Process Solutions

Honeywell

White Paper

Cyber Security Regulations: Pipe Dream or Reality?

Executive Summary

The Transportation Security Administration (TSA) recently released a revision to their existing TSA Pipeline Security Guidelines[1] to incorporate recommendations for improving pipeline security practices. This revision encourages pipeline operators to develop and implement a risk-based cyber security plan. The TSA recognizes the need for more stringent cyber security controls and these guidelines have set the stage for future regulatory compliance.

However, getting ready for this potential regulatory compliance in a pipeline environment doesn't have to be overwhelming – embracing cyber security and leveraging well established best practices and strategies is the epitome to developing a holistic security program and effectively reducing the risk.

[1] See http://www.tsa.gov/assets/pdf/guidelines_final_apr2011.pdf

Table of Contents

Scope of Guidelines

Who is Affected? Which Types of Pipelines are Mentioned in the Guidelines?

The TSA guidelines are applicable for pipeline operators who are responsible for the following types of pipelines:

- Natural gas and hazardous liquid transmission pipelines
- Natural gas distribution pipelines
- Liquefied natural gas facility operators
- Pipelines that transport toxic inhalation hazards (TIH) materials

Figure 1: The TSA guidelines are applicable for all types of pipelines.

Cyber Security Best Practices for Pipelines: Security Plans

The TSA Pipeline Security Guidelines outline the necessary framework to enable pipeline operators to develop and implement a risk-based cyber security program. A risk-based approach will allow pipeline operators to customize their security program to the needs, and more importantly, the viable security risks associated with their company.

Elements

TSA defines the recommended elements of a security program that all pipeline operators should incorporate into their program. These elements include:

- System(s) description
- Security administration and management structure
- Risk analysis and assessments
- Physical security and access control measures
- Equipment maintenance and testing
- Personnel screening
- Communications
- Personnel training
- Drills and exercises
- Security incident procedures
- NTAS response procedures
- Plan reviews
- Recordkeeping
- Cyber/SCADA system security measures
- Essential security contact listings
- Security testing and audits

Security Framework

As part of the framework, the TSA has outlined a three-step process for pipeline operators to follow during the design and development of their security program. The first step involves performing a criticality assessment using the set of criteria outlined in the guideline. The outcome of the assessment is to properly identify critical and non-critical facilities in order to ensure the most vital assets in the pipeline industry have the highest security protection applied.

Baseline vs. Enhanced Facility Security Measures

The second step in the process involves identifying the necessary facility security measures that are to be implemented. For non-critical facilities, the TSA recommends the pipeline owner to adopt the baseline security measures. The baseline security measures include:

- Physical security and access controls (i.e. secure doors, gates, or entrances)
- Personnel security (i.e. ID badges, pre-employment background checks)
- Equipment maintenance and testing
- Personnel training (i.e. teaching employees how to identify social engineering attacks[2])
- Exercise and drills
- Incident response
- Document management (i.e. information protection; making security documentation available to personnel)

[2] See http://www.microsoft.com/security/resources/socialengineering-whatis.aspx

For critical facilities, pipeline operators are to perform a security vulnerability assessment to identify, evaluate, and prioritize their risks. The outcome of this assessment will determine the appropriate security measures required to properly mitigate or reduce risks. The security vulnerability assessment may include asset characterization, threat assessment, vulnerability assessment, risk determination and possible countermeasures to reduce the risk. Once completed, the pipeline operators are to adopt both baseline and enhanced facility security measures.

Baseline vs. Enhanced Cyber Asset Security Measures

The final step is critical asset identification. This includes identifying and classifying all cyber assets to determine the appropriate cyber asset security measures to implement.

Cyber assets that are not essential to the safety and/or reliability objectives of the facility are classified as non-critical and baseline cyber security measures are to be applied to these assets. Baseline cyber security measures include strict access control, system and restoration recovery plans, secure system and network architecture and defining cyber security roles and responsibilities.

Alternatively, cyber assets that are essential to the safety and/or reliability objectives of the facility are classified as critical. These cyber assets are subject to both the baseline and enhanced cyber security measures. Enhanced cyber security measures require stricter access control requirements and periodical vulnerability assessments.

It’s important to note that the TSA guidelines strongly recommend that **both critical facilities and non-critical facilities** should implement the Department of Homeland Security’s National Terrorism Advisory System (NTAS) threat level protection measures. If there is a heightened threat of terrorism, the NTAS measures supply strict security measures that will help protect pipeline facilities.

Security: Beyond External Threats

In recent years, cyber security concerns in industrial environments have significantly increased. The shift from proprietary, isolated control systems to open standards and interconnected networks has increased the cyber security threats.

The impact of a cyber security breach within the pipeline environment is far-reaching, including but not limited to:

- Unauthorized access, theft, or misuse of SCADA information
- Communication failure
- Line down, resulting in loss of transportation capacity
- Equipment damage
- Environmental damage
- Public health and safety
- Personal injury
- Violation of legal and regulatory requirements

Pipeline operators need to recognize cyber security's crucial role in the reliability and robustness of their networks and systems. Cyber security will continue to become entrenched in the pipeline industry as systems continue to shift to open standards and protocols and as accessibility and sharing of information, whether with governmental bodies or corporate systems, increases.

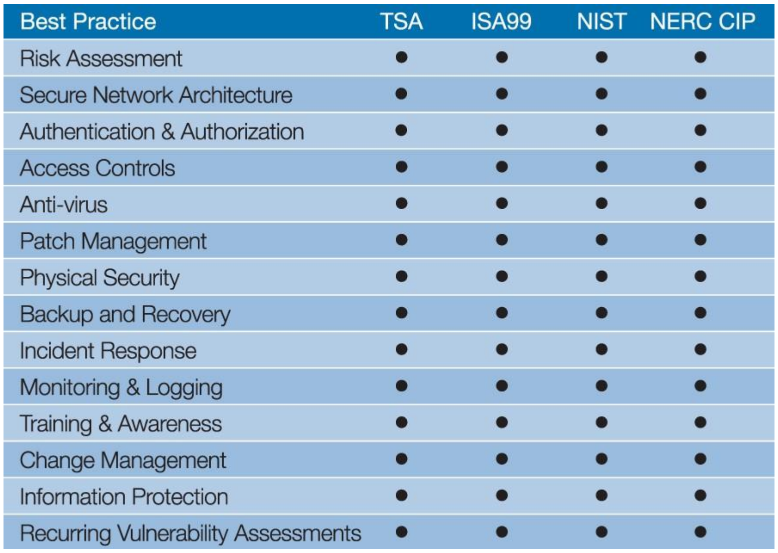
The focus tends to be on protecting against the outsider threats (i.e. hackers, terrorists) and this is demonstrated through the recurring news headlines highlighting yet another cyber attack. However pipeline security has greater implications than only preventing targeted and motivated cyber attacks. Pipeline operators need to consider the risks associated with a far more probable threat vector, the inadvertent and non-malicious cyber breach. This includes insiders who are in trusted situations and locations circumventing security policies without understanding the repercussions and risks of doing so. In the future, cyber security should become as visible as safety in the workplace – with physical and cyber security of equal importance to continued operational success.

Figure 2: Cyber security will continue to be an important aspect of pipeline operations in the future.

The TSA Pipeline Security Guidelines are only recommendations. As a result, they are not mandatory – nor are the guidelines enforced. However, with the escalating spotlight on the cyber security threats in the industrial environment and public awareness of cyber incidents, regulation may be a possibility for the pipeline industry (similar to the NERC CIP regulations in the power industry). It's a good idea to be prepared – pipeline operators should shift from reactive to proactive and begin the process of adopting a long-term cyber security strategy before regulations become mandated and pipeline operators are forced to comply.

Executing Guideline Requirements

The recommendations in the TSA guidelines are quite similar to other well established industry standards. The overall premise of the TSA guidelines and other industry standards is to assess and mitigate cyber security risk. Pipeline operators need to recognize that the most important part of a security program is is not the specific standard you chose to use. The importance is on understanding your business risks, being proactive, embracing a security philosophy and developing a long-term security strategy that eliminates (or reduces) the risk. Pipeline operators can use both the TSA guidelines and other similar standards to create their own best practices. Although targeted to the power industry, NERC CIP guidelines are a good resource for cyber security best practices.



Best Practice	TSA	ISA99	NIST	NERC CIP
Risk Assessment	●	●	●	●
Secure Network Architecture	●	●	●	●
Authentication & Authorization	●	●	●	●
Access Controls	●	●	●	●
Anti-virus	●	●	●	●
Patch Management	●	●	●	●
Physical Security	●	●	●	●
Backup and Recovery	●	●	●	●
Incident Response	●	●	●	●
Monitoring & Logging	●	●	●	●
Training & Awareness	●	●	●	●
Change Management	●	●	●	●
Information Protection	●	●	●	●
Recurring Vulnerability Assessments	●	●	●	●

Figure 3: Comparison of best practices recommended in different standards.

Steps to Get Started

Before drafting a proactive, long-term cyber security strategy, it's imperative to involve all communities of interest, such as operations, engineers, IT, etc. in order to ensure that stakeholders have appropriate input and buy-in.

Shifting to proactive long-term cyber security strategy includes:

- **Start with an IT inventory:** Identify all assets in the facility (i.e. operator stations, servers, network equipment). Record information such as the type of operating system, IP address and subnet mask, and the vendor software each asset uses.
- **Perform a risk assessment:** Identify all the risks within your environment. This includes identify all the possible threats and associated security vulnerabilities.
- **Create an action plan:** Create an action plan that prioritizes all the vulnerabilities identified during your risk assessment. The action plan must outline the necessary remediation steps to minimize (or eliminate) the risk. Timelines should be included.
- **Remember PPT (People, Process, and Technology):** There are three main components of security: people, process and technology. For a security program to be successful, all three of these elements must be accounted for in the security strategy.

For example, a facility could conduct employee security awareness training (the People component); create an incident response plan (the Process component); and maintain up-to-date anti-virus software (the Technology component).

Moving Forward

The bottom line is that TSA acknowledges the severity of the cyber security risks and the gap in the use of proper security controls within the pipepline industry through the release of the revised Pipeline Security Guidelines. The pipeline industry seems to be following in the footsteps of the power industry (with NERC CIP) and as a result, mandatory compliance may be looming. Regardless what the future holds for the pipeline industry, pipeline operators have a tremendous opportunity right now to think beyond the bureaucracy of compliance and regulation and understand that cyber security is really about ensuring safe, reliable and expected system behavior.

The benefits of a long-term security strategy allows pipeline operators time to socialize the concept of security, increase employee support, induce a security culture and spread the costs and effort over a greater length of time. Moreover, this will favorably position organizations when regulatory standards are mandated across the pipeline industry. Remember, security should not be viewed as a single project – it is an ongoing program and culture.

The TSA Pipeline Security Guidelines provide a practical place to start for both large and small, critical and non-critical pipeline facilities. Implementing even a baseline security model across a pipeline facility increases the likelihood of safe, reliable operations and minimizes potential security incidents. In other words, even small cyber security improvements lessen risk!

by Stacey Kelly, MIT, CISSP
Senior Sales Support Consultant, Honeywell Industrial Cyber Security Solutions

For More Information
Learn more about how Honeywell can help you secure your control systems and networks and help you comply with cyber security regulations, visit www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

WP-12-13-ENG
Nov 2014
Printed in USA

Honeywell