ARMEXA

Q&A with Armexa's Co-Founders:

Complying with TSA's Pipeline Cybersecurity Directives

Q&A with Armexa's Co-Founders:

Complying with TSA's Pipeline Cybersecurity Directives

The ransomware attack on the Colonial Pipeline could have happened to any midstream company. The event exposed risks and vulnerabilities within critical infrastructure — and prompted the Transportation Security Agency (TSA) to issue a number of new security directives.

The guidelines mandate for pipeline owners and operators significantly upgrade their defenses to safeguard their information and data streams against cyberattacks. Although compliance might seem challenging, complying with the regulations can unlock benefits for your organization far beyond the security scope.

In this Q&A, Jacob Marzloff, president and co-founder of Armexa, and Eric Forner, chief technology officer and co-founder of Armexa, share their operational technology (OT) security insight into how midstream operators can create a seamless cybersecurity framework that complies with the TSA's new directives while driving value across the enterprise.

1. How can organizations begin meeting TSA's new pipeline security directives if their security measures are limited?

Organizations with limited measures should start by defining and agreeing on goals and policies between IT and OT, then focus on perimeter security. It's best to take small steps and work toward an extensible security framework. This way, if you operate in both the upstream and midstream markets, the same framework can be scaled to serve both segments andeliminate the need to restart your security journey asmore directives are released in the future.

Treat the deployment process like any other safety program. If you secure the network, endpoint, and access, then you are on the right track. Focus on perimeter security and define and agree on IT and OT goals and policies. The framework should secure unprotected areas in your OT environment and push security controls deeper into the OT over time. It should also tighten firewall policies, route traffic through the firewall, and include a plan for training your employees on the new security policies.

2. Does the TSA accept alternative measures toward an interpretation of the directives versus the written regulations?

Yes, the TSA can accept alternative measures. If you are unsure about the interpretation, taking a few small steps will help increase compliance with the directives. That includes establishing mitigation controls and implementing a mitigation plan around the guidelines you can't meet or are unsure about. In our experience, focusing on foundational OT security controls and implementing them well can be seen as an acceptable alternative to strict compliance. Your mitigation plan also needs to span a few years and include a detailed implementation roadmap.

We suggest starting with perimeter security with a flexible roadmap that allows for device upgrades and/or replacement at the end of service life.

3. Does any company that wants to operate in the United States need to comply with the directives? What if the company is not an identified operator with access to the TSA guidelines?

Currently, the TSA Security Directive 2 for Pipeline applies to select midstream operators. If you are not an identified midstream operator with access to the directives, other publicly available OT security standards are suitable. Many clients have successfully complied with the TSA directives by using public standards as a framework.

We suggest that all midstream operators understand the guidelines and begin planning. We also recommend considering compliance measures in the design phase, which offers the chance to architect the network correctly the first time. While building out panels and OT infrastructure, we recommend guiding the system integrators to enable security features with firmware that complies with the TSA directives or other public standards. This forward-thinking approach can help ensure long-term compliance as regulations evolve.

4. What is the business case for dealing with TSA directives? How can an organization justify the effort to business line managers?

Correct implementation of operational security delivers tremendous business-enablement value. A thorough understanding of the network environment, its overall health, and its connectivity offers more advantages than just improving your overall OT security posture. Expert OT insight can identify and ameliorate issues that impact business operations and productivity.

For example, one company experienced a network issue that caused a compressor station to go offline. The issue went unnoticed for years. After collaborating with the team to better understand the network, we implemented a solution that resolved the root issue and increased the compressor station's uptime. This demonstrates that security expertise can unearth opportunities to improve operational processes and maximize uptime, in line with business line managers' objectives.

Jacob and Eric were guests on the Oil & Gas Journal webinar, "TSA's New Security Directives: How can your company meet compliance more efficiently?" Watch the full webinar on demand to learn more about how your organization can accelerate compliance with the new regulations—and optimize business operations in the process.