Recent Headlines:

Hackers stole Social Security numbers from 21.5 million, gov't admits
- Fox News, July 9, 2015

Cyber Attacks Against SCADA Systems Doubled In 2014, Says Dell Threat Report
- Homeland Security Today, April 15, 2015

Anthem now says 78.8M were affected by breach
- IDG News Service, February 24, 2015

FYI for TMEPA members:

Leaders do not need to become experts or spend millions on cyber security to protect their organizations and customers. BUT, you do need to know enough to oversee and carry on the conversation. Where to start:

1. **Educate yourself** – The buck stops with you. When something happens, answers will be demanded. Get in the conversation and ask questions of those that you trust to handle cyber security for you.
2. **Measure your status** - Measure against accepted standards. This is more than asking your IT guys to check the firewall. Standards are multi-dimensional, covering all areas. CIP is the most applicable to TMEPA. *More about CIP standards on page 2.*
3. **Develop a plan to close holes –** There is no such thing as 100% security which always leaves room for improvement. The gaps should be ranked by risk and prioritized. Regular meetings and documented progress against risks will show the level of commitment to security.
4. **Develop a security program –** The rapid pace of change does not allow you to *set-it-and-forget-it*. Policies need to be written and responsibilities assigned. The program will require monitoring and regular reporting.
5. **Train your staff –** This is the biggest bang for the buck. Communicate the commitment to protecting customers and that it is everyone's responsibility. If they know how to respond to a situation, you may have just prevented a breach.

3 Critical Steps in protecting SCADA systems

1. **Isolate the SCADA network -** It is critical to isolate the SCADA network from the corporate network. When the Human Machine Interface (HMI) network is separated, internal boundary controls can protect sensitive systems through the use of standard security solutions such as firewall, intrusion detection systems and anti-malware solutions.
2. **Segregate Administrators and Users -** Ensure permission to the HMI is set properly. Those with read-only access should not be able to modify configuration.
3. **Be prepared to manage inherently insecure systems -** Many SCADA systems run on proprietary or dated systems. In some cases, these systems have limited ability to receive upgrades or patches. Even the simplest system can be used as an entry point in to a network. Additional mitigation controls may be needed to protect these systems.

www.securit360.com
David Forrestall | 205.410.3864 | david@securit360.com

SecurIT360

The physics of securing IT

About CIP Standards

In December 2010, NERC approved an enhancement to its Critical Cyber Asset Identification standard (CIP-002 Version 4) that establishes bright-line criteria for the identification of critical assets. CIP v5 has been approved with increased responsibilities. TMEPA members may not be required to following these standards, but it is a good starting point to put you at a much lower risk of breach and damages. A high-level summary of the CIP standards:

CIP-001: **Sabotage Reporting -** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies

CIP-002: **Critical Cyber Asset Identification** – Measurement of risk. This requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-003: **Security Management Controls -** requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. This is a security program, which includes: Policies, Leadership, Measurement, and other controls to protect information.

CIP-004: **Personnel & Training -** requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

CIP-005: **Electronic Security Perimeter(s) -** manage electronic access to BES (Bulk Electric System) Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-006: **Physical Security of BES Cyber Systems -** manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-007: **System Security Management -** manage system security by establishing specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-008: **Incident Reporting and Response Planning –** implement systems that ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

CIP-009: **Recovery Plans for Critical Cyber Assets –** ensure that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

CIP-010: **Configuration Management and Vulnerability Assessments** - requires that Responsible Entities have minimum configuration management and vulnerability assessment controls in place to protect BES Cyber Assets and BES Cyber Systems.

*CIP-011**[NEW]***: **Information Protection** - requires prevention of unauthorized access to BES Cyber System Information against compromise that could lead to misoperation or instability in the BES.

www.securit360.com
David Forrestall | 205.410.3864 | david@securit360.com