CONOPS

Trucking Fleet Concept of Operations (CONOPS) for Managing Mixed Fleets

RESEARCH BRIEF

Securing Fleet Operations: Navigating the Cybersecurity Landscape

Understanding Risks and Roles in a Connected Fleet Environment

Introduction

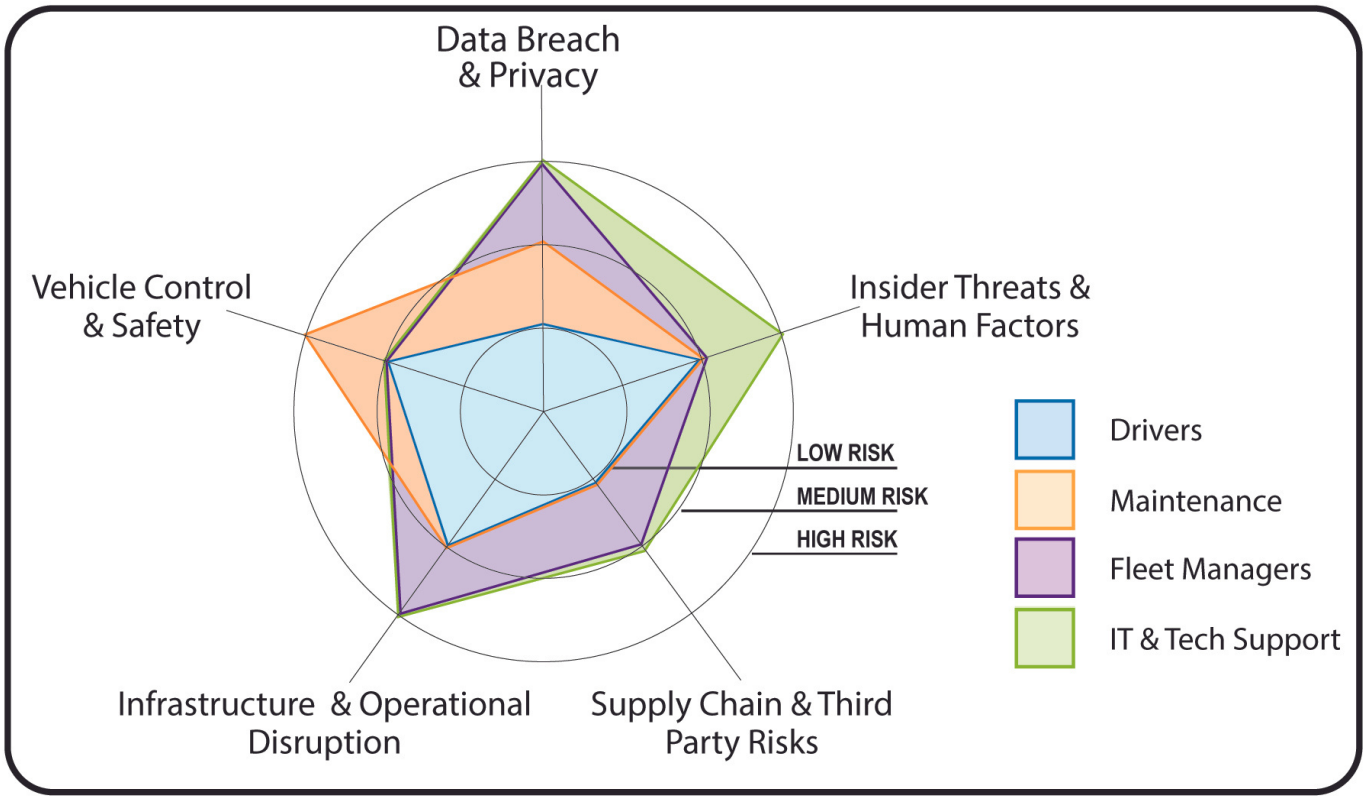
The adoption of driving automation systems in commercial motor vehicle (CMV) fleets is rapidly expanding and is expected to continue growing. According to the 2021 United States Department of Transportation (USDOT) comprehensive plan for automated vehicles, automated trucking companies are actively developing Level 4 Automated Driving Systems (ADS). However, as CMV fleets with ADS become more prevalent, they may attract the attention of malicious actors seeking to exploit vulnerabilities for financial gain, data theft, and disruption of operations. This poses risks not only to fleets but also to public safety, endangering drivers, passengers, and other road users. Malicious interference with the operation of CMVs could lead to accidents, disrupted traffic flow, cargo and supply chain disruption, and even loss of life. As fleets increasingly adopt a connected and data-driven approach, the importance of cybersecurity becomes obvious in protecting against physical tampering, unauthorized data access, and various cybersecurity threats.

Cyber risks pose danger to

- **Safety of drivers, cargo, and other road users**
- **Financial/reputation loss**
- **Privacy leaks**
- **Public trust in automated trucking technologies**

VTTI CONOPS

Fleet Cybersecurity Threat Radar



Threat Examples Severity Matrix

Severity \ Threats	Vehicle Control & Safety	Data Breach & Privacy	Supply Chain & Third-Party Risks	Infrastructure & Operational Disruption	Insider Threats & Human Factors
Low Impact	Unauthorized access to vehicle systems	Unauthorized access to fleet data	Inventory error	DDoS* attacks on operations	Poor cyber hygiene
Medium Impact	Spoofing of sensor data	Sensitive customer information theft	Insecure IoT* devices	GPS spoofing	Unintentional data leaks
High Impact	Manipulation of automated systems	Data tampering	Compromised software updates	Critical infrastructure tampering	Insider attacks
Critical Impact	Remote vehicle takeover	Ransomware attacks	Fraudulent parts	Malware attacks	Social engineering exploits

*DDoS (Distributed Denial of Service): A cyber attack where numerous compromised computers flood a target system with traffic, making it unavailable to users.
*IoT (Interest of Things): The everyday devices that are connected to the internet for sending and receiving data.

DIVISION OF FREIGHT, TRANSIT, & HEAVY VEHICLE SAFETY
DHVY
VIRGINIA TECH TRANSPORTATION INSTITUTE