



The Need for Cyber Resilience in Intelligent Transpiration Systems

September 24, 2015

Dr. Nader Mehravari, MBCP, MBCI

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



Contents

Operational Stress

Cyber-Induced Operational Stress on Transportation Sector

Prevention is Futile

Resilience & Cyber Resilience

Investing in Techniques for Improving and Managing Cyber Resilience

What do you see here?



A set of well looking evergreens.

Look Again!



A tree under **operational stress**

Operational Stress



Examples of Cyber-Induced Operational Stress on Transportation Sector

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. Ten people were injured in one of the incidents.

January 2012

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION

Hackers Breached Railway Network, Disrupted Service

BY KIM ZETTER 01.24.12 | 11:15 AM | PERMALINK

HACKERS MANIPULATED RAILWAY COMPUTERS, TSA MEMO SAYS



Lenny Ignelzi/AP File

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 an attack on a Northwest rail company's computers that disrupted railway signals for

Not fare: Hacker app resets subway card for free rides

Sep 23, 2012 by [Nancy Owano](#) [report](#)



They tested the app's success on two transit systems, **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,

To Move Drugs, Traffickers Are Hacking Shipping Containers

October 21, 2013 // 06:45 PM CET



The port of Antwerp. Flickr ([Dominic Sommers](#))

The scheme sounds like a work of near science fiction. But police in the Netherlands and Belgium insist it's 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.

February 11, 2014

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY

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 airport security systems 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 flaws in security 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 Projection](#) system is a [someday hackfire](#).

August 4, 2014



 **REUTERS** EDITION: IN ▼ SIG

HOME BUSINESS ▼ MARKETS ▼ INDIA ▼ WORLD ▼ TECH ▼ OPINION ▼ BREAKINGVIEWS ▼

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.

July 21, 2015

WIRED After Jeep Hack, Chrysler Recalls 1.4M Vehicles for ... SUBSCRIBE

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX



WIRED Hackers Remotely Kill a Jeep on the Highway—With ... SUBSCRIBE

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

August 11, 2015

A screenshot of a Wired article header with a torn paper effect. The Wired logo is on the left, followed by the article title "Hackers Cut a Corvette's Brakes Via a Common Car ...". On the right, there is a "SUBSCRIBE" button and a search icon. Below the title, the author "ANDY GREENBERG" is listed along with "SECURITY 08.11.15 7:00 AM". The main headline is "HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET".

WIRED Hackers Cut a Corvette's Brakes Via a Common Car ... **SUBSCRIBE** 🔍

ANDY GREENBERG SECURITY 08.11.15 7:00 AM

HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET

The Verge logo, consisting of a red square with a white hamburger menu icon on the left and the text "THE VERGE" in white on the right.

☰ **THE VERGE**

A snippet of a The Verge article with a torn paper effect. The main headline is "Researchers wirelessly hack a Corvette's brakes using an insurance dongle". Below it is a sub-headline in italics: "The company has patched the fix, but the hack could be used on other cars".

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

Prevention is Futile



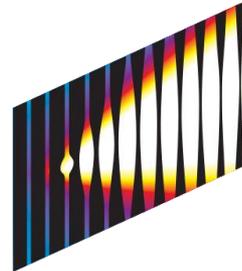
Cyber Intrusions are a Fact of Life

]HackingTeam[

ASHLEY
MADISON®
Life is short. Have an affair.®



UCLA Health System



U B E R



SONY
PICTURES



JPMORGAN CHASE & CO.



Forbes



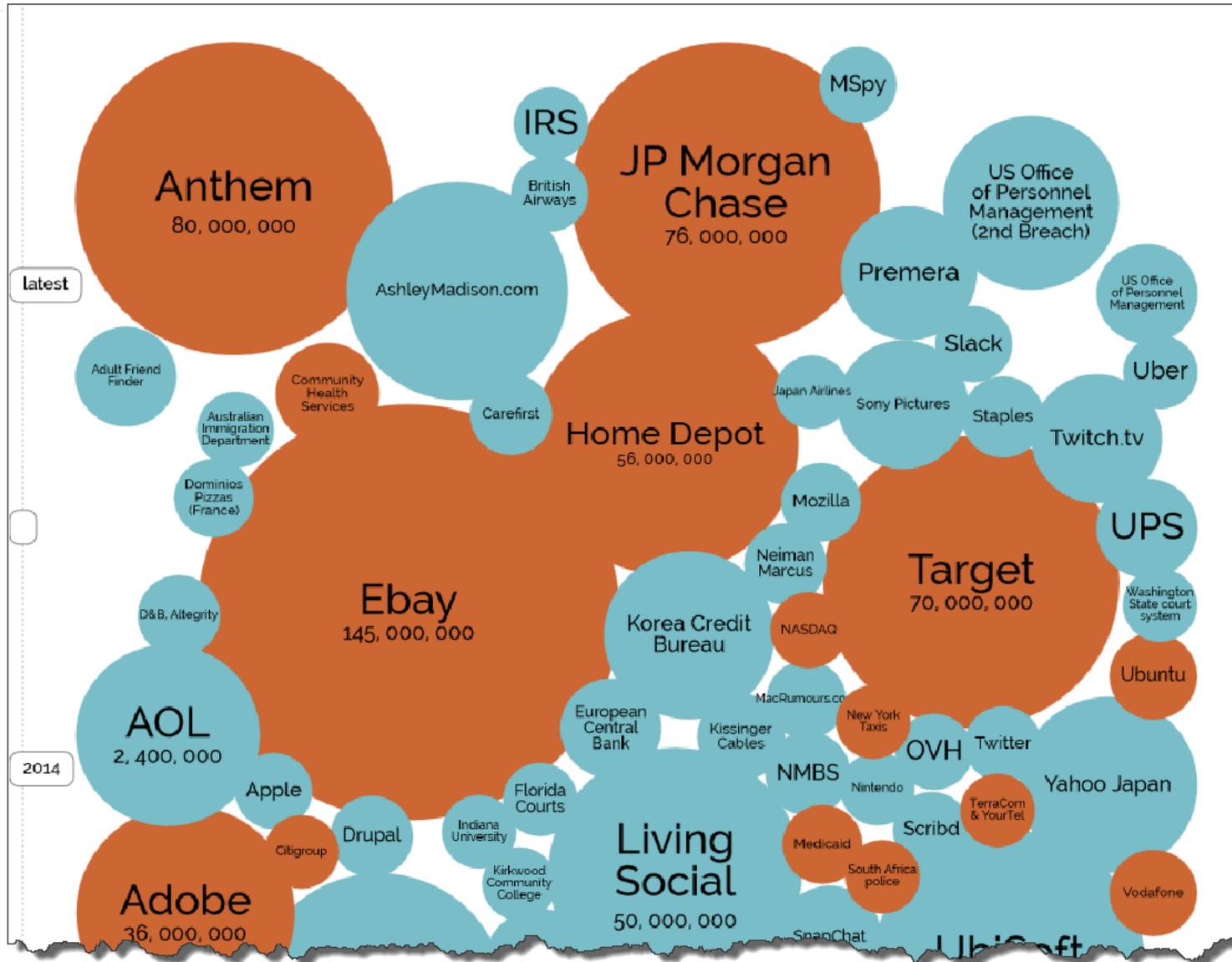
Anthem®

ebay

ToysRUs



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



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.



Investing in Techniques for Improving and Managing Cyber Resilience

Organizational Aspects

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

Example:

- “Traditional” vs. “Modern” chief information security officer (CISO)

Modern Information Security Functions

**Protect / Shield /
Defend / Prevent**



Monitor / Detect / Hunt



**Respond/ Recover /
Sustain**



**Management,
Governance,
Compliance,
Education,
Risk Management.**



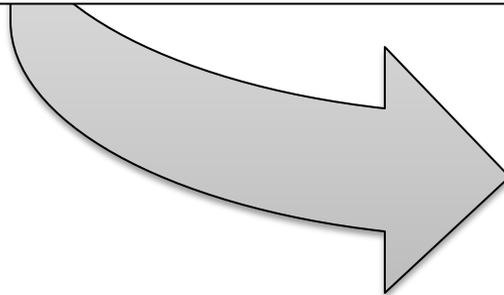
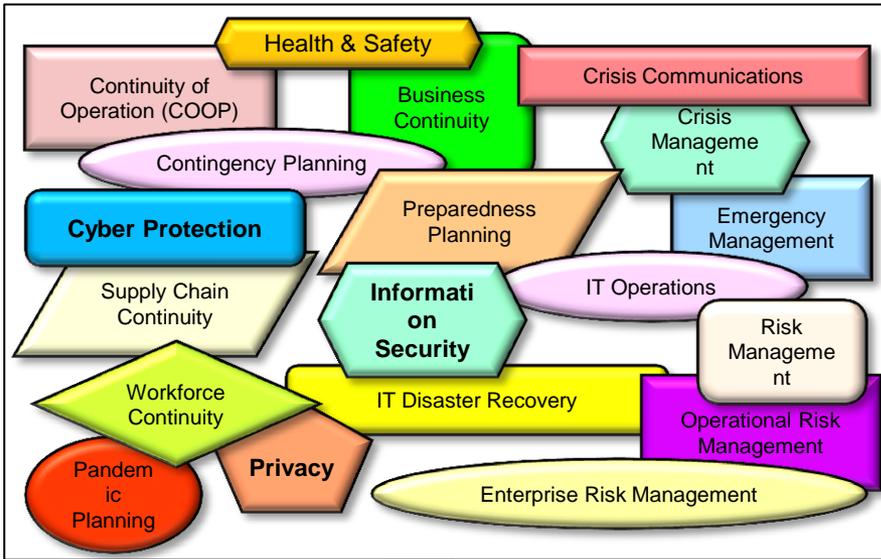
Operational Risk Aspects

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

Example:

- Integration and convergence of operational risk management activities.

Desired Solution Approach



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

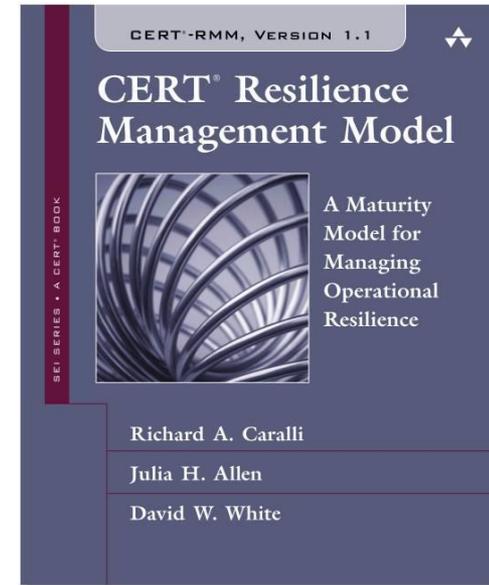
Guides implementation, mgmt, and sustainment of operational risk management activities

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



Thank you for your attention.

References

1. J. H. Allen, R. H. Caralli, and D. W. White, *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*, Addison-Wesley Professional, 2010.
2. N. Mehravari, J. Allen, P. Curtis, and G. Crabb, "A Proven Method for Identifying Security Gaps in International Postal and Transportation Critical Infrastructure," *93rd Annual Transportation Research Board Conference*, Washington, DC, January 13-18, 2014.
3. N. Mehravari, J. Allen, P. Curtis, and G. Crabb, "Improving the Security and Resilience of U.S. Postal Service Mail Products and Services," *93rd Annual Transportation Research Board Conference*, Washington, DC, January 13-18, 2014.
4. N. Mehravari, "Cybersecurity Update," a lecture as part of the Business Continuity and Crisis Management Summer School, Massachusetts Institute of Technology, July 2015.
5. N. Mehravari, "Cyber and Operational Resilience Management," half-day tutorial, planned for *2015 IEEE Military Communications Conference (MILCOM'15)*, Tampa, FL, October 26-28, 2015.
6. N. Mehravari, "Principles and Practice of Operational Resilience," half-day tutorial, *IEEE Systems Conference*, Vancouver, BC, April 12-16, 2015.
7. N. Mehravari, "Information Resilience in Today's High-Risk Economy," *Software Engineering Institute Blog*, November 17, 2014.

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.

This material has been approved for public release and unlimited 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-0002783