

Balancing the Books

How Financial Services Can Close Gaps
in Communication & Compliance



How Modern Communication Solutions Strengthen Data Privacy, Incident Response & Compliance Readiness

Financial services organizations face mounting pressure to ensure data privacy, mitigate cybersecurity threats, and navigate complex regulatory landscapes. With sensitive financial data at stake, the costs of breaches, compliance failures, and operational disruptions can be catastrophic.

To achieve resilience and protect against these risks, financial services firms need seamless, secure collaboration that keeps teams aligned, informed, and ready to respond.

Operational Efficiency Keeps Critical Infrastructure Secure

Financial services organizations are high-value targets for hackers due to the sensitive nature of the data they manage, including personal information, account credentials, and transaction histories. This data is highly attractive to cybercriminals for the purposes of fraud, identity theft, and financial gain in particular, which is the main driver of 95% of all data breaches, per [Verizon's 2023 Data Breach Investigations Report](#).

In addition to being a top target, the financial services industry ranks among the most expensive sectors for breach recovery. According to [IBM's 2024 Cost of a Data Breach Report](#), the average breach costs \$4.88 million to resolve. For financial services, that number shoots up to \$6.08 million — 22% higher.

While protecting against cyberthreats, financial services firms must also comply with evolving regulatory standards — like GDPR, PCI DSS, and SOX — which requires more than box-checking. Maintaining compliance demands real-time visibility, auditability, and control.

To stay secure and keep pace with regulations, financial services organizations need integrated platforms that support AI-powered threat detection, embedded compliance, and secure, cross-functional communication.



What You'll Learn

In this guide, we'll examine how secure, real-time collaboration enhances resilience within financial organizations, helping firms overcome the major challenges they face. We'll also share best practices for ensuring compliance and security, along with a real-world example of how a leading financial institution leverages Mattermost to secure and streamline operations.



Industry Challenges:

Inside the High-Stakes Realities of Data Privacy, Incident Response, and Compliance



Whether it's safeguarding millions of client records, coordinating responses to high-stakes cyber incidents, or navigating a maze of global compliance mandates, large financial institutions face immense operational and regulatory pressure. These pressures are amplified by three persistent challenges: maintaining data privacy and client trust, orchestrating swift and effective incident response across teams, and continuously monitoring and reporting on compliance in a rapidly evolving regulatory landscape.

Challenge #1: Data Privacy and Client Trust

Financial institutions deal with highly sensitive client data every day. Breaches or mishandling of this information can result in severe reputational damage, financial penalties, and the loss of client trust.

As IBM's 2024 Cost of a Data Breach Report revealed, the average cost of a data breach in the financial sector is among the highest of all industries. Beyond financial penalties, data breaches can significantly damage client trust and confidence, often resulting in loss of business and brand reputation.

To protect against these risks, financial services firms must adopt a proactive approach to data protection, ensuring that sensitive information is encrypted, accessible only to authorized personnel, and rigorously monitored.

In late 2023, Fidelity Investments Life Insurance Co. [disclosed a data breach](#) involving its third-party vendor Infosys McCamish Systems, which exposed the personal information of over 28,000 customers. The breach raised serious concerns about the security of client data managed by financial institutions and their vendors.

For clients, such incidents can severely erode confidence in a bank's ability to protect their most sensitive information. Even if the breach is the fault of a third-party vendor, customers often hold the institution accountable. Unfortunately, the loss of trust can lead to long-term reputational damage, customer attrition, and increased regulatory scrutiny.



The financial sector's breach recovery costs are
22% HIGHER than the average organization.
(IBM, 2024)

Industry Challenges:

Inside the High-Stakes Realities of Data Privacy, Incident Response, and Compliance

Challenge #2: Incident Response Coordination

In the event of a security breach or cyberattack, rapid and coordinated response is critical for protecting data and assets, keeping systems operational, and preserving the bottom line. According to a report from [Pingdom](#), brokerage services incur some of the highest downtime costs in the world at \$6.48 million per hour. When financial services firms rely on fragmented communication systems, incident response efforts are delayed, which magnifies the impact of attacks.

In 2016, a group of hackers launched a [successful cyberattack](#) on the SWIFT banking network, exploiting weaknesses in internal communication and authentication processes to steal \$81 million from Bangladesh Bank's account at the Federal Reserve Bank of New York — a powerful reminder of the cost of poor coordination. Although most of the transactions were blocked — the cybercriminals tried to pilfer a total of \$951 million — miscommunication between teams and delayed internal alerts allowed much of the fraudulent activity to go undetected until it was too late.

This incident underscores how even well-defended institutions are vulnerable when collaboration breaks down. For financial services organizations — especially those operating across borders and time zones — having a secure, centralized communication platform is not optional. It's foundational to ensuring teams can detect threats, coordinate in real time, and contain incidents before they escalate.



NEARLY 80% OF FINANCIAL SERVICES FIRMS
are concerned about their ability to protect
against cyberattacks. ([Mayer Brown](#), 2024)

65% OF FINANCIAL SERVICES ORGANIZATIONS
were victims of ransomware attacks in 2024.

([Sophos](#), 2024)



Industry Challenges:

Inside the High-Stakes Realities of Data Privacy, Incident Response, and Compliance

Challenge #3: Integrating Compliance Monitoring and Reporting

Financial services organizations are under constant pressure to meet rigorous compliance mandates — across jurisdictions, systems, and communication channels. From GDPR and SOX to PCI DSS and CCPA, maintaining compliance isn't just a checklist exercise — it requires continuous oversight and airtight documentation.

Yet many large banks struggle with siloed communication systems that make it difficult to enforce policies consistently or track user activity effectively. Fragmented tools can result in audit blind spots, inconsistent enforcement, and costly delays in generating reports or demonstrating proof of compliance.

One notable example comes from 2020, when the New York Department of Financial Services fined [Deutsche Bank over \\$150 million](#) for compliance failures — including inadequate monitoring of communications related to high-risk clients. Regulators noted that despite warnings, the bank lacked sufficient control over how teams communicated and documented decision-making — underscoring the importance of secure, trackable collaboration workflows.

This case illustrates how gaps in communication oversight can translate directly into regulatory penalties and reputational harm. As the [Wall Street Journal notes](#), financial institutions increasingly grapple with expanding cyber regulations that require more detailed, real-time evidence of security and compliance across teams and platforms.



€20 MILLION OR 4% OF ANNUAL GLOBAL TURNOVER

Financial services firms can be fined up to €20 million or 4% of annual global turnover, whichever is greater, for violating GDPR.

([GDPR.eu](https://gdpr.eu), 2025)



Industry Challenges:

Inside the High-Stakes Realities of Data Privacy, Incident Response, and Compliance

How Mattermost Bridges the Gap

Improving data security

As a secure collaboration solution that can be self-hosted, deployed in air-gapped environments, or delivered through a single-tenant private cloud, Mattermost helps financial services firms keep sensitive customer and business data secure by providing complete data sovereignty, which strengthens customer trust.

Mattermost also delivers [encryption capabilities](#) and [role-based access controls](#) (RBAC), which safeguard sensitive communications and keep bad actors at bay. Combined with logging and monitoring capabilities, Mattermost strengthens incident response and prevention, which is essential to maintaining client trust and regulatory confidence.

Accelerating incident response

Mattermost's real-time communication capabilities enable rapid coordination across response teams, improving both detection and containment efforts during incidents. By providing a centralized communication hub with secure messaging, file sharing, incident tracking, screensharing, and more, Mattermost helps teams reduce response times and enhance situational awareness during crises.

As an open source solution, Mattermost also seamlessly integrates with other incident response tools, minimizing context switching while increasing visibility and coordination throughout the response lifecycle. Altogether, these capabilities help financial services firms protect against cyberthreats and rapidly resolve incidents should they occur.

Automated reporting and real-time compliance tracking

Modern compliance requires collaboration platforms that embed security and visibility into every exchange. Mattermost offers automated logging, encrypted messaging, and granular access controls to help institutions simplify audit preparation and maintain real-time compliance tracking.

With customizable reporting and integrations that support financial governance frameworks, Mattermost helps organizations strengthen accountability without slowing down operations. As a result, financial services firms can protect their reputations — and their bottom lines.

Secure collaboration in financial services isn't just about technology — it's about building operational strategies that reduce risk, maintain compliance, and improve organizational resilience.

By following these proven best practices, financial services firms can develop a communication ecosystem that's purpose-built for high-stakes environments.

Best Practices:

How Secure Collaboration Improves Energy Resilience

Secure collaboration in financial services isn't just about technology — it's about building operational strategies that reduce risk, maintain compliance, and improve organizational resilience.

By following these proven best practices, financial services firms can develop a communication ecosystem that's purpose-built for high-stakes environments.

1. Design Security Around Collaboration, Not Just Infrastructure

In highly regulated environments like banking, communication security must go beyond firewalls and VPNs. Institutions need platforms where every message, file, and user action is encrypted, logged, and access-controlled by design — not as an afterthought.

Practical execution steps:

- Enforce encryption across all messaging channels
- Apply role-based access controls to ensure only authorized users can access mission-critical information
- Centralize administrative oversight with audit-ready activity logs
- Integrate secure messaging with key business systems

2. Ensure Incident-Ready Communication

Security incidents require immediate, coordinated responses across departments — from security and compliance to legal and executive teams. Delays caused by siloed communication or unclear chains of command can escalate breaches and increase costs.

Practical execution steps:

- Use always-on, secure messaging for crisis coordination
- Enable offline messaging in degraded environments
- Integrate alerting and ticketing systems with collaboration tools
- Designate response channels and escalation playbooks for rapid activation



Best Practices:

How Secure Collaboration Improves Energy Resilience

3. Embed Compliance into Daily Workflows

Compliance should be baked into the infrastructure of team communication — not a separate burden added after the fact. Collaboration tools should automate the creation of audit trails, offer real-time access logs, and enable encrypted storage and communication.

Practical execution steps:

- Enable real-time compliance logging and activity tracking
- Automate data retention and deletion policies
- Use secure file sharing and role-based document access
- Generate audit-ready reports from within the platform

4. Enable Cross-Border and Cross-Team Alignment

Large banks operate across multiple jurisdictions, with different regulatory requirements and cultural expectations. Collaboration platforms must support [multilingual teams](#), comply with regional data residency laws, and integrate with systems across business units.

Practical execution steps:

- Offer multilingual UIs and local data hosting options
- Align communication access with organizational roles and hierarchies
- Build connectors to core systems across business units
- Maintain audit trails across geographies for consistent oversight

5. Prioritize Human-Centric Security Culture

From phishing attempts to misdirected messages, human behavior is one of the biggest variables in cybersecurity risk. In fact, a recent [Harvard Business Review](#) report found that human error accounts for more than 80% of all cyber incidents. In financial services — where trust, confidentiality, and precision are non-negotiable — seemingly small communication errors can have outsized consequences.

Practical execution steps:

- Embed training and onboarding directly into collaboration platforms
- Use built-in prompts to guide secure file sharing and message handling
- Create persistent channels for security updates and peer learning
- Highlight and reward teams that demonstrate strong security habits



Mattermost:

The Secure Collaboration Platform Purpose-Built for Financial Services

Financial institutions operate under extraordinary pressure. They must secure sensitive client data, respond to threats in real time, and navigate global compliance standards — all while maintaining the trust of customers and regulators.

Mattermost is built for these realities. As a self-hosted secure collaboration platform, Mattermost gives financial institutions complete control over their collaboration data and entire communication environment — without sacrificing speed, agility, or usability.

Whether you're responding to a breach, coordinating with global risk teams, or preparing for a compliance audit, Mattermost helps your organization:

- **Protect sensitive communications** with encryption, granular permissions, and full data ownership
- **Accelerate incident response** with secure messaging, file sharing, and robust integrations with security tools and governance, risk, and compliance (GRC) solutions
- **Prove compliance, not just claim it**, through automated audit logs, access tracking, and secure data retention
- **Unify cross-border collaboration** while meeting data residency and jurisdictional requirements
- **Maintain operations during outages** with out-of-band messaging and mobile access in critical moments

What does this look like in the real world?

For a top-three global bank, managing critical incidents requires coordinated and rapid response across a large, highly distributed IT organization. The team uses Mattermost as their command center for incident response, ensuring that context can be shared quickly, stakeholders can be brought into the conversation securely, and details of the incident are appropriately recorded. After implementing Mattermost, the organization was able to reduce average incident response time by 90% — from 20 minutes to 2 minutes. [Learn more about how the financial services firm uses Mattermost.](#)

Mattermost is trusted by some of the world's most security-conscious teams — including the [United States Air Force](#), [Fujitsu](#), and [CERN](#) — because it meets high-stakes demands without compromise.

**Take the next step in your
secure collaboration journey**

**Schedule a Demo of
Mattermost**



Schedule a Demo



The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.