CYBER RISK EXPOSURE SCORECARD - TRUCKING

DEELEY insurance group
Be sure.

Motor carriers and drivers may not seem like high-priority targets for hackers, but the reality is that the transportation industry is one of the most frequent targets for cyber attacks. Customer data, supply chain logistics, data lists and product data can be extremely valuable to hackers. Additionally, motor carriers and individual drivers can be put at greater risk because of outdated data systems, unsecured vehicles, location-based tracking systems and more.

If any of your business devices or vehicles are compromised, you could face ransomware attacks, social engineering schemes or even physical damage if a vehicle has self-driving technology. You also need to protect your customers' and employees' personal information, as a data breach can lead to damaging lawsuits and a tarnished reputation.

Instructions: Begin by answering the questions below. Each response will be given a numerical value depending on the answer:

Yes: 5 points | **No:** 0 points | **Unsure:** 5 points

After completing all of the questions, total your score to determine your level of cyber risk using the scale below.

QUESTIONS	YES	NO	UNSURE	SCORE
1. Do any of your drivers use mobile networks on the road, such as mobile hotspots or phones with Wi-Fi hotspot features?	☐	☐	☐	
2. Does your organization have a "bring your own device" policy that allows drivers or other employees to use personal devices for business use or on a company network?	☐	☐	☐	
3. Does your business operate at multiple internet-connected worksites—including third-party vendors and shippers—simultaneously?	☐	☐	☐	
4. Can any of your clients or drivers access administrative privileges on your networks or devices?	☐	☐	☐	
5. Do you allow drivers to let friends or family members ride as passengers?	☐	☐	☐	
6. Does your business track the location of drivers, shipments, or clients in a central or unencrypted location?	☐	☐	☐	
7. Does your business have a website or online platform that's used to collect data such as shipment progress, supply chain management or employee communications?	☐	☐	☐	
8. Does any software used on your worksites or vehicles require an update?	☐	☐	☐	

QUESTIONS	YES	NO	UNSURE	SCORE
9. Have any of your drivers ever failed to secure their vehicles at home, a rest stop or any other area?	☐	☐	☐	
10. Does your business use a third-party vendor for data storage or task management?	☐	☐	☐	
11. Does anyone at your business use computers to access bank accounts or initiate money transfers?	☐	☐	☐	
12. Does your business store sensitive information (e.g., financial reports, personal information and roadmaps) that could potentially compromise you if stolen?	☐	☐	☐	
13. Is it possible for an unauthorized person to access one of your vehicle's data diagnostic ports, either while it's at one of your worksites or out on the road?	☐	☐	☐	
14. Is network and cyber security training for employees or drivers optional?	☐	☐	☐	
15. Has your business ever failed to confirm that your third-party vendors use sufficient data protection procedures?	☐	☐	☐	
16. Have any of your employees or drivers failed to keep track of devices such as smartphones, laptops, tablets, hard drives or USB drives?	☐	☐	☐	
17. Has your business ever failed to train employees or subcontractors to recognize social engineering scams?	☐	☐	☐	
18. Would your business lose critical information in the event of a system failure or other network disaster?	☐	☐	☐	
19. Do any of your drivers use third-party services or apps to process deliveries or payment?	☐	☐	☐	
20. Has your business neglected to review its data security or cyber security policies and procedures within the last year?	☐	☐	☐	
TOTAL SCORE				

0-10 | Low risk.

15-25 | Moderate risk.

30-50 | High risk.

55-100 | Escalated risk.