Effective Practices for the Protection of Transportation Infrastructure from Cyber Incidents

Transportation Research Board Webinar
November 17, 2015
Webinar Presenters

David Fletcher
Western Mgmt and Consulting, LLC

Ernest “Ron” Frazier
Countermeasures Assessment & Security Experts, LLC

Patricia Bye
Western Mgmt and Consulting, LLC

Yuko Nakanishi
Nakanishi Research and Consulting, LLC
Today’s Agenda

Overview of the research

Preview research results

Highlight best practice & approaches
  - Risk Management
  - Security Programs
  - Countermeasures
  - Training

Primer: Cybersecurity 101
NCHRP 2015
Identify effective practices that can be used to protect transportation systems from cyber events and to mitigate damage should an incident or breach occur.

**Scope**
- Both transit and highway operations
- All transportation systems - industrial control, transportation control and enterprise data systems

**Deliverables**
- Executive Briefing template to awareness
- Cybersecurity Primer with best practices for operations
Today’s transit systems are cyber
Today’s highways are going cyber
# Cyber Transportation Systems

Control systems and IT systems

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Transit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Systems</td>
<td>Control Systems</td>
<td>Train Control System, Bus Control Systems</td>
</tr>
<tr>
<td></td>
<td>SCADA</td>
<td>Traction Power, Emergency Ventilation System, Monitoring (Pumps, Alarms)</td>
</tr>
<tr>
<td></td>
<td>Signaling</td>
<td>Train Signals, Signal Priority Systems</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>Communications, DSRC</td>
</tr>
<tr>
<td></td>
<td>Fare Collection Systems</td>
<td>Entry/Exit Gates, Ticket Vending Machines, Fare Boxes, Fare Validators,</td>
</tr>
<tr>
<td></td>
<td>HVAC/Building Management</td>
<td>HVAC systems (not integral part, but loss could result in failure of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>critical systems)</td>
</tr>
<tr>
<td>Enterprise Data</td>
<td>Business/Revenue/3rd Party</td>
<td>Asset Management</td>
</tr>
<tr>
<td>Systems</td>
<td>systems: Finance, HR,</td>
<td>BYOD</td>
</tr>
<tr>
<td></td>
<td>Messaging (email), Archives</td>
<td></td>
</tr>
<tr>
<td>Engineering Systems</td>
<td>Design, Construction</td>
<td>Track Inspection</td>
</tr>
</tbody>
</table>

### CONTROL SYSTEMS

Monitor/control **PHYSICAL WORLD** with emphasis on **SAFETY & AVAILABILITY**. Risks loss of life or equipment destruction.

### IT SYSTEMS

Collect/process **DATA or INFORMATION** with emphasis on **INTEGRITY & CONFIDENTIALITY**. Risk loss of services or confidential information.
## Control System Security Challenges

<table>
<thead>
<tr>
<th>SECURITY TOPIC</th>
<th>INFORMATION TECHNOLOGY</th>
<th>CONTROL SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus &amp; Mobile Code</td>
<td>Common &amp; widely used</td>
<td>Uncommon and can be difficult to deploy</td>
</tr>
<tr>
<td>Support Technology Lifetime</td>
<td>3-5 years</td>
<td>Up to 20 years</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Common/widely used</td>
<td>Rarely used (vendor only)</td>
</tr>
<tr>
<td>Application of Patches</td>
<td>Regular/scheduled</td>
<td>Slow (vendor specific)</td>
</tr>
<tr>
<td>Change Management</td>
<td>Regular/scheduled</td>
<td>Legacy based – unsuitable for modern security</td>
</tr>
<tr>
<td>Time Critical Content</td>
<td>Delays are usually accepted</td>
<td>Critical due to safety</td>
</tr>
<tr>
<td>Availability</td>
<td>Delays are usually accepted</td>
<td>24 x 7 x 365 x forever</td>
</tr>
<tr>
<td>Security Awareness</td>
<td>Good in private and public sector</td>
<td>Generally poor regarding cybersecurity</td>
</tr>
<tr>
<td>Security Testing/Audit</td>
<td>Scheduled and mandated</td>
<td>Occasional testing for outages / audit</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Secure</td>
<td>Remote and unmanned</td>
</tr>
</tbody>
</table>

Source: Volpe
Myth Buster: “Control system cybersecurity is the same as IT cybersecurity.”

“[The] logic executing in ICS has a direct effect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment”

Cybersecurity is generally the responsibility of IT personnel. Control systems are usually the responsibility of engineering and operations personnel.

Critical to foster closer communication between the IT, engineering and operations groups.
Disparate institutional, cultural and organizational domains collide
Ernest “Ron” Frazier, CASE™, LLC

CYBERSECURITY RISK
Cybersecurity Risk

Risk of intentional cyber attack by criminals, hackivists, terrorists, hostile nation-states, or individuals seeking recognition has become a top priority for governments and private industry world-wide.

Coupled with unintentional acts or disruptions caused by natural events, securing transportation critical infrastructure and the control systems associated with that infrastructure becomes more daunting day by day.
System Vulnerabilities

Inherent openness and accessibility of transportation systems creates significant opportunities to penetrate, commandeer or otherwise neutralize the effectiveness or security of cyber systems.

Backdoors and “Holes” (Intentional or Not) in Network Perimeter Devices with Little/No Security (Modems, Legacy Control Devices)
Protocol Vulnerabilities
Physical Vulnerability of Field Devices
Communication Hijacking and Man-in-the Middle (MitM) Attacks
Inadequate or nonexistent patching of software and firmware
Inadequate security procedures for internal AND external personnel
Lack of control systems specific mitigation technologies
Myth Buster: “It won’t happen to us.”
There have been many reported cyber incidents in transportation already.
Managing cyber risks can prove to be intractably challenging

Known issues are growing.
- 50,000+ recorded vulnerabilities with more added hourly
- 86,000 new malware reported each day

Breaches are hard to detect.
- 229 days average time to detect breach
Cybersecurity Risk Dependency

Coordinated collaboration among all stakeholders

Designers & manufacturers
Equipment suppliers
System integrators
University & government researchers
Testing organizations
Users
Infrastructure operators
Standards organizations
Regulators
Risk Transfer And Acceptance

Insurer identified cloud computing as major liability concern.

ISSUES
Lack of clarity about who’s responsible for what losses in the cloud.

Cloud service providers will not accept liability for data losses.

Aggregation risk is a specific worry - small number of dominant platforms supporting cloud services sets the stage for potentially large losses. If one such platform goes down, thousands of users could be impacted simultaneously.

POTENTIAL IMPACT
Could bankrupt a single carrier who insures a significant percentage of those users overnight. Could give rise to “many, many” claims.
Cybersecurity Risk Management
NIST Framework Information & Decision Flows

Source: NIST Cybersecurity Framework
Cybersecurity Evaluation Tool (CSET®)

Four Step Process

System and Process Evaluation
- Select Standards
- Determine Assurance Level

Network Architecture Evaluation
- Create Control Network Diagram
- Answer Questions


Consequences of a successful cyber attack (SAL 1-5)
Define cyber security zones, critical components and communication conduits
Network topology and security standards

Standard Questions
Weighted Answers
Component Questions
Reports
Case Study - Metropolitan Atlanta Rapid Transit Authority (MARTA)

CSET Assessment
Gap Analysis
Risk Prioritization
Roadmap

<table>
<thead>
<tr>
<th>Administrative</th>
<th>Initial CSET Gaps</th>
<th>Priorities</th>
<th># Related APTA Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policy &amp; Procedures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Program Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Development &amp; Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical &amp; Environment Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System &amp; Information Integrity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Architecture</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System &amp; Communication Protection</td>
<td>16</td>
<td>13</td>
<td>tbd</td>
</tr>
</tbody>
</table>

Priority = Highest Risk Based on Availability, Probability and Severity
Cybersecurity Guidance

Cybersecurity and Critical Infrastructure Policy Frameworks

Executive Order 13636 (EO) Improving Critical Infrastructure Cybersecurity (2013)
NIST Cybersecurity Framework (2014)

Control System Cybersecurity Strategy And Roadmaps

Transportation Industrial Control Systems Cybersecurity Standards Strategy (2012)
A Roadmap to Secure Control Systems in Transportation (2012)

National and International Standards

NIST Special Publications
Organization for Standardization (ISO)
Information Systems Audit and the Control Association (ISACA)
Control Objectives for Information and Related Technology (COBIT)
COUNTERMEASURES

Patricia Bye
Western Management & Consulting LLC
Countermeasures

There are approaches to reduce risks & mitigate impacts. Expert resources & guidance exist to help.

- NIST Framework
- NIST ICS Guide
- COBIT & SANS
- Industry Textbooks & Technical Papers
- DHS & FHWA Resources
- APTA Recommended Practices

https://ics-cert.us-cert.gov/Standards-and-References
With resource constraints it is impossible to do everything

APTA Control Systems Recommended Practices
Defines priorities by security zone classes
Recommends minimum set of controls for zones

<table>
<thead>
<tr>
<th>Importance</th>
<th>Zone</th>
<th>Example System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Critical</td>
<td>Safety Critical Security</td>
<td>Field signaling</td>
</tr>
<tr>
<td></td>
<td>Fire, Life-Safety Security</td>
<td>Fire Detection/suppression</td>
</tr>
<tr>
<td></td>
<td>Operationally Critical</td>
<td>Traffic Management</td>
</tr>
<tr>
<td></td>
<td>Enterprise</td>
<td>HR, Accounting</td>
</tr>
<tr>
<td>Most Public</td>
<td>External</td>
<td>Communications with public, vendors, others</td>
</tr>
</tbody>
</table>
APTA Recommended Practices
Securing Control and Communications Systems

Part I identifies steps to set up a successful cybersecurity program and stages in conducting risk assessment and managing risk. (2010)

Part II defines recommended security zone classifications and minimum set of recommended security controls for the most critical classifications: safety-critical (SCSZ) and FLSZ zones. (2013)

Part IIIa covers the attack modeling procedure for transit agencies and systems integrators and vendors. (2015)
## Model Control & Communication System Categories

<table>
<thead>
<tr>
<th>EXTERNAL ZONE:</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN to other Vendors</td>
<td>V/S</td>
<td>V/S</td>
</tr>
<tr>
<td>VPN to other Agencies</td>
<td>V/S</td>
<td>V/S</td>
</tr>
</tbody>
</table>

### OCC
- Access Control System
- Advertising
- Fare Sales / Collection
- Credit Card Processing
- Logging

### Train station / Station Equipment Room
- Access Control / Intrusion Detection
- Advertising
- Fare Sales / Collection
- Passenger information system
- CCTV

### SIGNAL BUNGALOW – or equivalent
- N/A

### EN
- Dispatch / ATS
- Non-Emergency Voice Communications
- SCADA

### OC
- Traction Power
- PA System – Passenger Information Display
- Vertical Lift Devices
- Tunnel pumping / draining

### OC
- Emergency Ventilation Systems
- Emergency Management Panel
- Fire Detectors / Alarms / Suppression systems
- Safety Critical Physical Intrusion Detection
- Traction Power Emergency Cutoff
- Traction Power Protection Relaying
- Gas Detection
- Mass Notification PA
- Seismic Monitoring

### FL
- Emergency Communications
- Fire Alarm & Suppression Enunciaters
- Fire / Life-Safety, Emergency Ventilation Control
- Status displays

### FL
- Vital Signaling, ATP
- Platform Gate Control

### SC
- Vital Signaling, ATP
- Crossing Gates

### LEGEND
- **EN**: Enterprise Network (Admin, IT, HR)
- **FL**: Fire, Life-Safety Security Zone
- **OC**: Operationally Critical Security Zone (Traction Power)
- **SC**: Safety Critical Security Zone
APTA Recommended Practices
Future Publications

Part III B: Covers the **Operationally Critical Security Zone (OCSZ)**.

Part III c: Application of 3 security zones (SZ) - the Operationally Critical SZ, Fire Line SZ, and Safety Critical SZ - to **rail transit vehicles**.
Cybersecurity Bar Keeps Increasing

Only 3% of breaches require difficult or expensive actions.

- 90% breaches avoided with simple security practices (Symantec/Verizon 2012)
- 96% breaches avoided with intermediate approaches (Symantec/Verizon 2012)
- 97% breaches have been breached (Firefly 2014)

Access Management
Anti-Malware
Firewalls
Defense-In-Depth
Recommended Best Practices

Cyber Hygiene
Access Control
Data Security and Information Protection
Protective Technology
Boundary Defense and Network Separation
Configuration Management
Training
Cyber Hygiene: Basics Matter

Airports Targeted: 75 Impacted, 2 Compromised

Phishing email
Redirect to site
Public document source of phishing emails
Access Control: Cyber and Physical

Vulnerabilities

Legend
- network vulnerabilities
- social engineering weaknesses
- confidential information
- open locks

Physical Access Control
Identification and Authorization Procedures
Password Policies
Boundary Defense and Network Separation
Safety Critical Signaling
Safety Critical Fire
Network Separation: HVAC

55000+ HVACs have known vulnerabilities
Be aware how systems are connected
To Internet
To your network
Myth Buster: “It's possible to eliminate all vulnerabilities in systems.”

It is impossible to achieve perfect security. Cybersecurity today is CYBER RESILIENCE.

According to a recent Cisco Security Report, all of the organizations examined showed evidence of suspicious traffic and that networks had been breached.

More effective strategy is to assume that cybersecurity incidents will happen and focus on mitigating the consequences.
Monitoring and Detection

Critical to monitor, log, and analyze anomalies, successful & attempted intrusions, accidental & unintended incidents.

Challenges
- Too much data
- Too many alerts and false positives
- Incomplete visibility of network & endpoints

Detection-in-Depth is an APTA Recommended Practice

Month to Month Comparison
November 2013 and December 2013

Month to Month Comparison of IT Security Incidents by Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Dec</th>
<th>Nov</th>
<th>% Increase/Decrease from Previous Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized</td>
<td>14,897</td>
<td>2,467</td>
<td>+139%</td>
</tr>
<tr>
<td>Malicious Code</td>
<td>7,869</td>
<td>6,243</td>
<td>+219%</td>
</tr>
<tr>
<td>Improper Usage</td>
<td>79</td>
<td>42</td>
<td>+88%</td>
</tr>
<tr>
<td>Phishing</td>
<td>1,009</td>
<td>549</td>
<td>+84%</td>
</tr>
<tr>
<td>Probes</td>
<td>1,172</td>
<td>1,020</td>
<td>+15%</td>
</tr>
<tr>
<td>Potential Attacks</td>
<td></td>
<td></td>
<td>-13%</td>
</tr>
<tr>
<td>Investigations</td>
<td>14</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

Source: Utah Transit Agency
Response and Recovery

Have a Cyber Response/Recovery Plan. Planning ahead can ensure less damage after an incident.

Develop and TEST plan.

Know who to call.
Threat response/recovery
FHWA & ICS-CERT

FBI if suspect criminal activity

Be prepared to isolate systems & preserve forensic evidence.
Myth Buster: “It’s all about IT.”

“Cybersecurity involves People, Technology, & Process…”

“People, essential in the creation of a cybersecurity culture, are often thought to be the most vulnerable element and therefore require significant attention…”

“Culture is fueled by good basic practices which some describe as Cyber Hygiene and Sustained Awareness by all employees.”

Images: APTA.com
To create a **Cybersecurity Culture**, Management must:

- Establish **policies and procedures**
- Allocate **resources** for *training, awareness and implementation*
- Support and champion **good practices**

**Cybersecurity Learning Continuum**

- Security Awareness
- Cybersecurity Essentials
- Role-Based Training
- Education &/or Experience

→ → *Increasing Knowledge and Skills* → →
## Training and Cybersecurity Culture

<table>
<thead>
<tr>
<th>Cybersecurity Functions</th>
<th>Roles &amp; User Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>All Users &amp; Third Party Stakeholders</td>
</tr>
<tr>
<td>PROTECT</td>
<td>Privileged Users</td>
</tr>
<tr>
<td>DETECT</td>
<td>Managers/Senior Executives</td>
</tr>
<tr>
<td>RESPOND</td>
<td>Training Personnel</td>
</tr>
<tr>
<td>RECOVER</td>
<td>IT/Cybersecurity Personnel</td>
</tr>
<tr>
<td></td>
<td>Physical Security Personnel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NIST Pubs</th>
</tr>
</thead>
<tbody>
<tr>
<td>800-16 Rev 1</td>
</tr>
</tbody>
</table>
Cybersecurity Training Resources

National Initiative for Cybersecurity Careers & Studies (NICCS)
National Initiative for Cybersecurity Education (NICE)
NIST National Cybersecurity Center of Excellence (NCCoE)

NIST Special Publications (SP) on Training

- SP 800-16 Information Technology Security Training Requirements
- SP 800-50 Building an Information Technology Security Awareness & Training Program

DHS/ICS-CERT Courses

- Introduction to Control Systems Cybersecurity (101)
- Intermediate Cybersecurity for Industrial Control Systems (201)
- Intermediate Cybersecurity for Industrial Control Systems (202)
- ICS Cybersecurity (301)

DHS Federal Virtual Training Environment (FedVTE)
Cybersecurity Training Resources

FEMA Emergency Management Institute Courses
• IS-0523 Resilient Accord: Exercising Continuity Plans for Cyber Incidents
• E0553 Resilient Accord Cyber Security Planning Workshop

Information Sharing Sites
• Public Transportation Information Sharing and Analysis Center
  http://www.apta.com/resources/safetyandsecurity/Pages/ISAC.aspx
• Over-the-Road Bus Information Sharing and Analysis Center
• Multi-state-ISAC (MS-ISAC): http://msisac.cisecurity.org/
• Surface Transportation: https://www.surfacetransportationisac.org/
Summary: What Can You Do

Evaluate and manage your organization’s specific cyber risks.

Implement industry standards and effective practices.

Develop and test incident response plans and procedures.

Coordinate cyber security and response planning across the enterprise.

Maintain situational awareness of cyber threats.

Communicate frequently and often.

Pro Tip

• Take a balanced approach.
• Learn from experience.
• Focus on standards.
• Look for efficiencies.
• Provide solutions that add value while being cost effective.
• Understand that you can’t be masters at everything.
• Communicate, communicate, communicate – to users, business partners, vendors, and media.
Thank You

For additional information please contact:

Ron Frazier
ronfrazier@caseexperts.com

Dave Fletcher
fletcher.d@att.net
Questions

- Who
- When
- How
- Why
- What
- Where