APTA Enterprise Cyber Security Standards

Lurae Stuart

Good Harbor Consulting,
Principal- Surface Transport

Arlington, VA

Enterprise Cyber Security Working Group

Cyber attacks are a major threat to every aspect of modern life that is touched by information technology.

We know that transit systems are heavily dependent on a variety of information technology systems and therefore "at risk."

What are the vulnerabilities and risks and how should a transit agency provide appropriate safeguards against those risks?

Threat to operational, business and service provider systems

- Cyber attacks may be targeted toward one or more of the **system layers* that Transit agencies depend on:
  - Operational systems which are dependent upon SCADA and manufacturer (OEM) technologies.
  - Business systems (sometimes referred to as 'enterprise systems') which are used to manage the organizational needs of the agency.
  - And 3rd party systems which are interconnected or share dependencies with operational and business platforms.

*See "system layers detail" slide

Risk to organizational and personal Safety, Security and Privacy.

- Cyber attacks can destroy a transit agency's physical systems, render them inoperable, or hand over control of those systems to an outside entity.
- Cyber attacks can also destroy or compromise critical organizational information or personal data related to employees or customers.
  - Employee information resides in business systems like HR and Payroll.
  - Customer information is transacted through 3rd party systems like the Visa Mastercard interchange, point of sale (POS) networks and rider account systems.
-

Constantly evolving in nature.

- Cyber attacks rarely take the same form the second or third time that they occur due to the "arms race" nature that exists between the initiating elements (criminal, state actors, activist or 'hacktivist') and the mitigating elements (government, industry and law enforcement).
- If an attack is developed that succeeds a counter measure is soon behind.
- Some advanced attacks now attempt to 'hide' in the system and circumvent detection, quarantine and removal by gaining control of the software that is designed to capture the malware. (e.g. Stuxnet).

Awareness, information sharing, vigilance and detection.

- Transit agencies must rely on forums that enable sharing and collaboration to promote awareness of new attacks – particularly industry specific attacks.
- Raising awareness and knowledge about the potential risks should improve the overall vigilance that an agency applies to these threats.
- Specific directives and guidelines for the protection of systems and the detection of threats will be developed by the Enterprise Cyber Security working group.

Enterprise Cyber Security Working Group

Summary

- Cyber attacks pose a threat to operational, business and service provider systems.
- They present a risk to organizational and personal Safety, Security and Privacy.
- Cyber threats are constantly evolving in nature.
- Mitigating Cyber risks requires awareness, information sharing, vigilance and detection capabilities.
- Best practices for policies and procedures should be identified by this WG and captured in the Enterprise Cyber Security guidelines.

System Layers (Detail)

Operational Systems	Business Systems	3rd Party Systems
•SCADA	•Human Resources Payroll •Directory Management •ERP •Email	•Payment Systems •Account Management Systems