2015 Transit Safety Summit

Cybersecurity In Transit

AMERICAN PUBLIC TRANSPORTATION ASSOCIATION

APTA Standards Development Program
Lead the Way

Vulnerable Systems

APTA Standards Development Program
Lead the Way

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 ('enterprise systems') which are used to manage the organizational needs of the agency.
  - -websites, servers
  - -payroll programs
  - -enterprise, IT systems
- And 3rd party systems which are interconnected or share dependencies with operational and business platforms.

TRANSIT CASE STUDIES

May 2008 - Fare collection vulnerability

College students created a report demonstrating weaknesses in a transit agency automated fare collection system.

- Revealed the Crypto RFID's and Magstripes of Ticketing Systems vulnerabilities.
- Proposed releasing report to public & the DEF CON hacker convention which claimed to review and demonstrate how to reverse engineer the data on the magstripe card.

Litigation later occurred which eventually resulted with the agency working with security experts to address the vulnerability.

TRANSIT CASE STUDIES

August 2011 – "Anonymous" attack

- A transit agency cut off cell phone service to interrupt protestor communications.
  - "Anonymous" responded by launching a DDoS attack on the agency public website.
- A second attack stole contact information and passenger data. At least 120 law enforcement officers' personal information was posted online.

TRANSIT CASE STUDIES

December 2012 – Payroll system hacked

- 16 Fake employees were added to the payroll
  - Resulted in $26,000/month in potential losses

TRANSIT CASE STUDIES

January 2014 – Fare collection vulnerability

- Seven individuals are facing charges of theft, fraud, and racketeering for allegedly selling counterfeit fare cards.
  - The $1 cards were purchased and the security features were hacked to boost the cards' values.
  - The agency, supplier are working together to identify and hotlist any additional fraudulent cards.

Intent

- **Political:** Defending violations specific to perceived social injustices, censorship, and restrictions on Internet freedoms: Stop Online Piracy Act; Occupy support; Arab Spring
- **Retaliation:** Members of “Anonymous” and associated groups conduct cyber attacks in retaliation : FBI; CIA; Interpol ; Law Enforcement
- **Security Awareness:** Exploiting vulnerabilities to demonstrate that they exist : Pr0f/C4d4 and Industrial Control Systems
- **Criminal /Financial:** Bypassing fare cards, theft of credit card information for personal gain or for bribery.

SECURITY STANDARDS

Addressing Cybersecurity

Control & Communications Cybersecurity Workgroup Update

AMERICAN PUBLIC TRANSPORTATION ASSOCIATION

APTA Standards Development Program
Lead the Way

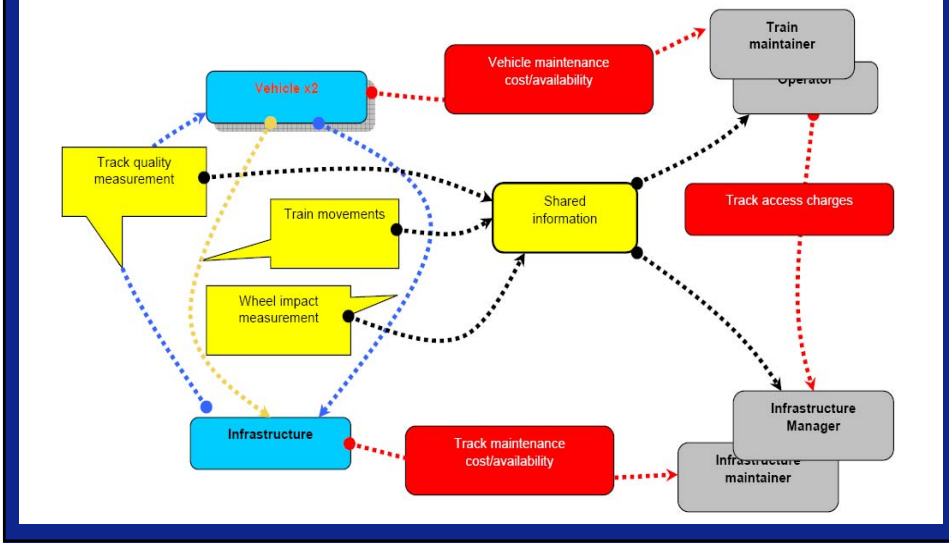
Rail Vehicle Systems

APTA Standards Development Program
Lead the Way

- Safety / Security
  - CCTV
  - Fire Detection
  - Emergency PIS
  - Train Operation – Propulsion, Braking
  - Signalling Interface
  - PA system
  - Door Control
- Maintenance
  - Remote Diagnostics/Fault Monitoring
  - Remote Software Updates
- Passenger Interfaces
  - Real-time Travel Information
  - Wi-Fi Internet Access
  - On-board Entertainment
- Management
  - Passenger Counters
  - E-Ticketing
  - Fleet Tracking and Asset Control

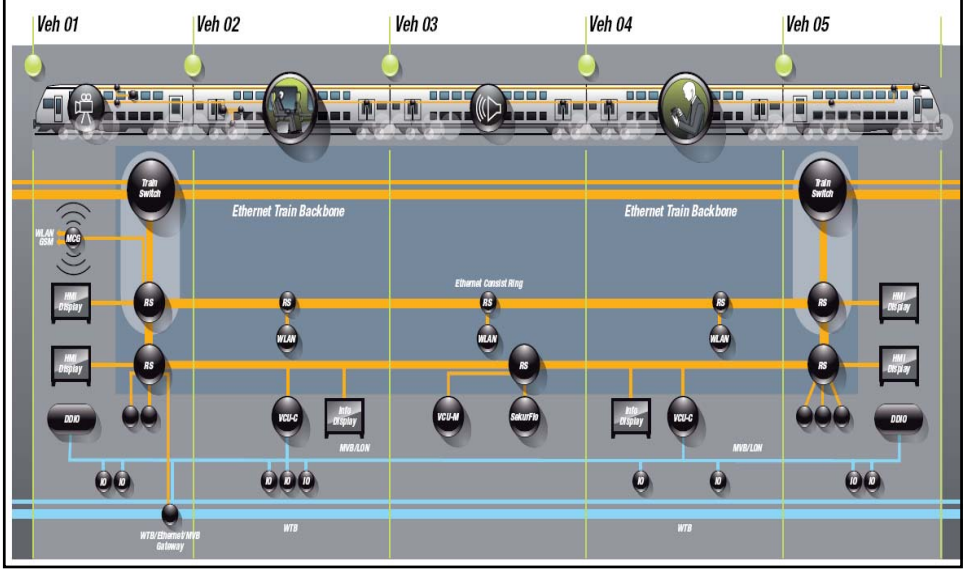
Rail Vehicle Systems Share Information

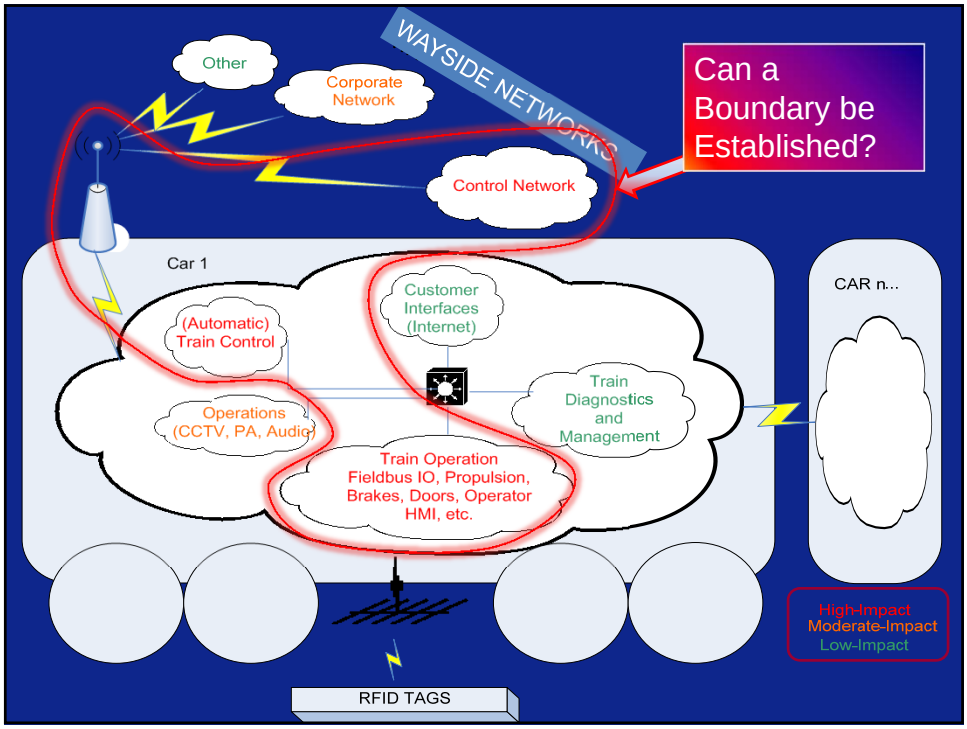
APTA Standards Development Program
Lead the Way

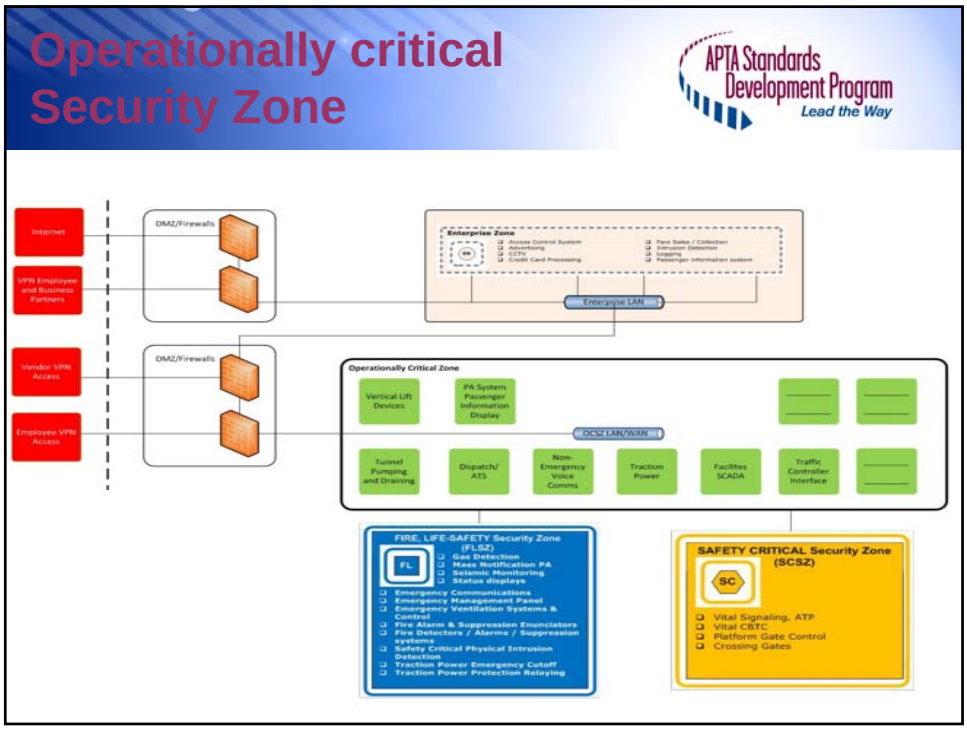


Systems Are Now IP Enabled

APTA Standards Development Program
Lead the Way



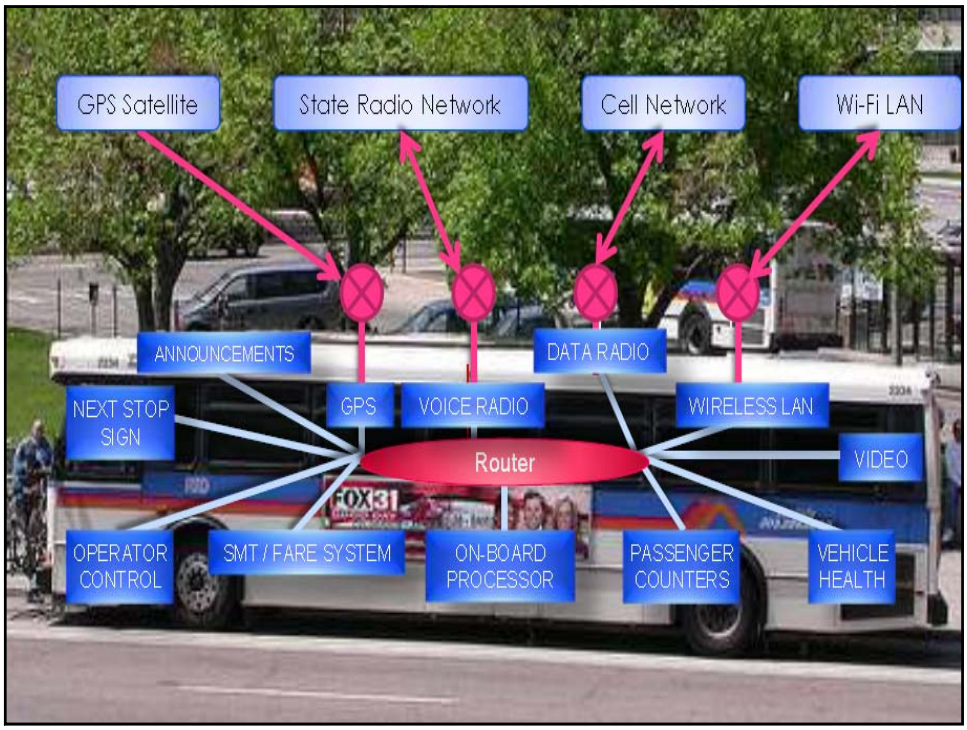

WAYSIDE NETWORKS
Other
Corporate Network
Control Network
Can a Boundary be Established?
Car 1
CAR n...
Customer Interfaces (Internet)
(Automatic) Train Control
Train Diagnostics and Management
Operations (CCTV, PA, Audio)
Train Operation Fieldbus IO, Propulsion, Brakes, Doors, Operator HMI, etc.
High-Impact
Moderate-Impact
Low-Impact
RFID TAGS


Operationally critical Security Zone
APTA Standards Development Program
Lead the Way
Internet
VPN Employee and Business Partners
Vendor VPN Access
Employee VPN Access
DMZ/Firewalls
DMZ/Firewalls
Enterprise Zone
Enterprise LAN
Operationally Critical Zone
Vertical Lift Devices
PA System Passenger Information Display
OCSZ LAN/WAN
Tunnel Pumping and Draining
Dispatch/ ATS
Non-Emergency Voice Comms
Traction Power
Facilities SCADA
Traffic Controller Interface
FIRE, LIFE-SAFETY Security Zone (FLSZ)
Gas Detection
Mass Notification PA
Seismic Monitoring
Status displays
Emergency Communications
Emergency Management Panel
Emergency Ventilation Systems & Control
Fire Alarm & Suppression Enunciators
Fire Detectors / Alarms / Suppression systems
Safety Critical Physical Intrusion Detection
Traction Power Emergency Cutoff
Traction Power Protection Relaying
SAFETY CRITICAL Security Zone (SCSZ)
Vital Signaling, ATP
Vital CBTC
Platform Gate Control
Crossing Gates

Cyber WG developments

APTA Standards Development Program
Lead the Way

- Control & Communications Cybersecurity Standard Part I, II are published. Currently developing part IIIb.\
  - "Securing Control and Communications Systems in Transit Environments Part 1"
  - "Securing Control and Communications Systems in Rail Transit Environments Part 2"
- Enterprise Cybersecurity WG approved a draft;
  - "*Cybersecurity Considerations for Public Transit" (published June 2014)*
- Next Standards; Cybersecurity Considerations for Buses



Stay Informed

APTA Standards Development Program
Lead the Way

Utilize tools and resources

- Identify available resources, guidance (DHS, ICS-CERT, Cyber Alerts, etc.)
- Use available tools (CSET) for performing an agency specific risk assessment
- APTA Standards

CSET

APTA Standards Development Program
Lead the Way

Homeland Security

Cyber Security Evaluation Tool (CSET)

Performing a Self-Assessment

The Cyber Security Evaluation Tool (CSET) provides users with a systematic and repeatable approach for assessing the cybersecurity posture of their industrial control system networks. This tool also includes both high-level and detailed questions applicable to all industrial control systems (ICS). CSET was developed under the direction of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP).

What is it?

The CSET is a stand-alone desktop software tool that enables users to assess their network and ICS security practices against recognized industry and government standards, guidelines, and practices. The completed CSET assessment provides a prioritized list of recommendations for increasing the cybersecurity posture of an organization's ICS or enterprise network and identifies what is needed to achieve the desired level of security within the specific standard(s) selected.

Security Standards

- DHS Catalog of Control Systems Security: Recommendations for Standards Developers, Revisions 6 and 7
- NIST SP800-82
- NIST SP800-53, revision 3
- NRC Regulatory Guide 5.71
- CFATS Risk Based Performance Standard (RBPS) 8
- NERC CIP-002-009 revisions 2 and 3
- ISO/IEC 15408 revision 3.1
- DoDI 8500.2
- Consensus Audit Guidelines 2.3.

After the user selects the applicable standard(s), CSET generates questions that are specific for those requirements.

CSET Process Flow

CSET

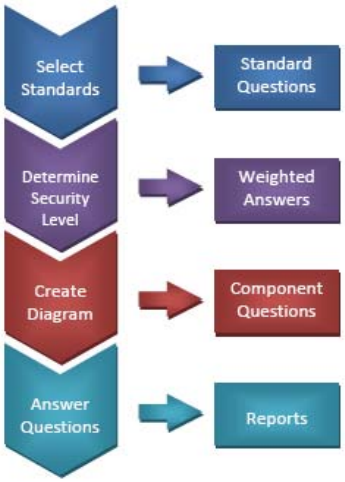
APTA Standards Development Program
Lead the Way

Downloadable via the Internet at:
http://us-cert.gov/control_systems/csetdownload.html

The Assessment Process

Four basic steps are available to complete an assessment using CSET. The process is shown in the CSET Process Flow figure.

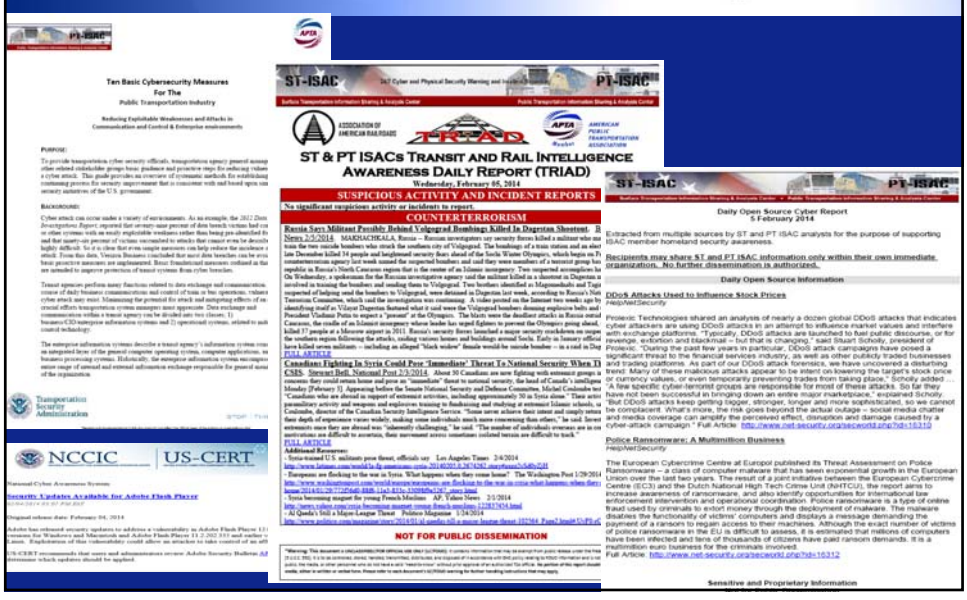
STEP 1-Select Standards: Users are given the option to select one, several, or all the following industry and government-recognized cybersecurity standards.



http://www.us-cert.gov/control_systems/satool.html

Cyber Alerts

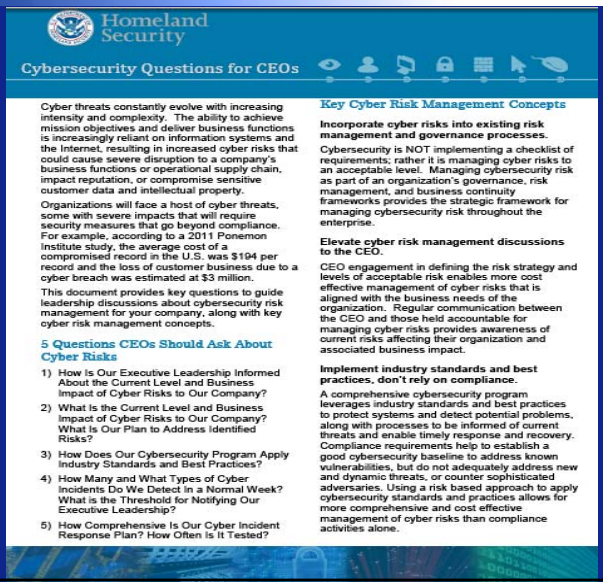
APTA Standards Development Program
Lead the Way



What Your Agency Should Be Doing Now

- Update systems and software
- Strong passwords, secure any default passwords
- Apply firewalls to implement network segmentation
- Minimize network exposure for all control system networks
- Implement cybersecurity best practices to reduce likelihood of an attack
- Establish privileges to control account access
- Limit use of removable external drives
- Develop and reinforce policies on mobile devices
- Develop cybersecurity incident response plan

CEO Considerations



Homeland Security

Cybersecurity Questions for CEOs

Cyber threats constantly evolve with increasing intensity and complexity. The ability to achieve mission objectives and deliver business functions is increasingly reliant on information systems and the Internet, resulting in increased cyber risks that could cause severe disruption to a company's business functions or operational supply chain, impact reputation, or compromise sensitive customer data and intellectual property.

Organizations will face a host of cyber threats, some with severe impacts that will require security measures that go beyond compliance. For example, according to a 2011 Ponemon Institute study, the average cost of a compromised record in the U.S. was $194 per record and the loss of customer business due to a cyber breach was estimated at $3 million.

This document provides key questions to guide leadership discussions about cybersecurity risk management for your company, along with key cyber risk management concepts.

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect in a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Key Cyber Risk Management Concepts

Incorporate cyber risks into existing risk management and governance processes.

Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. Managing cybersecurity risk as part of an organization's governance, risk management, and business continuity frameworks provides the strategic framework for managing cybersecurity risk throughout the enterprise.

Elevate cyber risk management discussions to the CEO.

CEO engagement in defining the risk strategy and levels of acceptable risk enables more cost effective management of cyber risks that is aligned with the business needs of the organization. Regular communication between the CEO and those held accountable for managing cyber risks provides awareness of current risks affecting their organization and associated business impact.

Implement industry standards and best practices, don't rely on compliance.

A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current threats and enable timely response and recovery. Compliance requirements help to establish a good cybersecurity baseline to address known vulnerabilities, but do not adequately address new and dynamic threats, or counter sophisticated adversaries. Using a risk based approach to apply cybersecurity standards and practices allows for more comprehensive and cost effective management of cyber risks than compliance activities alone.

Thank you!

David Hahn
Sr. Program Specialist – Safety & Security
American Public Transportation Association
dhahn@apta.com
202-496-4813

Roundtable Discussion

What is your agency doing to prevent,
and recover from an attack?