ASLRRA Webinars

TSA Security Directive 1582-21-01 Compliance

Rick Holmes, Assistant Vice President Information Assurance, Union Pacific Railroad
Seenu Chundru, CEO and President, PS Technology

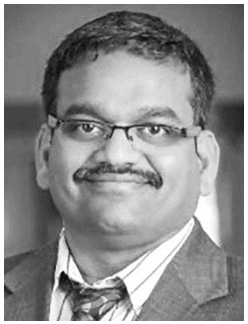
February 8, 2022

Sponsored By

PST
ENTERPRISE DETAILS DONE WELL

Speakers

- **Rick Holmes**, Assistant Vice President of Information Assurance and Chief Information Security Officer, Union Pacific Railroad



- **Seenu Chundru**, CEO and President of PS Technology

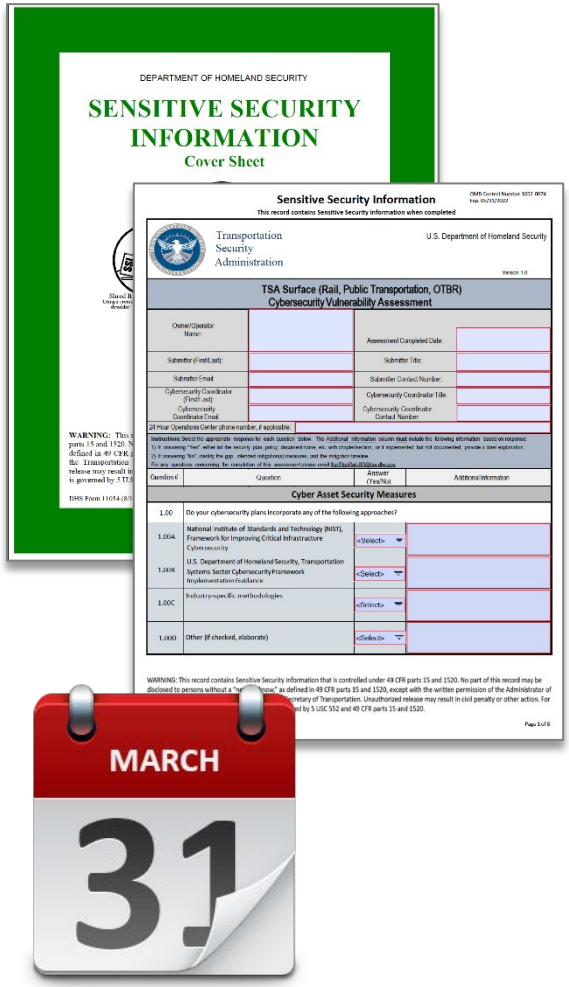
ASLRRA Webinars

What We'll Cover

We'll share our lessons-learned in addressing this at Union Pacific, but focus on those things which can impact Short Line operations.

- Understand our current interpretation of the directive
- Understand the implications of the required vulnerability assessment
- Discuss how to approach incident response planning

Disclaimer – I'm not a regulator, just a security professional trying to meet the directive requirements. I will offer my interpretations, but you need to make your own compliance determinations.



Defender Dilemma

- **What's the "right thing" to do?**
- **How much do I need to do?**
- **How do I actually do it?**
- **How do I convince others that I have done the "right thing"**

Threat Assessment – Likelihood of Event is Increasing

Adversaries

- Cyber attack frequency and severity is on the rise
- Attack techniques are becoming more sophisticated
- Criminal enterprises willing to attack critical infrastructure
- Nation States are openly engaging in espionage, disinformation and disruption campaigns

Stakeholders

- Customers expect data protection and availability
- Competing state and national privacy regulations
- TSA Directive requires incident reporting, risk assessment disclosure, and response plan development

21 Days
Average Downtime of a Ransomware Attack

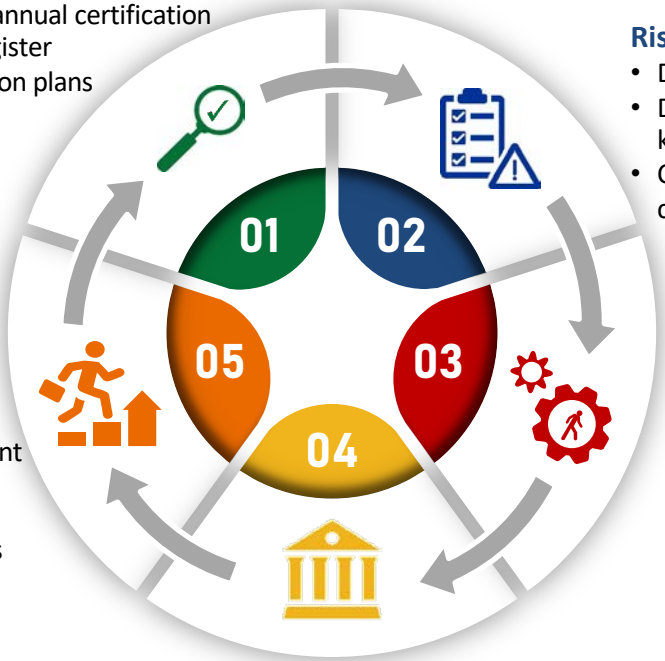
50%
Fortune 250 Companies Breached in Last 10 Years

4,060
2021 Critical Software Vulnerabilities Identified

ASLRRA Webinars

Cyber Risk Management Process

Control Assessment
- Document CIS Control Compliance
- Control Owner annual certification
- Develop gap register
- Identify mitigation plans



Risk Assessment
- Developed risk model
- Determined resiliency of key systems
- Calculated inherent risk curve

Internal & External Assessments
- Continuous assessment of controls and processes
- 3rd Party Assessments
- Red Team Exercises

Mitigation Planning
- Mapped controls to MITRE ATT&CK tactics
- Modeled relative strength of each control
- Simulated the benefit of mitigating gaps
- Results in risk mitigation priorities

Risk Governance

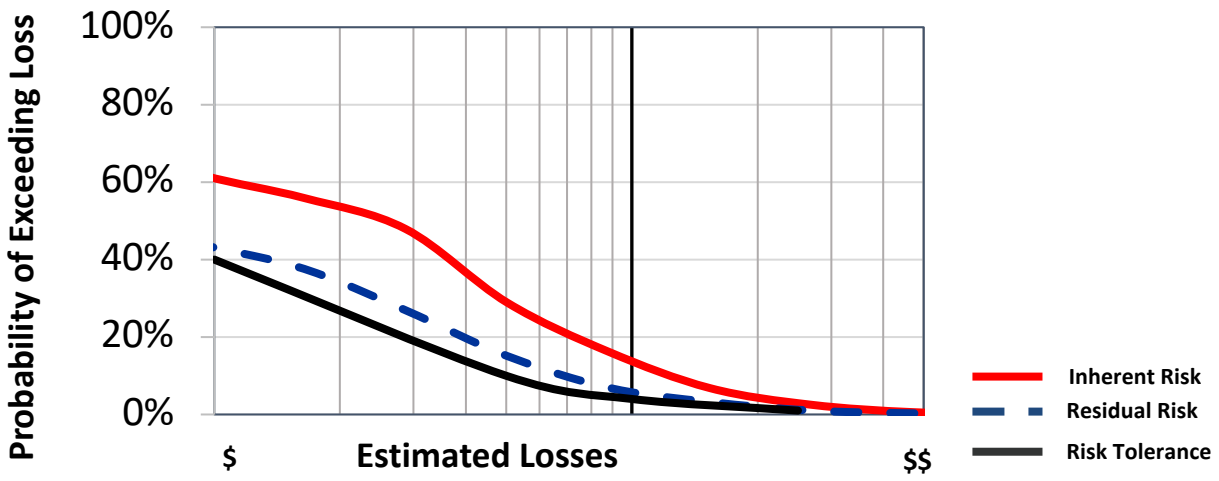
Executive Management risk discussions include:
- Risk posture,
- Emerging threats and regulations
- Approval of mitigation plans

ASLRRA Webinars

Risk Assessment & Mitigation Planning

Determine Your Risk Profile

Example Risk Curve



Evaluate Gaps to Prioritize Remediation or Skip to CIS Implementation Groups

Utility Assessment

Mitigation	Utility
Application Safe Listing	85%

Impact Assessment

Computer Type	Annual Likelihood of Compromise
Windows Workstations	8%
Windows Servers	.5%
Linux Servers	.1%

Opportunity

Risk Reduction	Annual Cost
$740K	$1.2M
$20K	$.4M
$100K	$1.2M

Assessment

The initial assessment is due March 31st.
Is this hard to complete?

- Maybe… There's no room for it depends
  - Anyone that takes a risk-based approach to mitigation will face a Yes / No dilemma
- Existing gap assessments against common frameworks may jump start the response
  - NIST (What to do) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov) 1-4 Partial, Risk Informed, Repeatable, Adaptive
  - CIS (How to do it) CIS Critical Security Controls (cisecurity.org)
  - TSA – uses same functions and categories as NIST

    Similarities Stop There

    FAQ 47 Current and accurate assessment information can be used to complete the TSA Vulnerability Assessment
- Start thinking through your mitigation plans
  - The additional information column **must** include the following information based on the response:

    Yes – list the security plan, policy, document name or provide a brief explanation

    No – Identify the gap, **intended mitigation measures**, and the **mitigation timeline**.
- Currently there is no specific public funding available for companies to meet the requirements of the security directives

There is work to do here, but understanding your current environment is a required starting point.

Sensitive Security Information

OMB Control Number 1652-0074
Exp. 05/31/2022

This record contains Sensitive Security Information when completed

7.02	Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented?	<Select>	
7.03	Does your company ensure user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company?	<Select>	
7.04	Has your company implemented the following measures?		
7.04A	Establish and enforce access control policies for local and remote users.	<Select>	
7.04B	Have procedures and controls in place for approving and enforcing remote and third-party connections.	<Select>	
7.05	Are access control levels of permission and privileges defined in the IT/ OT security plan?	<Select>	
7.06	Does your company ensure appropriate segregation of duties is in place and where this is not feasible, apply appropriate compensating security controls?	<Select>	

Operational Technology (OT) Systems

Operational Technology System is a general term that encompasses several types of control systems, including industrial control systems (ICS), supervisory control and data acquisition systems (SCADA), distributed control systems (DCS), and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment

Cyber Assets that are operational technologies that can control surface operations?

- Signals
- Grade Crossing
- Dispatch
- PTC
- Transportation Management
- Bill of Lading / Customer Orders

Cyber assets that are OT systems that monitor surface operations?

- Hot Box Detectors
- Wheel Impact Load Detectors
- Dragging Equipment Detectors
- AEI Readers
- Presence Detectors

Response Plan

180 Days to Implement a Cybersecurity Incident Response Plan.

- Include measures to reduce the risk of operational disruption
- Prompt identification
- Isolation and segregation of infected systems
- Limit the spread of malware
- Deny continued attacker access
- Determining the extent of compromise
- Preservation of evidence
- Establishing offline backup capabilities
- Establish capability to for isolating IT and OT systems

Plans must be exercised annually

Security Coordinator must certify requirements have been met.

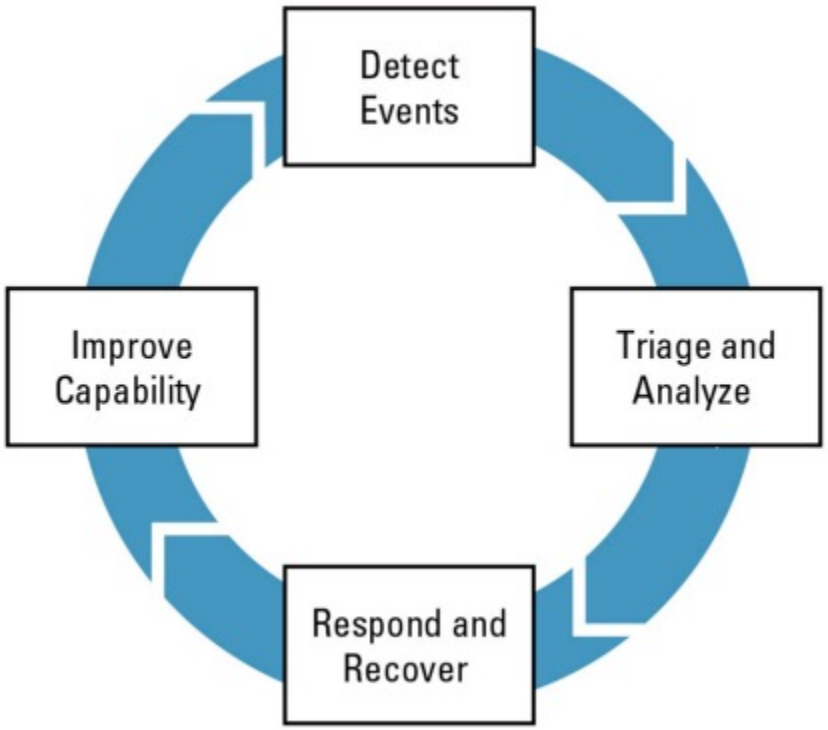
Testing the plans drives continuous improvement

Response Plan

CRR Supplemental Resource Guide Volume 5 Incident Management Version 1.1

[CRR Supplemental Resource Guide, Volume 5: Incident Management (cisa.gov)]

< 56 Days



3 Days

18 Days

Business Sustainment Plans for Interim

[Cyber Incident Checklist (cisecurity.org)]

Establish Reliable Facts and a way to Stay Informed

- Who is reporting the problem
- What do we know so far
- When did the breach occur
- Where did the breach occur
- How much do we know
- How will we stay informed

Mobilize a Response

- Who has the lead
- Who else has been notified
- Who else should be notified
- What expertise is on hand to work the problem
- What additional help do you need
- Who will provide it

Communicate What You Know

- Bad news does not get better with age
- General rule is that the first report is always wrong
- Release your initial public statement as soon as you have a reasonable command of the problem and can explain what you are doing
- Be prepared to explain the pre-existing cybersecurity posture and the measures that were in place to prevent events
- Establish a regular cadence of updates

ASLRRA Webinars

Incident Reporting

Requirement is in force as of January 1st

Owner Operators must report with 24 hours

- Unauthorized access- includes non-malicious policy violations
- Discovery of malicious software on a system
- Activity resulting in a denial of service
- Any cybersecurity incident that results in operational disruption

TSA Guidance

- Reports should focus on activity that is ~~significant~~ from a cybersecurity perspective
- FAQ 27 – To the extent Owner / Operators have questions regarding whether a specific type of cybersecurity incident must be reported, please email your questions TSA
- Owner / Operators should not expect a response from CISA after reporting a cybersecurity incident.
- Individual reports of cybersecurity incidents is required. Consolidated logs are not allowed

What to include in the reporting

- Affected rail systems or facilities
- Description of threat or incident
- Earliest date of compromise
- Date of detection
- Who has been notified
- Steps that have been taken
- Any relevant information collected
- Any known threat information including source of threat
- Description of impact or potential impact
- Description of all responses that are planned or under consideration including a reversion to manual operations

In order to meet the 24-hour reporting time frame, supplemental report will be required

Q&A

What should my RR know from UP experience?

Is the assistance available to help hit the March 31st assessment deadline?

Questions, Please Contact:

Jeanne Petty, VP, Product Development, PS Technology

Phone: (402) 544-0705 Email: Jeanne.Petty@pstechnology.com

https://pstechnology.com/pst-technology-services-for-the-rail-industry/

Webinar Feedback / Suggestions, Please Contact:

Sabrina Waiss, SVP, Education & Business Services, ASLRRA (Swaiss@aslrra.org (202)585-3434)

Thanks to Our Generous Sponsor

PST

ENTERPRISE DETAILS DONE WELL