NCHRP Research Report 221:
Protection of Transportation Infrastructure from Cyber Attacks: A Primer

NCHRP Project 20-59(48)
NCHRP is a State-Driven Program

- Sponsored by individual state DOTs who
  - Suggest research of national interest
  - Serve on oversight panels that guide the research.
- Administered by TRB in cooperation with the Federal Highway Administration.
Practical, ready-to-use results

- Applied research aimed at state DOT practitioners
- Often become AASHTO standards, specifications, guides, syntheses
- Can be applied in planning, design, construction, operations, maintenance, safety, environment
A range of approaches and products

• Traditional NCHRP reports
• Syntheses of highway practice
• IDEA Program
• Domestic Scan Program
• Quick-Response Research for AASHTO
• Other products to foster implementation:
  - Research Results Digests
  - Legal Research Digests
  - Web-Only Documents and CD-ROMs
Today’s Speakers

- Dave Fletcher, Introduction to the Primer
- Ernest (Ron) Ron Frazier, Cyber Security Risk
- Pat Bye, Countermeasures
- Yuko Nakanishi, The Importance of Cybersecurity Training
- Dave Fletcher, Moderator
INTRODUCTION TO THE PRIMER

Dave Fletcher, GPC, Inc.
Today’s Agenda

Overview of TRB project

Preview of the Primer

Highlight key topics
- Risk Management
- Countermeasures
- Training
TRB Research Project NCHRP 20-59 (48)

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 highway and transit 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
Protection of Transportation Infrastructure from Cyber Attacks: A Primer

• Introduction - The Business Case for Cybersecurity
• Chapter 1 - Top Myths of Transportation Cybersecurity
• Chapter 2 - Cybersecurity Risk Management, Risk Assessment and Asset Evaluation
• Chapter 3 - Cybersecurity Plans and Strategies, Establishing Priorities, Organizing Roles and Responsibilities
• Chapter 4 - Transportation Operations Cyber Systems
• Chapter 5 - Countermeasures: Protection of Operational Systems
• Chapter 6 - Training: Building a Culture of Cybersecurity
• Chapter 7 - Security Programs and Support Frameworks
Today’s Highways are going Cyber
## Cyber Transportation Systems

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Example System (Highways)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations Systems (ICS)</strong></td>
<td>Control Systems</td>
<td>Traffic Management Center</td>
</tr>
<tr>
<td></td>
<td>SCADA</td>
<td>Road/Weather Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Traffic Monitoring and Surveillance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GPS/Vehicle Location Systems</td>
</tr>
<tr>
<td></td>
<td>Signalling</td>
<td>RR Crossing Signals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Highway Signals</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>Traveller Information Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DMS/VMS</td>
</tr>
<tr>
<td></td>
<td>Toll Collection Systems</td>
<td>Electronic Toll Collection (EZ-Pass)</td>
</tr>
<tr>
<td></td>
<td>HVAC</td>
<td>Tunnel Ventilation</td>
</tr>
<tr>
<td></td>
<td>Building Management</td>
<td>Building/Property Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fire Detection/Suppression</td>
</tr>
<tr>
<td><strong>IT Systems</strong></td>
<td>&quot;Retail&quot;</td>
<td>Driver Licences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vehicle Titling and Registration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Crash Reporting</td>
</tr>
<tr>
<td></td>
<td>Business Management</td>
<td>Accounting Systems</td>
</tr>
<tr>
<td><strong>Engineering Systems</strong></td>
<td>Design/Construction</td>
<td>CADD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electronic Bidding</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.”

Critical to facilitate discussion and interaction between the IT, engineering and operational groups.

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

Implementing cybersecurity for transportation control systems requires having a good understanding of security AND the controls systems AND the operational environments.
Disparate institutional, cultural and organizational domains collide

Transportation Professionals

Cybersecurity Professionals

Transportation Cyber Specialists
CYBERSECURITY RISK

Ernest “Ron” Frazier
CASE™, LLC
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 Management

Risk Scenarios

Risk Analysis

Risk Map

Risk Exceeding Risk Appetite

Select Risk Response Options

Risk Response Parameters

- Efficiency of Response
- Exposure
- Response Implementation Capability
- Effectiveness of Response

Risk Responses

Prioritise Risk Responses

Risk Action Plan with Prioritised Risk Responses

Source: COBIT 5 for Risk, the Information Systems Audit and Control Association - www.isaca.org
Cybersecurity Risk Dependency

Coordinated collaboration among all stakeholders

Designers & manufacturers
Equipment suppliers
System integrators
Testing organizations
Users
Infrastructure operators
Standards organizations
Regulators
University & government researchers
Cybersecurity Risk Spreading
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 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.
Cybersecurity Bar Keeps Increasing

Only 3% of breaches require difficult or expensive actions.

90% breaches avoided with simple security practices.

96% breaches avoided with intermediate approaches.

97% have been breached.

Access Management

AntiMalware

Firewalls

Defense-In-Depth
With resource constraints it is impossible to do everything

Example prioritization approach from transit (APTA)

Control Systems Recommended Practices define priorities by security zone classes & recommend minimum set of controls for most critical.

<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>
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: Field Devices

Change default passwords on field devices.
Ramp/Gate/Signal Controllers
Fixed Dynamic Message Signs
Portable Dynamic Message Signs

FHWA & ICS-CERT:
Change default password to strong one
Place displays on private networks
Disable telnet, webpage, and web LCD interfaces if not needed.
Boundary Defense and Network Separation
Boundary Defense and Network Separation
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 SURVIVABILITY.

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

Yuko Nakanishi
Nakanishi Research & Consulting, LLC
Myth Buster: “It’s all about IT.”
People, processes & technology are key to cybersecurity.

Fostering a CYBERSECURITY CULTURE goes a long way towards preventing and mitigating cyber incidents.

There are parallels to safety. A cybersecurity culture is an environment in which cybersecurity best practices are a way of life.

Awareness and training along with established security policies and procedures are important aspects of building cybersecurity culture.

Requires active management support in a visible manner.
Importance of Cybersecurity Training

Importance of training for security and safety within transportation agencies is well-understood.

Insufficiently trained personnel are often the weakest security link in organization’s security.
Cybersecurity Learning Continuum

NIST Framework includes Awareness & Training as component of the Protect function.
All users need awareness education.
Only certain positions require role- and/or responsibility-specific training.

Source: NIST SP 800-16, Revision 1 (Third Draft) October, 2014
Cybersecurity Training Resources

National Initiative for Cybersecurity Careers and Studies (NICCS)

National Initiative for Cybersecurity Education (NICE)

DHS Cybersecurity Education and Awareness

Cyber Resilience Review (CRR) – Resource Guide on Training and Awareness
Cybersecurity Training Resources

NIST Special Publications (SP) on Training

SP 800-16 A Role-Based Model for Federal Information Technology/Cybersecurity Training, Revision 1 (Third Draft, 2014)
SP 800-50 Building an Information Technology Security Awareness and Training Program (2003)
SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (2006)

DHS/ICS-CERT Courses

Introduction to Control Systems Cybersecurity (101) – available online
Intermediate Cybersecurity for Industrial Control Systems (201) – lecture
Intermediate Cybersecurity for Industrial Control Systems (202) – lecture/lab
ICS Cybersecurity (301) – hands-on 5 days course
Cybersecurity Training Resources

FEMA EMI Courses
- IS-0523 Resilient Accord—Exercising Continuity Plans for Cyber Incidents
- E0553 Resilient Accord Cyber Security Planning Workshop

Consortium for ITS Training and Education (CITE)
- Cyber Security, Connected Vehicle/Automated Vehicle, etc.

Software Engineering Institute (SEI) Institute
- Cyber-Physical Systems, Risk Management, etc.

NAS/TRB Resources
- NCHRP/ACRP/TCRP Reports
- TRB Subcommittee on Cybersecurity
- TRB Cybersecurity Resource Center
- NAS Cyber Physical Systems Study
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

• Have 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.
Ways to Get Involved

- TRB Subcommittee on Cybersecurity
  https://sites.google.com/site/abe406cybersecurity

- TRB Cybersecurity Resource Center
  http://trbcybersecurity.erau.edu/index.html

- APTA Security Programs
  - Peer Review Panels
  - Standards Program
  - Emergency Response Preparedness Program (ERPP)
  - Information Sharing & Analysis Center (PT-ISAC)
  - TCRP Publications on Transit Security
    http://www.apta.com/resources/safetyandsecurity/Pages/securityresources.aspx
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