



FLEET CYBERSECURITY

Cybercrimes within the automotive industry have risen 400% in the last five years. Have you taken measures to protect your fleet from potential cyberattacks?

UNDERSTANDING CYBERATTACKS

Data Breach



When unauthorized individuals gain access to sensitive information of customers and drivers. The data is then used for identity theft and other crimes.

Ransomware



When malicious software infiltrates a company's systems and encrypts critical data. The attackers then demand a ransom in exchange for releasing the data.

System Hacking



When a hacker gains control of a fleet's telematics system and can access the routing and tracking for the entire fleet, potentially rerouting high-value loads to steal.

BUSINESS RISKS OF CYBERATTACKS



Cargo / Identity Theft

The trucking industry faced a 600% increase of identity theft and cargo theft from 2021 to 2022.



Reputation Damage

A company can face backlash and have their reputation tarnished when for years after a cyberattack.



Customer Loss

When customers no longer have confidence in a company, they will stop doing business with them.

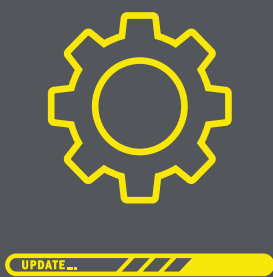


Financial Impact

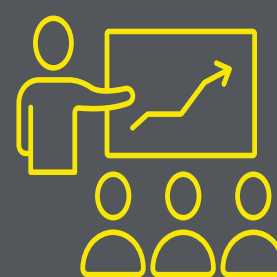
From ransom payments to lost jobs to recovery costs, cyberattacks can cause major financial losses.

PROTECTING AGAINST ATTACKS

Perform Regular Software Updates



Hold Employee Trainings



Use Threat Detection Systems



Encrypt all Sensitive Data



Conduct Routine Security Audits



Create an Incident Response Plan

