



Cyber-Safe Roads:

Mitigating Cyber Threats in Transportation and Logistics

Michelle Vayle | RENOVO DATA

IN TRANSPORTATION AND logistics, staying connected and accessing real-time data is critical to keeping freight - and business operations - moving. For 3PLs and logistics companies to be competitive, they must invest in their own tools, technologies and services to create a digital advantage. However, this advantage also brings increased cyber threat.

As the industry continues to embrace cloud platforms, automation, and data-driven technologies, it has become an increasingly attractive target for cyber attackers.

Understanding the risks that threaten supply chain systems and logistics providers is the first critical step. From there, building an actionable roadmap to prepare, prevent, and recover from cyber incidents can make a meaningful difference in operational resilience and business continuity.

Cyber Risk in Motion

As the logistics industry has evolved, your operations now depend on technology. At a 3PL, nearly every critical job function depends on having the most accurate and up-to-date data available- and that level of data dependence introduces new vulnerabilities.

Unfortunately, bad actors have recognized the criticality of data to your business. An estimated 94% of companies face attempted ransomware or fraud attacks, and more than half report real breaches. These incidents often involve stolen data or ransom demands, but the consequences extend far beyond the lost information. A cyberattack can disrupt shipments, stall operations, and bring logistics workflows to a standstill.

Know Your Threats

You must know what you're up against. The first step in any solid cybersecurity plan is identifying where your risk vectors lie.

Start with a cyber risk assessment. When evaluating your infrastructure, are there outdated systems exposing you to risk? Are unsecured devices connecting to your network? Are regular Email phishing tests being conducted? Are there other opportunities to train employees?

This assessment gives you the visibility you need to build a smarter more proactive strategy. What vulnerabilities can you identify- and address- before they lead to a data disaster?

Lock Down Access: Strengthen & Secure Your Network

Once you've identified your risks, the next step is to control who gets access to what — and how.

Start with strong user authentication initiatives. Require multi-factor authentication, enforce passwords, and implement role-based access controls so that employees only see what they need to do their jobs.

Network segmentation can add another layer of defense, preventing threats from moving freely across your systems. Ensure that if a hacker gained access to one aspect of your IT environment, they can't automatically move through your entire network.

The basics of IT security are more important ever. Keep your software patched, deploy endpoint detection tools, and consider shifting toward a Zero-Trust model where user and device access is never assumed, but instead it's always verified.



Invest in Disaster Recovery Solutions and Planning

Even the most secure environments can be breached. That's why investment in disaster recovery solutions and planning is not optional – it's essential.

Align your disaster recovery strategy with your business priorities creating synergy in operations and recovery. How long can your business survive without access to your critical applications? What's the cost of a day's IT downtime?

Key tools to consider include:

- **Continuous data protection**, which updates backups in real time
- **Real-time replication** to mirror key systems to alternate environments
- **Immutable backups** that can't be altered — even by ransomware
- **Prebuilt recovery sites** to quickly spin up operations when your primary systems go down

And remember — Disaster Recovery isn't something you do once and forget. Your plan must evolve with your systems, operations, and threats.

Keep Your Plan Sharp

Ask yourself regularly: Is our disaster recovery plan ready for action?

If you're not sure who's involved in the process, when the last test happened, or whether your alternate site still meets your needs, it might be time for a refresh.

Review your recovery time objectives (RTOs) recovery point objectives (RPOs), test your tools, and - maybe most importantly - learn from past incidents. Simulations and real-world events offer valuable insights, but only if you act on them.

An out-of-date DR plan won't help much in a real emergency. Make updates part of your regular business continuity rhythm.

Find Strong Cybersecurity Partners

When a cyber incident hits, you don't want to be figuring things out from scratch.



HOW LONG CAN **YOUR BUSINESS SURVIVE** WITHOUT ACCESS TO YOUR **CRITICAL APPLICATIONS**? WHAT'S THE **COST OF A DAY'S IT DOWNTIME?**

Having the right partner - one who understands the industry and the infrastructure that supports it - can save you time, money, and reputational loss.

Look for partners who offer:

- Secure, scalable cloud environments
- White-glove support
- Ongoing employee training, including phishing simulations
- Pen testing and continuous monitoring for vulnerabilities

Cybersecurity is not something that can be achieved alone. Partner with experts to recover faster, reduce risk, and build a more resilient future.

Keep Freight Moving, Even in a Crisis

Cyber risk is part of doing business in transportation and logistics. With the right strategy in place - one that emphasizes awareness, prevention, and recovery - it's manageable. It's about protecting your people, your operations, and your ability to serve customers. Prepare, Prevent, Recover. That's how you keep your business on cybersafe roads. ➡

RenovoData is a leading cloud backup, Disaster Recovery, Infrastructure as a Service (IaaS), and DR Planning service provider helping companies protect critical data and systems worldwide. For more information and guidance, please call toll-free at 877-834-3684, [email us at info@renovodata.com](mailto:info@renovodata.com), or reference our website at www.renovodata.com