Meet TSA Directive Requirements.

Eliminate Guesswork

We can help get your paperwork and responses in order, help connect you with technology solutions and more.

Schedule A Call

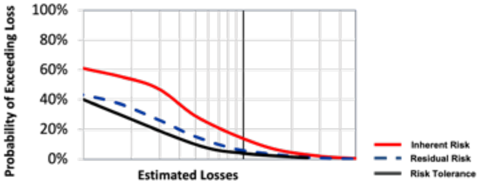
Cybersecurity

Leverage years of business and rail knowledge.

PST will help you navigate the "Defender's 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"?*

PST has significant experience in managing regulatory requirements while not losing sight of how railroads need to do business. We do not sell hardware or security solutions. However, we are fluent in assessments and in establishing response plans.



During our evaluations, we help you understand any gaps and then prioritize remediation. This is done by understanding the initial assessment, then reviewing the assessment findings and finally, looking at the risk reduction as compared to the annual cost of that reduction.

What does it mean to comply?

The answer is different for every railroad. During the assessment process, PST keeps a close eye on what an assessment item might mean when engaging a response plan. Not all risks are the same and not all responses deserve the same weight.

The Response Plan is how manage the items found by the Risk Assessment. PST can help you establish and even engage your railroad's response plan.

Key Approaches and Outcomes

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

Common Frameworks

Approach

This a “What to do” element. PST utilizes the tried and true National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity. The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes.

Outcome

The Framework offers a flexible way to address cybersecurity, including cybersecurity’s effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT).

Identification Methods

Approach

The next step is identifying the response methods. This is not a plan per se, but a way of thinking about the risk and what might be done. We use the Center for Internet Security (CIS) controls approaches to provide context for the action.

Outcome

The CIS Critical Security Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software.

Continuous Assessment

Approach

Between the NIST and CIS framework reviews, railroads will have enough to complete the current [03-31-2022] assessment requirements.

Outcome

While the initial assessment will fulfill the requirement, preparing for a way to perform continuous assessments is highly recommended. This will protect railroads from allowing technology, process or assessment debt from building up which might require more significant time and response requirements in the future.

TOP

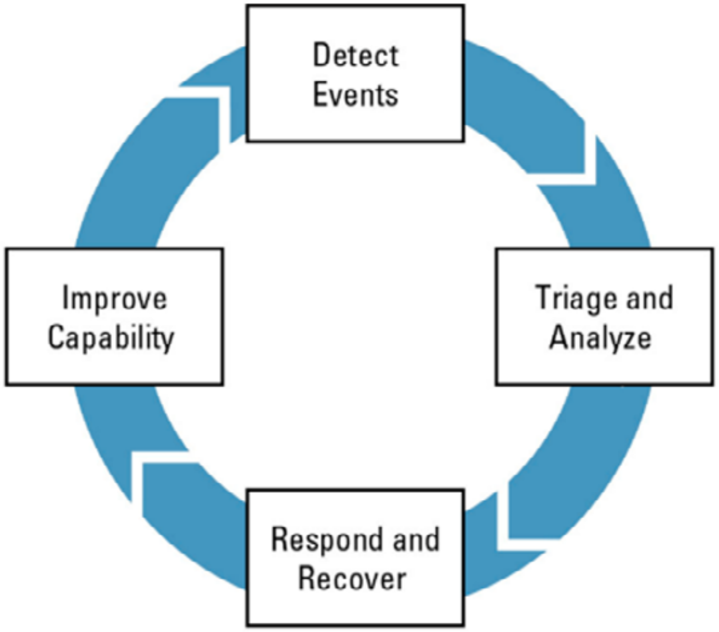
A Business Sustainment plan for Incident management response is also suggested.

Response Plans

*Railroads must then develop and activate a response plan to deal with outcomes of the cybersecurity assessment. **Third parties, such as PST, can be engaged to manage a railroad's response plan.** Establishing and activating a response plan is not difficult, but it is very comprehensive and covers:*

- » 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 off-line backup capabilities
- » Establish capability to for isolating IT and OT systems

Plans must be exercised annually. A Security Coordinator must certify requirements have been met.



Other Necessities

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

PST Technology Services

With over 30 years of providing software and technology services to freight and passenger roads of all sizes, there is virtually nothing PS Technology hasn't done or integrated with.

Technical Services that we can help with:

- Cybersecurity and TSA Compliance
- Tech Obsolescence Planning
- Legacy Systems and Coding Maintenance
- Railroad Business Process Improvement
- Technology or Network Upgrade Paths and Design
- System Upkeep
- Custom Coding
- SAP™, Oracle™, Azure™ Integration
- ERP selection and integration

Want to schedule a Call?

Click Here.

PSTechServices™

PS Technology
248 Centennial Parkway
Suite 150
Louisville, CO 80027

800-766-1630

www.pstechnology.com

TOP