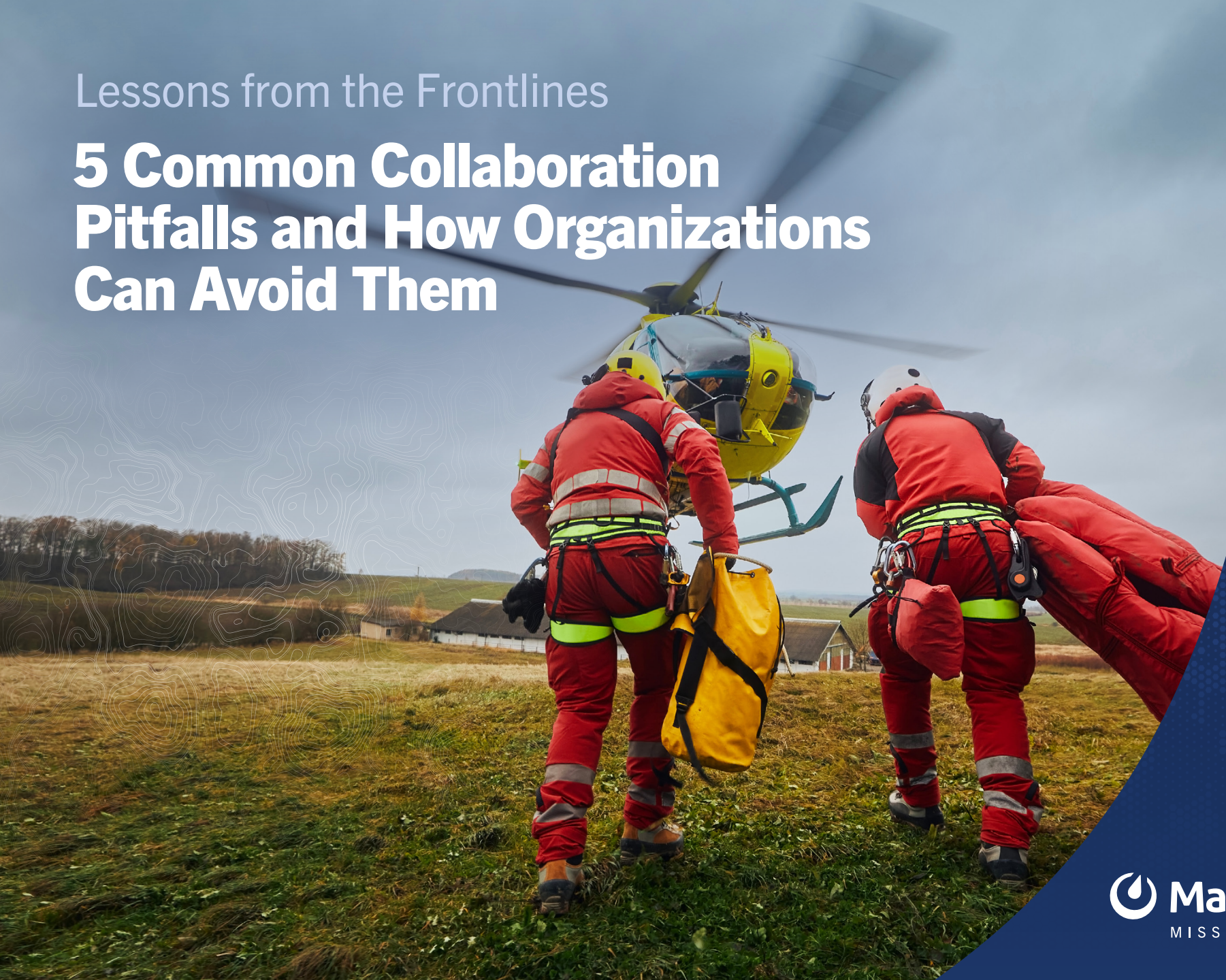
Lessons from the Frontlines

5 Common Collaboration Pitfalls and How Organizations Can Avoid Them



Mattermost

MISSION IN MOTION

In critical infrastructure sectors, secure and reliable communication is essential.

But critical infrastructure organizations face increasing challenges and complexity when it comes to security and operational efficacy. Increasingly sophisticated cyber attacks put essential operations at risk, whether by compromised supply chains, direct attack, or exploitation of vulnerabilities in aging systems. At the same time, the expansion of connected devices and reliance on digital transformation introduce new attack vectors, making it increasingly difficult to secure critical systems while ensuring uninterrupted operations.

Communication and collaboration failures can lead to real-world consequences—from security breaches, operational breakdowns, regulatory fines, and financial losses, all of which can have downstream impacts on the safety, security and well-being of the people served by critical infrastructure organizations.

This guide highlights five of the most common collaboration pitfalls and their impact, featuring real-world case studies of collaboration challenges in the wild:

1. Lack of visibility across organization
2. Disconnected tools slow down response times
3. Compliance risks for unsecured information
4. Cross-sector dependencies and coordination
5. Software supply chain security and reliability

Each section provides actionable strategies to help organizations improve efficiency, strengthen security, and ensure compliance.

Pitfall #1
Lack of Visibility Across Teams

The Colonial Pipeline Wakeup Call — A Communication Breakdown That Shook the U.S. Energy Sector

In May 2021, the Colonial Pipeline ransomware attack disrupted fuel distribution across the East Coast for six days, causing widespread shortages and economic strain. But beyond the attack itself, post-incident reports revealed a critical issue: teams lacked real-time visibility into system status, threat intelligence, and response actions.

Security teams couldn't immediately assess the breach's scope. Operational teams struggled to coordinate containment. Leadership had no centralized view of response efforts, leading to misaligned decision-making. This fragmentation delayed recovery, forcing Colonial to pay a $4.4 million ransom to regain control (U.S. DOJ, 2023).

The Impact of Disconnected Teams

- Security Gaps
  Without a single source of truth, teams operate in silos, increasing the risk of missed threats and duplicated efforts. Nearly 60% of cybersecurity teams report that miscommunication between IT and security leads to unresolved security gaps (Ponemon Institute, 2023).
- Operational Disruptions
  Teams without shared real-time data struggle to coordinate, leading to longer outages, unplanned downtime, and regulatory penalties. Unplanned power outages cost U.S. businesses between $28 billion and $169 billion annually, with cybersecurity incidents a leading cause (U.S. DOE, 2023).
- Delayed Decision-Making
  Leadership needs full visibility into incident status, remediation efforts, and operational impact—without it, response plans falter. 42% of IT and security leaders say they lack real-time visibility into security incidents, slowing their ability to make decisions (IBM X-Force, 2023).

The Fix: Strengthening Real-Time Coordination

- Real-Time Collaboration Across Teams
  Mattermost ensures secure communication between ground stations, operators, and command centers. By centralizing mission-critical conversations and data sharing, the platform supports dynamic coordination during high-stakes operations.
- Unified Data Integration
  Mattermost integrates seamlessly with existing systems, consolidating inputs from satellites, ground stations, and sensors into a single platform. This reduces data silos, enabling faster threat assessments and operational decisions.
- Secure and Scalable Communication
  With end-to-end encryption, role-based access controls, and deployment flexibility, Mattermost protects mission-critical communications from cyber threats, even in contested environments.

Industry Insight:
The Cost of Fragmented Visibility

Power outages cost the U.S. economy between $28 billion and $169 billion annually, with cyber incidents being a leading cause (U.S. DOE, 2024).

40% of energy companies fail security audits due to collaboration gaps (SANS, 2023).

Organizations with centralized visibility and automated response coordination reduce downtime by 40% and cut cyber incident resolution time in half (IBM X-Force, 2023).

Pitfall #2
Slow Response Times Due to Disconnected Tools

The Rogers Communications Nationwide Outage — A Case Study in Telecom Failure

In July 2022, Rogers Communications, one of Canada's largest telecom providers, suffered a catastrophic nationwide outage that disrupted internet, mobile, and banking services for nearly 12 million customers. The outage lasted over 19 hours, crippling 911 emergency services, financial transactions, and critical government communications.

While a network update triggered the failure, the real issue was Rogers' inability to coordinate a rapid response across its internal teams and with external agencies. Without a centralized real-time collaboration platform, technicians were forced to rely on phone calls, emails, and siloed communication tools to diagnose and resolve the problem.

Customers, emergency responders, and businesses were left in the dark, as Rogers lacked an efficient way to communicate status updates. The absence of an integrated escalation process prolonged the disruption, leading to public backlash, regulatory scrutiny, and an estimated $150 million in economic losses (CRTC, 2024).

The Impact of Disconnected Tools

- Critical Infrastructure Impact
  The outage affected 911 services, hospitals, and financial institutions, demonstrating the danger of relying on outdated, fragmented communication tools (Reuters, 2022).
- Operational Disruptions
  Without a centralized, secure collaboration hub, engineers and response teams were delayed in diagnosing and mitigating the issue (Reuters, 2022).
- Delayed Decision-Making
  The failure led to new government mandates requiring telecom companies to improve emergency response coordination and cross-carrier resilience plans (Reuters, 2022).

The Fix: Strengthening Real-Time Coordination

- Centralize Incident Management & Coordination
  A unified collaboration hub ensures that network teams, emergency responders, and business partners stay connected and receive real-time updates. By consolidating all communication into a single secure environment, teams can rapidly assess, prioritize, and respond to outages.
- Automate Incident Escalation & Notification Workflows
  Manually managing incident escalation leads to confusion and delays. Automating escalation workflows ensures the right teams are notified instantly when critical issues arise. Structured playbooks enable seamless handoffs between teams, reducing downtime and increasing response efficiency.
- Enhance Network Resilience with Secure Offline Communication
  During infrastructure failures, teams often lose access to standard communication tools. Implementing offline-capable collaboration solutions ensures that response teams can coordinate and troubleshoot issues—even when traditional networks are down.

Industry Insight:
The Cost of Fragmented Tools

Effective communication is crucial during incidents, as studies show that 87% of business stakeholders desire updates, and 56% are more frustrated by a lack of communication than by the incident itself. (Atlassian)

Pitfall #3
Compliance Risks from Unsecured Communication

The SEC Crackdown on WhatsApp — A Case Study in Financial Compliance Failures

In 2022, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) issued record-breaking fines exceeding $2 billion to major financial institutions for violating record-keeping and compliance laws. The violations stemmed from employees using unauthorized messaging apps like WhatsApp, iMessage, and Signal to conduct business conversations that bypassed official record-keeping systems.

Leading banks, including JPMorgan Chase, Goldman Sachs, and Morgan Stanley, were caught failing to capture and archive business-related communications, a direct violation of SEC Rule 17a-4, which mandates that broker-dealers retain and monitor all electronic communications. Regulators emphasized that unmonitored messaging channels create compliance blind spots, opening the door to misconduct, insider trading risks, and audit failures.

The crackdown sent a clear message: financial institutions must enforce strict communication policies, implement secure collaboration tools, and maintain audit-ready records to avoid multi-million-dollar penalties and reputational damage (SEC, 2024).

The Impact of Unsecured Communication

- Regulatory Penalties
  Financial firms faced over $2 billion in fines for failing to properly retain business-related communications, setting a precedent for stricter oversight (Bloomberg, 2022).
- Increased Risk of Fraud & Insider Trading
  Unmonitored communication channels bypass compliance checks, increasing the risk of regulatory breaches and financial misconduct (Bloomberg, 2022).
- Operational Disruptions
  Banks were forced to fire employees, overhaul policies, and spend millions on new compliance tools to regain regulatory approval (Bloomberg, 2023).

The Fix

- Implement Secure, Enterprise-Grade Collaboration Tools
  Regulated organizations like banks must adopt self-hosted, compliant communication platforms with built-in audit trails and encryption. These tools ensure secure, monitored, and legally compliant business communication.
- Automate Message Retention & Compliance Audits
  Deploy automated retention policies that capture, store, and index all business-related communications, ensuring compliance with SEC and CFTC regulations.
- Train Employees & Enforce Communication Policies
  Strict enforcement of approved communication channels and regular compliance training are critical to preventing violations. Organizations must actively monitor and audit employee messaging practices to maintain compliance.

Pitfall #4
Inefficient Cross-sector Coordination

The Hurricane Katrina Emergency Response Delays — A Case Study in Crisis Coordination Failures

In August 2005, Hurricane Katrina devastated the Gulf Coast, causing catastrophic flooding and displacing over a million residents. While the storm itself was inevitable, the delayed and disjointed response from federal, state, and local agencies exacerbated the crisis, turning a natural disaster into one of the deadliest and costliest humanitarian failures in U.S. history.

Key reports found that lack of centralized communication, delayed escalations, and fragmented coordination across emergency response teams led to preventable loss of life and prolonged suffering. The Federal Emergency Management Agency (FEMA), the National Guard, and local emergency responders operated in silos, unable to efficiently share real-time updates on rescue operations, supply distribution, and evacuation plans.

The inability to coordinate effectively left thousands of people stranded in the Superdome without adequate food, water, or medical aid. Communications breakdowns between agencies meant that critical resources were delayed or misallocated, further compounding the disaster's impact.

The Impact of Poor Incident Coordination

- Delayed Emergency Response
  Lack of centralized coordination resulted in emergency responders struggling to allocate resources effectively, leading to a 48-hour delay in critical aid deployment (FEMA, 2005).
- Breakdowns in Communication
  First responders and federal agencies relied on disjointed communication systems, preventing real-time updates on rapidly changing conditions (FEMA, 2005).
- Public Distrust and Systemic Failures
  The response failures led to a nationwide reckoning on disaster preparedness, pushing agencies to adopt new emergency response protocols (FEMA, 2005).

The Fix

- Establish a Unified Crisis Collaboration Hub
  Disjointed communication during crises delays response efforts. A centralized, secure collaboration platform enables federal, state, and local agencies to share real-time updates on rescue efforts, supply chains, and emergency response plans without reliance on fragile infrastructure.
- Automate Emergency Alerting & Escalation Protocols
  Manual coordination leads to delays in deploying resources where they're needed most. Implementing automated escalation workflows and real-time alerts ensures that decision-makers receive critical information immediately, reducing response time and improving outcomes.
- Ensure Resilient, Offline-Capable Communication
  Disasters often wipe out traditional telecom infrastructure, cutting off emergency responders from critical updates. Secure, offline-capable collaboration tools ensure that emergency personnel can continue coordinating efforts even when networks fail.

Pitfall #5
Software Supply Chain Security and Reliability

SolarWinds Orion Attack — A Case Study in Supply Chain Vulnerabilities

In December 2020, cybersecurity firm FireEye discovered what would become one of the most sophisticated and far-reaching supply chain attacks in history. Hackers had compromised SolarWinds' software development environment and inserted malicious code into updates of their Orion network monitoring platform—software used by over 33,000 organizations worldwide, including government agencies and Fortune 500 companies.

The compromised updates, digitally signed and appearing legitimate, were downloaded by approximately 18,000 SolarWinds customers between March and June 2020. This gave attackers backdoor access to these organizations' networks, where they could move laterally, exfiltrate data, and remain undetected for months. High-profile victims included multiple U.S. government departments (Treasury, Justice, Energy), Microsoft, and dozens of other organizations critical to national security.

What made this attack particularly devastating was not just its technical sophistication, but the breakdown in secure collaboration and oversight within the development pipeline. Post-incident investigations revealed that SolarWinds lacked proper access controls, code review processes, and secure communication channels between development, security, and operations teams—creating blind spots that allowed the compromise to remain undetected.

Industry Insight:
The Cost of Supply Chain Attacks

Software supply chain attacks increased by 742% in 2023 alone (Sonatype, 2023).

The average cost of a software supply chain breach exceeds $9.4 million, with remediation efforts often continuing for 12+ months (IBM, 2024).

The Impact of Insecure Software Supply Chains

- Extended Attack Surface
  Organizations unwittingly introduced malware through trusted software updates, bypassing traditional security controls and enabling attackers to access sensitive systems (CISA, 2022).
- Prolonged Detection Time
  The average dwell time for attackers in affected networks exceeded 250 days, allowing extensive data exfiltration and reconnaissance while avoiding detection (Mandiant, 2021).
- Cascading Trust Failures
  The incident triggered a chain reaction of security reassessments across thousands of organizations, requiring extensive forensic analysis and remediation efforts costing billions (IBM, 2024).

The Fix

- Implement End-to-End Supply Chain Verification
  Organizations must verify the integrity of software throughout the development lifecycle. This requires implementing a secure software bill of materials (SBOM), code signing procedures, and automated security scans in a collaborative environment where development and security teams share responsibility and communicate effectively.
- Establish Cross-Functional Security Collaboration
  Siloed teams increase risk of compromise. Creating dedicated secure channels for developers, security analysts, and operations personnel ensures that potential vulnerabilities are identified, documented, and remediated quickly, minimizing exposure windows and preventing issues from slipping through cracks in communication.
- Deploy Real-Time Threat Intelligence Sharing
  Effective defense requires timely information. Implementing automated feeds of software vulnerability alerts and establishing protocols for sharing threat intelligence across teams helps organizations rapidly respond to emerging supply chain threats before they can be exploited.

Future-Proof Your Mission-Critical Collaboration with Mattermost

The case studies in this guide illustrate a harsh reality: when communication fails, the consequences can be severe. Whether it's a cyberattack crippling an energy pipeline, a nationwide telecom outage, or a compliance breach resulting in billions in fines, one thing is clear—fragmented collaboration puts organizations at risk.

To prevent these failures, organizations need a secure, real-time collaboration platform built for mission-critical operations. Mattermost provides:

- **Centralized, Secure Communication** – Keep all teams aligned with real-time messaging, file sharing, and automated workflows.
- **Automated Incident Response & Escalation** – Ensure immediate alerts and seamless coordination during crises.
- **Compliance-Ready & Self-Hosted Options** – Maintain full control over sensitive communications and meet regulatory requirements.
- **Offline-Capable & Resilient Infrastructure** – Keep operations running even when networks fail.

Don't wait for the next crisis to expose gaps in your collaboration. Schedule a demo today to see how Mattermost can help you improve security, streamline workflows, and ensure compliance in your mission-critical environment.

Learn more at Mattermost.com »