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

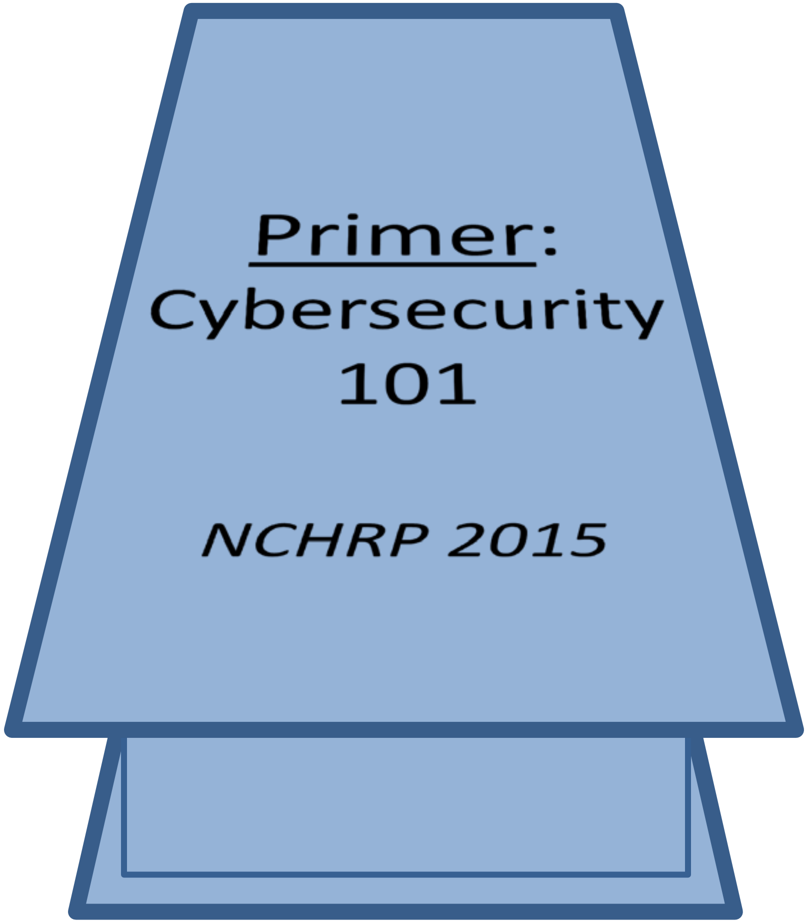
Today’s Agenda

Overview of the research

Preview research results

Highlight best practice & approaches

- Risk Management
- Security Programs
- Countermeasures
- Training



Primer:
Cybersecurity
101

NCHRP 2015

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

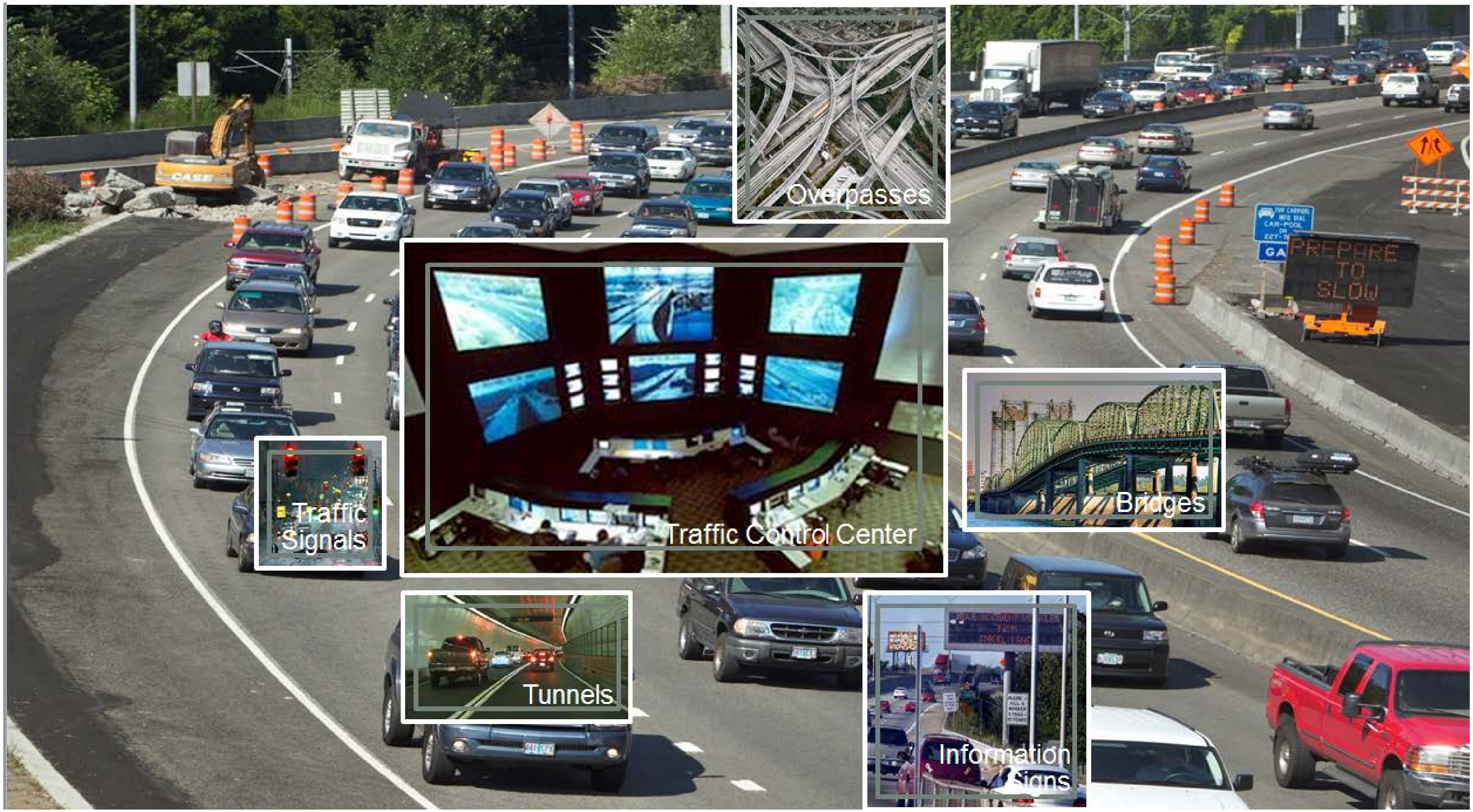
- Both transit and highway operations
- All transportation systems - industrial control, transportation control and enterprise data systems

Deliverables

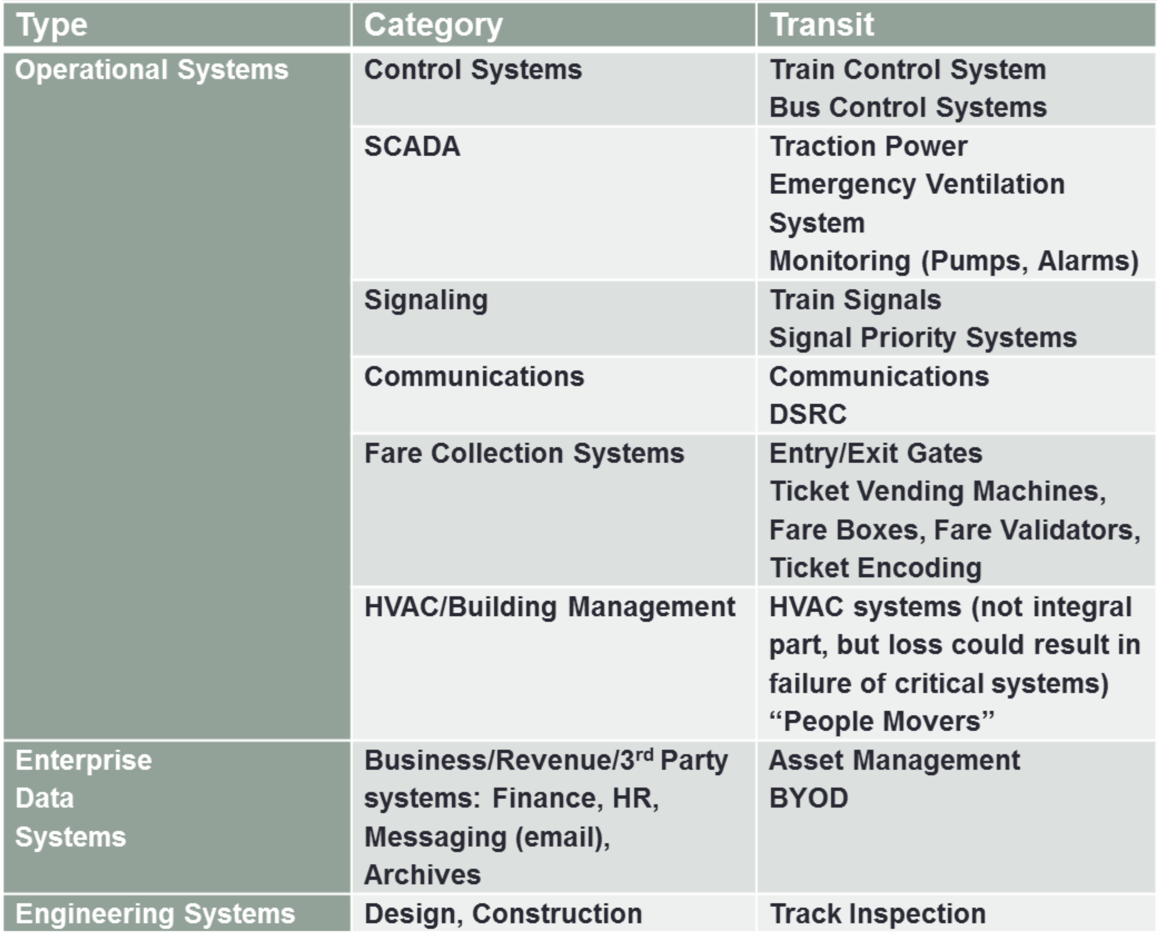
- Executive Briefing template to awareness
- Cybersecurity Primer with best practices for operations

Today’s transit systems are cyber

Today’s highways are going cyber



Cyber Transportation Systems
Control systems and IT systems



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

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

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

Source: Volpe

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

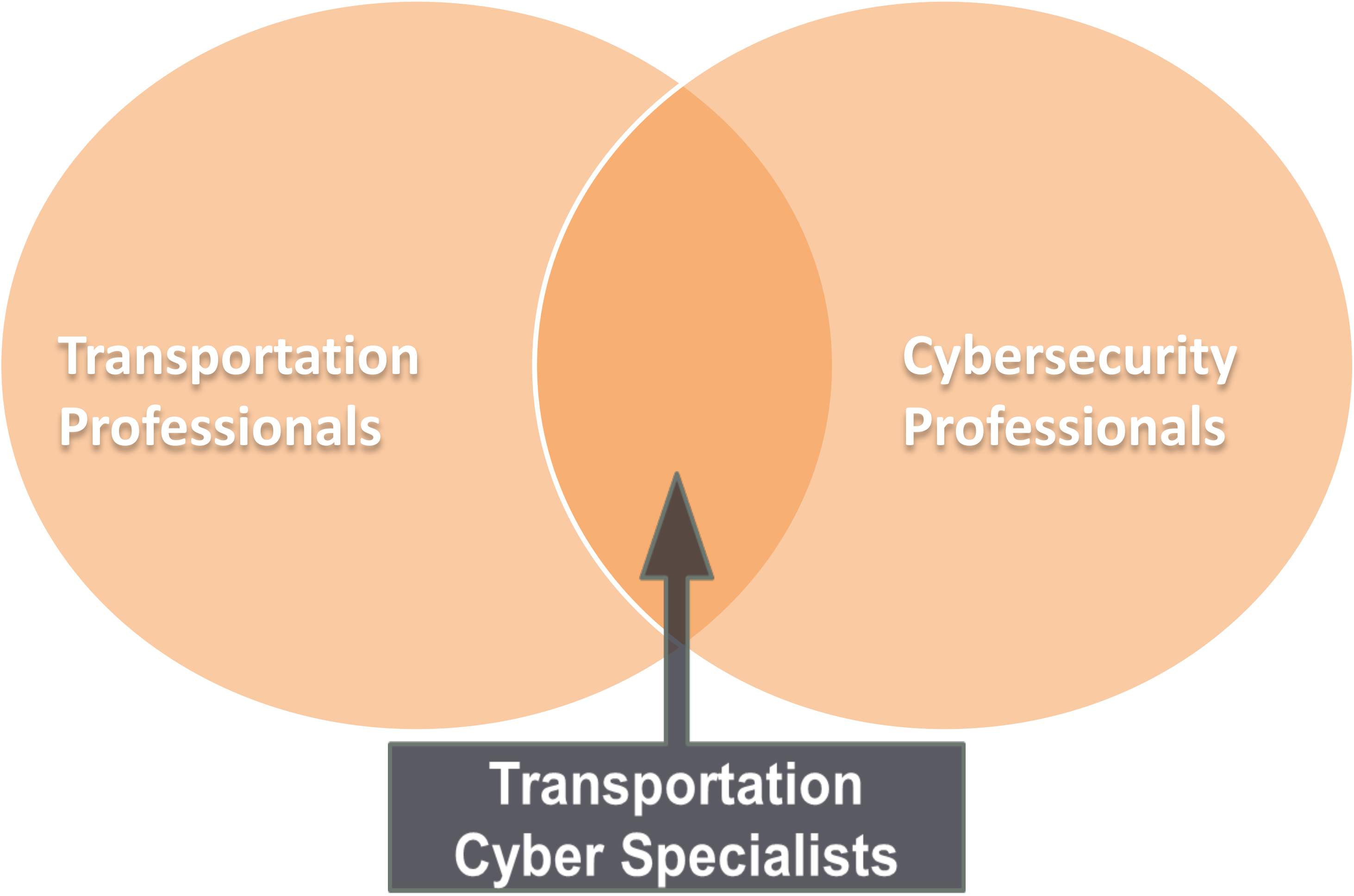
“[The] logic executing in ICS has a direct effect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment”

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


Transportation Professionals
Cybersecurity Professionals
Transportation Cyber Specialists

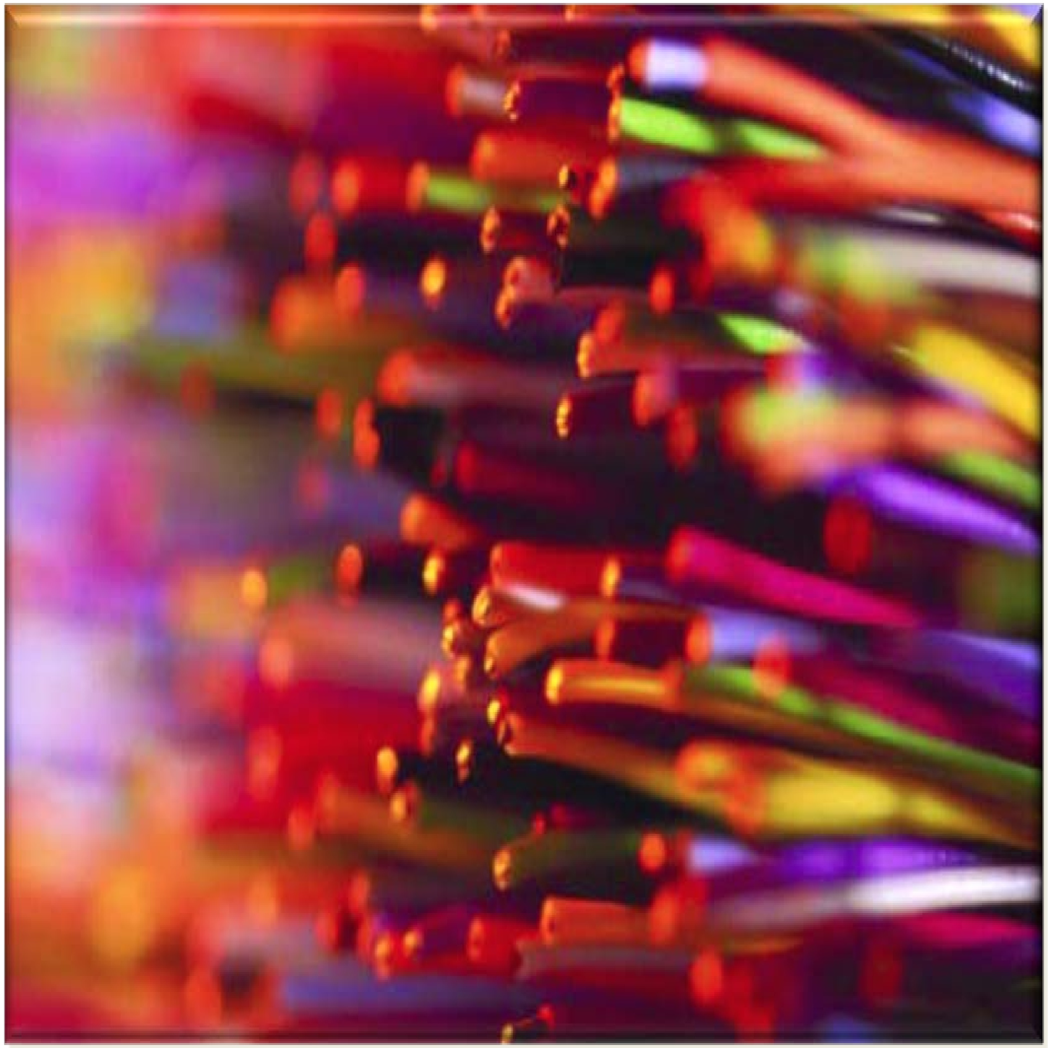
Ernest “Ron” Frazier,
CASE™, LLC

CYBERSECURITY RISK

Cybersecurity Risk

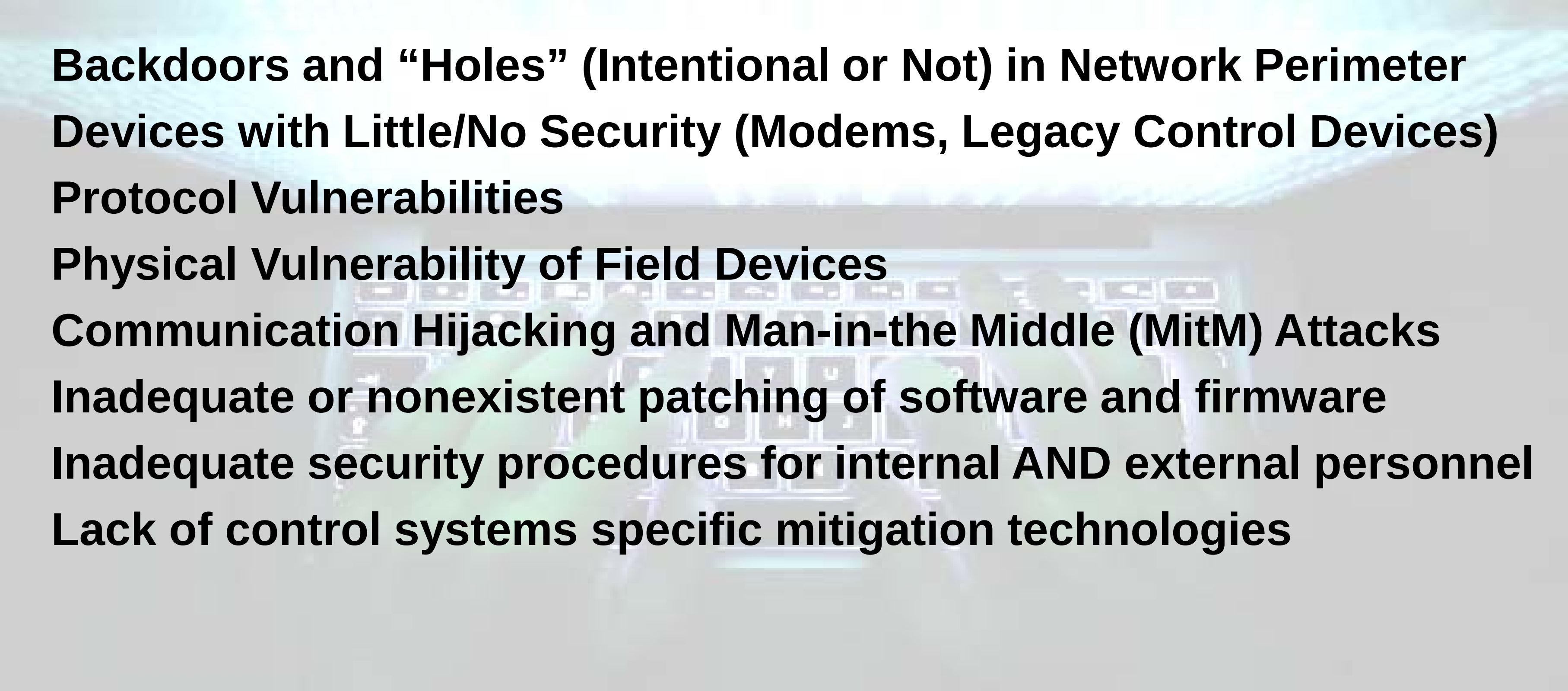
Risk of intentional cyber attack by criminals, hackivists, terrorists, hostile nation-states, or individuals seeking recognition has become a top priority for governments and private industry world-wide.

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.

12:00P 2213 ACELA EXPRESS WASHINGTON DELAYED
12:03P 2250 ACELA EXPRESS BOSTON ON TIME
12:05P 157 REGIONAL R WASHINGTON DELAYED
12:07P 7241 NJCOAST SEC EWR BAYHEAD DELAYED
6923 MID DIRECT SEC DOVER DELAYED
12:13P 7847 NE CORR SEC EWR TRENTON ON TIME
12:55P 145 REGIONAL R WASHINGTON DELAYED
SEC-STOPS AT SECAUCUS EWR-STOPS AT NEWARK-AIRPORT

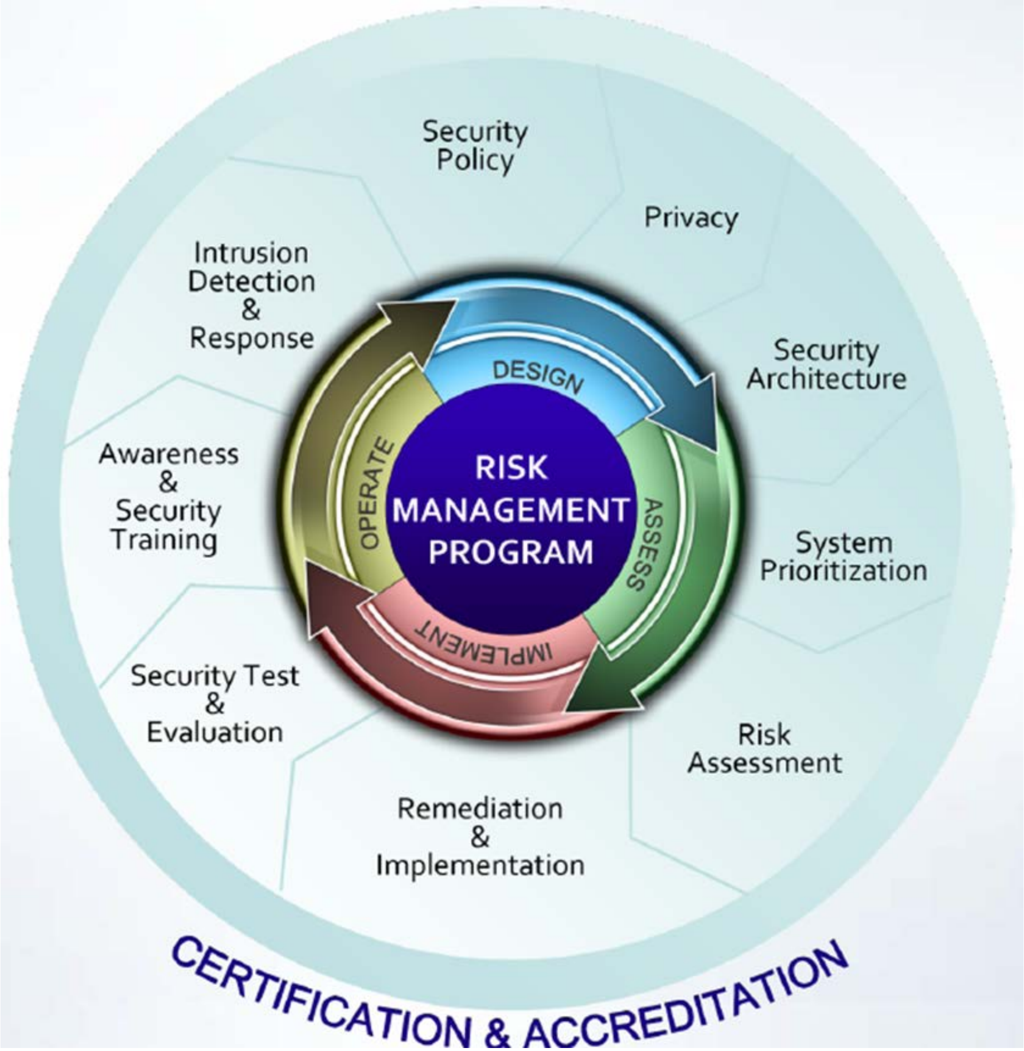
Managing cyber risks can prove to be intractably challenging

Known issues are growing.

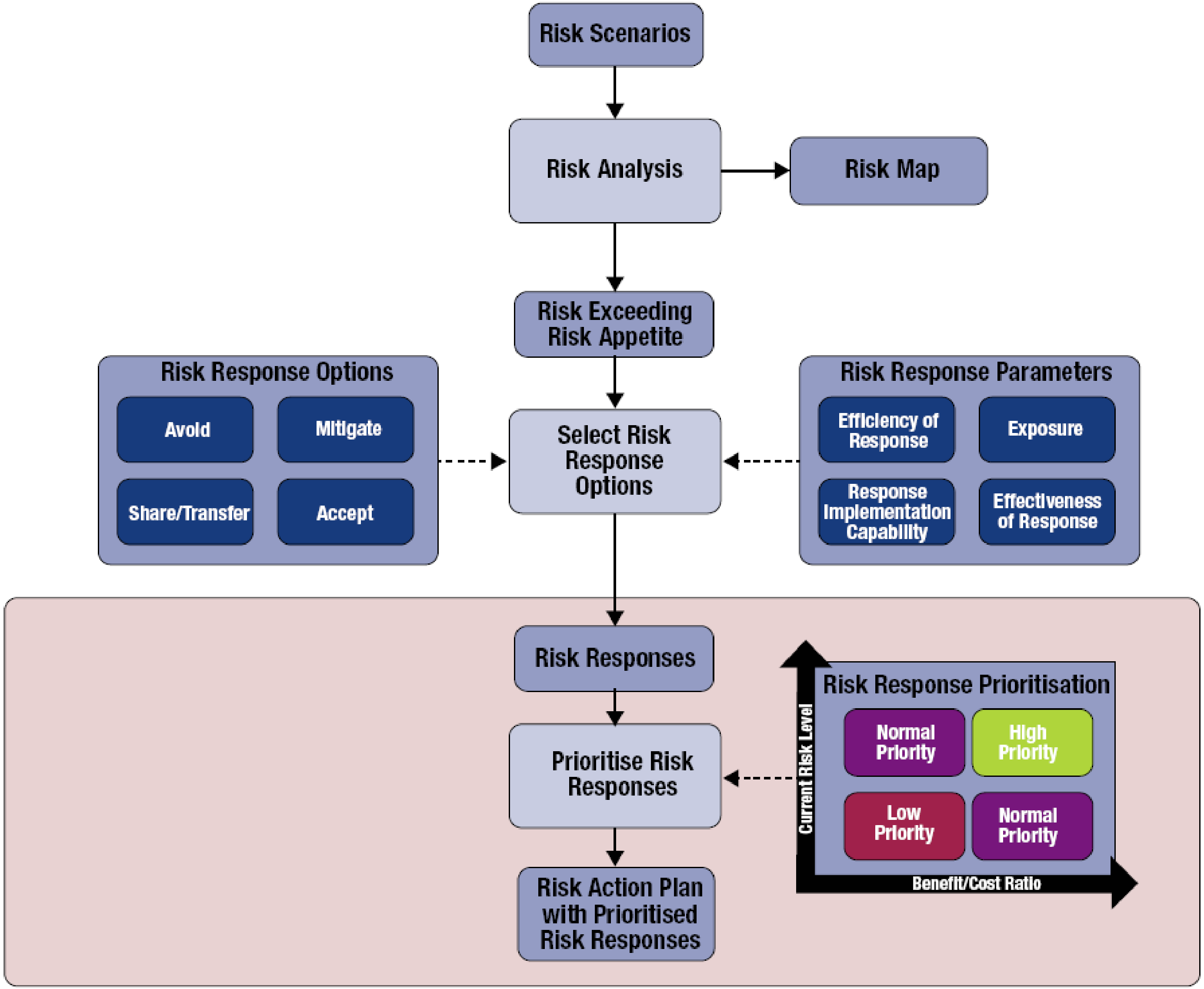
- 50,000+ recorded vulnerabilities with more added hourly
- 86,000 new malware reported each day

Breaches are hard to detect.

- 229 days average time to detect breach


Security Policy
Privacy
Security Architecture
System Prioritization
Risk Assessment
Remediation & Implementation
Security Test & Evaluation
Awareness & Security Training
Intrusion Detection & Response
DESIGN
ASSESS
IMPLEMENT
OPERATE
RISK MANAGEMENT PROGRAM
CERTIFICATION & ACCREDITATION

Cybersecurity Risk Management



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

University & government researchers

Testing organizations

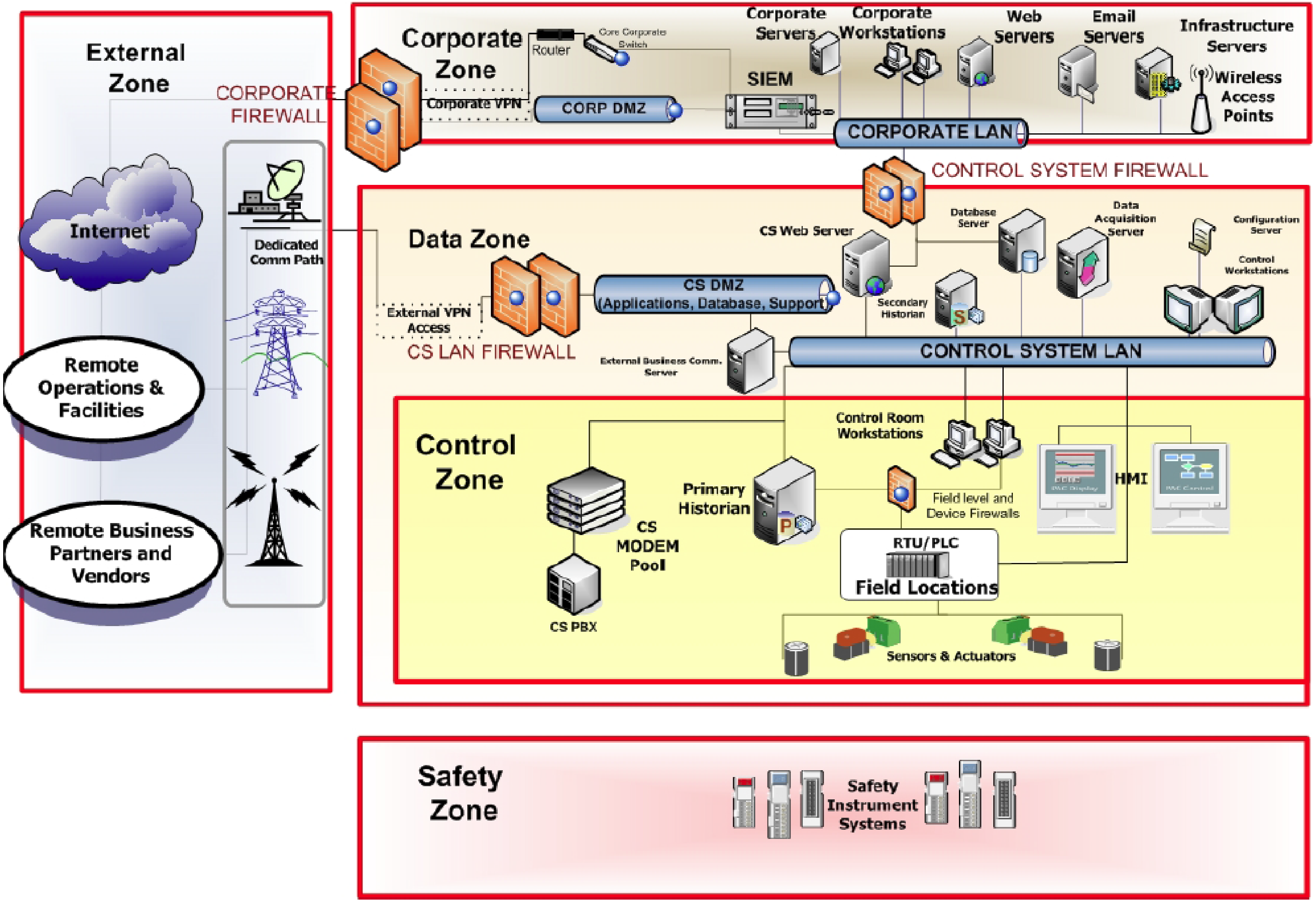
Users

Infrastructure operators

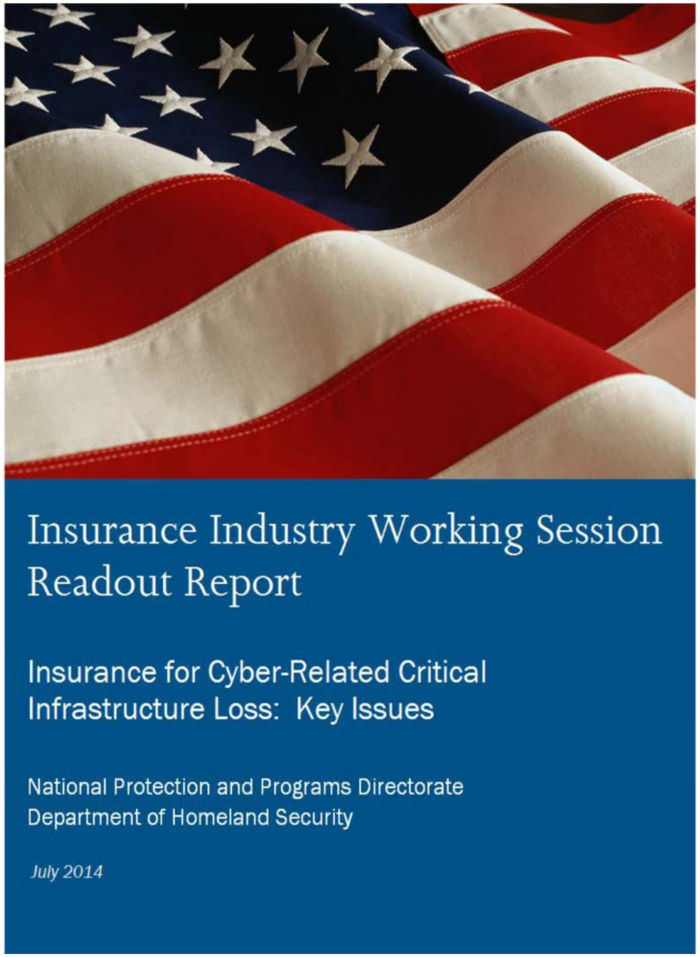
Standards organizations

Regulators

Cybersecurity Risk Spreading



Risk Transfer And Acceptance



Insurance Industry Working Session
Readout Report

Insurance for Cyber-Related Critical
Infrastructure Loss: Key Issues

National Protection and Programs Directorate
Department of Homeland Security

July 2014

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.

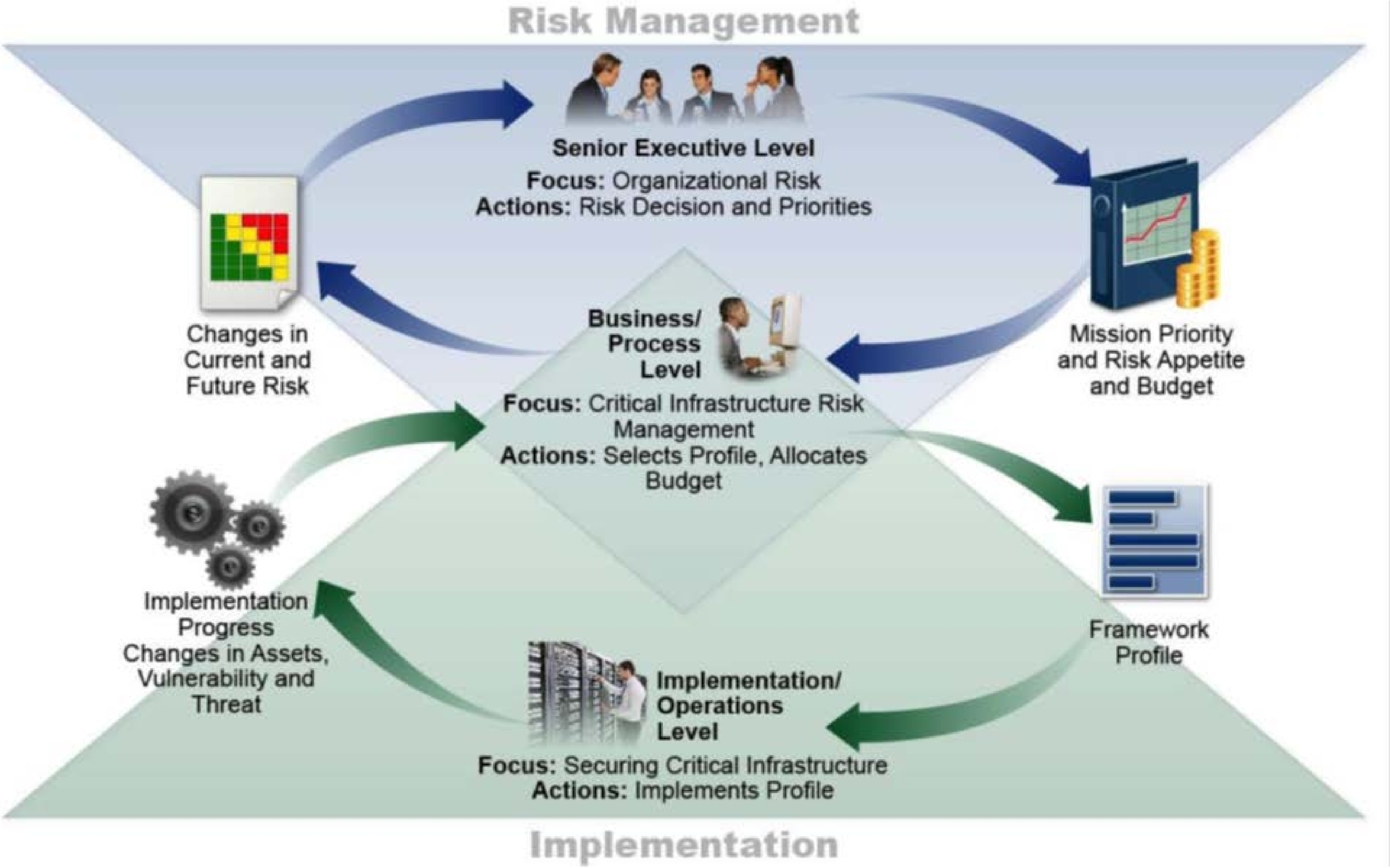
Aggregation risk is a specific worry - small number of dominant platforms supporting cloud services sets the stage for potentially large losses. If one such platform goes down, thousands of users could be impacted simultaneously.

POTENTIAL IMPACT

Could bankrupt a single carrier who insures a significant percentage of those users overnight. Could give rise to “many, many” claims.

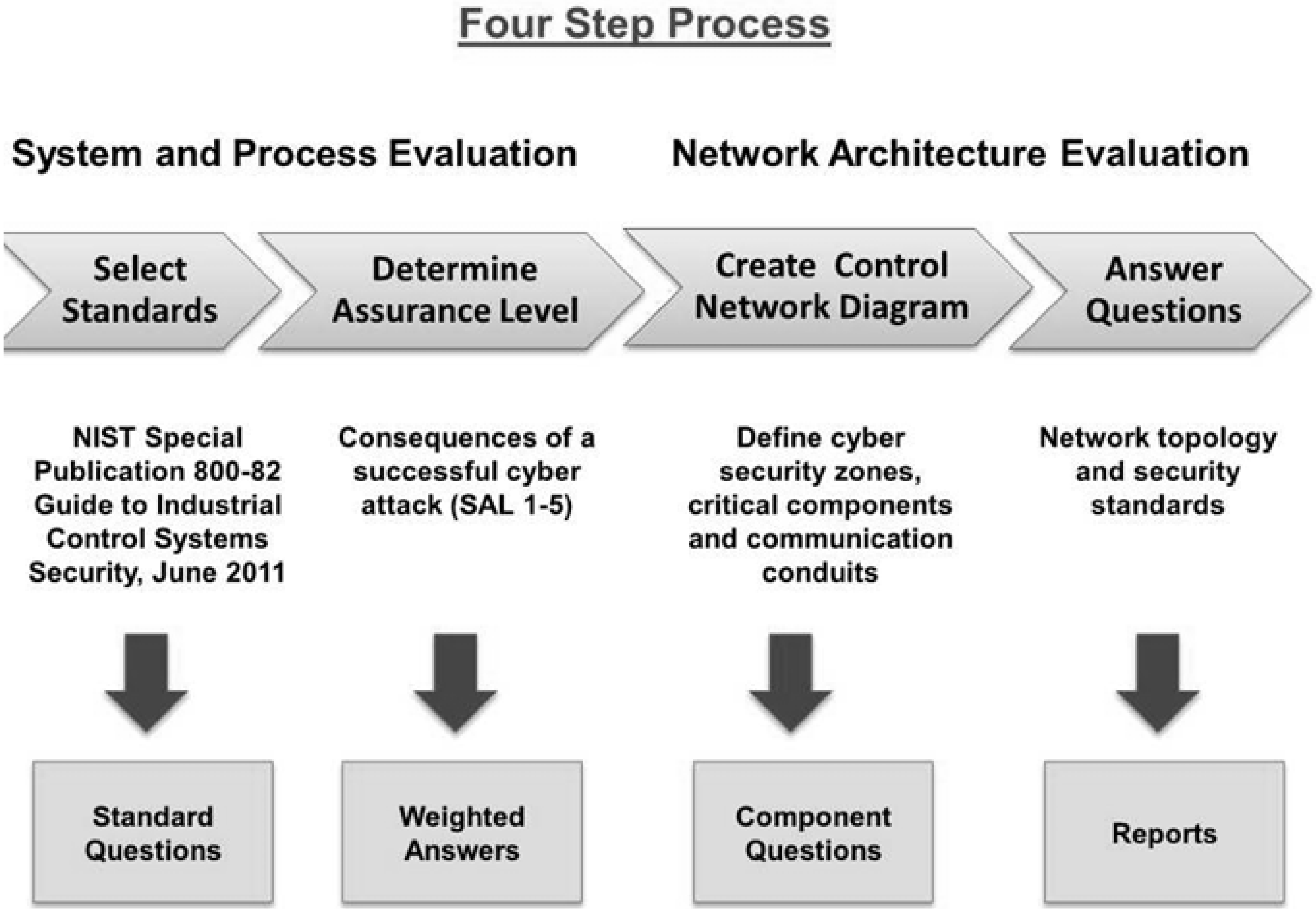
Cybersecurity Risk Management

NIST Framework Information & Decision Flows


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Source: NIST Cybersecurity Framework

Cybersecurity Evaluation Tool (CSET®)



Four Step Process

System and Process Evaluation

Network Architecture Evaluation

Select Standards

NIST Special Publication 800-82 Guide to Industrial Control Systems Security, June 2011

Standard Questions

Determine Assurance Level

Consequences of a successful cyber attack (SAL 1-5)

Weighted Answers

Create Control Network Diagram

Define cyber security zones, critical components and communication conduits

Component Questions

Answer Questions

Network topology and security standards

Reports

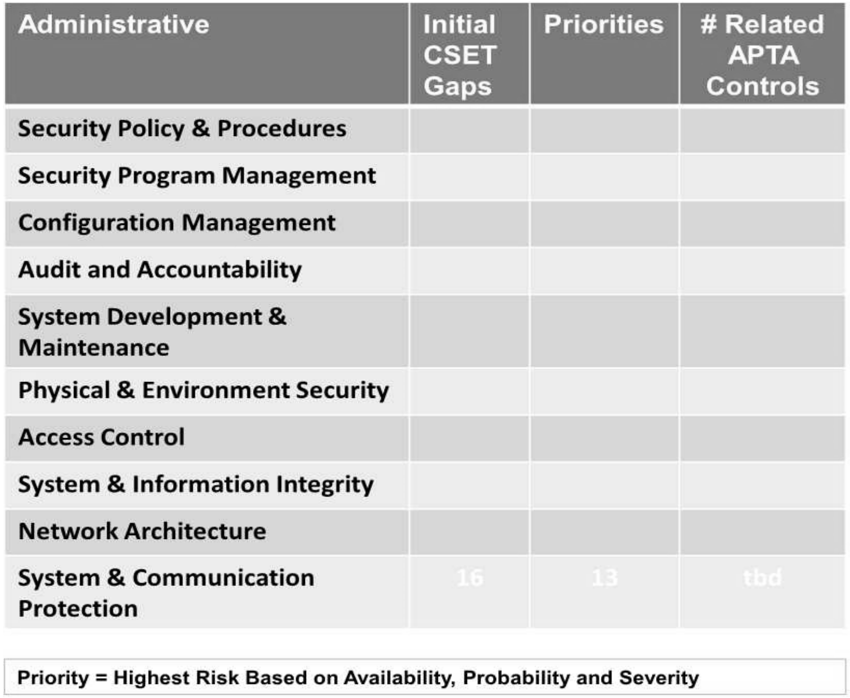
Case Study - Metropolitan Atlanta Rapid Transit Authority (MARTA)

CSET Assessment

Gap Analysis

Risk Prioritization

Roadmap



Administrative	Initial CSET Gaps	Priorities	# Related APTA Controls
Security Policy & Procedures			
Security Program Management			
Configuration Management			
Audit and Accountability			
System Development & Maintenance			
Physical & Environment Security			
Access Control			
System & Information Integrity			
Network Architecture			
System & Communication Protection	16	13	tbd

Priority = Highest Risk Based on Availability, Probability and Severity

Cybersecurity Guidance

Cybersecurity and Critical Infrastructure Policy Frameworks

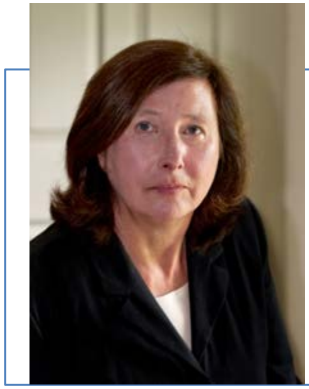
- USA Patriot Act of 2001and National Strategy To Secure Cyberspace (2003)
- Presidential Policy Directive 8: National Preparedness (2011) and National Infrastructure Protection Plan (2013)
- Executive Order 13636 (EO) Improving Critical Infrastructure Cybersecurity (2013)
- NIST Cybersecurity Framework (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)



Patricia Bye

Western Management & Consulting LLC

COUNTERMEASURES

Countermeasures

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

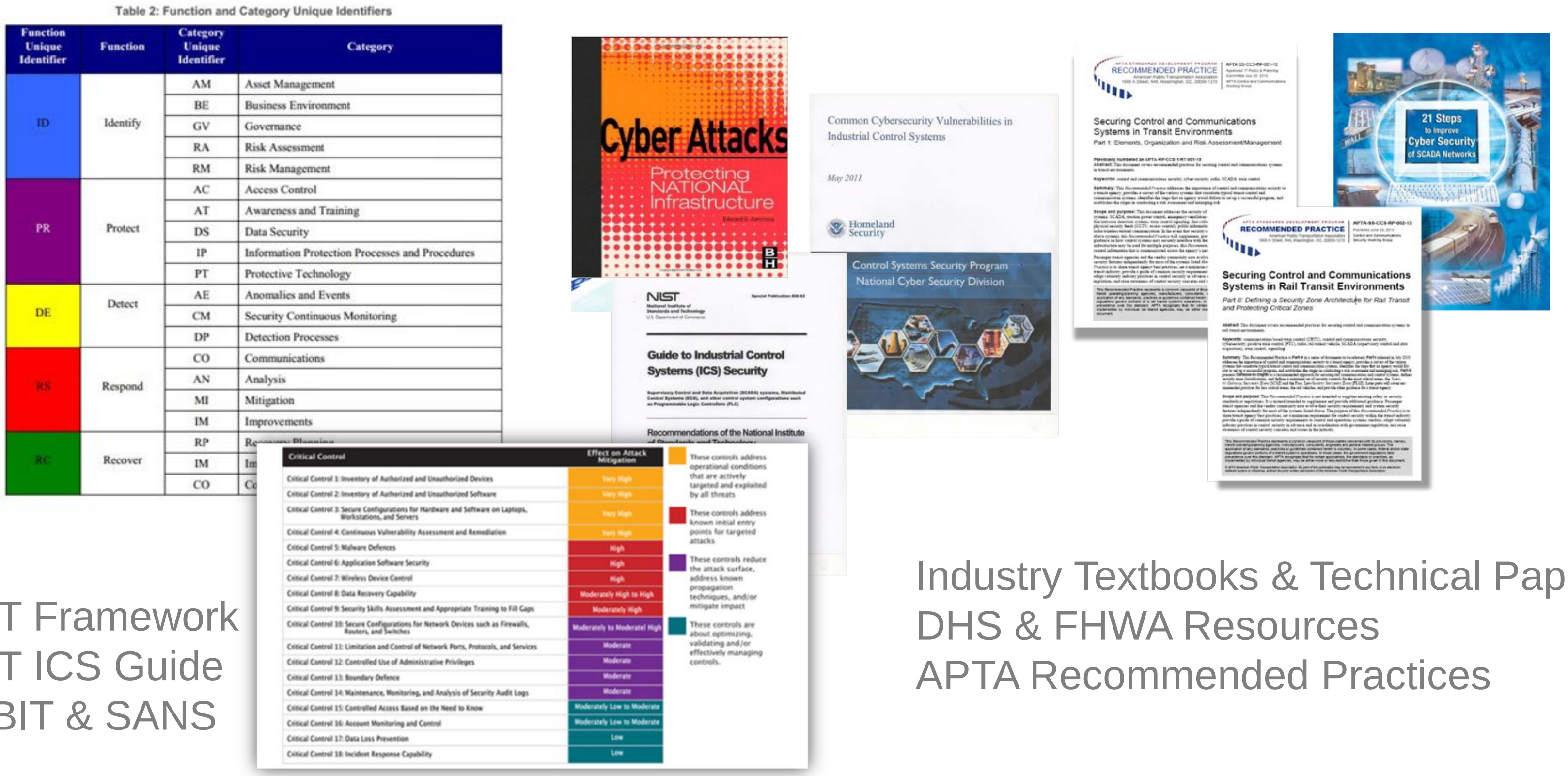


Table 2: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Im
		CO	Co

Critical Control	Effect on Attack Mitigation
Critical Control 1: Inventory of Authorized and Unauthorized Devices	Very High
Critical Control 2: Inventory of Authorized and Unauthorized Software	Very High
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
Critical Control 4: Continuous Vulnerability Assessment and Remediation	Very High
Critical Control 5: Malware Defences	High
Critical Control 6: Application Software Security	High
Critical Control 7: Wireless Device Control	High
Critical Control 8: Data Recovery Capability	Moderately High to High
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately to Moderatel High
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	Moderate
Critical Control 12: Controlled Use of Administrative Privileges	Moderate
Critical Control 13: Boundary Defence	Moderate
Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
Critical Control 15: Controlled Access Based on the Need to Know	Moderately Low to Moderate
Critical Control 16: Account Monitoring and Control	Moderately Low to Moderate
Critical Control 17: Data Loss Prevention	Low
Critical Control 18: Incident Response Capability	Low

🟧 These controls address operational conditions that are actively targeted and exploited by all threats

🟥 These controls address known initial entry points for targeted attacks

🟪 These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact

🟦 These controls are about optimizing, validating and/or effectively managing controls.

Cyber Attacks
Protecting NATIONAL Infrastructure
Edward G. Amoroso
BH

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Special Publication 800-82

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Recommendations of the National Institute of Standards and Technology

Common Cybersecurity Vulnerabilities in Industrial Control Systems

May 2011

Homeland Security

Control Systems Security Program
National Cyber Security Division

APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA SS-CCS-RP-001-10

Securing Control and Communications Systems in Transit Environments
Part 1: Elements, Organization and Risk Assessment/Management

21 Steps to Improve Cyber Security of SCADA Networks

APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA-SS-CCS-RP-002-13

Securing Control and Communications Systems in Rail Transit Environments
Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

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

APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA SS-CCS-RP-001-10
Approved: IT Policy & Planning Committee July 30, 2010
APTA Control and Communications Working Group

Securing Control and Communications Systems in Transit Environments
Part 1: Elements, Organization and Risk Assessment/Management

Previously numbered as APTA-RP-CCS-1-RT-001-10
Abstract: This document covers recommended practices for securing control and communications systems in transit environments.

Keywords: control and communications security, cyber-security, radio, SCADA, train control

Summary: [illegible]

APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA-SS-CCS-RP-002-13
Published June 26, 2013
Control and Communications Security Working Group

Securing Control and Communications Systems in Rail Transit Environments
Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

Abstract: This document covers recommended practices for securing control and communications systems in rail transit environments.

Keywords: [illegible]

Importance	Zone	Example System
Most Critical	Safety Critical Security	Field signaling
	Fire, Life-Safety Security	Fire Detection/suppression
	Operationally Critical	Traffic Management
	Enterprise	HR, Accounting
Most Public	External	Communications with public, vendors, others

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

	OCC	Train station / Station Equipment Room	SIGNAL BUNGALOW – or equivalent
EXTERNAL ZONE:	□ VPN to other Vendors □ VPN to other Agencies	□ N/A	□ N/A
EN	□ Access Control System □ Advertising □ Fare Sales / Collection □ Credit Card Processing □ Logging	□ Access Control / Intrusion Detection □ Advertising □ Fare Sales / Collection □ Passenger information system □ CCTV	□ N/A
OC	□ Dispatch / ATS □ Non-Emergency Voice Communications □ SCADA	□ Traction Power □ PA System – Passenger Information Display □ Vertical Lift Devices □ Tunnel pumping / draining	□ Traffic Controller Interface
FL	□ Emergency Communications □ Fire Alarm & Suppression Enunciators □ Fire / Life-Safety, Emergency Ventilation Control □ Status displays	□ 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	□ Safety Critical Physical Intrusion Detection
SC	□ Vital CBTC	□ Vital Signaling, ATP □ Platform Gate Control	□ 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

LEGEND

⬚	Enterprise Zone Perimeter	▭	Fire, Life-Safety Security Zone Perimeter
⋯	Operationally Critical Security Zone Perimeter	▭	Safety Critical Security Zone Perimeter

APTA Recommended Practices
Future Publications

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

Part IIIc: Application of 3 security zones (SZ) - the Operationally Critical SZ, Fire Line SZ, and Safety Critical SZ - to **rail transit vehicles**.

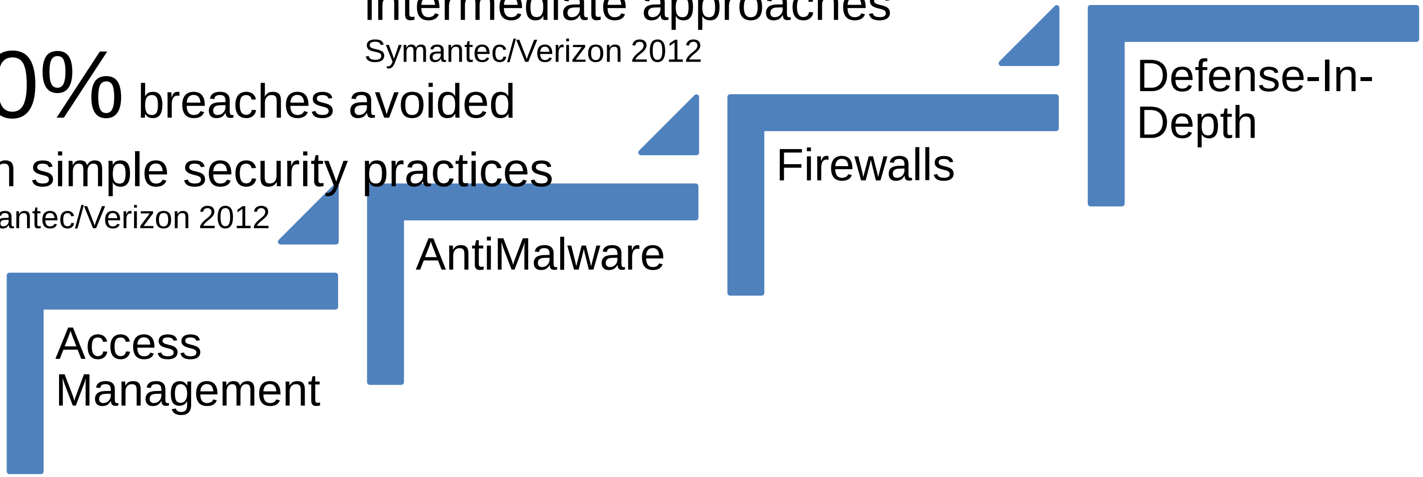
Cybersecurity Bar Keeps Increasing

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% have been breached
Firefly 2014



Access Management

AntiMalware

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

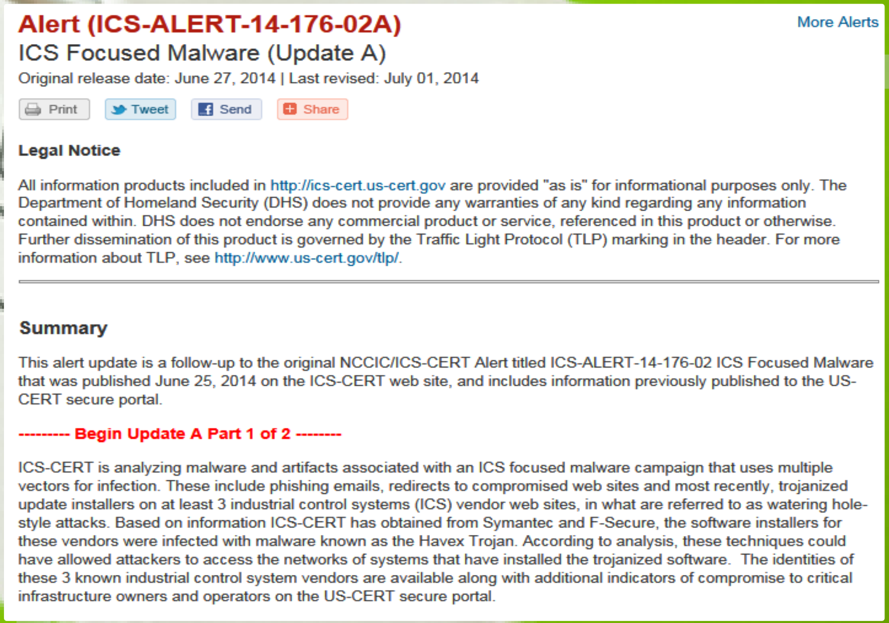
Cyber Hygiene: Basics Matter

Airports Targeted: 75 Impacted, 2 Compromised

Phishing email

Redirect to site

Public document source
of phishing emails



Alert (ICS-ALERT-14-176-02A)

ICS Focused Malware (Update A)

Original release date: June 27, 2014 | Last revised: July 01, 2014

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

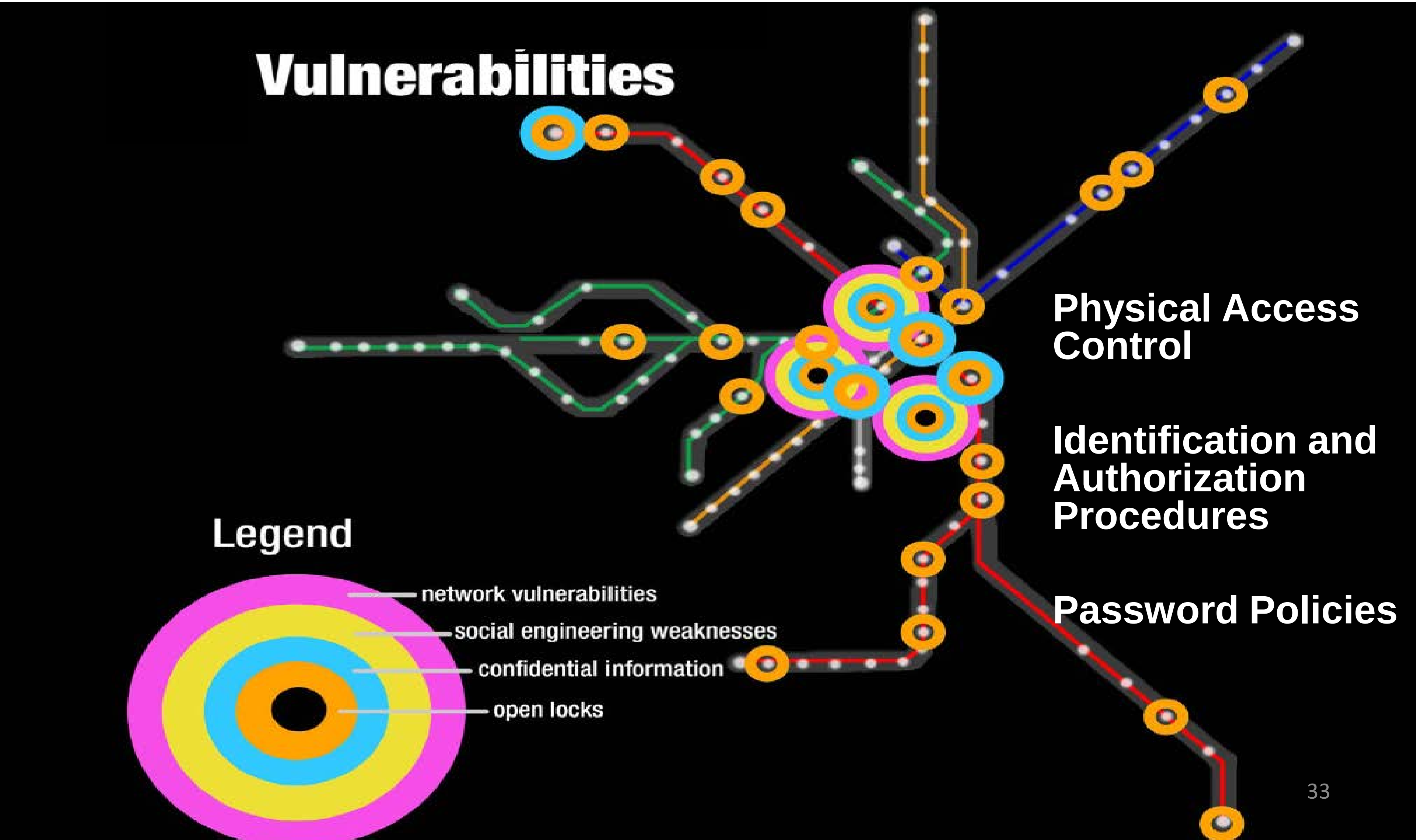
Summary

This alert update is a follow-up to the original NCCIC/ICS-CERT Alert titled ICS-ALERT-14-176-02 ICS Focused Malware that was published June 25, 2014 on the ICS-CERT web site, and includes information previously published to the US-CERT secure portal.

--------- Begin Update A Part 1 of 2 --------

ICS-CERT is analyzing malware and artifacts associated with an ICS focused malware campaign that uses multiple vectors for infection. These include phishing emails, redirects to compromised web sites and most recently, trojanized update installers on at least 3 industrial control systems (ICS) vendor web sites, in what are referred to as watering hole-style attacks. Based on information ICS-CERT has obtained from Symantec and F-Secure, the software installers for these vendors were infected with malware known as the Havex Trojan. According to analysis, these techniques could have allowed attackers to access the networks of systems that have installed the trojanized software. The identities of these 3 known industrial control system vendors are available along with additional indicators of compromise to critical infrastructure owners and operators on the US-CERT secure portal.

Access Control: Cyber and Physical

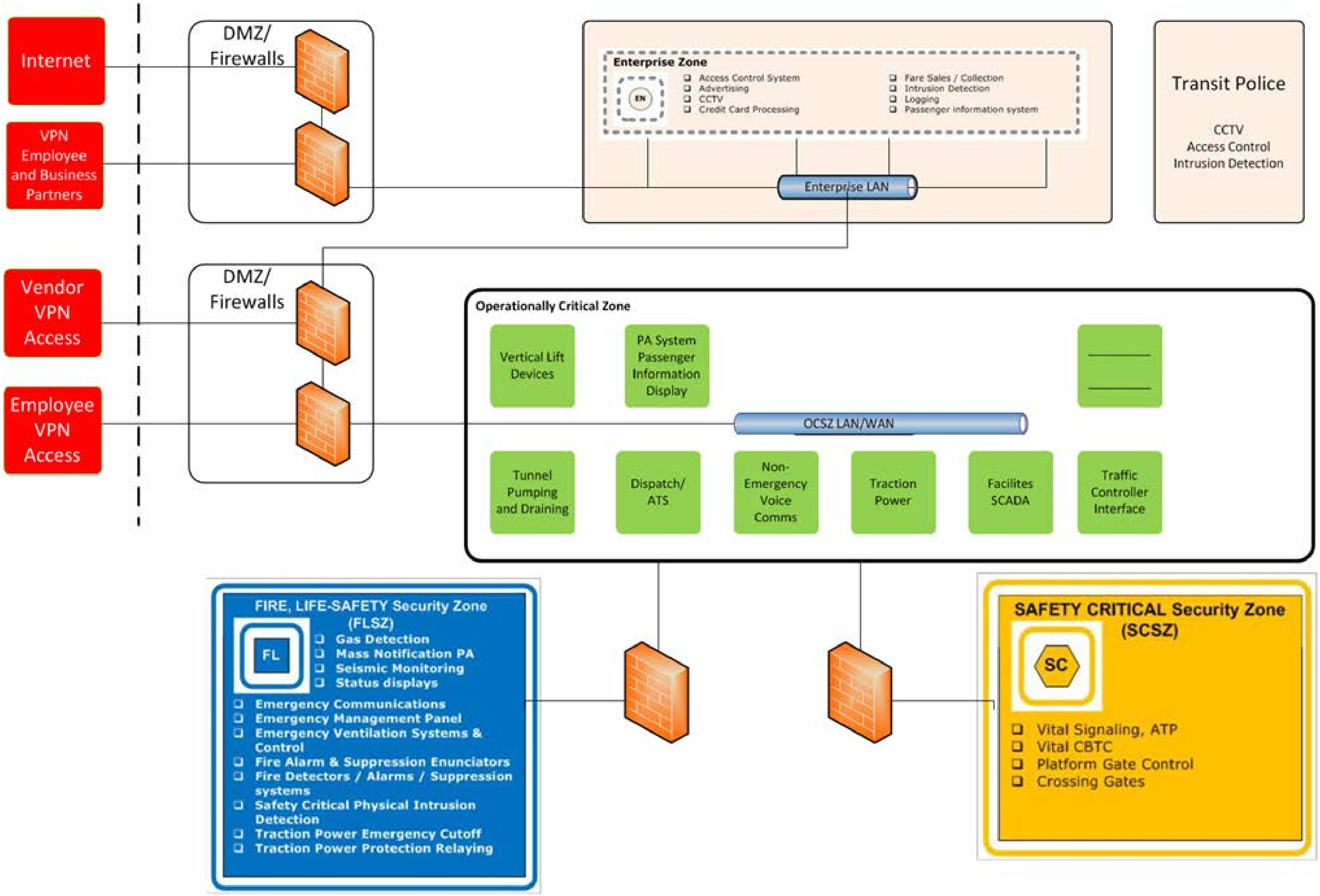


Physical Access Control

Identification and Authorization Procedures

Password Policies

Boundary Defense and Network Separation



Internet

VPN Employee and Business Partners

Vendor VPN Access

Employee VPN Access

DMZ/ Firewalls

DMZ/ Firewalls

Enterprise Zone

EN

□ Access Control System
□ Advertising
□ CCTV
□ Credit Card Processing
□ Fare Sales / Collection
□ Intrusion Detection
□ Logging
□ Passenger information system

Enterprise LAN

Transit Police

CCTV
Access Control
Intrusion Detection

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

Facilites SCADA

Traffic Controller Interface

FIRE, LIFE-SAFETY Security Zone (FLSZ)

FL

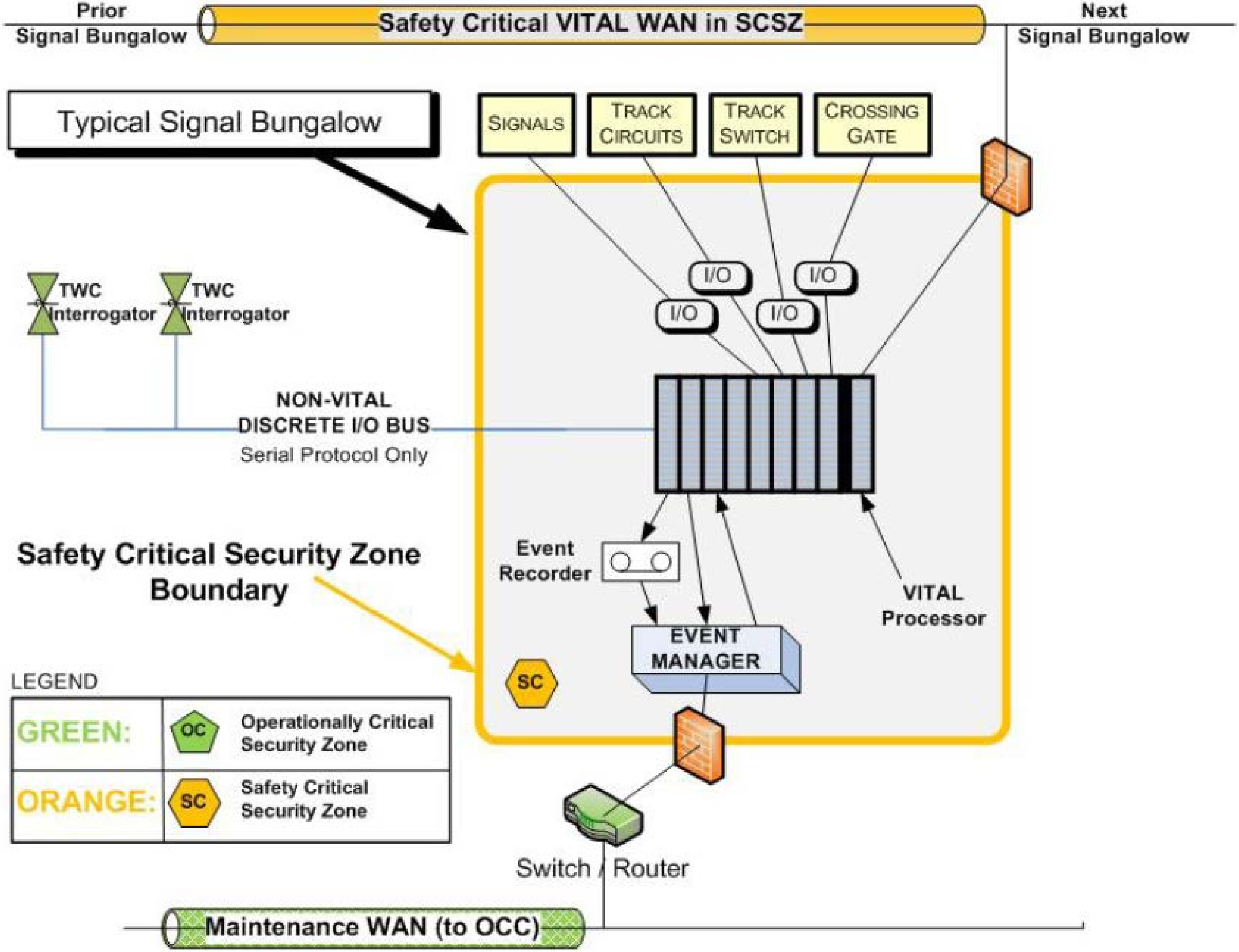
□ Gas Detection
□ Mass Notification PA
□ Seismic Monitoring
□ Status displays
□ Emergency Communications
□ Emergency Management Panel
□ Emergency Ventilation Systems & Control
□ Fire Alarm & Suppression Enunciators
□ Fire Detectors / Alarms / Suppression systems
□ Safety Critical Physical Intrusion Detection
□ Traction Power Emergency Cutoff
□ Traction Power Protection Relaying

SAFETY CRITICAL Security Zone (SCSZ)

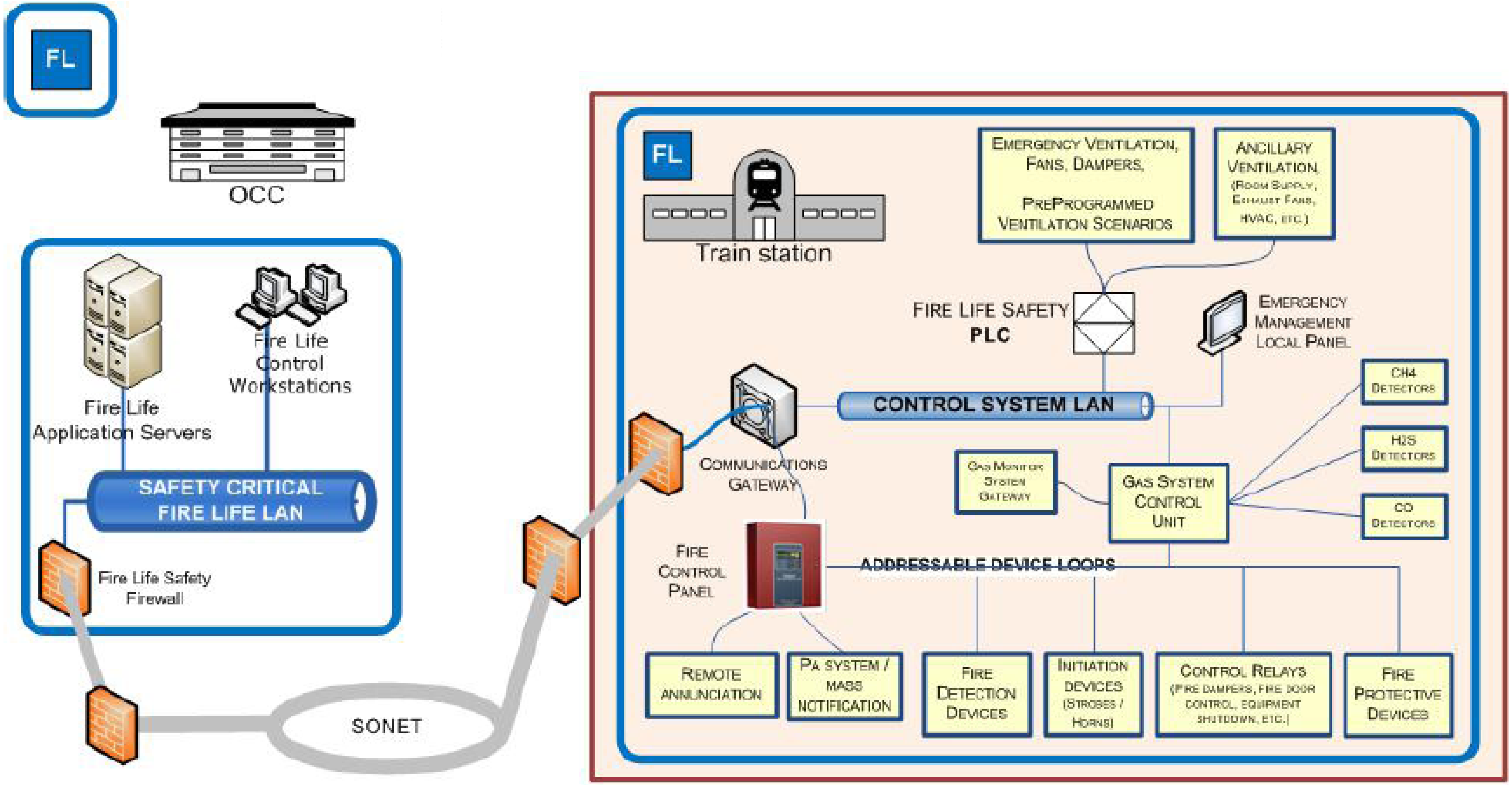
SC

□ Vital Signaling, ATP
□ Vital CBTC
□ Platform Gate Control
□ Crossing Gates

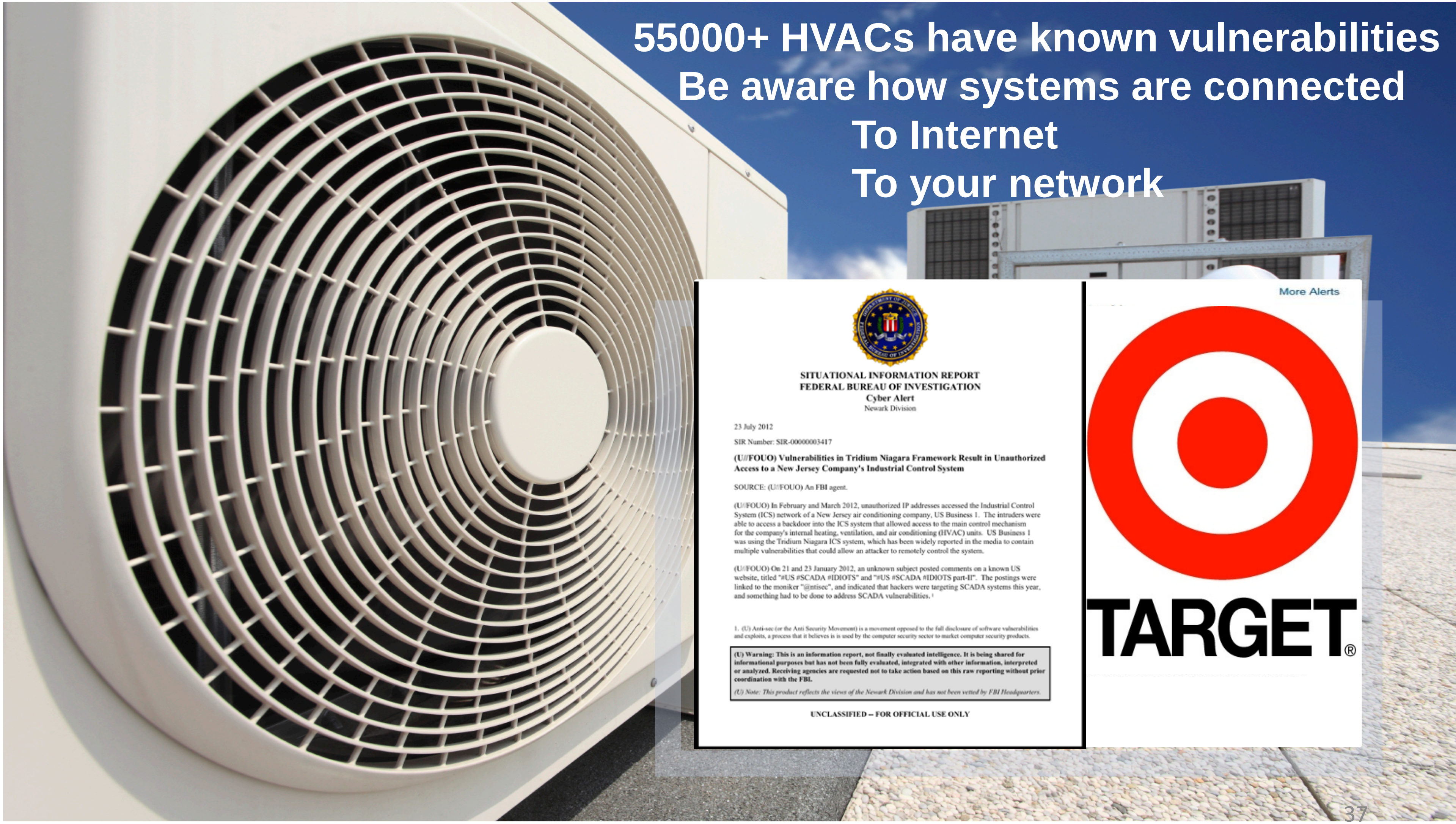
Safety Critical Signaling



Safety Critical Fire


FL
OCC
Fire Life Application Servers
Fire Life Control Workstations
SAFETY CRITICAL FIRE LIFE LAN
Fire Life Safety Firewall
SONET
FL
Train station
EMERGENCY VENTILATION, FANS, DAMPERS,
PREPROGRAMMED VENTILATION SCENARIOS
ANCILLARY VENTILATION, (ROOM SUPPLY, EXHAUST FANS, HVAC, ETC.)
FIRE LIFE SAFETY PLC
EMERGENCY MANAGEMENT LOCAL PANEL
CONTROL SYSTEM LAN
COMMUNICATIONS GATEWAY
CH4 DETECTORS
H2S DETECTORS
CO DETECTORS
GAS MONITOR SYSTEM GATEWAY
GAS SYSTEM CONTROL UNIT
FIRE CONTROL PANEL
ADDRESSABLE DEVICE LOOPS
REMOTE ANNUNCIATION
PA SYSTEM / MASS NOTIFICATION
FIRE DETECTION DEVICES
INITIATION DEVICES (STROBES / HORNS)
CONTROL RELAYS (FIRE DAMPERS, FIRE DOOR CONTROL, EQUIPMENT SHUTDOWN, ETC.)
FIRE PROTECTIVE DEVICES

Network Separation: HVAC



55000+ HVACs have known vulnerabilities

Be aware how systems are connected

To Internet

To your network

SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
Cyber Alert
Newark Division

23 July 2012

SIR Number: SIR-00000003417

(U//FOUO) Vulnerabilities in Tridium Niagara Framework Result in Unauthorized Access to a New Jersey Company's Industrial Control System

SOURCE: (U//FOUO) An FBI agent.

(U//FOUO) In February and March 2012, unauthorized IP addresses accessed the Industrial Control System (ICS) network of a New Jersey air conditioning company, US Business 1. The intruders were able to access a backdoor into the ICS system that allowed access to the main control mechanism for the company's internal heating, ventilation, and air conditioning (HVAC) units. US Business 1 was using the Tridium Niagara ICS system, which has been widely reported in the media to contain multiple vulnerabilities that could allow an attacker to remotely control the system.

(U//FOUO) On 21 and 23 January 2012, an unknown subject posted comments on a known US website, titled "#US #SCADA #IDIOTS" and "#US #SCADA #IDIOTS part-II". The postings were linked to the moniker "@ntisec", and indicated that hackers were targeting SCADA systems this year, and something had to be done to address SCADA vulnerabilities.[1]

[1] (U) Anti-sec (or the Anti Security Movement) is a movement opposed to the full disclosure of software vulnerabilities and exploits, a process that it believes is is used by the computer security sector to market computer security products.

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) Note: This product reflects the views of the Newark Division and has not been vetted by FBI Headquarters.

UNCLASSIFIED -- FOR OFFICIAL USE ONLY

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.

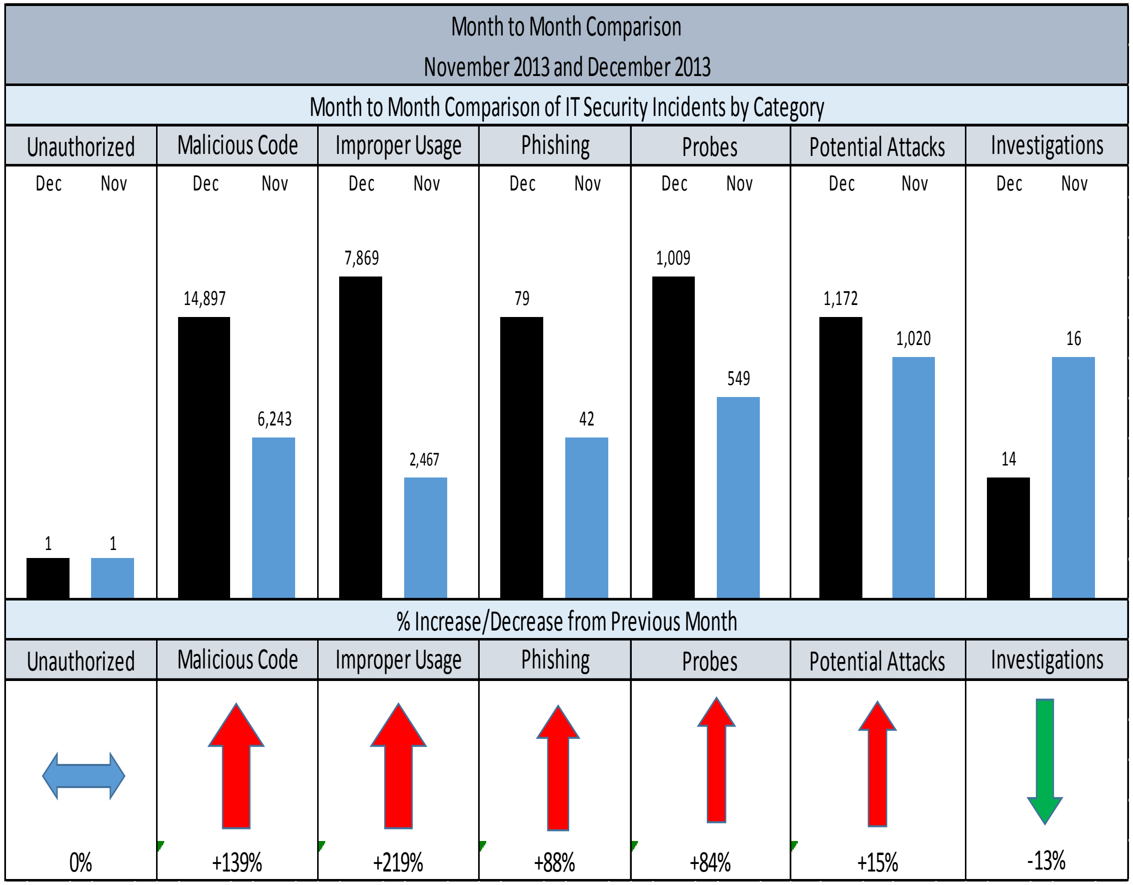
Monitoring and Detection

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



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.”

Everyone from ***frontline personnel****…*

… to ***senior managers***

“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.”

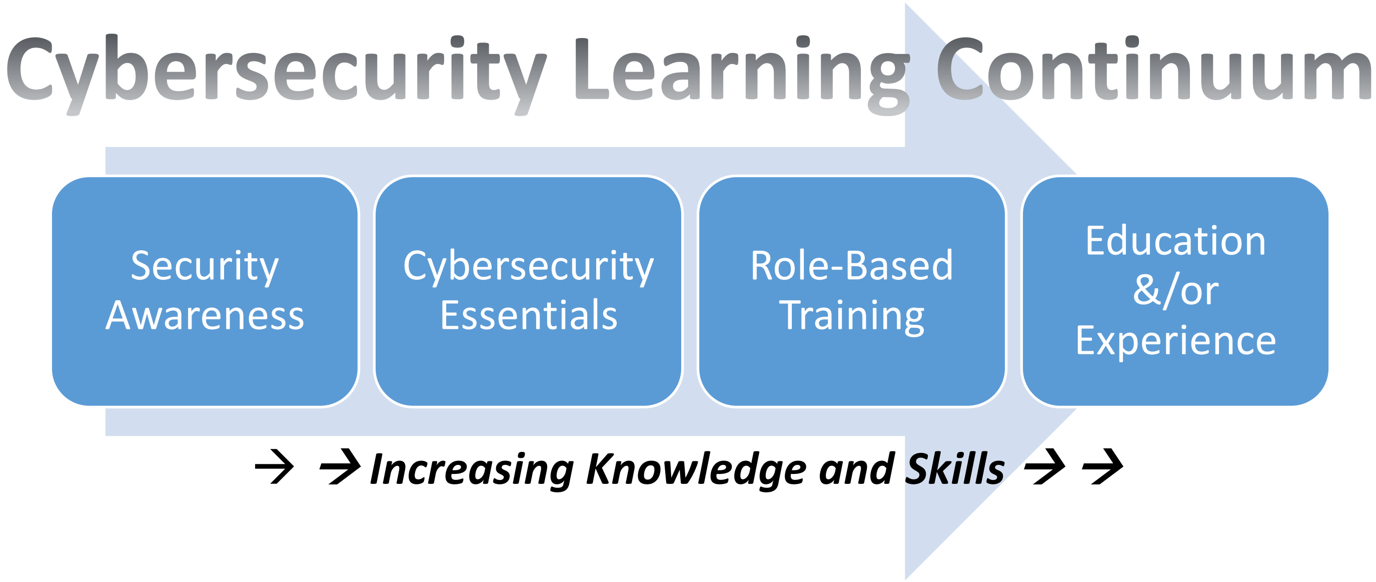
<span>Images</span>: APTA.com

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

Cybersecurity Functions
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Roles & User Categories
All Users & Third Party Stakeholders
Privileged Users
Managers/Senior Executives
Training Personnel
IT/Cybersecurity Personnel
Physical Security Personnel

NIST Pubs	
800-16 Rev 1	Cybersecurity Framework

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