TRUCKING INDUSTRY CYBERSECURITY

CYBER TECH CYBERGUARD

Trucking Industry Cybersecurity Guide

TSA and Surface Transportation Systems Sector (TSS) industry partners collaboration

- Addresses common **cyber threats and protection strategies** for company data, computer systems, vehicle fleets, and personal information.
- Emphasizes a comprehensive trucking operation cybersecurity approach encompassing both IT and operational technology.
- Provides detailed information on the safe use of Global Positioning Systems (GPS), Electronic logging devices (ELD), fleet management systems, mobile technology and social networks.

Cybersecurity

Cyber-attacks involve unauthorized access attempts to computers, computing systems/networks with the intent to cause damage.

- Transportation and logistics sector, including fleets, is increasingly targeted by cybercriminals due to rapid digitization.
- Cybersecurity is a crucial aspect of safeguarding assets, employees, passengers, cargo, and customers.
- Cybersecurity involves preventing, detecting, and responding to attacks to protect critical industry information resources.

Cybersecurity Importance

- Cyber-attacks on critical infrastructure, exploiting vulnerabilities and adapting to security measures.
- Growing threat due to remote and anonymous connectivity and ability to cause physical consequences virtually.

Cybersecurity Trucking Industry Threats

Hackers target trucking companies for various reasons, including:

- Accessing financial data, GPS tracking, customer information, credit cards, and personal info for illicit purposes.
- Using trucks as weapons and stealing the contents of truck payloads.

TRUCKING INDUSTRY CYBERSECURITY

CYBER TECH CYBERGUARD

Cybersecurity Challenges: Heavy Duty Fleets/Trucks

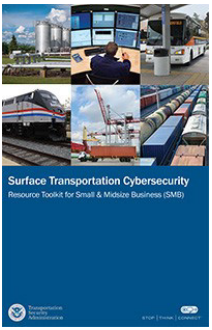
- Satellite/Cellular communications links heavy-duty trucks to telematics, fleet management, engine management apps, and Bluetooth.
- The above, along with smart devices connected to commercial vehicles, makes them vulnerable to cyber-attacks.
- Internal interconnected systems in heavy-duty vehicles are a significant cyber threat target
  - Commercial vehicle fleets with similar electronic configurations can be targeted by adversaries to develop exploits that attack multiple vehicles at once.

Data Sharing Leads to Cyber-Opportunity

- Fleet management systems pose multiple cybersecurity risks, including data storage, applications, and endpoint devices.
- Telematics involves technologies used by fleets to share data between vehicles and control centers
  - In-Vehicle Networks/CAN, GPS Tracking, TPMS, Electronic Logging Devices (ELDs), Bluetooth
- **DG Technologies offers the DPA XL: The first Cybersecure Vehicle Diagnostic Adapter for vehicle networks!**

Cybersecurity Attacks & Protection

- Attacks: Malware, Ransomware, Insider Threats, Spam/Email Scams, Social Networking
- Protection: Privacy and security settings, Info privacy, Password strengths and constant uniqueness.
- **Devices: Use of Cybersecure devices, like DG's DPA XL!**



The Transportation Security Administration (TSA) provides a Surface Transportation Cybersecurity Toolkit

https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit

DG TECHNOLOGIES
Vehicle Network Solutions
www.dgtech.com/cyber-security

SYNERCON TECHNOLOGIES
A DEARBORN GROUP COMPANY

DG Technologies supports industry, state/government and college/vocational vehicle cybersecurity testing efforts