Medical Transportation
Why Cyber Insurance?

Do you:

- Use medical software systems to manage booking and appointments?
- Store your patients' medical data on a shared network drive?
- Accept payment from patients or insurance companies electronically?
- Communicate with employees and hospitals via email on mobile devices?
- Allow drivers to access systems and client data from their own devices?

If you answered "Yes" to any of the above, you are a target for cyberattacks. Cyber insurance covers losses and expenses to recover from an incident including legal and policyholder notification services.

Common Cyber Risks for Medical Transportation Companies

Business Interruption (BI)

- A cyberattack could sabotage operations by shutting down booking and appointment systems leading to business interruption and loss of revenue.

Cyber insurance can cover revenue loss and the cost to rebuild systems.

Compromised Patient Information

- If your patients' data is stored electronically, you are vulnerable to cyber incidents that may compromise their medical and other private information.
- This can result in a lawsuit from affected patients and regulation penalties.

Cyber insurance with third party liability coverage can cover expenses related to the incident and more.

Phishing and Email Scams

- The number of phishing attacks have skyrocketed, and these could lead to unauthorized access of your system and digital assets.

A cyber insurance policy with first party liability and cybercrime coverage can cover the cost of such incidents. Our policies come with cybersecurity awareness training for employees which can help prevent phishing attacks.

Lost or Stolen Mobile Device

- Drivers and employees might operate and communicate with patients and medical services using mobile devices. When such devices are stolen or lost, sensitive data might get compromised potentially resulting in lawsuits from patients.

Cyber insurance can cover breach investigation, notification of impacted individuals and legal services if needed.

COWBELL® CYBER

Why Cowbell For Your Cyber Insurance Needs?

As a business, it might seem easier to get cyber coverage as an endorsement to another commercial policy (Business Owner Policy or other). Below is a summary of how standalone cyber from Cowbell provides more robust protection and additional value.

	Packaged Cyber Data Breach Endorsement	Standalone Cyber Cowbell Prime
Data breach coverage	✓	✓
Broad coverage for cyber incidents*		✓
Third party liability coverage		✓
Online, simplified application process		✓
Continuous risk assessment *(Cowbell Factors)*		✓
Industry risk benchmarking		✓
Risk insights and recommendations		✓
Customizable policies		✓
Cybersecurity awareness training *(for employees)*		✓
Pre- and post-breach services		✓
Claims handled by security experts		✓

*Ransomware, cyber crime, fraudulent transfers and more.

Cowbell Supports Closed-loop Risk Management

Cowbell's cyber policies are admitted, written on "A"rated paper, and available nationwide. Our goal is to deliver value to our policyholders on Day One with a closed-loop approach to risk management: Assess, Insure, Improve. Every policy includes continuous risk assessment and benchmarking, recommendations for risk improvement, risk engineering, and cybersecurity awareness training for employees.

Additional Resources:

- Recommendations to prepare a cyber insurance policy
- Cowbell Prime 100 vs BOP data breach endorsement
- Cowbell Factors Overview
- Getting more than a policy with Cowbell
- More industry-specific resources
- Unlock cybersecurity awareness training for your employees