SERIOUSLY

Cyber attacks are real, and critical infrastructure is a major target. Be aware and prepared.

SEL SCHWEITZER ENGINEERING LABORATORIES, INC.

For information about SEL cybersecurity solutions or copies of this poster, visit **www.selinc.com/cybersecurity**.

TEN TIPS FOR IMPROVING THE SECURITY OF YOUR ASSETS

EDMUND O. SCHWEITZER, III

KNOW ALL COMMUNICATIONS PATHS TO YOUR ASSETS

Make sure to include paths that are accessible locally, such as a thumb drive. Draw a picture!

- SCADA
- EMS
- Engineering access
- Maintenance
- Telephone lines
- Wireless
- Internet
- System interconnections and bridges

USE AND MANAGE STRONG PASSWORDS

SEL equipment makes this easy: you can use virtually all printable ASCII characters. Use a password manager, such as KeyPass® or Lastpass®, to generate long, complex passwords for each unique login you have. Strengthen a password, like the one below, with a few changes:

Weak: Webster **Strong:** W3bTerd1Ct10n@ry

- Do not use default passwords
- Change them periodically
- Change them when people leave
- Use different ones in different regions
- Control them

SECURE COMMUNICATIONS WITH ENCRYPTION AND AUTHENTICATION TOOLS

- Wire, fiber, and radio
- SCADA, engineering access, maintenance, and informational data (bulk, video, etc.)

PRACTICE A "NEED-TO-KNOW" POLICY, COMPARTMENTALIZE KNOWLEDGE, AND GUARD YOUR ACCESS TOOLS

Keep your designs safe, and limit access to system details to those who really need to know to do their job. Be especially careful to protect:

- Computers
- Passwords
- Software
- Instruction manuals
- Encryption equipment and keys

FOR KEY ASSETS, HAVE MORE THAN ONE (SECURE!) COMMUNICATIONS PATH

- Minimize the impact of denial-of-service attacks
- Send security alarms through a second path

TAKE ACTION NOW

Don't wait for a government mandate—ensure that your system is ready now. There are practical steps you can take today to prepare your team and prevent an event from happening in the first place.

REVIEW LOG FILES ON FIREWALLS, ALARMS, AND ACCESS ACTIVITY

DON'T FORGET PHYSICAL SECURITY

PRACTICE "SECURITY IN DEPTH"

- Physical
- Cyber
- Communications
- Training
- Culture

HAVE AN INCIDENT RESPONSE PLAN READY AHEAD OF TIME

So a cyber event happens—now what? During the event is not the best time to create a plan and try it out. You should have a clear, concise, and well-thought-out plan in place beforehand about how your company will respond to a cyber incident.