eSHARE

Positioning External Data Sharing Risks: Opportunities to Drive Secure Collaboration

Mike Towers
Chief Strategy & Trust Officer

Executive Summary

CISOs and their teams have historically under-prioritized outbound data sharing risks - particularly email attachments, uncontrolled guest access, shadow sharing solutions, and emerging AI agent data exchange. This strategic blind spot stems from perceptual, operational, and historical factors documented in industry reports (e.g., Verizon DBIR, IBM Cost of a Data Breach, Gartner).

However, three convergent shifts have elevated this from a "slow bleed" to C-level urgency: platform proliferation creating visibility gaps, AI agent autonomy enabling machine-to-machine data exchange at scale, and regulatory evolution demanding demonstrable control over external data flows. This document positions these risk scenarios through the lens of pain points, including risk exposure, compliance, resource allocation, user experience friction, and business impact, while showcasing eSHARE's unique value as a secure collaboration enabler that solves the user experience paradox.

This is an opportunity to transform a pervasive liability into a strategic differentiator, by implementing preemptive governance without overhauling existing defenses or sacrificing productivity.

Introduction

Over the years, I've seen how external data sharing risks - those seemingly innocuous email attachments, overshared Teams channels, or expedient WeTransfer links - can accumulate into major exposures. Yet these outbound risks remain deprioritized amid the chaos of inbound threats like phishing and ransomware.

This document reframes the issue constructively, highlighting its expanding scale while showcasing how eSHARE empowers organizations to contain it. By drawing on updated data, regulatory realities, and empathetic understanding of CISO challenges, we position eSHARE as a collaborative business enabler. This can turn a "silent" multi-channel threat into a strategic advantage that supports revenue growth, partnership velocity, and zero-trust maturity.

Why This Matters More Now Than Ever

Outbound email risks have existed for years, yet the primary threat was human error with attachments. That risk hasn't disappeared, but three fundamental shifts have transformed it from an operational concern into a strategic imperative:

Platform Proliferation and Visibility Gaps

External data sharing no longer happens primarily through email. Today's knowledge workers share sensitive information across email attachments, Microsoft Teams external guest access, SharePoint/OneDrive "anyone with the link" shares, shadow sharing solutions, and emerging AI agent-to-agent data exchange. The result: most organizations cannot answer the diagnostic question "How many external shares occurred across all channels last month?" This fragmented visibility creates continuous exposure where sensitive data flows externally through dozens of unmonitored pathways.

AI Agent Autonomy and Machine-Speed Data Exchange

At the 2025 Gartner IT Symposium/Xpo, analysts predicted that 90% of B2B buying—representing over $15 trillion in transactions—will be AI agent-intermediated by 2028. Consider procurement: today, a human specialist requests quotes and negotiates terms with security review opportunities at each step. By 2028, an AI procurement agent does this autonomously, sharing budget parameters, technical requirements, and internal constraints with vendor AI sales agents - at machine speed, potentially thousands of times per day, with minimal human oversight.

IBM's 2025 Cost of a Data Breach Report validates this concern: 97% of organizations that experienced AI-related security incidents lacked proper AI access controls, and 63% lacked AI governance policies. This represents a 10-100x multiplication of external data sharing velocity operating on today's governance foundations—or more accurately, the lack thereof.

Regulatory Evolution Demanding Demonstrable Control

Regulatory frameworks have evolved from "implement reasonable security measures" to "demonstrate continuous control over external data flows:"

- **GDPR (EU):** Fines up to €20 million or 4% of global revenue for failing to protect personal data transfers
- **HIPAA (US Healthcare):** Penalties up to $50,000 per incident for impermissible disclosures of protected health information
- **Sector-Specific Frameworks:** FDA 21 CFR Part 11 and EU GMP Annex 11 require data integrity controls for life sciences

The shift is from retroactive breach notification to preemptive data governance. Regulators now expect organizations to know, in real-time, where sensitive data is shared externally, who has access, and what controls prevent unauthorized disclosure.

The Convergence

These three shifts converge on a single capability gap that fewer than one in four organizations have addressed: unified external data governance. The outbound email problem security teams have managed for 20 years is becoming the outbound multi-channel, AI-accelerated data governance crisis of 2025-2028.

The Problem: External Data Sharing as a Silent, Multi-Channel Risk

Email attachments, Teams guest access, SharePoint external links, and shadow sharing tools remain staples of business collaboration. Gartner's 2024 Digital Worker Experience Survey shows that 60% of enterprise data sharing still occurs via email, with users citing familiarity and universal access as primary reasons. This persistence creates multiple exposure vectors:

Data Leakage Across Channels:

- Accidental email sends to wrong recipients
- Overly permissive Teams guest access granting external parties access to entire channel histories
- SharePoint "anyone with the link" shares that never expire
- Shadow IT adoption when enterprise tools are too restrictive
- AI agents autonomously sharing proprietary data during procurement or partnership workflows

Compliance Violations and Financial Impact:

- GDPR fines reaching €20 million+ for inadequate data transfer controls
- HIPAA penalties of $50,000+ per incident for impermissible PHI disclosures
- EU GMP Annex 11 data integrity failures delaying regulatory approvals

Intellectual Property and Reputational Harm:

- Leaked clinical trial protocols delaying FDA approvals
- Proprietary pricing models shared with competitors
- M&A due diligence materials disclosed prematurely

Third-Party Risk Amplification:

Verizon's 2025 DBIR found that breaches involving third-party participation doubled year-over-year. When organizations share data externally without governance, they multiply their attack surface by the security posture of every recipient.

Unlike inbound phishing or ransomware, these risks accumulate gradually, rarely cause immediate crises, and require sophisticated analytics to detect. This creates a "boiling frog" problem where continuous exposure goes unnoticed until a major incident forces visibility.

Why Has This Been Under-Prioritized?

CISOs focus resources on high-visibility threats, but external data sharing risks slip through due to a self-reinforcing cycle:

Inbound Threats Dominate Visibility and Urgency

Phishing campaigns and ransomware cause immediate business disruptions, such as encrypted systems, halted operations, emergency responses, that trigger C-level scrutiny. Verizon's 2025 DBIR shows that credential-based attacks and social engineering remain the primary initial access vectors, naturally focusing CISO attention on email security gateways and endpoint detection.

In contrast, outbound data leaks are "silent;" they don't trigger alarms, don't encrypt databases, and don't generate panicked help desk calls. They require advanced DLP analytics and manual investigation to detect. The result: SOCs allocate resources to threats that "scream" (ransomware) rather than those that "whisper" (data exfiltration).

Cultural and Behavioral Inertia

Users view email and familiar sharing methods as reliable and frictionless. Gartner's research indicates that 70% of users prefer email for external sharing because it "just works;" no account creation, no training, no platform compatibility concerns. Without compelling metrics demonstrating true cost, the risk remains theoretical.

McKinsey characterizes this as "behavioral inertia" - the assumption that shifting collaboration habits will meet organizational resistance, generate helpdesk tickets, and ultimately fail due to shadow IT adoption. This creates a paradox: the more critical external collaboration is to business velocity, the more resistant organizations become to imposing governance.

A Structural Governance Mismatch

Traditional data governance assumed a structured, bounded environment - databases, file servers, applications with clear perimeters. These models worked reasonably well for machine-to-machine and client-to-server collaboration where data moved through predictable pathways.

Modern productivity suites (e.g., Microsoft 365, Google Workspace, Slack) operate fundamentally differently: interconnected, fluid platforms where a single document can be edited, shared via multiple channels, synchronized, and externally distributed within seconds. The old governance models become fragile and counterproductive:

- Restrictive controls drive shadow IT adoption
- Point-in-time permissions don't account for cascading shares
- Channel-specific policies create inconsistent user experiences
- Policy decisions based on static metadata rather than real-time signals

This structural mismatch explains why even sophisticated organizations struggle: they're applying database-era control models to collaboration-era platforms. eSHARE bridges this gap with governance-native architecture designed for fluid, interconnected environments.

Resource and Tooling Constraints

Security teams operate under constant resource pressure. SOC analysts naturally prioritize alerts indicating active malware or lateral movement over DLP alerts flagging potential data leakage. Furthermore, outbound DLP implementations face high false positive rates, classification challenges, multi-channel fragmentation, and user friction.

Gartner's research indicates that only approximately 40% of enterprises have mature, actively enforced outbound DLP programs. When budgets tighten, external data governance gets deprioritized.

User Experience Friction: The Historical Barrier

This has been a significant factor in most organizations: CISOs have been conditioned for years to avoid security controls that require active user participation. Traditional security controls, such as firewalls, antivirus, encryption, and logging/monitoring, operate invisibly or restrictively without requiring users to change workflows. When controls do impact users (complex password policies, restrictive application whitelisting), the result is predictable: helpdesk floods, executive complaints, and shadow IT adoption.

Ponemon Institute's 2024 Cost of Insider Threats Report documented that 60% of CISOs cite productivity concerns as the primary barrier to implementing stronger data exfiltration controls. eSHARE fundamentally solves this paradox by making secure sharing easier than insecure sharing; the control becomes the path of least resistance rather than an obstacle.

Perception of Existing Mitigation

Many organizations assume their current investments provide adequate protection, including email security gateways, CASBs, DLP tools, encryption requirements. These controls address portions of the problem but share critical limitations:

Modern productivity suites (e.g., Microsoft 365, Google Workspace, Slack) operate fundamentally differently: interconnected, fluid platforms where a single document can be edited, shared via multiple channels, synchronized, and externally distributed within seconds. The old governance models become fragile and counterproductive:

Retroactive, Not Preemptive: They detect violations after data has been shared

Channel-specific policies create inconsistent user experiences

Signature-Based, Not Context-Aware: They miss contextual sensitivity

In regulated industries, security focuses on internal systems – enterprise core applications, clinical trial management, document management. This overlooks the reality that users routinely extract data from governed systems to share externally when business velocity demands it.

The "Email is Declining" Fallacy

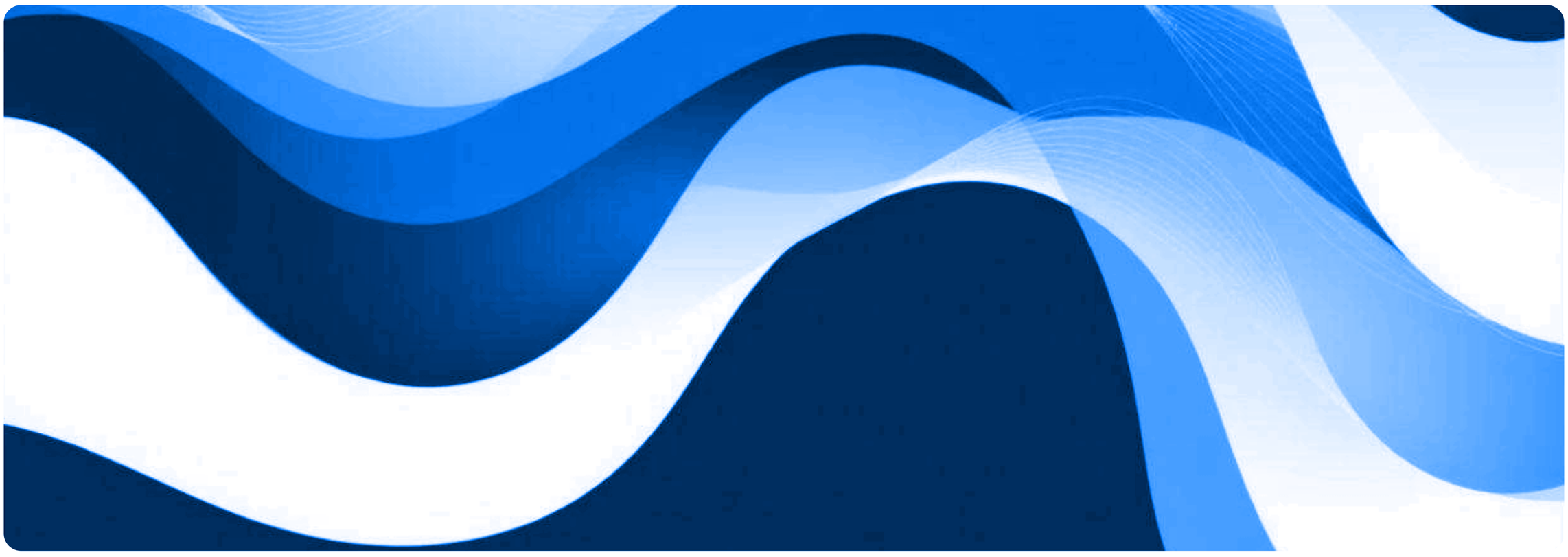
Some security leaders assume email-centric risks are naturally declining as collaboration platforms gain adoption. This is dangerous for two reasons:

- **Email attachments persist at scale.** Verizon's 2025 DBIR indicates that email remains a factor in approximately 20% of data exposure incidents. Email works across organizational boundaries and requires no recipient account setup.
- **The risk has metastasized to new channels.** Teams external guest access, SharePoint external sharing, and OneDrive link sharing create the same exposure patterns with even less visibility. The total volume of external data sharing has increased while visibility and control have fragmented.

The Convergence: A Self-Reinforcing Cycle

These factors create a self-reinforcing cycle where inbound threats consume resources, outbound risks remain "silent," users resist workflow changes, existing tools provide false confidence, and budget flows to "screaming" threats. It's a "boiling frog" problem where outbound risks accumulate gradually without the drama of ransomware headlines.

Quantifying the Scale and Impact



Prevalence: The Volume of External Data Sharing

Gartner's 2024 Digital Worker Experience Survey:

60% of enterprise data sharing still occurs via email

Microsoft's Power Platform Community Conference:

3 million AI agents were built in FY25

Pharma/Life Sciences Collaboration

External collaboration is foundational. Sharing clinical protocols with CROs, submitting regulatory dossiers, exchanging research data with academic partners.

This volume creates a massive attack surface; every external share is a potential exposure point.

Risk Exposure: When External Sharing Goes Wrong

2x

Verizon's 2025 DBIR

Breaches involving third-party participation doubled year-over-year

$4.4 million

IBM's 2025 Cost of a Data Breach Report

Global average cost reached $4.4 million

97%

IBM's 2025 Report - AI Security Gap

97% of organizations with AI security incidents lacked proper access controls; 63% lacked AI governance policies

Outbound data sharing may contribute to 20% of breaches with an average incident cost approaching $4.4 million.

Sector-Specific Impact: The Regulated Industry Multiplier

GDPR:
Fines up to €20 million or 4% of global annual revenue

HIPAA:
Penalties ranging from $100 to $50,000 per violation (per record, per day)

EU GMP Annex 11:
Data integrity failures can delay regulatory submissions

Intellectual Property and Competitive Impact:

- Leaked clinical trial protocols enable competitor patents or delay FDA approval
- Disclosed pricing models eliminate competitive leverage
- Premature M&A disclosure torpedoes deals

Broader Trends: Remote Work and AI Acceleration

Ponemon Institute's 2024 Report
60% of CISOs cite productivity concerns as the primary barrier to data exfiltration controls

McKinsey's Research:
CISOs allocate only approximately 15% of security budgets to data exfiltration prevention

Gartner's Predictions:
90% of B2B buying becoming AI agent-intermediated by 2028 requires preparing for a 10-100x increase in external data exchange velocity

Conclusion: A Path Forward

The strategic blind spot around outbound data governance isn't a failure of CISO team competence, rather it's the natural result of historical factors. But three convergent shifts have transformed this into a strategic imperative:

- Platform proliferation has multiplied channels while fragmenting visibility
- AI agent autonomy will create a 10-100x increase in data exchange by 2028
- Regulatory evolution demands demonstrable, continuous control over external flows

eSHARE enables CISOs to lead this evolution, turning hidden liabilities into strategic advantages. The key question for leadership teams:

"Can we identify every instance where our data was shared externally last month—across email, Teams, SharePoint, shadow IT, and AI agents?"

When the answer is "no," that's the business case for unified external data governance. Don't wait for a breach or regulatory action. The 3 million AI agents already deployed will operate in the 2028 environment Gartner predicts. Implement a Trusted Collaboration Fabric and build governance frameworks now, while it's a strategic opportunity rather than a crisis response.

References

Industry and Advisory Reports

- Verizon Data Breach Investigations Report (DBIR) 2025
- IBM Cost of a Data Breach Report 2025
- Ponemon Institute - 2024 Cost of Insider Threats Global Report
- Gartner 2024 Digital Worker Experience Survey
- Gartner IT Symposium/Xpo 2025 - Key Predictions: synthesis of conference sessions (October 2025, Orlando, FL)
- Microsoft Power Platform Community Conference 2024: synthesis of conference sessions (October 2025, Las Vegas, NV)
- McKinsey & Company: Cybersecurity Reports (e.g., "Cybersecurity in a Digital Era" and related 2024 insights)

Regulatory and Compliance

- EU General Data Protection Regulation (GDPR)
- U.S. Department of Health and Human Services (HHS) – HIPAA Enforcement
- EU GMP Annex 11 Draft Revision
- FDA 21 CFR Part 11 (Electronic Records; Electronic Signatures)

Mike Towers
Chief Strategy & Trust Officer

Positioning External Data Sharing Risks: Opportunities to Drive Secure Collaboration

eSHARE

About eSHARE

Get in touch to weave your Trusted Collaboration Fabric. eSHARE secures every share while teams move faster with intelligent, Zero-Trust guardrails.

LinkedIn
Contact Us
www.eshare.com