Pipeline Cyber Security Issues
October 20, 2021
Scott Gorton • Tim Gaither

Scott C. Gorton, Executive Director

Surface Policy Division

- In present position since 2019
- Over 15 years with TSA
- He is responsible for the development and sustainment of policies and guidance for the surface modes of transportation including freight rail, mass transit, highway motor carrier, pipeline, and maritime. He leads TSA's engagement with surface industry trade associations and national working groups

Tim Gaither, Director

Preparedness, Emergency Support, and Security Division (PESS)

- PESS Director since December 2020
- Former Assoc. Director of DOT's Crisis Management Center
- Over 16 years of emergency management and preparedness experience
- United States Navy Veteran
- BS in Business Management
- Master's in Strategic Security Studies
- War College Diploma in International Security and Combatting Terrorism

Agenda

- Case Study
- Security Issues/concerns
- TSA and PHMSA Memorandum of Understanding
- TSA Security Directives
- PHMSA Cyber Hygiene Discussions
- Lessons Learned and Path Forward

Case Study

Colonial Cybersecurity Incident

Overview

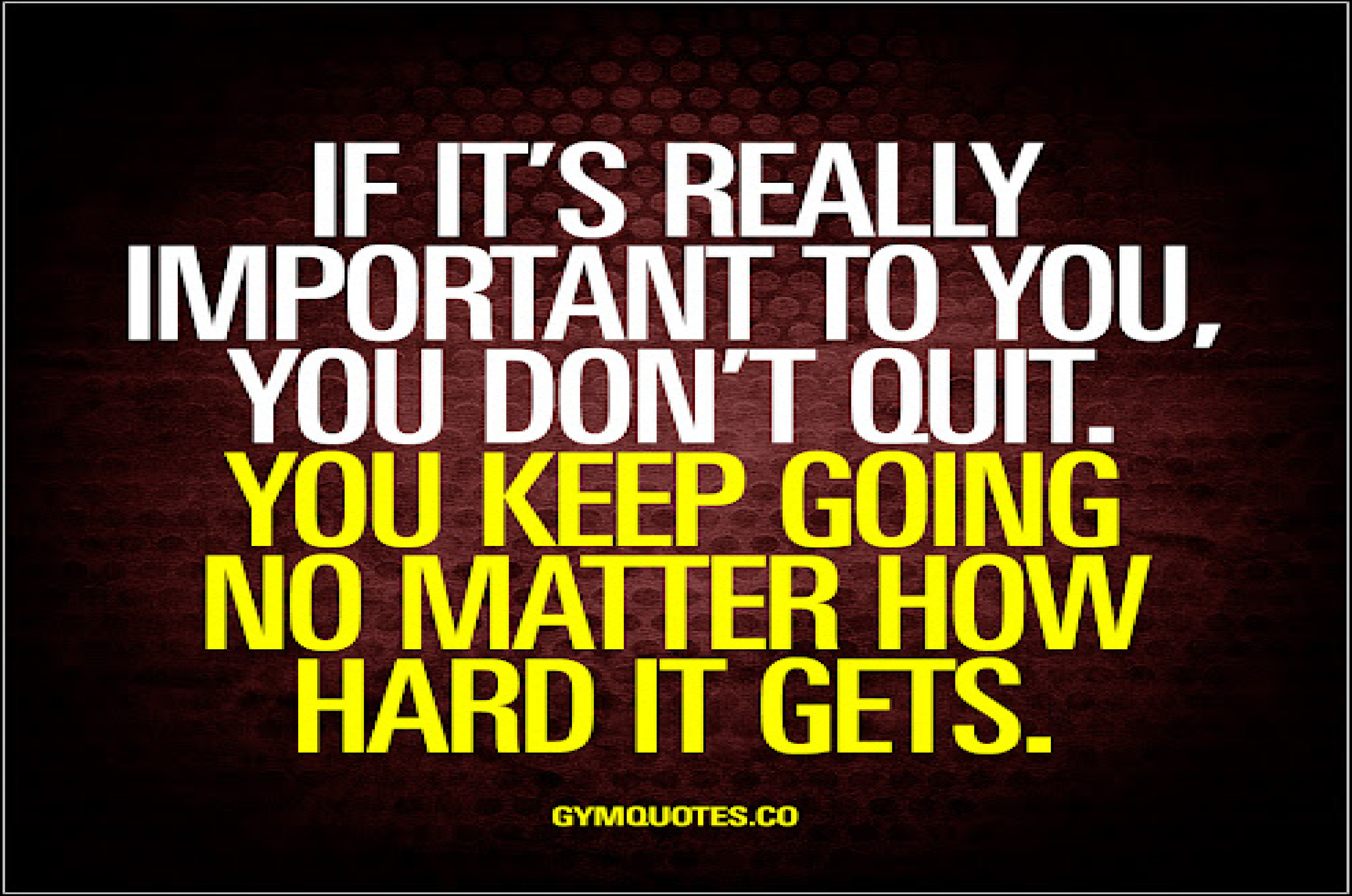
Coordination

- Response
  - Information Sharing
  - Collaboration between government and private industry
  - Supply shortages, vector of attack, resolved when
- Next Steps
  - Security Directives
  - Review of current policy

Agency Perspectives

- TSA
  - The Colonial event demonstrated the continued need for pipelines to plan for cybersecurity incidents and take measures to protect both IT and OT systems
- PHMSA
  - Demonstrated that operators need to ensure they can conduct manual operations safely
  - Need to be prepared to activate emergency response plans to address accidents of all types

Security Issues/concerns



IF IT'S REALLY IMPORTANT TO YOU, YOU DON'T QUIT.

YOU KEEP GOING NO MATTER HOW HARD IT GETS.

GYMQUOTES.CO

Ongoing Threats

- Who would attack U.S. pipeline infrastructure?
  - Criminal Actors (Ransomware), Nation-State Actors (Exfiltration of data)
- ODNI Worldwide Threat Assessment of the US Intelligence Community
  - "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States." (January 2019)
- CISA/FBI Joint Alert AA21-201A
  - This Joint Cybersecurity Advisory—coauthored by the Cybersecurity and Infrastructure Security Agency and the FBI—provides information on a spearphishing and intrusion campaign conducted by state-sponsored Chinese actors that occurred from December 2011 to 2013, targeting U.S. oil and natural gas (ONG) pipeline companies
  - "CISA and the FBI assess that this activity was ultimately intended to help China develop cyberattack capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations."

Implications for Security

- The primary concern with cyber attacks on pipelines (and other critical infrastructure) is the potential for cyber attacks to produce kinetic effects
    - Shutdowns, reductions in service
    - Potential for physical damage

Implications for Safety

- Adversaries can change pressure levels, control pipeline systems, and shutdown pipelines
- Can lead to:
  - Impacts to environment
  - Impacts to the public
  - Impact to employees

TSA/PHMSA
Memorandum of Understanding

Overview

- PHMSA provides pipeline incident and accident information
- TSA shares security incidents and threats to pipeline infrastructure
- Establishes communication protocols to ensure PHMSA supports CISA with its cybersecurity protocols

TSA Security Directives

TSA’s Security Directive Authority

- In response to the ongoing cybersecurity threat to pipeline systems, TSA used its authority under 49 U.S.C. 114 to issue security directives to owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas. to implement a number of urgently needed protections against cyber intrusions
- 49 U.S.C. 114(*l*)(2)(A), authorizes TSA to issue emergency regulations or security directives without providing notice or public comment where “the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security. . . .”
- Security directives issued pursuant to the procedures in 49 U.S.C. 114(*l*)(2) “shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Transportation Security Oversight Board or rescinded by the Administrator.”

Security Directive Development

- When developing Security Directives, TSA consults with both industry and government partners to get critical input on the applicability and provisions of the proposed directive.
- In the case of the pipeline directives, TSA initially consulted with the Department of Transportation (PHMSA), Department of Energy (CESER), Coast Guard, and Federal Energy Regulatory Commission
- TSA then provided a draft of the SDs with the trade associations representing pipelines and the Pipeline Working Group of the ONG Sector Coordinating Council
- In addition to accepting written comments, TSA held conference calls with the industry reviewers.
- Where appropriate, the comments and suggestions provided by industry and government partners were incorporated into the SD

Security Directive No. 1

- On May 28, 2021 TSA issued a Security Directive (Pipeline-2021-1)
- The SD is applicable to the owners and operators of hazardous liquid and natural gas pipelines that have been identified as critical by TSA
- The SD requires three actions:
  1) Designation of a Cybersecurity Coordinator
  2) Reporting of cybersecurity incidents to CISA Central within 12 hours of identification
  3) Conducting a self-assessment of the Owner/Operators' practices and activities in relation to the cybersecurity guidelines contained in the TSA Pipeline Security Guidelines
     - Owner/Operators must submit the results of their assessment to TSA

- The TSOB ratified the Security Directive on July 3, 2021

Security Directive No. 2

- Security Directive Pipeline-2021-02 was effective on July 26, 2021
- The SD is applicable to the same group of critical pipeline Owner/Operators covered by the first SD
- The SD requires three major actions-
  1) Implementation of critically important mitigation measures to reduce the risk of compromise from a cyberattack
  2) Development of a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption or significant business or functional degradation of necessary capacity, should the Information and/or Operational Technology systems of a pipeline are affected by a cybersecurity incident
  3) Testing of the effectiveness of the Owner/Operator's cybersecurity practices through an annual cybersecurity architecture design review

- The TSOB ratified the Security Directive on August 4, 2021

Actions Since Issuance of SDs

- There has been 100% compliance with the provisions of the first security directive
- There is a high degree of compliance with the provisions of the second security directive, but due to the complexity of the requirements, many of the owner/operators have requested alternative measures or extensions of time to complete required actions
- Safe operations without disruption is a primary concern and TSA is committed to working with the pipelines to implement the required measures in a manner that achieves the intended security outcome without compromising safety or operations

PHMSA Actions

- Information sharing
- Review Security Directives for any issues impacting safety and operations
- Alternate Plan review
- Guidance
  - Be specific about impacts to safety and operations
  - Continue to work with TSA and provide feedback

PHMSA Cyber Hygiene Discussions

Overview

- Based on TSA's Pipeline Security Guidelines
- Offered to Operators during Control Room Management Inspections
- Advanced Cyber Hygiene Awareness
- Discussions are NOT Inspections
- Document the occurrence of discussions, but no details
- About half of operators participate in discussions

Current Progress

- Years 1 & 2:
  - Offered to have discussions with 113 pipeline operators
  - Approximately 50% have declined
- Years 3 – 5:
  - Offer to have cyber discussions with 153 operators
- If PHMSA discovers:
  - Significant cybersecurity risks
  - Significant cybersecurity vulnerabilities
- Discretely shared with TSA and CISA

Lessons Learned and Path Forward

TSA Next Steps

- TSA will review and analyze the results of the assessments required by the security directives to determine what, if any, future actions may be required to address the cybersecurity of pipelines
- TSA will continue to work with PHMSA and other partners to assess and evaluate threats to pipelines and informing operators
- TSA is also working on establishing cybersecurity standards through rulemaking that will apply to pipelines and other modes of transportation

PHMSA Next Steps

- Continue to improve cooperation and collaboration
- Improve information sharing of pipeline incidents that significantly threaten fuel supply chains
- Private sector engagement
- Review regulations
- How can we improve as our adversaries improve

Points of Contact

Contact Information

- TSA
  - General inquiries TSA-Surface@tsa.dhs.gov
  - Pipeline Industry Engagement Manager
    - Chuck Phillips Charles.E.Phillips@tsa.dhs.gov
  - Pipeline Security Assessment Team
    - Ray Reese Raymond.Reese@tsa.dhs.gov
- PHMSA
  - Pipeline security concerns:
    - Timothy Gaither Timothy.Gaither@dot.gov
    - Jaime Espinoza Jaime.Espinoza@dot.gov

Questions