SANS Automotive Cybersecurity Summit 2017
Heavy Vehicle Cybersecurity Update

NMFTA Resources list:

NMFTA Web Site
http://www.nmfta.org/pages/HVCS

NMFTA Heavy Vehicle Cyber Security Bulletin
http://www.nmfta.org/documents/hvcs/NMFTA%20HVCS%20Bulletin%2009.09.2016.pdf

NMFTA Heavy Vehicle Cyber Security List Service
https://hvcslistservice.nmfta.org/

University of Tulsa & NMFTA CAN Data Logger
https://github.com/heavy-Vehicle-Networking-at-U-Tulsa/NMFTA-CAN-Logger

General J1939 Resources

University of Tulsa

The University of Tulsa's Crash Reconstruction Research Consortium
http://tucrrc.utulsa.edu/index.html
http://tucrrc.utulsa.edu/DecodingDataDumpIDs.html
http://tucrrc.utulsa.edu/J1939Database.html

SAE International

http://www.sae.org/standardsdev/groundvehicle/j1939a.htm

… in particular

http://standards.sae.org/j1939/21_201012/
http://standards.sae.org/j1939da_201611/

About NMFTA

The National Motor Freight Traffic Association, Inc. is a nonprofit membership organization headquartered in Alexandria, Virginia. NMFTA's membership is comprised of approximately 550 less-than-truckload motor freight carriers operating in interstate, intrastate and foreign commerce.

Since 1956, NMFTA has helped members meet the challenges confronting the transportation industry through representation, research, education, and the publication of specifications, rules, transportation codes and the preparation and dissemination of studies, reports and analyses. NMFTA has represented the interests of the LTL motor carrier industry in legislative matters before the United States Congress, issues involving regulatory agencies including the General Services Administration, Federal Motor Carrier Safety Administration and Military Surface Deployment and Distribution Command, and in judicial proceedings at the federal and state level.

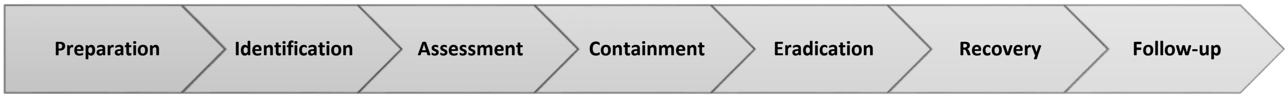
An excerpt from the NMFTA Heavy Vehicle Cyber Security Bulletin of September 2016…..

How can motor carriers prepare for a cyber security attack?

Given the increasing odds of a security breach, it is necessary to develop a plan to ensure you know how to recover and survive a breach or attack. A standard part of system security is an incident response plan. This plan outlines the process and procedures to follow in the event of an incident. It is highly recommended that all motor carriers immediately start working with heavy vehicle manufacturers and telematics providers, and associated third parties to develop a plan on how to recover.

Incident Response Plan

The following generic steps have been identified for responding to a major incident. Many steps can occur in parallel depending on the nature of the situation, e.g. multiple attack vectors or vulnerabilities, carriers, etc.



Preparation	Create team Establish communication plan and crisis management structure Conduct exercises
Identification	Identify if attack has occurred or is ongoing Identify the impacted assets
Assessment	Assess the scope, impact and risk of the incident Investigate the cause and establish first course of action Collect forensics and critical data for next steps Create profile of affected units
Containment	Minimize and isolate the damage or risk Use profile to strategically contain affected units Implement contingency plans to maintain continuity of business
Eradication	Determine the root cause Conduct analysis on forensics data collected and assets Restore / rebuild systems affected
Recovery	Implement irrevocable corrective actions Restore normal operations
Follow-up	Lessons learned collected and incident response plan is updated Identify other units with similar vulnerability and create remediation plans