



MANTENGA

EL

INTERNET

AFUERA

DE LA

CERCA



SCHWEITZER ENGINEERING LABORATORIES

Para obtener información sobre las soluciones de seguridad cibernética de SEL o recibir copias de este cartel, visite selinc.com/cybersecurity.
© 2019 por Schweitzer Engineering Laboratories, Inc. • 20190417

Ten Tips for Improving the Security of Your Assets

Edmund O. Schweitzer, III

Know all communications paths to your assets.

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

- SCADA
- Energy management system (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. Strengthen a password, like the one below, with a few changes.

Weak: `Webster` **Strong:** `W3b$Ter$d1Ct10n@ry`

To keep passwords secure:

- 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.

Secure all communications, including:

- 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!) path.

Redundant paths allow you to:

- 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 “defense in depth.”

Comprehensive security includes:

- 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. Have a clear, concise, and well-thought-out plan in place beforehand about how your company will respond to a cyber incident.



Designing the Future of Substation Cybersecurity

True cybersecurity requires a combination of people, processes, and technology. At SEL, our defense-in-depth philosophy and commitment to building security-aware cultures lead to the most secure and compliant solutions. Backed with years of experience, our Engineering Services team will:

- **Assess regulatory requirements** to document and resolve risks and gaps in power system infrastructure.
- **Identify and analyze cyber threats** to minimize their impact on substation operations.
- **Review substation cybersecurity operations** to provide sensible security solutions.
- **Design and implement solutions** to enhance and protect mission-critical power systems.

Take the first step to substation security and compliance today at selinc.com/cybersecurity.

