valuable tools in assessing cyber-threats within an industrial control-system environment.

User-account management

Individual user accounts with appropriate permissions should be part of every organization's security policy. Properly assigning user permissions also has a strong impact on cybersecurity. While it may seem easier to give every user high privilege access to the system, this approach increases the impact of a cyberattack, no matter which account is stolen. Developing and applying guidelines for user accounts is the first step, but setting a strategy for account management, based on those guidelines, is key to long-term control-system cybersecurity support.

Strict enforcement of password complexity and change routines will make it harder for unauthorized users to gain access using stolen passwords or brute-force attacks. A best practice is for each user to have a unique username and password for the control system that is distinct from those they use on enterprise business systems.

Patch/security management

Properly maintaining a control system means keeping hardware and software up to date. When a system is unpatched or outdated, the organization is exposed to cyberattacks.

Organizations need to keep track of operating system updates, antivirus updates, and software hotfixes that are available for their systems and regularly apply these patches. Unpatched systems are vulnerable to cyberattacks that are based on known vulnerabilities. Appropriate, timely patch management can be accomplished internally or by using support programs available from automation-system vendors.

Bottom line

Not only is it easy to overlook cybersecurity, it's difficult for plants to justify allocating resources for it if they've never been attacked (or have been, but don't know it). Unfortunately, when security vulnerabilities are exploited, the costs required to recover a system are high and the impact widespread.

Focusing on the right first steps today can help secure your industrial-control system and develop an internal cybersecurity posture in your organization. **MT**

For more information on cybersecurity, go to emerson.com/cybersecuritymanagement.