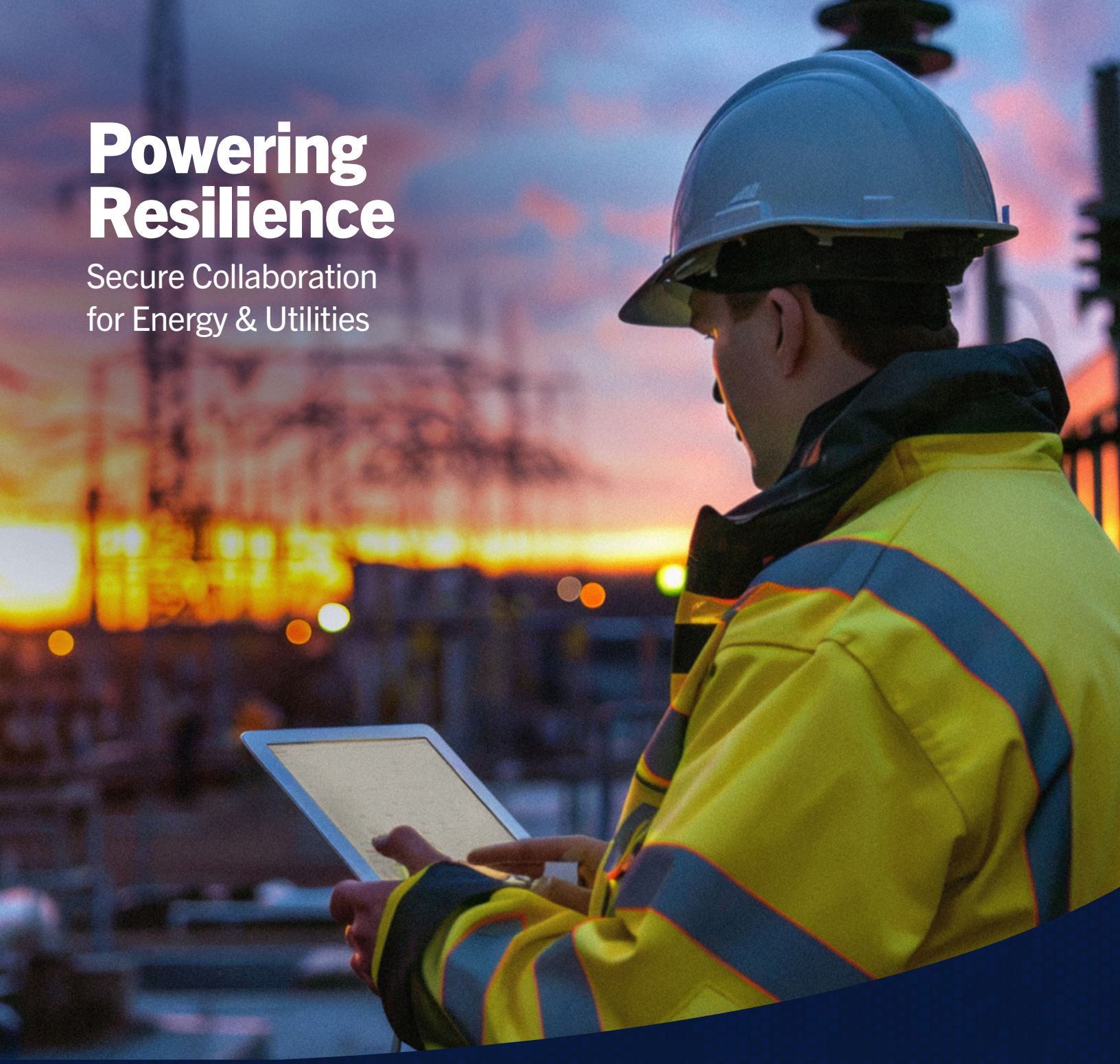


Powering Resilience

Secure Collaboration for Energy & Utilities

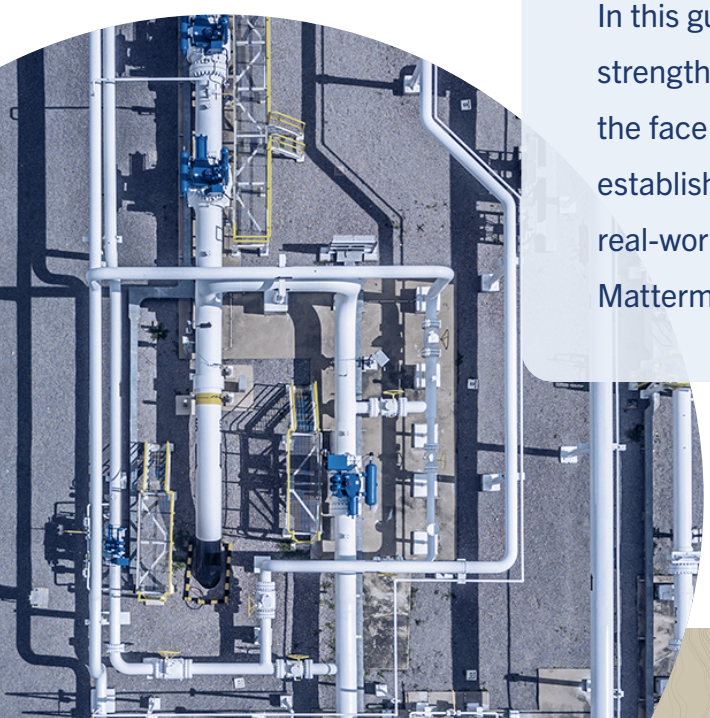
Mattermost

How Modern Communication Solutions Strengthen Compliance, Cyber Resilience, and Operational Efficiency

Energy and utilities providers are under constant pressure to keep operations running smoothly while defending against cyber threats and meeting complex regulatory requirements. The stakes are high — disruptions can lead to costly downtime, regulatory penalties, and even national security risks. To stay ahead, organizations need **seamless, secure collaboration** that keeps teams connected, informed, and in control.

Operational Efficiency Keeps Critical Infrastructure Secure

As energy systems become more digitized, vulnerabilities increase. The World Economic Forum's Global Cybersecurity Outlook 2025 reports that nearly 60% of organizations say geopolitical tensions have influenced their cybersecurity strategy. Additionally, 45% of cyber leaders are concerned about operational disruptions, and 72% report rising cyber risks, with ransomware remaining a top concern. These numbers make one thing clear: security and resilience must be built into every aspect of operations.



What You'll Learn

In this guide, we'll examine how secure, real-time collaboration strengthens the resilience of critical infrastructure organizations in the face of mounting challenges. We'll also share best practices for establishing secure collaboration for your organization, including a real-world example of how one energy & utilities provider is using Mattermost to secure and accelerate operations today.

Industry Challenges:
Navigating an Evolving Threat Landscape

Energy providers face mounting cyber threats, stricter compliance requirements, and the challenge of keeping remote teams securely connected—all while maintaining uninterrupted service. Without reliable coordination, organizations risk operational disruptions, financial penalties, and security breaches. Let's explore three critical industry challenges faced by energy providers.

1. Cyber & Operational Resilience Risks

Cyberattacks Are More Frequent—and More Disruptive

Critical infrastructure is a prime target for attackers, with ransomware, phishing, and credential theft causing significant business disruptions.

According to the IBM Security X-Force Threat Intelligence Index 2024, cyberattacks exploiting stolen credentials have surged 71% year over year. These breaches don't just compromise data—they disrupt operations, delay recovery efforts, and expose vulnerabilities that lead to increased regulatory scrutiny.

The Colonial Pipeline Attack: A Cautionary Tale

The Colonial Pipeline ransomware attack in 2021 revealed how a single compromised password can create widespread disruptions. The response was delayed and inefficient, showing the risks of poor real-time collaboration. Faster coordination between response teams, operators, and government agencies could have minimized the impact.

To address this, the Cybersecurity and Infrastructure Security Agency (CISA) launched the Joint Cyber Defense Collaborative (JCDC) to strengthen cross-sector coordination and improve cyber resilience. However, energy providers still need internal, secure collaboration platforms that ensure rapid response when the stakes are high.

71% INCREASE
in cyberattacks exploiting stolen credentials.
(IBM X-Force, 2024)

Industry Challenges:
Navigating an Evolving Threat Landscape

2. Compliance-Driven Security & Access Control

Stricter Regulations Demand Proactive Security

Regulatory frameworks such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), U.S. Department of Energy (DOE) Cybersecurity Directives, and Environmental Protection Agency (EPA) guidelines are designed to safeguard operations—but they also introduce complex compliance challenges.

The Federal Energy Regulatory Commission (FERC) imposes fines of up to $1 million per day per violation, making compliance critical. In one case, Powhatan Energy Fund faced $16.8 million in penalties for violations, illustrating the real consequences of regulatory missteps.

Why Compliance Can't Be an Afterthought

A fragmented security strategy makes compliance harder. Without centralized access controls, organizations struggle to enforce security policies consistently.

Secure collaboration platforms help organizations stay audit-ready by offering real-time access control, encrypted communication, and compliance tracking. By integrating compliance enforcement into workflows, companies reduce risk while maintaining operational efficiency.

$1 MILLION – PER DAY

"FERC fines can reach $1 million per day for non-compliance." (FERC, 2023)

Industry Challenges:
Navigating an Evolving Threat Landscape

3. Coordinating Remote & Field Teams Securely

Energy Operations Are More Distributed Than Ever

Energy teams operate across vast and often remote locations, where maintaining real-time, secure communication is essential to avoiding costly delays and security risks. Yet many still rely on outdated, unsecured communication tools, increasing security risks and delaying response times.

According to the Uptime Institute's Annual Outage Analysis 2023, two-thirds of power outages cost over $100,000. These disruptions can slow emergency response, prolong downtime, and impact essential services that communities depend on.

Bridging the Communication Gap with Secure Collaboration

A modern, secure collaboration platform must be flexible enough to fit the needs of real-world workflows, to ensure that the team using it has access to information they need when and where they need it. This includes:

- Instant messaging & secure document sharing for seamless coordination.
- Offline-capable communication for remote and disaster recovery scenarios.
- Role-based access controls (RBAC) to ensure only authorized personnel handle sensitive data.
- Integration with operational tools to streamline workflows and improve efficiency.

$100,000

"Two-thirds of outages cost over $100,000." (Uptime Institute, 2023)

Best Practices:
How Secure Collaboration Improves Energy Resilience

Secure collaboration is a complex, multifaceted challenge. Success requires a synchronized approach that balances technological innovation, human capability, and strategic foresight.

The energy and utilities sector doesn't just communicate—it orchestrates critical infrastructure's lifeline through intelligent, secure, and resilient communication strategies.

Each organization is unique, but these best practices can provide a framework for developing a secure collaboration strategy that aligns with your specific needs.

1. Adopt a Comprehensive Communication Security Framework

In the energy and utilities sector, a comprehensive communication security framework is the foundational shield against increasingly sophisticated cyber threats. In most cases, communication security is an extension of a broader security framework. This will include adopting collaboration tooling that keeps data controlled and secure, implementing access control policies for communication systems, and offering training programs to ensure team members use communication tools appropriately.

Practical Execution Steps

1. Conduct comprehensive communication infrastructure audits
1. Implement security measures including advanced encryption and multi-factor authentication across all communication channels
1. Train the team on appropriate use of secure communication channels

2. Implement Resilient Communication Infrastructure

Resilient communication infrastructure represents the nervous system of modern energy operations. It's not merely about maintaining connectivity, but ensuring mission-critical information flows seamlessly during both routine operations and extraordinary circumstances.

When developing your communication infrastructure, consider redundancy as a core architectural requirement. Ensuring that backup communication channels are in place is a critical step in ensuring that everything from system outages to cybersecurity breaches can be resolved quickly, with minimal disruption to consumers.

Technical Implementation Strategies

- Use self-hosted or private cloud-based communication software to increase control over your organization data
- Implement backup "out-of-band" communication systems to be used when primary channels are compromised
- Leverage High Availability (HA) deployment for communication systems
- Design communication protocols that can operate in degraded environments

3. Operational Efficiency Through Integrated Collaboration

Modern energy operations require a seamless, intuitive collaboration environment that breaks down traditional organizational silos. The goal is to create a unified communication platform that enhances decision-making speed and accuracy.

Look for solutions that can serve as a collaboration hub that pulls together data from across multiple sources, giving your organization a full picture of the situation when and where they need it most.

Technological Enablement

1. Implement adaptable, extensible collaboration tooling that fits into your existing toolset
2. Document and share critical workflows to ensure fast access and consistent execution
3. Integrate machine learning for intelligent routing of information

4. Conduct Continuous Training and Awareness

From phishing to MITM attacks, cybersecurity in communication is fundamentally a human challenge. Continuous training transforms security from a technical constraint to an organizational cultural norm.

Implementation Tactics

1. Develop role-specific cybersecurity communication training modules
2. Create mandatory quarterly training refreshes
3. Implement peer-to-peer knowledge sharing mechanisms
4. Establish recognition programs for security-conscious behaviors

5. Adopt Advanced Threat Detection and Response Techniques

Security teams must anticipate potential communication-based vulnerabilities before they can be exploited. From automating response mechanisms to kick off incident response protocols the moment they're detected to using AI to identify anomalies, the best-prepared organizations have evolved their threat detection strategies from evolves from reactive monitoring to predictive intelligence.

Upleveling Threat Response:

1. Develop multi-tier incident response protocols
2. Create automated threat containment processes
3. Establish consistent feedback loop to evaluate and iterate incident response protocols
4. Adopt AI-enhanced threat response tooling to accelerate response

Mattermost:
The Secure Collaboration Solution for Energy Resilience

As energy providers navigate increasing cyber threats, regulatory demands, and operational challenges, secure collaboration has become an essential part of their operational infrastructure. The ability to communicate in real time, maintain compliance, and integrate seamlessly with existing infrastructure ensures that teams can respond effectively when the stakes are high.

Mattermost provides a self-hosted, secure collaboration platform purpose-built for high-security environments like energy, utilities, and critical infrastructure. By adopting a secure, real-time communication solution, organizations can:

- Improve cybersecurity incident response and minimize downtime
- Ensure regulatory compliance without slowing operations
- Modernize outdated communication infrastructure for better situational awareness

How Mattermost Supports Energy Resilience

- Self-Hosted & Air-Gapped Deployments – Full control over data and security with on-premises or private cloud hosting.
- Data Encryption – Protect sensitive operational discussions with encryption-in-transit and encryption-at-rest capabilities.
- Granular Access Controls – Ensure only authorized personnel access critical communications.
- Customizable integration with SCADA, EMS, and GIS – Streamline real-time alerts and notifications.
- Offline & Out-of-Band Communication – Maintain connectivity during network failures.

Mattermost:
The Secure Collaboration Solution for Energy Resilience

Mattermost in the Field:
Improving Operational Efficiency and Securing National Energy Infrastructure with RTE

As a crucial part of France's energy infrastructure, Réseau de Transport Électrique (RTE) plays a key role in balancing electricity supply and demand in real-time while maintaining the stability and security of the grid. RTE uses Mattermost to collaborate in real time during electrical outages and other incidents.

Mattermost lets operational teams in the field send and receive notifications directly on their phones, streamlining communication and keeping incident information centralized. By using Mattermost, RTE has reduced its time to manage incidents and improve responsiveness during outages.

> "Feedback showed that we needed to strengthen our reporting procedures with tools dedicated to the crisis."
>
> —**Rémi Bayle,**
> Operations Manager, RTE

Take the Next Step Toward Energy Resilience

Secure collaboration is a force multiplier for energy and utility providers. Ensure your teams can respond, comply, and operate efficiently—no matter what challenges arise.

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

Mattermost