

**Effective Practices
for Protection of
Transportation Infrastructure
from Cyber Incidents**

Transportation Research Board
Webinar
May 13, 2015

Webinar Presenters



David Fletcher
Western Mgmt and
Consulting, LLC



Jennifer Bayuk
Jennifer L. Bayuk,
LLC



Patricia Bye
Western Mgmt and
Consulting, LLC



Yuko Nakanishi
Nakanishi Research
and Consulting, LLC

Today's Agenda

Overview of TRB project

Preview research results

Highlight best practice & approaches

- Risk Management

- Security Programs

- 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 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 Highways are going Cyber



Cyber Transportation Systems

Control systems and IT systems

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

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

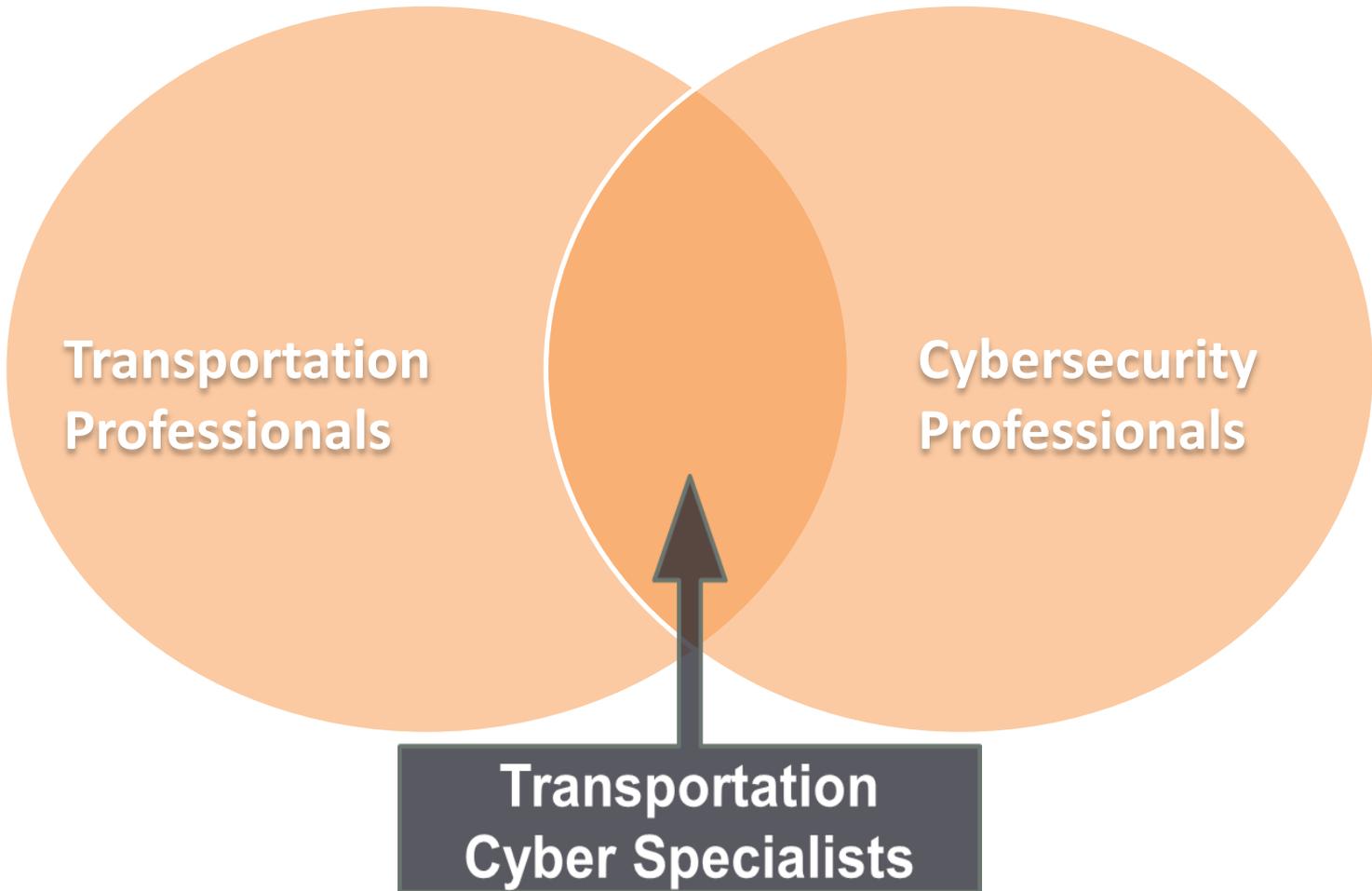
Myth Buster: “Control system cybersecurity is the same as IT cybersecurity.”

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





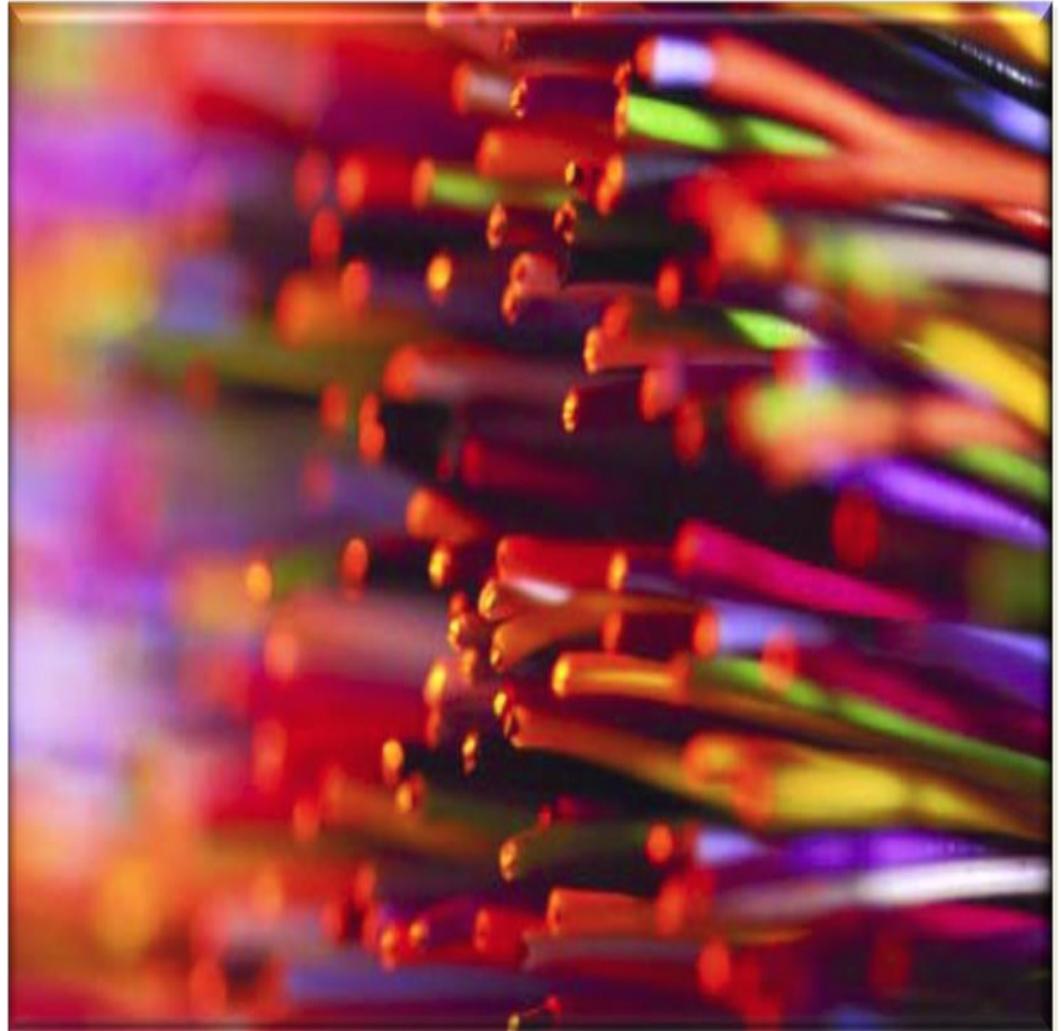
Jennifer Bayuk
Jennifer L. Bayuk, LLC

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

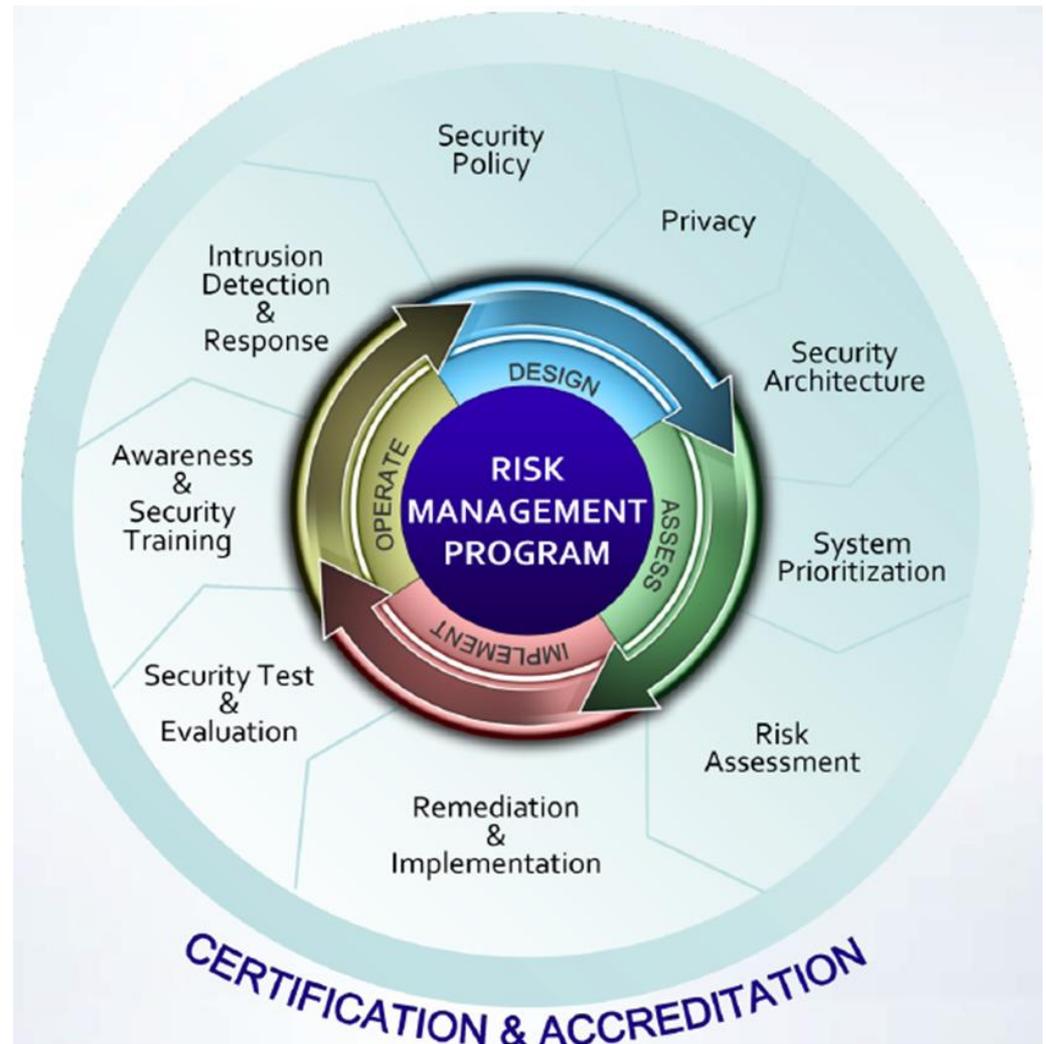
Known issues are growing.

50,000+ recorded vulnerabilities with more added hourly

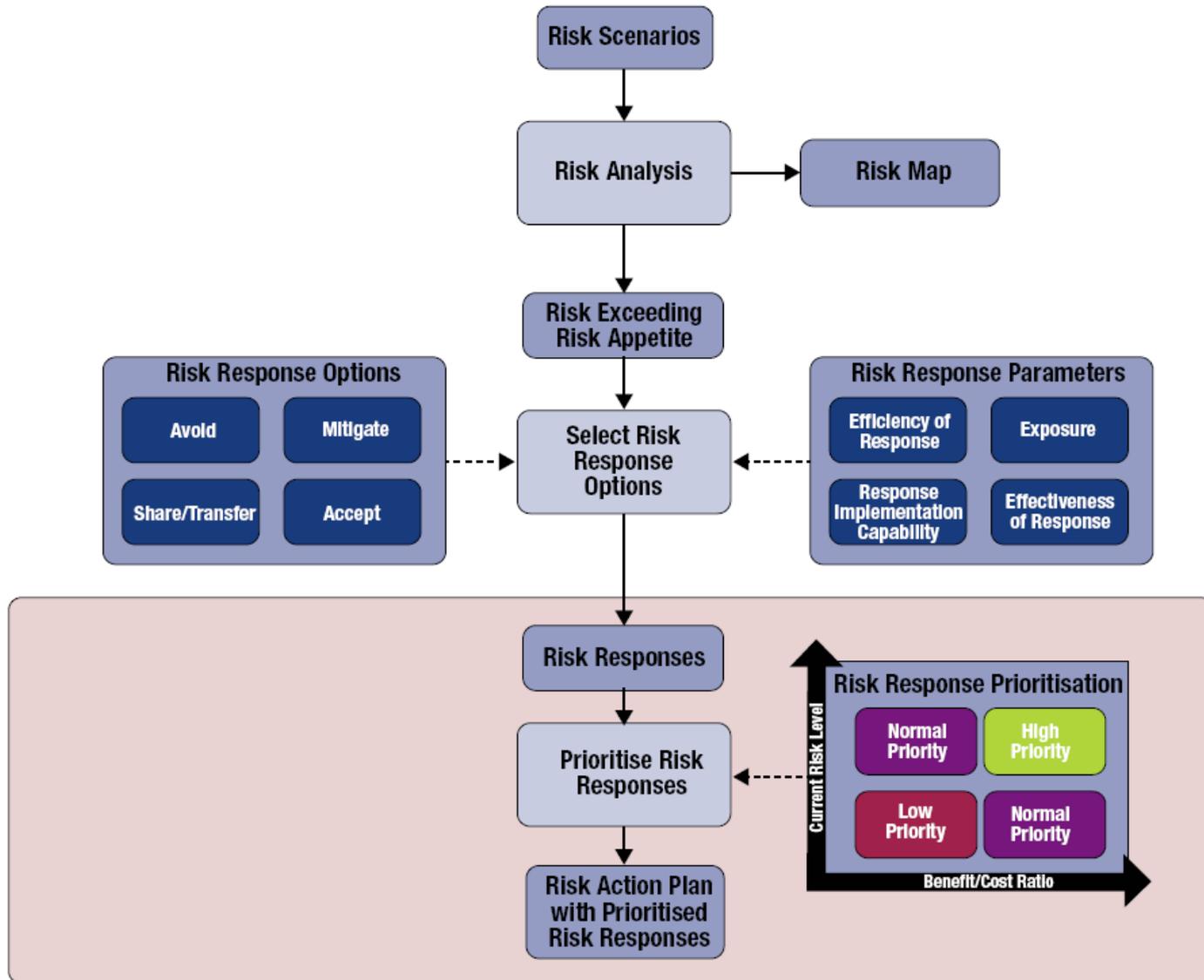
86,000 new malware reported each day

Breaches are hard to detect.

229 days average time to detect breach



Cybersecurity Risk Management



Cybersecurity Risk Dependency

Coordinated collaboration among all stakeholders

Designers & manufacturers

Equipment suppliers

System integrators

University & government
researchers

Testing organizations

Users

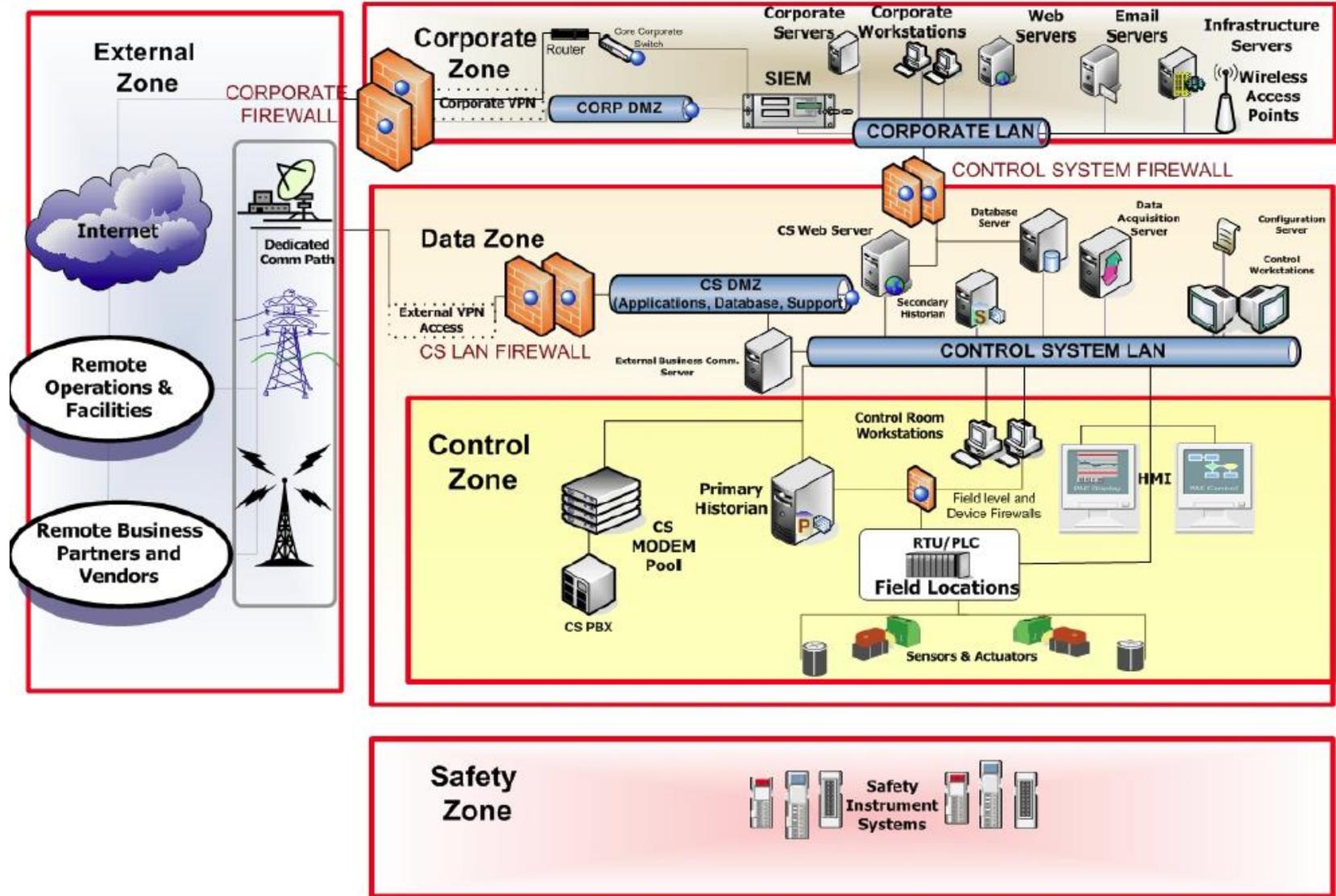
Infrastructure operators

Standards organizations

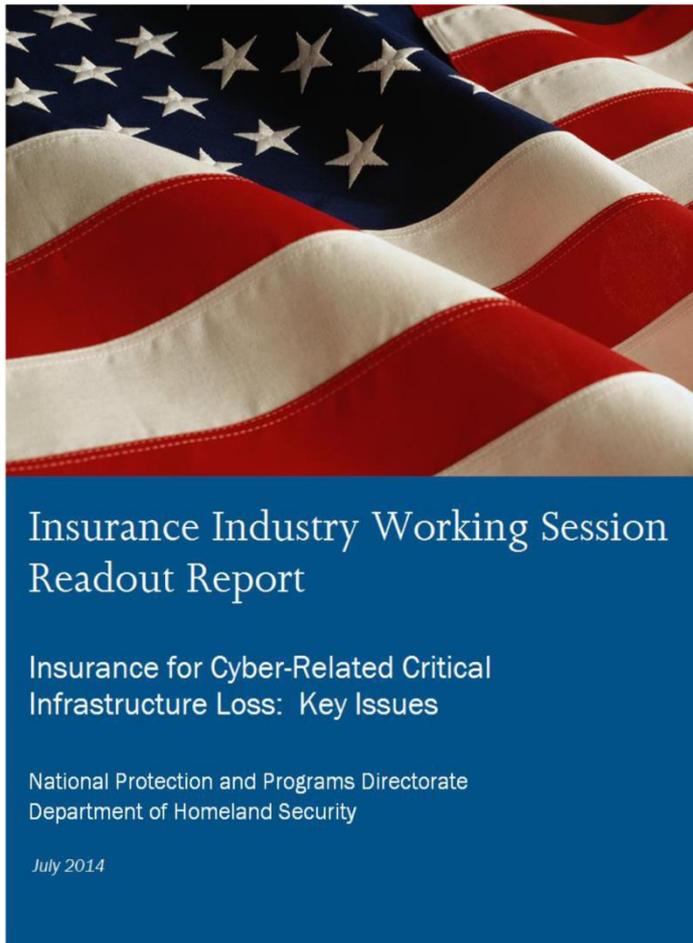
Regulators



Cybersecurity Risk Spreading



Risk Transfer And Acceptance



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.

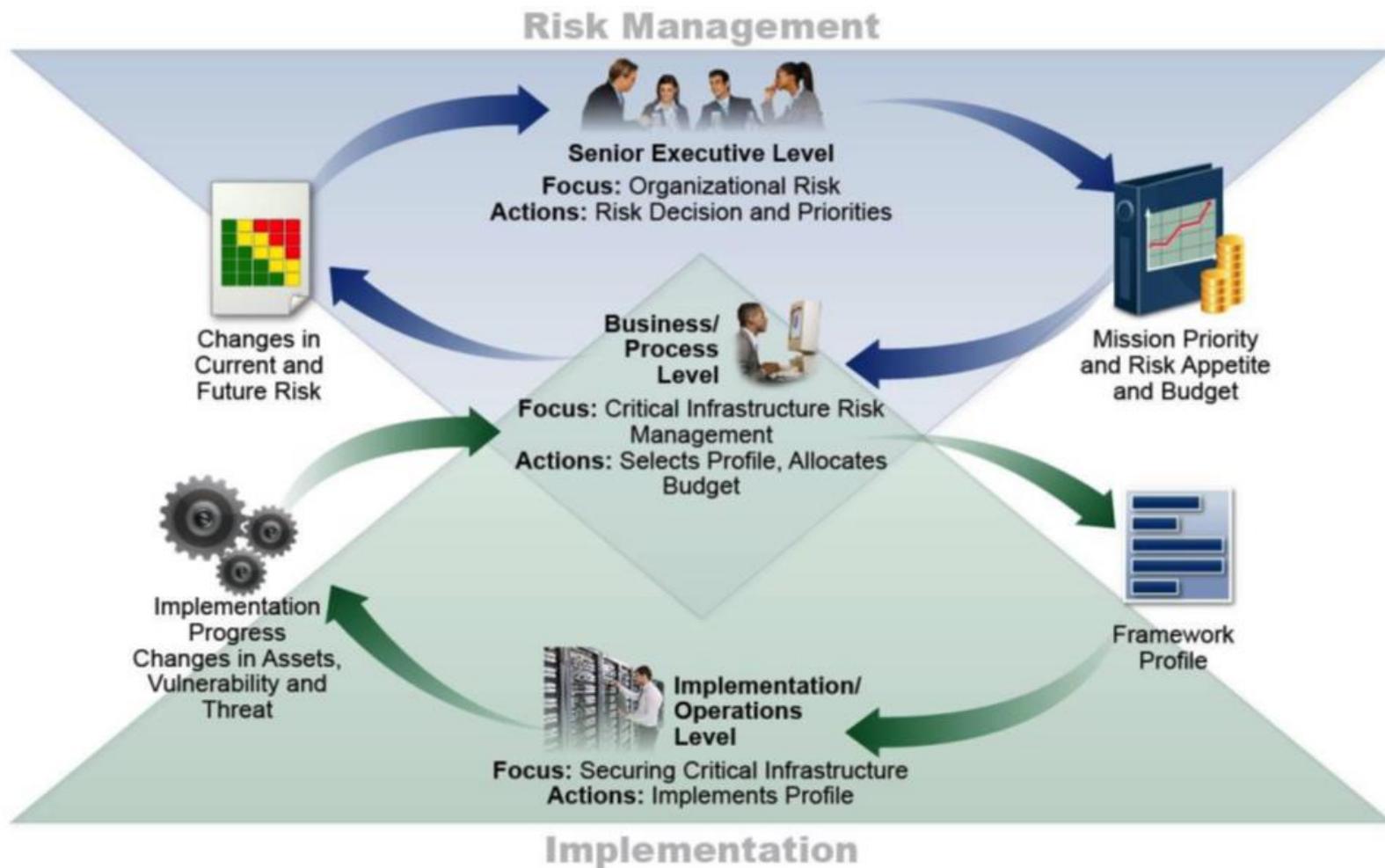
Aggregation risk is a specific worry - small number of dominant platforms supporting cloud services sets the stage for potentially large losses. If one such platform goes down, thousands of users could be impacted simultaneously.

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



Cybersecurity Guidance

Cybersecurity and Critical Infrastructure Policy Frameworks

USA Patriot Act of 2001 and 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

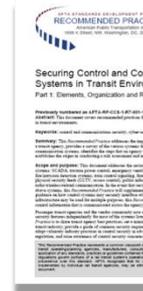
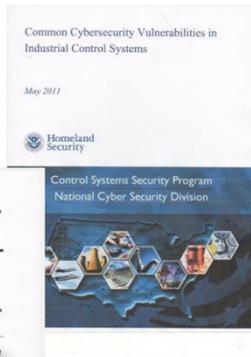
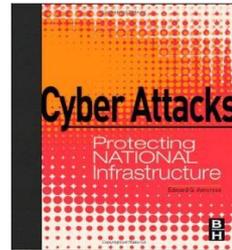
COUNTERMEASURES

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
PR	Protect	RM	Risk Management
		AC	Access Control
		AT	Awareness and Training
		DS	Data Security
DE	Detect	IP	Information Protection Processes and Procedures
		PT	Protective Technology
		AE	Anomalies and Events
RS	Respond	CM	Security Continuous Monitoring
		DP	Detection Processes
		CO	Communications
RC	Recover	AN	Analysis
		MI	Mitigation
		IM	Improvements
		RP	Recovery



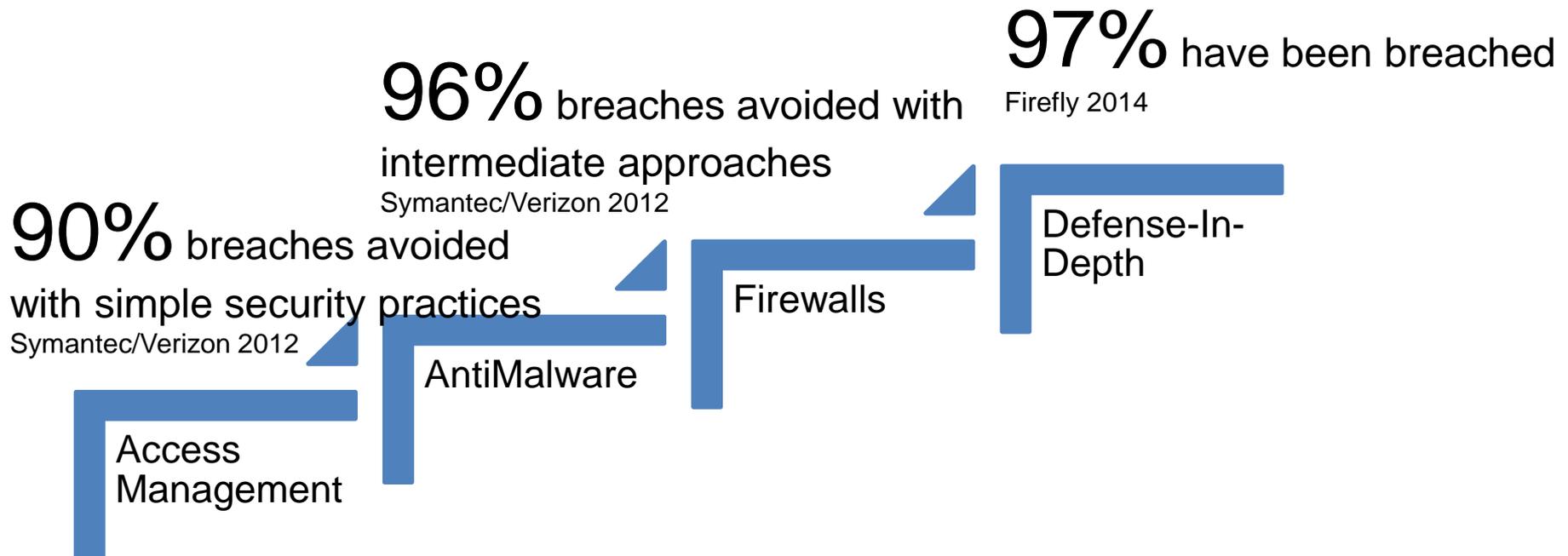
Critical Control	Effect on Attack Mitigation	Notes
Critical Control 1: Inventory of Authorized and Unauthorized Devices	Very High	These controls address operational conditions that are actively targeted and exploited by all threats.
Critical Control 2: Inventory of Authorized and Unauthorized Software	Very High	
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High	These controls address known initial entry points for targeted attacks.
Critical Control 4: Continuous Vulnerability Assessment and Remediation	Very High	
Critical Control 5: Malware Defenses	High	These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.
Critical Control 6: Application Software Security	High	
Critical Control 7: Wireless Device Control	High	
Critical Control 8: Data Recovery Capability	Moderately High	These controls are about optimizing, validating and/or effectively managing controls.
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 Moderately 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 Defense	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	

NIST Framework
NIST ICS Guide
COBIT & SANS

Industry Textbooks & Technical Papers
DHS & FHWA Resources
APTA Recommended Practices

Cybersecurity Bar Keeps Increasing

Only 3% of breaches require difficult or expensive actions.



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.

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

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)

[More Alerts](#)

ICS Focused Malware (Update A)

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

[Print](#) [Tweet](#) [Send](#) [Share](#)

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: 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.



Alert (ICS-ALERT-14-155-01A)

[More Alerts](#)

Daktronics Vanguard Default Credentials (Update A)

Original release date: June 05, 2014 | Last revised: June 06, 2014

[Print](#) [Tweet](#) [Send](#) [Share](#)

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-14-155-01 Daktronics Vanguard Hardcoded Credentials that was published June 4, 2014, on the ICS-CERT web page.

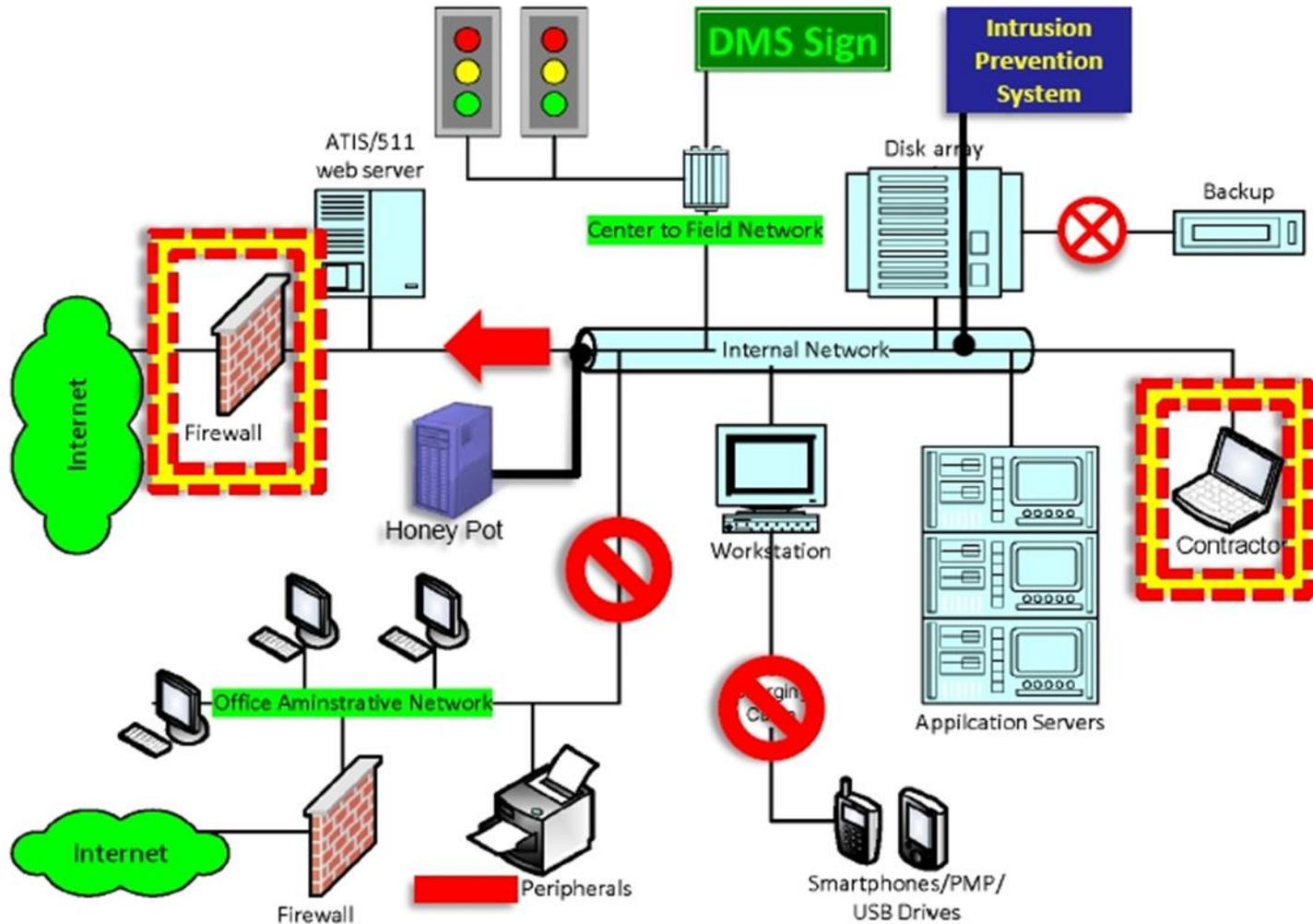
----- Begin Update A Part 1 of 2 -----

ICS-CERT is aware of a public report of a hardcoded password vulnerability affecting Daktronics Vanguard highway dynamic message sign (DMS) configuration software. According to this report, the vulnerability is a hardcoded password that could allow unauthorized access to the highway sign. This report was reported to ICS-CERT by the Federal Highway Administration. ICS-CERT has notified the affected vendor of the report and has asked the vendor to confirm the vulnerability and identify mitigations. **Daktronics reports that the password is not hardcoded as reported, but is a default password that can be changed upon installation.** ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

Proof of Concept is known to be publicly available. ICS-CERT recommends entities review sign messaging, update access credentials, and harden communication paths to the signs.

Vulnerability Type	Remotely Exploitable	Impact
Default credentials	Yes	Modification of sign text

Boundary Defense and Network Separation



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.

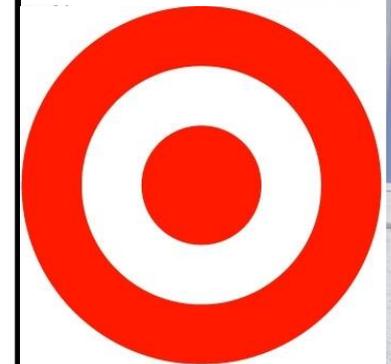
1. (U) Anti-sec (or the Anti Security Movement) is a movement opposed to the full disclosure of software vulnerabilities and exploits, a process that it believes is used by the computer security sector to market computer security products.

(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

More Alerts



TARGET®

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.

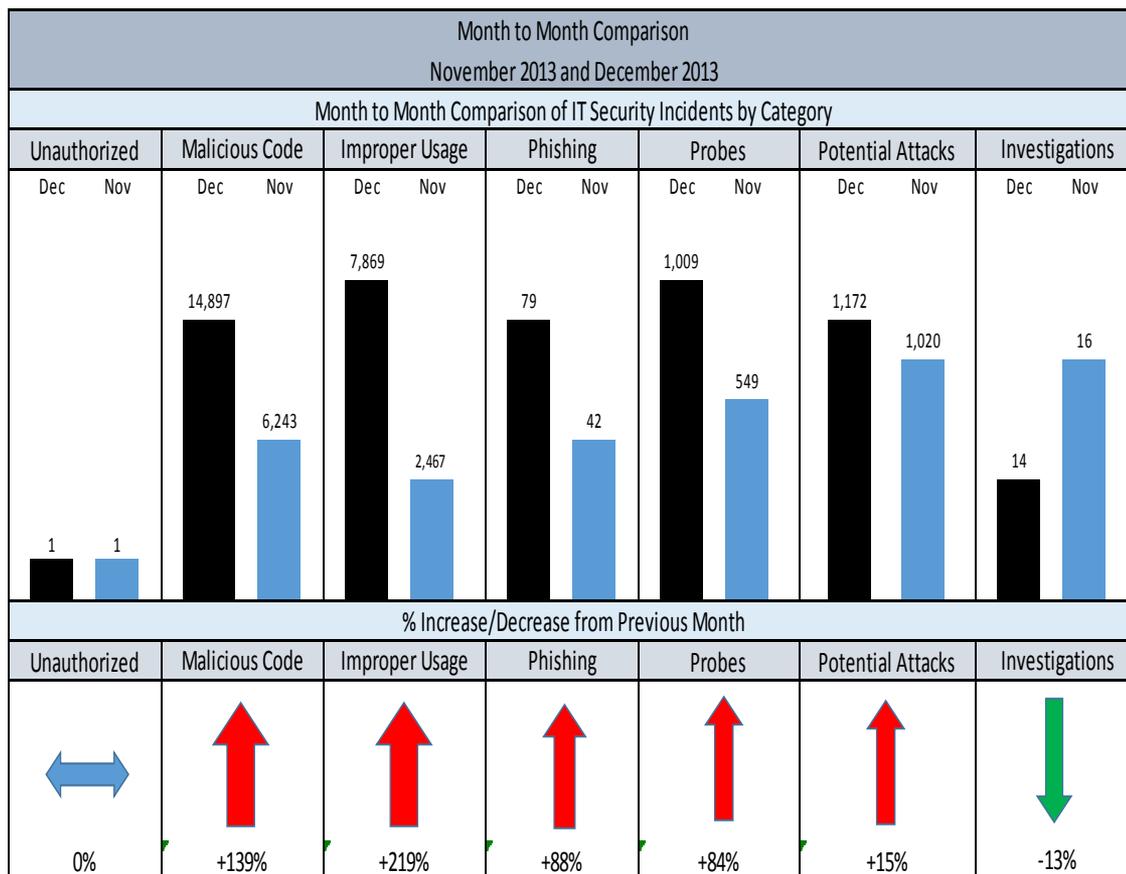
Challenges

Too much data

Too many alerts and false positives

Incomplete visibility of network & endpoints

Detection-in-Depth is an APTA Recommended Practice



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.





Yuko Nakanishi
Nakanishi Research & Consulting LLC

CYBERSECURITY TRAINING

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.

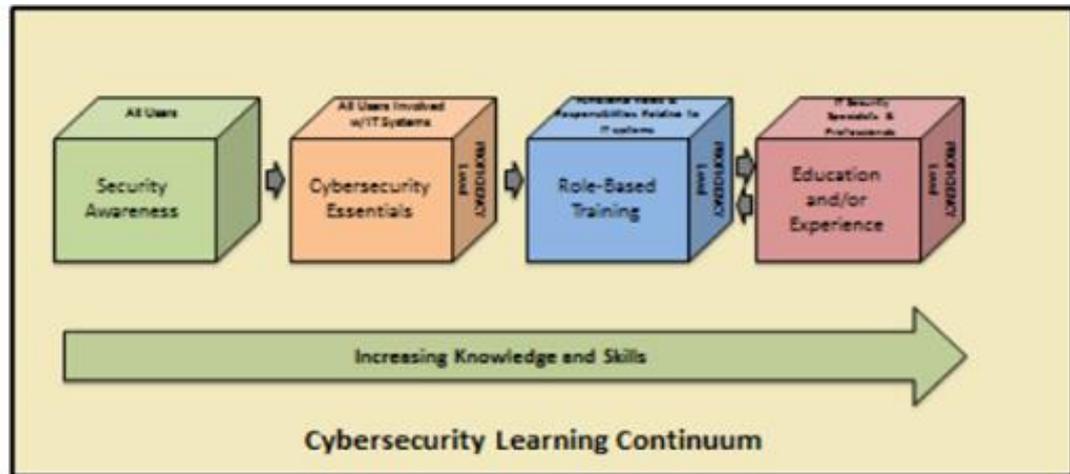


Cybersecurity Learning Continuum

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

NIST Special Publications (SP) on Training

SP 800-16 Information Technology Security Training Requirements: a Role- and Performance-Based Model (1998)

SP 800-50 Building an Information Technology Security Awareness and Training Program (2003)

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

FEMA EMI Courses

IS-0523 Resilient Accord—Exercising Continuity Plans for Cyber Incidents

E0553 Resilient Accord Cyber Security Planning Workshop

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.

Thank You

For additional information please contact:

Ron Frazier

ronfrazier@caseexperts.com

Dave Fletcher

fletcher.d@att.net

Questions

