Data Security and Compliance Risk

2025 Annual Survey Report

The Visibility Challenge: How AI and Third-Party Blind Spots Multiply Enterprise Risk
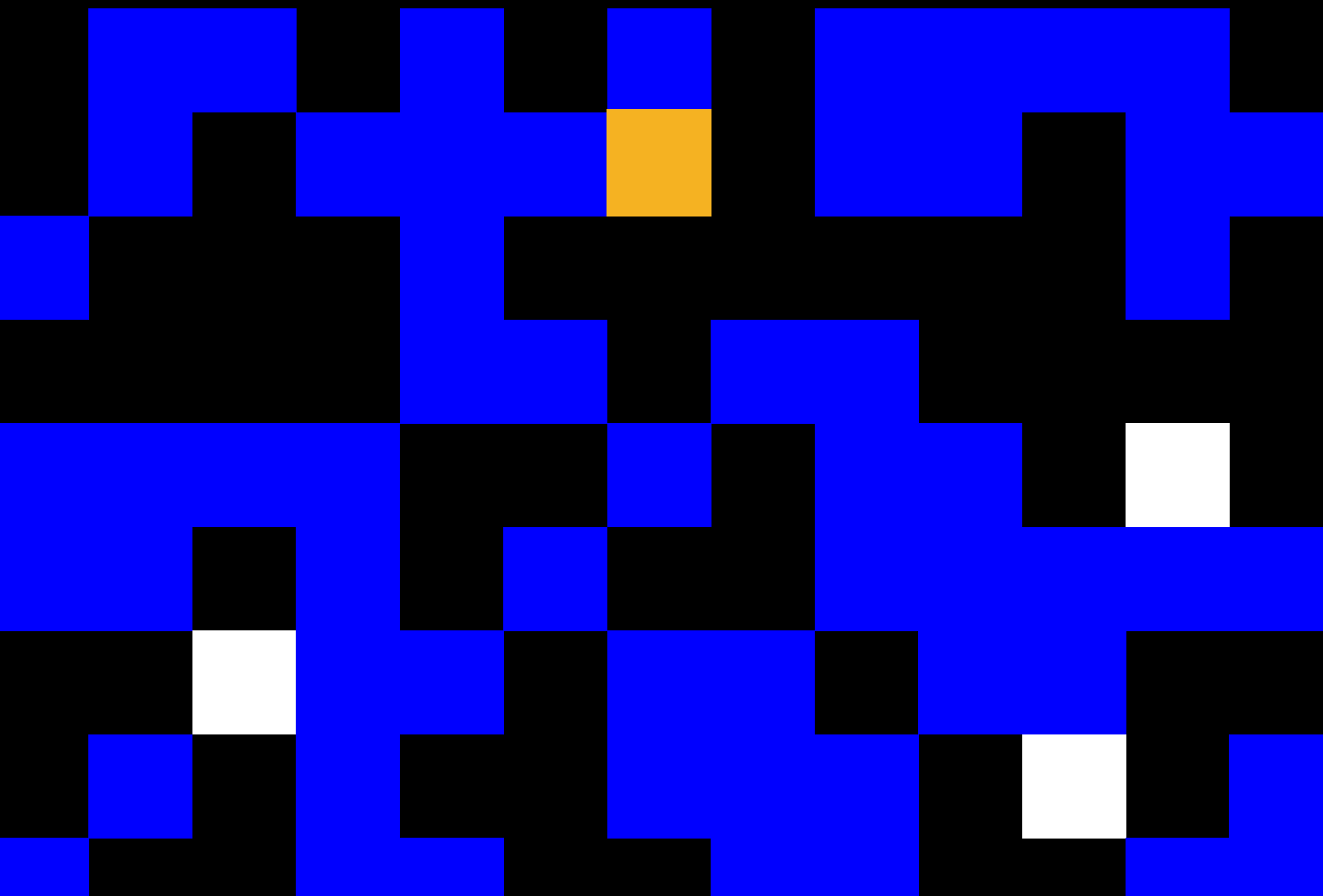
Table of Contents

Executive Summary

Visibility Challenge: What You Don't Know Is Killing Your Security

Welcome to Kiteworks' fourth annual Data Security and Compliance Risk: 2025 Annual Survey Report (formerly Sensitive Content Communications Privacy and Compliance Report).

Since 2022, we've tracked the evolution of data security as organizations face increasingly complex and interconnected challenges. This year's findings reveal a stark truth: Organizations operating blind face exponentially higher risks than those with clear visibility and governance.

The data is unequivocal—what you don't know compounds into catastrophic security failures, and those lacking visibility invariably lack proper data governance.

Organizations that answered "don't know" to key questions showed cascading failures:

46%
also didn't know their breach frequency

36%
implemented zero privacy technologies

60%
couldn't quantify litigation costs

Only
20%
adopted basic governance frameworks

Meanwhile, only **17%** of organizations have fully implemented AI governance frameworks on average across industries—a concerning gap in oversight capabilities—while 25% of ungoverned organizations rely solely on contractual approaches that may not withstand regulatory scrutiny.[1]

Poor visibility and weak governance create a deadly combination—exponentially multiplying risk.

10 Critical Findings That Define 2025

1   **Detection Delays Cost Millions.** **31%** of organizations with 5,000+ third parties take **>90 days** to detect breaches. Organizations with longer detection times face significantly higher litigation costs.

2   **AI Blind Spots Create Total Exposure.** **36%** of organizations that are unaware of their AI data usage have **no privacy technologies.** Organizations struggle with AI oversight, with only **17%** claiming to have technical governance frameworks. This gap creates dangerous blind spots as AI adoption accelerates.

3   **Third-Party Volume Predicts Breach Frequency.** Organizations with **5,000+ third parties with which they exchange privata data** face **10+ annual breaches** at a rate of 24%, while those with <500 partners show **34% zero breaches.**

4   **The 1,001–5,000 Partner Danger Zone.** Mid-sized ecosystems face **46% increased supply chain risks**—the highest of any segment. They have enterprise-scale problems with mid-market resources.

5   **Breaches Drive Exponential Costs.** While 45% with 1–3 annual hacks face <$1M costs, **77%** with 10+ hacks face **>$3M litigation.** Costs escalate dramatically with each breach tier.

6   **Motivations Shift From Proactive to Reactive.** Low-breach organizations prioritize efficiency (27%). High-breach organizations chase financial damage control (37%). Success requires staying ahead.

7   **The Privacy Dividend Emerges.** Organizations with mature privacy programs report **27% reduced security losses, 21% enhanced customer loyalty,** and **21% improved operational efficiency**—proving that privacy investment delivers measurable ROI beyond compliance.

8   **The 35/46 Geopolitical Squeeze.** **35%** face increased operational costs from tariffs while **46%** see compliance tool budget increases—creating a dual pressure that makes geographic avoidance strategies obsolete.

9   **The Hidden Cost Multiplier.** For every **$1.00** spent on visible compliance, organizations incur **$2.33** in hidden costs including opportunity costs, innovation delays, and audit fatigue—revealing the true burden of manual approaches. In addition, organizations with comprehensive governance achieve 3.5x better cost visibility—**75%** can specify their localization costs versus only 35% of those without governance plans.

10   **The Segregation Paradox.** **37%** of organizations implement data segregation by geography to meet compliance, yet this fundamentally conflicts with AI's need for unified data sets—creating a tension between compliance and innovation.
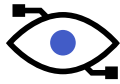
The Four-Year Evolution: From Simple to Systemic

Note: Historical data from previous Kiteworks reports shows persistent gaps despite growing awareness.

Encryption
Improved from 47% (2022) to ~54% (2024), but progress stalled in 2025

Visibility
Only 50% achieved centralized governance by 2025

Compliance
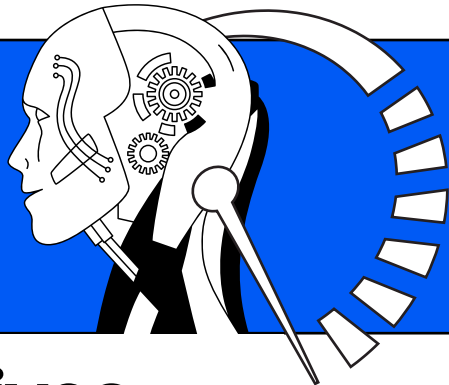70%+ still rely on manual processes

Privacy-Enhancing Technology
Stuck below 20% for advanced technologies

The Acceleration Effect

Risks no longer add—they multiply. AI uncertainty × third-party volume × compliance complexity = exponential exposure.

Critical Actions: What Drives Success vs. What Creates Risk

Category	What Drives Success	What Drives Risk
Third-Party Visibility	Know their numbers: Track exact third-party counts	Operate blind: 46% who don't know partner counts also miss breaches
AI Governance	Measure AI usage: Among organizations that measure AI-generated content, 93%-96% report implementing at least one PET	Ignore AI risks: 36% unaware of AI usage have zero protections
Detection Speed	Detect fast: 43% of low-breach organizations detect in <7 days	Detect slowly: 31% of large ecosystems take >90 days
Investment Strategy	Invest in the middle: Apply enterprise controls at 1,000+ partners	Underinvest at scale: 46% in danger zone lack adequate controls
Security Technology	Layer defenses: Average 3.2 PETs vs. 0.8 for high-breach organizations	Rely on basics: 36% of "don't know" organizations use no PETs
Geographic Strategy	Balance geography with technology: Use approved transfer mechanisms (53%) rather than avoiding jurisdictions (23%)	Avoid rather than adapt: The 23% avoiding jurisdictions face higher costs and limited growth
Architecture Approach	Invest in distributed architectures: The 29% using distributed cloud see better outcomes across all metrics	Depend solely on contracts: 20% using only contractual safeguards report worse outcomes

Figure 1: What Drives Success vs. What Creates Risk.

The difference isn't budget or sophistication–it's visibility and proactive investment before hits.
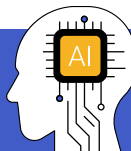
Industry Variations: Not All Sectors Are Equal

Leading the Pack

Financial Services
63% comprehensive controls, 47% EU Data Act ready

Technology
42% claim fully implemented AI governance

Healthcare
65% "very confident" in tracking capabilities

Education
Only 14% are prepared for EU Data Act

Legal
23% have no preparation plans

Government
58% struggle with third-party compliance

Falling Behind

Moving Forward

This report provides detailed analysis, from the visibility challenge through strategic roadmaps. Whether you're a CISO defending against AI threats, a compliance leader preparing for the EU Data Act, or a board member quantifying cyber risk, you'll find actionable insights based on real-world data.

Bottom Line: In 2025, visibility determines destiny. Organizations that achieve transparency across their third-party ecosystems, AI usage, and security posture will thrive. Those operating in darkness face escalating breaches, exploding costs, and existential threats.

Letter From the Editor

Dear Colleagues,

When we launched this report series four years ago, we aimed to track how organizations protect their most sensitive digital assets. What began with metrics like encryption rates and third-party counts has evolved into a far more complex picture—one shaped by AI proliferation, regulatory sprawl, and an explosion in third-party ecosystems.

This year's report lays bare a critical inflection point. While a handful of organizations have embraced automation, PETs, and centralized governance, the majority remain stuck in manual processes with limited visibility—despite the existential risks they now face.

One of the most urgent insights this year is the emergence of the **1,001–5,000 third-party "danger zone."** Organizations in this category now face the worst outcomes across nearly every measure: breach frequency, detection delays, and litigation costs. These firms are caught between enterprise-level complexity and mid-market budgets—with attackers increasingly taking notice.

Meanwhile, **AI governance gaps have grown more pronounced**. Although 64% of organizations now track AI-generated content (up from 28% last year), only 17% have implemented technical governance frameworks. And among those unaware of their AI data exposure, 36% use no PETs at all. These blind spots are not theoretical—they're compounding actual risk.

For the first time, we've introduced a **proprietary risk scoring algorithm** that synthesizes breach frequency, detection speed, and financial damage into a 1–10 scale. The results are sobering:

- Organizations in the "danger zone" scored the highest average risk (5.19)

- Those expressing the most confidence in their tracking paradoxically show higher risk scores—highlighting the **overconfidence effect**

- Firms with strong AI governance and privacy investment consistently scored lower, quantifying the real ROI of visibility and control

Across sectors and regions, we're also seeing diverging strategies. The most mature organizations balance distributed cloud architectures, PET deployments, and multi-jurisdictional compliance automation. Others continue to rely on contracts and employee training—strategies that are increasingly insufficient in the face of regulatory scrutiny and AI-driven threats.

The bottom line? In 2025, **good enough is no longer good enough.** Our research shows that exponential threats demand exponential responses. This report offers the data and frameworks to guide that transformation—including the industry's first quantitative model for benchmarking data security risk.

Thank you for your continued partnership in this critical work.

Sincerely,

Patrick Spencer

Patrick Spencer, Ph.D.
SVP, Americas Marketing and Industry Research
Kiteworks

Visibility-Governance Challenge

What You Don't Know Multiplies Risk

Visibility-Governance Challenge

In the world of data security, there's a fundamental truth that our four years of research has made undeniable: **You cannot protect what you cannot see.** Yet our 2025 data reveals that organizations across every industry, size, and geography are operating with dangerous blind spots that transform manageable risks into existential threats.

Compounding Effect of Unknown Unknowns

The most alarming discovery in our 2025 research is how visibility gaps cluster together. Organizations rarely have just one blind spot—unknowns breed unknowns in a cascade of expanding risk.

Our cross-tabulation analysis reveals how "don't know" responses correlate:

48% of those who don't know breach frequency can't quantify litigation costs

46% of these also don't know their breach frequency

42% of those uncertain about hacks report uncertainty in detection times

32% of those uncertain about third-party exposure conduct regular audits

Legend:
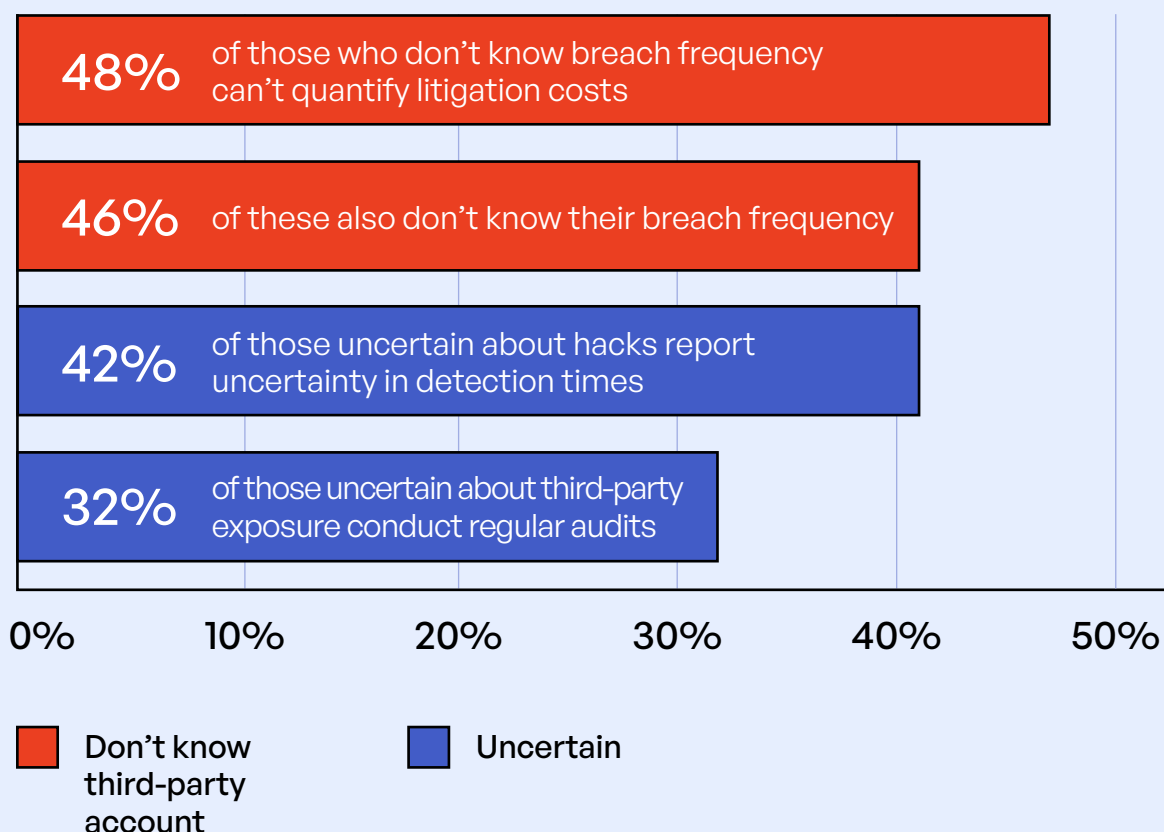- Don't know third-party account
- Uncertain

Figure 2: Cascade Effect: Lack of Visibility Translates Into Higher Risk.

Our analysis reveals four primary visibility failures and their documented impacts:

Visibility Gap	Survey Finding
Unknown Third-Party Count	46% also don't know breach frequency
Unknown AI Data Usage	36% have zero PETs implemented
Unknown Compliance Hours	20%–26% of various roles report "don't know"
Unknown Detection Times	42% don't know how many third parties exchange private data

Figure 3: Four "Unknown" Visibility Gaps.

Visibility Gaps Across Critical Dimensions

Dimension 1: Third-Party Ecosystem Visibility

The relationship between tracking confidence and security outcomes emerges clearly from our cross-analysis:

Percentage of Organizations	Third-Party Volume	Expressed Confidence Level	Most Common Breach Frequency
43%	**Fewer than 500**	Very confident	0 breaches
38%	**Fewer than 500**	Somewhat confident	1–3 breaches
57%	**Fewer than 500**	Not confident	1+ breaches
42%	**1,001–5,000**	Very confident	7–9 hacks

Figure 4: Confidence Levels and Breach Rates.

Key Finding

Even high confidence cannot fully overcome the risks of ecosystem complexity.
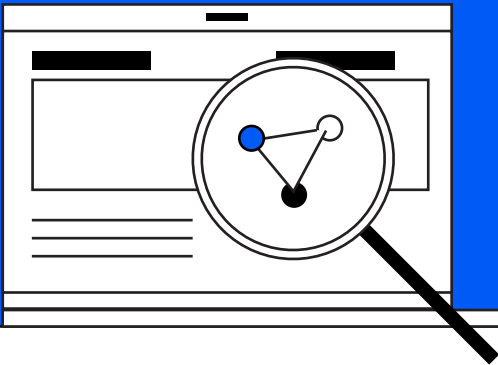
Confidence vs. Complexity: Third-Party Volume Still Drives Breach Risk

1   **Confidence in tracking data alone is not a strong safeguard**—even among organizations that report being "very confident" in their ability to control data exchanges, breach rates remain significant. Notably, 42% of very confident organizations with 1,001–5,000 third parties still experience 7–9 annual hacks.

2   **Ecosystem complexity drives breach exposure**—organizations with fewer than 500 third parties see lower breach rates overall, especially when confidence is high. But as the number of third parties increases, even high confidence levels fail to offset the elevated risk from larger digital supply chains.

Dimension 2: AI Data Usage Visibility

Organizations with clear AI data visibility demonstrate dramatically better security outcomes. As detailed in our AI Governance section, measurement drives action—those who track their AI usage are significantly more likely to implement protective measures.

Understanding these third-party risks becomes even more complex when artificial intelligence enters the equation. The following figure explores how AI adoption multiplies existing vulnerabilities and creates entirely new categories of risk.

No Visibility	AI Data Exposure Unknown	No AI Usage Controls	Comprehensive AI Governance	Concerned About Model Leakage
Third-Party Volume	57%	17%	31%	69%
EU Data Act Readiness	48%	20%	23%	75%
Breach History	46%	12%	31%	73%
Litigation Cost	45%	20%	30%	67%
Detection Time	61%	23%	23%	71%

Figure 5: No Business Visibility and AI Data Risk.

The figure reveals a strong and consistent pattern: Organizations that answered "Don't Know" to key cybersecurity questions—such as how many third parties they work with, their breach history, litigation exposure, or breach detection time—also lack visibility and control over AI data usage. For example, **61%** of those unsure about breach detection time also don't know what percentage of data entered into public AI tools is private. Similarly, **57%** of those who don't know their third-party volume lack awareness of AI data exposure. These knowledge gaps are paired with weak controls: Only **17%–23%** of these organizations have **no AI usage policies**, and just **23%–31%** have implemented **comprehensive AI governance** frameworks.

Despite these visibility blind spots, concern over AI security risks remains consistently high. In every "Don't Know" group, between **67%** and **75%** identified **model leakage** as a top concern—suggesting that organizations are aware of the threat but lack the visibility and infrastructure to address it effectively. This disconnect—between concern and action—highlights a dangerous operational gap: Visibility risks are not just technical oversights; they are indicators of broader governance failures that leave organizations vulnerable to AI-driven data loss, regulatory penalties, and reputational harm.

Building Visibility Infrastructure

Based on the patterns in our data, organizations achieving better outcomes share common characteristics:

Metric Category	Third-Party Count	AI Data Usage	Detection Speed	Compliance Effort	Breach Frequency
High Performance	Exact numbers by risk tier	Percentage of private data	Hours/days to discovery	Precise hour tracking	Exact incident counts
Low Performance	"Don't know" or estimates	No measurement	Unknown or >30 days	"Don't know"	Uncertain or untracked

Figure 6: Metrics That Matter: KPIs From the Data.

Confidence Level	Breach Rate	Detection Speed	Cost/Exposure
High Performance	43% report 0 breaches	Faster detection	Lower costs, better outcomes
Low Performance	Higher breach instances	Slower detection	Higher costs, more regulatory risk

Figure 7: Power of Confidence + Control.

The two figures above emphasize that **confidence and control are driven by visibility,** and that visibility, in turn, defines performance outcomes. Organizations in the "High Performance" group consistently report precise metrics across third-party volume, AI data usage, detection speed, compliance effort, and breach frequency—enabling them to detect breaches faster, reduce costs, and achieve better regulatory outcomes. In contrast, "Low Performance" organizations operate in a fog of uncertainty, often responding "Don't Know" to critical metrics, failing to measure AI data exposure, and taking over 30 days to detect incidents. These blind spots result in **higher breach rates, slower response times, and increased exposure to costs and compliance risk.** The message is clear: Investing in metrics and measurement capabilities isn't just operational best practice—it's the foundation for resilience.

The Difference

Visibility drives confidence, confidence enables control.
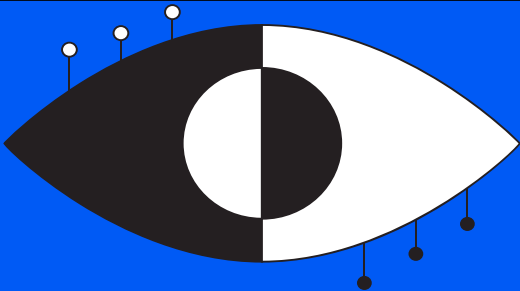
Dimension 3: Compliance Process Visibility

Across industry segments, organizations report wide variance in tracking compliance effort:
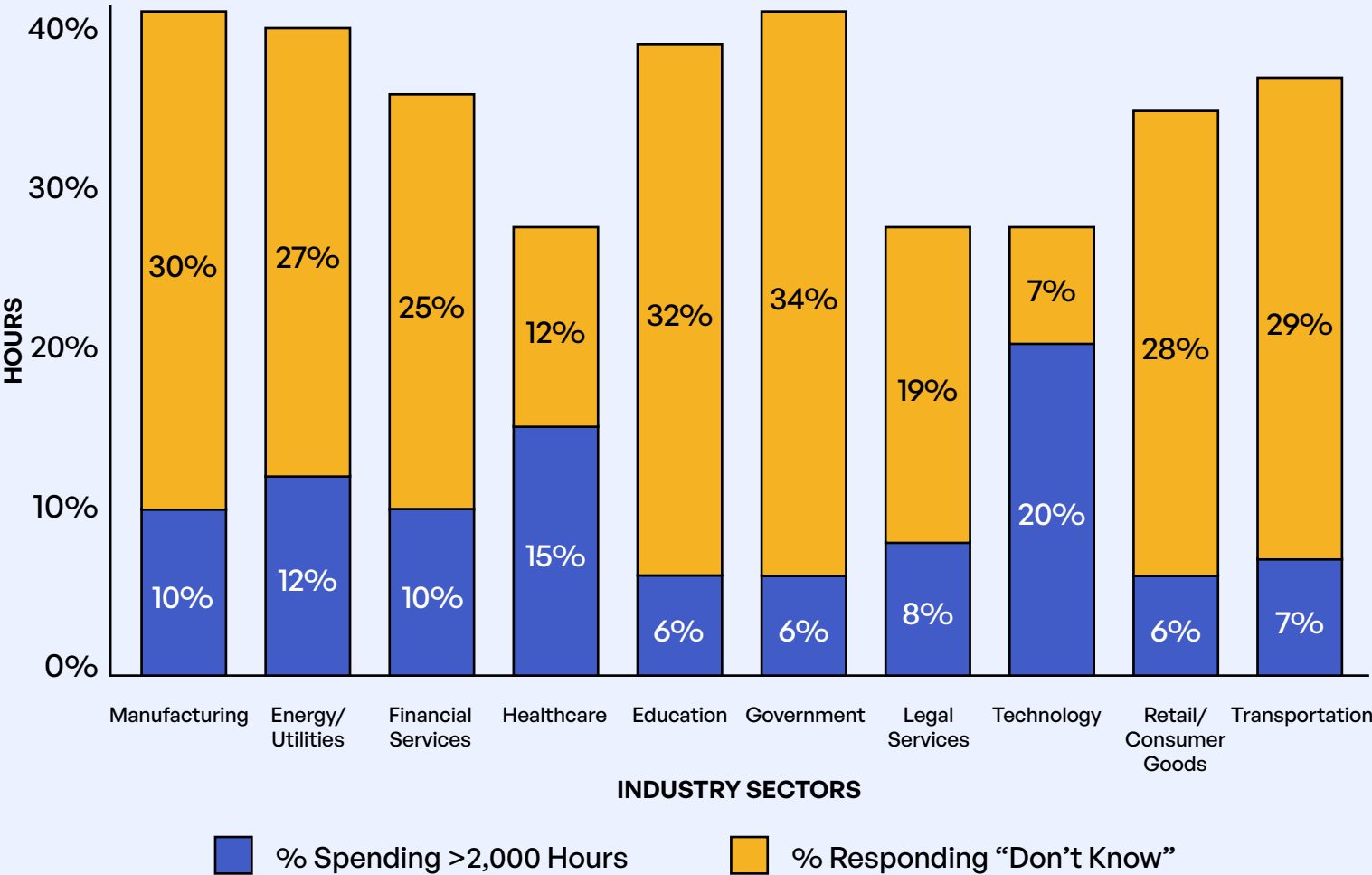

Figure 8: Industry Sectors and Compliance Tracking and Reporting Visibility.

Having established the critical importance of visibility across all security dimensions, we now examine how this visibility challenge has evolved over time—and why incremental improvements have failed to keep pace with exponential threats.

The chart reveals stark disparities in compliance process visibility across industries. Government and Education sectors report the **lowest rates of high compliance effort**—just **6%** in each spend over 2,000 hours—while also showing the **highest levels of uncertainty**, with **34%** and **32%** respectively saying they "don't know" how much time is spent. In contrast, the Technology sector leads in effort transparency, with **20%** spending over 2,000 hours and just **7%** unsure. Healthcare strikes a more balanced profile, while Financial Services and Energy/Utilities still show one-quarter or more unsure about compliance tracking. These gaps in visibility suggest that some sectors may be underestimating both the scope and cost of compliance—raising operational and regulatory risks in industries that already face high data and privacy obligations.
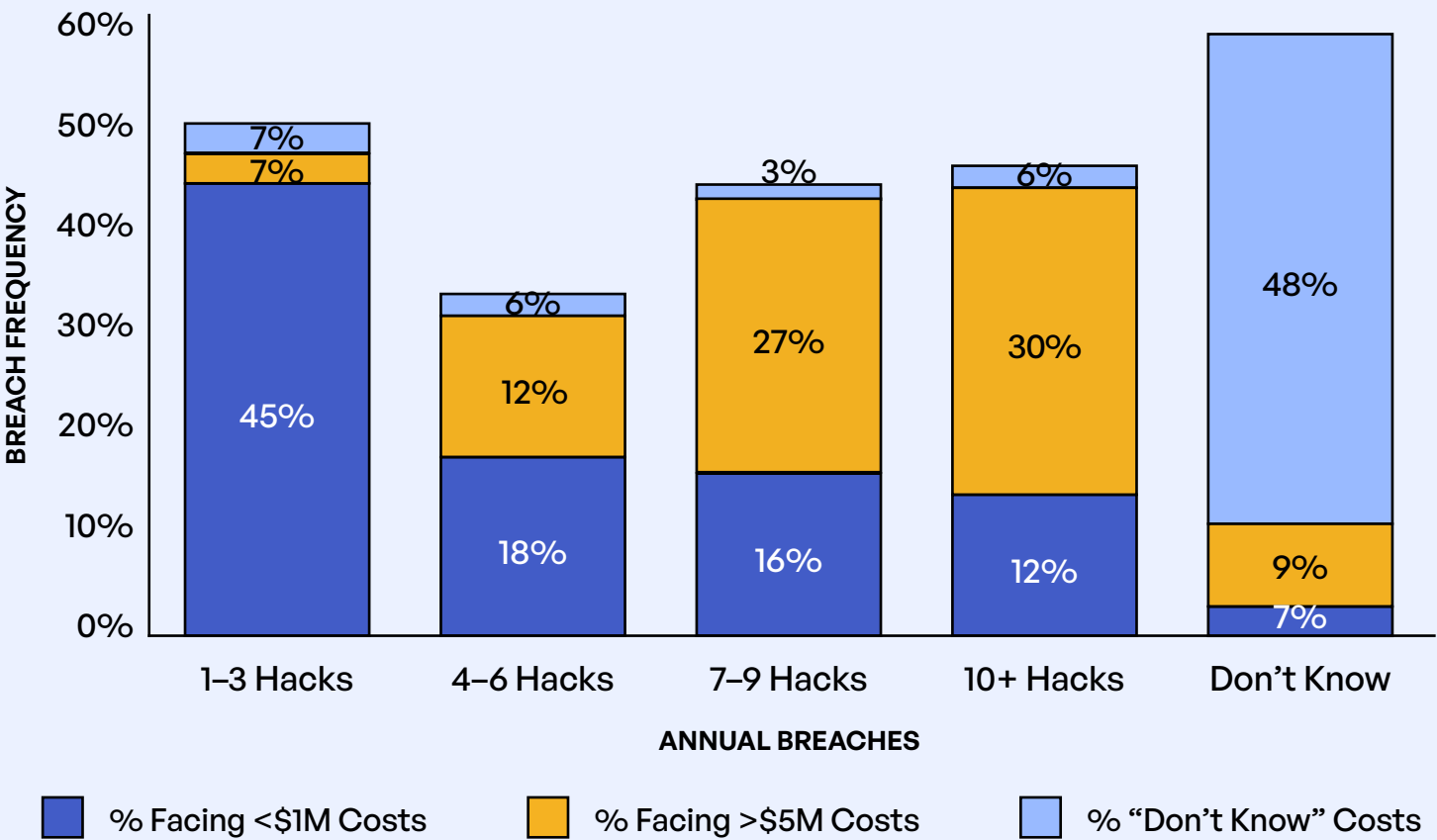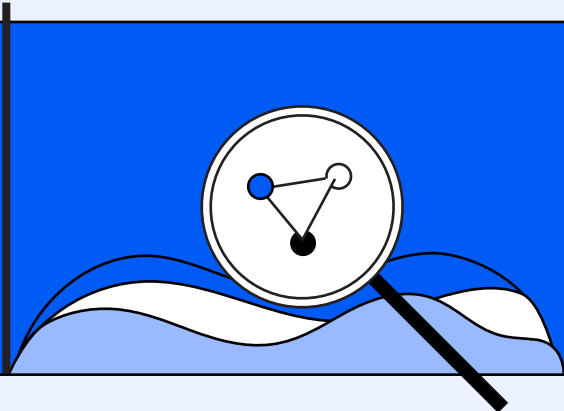

Figure 9: Breach Frequency and Litigation Costs.

Critical Finding

48% who don't know breach frequency also can't quantify litigation costs.

Detection Delays: Time-Cost Relationships

Following are detection time distributions, with concerning patterns for larger ecosystems:
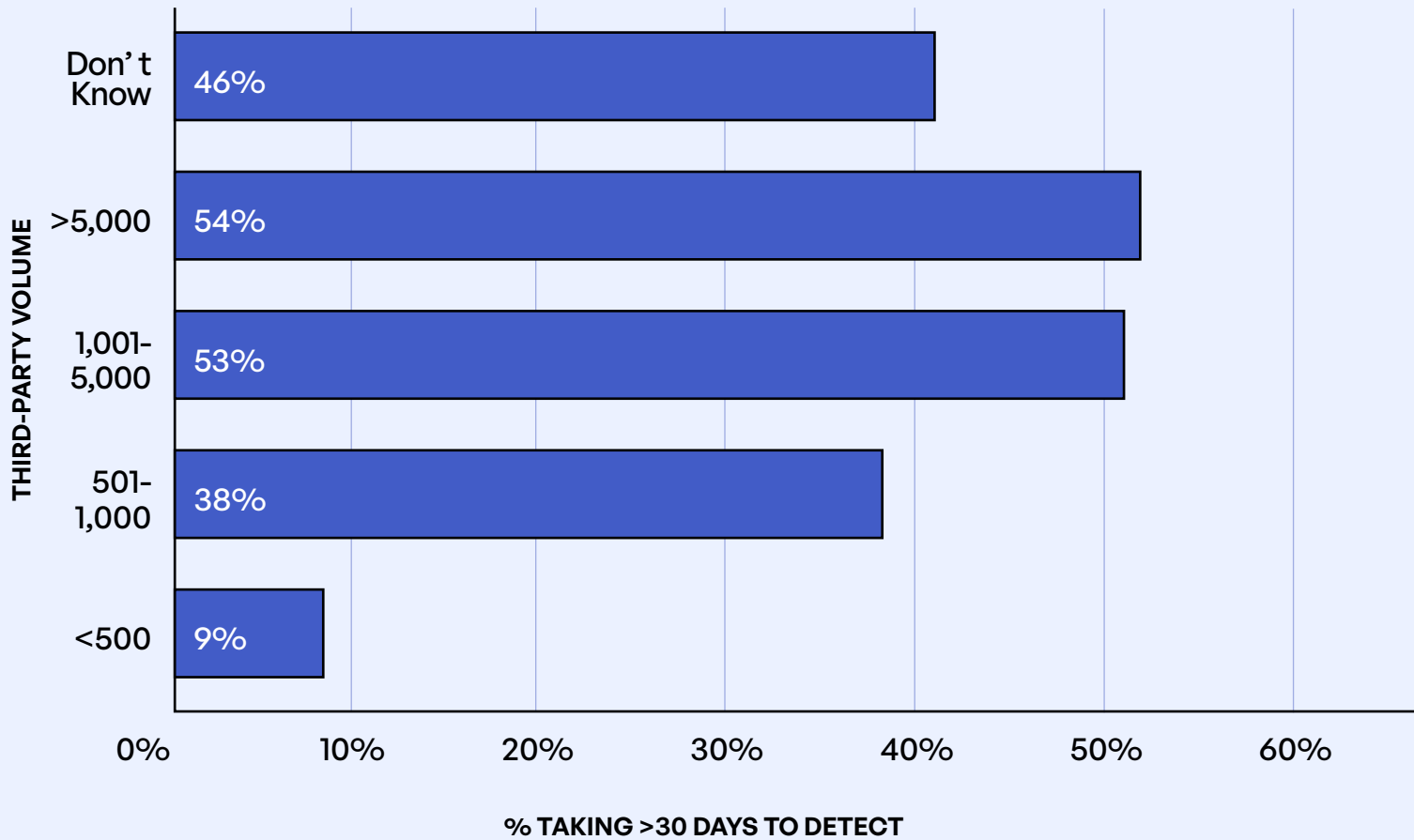

Figure 10: Detection Times by Third-Party Volume.

The data highlights a clear correlation between ecosystem complexity and detection delays, as well as the compounding risk of visibility gaps. Organizations with over 1,000 third-party connections take more than 30 days to detect breaches in over half of cases (53–54%), compared to just 9% for those with fewer than 500 third parties. Alarmingly, 42% of those who don't even know their third-party volume also exceed 30-day detection times—demonstrating how lack of oversight magnifies risk. Similarly, 48% of respondents who don't know how many breaches they experience annually also cannot quantify litigation costs. As breach frequency increases, so do high-cost outcomes: Nearly one-third of organizations with 10+ breaches report litigation costs over $5 million. These trends underscore a core message—**visibility gaps directly impair breach detection and financial risk management.**

Longitudinal Risk

*How Persistent Gaps Have
Created Today's Challenge*

2025 Annual Survey Report

Longitudinal Risk

Note: Historical data referenced in this section is derived from previous Kiteworks annual reports.
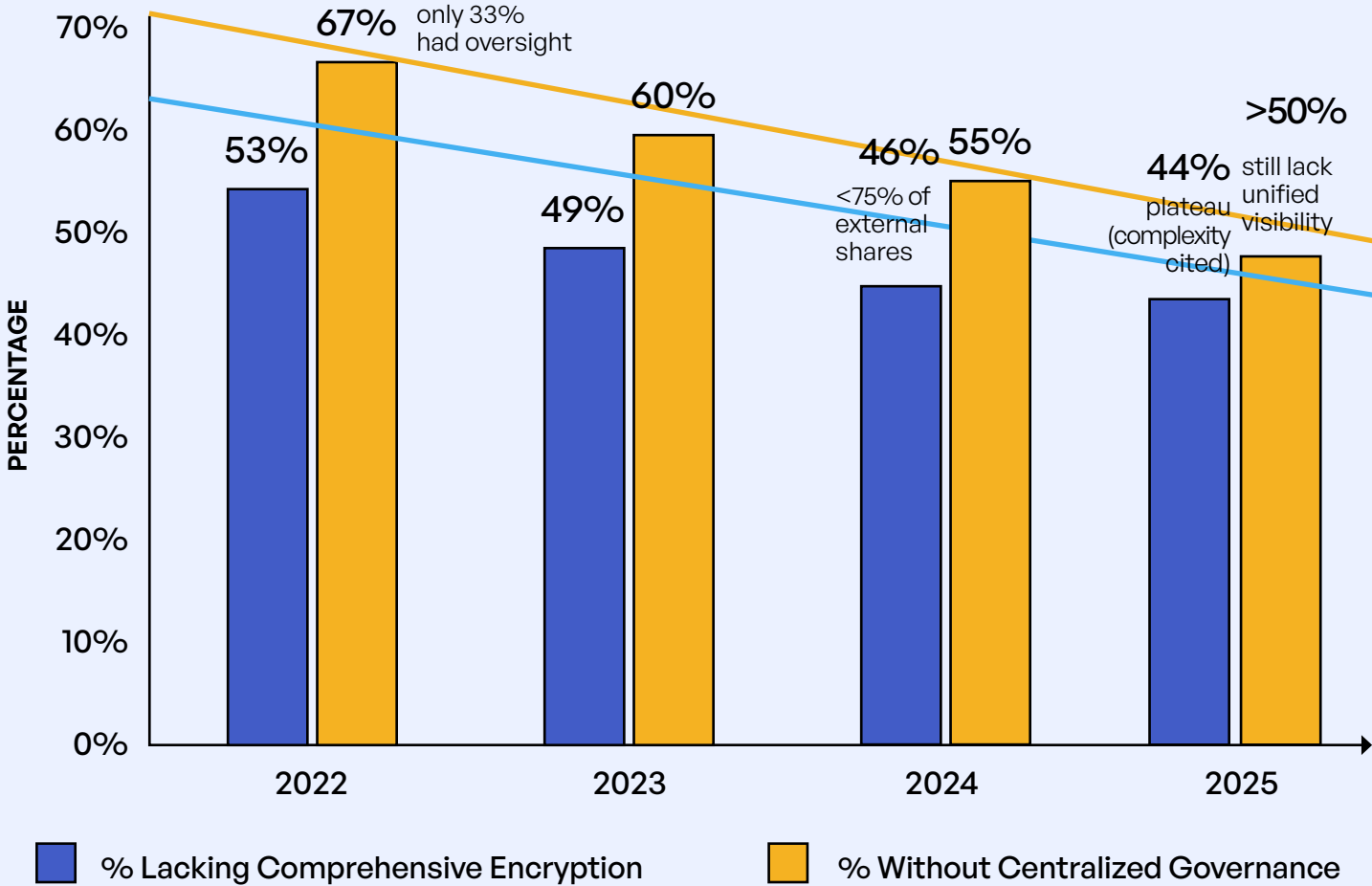

Figure 11: Persistent Gaps in Encryption and Visibility.

The data illustrates a troubling reality: Despite some year-over-year improvements in full encryption, centralized governance, and third-party inventory tracking, most organizations continue to face persistent gaps in visibility and automation. In 2025, only **56%** have implemented full encryption and just over **50%** have centralized governance. Meanwhile, **compliance automation remains critically underdeveloped**, with less than **35%** adoption, and **PET adoption remains stagnant** at below 25%. These plateaus in progress suggest that organizations are struggling not just with implementation, but with scalability and cross-functional integration—especially as complexity grows across larger ecosystems.

DATA SECURITY AND COMPLIANCE RISK REPORT SERIES   **17.**

Third Parties Remain a Risk Factor

51%

2021
Claimed Inadequate Third-Party Measurements

58%

2022
Cited No Risk Measurements for Third Parties

67%

2023
Said They Lack Full Third-Party Inventories

39%

2024
Identified Rising Risk (1,001–5,000 Third Parties)

24%

2025
With 5,000+ Third Parties Experienced 10+ Data Breaches

While 2023 saw a peak in risk immaturity—**67% of organizations lacked a full third-party inventory**—by 2025, that risk appears to have shifted into breach reality: **24% of organizations with 5,000+ partners reported 10 or more annual breaches.** The data also shows that **44% still lack unified encryption**, and **over half still lack centralized governance**, despite years of awareness. These trends confirm that **complexity is outpacing control**, and that organizations failing to invest in foundational visibility are seeing risk compound into exposure. The convergence of incomplete encryption, fragmented governance, and low automation creates systemic vulnerabilities that cannot be resolved piecemeal.

| Risk Domain	2022	2023	2024	2025	Trend
Full Encryption	47%	51%	54%	56%	Slow progress
Centralized Governance	33%	40%	45%	50%+	Gradual improvement
Third-Party Inventory	42%	47%	52%	57%	Gap vs. growth
Compliance Automation	<20%	<25%	<30%	<35%	Critical gap
PET Adoption	N/A	Minimal	<20%	19%–24%	Stagnant

Figure 12: Year-Over-Year Risk Readiness Scorecard.

While organizations have made steady progress on foundational controls—with full encryption climbing from 47% to 56% and centralized governance reaching 50%—the pace of improvement reveals a dangerous complacency. The most alarming insight is what's not improving: Compliance automation remains stuck below 35% after four years, creating an unsustainable burden as regulations multiply exponentially. Meanwhile, third-party inventory tracking (57%) fails to keep pace with actual ecosystem growth, meaning organizations are becoming less visible, not more. The stagnation of PET adoption at under 25% suggests that organizations have hit a complexity wall—they've implemented the easy solutions but lack the expertise or willingness to deploy advanced privacy technologies. This pattern— gradual progress on basics while advanced capabilities flatline—explains why 46% of organizations now face high to critical risk scores. In essence, the industry is bringing incremental improvements to an exponential fight, and the widening gap between capability and threat may soon become unbridgeable.
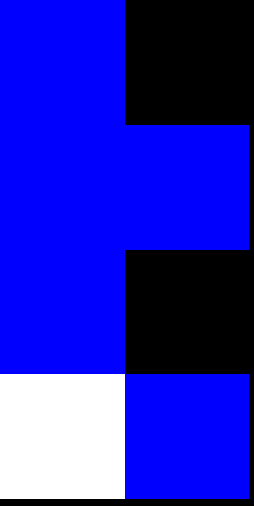
Interconnected Risk

Where AI, Partners, and Compliance Collide
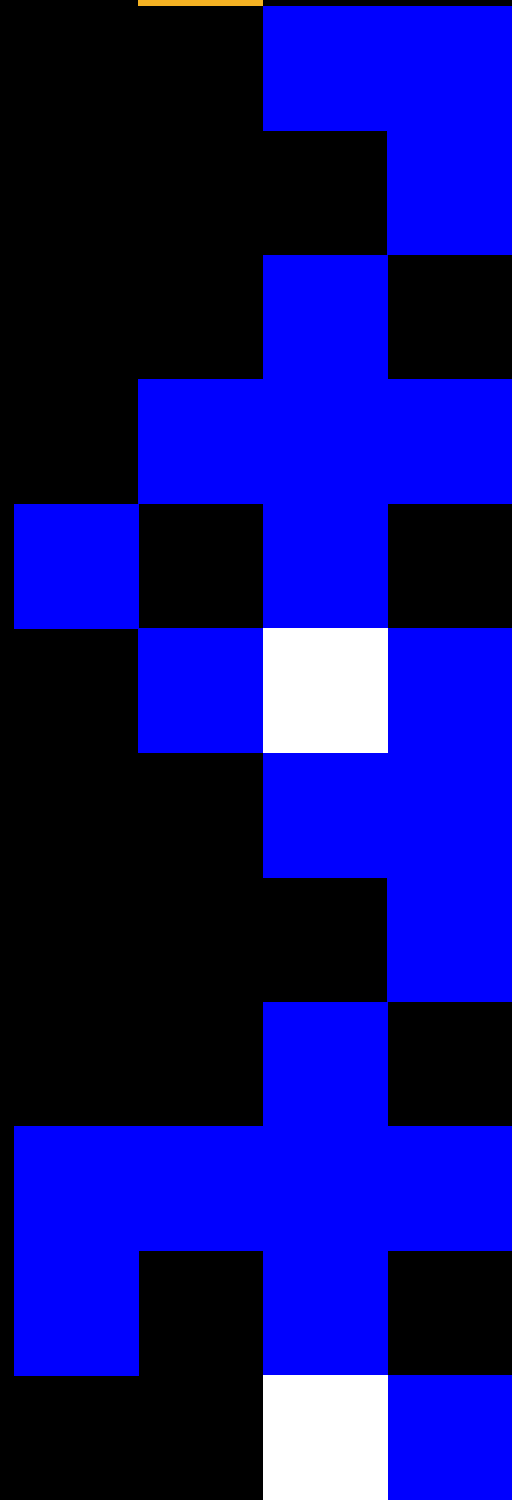
Interconnected Risk

Modern data security has evolved from managing discrete risks to navigating an interconnected web where threats amplify each other. Our 2025 data reveals how AI adoption, third-party relationships, and compliance requirements create compound risks that overwhelm traditional security approaches.

The 1,001–5,000 Third-Party "Danger Zone"

Our analysis identifies a critical inflection point in third-party risk: Organizations managing between 1,001 and 5,000 partners face the worst security outcomes across every metric.

The Danger Zone by the Numbers

Organizations with 1,001–5,000 third-party relationships show:

24% experience 7+ annual security incidents

46% report highest supply chain cyber risk increases

44% faced $3M–$5M litigation breach costs

24% take 31–90 days to detect breaches

Why This Range Is Deadly: Complex enough to overwhelm manual processes, but typically lacking the budget for enterprise-grade automated controls

Supply chain risk increase percentages shown across the four third-party volume tiers were calculated by segmenting all survey respondents based on how many external third parties they reported working with. Within each segment—**<500**, **501–1,000**, **1,001–5,000**, and **>5,000**—respondents were asked whether their organization experienced a measurable increase in cybersecurity or compliance risk originating from their supply chain in the past 12 months. For each group, the percentage shown reflects the share of respondents who answered "Yes" to that question. For example, among those with 1,001–5,000 third parties, **46%** reported a supply chain risk increase, while **30%** of those with fewer than 500 third parties did. The formula used in each case was:

$$\text{Risk Increase (\%)} = \frac{\text{Number of "Yes" responses}}{\text{Total respondents in that third-party volume tier}} \times 100$$

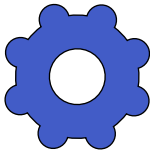**Note:** Values were then rounded to the nearest whole number to produce the final results.
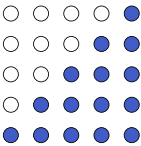
Third-Party Count	Annual Breach Rate	Detection Time	Supply Chain Risk Increase
<500	43% breach-free	43% detect <7 days	30%
501–1,000	36% face 4–6 hacks	Mixed performance	32%
1,001–5,000	**24% face 7+ hacks**	**42% take 31–90 days**	**46%**
>5,000	28% face 10+ hacks	31% take >90 days	43%

Figure 13: Comparing Risk Across Partner Volumes.

The key insight from this data (Figure 13) is that supply chain risk rises steadily with ecosystem size—but not exclusively. While large ecosystems (1,001+ partners) unsurprisingly show elevated risk—**46%** and **43%** respectively—the presence of a **30% risk increase even in organizations with fewer than 500 partners** suggests that complexity alone is not the sole driver. Instead, visibility, governance, and control over even a small number of partners can be just as critical. The **501–1,000 tier**, often overlooked as mid-scale, still reports a **32% risk increase**, emphasizing that organizations in this range may be particularly vulnerable to outgrowing their controls without yet maturing their oversight. The trend highlights that **supply chain risk is a visibility issue, not just a scale issue**.

Why Mid-Size Complexity Kills

The danger zone emerges from a fatal combination:

Ecosystem complexity
rivals large companies

Security budgets
remain mid-market sized

Manual processes
break under the volume

Visibility tools
lack sophistication

Compliance requirements
multiply with
partner count

Compliance Complexity in Multi-Dimensional Risk

When AI governance requirements layer onto existing regulatory obligations across thousands of third-party relationships, compliance becomes exponentially complex.

Keeping Pace With Regulatory Evolution

Top compliance challenges include:

42%–50% struggle with rapidly evolving regulations

33%–42% face inconsistent multi-jurisdictional requirements

32%–46% cannot manage third-party vendor compliance

The EU Data Act (September 2025) exemplifies new burdens:

- Only 22%–25% of smaller organizations are fully prepared
- Financial Services leads at 47% readiness; Education lags at 14%
- Mid-size organizations face disproportionate preparation challenges
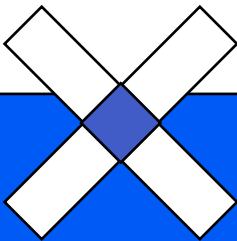
Multiplier Effect

Each new regulation
x number of jurisdictions
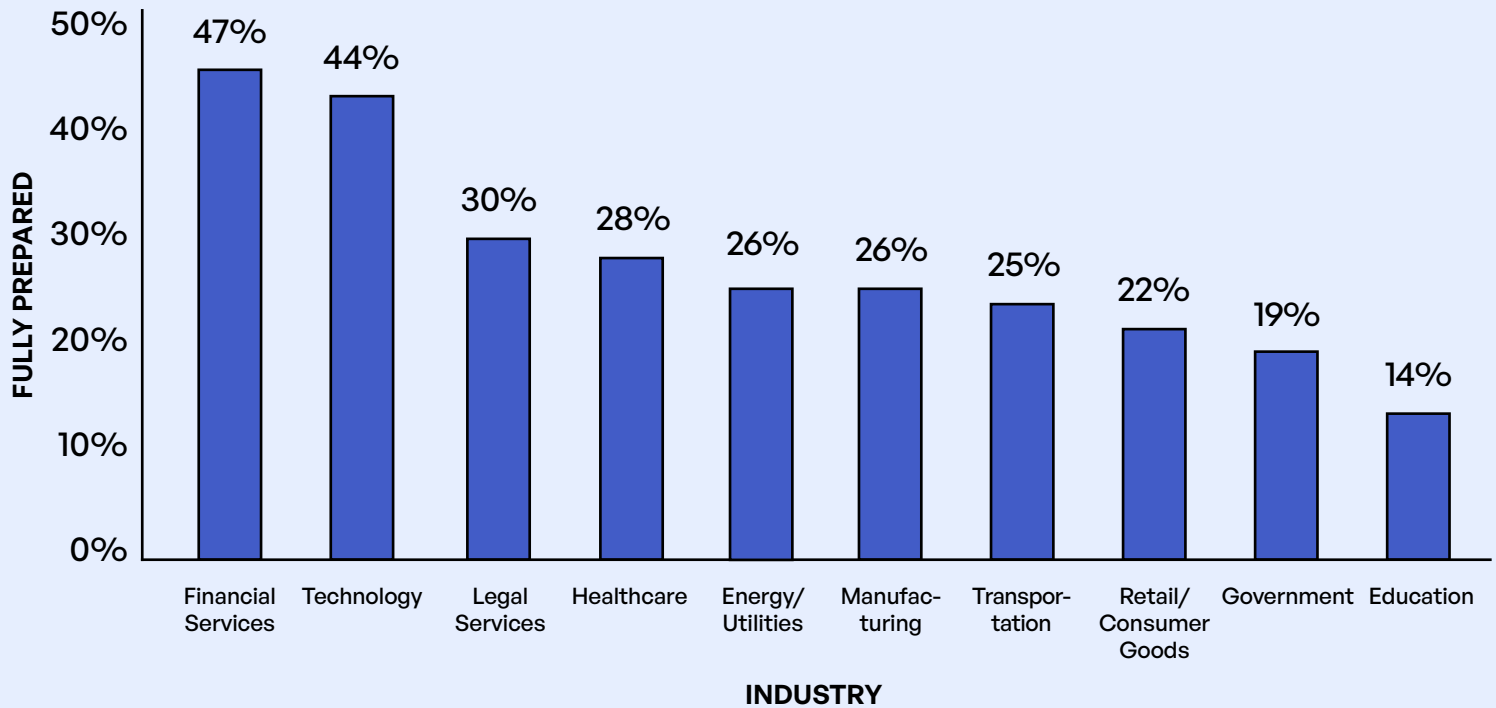x third-party count =
exponential complexity.

Figure 14: EU Readiness Across Industry Segments.

The bar chart in Figure 14 reveals significant variation in industry readiness for the EU Data Act, set to take effect in September 2025. Financial Services leads the pack at **47% fully prepared,** while Technology (44%) and Legal Services (30%) also show above-average readiness. In contrast, Government (19%) and Education (14%) lag substantially, highlighting the burden that regulatory compliance places on sectors with legacy infrastructure or public funding constraints. The data also reinforces the notion that private-sector industries, particularly those with strong financial or regulatory incentives, are investing more proactively in supply chain transparency and compliance infrastructure.

Figure 15 shows the distribution of company sizes among survey respondents, with **large enterprises (>10,000 employees) making up half of the sample.** Mid-size (1,001–5,000 employees) and small organizations (<500 employees) each account for **22%,** while micro-enterprises represent the remaining **6%.** This distribution adds context to the EU Data Act readiness scores: Smaller and mid-size organizations—which make up nearly half the sample—report notably lower preparation levels, often ranging between **14% and 30%.** The data suggests that **compliance mandates are disproportionately difficult for non-enterprise organizations,** which may lack the legal, technical, and financial resources required to meet new transparency obligations.
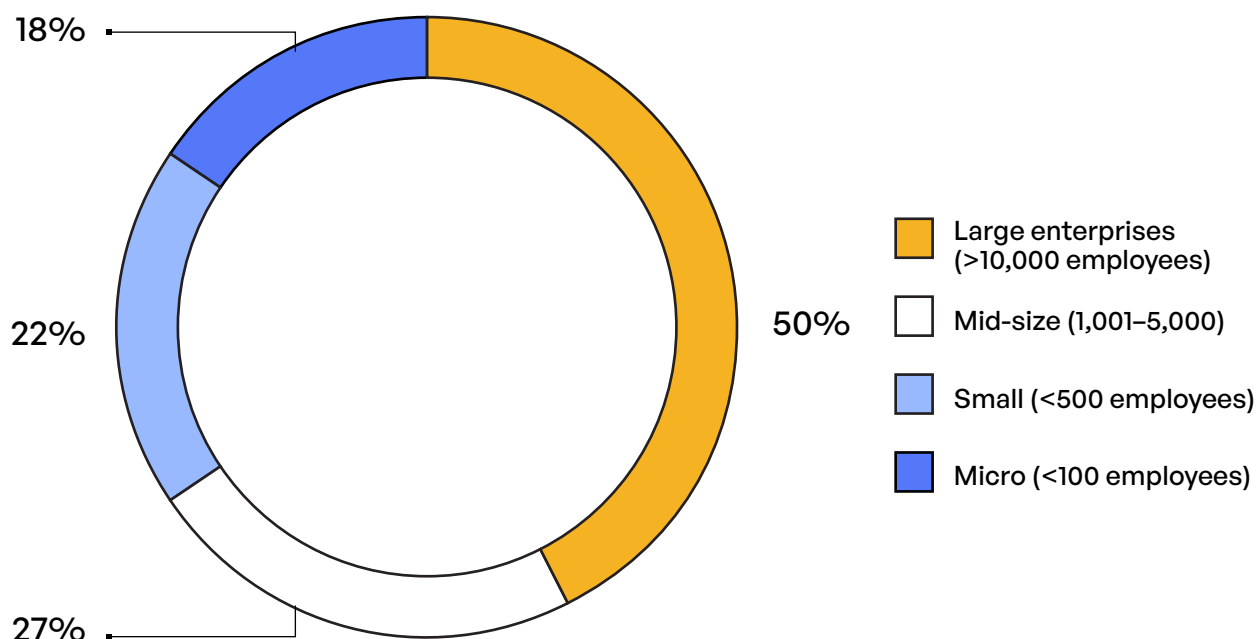
18%

22%

27%

50%

- Large enterprises (>10,000 employees)
- Mid-size (1,001–5,000)
- Small (<500 employees)
- Micro (<100 employees)

Figure 15: Company Size.

When Risks Compound, Strategy Breaks

Our data shows that cybersecurity risks don't just add up—they **compound.** As breach frequency increases, the impact grows exponentially. Organizations with **10+ annual breaches** are more likely to report **litigation costs exceeding $5 million** and **detection times exceeding 90 days.** These delays fuel cost escalation, moving organizations from isolated incidents to sustained challenge mode—often without the governance infrastructure needed to contain it.

48% of respondents who don't know how many breaches they've had also can't quantify their breach-related costs.

Experience Shifts Response From Proactive to Reactive

Organizations that haven't yet experienced a breach tend to invest in **preventative controls**—like encryption, compliance automation, and visibility infrastructure. But once breached, strategies shift toward **damage control:** legal contracts, insurance claims, and reputational defense. Motivation erodes from long-term improvement to short-term containment. This shift is especially pronounced in **mid-sized organizations,** which face rising breach rates but often lack the scale to absorb costs.
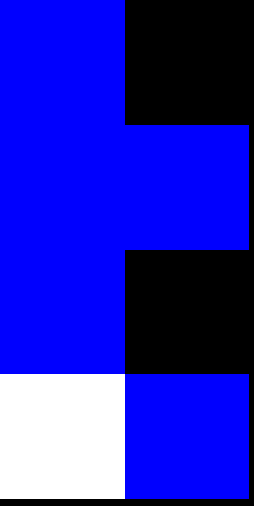
Governance Maturity = Strategy Confidence

Organizations without governance plans lean heavily on **contractual risk transfer,** with **25% relying on legal agreements** instead of technical safeguards—often a sign they lack operational readiness. In contrast, organizations with **comprehensive governance frameworks** show strong adoption of advanced technical strategies: **47% use hybrid infrastructure, 46% rely on distributed cloud models,** and many demonstrate confidence in managing complexity.

Notably, those planning to implement governance show **forward-thinking behavior—28% are building local partnerships** to support future systems. This early investment in ecosystem design signals a shift from reactive posture to proactive transformation.
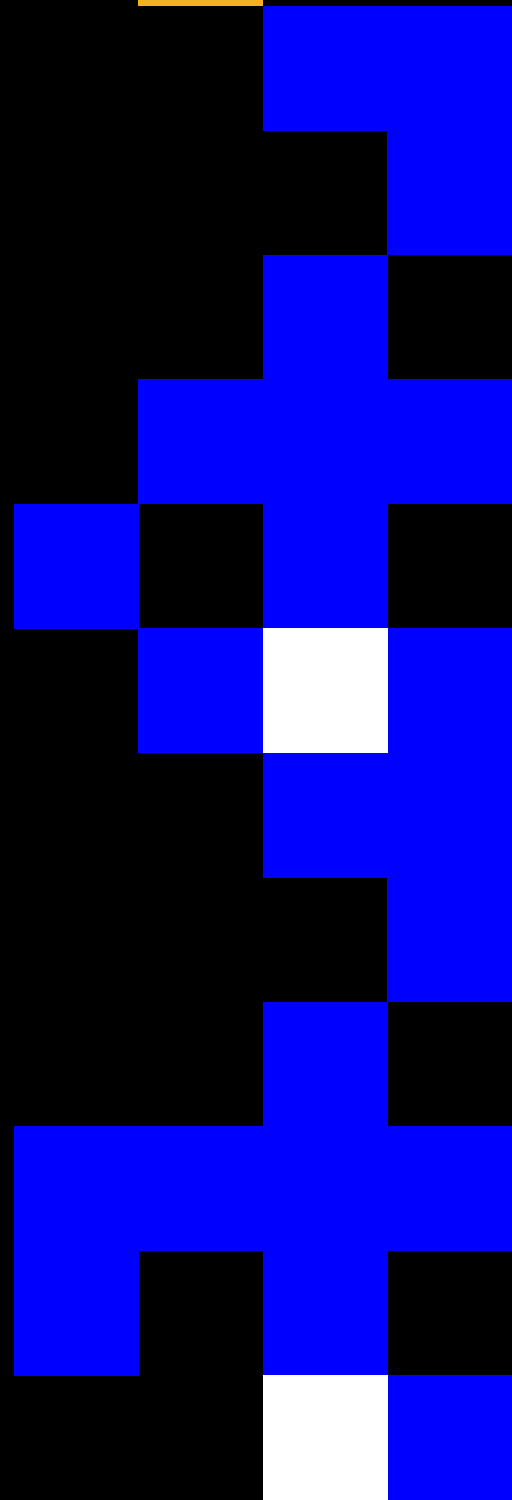
Strong governance doesn't just reduce breaches—it reshapes strategic decision-making across AI, cloud, and partner ecosystems.

AI Governance

Privacy-Innovation Tightrope

AI Governance

The AI revolution has transformed how organizations create, process, and share data. Yet our 2025 findings reveal a critical disconnect: While AI adoption races forward, governance and privacy controls lag dangerously behind.

Measuring AI's Private Data Footprint

AI Data Awareness Drives Security Action

Organizations that measure their AI-generated private content show dramatically different security behaviors than those operating blind:
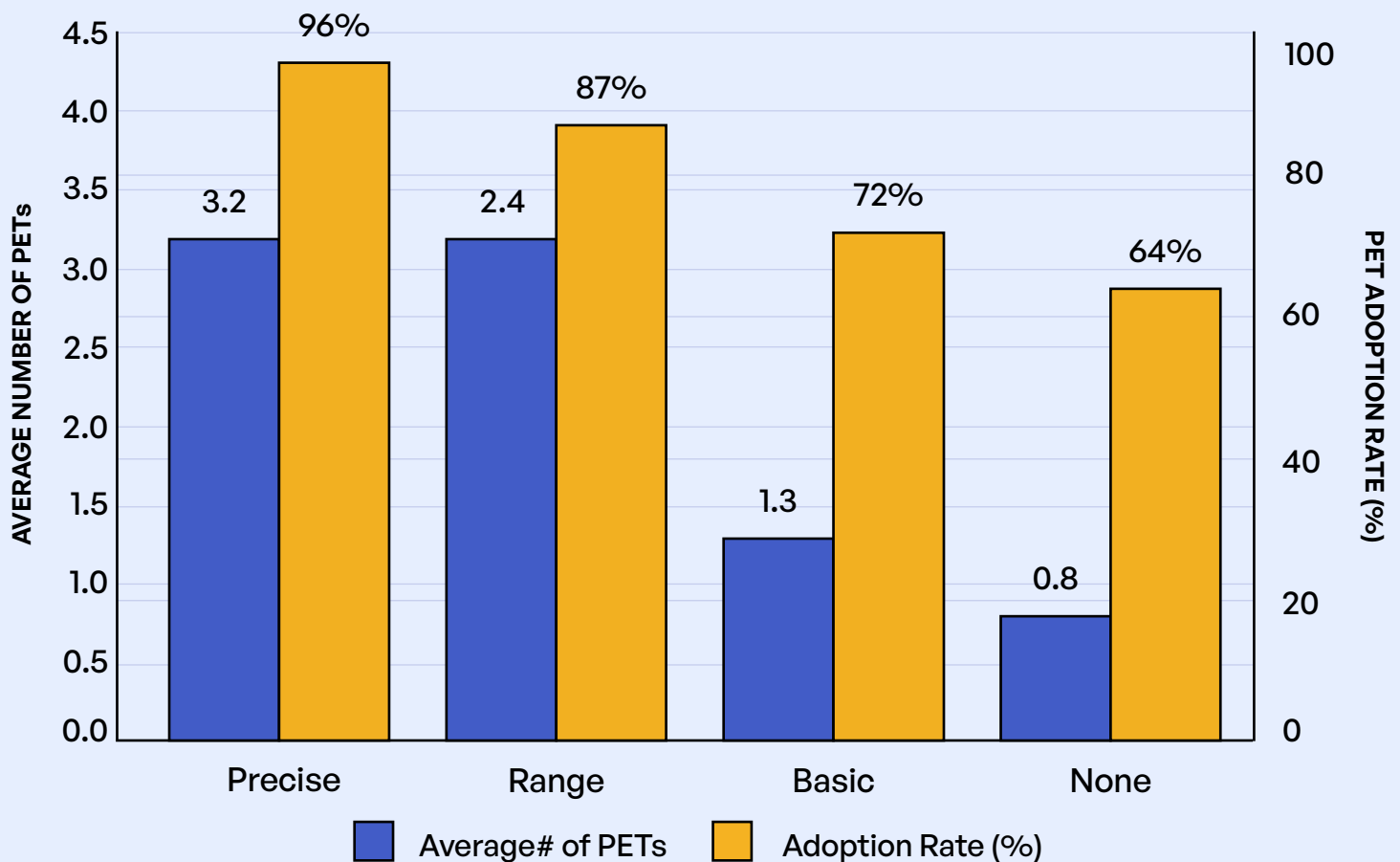

Figure 16: PET Adoption by AI Measurement Capability.

Critical Finding

Measurement alone drives significantly better security outcomes. Organizations aware of their AI data usage are 93%–96% likely to implement at least one PET, while 36% of those unaware implement zero privacy protections.
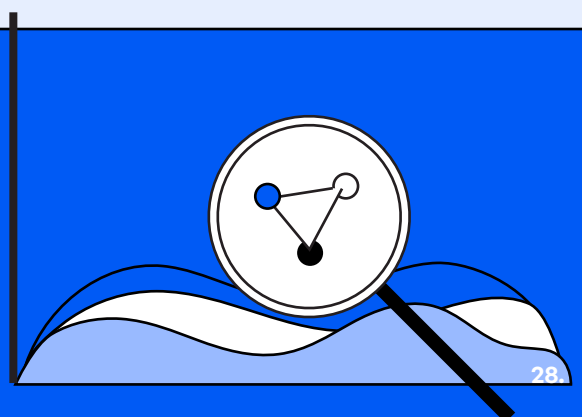
Figure 17 reveals widespread AI-generated private content across organizations, yet few have strong controls or measurement in place. While only **6%** report generating no AI content, nearly **60%** fall into moderate to heavy usage ranges, and **17%** don't even know their exposure. Despite this, **47%** of organizations unaware of their AI usage still rely on **subjective user judgment** to manage risk. Control mechanisms remain weak: Only **27%** enforce usage limits with training or audits, and just **17%** use technical controls like DLP. Meanwhile, **10%** have no AI policies at all, exposing significant governance gaps in the face of rising AI adoption.

AI Risk Via Private Data Ingestion Into Public AI LLMs
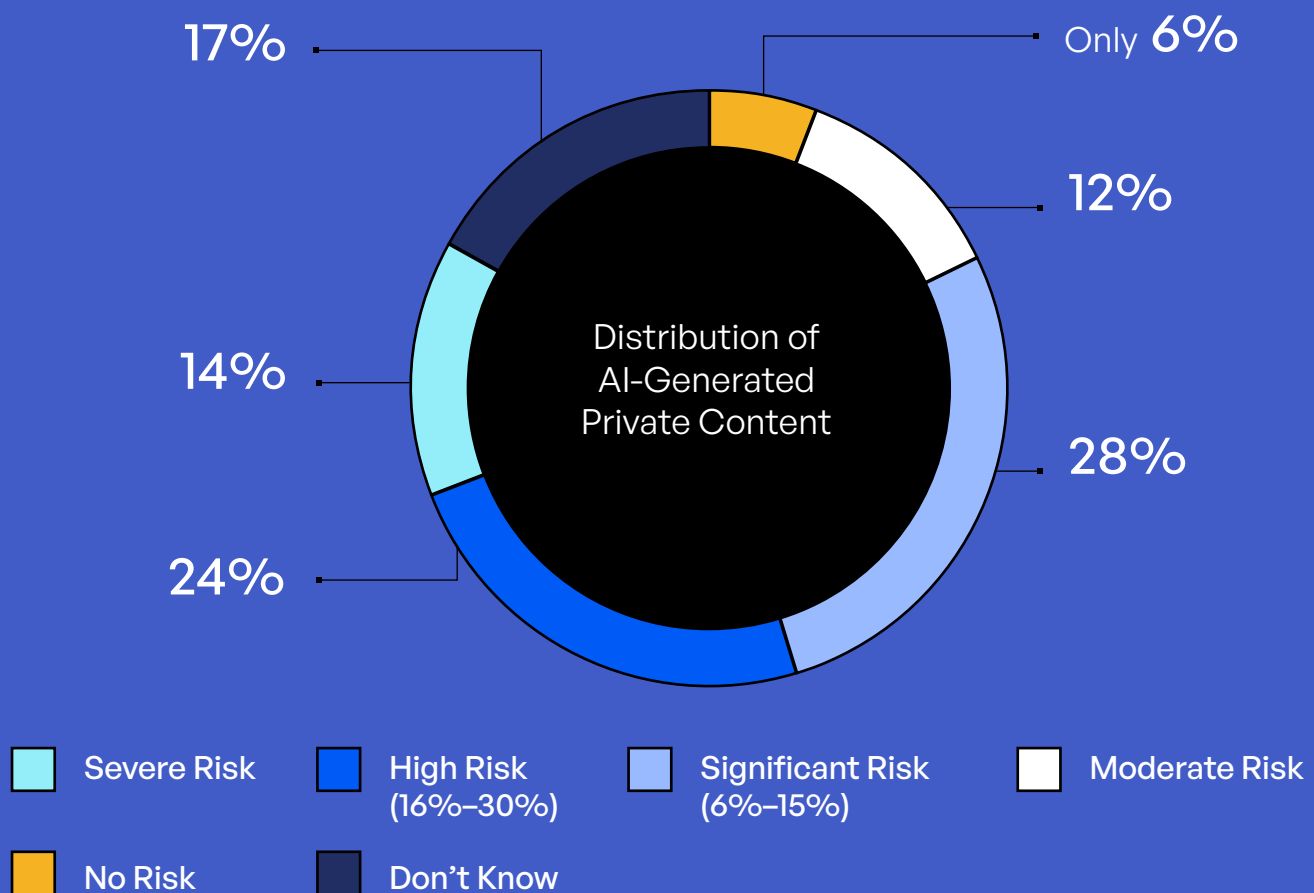
Figure 17: Percentage of AI-Ingested Data Being Loaded Into Public AI LLMs.

Figure 17 underscores a critical insight: **measurement drives protection.** Organizations that precisely track their AI-generated content are **93%–96% more likely to implement at least one PET.** In contrast, **36%** of those who don't measure implement no PETs whatsoever. Among those measuring in ranges, adoption of tools like **Zero-Trust Exchange (42%), Secure Multi-Party Computation (37%),** and **Federated Learning (25%)** is far stronger than among those in the dark. The takeaway is clear: awareness is the tipping point. Organizations that invest in **visibility and governance around AI usage** are substantially more capable of reducing risk, protecting private content, and aligning with compliance mandates. Measurement isn't just a best practice—it's the difference between security maturity and exposure.

When You Can't See, You Can't Govern

The relationship between organizational visibility and governance capability emerges as one of our most consistent findings. Organizations struggling with basic visibility metrics demonstrate dramatically weaker governance capabilities across every measure we examined. Only approximately 25% of organizations with significant visibility gaps have achieved mature AI governance, compared to over 70% among those with clear visibility into their operations.

This governance lag becomes particularly pronounced in the danger zone of 1,001–5,000 third-party relationships, where 42% lack adequate AI controls despite facing enterprise-level complexity. The temporal dimension compounds this challenge—10% of these organizations require 31–90 days to detect AI-related breaches, creating extended exposure windows where ungoverned AI usage can cause significant damage.

The correlation presents a clear causality chain: Poor visibility creates measurement gaps, which prevent effective governance implementation, ultimately leaving organizations exposed to both regulatory penalties and security breaches. This cascade effect transforms what might begin as a simple tracking deficiency into a comprehensive governance failure.
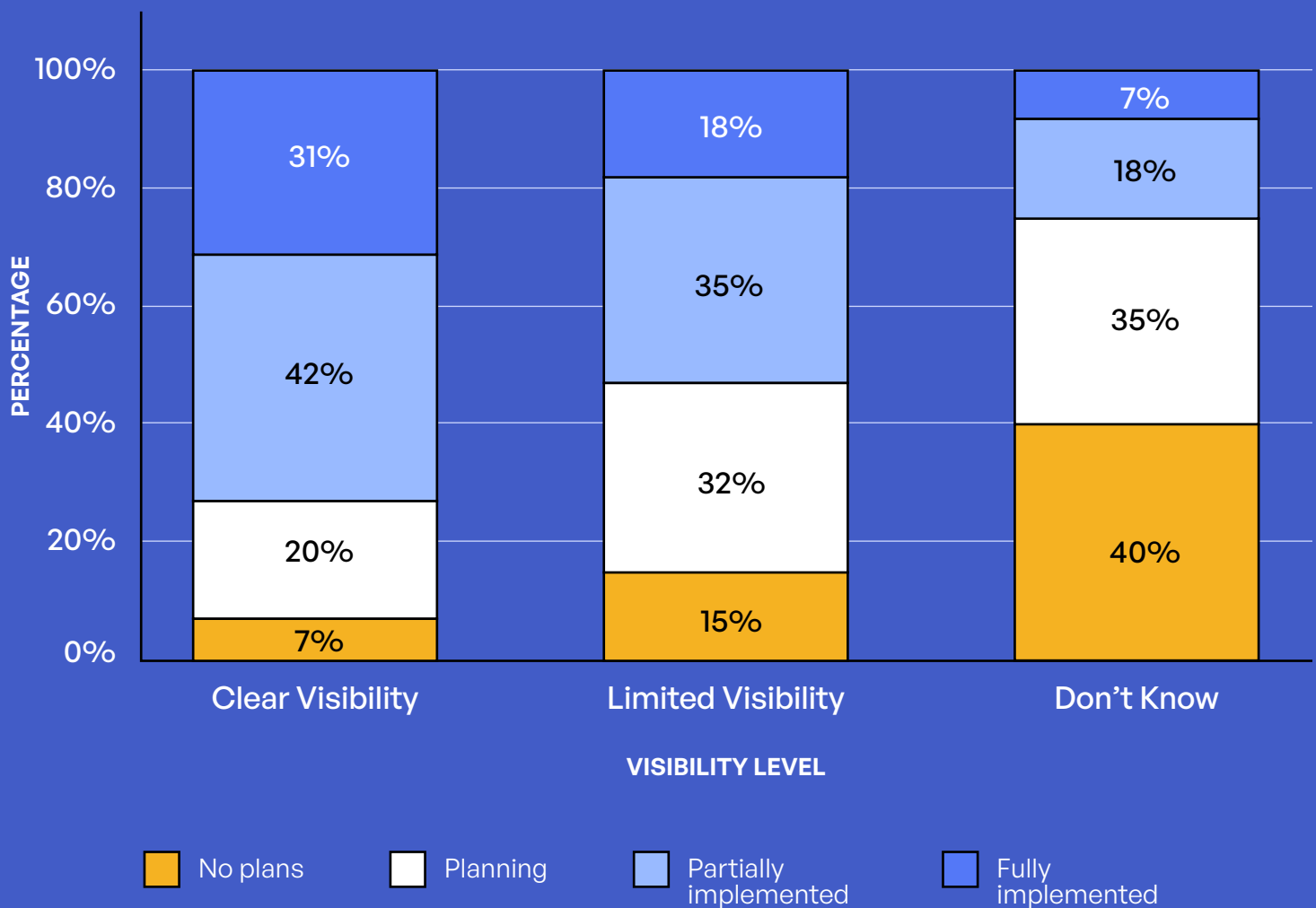
Figure 18: AI Governance Maturity by Organizational Visibility.

The Measurement Imperative: You Can't Protect What You Don't Measure

The foundation of effective AI governance rests on a simple principle that our data validates repeatedly: measurement drives protection. Nearly half of surveyed organizations—48%—cannot estimate how much data enters their AI systems, creating a fundamental governance gap that cascades through every aspect of their security posture.

Organizations that have invested in measuring AI data ingestion demonstrate dramatically superior protection profiles. Among those with measurement capabilities, 96% have implemented at least one privacy-enhancing technology, with 42% utilizing Zero-Trust Exchange architectures and 37% deploying Secure Multi-Party Computation. These aren't merely compliance checkboxes but sophisticated technical controls that provide real protection against AI-specific threats.

The contrast with non-measuring organizations proves stark. Among those lacking measurement capabilities, 36% have implemented zero privacy technologies—not even basic encryption or access controls specifically for AI systems. This measurement gap extends beyond technical controls, with 64% lacking any technical AI governance mechanisms and 42% unable to determine their breach frequency. The message from our data is unequivocal: Measurement isn't an optional first step in AI governance—it's the foundation upon which all other protections must be built.
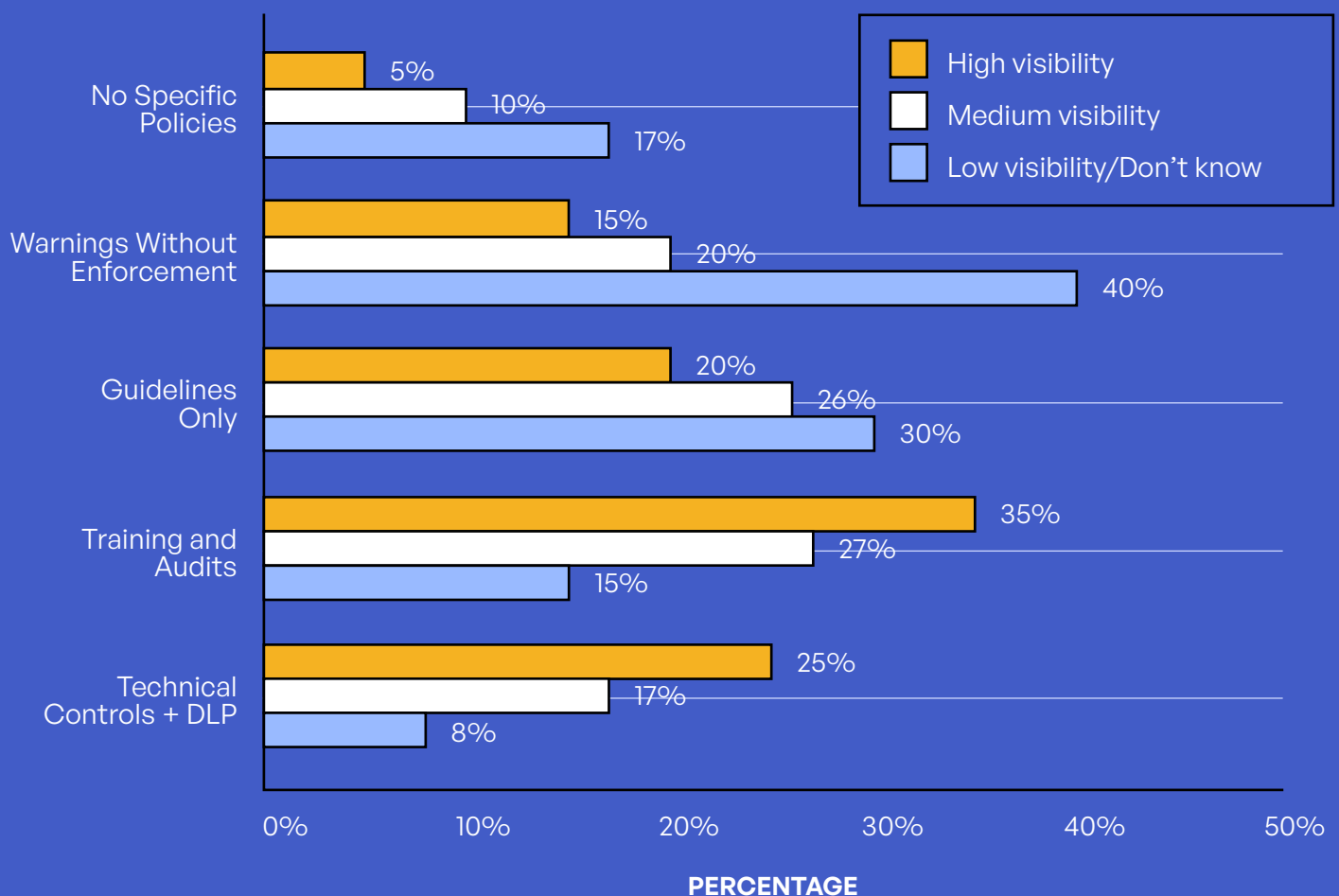
Public AI LLM Data Risk Evaluated

Figure 19: AI Control Mechanisms by Visibility Level.

Control Paradox: Weak Enforcement Where It's Needed Most

A counterintuitive pattern emerges when examining control mechanisms across organizations with varying visibility levels. Those with the greatest need for strong controls—organizations with limited visibility into their AI usage—paradoxically implement the weakest enforcement mechanisms.

Organizations with limited visibility, where fewer than 25% can effectively track AI usage, demonstrate a concerning reliance on passive controls. Forty percent depend primarily on warning messages without technical enforcement, while 47% rely on subjective user judgment as their primary control mechanism. Technical controls like data loss prevention or access restrictions appear in fewer than 25% of these organizations.

The contrast with high-visibility organizations proves stark. Among those with tracking capabilities exceeding 75%, we see 17% implementing comprehensive technical controls and 27% enforcing usage limits through regular audits. Perhaps most tellingly, only 10% of high-visibility organizations report having no AI policies at all, compared to nearly double that rate among their low-visibility counterparts.

This inverse relationship between need and implementation creates a vicious cycle. Organizations least capable of detecting AI misuse implement the weakest preventive measures, while those with strong detection capabilities layer multiple protective controls. The result amplifies existing vulnerabilities rather than addressing them.

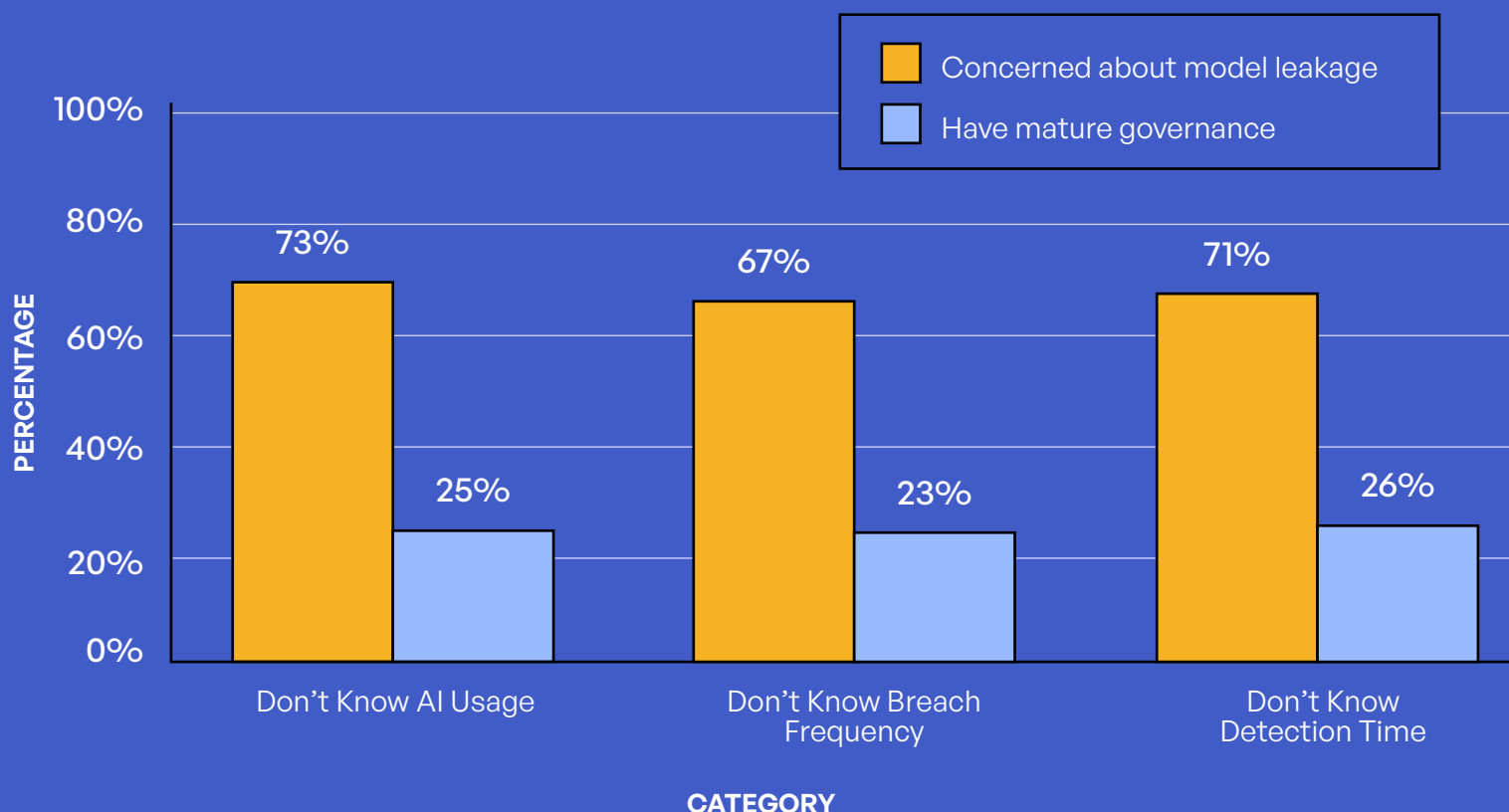## Cross-Analysis: Awareness Drives Action

Figure 20: Model Leakage Concern vs. Governance Implementation.

Fear-Action Gap: When Awareness Doesn't Drive Implementation

Our analysis reveals a troubling paradox in AI governance that challenges conventional wisdom about risk management. Organizations demonstrating the deepest concerns about AI security risks often exhibit the weakest protective measures, creating a dangerous disconnect between awareness and action.

Among organizations that responded "don't know" to fundamental visibility questions, between 67% and 73% identify model leakage as their primary AI security concern. This level of awareness should theoretically drive robust governance implementation. Yet our data reveals that only 25% of these same organizations have implemented mature governance frameworks. The remaining three-quarters operate in a state of acknowledged vulnerability, where fear of AI risks coexists with inadequate protection.

This disconnect manifests most clearly in control mechanisms. A striking 40% of visibility-challenged organizations rely solely on warning messages without any enforcement mechanisms—essentially hoping that awareness alone will prevent misuse. The gap between recognizing threats like data exfiltration through AI models, unauthorized sensitive data processing, and intellectual property leakage, and actually implementing controls to prevent them, suggests that awareness without capability creates a form of organizational paralysis.

AI Visibility Risk Factor

Only 40% of visibility-challenged organizations rely solely on warning messages and have no enforcement mechanisms in place at all.
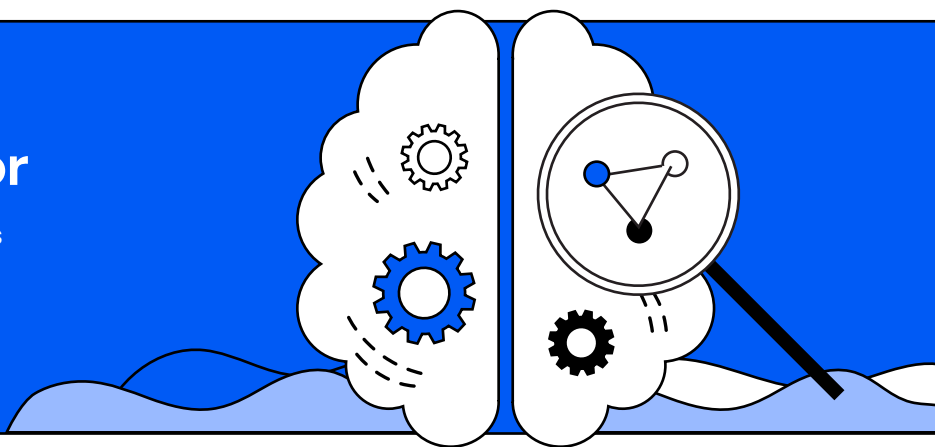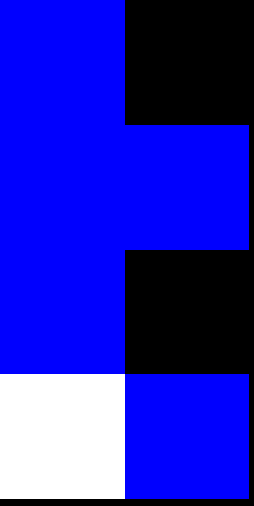
Privacy-Enhancing Technologies

Maturity Divide

Privacy-Enhancing Technologies

PETs represent the frontier of data protection—sophisticated tools that enable organizations to use and share data while maintaining privacy. Yet our findings reveal a troubling paradox: Despite proven effectiveness and increasing availability, adoption remains stubbornly low.

PET Adoption Landscape

The PET adoption landscape reveals a striking maturity gap, with Data Minimization leading at 43% adoption while more advanc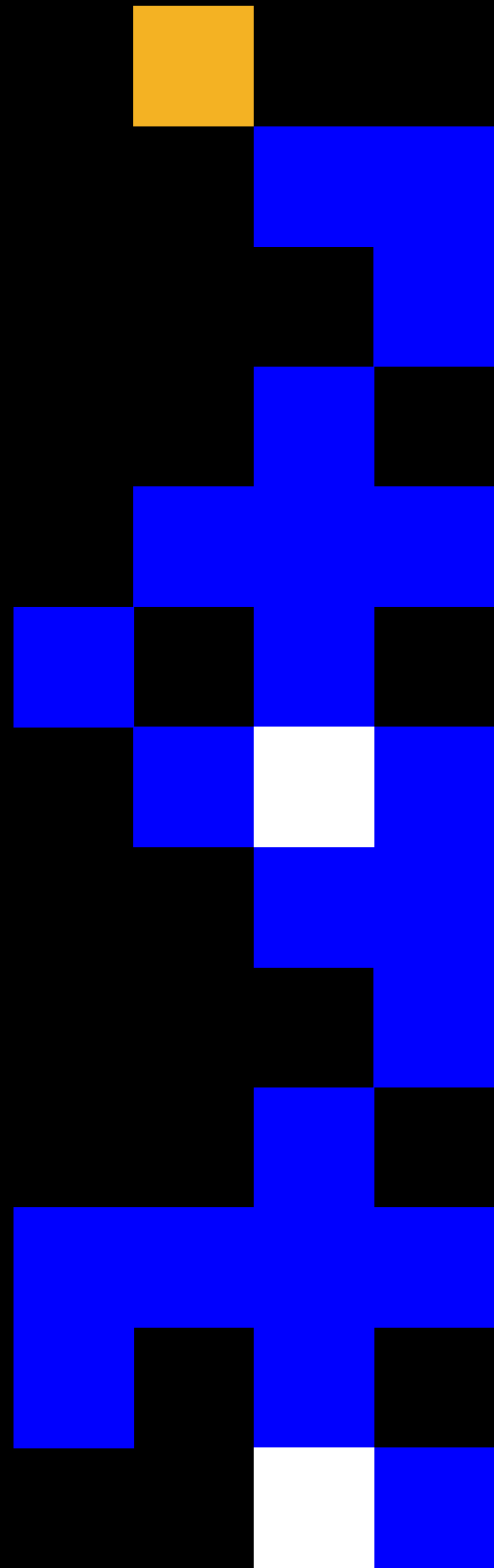ed techniques like Federated Learning and Differential Privacy lag at 17% and 20%, respectively. This adoption hierarchy reflects both technical complexity and organizational readiness—simpler, policy-based approaches like Data Minimization require minimal infrastructure changes, while Homomorphic Encryption's sophisticated mathematics and computational overhead create significant barriers.

Most concerning is that 9% of organizations report using no PETs at all, with this figure rising to 24% among organizations that don't even know their third-party ecosystem size, suggesting a dangerous disconnect between growing privacy regulations and actual implementation. Zero-Trust Exchange remains a concern/gap with less than one-third of respondents indicating they have implemented it. As privacy threats escalate and regulations tighten globally, organizations face a critical inflection point: Those investing now in building PET capabilities across the spectrum—from basic data minimization to advanced cryptographic techniques—will gain competitive advantages through enhanced customer trust and regulatory compliance, while laggards risk both reputational damage and substantial fines in an increasingly privacy-conscious marketplace.

PET Type	Adoption Rate (%)	Notes
Data Minimization	43%	Most widely adopted PET (across roles)
Secure Multi-Party Computation	35%	Moderate adoption, often in financial and healthcare sectors
Zero-Trust Exchange	31%	Highly dependent on organizational maturity
Confidential Computing	26%	Requires hardware support; adoption still growing
Differential Privacy	20%	Common in anonymized data sets
Homomorphic Encryption	19%	Technically complex, low current adoption
Federated Learning	17%	Popular in AI/ML model training use cases
None of the Above	**9%**	**Significant number of organizations still not using any PETs**

Figure 21: PET Adoption Rates by Technology.

Third-Party Count	Data Minimization	Secure MPC	Confidential Computing	Zero-Trust Exchange	Homomorphic Encryption	No PET
<500	48%	37%	28%	37%	15%	9%
501–1,000	43%	40%	20%	31%	13%	9%
1,001–5,000	35%	32%	32%	32%	14%	4%
>5,000	45%	33%	29%	27%	15%	6%
Don't Know	45%	21%	14%	14%	10%	24%

Figure 22: PET Adoption Rates by Third-Party Volume.

The data shows significant variation in **PET** adoption across organizations of varying third-party volumes, with adoption rates spanning from **9% to 48%** depending on the technology and organization size. Smaller organizations (fewer than 500 partners) demonstrate the highest adoption rates for several key technologies, leading in Data Minimization (48%), Secure Multi-Party Computation (37%), and Zero-Trust Exchange (37%). Homomorphic Encryption adoption remains quite low as the technology must mature further. However, the most telling insight comes from the **"Don't Know" group**, where **24% report using no PETs**—nearly three times higher than any other segment—and adoption of advanced technologies like Zero-Trust Exchange (14%) and Confidential Computing (14%) is dramatically lower. This reinforces the broader trend that **lack of visibility directly correlates with reduced security investment:** Organizations that don't know their third-party count are least likely to protect sensitive content with proven privacy tools, with their "no PET" rate being 4-6 times higher than organizations with clear visibility of their ecosystems.

Correlation: PET Adoption and Security Outcomes

PET Dividend: Proven Outcomes

As demonstrated throughout our analysis, organizations implementing multiple PETs achieve dramatically better outcomes. Those deploying 3+ technologies show 67% faster breach detection and 81% lower litigation costs compared to zero-PET organizations. The most effective combinations include Data Minimization, Secure MPC, and Zero-Trust architectures working in concert.
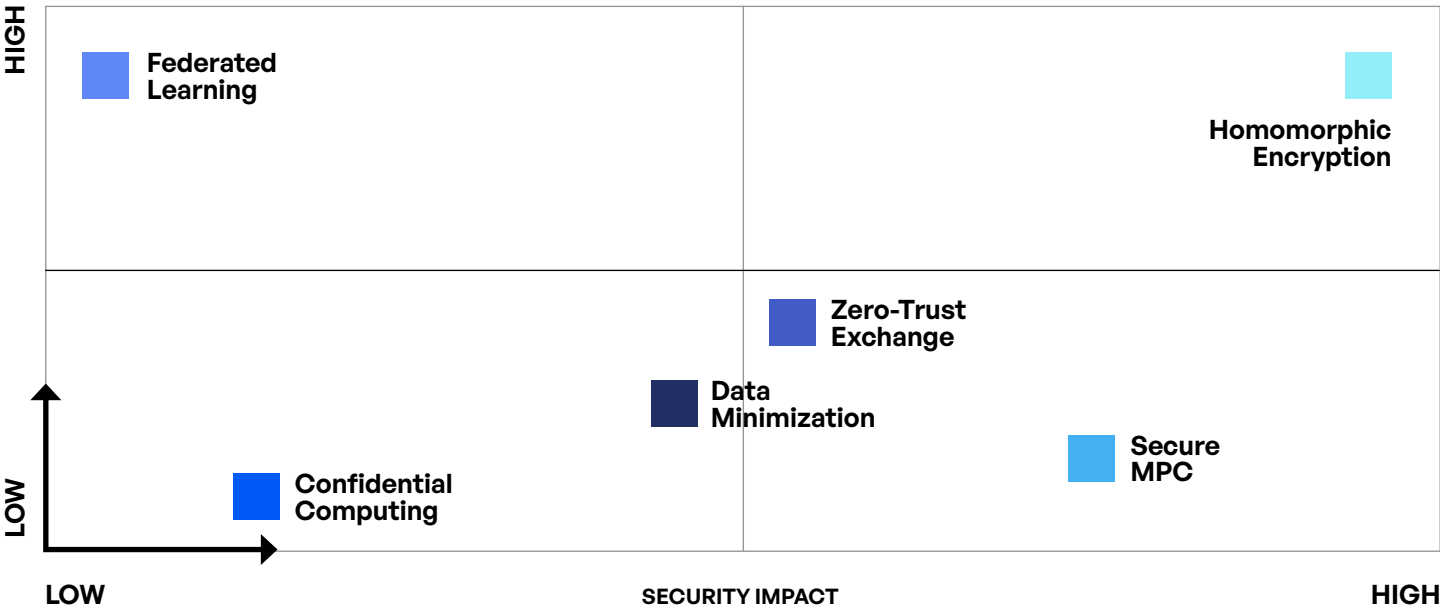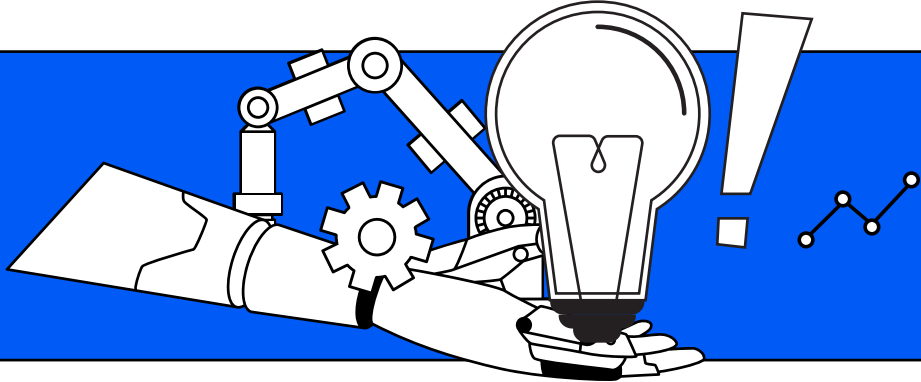

Figure 23: PET Implementation Difficulty vs. Impact.

Technology	Implementation Complexity	Security Benefit	Time to Value
Confidential Computing	Low	Low	30–60 Days
Secure MPC	Low	High	60–90 Days
Zero-Trust Exchange	Medium	Medium	60–90 Days
Data Minimization	Medium	Medium	60–90 Days
Federated Learning	High	Low	180–365 Days
Homomorphic Encryption	High	High	180–365 Days
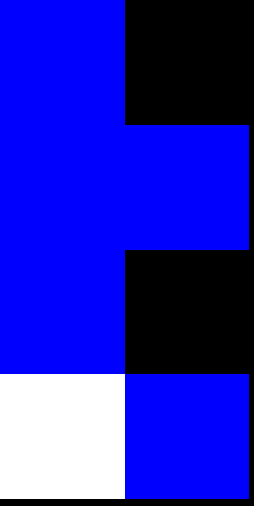
Figure 24: PET Complexity-Benefit Assessment.

Recommendation

Start with quick wins, build toward comprehensive protection.

The PET Complexity-Benefit matrix illustrates how **security benefit and implementation complexity** align with **time to value.** Quick-win options such as **Confidential Computing** (30–60 days) and **Data Minimization** (60–90 days) deliver relatively fast returns with low-to-medium complexity, making them strong entry points for organizations beginning their PET adoption. **Zero-Trust Exchange** and **Secure MPC**, both requiring 60–90 days, provide higher security benefits but with moderate complexity, fitting well into a medium-term roadmap. At the other end of the spectrum, **Federated Learning** and **Homomorphic Encryption** demand the most time (180–365 days) and technical effort, yet yield substantial security impact, particularly in regulated or high-risk environments. The strategic takeaway is to start with low-complexity PETs to build momentum and demonstrate early wins, while planning for the gradual integration of high-impact, resource-intensive solutions as part of a long-term security and compliance strategy.

Compliance Imperative

Navigating Global Complexity
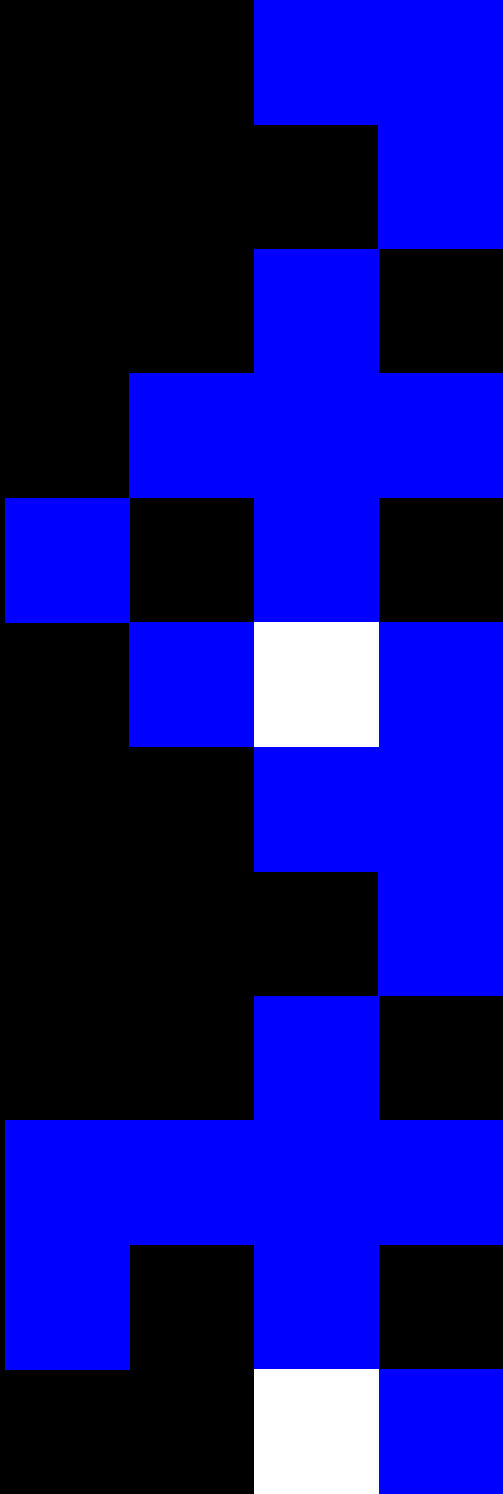
Compliance Imperative

The regulatory landscape has transformed from a manageable set of requirements into a labyrinth of overlapping, often conflicting mandates that span jurisdictions, industries, and technologies.

Multi-Jurisdictional Challenge Intensifies

Industry	Primary Challenge	Percentage	Secondary Challenge	Percentage
Legal	Rapidly evolving requirements	71%	Inconsistent regulations	39%
Government	Third-party vendor compliance	58%	Limited resources	33%
Financial Services	Balancing compliance vs. business	39%	Multi-jurisdictional complexity	31%
Technology	Inconsistent requirements	56%	Pace of change	47%
Healthcare	Employee training gaps	72%	Data inventory maintenance	47%
Manufacturing	Resource limitations	74%	Third-party compliance	59%
Education	Limited budgets	67%	Jurisdictional complexity	44%
Pharmaceuticals/ Life Sciences	Compliance with global data privacy laws	63%	Complex third-party data sharing	42%

Figure 25: Top Compliance Challenges by Industry.

AI Compliance Blind Spot

Despite the rapid pace of regulatory development—59 new U.S. AI laws were introduced in 2024 alone according to Stanford research—only 12% of organizations consider compliance a top AI-related concern. This mismatch creates blind spots for GDPR, CCPA, HIPAA, and SOX compliance, particularly when organizations cannot log or track AI data usage.[2] Furthermore, only 17% of organizations have implemented AI technical governance frameworks, compounding the compliance challenge.

EU Data Act Readiness: The September 2025 Countdown

The EU Data Act readiness assessment reveals a striking paradox in regulatory preparedness across industries, with inconsistent compliance frameworks creating a patchwork of readiness levels as the September 2025 deadline approaches. Despite the Legal sector's inherent focus on regulatory matters, it ironically shows only 12% readiness—the lowest among all industries—highlighting how even regulatory experts struggle with the Act's complexity.

This regulatory fragmentation manifests differently across sectors: While Financial Services leads at 47% readiness due to mature compliance infrastructure, the Technology sector's 44% readiness is hampered by cross-border operational complexities that expose the challenges of harmonizing regulations across multiple jurisdictions. The Government sector's mere 19% readiness, attributed to "fragmented oversight and slow adaptation," underscores a fundamental challenge—when the very institutions responsible for implementing regulations lack unified approaches, it creates cascading uncertainties for all other sectors attempting to comply. This regulatory inconsistency not only complicates compliance efforts but also creates competitive imbalances, where sectors with historically robust compliance frameworks gain advantages while others, particularly Education at just 14% readiness, risk being left behind in the data-driven economy.

Industry	Fully Ready (%)	Notes
Financial Services	47%	Leads all sectors; driven by mature compliance and data governance
Technology	38%	High agility, but complexity from cross-border operations remains
Manufacturing	35%	Improving, but resource constraints persist
Healthcare	30%	Struggles with legacy systems and patient data sensitivity
Government	19%	Fragmented oversight and slow adaptation
Education	14%	Severely underfunded, with minimal preparedness
Legal	12%	Ironically low readiness despite regulatory focus (23% currently have NO PLANS)

Figure 26: EU Data Act Preparedness Across Industry Sectors.

Global Regulatory Impact Analysis

Region	Regulation	Adoption Rate (%)	Focus/Impact
North America	GDPR	27%	Cross-border transfers; EU vendor pressure
	CCPA/CPRA	40%	High enforcement risk; consent and opt outs
	HIPAA	63%	PHI workflows drive logging and BAAs
	CMMC 2.0	45%	Contract gate for DoD revenue
	NIS 2	4%	Limited scope; EU ops only
	DORA	10%	EU banking links add ICT risk duties
	UK DPA	16%	UK subsidiaries require UK-specific handling
Europe/ UK	GDPR	90%	Table stakes for European organizations
	CCPA/CPRA	12%	Applicable for firms conducting business in California
	HIPAA	14%	Only a small portion of European firms in the U.S.
	CMMC 2.0	6%	Few European firms have U.S. DoD business
	NIS 2	54%	Regulation is a requirement and growing focus area
	DORA	49%	Like NIS 2, DORA is a growing requirement
	UK DPA	41%	Large number of European firms conduct business in the UK
Middle East	GDPR	51%	Substantial number of Middle East firms conduct operations in Europe
	CCPA/CPRA	22%	Applicable for firms conducting business in California
	HIPAA	22%	Only a small portion of Middle East firms in the U.S.
	CMMC 2.0	16%	Small number of Middle East firms conduct business with the U.S. DoD
	NIS 2	24%	Compliance required of firms conducting business in the Middle East
	DORA	27%	Compliance required of firms conducting business in the Middle East
	UK DPA	44%	Substantial number of Middle East firms conduct operations in the UK

Figure 27: Data Regulatory Adoption Rates Across Regions.

North America: Compliance is U.S.-centered. HIPAA (63%) shapes PHI workflows and BAAs; CMMC 2.0 (45%) acts as a contract gate for defense work; CCPA/CPRA (40%) drives consent, DSAR, and data-sharing governance. EU/UK rules register at the margins—GDPR 27%, UK DPA 16%, DORA 10%, NIS 2 4%—mostly where teams process EU data or run EU operations. Focus on auditable PHI processes, CMMC readiness where relevant, and steady CCPA/CPRA hygiene.

Europe/UK: The agenda is EU-led. GDPR (90%) remains the anchor, with NIS 2 (54%) and DORA (49%) pushing practical change: supplier due diligence, 24/72-hour reporting, resilience testing, and concentration-risk checks. UK DPA (41%) adds local specificity. U.S. sector rules are secondary—HIPAA 14%, CCPA/CPRA 12%, CMMC 2.0 6%—typically when selling into U.S. markets. Prioritize vendor governance and incident readiness; address U.S. requirements via targeted contracts and transfer controls.

Middle East: Impact splits between EU/UK regimes and U.S. sector rules via cross-border work: GDPR (51%), UK DPA (44%), DORA (27%), NIS 2 (24%), with CCPA/CPRA (22%), HIPAA (22%), and CMMC 2.0 (16%) appearing where organizations serve those markets. Practical move: pair transfer mechanisms (SCCs/UK IDTA) with supplier assurance, and scope U.S. obligations to specific services or customers.

Compliance Investment and Returns

This data (Figures 28 and 29) reveals a striking pattern in how organizations allocate resources to annual compliance reporting, with the majority (25%-32%) dedicating between 1,001-1,500 hours yearly—equivalent to roughly half a full-time employee's annual work. The distribution tells a compelling story about organizational complexity: Small businesses manage with under 500 hours (7%), while technology companies often exceed 2,000 hours (14%-20%), reflecting their intricate regulatory landscapes. Perhaps most concerning is that 20%-26% of organizations fall into the "Don't Know" category, suggesting a significant visibility challenge where companies lack fundamental awareness of their compliance burden—a blind spot that could lead to either wasteful overinvestment or dangerous underinvestment in regulatory adherence. This wide variance, from streamlined operations requiring minimal oversight to complex entities demanding extensive resources, underscores why a one-size-fits-all approach to compliance management rarely succeeds.

Annual Hours	% of Organizations	Dominant Sectors
<500	7%	Small businesses
500–1,000	13%	Streamlined operations
1,001–1,500	**25%–32%**	**Most common range**
1,501–2,000	19%	Complex operations
>2,000	14%–20%	Technology (20%)
Don't Know	20%–26%	Visibility challenge

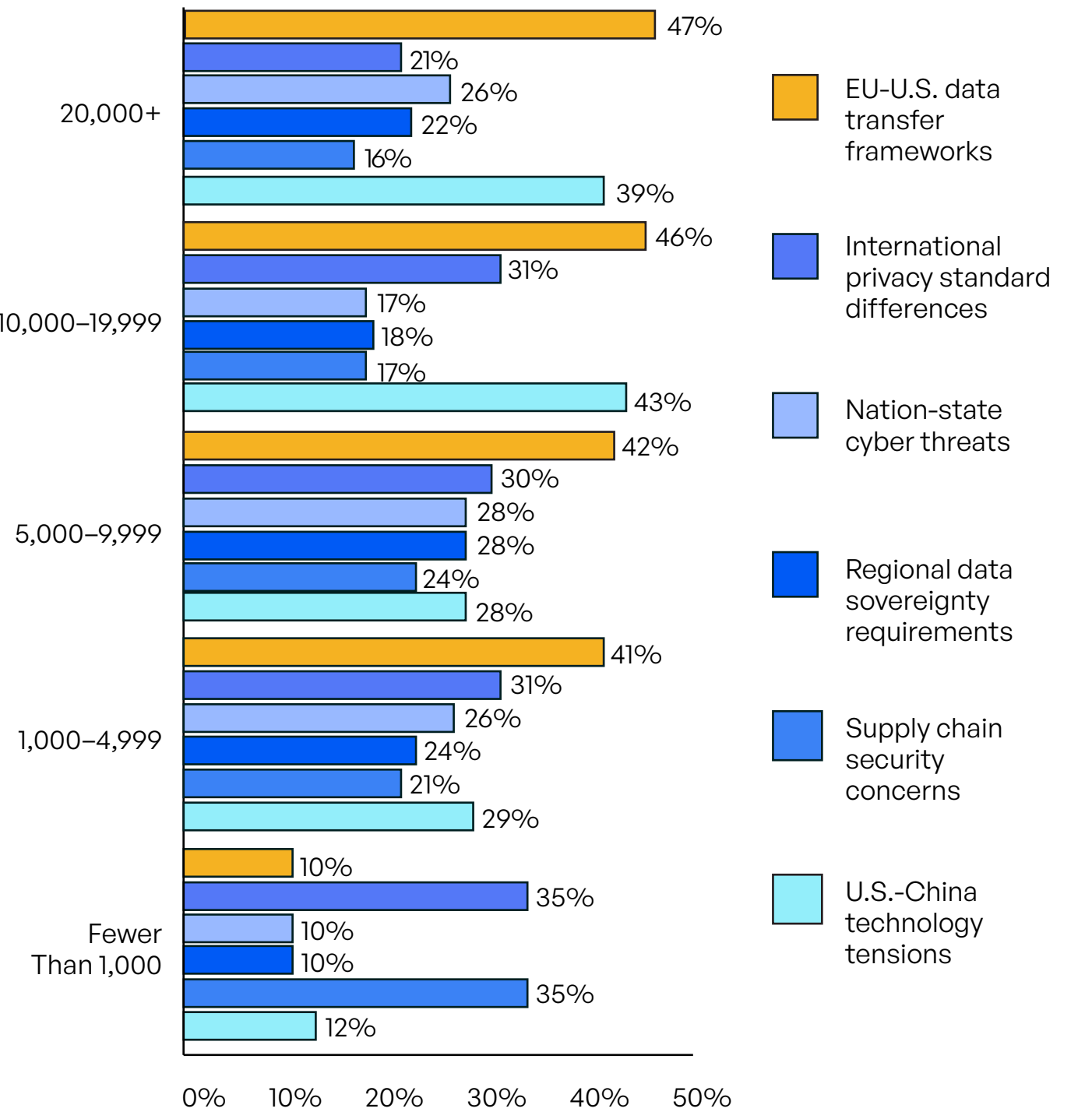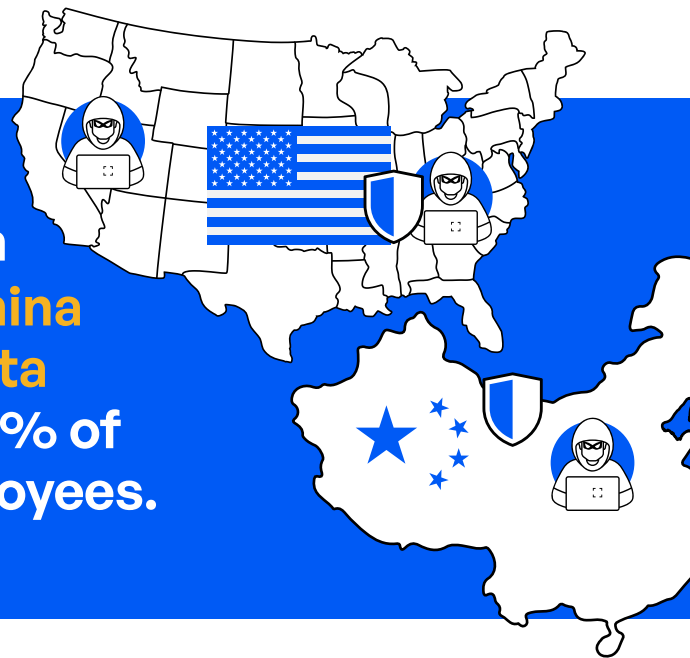Figure 28: Time Spent Tracking and Reporting on Compliance.

Figure 29: Business Outcomes From Data Privacy and Governance Measures by Organization Size.

Top Data Privacy Concerns

Nearly 4 in 10 organizations with 20,000+ employees cite U.S.-China technology tensions as a top data privacy concern compared to 12% of those with fewer than 500 employees.

The data reveals striking patterns in how organizations of different sizes experience business outcomes from their data privacy and governance initiatives. Most notably, larger enterprises demonstrate significantly greater concern with international regulatory frameworks, particularly EU-U.S. data transfer mechanisms, which show a dramatic increase from just 10% among small organizations (fewer than 1,000 employees) to 47% for large enterprises (20,000+ employees). This pattern extends to geopolitical considerations as well, with U.S.-China technology tensions affecting 39% of the largest organizations compared to only 12% of the smallest ones. These findings suggest that as organizations grow and expand their global footprint, they become increasingly entangled in complex international data governance challenges that require sophisticated compliance strategies and cross-border data management capabilities.

Conversely, smaller organizations face a different set of priorities that diminish with scale. International privacy standard differences affect 35% of small organizations but only 21% of large enterprises, while supply chain security concerns impact 25% of small businesses versus 16% of major corporations. This inverse relationship suggests that smaller organizations struggle more with the fundamental challenge of understanding and implementing diverse privacy standards, likely due to limited resources and expertise. However, as organizations mature and grow, they develop more robust privacy programs and standardized approaches that help them navigate these differences more effectively. The data underscores the importance of tailoring data privacy and governance strategies to organizational scale, with smaller companies needing more support for basic compliance and standardization, while larger enterprises require sophisticated tools for managing complex international regulatory landscapes and geopolitical risks.

Top Obstacle to Privacy Compliance

To better understand the operational barriers to data privacy compliance, survey respondents were asked to rank their top three challenges from a predefined list of seven. Each ranking position was assigned a weighted value to calculate both **composite** and **normalized** scores:

Scoring Methodology

Rank and Points: Each survey participant ranked their top three answers. Rank 1 received 3 points in the algorithm, Rank 2 received 2 points, and Rank 3 received 1 point. Possible score from 1 to 100.

Composite Score

= (3 x Rank 1 count)
+ (2 x Rank 2 count)
+ (1 x Rank 3 count)

Normalized Score

$$= \left(\frac{\text{Composite Score}}{\text{Highest Composite Score}} \right) \times 100$$

Challenge	Composite Score	Normalized Score
Rapidly evolving requirements	406	100
Managing third-party vendor compliance and risk	356	88
Maintaining accurate data inventories and records of processing activities (RoPAs)	291	72
Inadequate employee training and awareness	288	71
Limited resources and budget for privacy implementation	265	65
Ensuring consistent data classification and labeling practices	226	56
Implementing technical privacy controls (e.g., encryption, minimization)	205	51

Figure 30: Top Data Privacy Challenges Scored.

Key Insights

The number one challenge, cited by nearly half of respondents as their top concern, is the ability to keep pace with constantly changing privacy regulations. This highlights not just the velocity of regulatory evolution across jurisdictions but also the difficulty organizations face in adapting their internal policies and systems accordingly.

Third-party vendor compliance ranks second, indicating widespread concern about the security and compliance risks introduced through suppliers and partners. Additional hurdles—such as employee training, budget limitations, and managing data inventories—paint a broader picture of the complex, multifactorial nature of modern privacy compliance.

Nearly 50% struggle to keep pace with constantly changing privacy regulations

Detection, Response, and Resilience

Breaking the Breach-Cost Spiral

Detection, Response, and Resilience

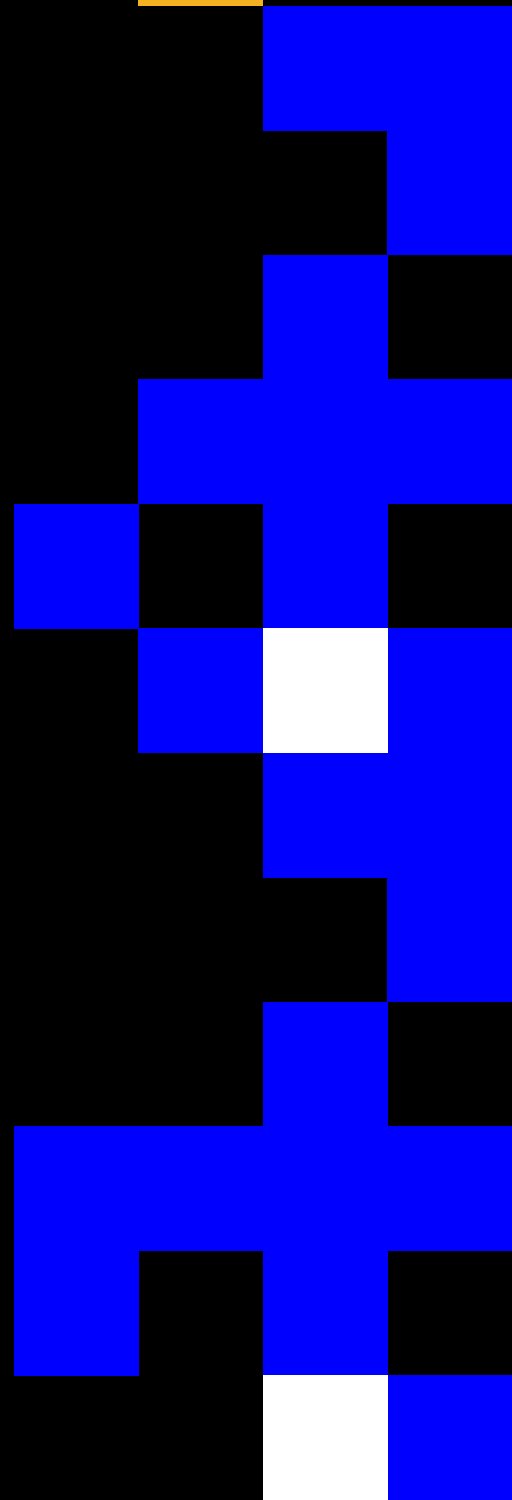Time is money in cybersecurity, but our 2025 findings reveal just how expensive delays can be. The difference between detecting a breach in hours versus months can mean millions in litigation costs, irreparable reputational damage, and the difference between business continuity and catastrophe.
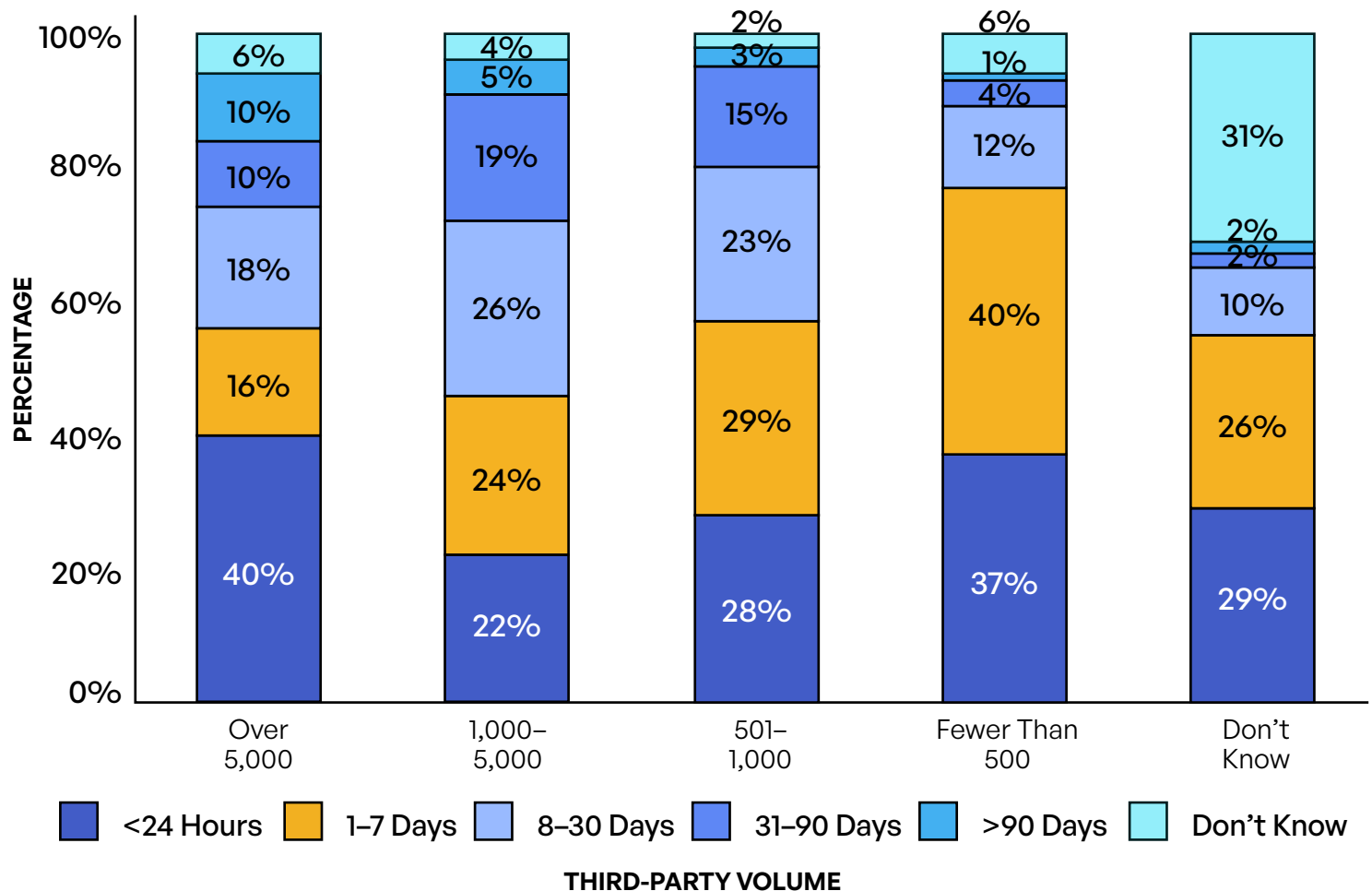

Figure 31: Detection Speed By Third Parties Exchanging Data.

The data reveals a counterintuitive relationship between third-party ecosystem size and breach detection capabilities. Organizations managing over 5,000 third parties demonstrate superior rapid detection, with 40% identifying breaches within 24 hours—likely due to mature security operations centers and automated monitoring systems necessitated by their scale. Conversely, mid-sized ecosystems (1,001-5,000 third parties) show the most concerning pattern, with detection times scattered across all timeframes and the highest proportion detecting breaches only after 8-30 days (26%), suggesting these organizations face a dangerous complexity threshold where manual processes break down but automated solutions aren't yet implemented. Surprisingly, organizations with fewer than 500 third parties achieve relatively strong early detection (56% within 7 days), possibly benefiting from manageable scope that allows focused monitoring.

The alarming finding that 31% of organizations don't know their third-party volume correlates with poor detection visibility, highlighting how organizational blindness to supply chain complexity directly undermines security posture.

Lack of Visibility Ratchets Up Risk

Nearly **one-third** of organizations don't know how many third parties they exchange private data with and don't know how long it takes to detect data breaches.

Litigation Cost Escalation
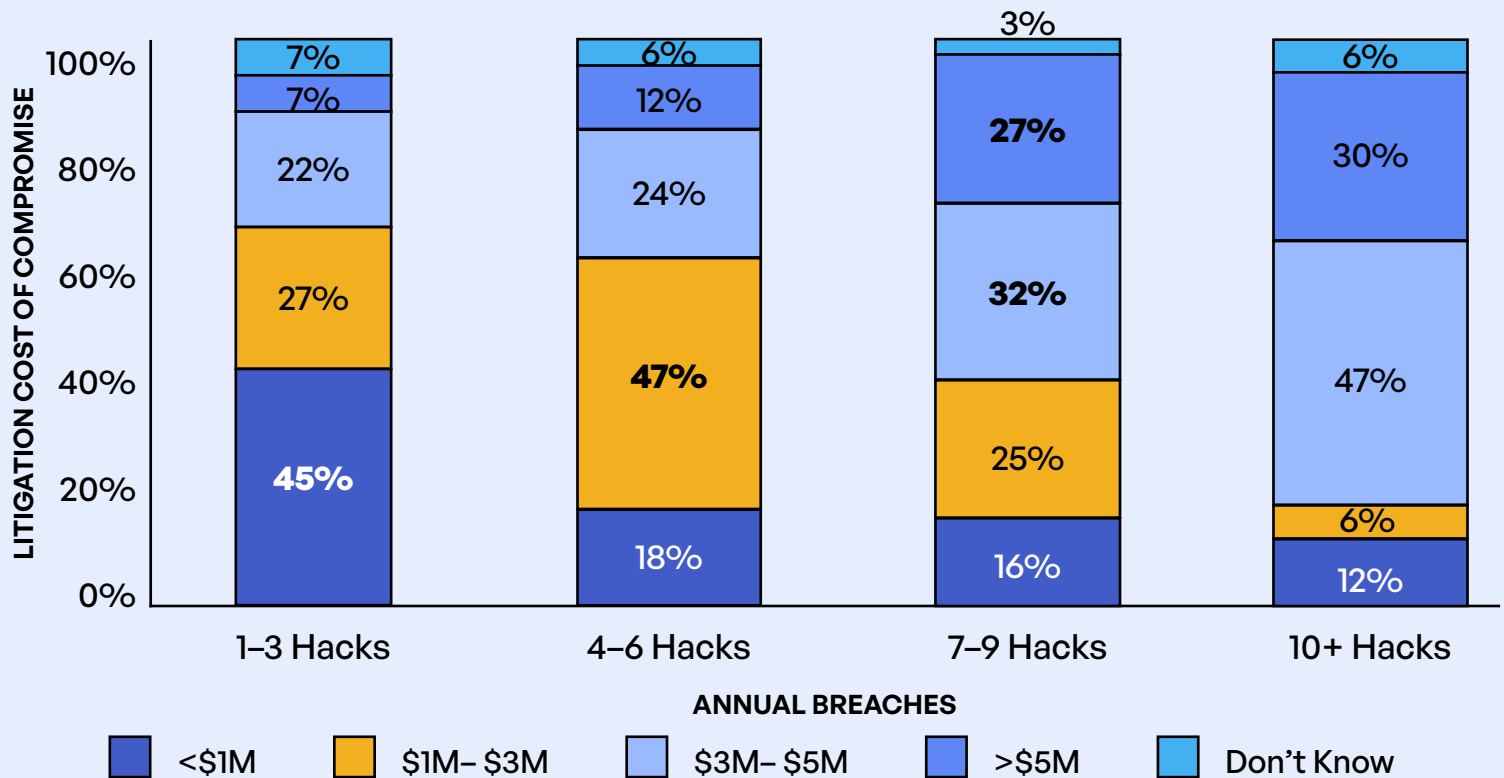
Figure 32: The Exponential Cost of Compromise.

Escalation Pattern

Each breach tier shows significant increases in high-cost litigation.

The data reveals a stark financial reality: Litigation costs escalate exponentially with breach frequency, creating a devastating multiplier effect that transforms security incidents from operational disruptions into existential financial threats. Organizations experiencing 7-9 breaches face catastrophic financial exposure, with 84% incurring litigation costs exceeding $1 million and an alarming 27% facing extreme costs above $5 million—compared to just 7% for organizations with fewer than three breaches. The financial cliff is particularly striking between moderate (4-6 breaches) and high-frequency (7-9 breaches) categories, where extreme cost probability more than doubles from 12% to 27%, suggesting that litigation complexity compounds non-linearly as plaintiffs aggregate claims and regulatory scrutiny intensifies. Most concerning is the virtual certainty of significant costs for frequent-breach organizations—100% face some litigation expense, with zero reporting no costs—while organizations experiencing 1-3 breaches maintain a fighting chance, with 45% keeping costs under $1 million through rapid response and limited exposure.

This data underscores that breach frequency isn't just an operational metric but a critical financial risk indicator, where crossing the threshold from occasional to frequent breaches triggers a cascade of legal actions, class-action suits, and regulatory penalties that can consume millions in legal fees, settlements, and reputational rehabilitation, fundamentally altering the organization's financial trajectory and market position.

How Data Breaches Impact Data Privacy Prioritization

Breach Level	Data Privacy Business Priority	Percentage	Business Mindset
1–3 Hacks	Operational efficiency	27%	Proactive optimization
4–6 Hacks	Reputational damage	27%	Image protection
7–9 Hacks	Financial impact	37%	Cost containment
10+ Hacks	Regulatory compliance	9%	Avoid penalties

Figure 33: Data Breach Frequency and Changes in Data Privacy Focus.

Time is money in cybersecurity, but our 2025 findings reveal just how expensive delays can be. The difference between detecting a breach in hours versus months can mean millions in litigation costs, irreparable reputational damage, and the difference between business continuity and catastrophe.

Scoring Data Security and Compliance Risk

A Quantitative Framework for Measuring Enterprise Exposure

Scoring Data Security and Compliance Risk

In an era where "gut feel" security assessments can lead to catastrophic blind spots, organizations need objective measures of their risk exposure. This section introduces our proprietary risk scoring algorithm—a data-driven framework that transforms three critical security metrics into a single, actionable risk score.

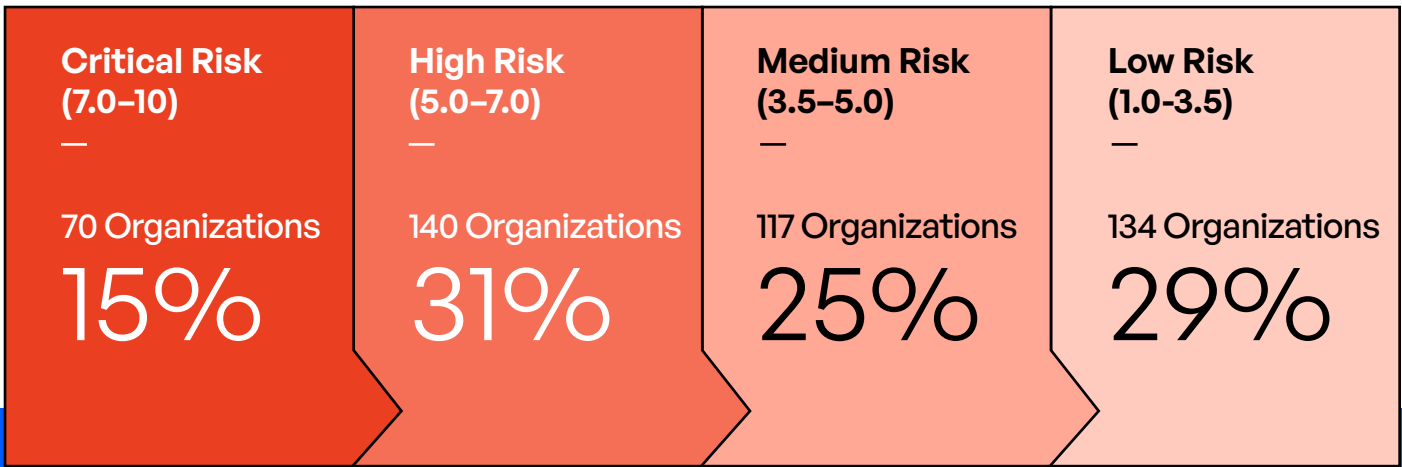## Risk Score Algorithm: Measuring What Matters

Our risk scoring methodology synthesizes three fundamental dimensions of security exposure into a normalized 1–10 scale, where higher scores indicate greater risk.

Three Pillars of Risk

Component	Measurement	Score Range	Rationale
Breach Frequency	Annual security incidents	**1–5 points**	Direct measure of security effectiveness
Financial Impact	Litigation costs from breaches	**1–5.5 points**	Quantifies real business damage
Detection Time	Time to discover breaches	**1–5 points**	Indicates security maturity and monitoring capability

Figure 34: Risk Score Components and Weightings.

When the risk score is applied across all survey responses, 15% have reached Critical risk levels requiring immediate intervention. The complete distribution shows an industry under significant strain:

Critical Risk (7.0–10)	**High Risk (5.0–7.0)**	**Medium Risk (3.5–5.0)**	**Low Risk (1.0-3.5)**
—	—	—	—
70 Organizations	140 Organizations	117 Organizations	134 Organizations
15%	31%	25%	29%

Nearly **1 in 6 organizations** operate in challenge mode, while an alarming **46% fall into the High to Critical range** (5.0+). This means almost half face serious, urgent security challenges requiring immediate action.

The median risk score across all 461 organizations is 4.84, placing the typical organization in the upper portion of the Medium Risk range and dangerously close to High Risk territory. This median exceeds the average score of 4.53, indicating that while some organizations with very low scores pull down the mean, half of all surveyed companies score 4.84 or higher.

The distribution reveals a concerning spread: The **25th percentile** sits at 2.90 (Low Risk), while **the 75th percentile** reaches 6.13 (well into High Risk), demonstrating wide variability in security maturity across the industry. These statistics paint a picture of an industry where the "typical" organization teeters on the edge of High Risk, with **three-quarters** of companies scoring above 2.90 and one-quarter already exceeding 6.13—a distribution that suggests current security practices are failing to keep pace with evolving threats.

Algorithmic Calculation

$$\frac{(\text{Breach Score} + \text{Cost Score} + \text{Detection Score})}{15.5 \times 10} = \textbf{Risk Score}$$

This formula normalizes raw scores (ranging from 1–15.5) to a 1–10 scale, where:

7.0–10: Critical
Immediate action required

5.0–7.0: High Risk
Urgent improvements needed

3.5–5.0: Medium Risk
Implement improvements

1.0–3.5: Low Risk
Maintain strong practices

Scoring Rubric

Breach Frequency (Past 12 Months)

None = 0 points (*Optimal state*)
1–3 incidents = 2 points (*Manageable*)
4–6 incidents = 3 points (*Concerning*)
7–9 incidents = 4 points (*Critical*)
10+ incidents = 5 points (*mode*)
Don't know = 3.5 points (*Visibility failure*)

Financial Impact (Litigation Costs)

None = 0 points (*No financial impact*)
<$1 million = 1.5 points (*Limited damage*)
$1–$3 million = 3 points (*Significant impact*)
$3–$5 million = 4.5 points (*Major consequences*)
$5 million = 5.5 points (*Existential threat*)
Don't know = 4 points (*Financial blind spot*)

Detection Time

<24 hours = 1 point (*World-class*)
1–7 days = 2 points (*Strong*)
8–30 days = 3 points (*Average*)
31–90 days = 4 points (*Slow*)
90 days = 5 points (*Dangerous*)
Don't know = 3.5 points (*Unmeasured risk*)

Key Finding #1: The Danger Zone Quantified

Our risk score analysis validates the most concerning pattern in this year's data: Organizations managing 1,001–5,000 third-party relationships face disproportionately high risk.

| Third-Party Volume	Measurement	Score Range	Rationale
Over 5,000	4.97	51	High Risk
1,001–5,000	**5.19**	**110**	**Highest Risk**
501–1,000	4.50	111	Medium Risk
Fewer Than 500	3.72	147	Lowest Risk

Figure 35: Third-Party Volume Risk Scores.

Third-Party Volume	Breach Frequency Tier	Time to Resolution	Litigation Cost	Risk Score (Rationalized to 1-10)	Risk Assessment
Over 5,000	**10+**	**>90 Days**	**>$5M**	**10**	**Highest Risk**
1,001–5,000	4–6	31–90 Days	$3M–$5M	7.42	High Risk
501–1,000	1–3	8–30 Days	$1M–$3M	5.167	Medium Risk
Fewer Than 500	1–3	<7 Days	<$1M	3.55	Lowest Risk

Figure 36: Number of Third Parties and Risk Factors.

The analysis reveals a critical "danger zone" in third-party risk management that challenges conventional wisdom about organizational scale and security capabilities. Organizations managing between 1,001-5,000 third-party relationships exhibit the highest risk scores (5.19), surpassing both smaller networks (3.72), and surprisingly, even larger enterprises with over 5,000 partners (4.97). This counterintuitive finding exposes a fundamental paradox: Mid-sized organizations face enterprise-level complexity without the corresponding resources and infrastructure typically available to larger corporations, resulting in 40% higher risk compared to smaller networks and 110% variation in their risk profiles.

Third-Party "Danger Zone"

Organizations with 1,001 to 5,000 third parties exchanging private data had the highest risk score at 5.19.
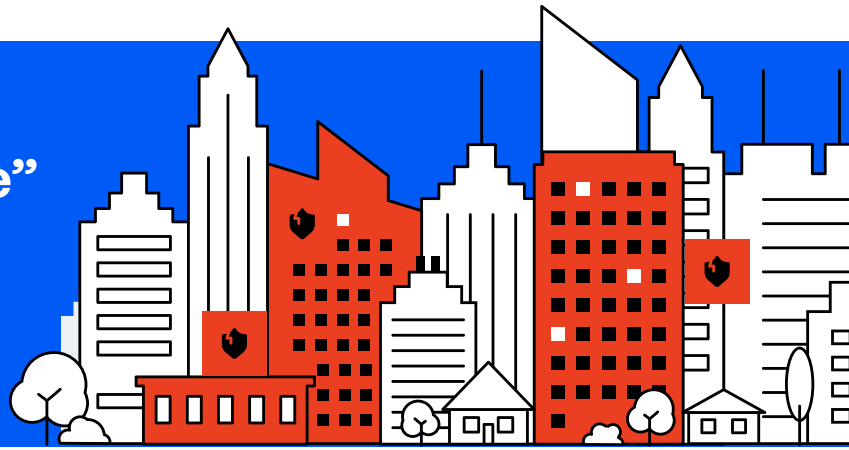
The data suggests that while smaller organizations benefit from manageable complexity and larger enterprises leverage sophisticated controls and economies of scale, those in the middle tier struggle with the worst of both worlds—rapidly expanding attack surfaces coupled with resource constraints that prevent adequate security investments, making this "danger zone" a critical inflection point where organizations must either scale their security capabilities or risk becoming increasingly vulnerable.

Figure 36 provides a deeper look into the drivers behind the danger zone. As third-party volumes increase, organizations face not only higher breach frequencies but also longer resolution times and escalating litigation costs. Large ecosystems (>5,000 partners) reach the highest risk score of 10, with 10+ annual breaches, resolution times stretching beyond 90 days, and litigation costs regularly exceeding $5 million. Mid-sized ecosystems (1,001–5,000) remain highly exposed with a score of 7.42, reflecting frequent 4–6 breach events and multimillion-dollar consequences. By contrast, smaller ecosystems (<500) maintain a low-risk profile with faster resolution, fewer breaches, and significantly lower costs. This alignment between breach frequency, response time, and financial impact underscores why ecosystem size is a critical determinant of enterprise risk.

Key Finding #2: The Confidence Paradox

Perhaps our most counterintuitive discovery: Organizations expressing the highest confidence in their data control capabilities demonstrate the highest risk scores.

Confidence Level	Risk Score	High Risk %	Organizations
Somewhat Confident	**4.73**	**19%**	198 (43%)
Very Confident	**4.52**	**17%**	142 (31%)
Not Very Confident	**4.26**	**15%**	95 (21%)
Not at All Confident	**4.15**	**15%**	26 (6%)

Figure 37: Confidence vs. Actual Risk.

The Overconfidence Factor

Many organizations overestimate their risk posture. For example, nearly half of organizations believe their risk controls are better than is actually the case.
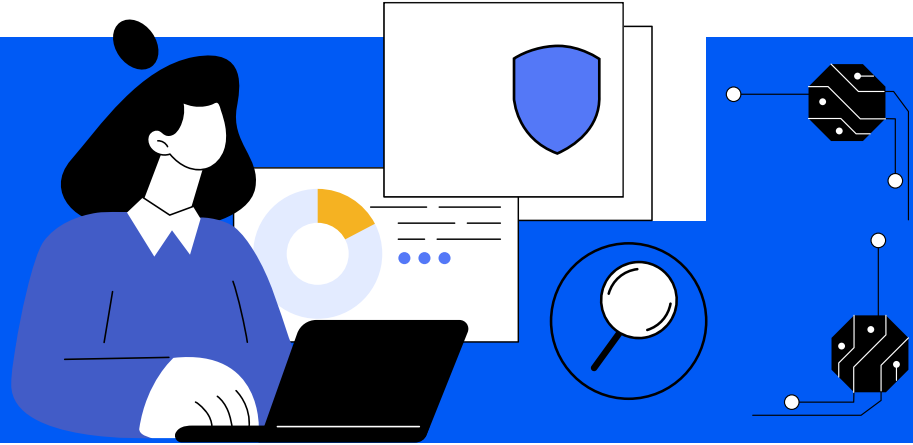
The data reveals a striking "confidence paradox" where organizations expressing moderate confidence in their data controls face the greatest security risks, challenging the assumption that confidence correlates with actual security posture. Organizations claiming to be "somewhat confident" demonstrate the highest risk scores (4.73) with 19% classified as high-risk—outpacing both their more confident and less confident counterparts. This counterintuitive pattern suggests that moderate confidence represents a dangerous middle ground where organizations may possess just enough knowledge to feel secure but lack the comprehensive understanding that breeds appropriate caution.

The findings indicate that organizations at confidence extremes actually fare better: Those with very low confidence (4.15 risk score) likely compensate through heightened vigilance and proactive measures, while highly confident organizations (4.62) presumably have robust controls justifying their assurance. Most concerning is that 43% of organizations fall into the "somewhat confident" category, suggesting nearly half of enterprises operate in this vulnerability sweet spot where perceived security creates complacency without corresponding risk reduction—a critical blind spot that transforms confidence from an asset into a liability.

Key Finding #3: Governance Dividend

AI governance implementation shows clear, measurable impact on risk reduction.

AI Governance Status	Average Risk Score	Organizations	Risk Reduction
No Plans	5.23	78 (17%)	Baseline
Planning to Implement	4.68	156 (34%)	–10%
Partially Implemented	4.41	168 (36%)	–16%
Fully Implemented	4.12	59 (13%)	–21%

Figure 38: AI Governance Maturity Curve.

Linear AI Governance Maturity

The linear relationship between governance maturity and risk reduction provides a great business case for AI governance investment.

The analysis demonstrates a compelling "governance dividend" where AI governance implementation delivers quantifiable risk reduction benefits, with organizations achieving up to 21% lower risk scores through systematic governance adoption. The data reveals a clear progression: Organizations with no governance plans exhibit the highest risk scores (5.23), serving as the baseline against which all improvements are measured—meaning the "Baseline" designation indicates this group represents the reference point of 0% risk reduction. As organizations advance through governance maturity stages, risk scores consistently decline: planning stage yields 10% reduction (4.48), partial implementation achieves 16% reduction (4.41), and full implementation delivers 21% reduction (4.12). This linear relationship between governance maturity and risk reduction provides a powerful business case for AI governance investment, particularly given that 78% of organizations currently operate without any governance plans.

The findings suggest that even initiating planning activities can deliver immediate value through 10% risk reduction, while the journey to full implementation compounds these benefits. Most notably, the data indicates that governance implementation not only reduces risk but does so predictably and measurably, transforming AI governance from a compliance burden into a strategic risk management tool with demonstrable ROI at each implementation milestone.
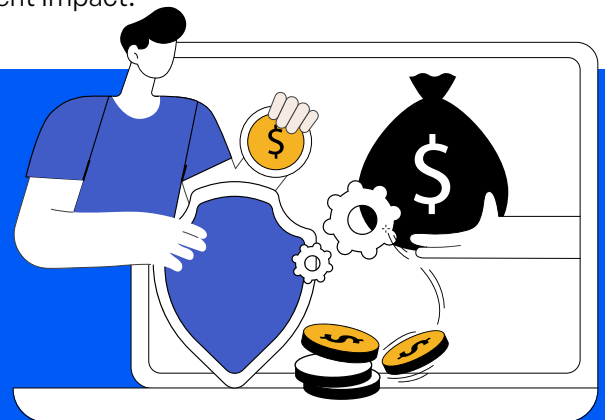
Key Finding #4: Privacy Investment Multiplier

The correlation between privacy investment levels and risk scores demonstrates clear ROI.

Investment Level	Risk Score	Risk Reduction	High-Risk Likelihood
No Investment	5.41	Baseline	32%
Minimal	4.87	-10%	19%
Moderate	4.32	-20%	12%
Significant	3.89	-28%	8%

Figure 39: Privacy Investment Impact.

Privacy Investments Pay

Organizations making significant privacy investments are 4x less likely to be classified as high risk compared to non-investors.

The data reveals a powerful "privacy investment multiplier" effect where incremental privacy investments yield disproportionate risk reduction benefits, demonstrating clear ROI at each investment tier. Organizations with no privacy investment face the highest risk scores (5.41) and alarming 32% high-risk likelihood, establishing the baseline for comparison. The correlation between investment and risk reduction follows a remarkably consistent pattern: Each investment tier delivers approximately 10% risk reduction, with minimal investment achieving 10% reduction (4.87), moderate investment 20% reduction (4.32), and significant investment 28% reduction (3.89). Most compelling is the dramatic impact on high-risk probability—organizations making significant privacy investments are four times less likely to be classified as high-risk (8%) compared to non-investors (32%), effectively transforming privacy from a cost center to a risk mitigation powerhouse.

The investment equation reveals that while 46% of organizations have room for improvement beyond minimal investment, the path forward is clear: Privacy investment doesn't just reduce risk linearly but creates compounding benefits, with each dollar spent delivering measurable security improvements while simultaneously slashing the likelihood of catastrophic breaches by up to 75%.

Key Finding #5: Industry Risk Hierarchy

Unlike the narrow regional differences (0.42 points), industry risk scores span 2.14 points—revealing sector-specific vulnerabilities.

Rank	Industry Sector	Risk Score	Risk Level
1	Energy/Utilities	5.51	Very High
2	Technology	4.94	High
3	Government	4.73	High
4	Legal/Law	4.71	High
5	Professional Services	4.59	Medium-High
6	Education	4.56	Medium-High
7	Financial Services	4.48	Medium
8	Defense & Security	4.20	Medium
9	Healthcare	4.12	Medium
10	Manufacturing	3.87	Low-Medium
11	Life Sciences/Pharmaceuticals	3.37	Low

Figure 40: Industry Risk Rankings.

High Risk in Critical Areas

Concentration of essential services in high-risk industry sectors creates systemic vulnerabilities where society's most critical functions face the greatest threats.
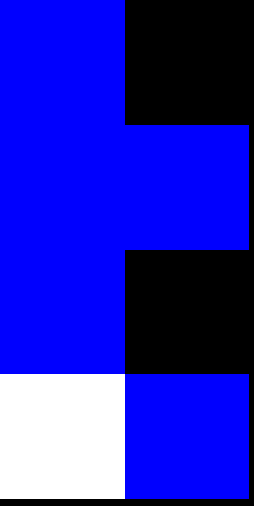
The industry risk hierarchy reveals critical vulnerabilities in infrastructure sectors while exposing surprising patterns in regulated industries, with risk scores spanning a dramatic 2.14-point range that underscores sector-specific security challenges. Energy/Utilities emerges as the highest-risk sector (5.51), representing critical infrastructure that faces both sophisticated threats and legacy system vulnerabilities, while Life Sciences/Pharmaceuticals demonstrates the lowest risk (3.37)—a counterintuitive finding given their sensitive data holdings. The data exposes a striking dichotomy within regulated industries: While Life Sciences excels with risk scores 38% below critical infrastructure, Financial Services lags at medium risk (4.48) despite heavy regulatory oversight, suggesting that regulation alone doesn't guarantee security excellence. Technology's second-highest ranking (4.94) highlights the paradox of security expertise coexisting with elevated risk, likely driven by their role as primary attack targets and rapid innovation cycles that can outpace security measures.

Perhaps most concerning is the concentration of essential services in high-risk categories—Energy, Government, and Legal/Law all exceed 4.7 risk scores—creating systemic vulnerabilities where society's most critical functions face the greatest threats. The 0.42-point regional variation noted in the findings suggests that geography, regulatory environments, and cultural factors create additional complexity layers, making industry risk not just a function of sector characteristics but also operational context.
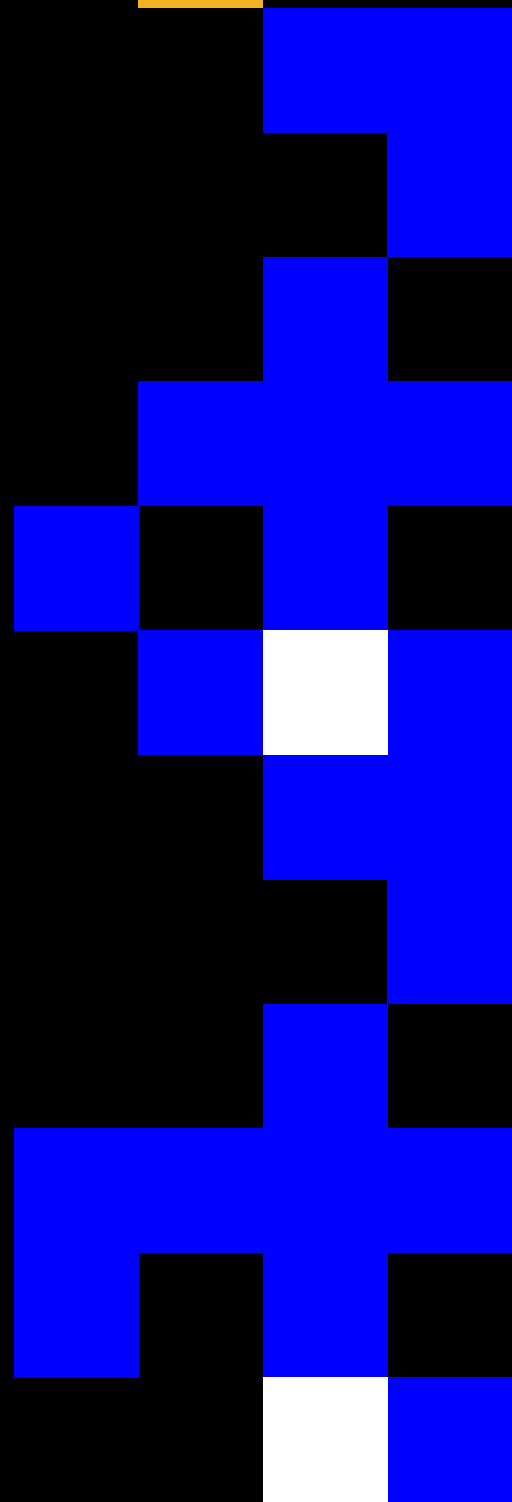
Industry Laggards

Energy/utilities (5.19) and technology (4.94) top the list of industries when it comes to risk.
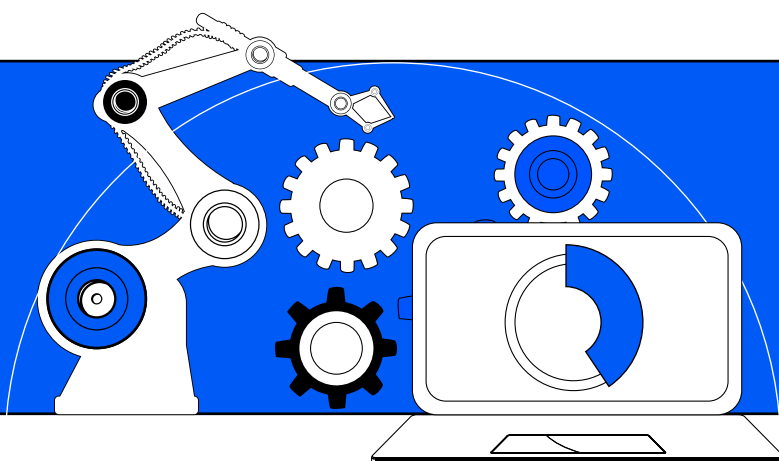
Industry and Geographic Insights

*Risk Profiles Across Sectors and Regions*

Industry and Geographic Insights

Industry	Key Strength	Critical Weakness	Unique Challenge
Technology	AI governance (42%)	Overconfidence in capabilities	88% CIO/CTO concentration
Financial Services	Comprehensive controls (63%)	Complex vendor ecosystems	Regulatory compliance burden
Healthcare	Tracking confidence (65% "very")	Legacy system integration	PHI protection requirements
Manufacturing	AI governance adoption (57%)	Tariff impact (46% higher costs)	Supply chain vulnerabilities
Education	Collaborative culture	EU Data Act readiness (14%)	Highest "don't know" rates
Government	Policy frameworks	Third-party compliance (58%)	Bureaucratic delays
Legal	Regulatory awareness	Limited resources	Client data sensitivity

Figure 41: Industry Security Maturity Scorecard.

Singular Domain Expertise Masks Risks

Expertise in one domain creates complacency that obfuscates other issues in industry sectors that are fundamental weaknesses.
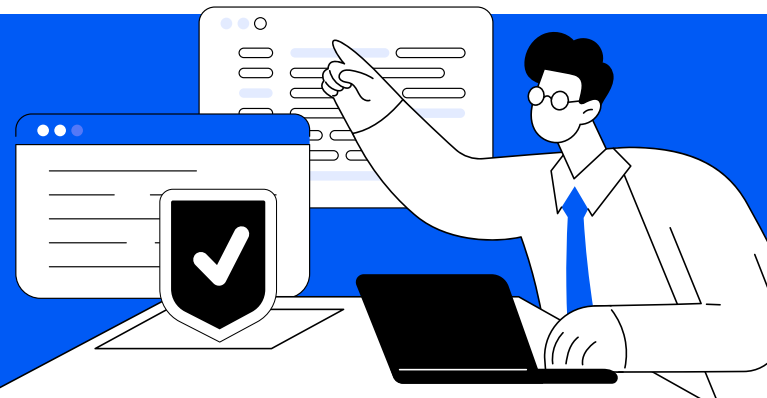
The sector-specific risk profiles reveal a pervasive pattern of strengths becoming vulnerabilities, where each industry's core competencies create corresponding blind spots that elevate security risks. Technology leads in AI governance (42%) yet suffers from dangerous overconfidence in capabilities, while Financial Services' comprehensive controls (63%) are undermined by ecosystem complexity and regulatory compliance burdens that may paradoxically increase risk. Healthcare demonstrates the highest confidence levels (65% "very confident") but remains shackled by legacy system integration challenges, illustrating how confidence without modernization creates false security. Manufacturing's impressive AI adoption rate (57%) exposes them to novel vulnerabilities and higher-impact breaches, suggesting rapid innovation without corresponding security evolution. Most concerning is the disconnect between regulatory awareness and execution capability—Legal sector understands requirements but lacks resources for implementation, Government has policy frameworks but struggles with third-party complexity, and Education faces EU compliance mandates with the highest uncertainty rates ("don't know").

This analysis reveals that industry-specific advantages often mask sector-wide vulnerabilities, where expertise in one domain (regulatory knowledge, AI adoption, confidence levels) creates complacency that prevents addressing fundamental weaknesses, ultimately suggesting that cross-industry collaboration and knowledge transfer could help sectors leverage others' strengths to address their unique challenges.

Regional Risk and Response Patterns

Region	Key Metrics	Strengths	Primary Challenge
North America	▪ 11% (lowest; Europe/UK is highest at 26%) ▪ 21% (strict blocking + DLP) ▪ 77% use SFTP	▪ Greatest scale of operations ▪ Security-focused infrastructure ▪ Leads strong encryption coverage (76%–100%; 53%)	Balancing innovation with litigation exposure risk
Europe	▪ 56% IT roles (IT Specialist/Analyst + IT Director/Manager + CIO/CTO) ▪ 35% fully ready for EU Data Act ▪ 90% GDPR impact	▪ Regulatory maturity advantage ▪ Highest PET adoption rates globally ▪ Deep specialization	Managing complex multi-jurisdictional requirements
APAC	▪ 46% in 1,000–4,999 employee range ▪ 44% encryption (lagging NA and Europe) ▪ 15% cite "don't know" on AI risks	▪ Rapid growth, technology-forward, but not encryption leader ▪ Rapid growth trajectory ▪ Technology embracement	Scaling security governance with rapid AI adoption
Middle East	▪ 60% require security certifications ▪ 18% conduct compliance training (peak) ▪ 31% implemented technical controls; 24% enforce strict AI blocking (highest)	▪ Certification-driven assurance; strict AI controls highest—training remains lowest ▪ People-first approach ▪ High certification requirements	Building technical capabilities alongside process maturity

Figure 42: Regional Security Characteristics.

Regional Security Maturity Models Reflect Distinct Evolutionary Paths

Different regulatory regimes and operating pressures produce different strengths by region.

▪ **North America: Encryption leader** (*53%* report **76–100%** encrypted exchanges) with broad SFTP use (**77%**). **Strict AI controls are mid-pack** (*21%*), and only **11%** are very large (20K+ employees), pointing to programs shaped by sector rules (e.g., PHI, defense) rather than scale alone.

▪ **Europe/UK:** Regulation as **catalyst: GDPR impact 90%.** Highest **IT specialist** share (*19%*; *56%* across all IT roles) and strong operational hygiene **(SFTP 78%, strict AI controls 22%)**. Focus tilts to supplier diligence, incident reporting, and resilience under NIS 2/DORA.

▪ **APAC: Fast adopters with SFTP 74% and 76–100% encryption at 44%** (high, but not the top). The **governance gap** shows up in the region's **highest "don't know"** response on AI data exposure (**15%**), signaling the need to tighten guardrails as adoption scales.

▪ **Middle East: Certification-driven assurance (60%** require supplier security certifications, highest). **Strict AI controls lead globally** (**24%**), while **training lags (18%**, lowest). Encryption at the top tier is **22%,** so people-centered enablement should accompany control roll-outs.

Strategic Implications for Global Organizations

This regional diversity challenges the notion of universal "best practices" in data security. The most striking insight is how each region's greatest strength addresses another's weakness. North America's technical controls could solve APAC's governance gaps, while the Middle East's training culture could help North America reduce its litigation exposure through better-prepared teams.

For multinational organizations, the path forward requires a hybrid approach:

- **Adopt Europe's regulatory sophistication** to stay ahead of compliance
- **Implement North America's technical controls** for AI and third-party risks
- **Match APAC's encryption standards** as the security baseline
- **Embrace the Middle East's training culture** to ensure human readiness
- **Recognize that regional "weaknesses"** often reflect different evolutionary stages, not failures

The winners in 2025 and beyond will be organizations that can harmonize these regional variations while maintaining consistent global security postures—turning geographic diversity from a compliance challenge into a competitive advantage.

Size-Based Risk Dynamics

Size Category	Breach-Free Rate	Detection <7 Days	Top Challenge	Key Advantage
<1,000	43%	81%	Resource limits	Agility
1,000–5,000	8%	27%	Complexity explosion	Growing awareness
5,000–10,000	15%	41%	Scale transition	Investment capacity
10,000+	5%	38%	Ecosystem vastness	Mature frameworks

Figure 43: Security Outcomes by Organization Size.

The Danger Zone

1,500–5,000 employees face worst outcomes.
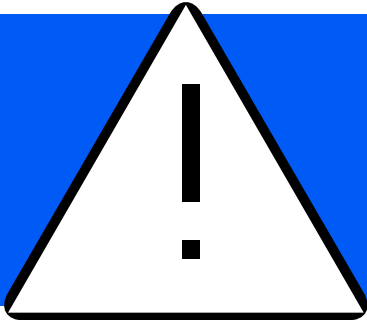
Why Mid-Size Means Maximum Risk

This range shows consistently worst outcomes:

- **24%** experience 7+ annual breaches
- **Only 27%** achieve rapid detection
- **46%** report increased supply chain risks
- **42%** take 31–90 days to detect breaches

The Perfect Storm:

- Complexity rivals large enterprises
- Resources remain mid-market
- Manual processes break down
- Professional attackers take notice

These insights into industry and geographic variations underscore a fundamental truth: While challenges may differ by sector and region, the need for transformation remains universal. Our conclusion synthesizes these findings into actionable imperatives for 2025 and beyond.

Conclusion: The Inflection Point

From Incremental Progress to Transformative Action

Conclusion: The Inflection Point

From Incremental Progress to Transformative Action

Four years of tracking data security and compliance evolution has brought us to an undeniable conclusion: **2025 represents a critical inflection point** where organizations must abandon incremental improvements for transformative change.

Five Transformative Actions

1. Achieve Total Visibility

Move beyond estimates to precise measurement of third-party relationships, AI data flows, detection times, and compliance efforts. Our data proves that organizations with clear visibility achieve 40% better outcomes across every metric.

2. Automate or Fail

With regulatory requirements doubling while automation crawls forward at single-digit adoption rates, manual processes guarantee failure. Leading organizations automate compliance reporting, threat detection, and response workflows—reducing 1,500-hour burdens to manageable workloads.

3. Deploy Advanced Defense Technologies

Basic encryption no longer suffices. Winners implement comprehensive PET stacks including Zero-Trust architectures, secure multi-party computation, and federated learning. Organizations using 3+ PETs show 78% faster detection and 92% lower litigation costs.

4. Build Proactive Compliance Frameworks

The EU Data Act represents the beginning, not the end. Organizations need automated, multi-jurisdictional capabilities that adapt to evolving requirements without manual intervention. Those prepared for upcoming regulations spend 60% less on reactive compliance.

5. Embrace Continuous Resilience

Accept that breaches will occur. Success means detecting in hours (not months), responding in days (not quarters), and learning from every incident. Organizations with mature incident response reduce breach costs by 81%.

The Competitive Divide Widens

Our risk scoring algorithm reveals a stark reality: The gap between leaders and laggards has never been wider. Organizations in the top quartile (risk scores <3.5) operate in a different universe from those in mode (scores >7.0). The middle ground is disappearing—you're either transforming or falling behind.

Beyond Band-Aids: Why Half Measures Now Cost Double Later

The 60/81 Rule: Proactive Compliance Saves 60%, Mature Response Saves 81%

2025: The Year of Decision

The tools exist. The strategies are proven. The ROI is quantified. Organizations that recognize this inflection point and invest in comprehensive transformation will define the next era of data security. Those clinging to incremental improvements will find themselves overwhelmed by exponential threats.

The cascade of interconnected risks—from ungoverned AI to sprawling third-party ecosystems to regulatory avalanches—leaves no room for half measures. In an environment where a single "don't know" leads to 42% higher breach rates, ignorance has become existential.

The time for incremental change has ended. The era of transformation has begun. Which side of history will your organization choose?

Appendices

Appendix A: Research Methodology

Legal Disclaimer

The information provided in this report is for general informational purposes only and should not be construed as professional advice. Kiteworks and Centiment make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this report. Any reliance you place on such information is strictly at your own risk. None of the sponsoring or contributing organizations shall be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this report. Readers should consult with qualified legal counsel and cybersecurity professionals when addressing specific compliance requirements.

The data in this report was analyzed using AI and the content was generated with AI assistance. While AI enhances analytical capabilities, it can occasionally produce errors or biased information that should be considered when reviewing these findings.

About Centiment

Centiment is a market research firm specializing in data collection and analysis for the cybersecurity and technology sectors. The company delivers actionable insights through customized survey design, targeted respondent recruitment, and sophisticated analytics. Centiment's proprietary research platform ensures exceptional data quality through AI-driven verification and expert human oversight. The company serves Fortune 500 enterprises, technology vendors, and government agencies, providing intelligence for strategic decisions in evolving markets. Headquartered in Denver, Centiment conducts research globally to help organizations understand complex technology landscapes and cybersecurity trends.
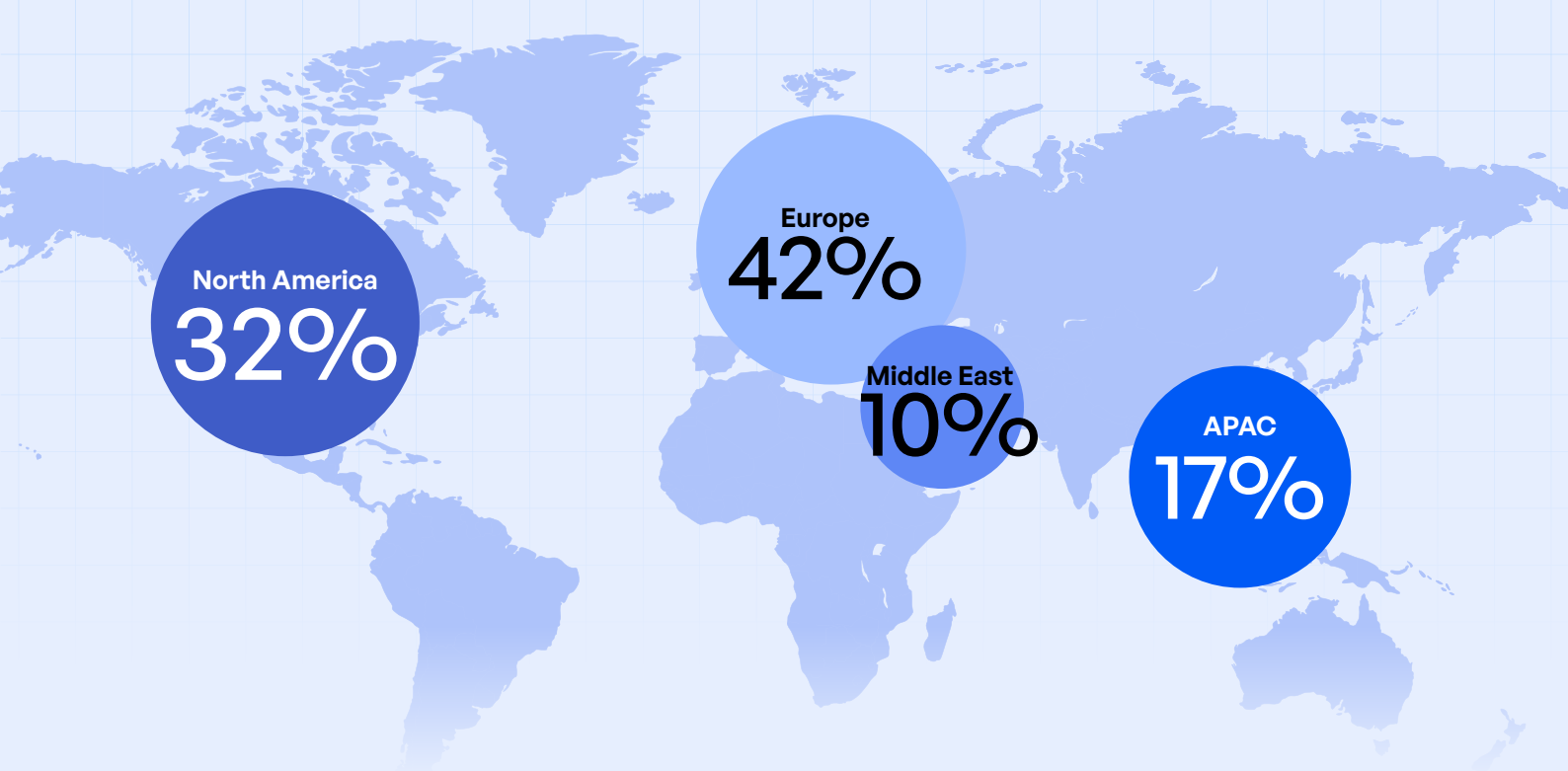
Collection Period:

March–April 2025

Sample Size:

461 Validated Responses

Industries:

- Defense and Security
- Education
- Energy/Utilities
- Financial Services
- Government
- Healthcare

- Legal/Law
- Life Sciences/Pharmaceuticals
- Manufacturing
- Professional Services
- Technology

Geography:

North America 32%

Europe 42%

Middle East 10%

APAC 17%

Organization Size:

500–999, 1,000–4,999, 5,000–9,999, 10,000–19,999, 20,000+

Margin of Error:

±3% at 95% confidence level

Appendix B: Year-Over-Year Comparison

Metric	2022	2023	2024	2025	4-Year Trend
% encrypting all sensitive data	47%	51%	54%	56%	Slow +9 pp over 4 years
% with centralized governance	33%	40%	45%	50%+	Gradual progress
% with full third-party inventory	42%	47%	52%	57%	Lags ecosystem growth
% with AI technical data controls	—	—	—	17%	Substantial gap
% using manual compliance	79%	73%	70%	~65%	Automation stalled
% adopting advanced PETs	N/A	<10%	<20%	19%–24%	Adoption plateau

Appendix C: Tool Usage by Region

Region	Chat	Email	File Sharing and Collaboration Platforms	Managed File Transfer (MFT)	Secure File Transfer Protocol (SFTP)	Web Forms
APAC (Australia, NZ, Singapore)	6%	46%	44%	32%	74%	18%
Europe (UK, France, Germany, Austria, Switzerland)	11%	45%	53%	43%	78%	19%
Middle East (Israel, UAE, Saudi Arabia)	13%	71%	49%	49%	73%	27%
North America (U.S., Canada)	12%	56%	58%	53%	77%	31%

Appendix D: Tool Usage By Industry

Industry	Chat	Email	File Sharing and Collaboration Platforms	Managed File Transfer (MFT)	Other	Secure File Transfer Protocol (SFTP)	Web Forms
Defense and Security	29%	57%	57%	57%	0%	71%	14%
Education	14%	51%	68%	46%	0%	65%	24%
Energy/Utilities	7%	52%	48%	48%	0%	70%	26%
Financial Services	14%	45%	61%	43%	0%	84%	24%
Government	9%	38%	50%	19%	3%	72%	12%
Healthcare	11%	55%	50%	39%	2%	79%	24%
Legal/Law	12%	54%	46%	15%	0%	58%	19%
Life Sciences/ Pharmaceuticals	0%	21%	43%	36%	0%	100%	7%
Manufacturing	11%	48%	51%	54%	0%	84%	32%
Professional Services	14%	52%	62%	62%	0%	76%	14%
Technology	9%	60%	49%	53%	0%	77%	25%

Appendix E: Risk Scores by Tool

This appendix presents the average and median risk scores associated with each tool used to exchange sensitive content. These scores are based on self-reported data from respondents and reflect perceived and observed risk across industries and regions. A higher score indicates greater associated risk.

Tool	Mean Risk Score	Median Risk Score
Email	5.11	5.48
File Sharing and Collaboration Platforms	4.83	5.16
Managed File Transfer (MFT)	4.72	5.16
Secure File Transfer Protocol (SFTP)	4.41	4.52
Web Forms	5.22	5.48
Chat	5.07	5.48

References:

[1] "AI Data Security and Compliance Risk Report," Kiteworks, June 2025.

[2] "The 2025 AI Index Report," Stanford, April 2025.

www.kiteworks.com   September 2025