Staying on Track

Overcoming Communication Challenges in Transportation & Logistics

Mattermost

MISSION IN MOTION

Why secure collaboration is mission-critical to transportation and logistics.

Transportation and logistics companies face persistent pressure to keep people, goods, and other cargo moving efficiently while navigating supply chain disruptions, rising costs, and strict compliance demands.

In this critical infrastructure sector, organizations need to move as fast as they can because delays can mean lost revenue, damaged reputations, and unhappy customers.

Transportation and logistics operators need secure, real-time collaboration tools to stay aligned, informed, and ready to rapidly respond to challenges that come their way — even when they're on the move.

Why Critical Infrastructure Organizations Need Security & Resilience

As the transportation and logistics industry continues on its digital transformation journey, operations become more efficient. However, cybersecurity vulnerabilities increase. According to one recent report, the sector experienced a 36% year-over-year increase in cyberattacks in 2023; 83% of these attacks disrupted core business functions, and bad actors made off with confidential data in 38% of them.

With attacks on the rise and the stakes getting higher every day — the average breach costs $4.88 million, according to IBM — organizations must bake as much security and resilience into their operations as they can to keep business humming along while protecting sensitive data, avoiding financial losses, and preserving their reputations.

What You'll Learn

In this guide, we'll explore how secure, real-time collaboration can help transportation and logistics companies increase operational resilience and secure their systems against increasingly sophisticated cyberthreats. We'll also provide best practices your organization can use to establish secure collaboration across your operations, including examples of how real-world companies are using Mattermost to accelerate and protect mission-critical work.

Industry Challenges:

Navigating an Evolving Threat Landscape

Like other critical infrastructure organizations, transportation and logistics companies face mounting cyberthreats, evolving compliance demands, and the challenge of keeping distributed teams securely connected — all while ensuring shipments stay on track. Without reliable coordination and protection, organizations risk delivery delays, financial losses, and data breaches.

Transportation and logistics companies must confront three major challenges head-on. With that in mind, let's take a closer look at the critical risks shaping the future of the industry — and what your organization can do to get ahead.

Challenge #1: Mitigating Cybersecurity Risks

Cyberattacks Are More Frequent — and More Disruptive

Transporation and logistics companies are prime targets for attackers because they operate complex, time-sensitive networks that are essential to global supply chains. Any disruption — whether through ransomware, data breaches, or system outages — can cause widespread delays, financial losses, and reputational damage.

Since many organizations in this sector rely on connected systems, third-party vendors, and legacy infrastructure, transportation and logistics companies have larger attack surfaces, making them vulnerable to increasingly sophisticated threats.

What Happens When Hackers Strike

Cyberattacks are on the rise these days, with 88% of security leaders saying they've experienced moderate-to-severe disruption to operations over the last year due to security breaches. When hackers infiltrate critical systems, operations grind to a halt, data is compromised, and financial and reputational damage can escalate rapidly.

88% **OF SECURITY LEADERS have experienced moderate-to-severe disruption to operations over the last year due to cyberattacks**

(OTORIO, 2024)

In 2017, for example, the Dutch logistics company Maersk was crippled by the NotPetya malware attack, which caused widespread operational disruptions, halted shipping schedules, and forced the company to reinstall over 4,000 servers and 45,000 computers. When the dust settled, Maersk had incurred more than $250 million in financial losses.

The outcomes can be even worse. In 2023, U.K. firm KNP Logistics was the victim of a ransomware attack that ultimately resulted in the company declaring itself insolvent and laying off 730 employees.

To avoid these kinds of devastating consequences, organizations must prioritize secure collaboration platforms, ensure data sovereignty, and adopt tools that enable rapid incident response. Together, these capabilities provide a secure foundation for teams to stay connected — even during critical incidents — and allow for quick action to contain and mitigate potential threats.

Challenge #2: Maintaining Regulatory Compliance

Navigating an Ever-Evolving Regulatory Landscape

Like all critical infrastructure organizations, transportation and logistics operators need to figure out how to navigate an ever-changing landscape of regulations to ensure compliance and avoid penalties like hefty fines, shipment holds, and reputational damage.

€20 MILLION OR 4% OF ANNUAL GLOBAL TURNOVER

Under the GDPR, organizations can be fined as much as €20 million or 4% of annual revenue, whichever is higher. (GDPR.eu, 2025)

Industry Challenges:

Navigating an Evolving Threat Landscape

In the United States, transportation companies need to follow regulations set by agencies like the Department of Transportation (DOT), the Transportation Security Administration (TSA), and the Federal Aviation Administration (FAA). These agencies impose strict guidelines on everything from safety standards and hazardous material handling to the security of freight, passenger transport, and air cargo. For example, the DOT mandates compliance with safety regulations, weight limits, and infrastructure requirements while the TSA oversees security of highways, railways, airports, and pipelines.

The Cost of Noncompliance

Violations of these regulations can lead to significant penalties. In December 2023, the DOT fined Southwest Airlines $140 million for cancelling 16,900 flights and stranding over 2 million passengers during the 2022 holiday season. In January 2025, the DOT hit JetBlue with a $2 million penalty for chronic flight delays. Both cases underscore the importance of strict adherence to regulatory standards.

Of course, such regulations aren't confined to the United States. European standards — like the EU Mobility Package and the General Data Protection Regulation (GDPR) — also impose stringent rules on working hours, cross-border logistics, and data security.

Companies operating in multiple European countries must navigate this regulatory maze, since failure to comply can also result in significant penalties. For example, in 2020, British Airways was fined £20 million under the GDPR after hackers stole the personal and credit card data of more than 400,000 customers.

To avoid costly fines and preserve their reputations, transportation and logistics companies need to prioritize compliance in all that they do. Achieving this requires seamless secure collaboration across teams, departments, and regions to streamline operations. It also requires effective data management; companies need to maintain complete control over their data to comply with standards like the GDPR. On top of this, organizations must be equipped with tools and protocols that enable rapid incident response, allowing them to address any breaches or compliance issues quickly and effectively.

Industry Challenges:

Navigating an Evolving Threat Landscape

Challenge #3: Keeping Distributed Teams Securely Connected

Operations Are More Distributed Than Ever

Transportation and logistics companies operate across extensive geographical regions, including remote locations. As such, real-time secure communication is critical when it comes to preventing costly delays and mitigating security risks.

However, many organizations in this sector still rely on outdated communication tools that slow down response times and expose them to additional cyberthreats. Unfortunately, hackers are increasingly targeting the transportation sector. In 2023, attacks against the industry increased 181% from the previous year — the largest year-over-year increase for any sector (financial services came in second at 177%).

Making matters worse, just 12% of U.S. trucking companies say they're "very prepared" for a cybersecurity incident. Should hackers put one of these organizations in their crosshairs, delayed communication can slow down incident response, extend downtime, and significantly impact essential services that communities rely on.

Bridging the Gap with Secure Collaboration

To overcome these challenges, logistics and transportation companies need a modern, secure collaboration platform that's adaptable to real-world workflows. With the right solution in place, operators can access the people, tools, and data they need when they need it — wherever they are.

Organizations looking to bring increased speed, focus, security, and resiliency to their operations should look for a collaboration solution that offers:

- Instant messaging and secure document sharing to facilitate seamless coordination among team members, reducing delays and enhancing operational efficiency.
- Full control of data with the ability to manage where data is stored, who has access to it, and how it's shared — something that's critical for meeting compliance requirements and protecting sensitive information.

ONLY 12% of U.S. trucking companies say they're very PREPARED FOR A CYBERSECURITY INCIDENT.

(Trimble, 2024)

Industry Challenges:

Navigating an Evolving Threat Landscape

- Role-based access controls (RBAC), which guarantee that only authorized individuals handle sensitive data, enhancing data security and ensuring compliance.

- Integration with operational tools to streamline workflows and improve efficiency by connecting communications with existing operational systems, threat intelligence platforms, and other mission-critical tools.

By implementing a platform with these capabilities, transportation and logistics companies can enhance security while bolstering resilience against cyberthreats, thereby ensuring that operations remain uninterrupted, cargo gets where it should be on time, and customers stay happy.

Best Practices:

How Secure Collaboration Strengthens Transportation & Logistics Resilience

The transportation and logistics industry doesn't just move goods and people. It keeps global supply chains running and economies in motion.

To meet business objectives, operators need fast, reliable, and secure communication across a highly distributed network of stakeholders — from dispatchers to drivers to warehouse teams and regulatory bodies.

While every organization has its unique operational nuances, there are many common threads that hold the industry together. By following these field-tested best practices, transportation and logistics companies can build their secure collaboration strategy on top of a strong foundation — making it that much easier to ensure uptime, maintain compliance, and maximize operational efficiency.

1. Establish a Unified Secure Communication Framework

In the transportation and logistics industry, secure communication isn't just about cybersecurity. It's about protecting the entire supply chain and keeping operations humming along.

With teams spread across vehicles, warehouses, ports, and command centers, fragmented communication tools open the door to delays, data breaches, and compliance violations. A unified secure communication framework helps logistics organizations maintain full control of their data, streamline coordination, and respond rapidly to unexpected events.

To achieve your goals, make sure you adopt communication tools that give you data sovereignty and seamlessly integrate into your broader security posture. Enforce access controls based on roles to ensure only authorized users can access mission-critical data. You'll also want to ensure that messages and documents are encrypted at rest and in transit. Since your team is always on the go, equip them with secure mobile tools that are reliable and easy to use.

Practical execution steps:

1. Audit your current communication infrastructure for security gaps and fragmentation
2. Deploy secure encrypted collaboration tools with features like multi-factor authentication (MFA) and role-based access controls (RBAC)
3. Ensure your organization retains complete control and visibility over all collaboration data

2. Build Resilience and Redundant Communication Systems

For transportation and logistics operators, resilient communication is critical for keeping goods moving and teams aligned — especially when disruptions occur. Whether it's a network outage, cyber incident, or severe weather event, communication systems must be robust enough to maintain continuity and ensure time-sensitive decisions can still be made.

Resilient infrastructure means more than uptime. It focuses on ensuring mission-critical updates, dispatch changes, compliance notices, and incident response activities flow to the right person at the right time — no matter the circumstances.

Practical execution steps:

1. Use self-hosted or private cloud-based communication platforms to maintain control over sensitive operational data
2. Deploy redundant out-of-band communication systems that can be brought online when primary channels go down
3. Implement High Availability deployments to reduce single points of failure in communication systems
4. Design communication protocols that work in degraded or offline environments — something that's critical for field teams and cross-border operations

3. Boost Efficiency with Integrated Collaboration Tools

In the fast-moving world of transportation and logistics, siloed communication slows down operations and introduces costly errors. By implementing an integrated collaboration solution that seamlessly connects with other mission-critical tools, you can unify teams across dispatch, compliance, field operations, security, and customer support — shattering silos and enabling faster, more informed decision-making.

As you begin searching for a secure collaboration solution, look for a platform that can serve as your single source of truth, pulling real-time data from across supply chain systems, telematics, fleet management tools, and compliance trackers. That way, your teams will have a complete picture of operations at all times. Open source collaboration platforms are especially valuable here, offering full customizability to fit your workflows, compliance requirements, integration needs, and infrastructure preferences.

Practical execution steps:

1. Implement adaptable, extensible collaboration tooling that fits into your existing tech stack
2. Document and share mission-critical workflows for consistency and rapid response
3. Integrate automation for intelligent routing of updates and alerts

4. Train Teams Continuously on Secure Communication Practices

From phishing schemes targeting dispatch centers to malware attacks targeting essential software systems, cybersecurity in transportation and logistics often boils down to human behavior. In fact, one report found that 88% of data breaches stem from human error.

Drivers, field teams, and operations personnel are on the front lines of digital communication. Hackers understand this perfectly and are always trying to dupe unsuspecting workers to gain access to critical systems.

By training teams continuously on secure communication practices, you can build a culture where security is second nature — not an afterthought.

Practical execution steps:

1. Develop role-specific secure communication training modules for dispatchers, drivers, warehouse staff, and admin teams
2. Require quarterly sessions to keep teams up to date with evolving threats and tools
3. Foster a peer-to-peer learning culture through internal forums, ride-alongs, or scenario-based workshops
4. Recognize and reward security-conscious behaviors to reinforce good habits across the organization

5. Implement Proactive Threat Detection and Incident Response Protocols

In transportation and logistics, communication systems are integral to tracking shipments, coordinating fleets, and keeping supply chains moving. That also makes them prime targets for cyberthreats.

By implementing proactive threat detection capabilities, your team can identify vulnerabilities before attackers do — and respond instantly when something goes wrong. From GPS spoofing to data breaches in fleet management systems, rapid, intelligent response is critical to minimizing downtime and damage while protecting sensitive information.

Best Practices:

How Secure Collaboration Strengthens Transportation & Logistics Resilience

Practical execution steps:

1. Build multi-layered incident response protocols tailored to various threat scenarios (e.g., fleet disruption, data loss, and ransomware)
2. Automate containment workflows to limit the spread of communication breaches
3. Maintain a continuous feedback loop to review incidents, adapt protocols, and close security gaps
4. Leverage AI-powered tools to detect anomalies and accelerate threat identification and response

Mattermost:

The Secure Collaboration Platform Purpose-Built for Transportation & Logistics

How Mattermost Helps Transportation & Logistics Firms Increase Resilience

As transportation and logistics firms face growing cybersecurity risks, stricter compliance standards, and increased demands of real-time coordination, secure collaboration is no longer a nice-to-have, it's mission-critical.

Whether managing cross-border shipments, coordinating a fleet, or optimizing warehouse logistics, teams need a platform that keeps them connected, compliant, and in control.

As a secure collaboration purpose-built for critical infrastructure organizations, Mattermost delivers a self-hosted platform designed for companies that operate in high-security, high-performance environments. By enabling secure real-time collaboration with Mattermost, organizations can:

- Speed up incident response times to minimize disruptions and delays
- Stay compliant with industry and regulatory requirements
- Replace outdated systems with a centralized, modern collaboration hub that integrates with other critical tools

What does this look like in the real world?

- In 2023, the U.S. Air Force's Air Mobility Command conducted a readiness exercise called Mobility Guardian 2023 (MG23) that brought together more than 15,000 U.S. and allied forces in the Indo-Pacific region. The exercises are largely unscripted to train troops on how to adapt when operations don't go as planned. During MG23, participants used Mattermost's ChatOps capabilities to stay connected in operationally limited environments. Read the full case study.
- As a wholesaler of cart parts and accessories for German and French automobiles, Schäferbarthold GmbH requires tight-knit coordination to manage inventory and ensure that products get to customers as efficiently as possible. To speed up communication and locate car parts faster, the company's logistics team uses Mattermost to stay connected. Read the full case study.

Mattermost:

The Secure Collaboration Platform Purpose-Built for Transportation & Logistics

The Mattermost Advantage

Mattermost is the ideal collaboration solution for transportation and logistics companies because it offers:

- Self-hosted and private cloud deployments that enable you to maintain complete control over your data while meeting industry-specific compliance requirements
- Secure communication across your operations, from driver check-ins to dispatch coordination to supply chain management, with encryption in transit and at rest, multi-factor authentication, and more
- Role-based access controls that enable you to ensure only authorized users can access critical logistics information
- Custom integrations that enable firms to connect all mission-critical tools together, including legacy systems, to centralize notifications, location data, and system alerts in one place while creating a single source of truth
- Out-of-band communication support that enables teams to stay connected during outages, low-signal zones, and infrastructure failures.

Ready to Build a More Resilient Operation?

For transportation and logistics companies, secure collaboration is a force multiplier. To learn more about the easiest way to ensure your teams can respond rapidly, comply with ever-evolving regulations, and work together efficiently in any circumstances, schedule a demo of Mattermost today.

Schedule a Demo of Mattermost **Schedule a Demo**

Mattermost
MISSION IN MOTION