SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

Ten Tips for Improving the Security of Your Assets

Edmund O. Schweitzer, III
November 2009

From the very beginning of SEL, I have stressed the importance of security in our relays, communications processors, meters, and other equipment. From our very first products, we have provided two levels of access with separate passwords and alarm contacts that signal access failures. For many years, we have emphasized the importance of security in integrated systems and published many papers describing threats, attack scenarios, and practical mitigation. In addition, SEL University offers a cybersecurity course, and SEL has several secure-communications products.

In recent years, cybersecurity has become increasingly important. Too many of us have had negative personal experiences, including identity theft, phishing, denial-of-service attacks, viruses, credit card fraud, and bank fraud. Broader threats come from hackers, disgruntled employees, terrorists, and countries with sophisticated information warfare plans and capabilities. These threats are just as real as the ones we may have personally experienced.

Given the rapidly changing world of technology, and the relatively new recognition of the importance of cybersecurity, it often seems as if there is no clear focus on the responsibility for security. Does it belong with the information services people, SCADA folks, protection engineers, customers, suppliers, government? The answer is it’s the responsibility of all of us. It has to be, because modern power systems use so many different kinds of electronic instruments, and so many different means of communications and access, for such a wide variety of purposes.

Fortunately, there are many simple and low-cost steps you can take to quickly reduce the threats to vital power system assets. Here are ten activities that I think you should seriously consider.

1. 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

2. Use and manage strong passwords.

SEL equipment makes this easy: you can use virtually all printable ASCII characters. Strengthen a password like the one below with a few changes:

Weak: **Webster**
STRONG: **W3b$st3r**

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

3. Secure communications with encryption and authentication tools.

- ✓ Wire, fiber, radio
- ✓ SCADA, engineering access, maintenance

4. Practice a “need-to-know” policy, compartmentalize knowledge—even 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
- ✓ Encryption equipment and keys
- ✓ Instruction manuals
- ✓ Software

5. For key assets, have more than one (secure!) communications path.

- ✓ Minimize impact of denial-of-service attack
- ✓ Send security alarms through a second path

6. Take action now. Don’t wait for a government mandate or for an attack.

7. Review log files on firewalls, alarms, and access activity.

8. Don’t forget physical security.

9. Practice “security in depth.”

- ✓ Physical
- ✓ Cyber
- ✓ Communications
- ✓ Training
- ✓ Culture

10. 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.