Cyber Risk Exposure Scorecard

– Trucking and Transportation

The transportation sector increasingly faces cybersecurity challenges in today's interconnected world. As the industry embraces digital transformation and relies on interconnected systems and networks, it's crucial to prioritize and safeguard the integrity, confidentiality and availability of critical transportation infrastructure. Therefore, a comprehensive cybersecurity scorecard is a valuable tool for assessing the overall security posture of companies in the transportation sector. This scorecard highlights key areas of focus, including network security, data protection, access control, patch management, incident response, employee awareness, vendor and supply chain security, regulatory compliance, security governance and cybersecurity incident reporting.

Please assign a score from 0-5 for each question based on your organization's compliance or implementation level. A higher score indicates a better cybersecurity posture. Consistently evaluating and updating the scorecard will aid in monitoring progress and pinpointing areas for enhancement.

SCS AGENCY INSURANCE

Questions	Score
Network Security	
Is the transportation network protected by a robust firewall, intrusion detection and prevention systems, and secure configurations?	
Is the network regularly monitored for any anomalies or suspicious activities?	
Data Protection	
Is there a system in place to encrypt and safeguard sensitive data, such as passenger information, cargo and freight data, maintenance and engineering data, fleet management data, and payment and financial data during both transportation and storage?	
Is personal and confidential information securely stored and is access restricted to authorized personnel?	
Are regular backups performed to ensure data availability and integrity?	
Access Control	
Is a strong authentication mechanism, such as multifactor authentication, implemented to access critical systems?	
Are user access rights regularly reviewed and updated based on the principle of least privilege?	
Are physical access controls in place to restrict unauthorized entry to critical infrastructure?	
Patch Management	
Is there a well-defined process to identify, test and deploy security patches in a timely manner?	
Are software and firmware updates regularly applied to network devices and systems?	
Incident Response	
Is there an incident response plan in place that includes roles, responsibilities and communication channels?	
Are employees trained to recognize and report potential security incidents?	
Is there a dedicated team responsible for investigating and responding to security incidents?	
Employee Awareness	

Questions	Score
Are employees provided with regular cybersecurity awareness training?	
Are there mechanisms in place to ensure employees adhere to cybersecurity policies and best practices?	
Vendor and Supply Chain Security	
Are security requirements included in contracts with vendors and third-party suppliers?	
Are regular security assessments conducted for critical vendors and suppliers?	
Regulatory Compliance	
Is the transportation sector compliant with relevant cybersecurity regulations and standards?	
Are regular audits and assessments conducted to ensure compliance?	
Is there a process to stay updated with emerging regulations and adapt cybersecurity practices accordingly?	
Security Governance	
Is there a dedicated cybersecurity team responsible for overseeing and managing security efforts?	
Are security policies, standards and procedures documented and regularly reviewed?	
Cybersecurity Incident Reporting	
Is there a process for reporting cybersecurity incidents to relevant authorities and regulatory bodies?	
Is there a mechanism for sharing threat intelligence with other organizations in the transportation sector?	

Very High Risk: 0-50

High Risk: 55 – 75

Moderate Risk: 80 – 95

Low Risk: 100-120