SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: 509.332.1890 • Fax: 509.332.7990
www.selinc.com • info@selinc.com

Twelve Tips for Improving the Security of Your Assets

Edmund O. Schweitzer, III
August 25, 2006

From the very beginning of SEL, I have stressed the importance of the security of SEL 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 which signal access failures. For many years, we have emphasized the importance of security in integrated systems, and have published many papers describing the 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.

We have become aware of the many threats, including 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 service 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 the vital assets of our power systems. Here are twelve activities that I think you should seriously consider. And, following the twelve tips are ten myths we all need to help bust!

1. **Know all communications paths to your assets: Draw a Picture!**

   SCADA
   EMS
   Engineering Access
   Maintenance
   Telephone Lines
   Wireless
   Internet
   Interconnections and bridges between systems
   Portable media

2. **Use strong passwords.**

   SEL equipment makes this easy: you can use virtually all printable ASCII characters

Weak:	**Webster**
STRONG:	**M$i4fp&r**

3. **Manage passwords.**

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

4. **Encrypt communications.**

   Wire, fiber, radio
   SCADA, engineering access, maintenance

5. **Practice “Need to Know” and compartmentalize knowledge.**

   Keep your designs safe and secure
   Limit access to system details to those who really “need to know” to do their jobs

6. **Isolate and restrict privileges and segregate duties.**

   Know your suppliers and their security practices

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

   Minimize impact of Denial of Service attack
   Send security alarms through second path

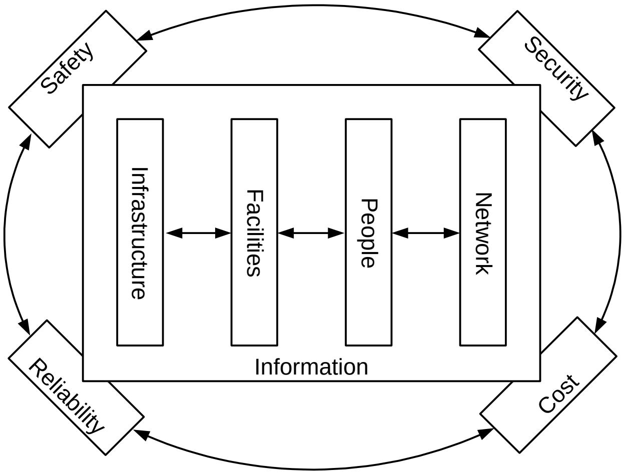
8. **Take action now. Don’t wait for a government mandate or for an attack.**

9. **Review alarms and access activity.**

10. **Don’t forget physical security.**

11. **Practice “Security in Depth.”**

    Physical, cyber, communications, training, culture, and career



12. **Guard your access tools.**

    Manage computers, passwords, encryption equipment and keys, instruction manuals, software, cryptographic keys, and portable media

When a problem emerges, such as cybersecurity, it’s human nature frequently to begin by denying its importance or even its existence. Myths, like the ones below, often become a form of denying the problem or delaying action.

Ten Security Myths

1. **I use XXX protocol and no hacker knows it.**

   While it's true that using a less-than-common protocol might slow down a hacker, protocol analyzers have surprisingly deep knowledge of protocols, old and new, even bit-oriented ones. Protocols, whether they are old or new, proprietary or open, are *known*.

2. **Spread-spectrum radios are inherently secure.**

   The main purpose of frequency hopping is to avoid interference with other signals, and not for communications security. You need encryption even with frequency hopping radios.

3. **My network is private, so there is little risk.**

   Insiders have access to private networks. And as soon as a circuit, cable, fiber, or signal crosses the fence, others have access too. Private networks, like public ones, are NOT secure and ARE at risk.

4. **It would be pretty hard to hack our SCADA over point-to-point radio**.

   The hacker can narrow down frequencies using your company name and the FCC radio license database; and even further by looking at the antenna types, sizes, and pointing directions. Is there a nameplate visible on the equipment? That will lead him to the manufacturer's website for more information. He can intercept your signals with a scanner purchased from a radio store. He can record your signals on the sound card of his computer. He can buy a transceiver and attack you by replaying his intercepts. You can foil the attack with encryption.

5. **I use WEP and it's secure.**

   WEP has holes. Although you can probably rely on it for many home and business applications, you should not rely on it for industrial or utility control. Add a second layer, such as 128-bit or 256-bit AES encryption.

6. **It's expensive to secure my systems.**

   Your equipment probably already has many security features that you may not be using: passwords, alarm contacts, etc. And, encrypting transceivers cost around $500 each ... a small price to secure a substation, or even a recloser control!

7. **I won't use wireless because it isn't secure.**

   While it is true that WEP is not secure, there are wireless transceivers available that add a second layer of security. They are very secure. Don't deny your operation the safety and convenience of wireless tools, for controlling reclosers, switches, and breakers. It's great for avoiding arc flash risk, for example.

8. **The Information Service guys are responsible for cybersecurity, i.e., it's not my job!**

   IS departments are great for designing and securing modern IT communications systems. However, they may be unaware of the many communications paths into substations and generating stations. Folks responsible for communications, metering, relaying, SCADA, remedial action schemes, as well as the IS team, need to focus on security, individually and in concert.

9. **The government will issue standards that will cover everything.**

   No matter how good any standards are or will be, we need to be aware the threats are immediate, and we cannot afford to wait. Furthermore, threats change faster than standards can keep up, so we need to apply good security practices as a matter of habit, not government dictate. Finally, those of us closest to the very assets and applications are in the best position to see what needs done, and to do it.

10. **It can't happen to me.**

    It can!

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: 509.332.1890 • Fax: 509.332.7990
www.selinc.com • info@selinc.com