The Need for Operational and Cyber Resilience in Transportation Systems

January 14, 2016

Dr. Nader Mehravari, MBCP, MBCI

Cyber Risk and Resilience Management
Software Engineering Institute
Carnegie Mellon University
nmehravari@sei.cmu.edu
http://www.cert.org/resilience/
Notices

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0003164
Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT Division – *Anticipating and solving our nation’s cybersecurity challenges*

- Largest technical program at SEI
- Focused on internet security, secure systems, operational resilience, and coordinated response to security issues
Cyber Risk & Resilience Management Team

Engaged in

• Applied research
• Education & training
• Putting into practice
• Enabling our federal, state, and commercial partners

In areas dealing with

• Resilience Management
• Operation Risk Management
• Cyber and Resilience Frameworks
• Integration of cybersecurity, business continuity, & disaster recovery
## Contents

Operational Stress

Cyber-Induced Operational Stress on Transportation Sector

Prevention is Futile

Operational Resilience & Cyber Resilience

Techniques for Improving and Managing Cyber Resilience

Summary
What do you see here?

A set of well looking evergreens.
Look Again!

A tree under operational stress
Operational Stress

- **Natural or Manmade**
- **Accidental or Intentional**
- **Small or Large**
- **Kinetic of Cyber**
- **Information Technology or Not**

- Fire
- Flooding
- IT failures
- Earthquakes
- Cyber attacks
- Severe weather
- Network failures
- Technology failures
- Organizational changes
- Loss of service provider
- Strikes or other labor actions
- Loss of customer or trading partner
- Chemical, biological, nuclear hazards
- Unavailability of workforce
- Failed internal processes
- Supply chain disruption
- Employee kidnappings
- Workplace violence
- Data corruption
- Product failure
- Power outages
- Civil unrest
- Terrorism
- Fraud
- Etc.

...through which risks are realized

Result in

Interruption of Business Mission

Today's Discussion
Examples of Cyber-Induced Operational Stress on Transportation Sector
AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT
THIS HACKER’S TINY DEVICE UNLOCKS CARS AND OPENS GARAGES

THE NEXT TIME you press your wireless key fob to unlock your car, if you find that it doesn’t beep until the second try, the issue may not be a technical glitch. Instead, a hacker like Samy Kamkar may be using a clever radio hack to intercept and record your wireless key’s command. And when that hacker walks up to your vehicle a few minutes, hours, or days later, it won’t even take those two button presses to get inside.
Hackers Cut a Corvette's Brakes Via a Common Car Gadget

Researchers wirelessly hack a Corvette's brakes using an insurance dongle

The company has patched the fix, but the hack could be used on other cars
January 2008

The Register®

SECURITY

Polish teen derails tram after hacking train network

Turns city network into Hornby set

By John Leyden, 11 Jan 2008  Follow  3,007 followers

A Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles in the process. Two people were injured in one of the incidents.
January 2012

Hackers Breached Railway Network, Disrupted Service

BY KIM ZETTER 01.24.12 | 11:15 AM | PERMALINK

Homeland Security News Wire

Transportation security
Hackers attack U.S. railways
Published 25 January 2012

Last month hackers took control of passenger rail lines in the Northwest, disrupting signals twice and creating delays

This story has been updated with new information from the railroad industry and to clearly state the industry’s contention that the TSA memo was inaccurate.

Hackers, possibly from abroad, executed...
They tested the app's success on two transit systems, the New Jersey Path and San Francisco Muni trains. Benninger and Sobell said that other systems might be vulnerable to such an exploit, in the form of an Android application that could make it possible for holders of a card to get free rides in Boston, Seattle, Salt Lake City, Chicago, and Philadelphia. Those other systems were not tested by the researchers.
Trains Vulnerable to Hacker Attacks: Researchers

By Eduard Kovacs on December 29, 2015
To Move Drugs, Traffickers Are Hacking Shipping Containers

October 21, 2013 // 06:45 PM CET

The scheme sounds like a work of near science fiction. But police in the Netherlands and Belgium insist its true, and say they have the evidence to prove it: two tons of cocaine and heroin, a machine gun, a suitcase stuffed with $1.7 million, and hard drive cases turned into hacking devices.
Coast Guard official: Cyber incidents with physical consequences impacting the maritime transportation system

October 13, 2015 | By Molly Bernhart Walker

"We have already seen incidents in the maritime transportation system that have resulted in physical consequences or significant near misses," said Thomas during an Oct. 8 House Homeland Security Committee hearing.

"In some cases, it would appear that these were intentional actions, perhaps by actors with malicious intent, but in other cases they were clearly accidents caused by improper use or maintenance of cyber systems," he said.
Cyber-attack concerns raised over Boeing 787 chip's 'back door'

Researchers claim chip used in military systems and civilian aircraft has built-in function that could let in hackers
Hacked X-Rays Could Slip Guns Past Airport Security

BY KIM ZETTER 02.11.14 6:30 AM

PUNTA CANA, Dominican Republic — Could a threat-simulation feature found in airports around the country be subverted to mask weapons or other contraband hidden in a traveler’s luggage? The answer is yes, according to two security researchers with a history of discovering holes in airport systems, who purchased their own x-ray control machine online and spent months analyzing its workings.

The researchers, Billy Rios and Terry McCorkle, say the so-called Threat Image Project could someday backfire.
Hacker says to show passenger jets at risk of cyber attack

BY JIM FINKLE
BOSTON | Mon Aug 4, 2014 5:39pm IST

(Reuters) - Cyber security researcher Ruben Santamarta says he has figured out how to hack the satellite communications equipment on passenger jets through their WiFi and inflight entertainment systems - a claim that, if confirmed, could prompt a review of aircraft security.

Santamarta, a consultant with cyber security firm IOActive, is scheduled to lay out the technical details of his research at this week’s Black Hat hacking conference in Las Vegas, an annual convention where thousands of hackers and security experts meet to discuss emerging cyber threats and improve security measures.
Alleged Airline Hack May Expose Transit Vulnerabilities

By MEGHAN KENEALLY • May 18, 2015, 4:13 PM ET

FBI Investigating Claim Computer Expert Hacked Plane In-Flight

By ABC NEWS • May 17, 2015, 3:17 PM ET
Researchers wirelessly hack a Corvette's brakes using an insurance dongle. The company has patched the fix, but the hack could be used on other cars.

Polish teen details train after hacking train network.

Not far: Hacker app resets subway card for free rides.

Trains vulnerable to hacker attacks: Researchers.

FBI investigating claim computer expert hacked plane in-flight.

Cyber-attack concerns raised over Boeing 787 chip's 'back door.'

Hacked X-Rays could slip guns past airport security.

Hacker says he showed passenger jets at risk of cyber attack.
Discussion is Applicable to All Subsectors
Discussion is Applicable to…

<table>
<thead>
<tr>
<th><strong>Transportation Subsectors</strong></th>
<th><strong>Primary Units of Transportation</strong></th>
<th><strong>Modes of Transportation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation</td>
<td>People &amp; Goods</td>
<td>Air</td>
</tr>
<tr>
<td>Highway Infrastructure &amp; Motor Carrier</td>
<td>People &amp; Goods</td>
<td>Ground</td>
</tr>
<tr>
<td>Maritime Transportation Systems</td>
<td>People &amp; Goods</td>
<td>Sea</td>
</tr>
<tr>
<td>Mass Transit &amp; Passenger Rail</td>
<td>People</td>
<td>Ground</td>
</tr>
<tr>
<td>Pipeline Systems</td>
<td>Oil &amp; Gas</td>
<td>Ground</td>
</tr>
<tr>
<td>Freight Rail</td>
<td>Goods</td>
<td>Ground</td>
</tr>
<tr>
<td>Postal &amp; Shipping</td>
<td>Mailpieces &amp; Goods</td>
<td>Air, Ground, Sea</td>
</tr>
</tbody>
</table>
Prevention is Futile
Cyber Intrusions are a Fact of Life
Traditional Information Security Function

- Protect / Shield / Defend / Prevent

- Is necessary
- Is not Sufficient
- Fails too frequently
Operational and Cyber Resilience
An Operationally Resilient Entity?

A tree under operational stress…
…while achieving its “business” mission
Operational Resilience

The **emergent** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

The ability of an entity to

- Prevent disruptions from occurring;
- And when struck by a disruption, the ability to quickly respond to and recover from a disruption in the primary business processes.
Sample Techniques for Improving and Managing Cyber Resilience
Organizational Aspects

How should organizational structures, roles, and responsibilities be adapted?

Example:

- “Traditional” vs. “Modern” information security functions
Modern Information Security Functions

- Protect / Shield / Defend / Prevent
- Monitor / Detect / Hunt
- Respond / Recover / Sustain

Management, Governance, Compliance, Education, Risk Management.
Operational Risk Aspects

How should organizations adapt their overall operational risk management principles and practices?

Example:

- Integration and convergence of operational risk management activities.
Today’s Operational Risk Management

- Health & Safety
  - Continuity of Operation (COOP)
  - Contingency Planning
- Crisis Communications
  - Crisis Management
- Business Continuity
- Preparedness Planning
- Emergency Management
- IT Operations
- Operational Risk Management
- Information Security
  - IT Disaster Recovery
  - Cyber Protection
  - Supply Chain Continuity
- Workforce Continuity
- Pandemic Planning
- Privacy
- Enterprise Risk Management
- Risk Management
- Supply Chain Continuity
  - Pandemic Planning
  - Workforce Continuity
  - Cyber Protection
  - Information Security
  - IT Operations
Desired Solution Approach

Operational Resilience

- Health & Safety
  - Continuity of Operation (COOP)
  - Contingency Planning
- Cyber Protection
  - Supply Chain Continuity
- Information Security
  - Preparedness Planning
  - Risk Management
- IT Disaster Recovery
  - IT Operations
  - Operational Risk Management
- Business Continuity
  - Crisis Communications
  - Crisis Management
- Emergency Management
  - Pandemic Planning
  - Enterprise Risk Management
- Workforce Continuity
  - Workforce Continuity
  - Supply Chain Continuity
- Privacy
  - Privacy

Enterprise Risk Management

Operational Risk Management

Physical Security

Crisis Management

IT Operations

Information Security

IT Disaster Recovery

Health & Safety

Emergency Management

Workforce Continuity

Certification Board

Software Engineering Institute

Carnegie Mellon University

© 2016 Carnegie Mellon University

Distribution Statement (A-F)
Tools and Techniques Aspects

What structured (i.e., not ad hoc) **frameworks** could guide and assist organizations?

**Example:**

- Resilience Management Model
What is Resilience Management Model?

Framework for managing and improving operational resilience

Guides implementation, mgmt, and sustainment of operational risk management activities

Improves confidence in how an organization manages and responds to operational stress

Focuses on “What” not “How”

Applicable to a variety of organizations
  - small or large
  - simple or complex
  - public or private

“…an extensive super-set of the things an organization could do to be more resilient.”
  - CERT-RMM adopter
A Sampling of RMM Success Stories
In Closing
Sampling of ITS Emerging Capabilities

**Convenience, Comfort, & Entertainment**
- Keyless entry
- Remote engine start
- Mobile device integration
- Infotainment

**Smart Transportation**
- Vehicle-to-infrastructure communications
- Smart intersection
- Traffic light control
- Collision avoidance
- Traffic management.

**Advanced Driver Assistant Systems (ADAS)**
- Smart lighting control
- Adaptive cruise control
- Lane departure warning
- Parking assist

**Autonomous Driving**

**Advanced fleet Management**
- Real-time telematics
- Driver fatigue detection
- Package tracking.

**Diagnostics & Maintainability**
- On-Board Diagnostics
- Software update in the garage
- Tire Pressure Monitoring

Etc., Etc., Etc. …
Commonalities in Emerging Capabilities

Convenience, Comfort, & Entertainment
- Keyless entry
- Remote engine start
- Mobile device integration
- Infotainment

Smart Transportation
- Vehicle-to-infrastructure communications
- Smart intersection
- Traffic light control
- Collision avoidance
- Traffic management

Diagnostics & Maintainability
- On-Board Diagnostics
- Software update in the garage
- Tire Pressure Monitoring

Advanced Driver Assistant Systems (ADAS)
- Smart lighting control
- Adaptive cruise control
- Lane departure warning
- Parking assist

Autonomous Driving

Advanced fleet Management
- Real-time telematics
- Driver fatigue detection
- Package tracking

Commonalities?

Information Technology & Communication Technology
Primary Risks to Common Elements

Intentional

Cybersecurity

Accidental

Design Flaws

Component Failures

Information Technology

&

Communication Technology

Component Failures
Cyber Risk Mitigation Challenge

Traditional IT cybersecurity contingencies are not feasible

- Failover over to a disaster recovery site
- Restoring from backup
- Failover to another vehicle
- Federal Motor Vehicle Safety Standards (FMVSS) timeframes precludes “Patch Tuesdays.”
- Can’t call a breach response team (AAA does not do that yet)

Successful management of cyber risk within ITS may require a (significant) shift in thinking and approach.
Promising and Proven Approach

Cyber Resilience Management
Thank you for your attention.
References


