**RESEARCH** BRIEF

# The Surprising Reason Why CISO-Led Fraud Teams Underperform

We thought CISO ownership of fraud would drive better outcomes. The data told a different story.

Accertify

Based on original research across 250 fraud and risk decision-makers Accertify + Liminal, 2026

## I / We Believed CISOs Should Own Fraud

In 2025, Accertify published a position paper making the case for CISO ownership of fraud. The argument was direct: CISOs understand attack paths, operate the "shift to the left," and already own the upstream identity controls - CIAM, session integrity, bot defense, device reputation - that fraud outcomes depend on.

Also, attackers do not distinguish between an employee login and a customer login. The same credential stuffing infrastructure hits both surfaces. The same account takeover playbook runs across both domains. Neither, we argued, should the CISO draw a line between protecting employees and protecting customers.

We stand behind that logic. But we wanted to test it - at scale, with data - against real-world organizational performance. So we commissioned original research from Liminal across 250 fraud and risk decision-makers spanning five industries: Retail/eCommerce, Travel, Restaurants/QSR, Entertainment & Media, and Marketplaces.

**What we found out about CISO-led fraud performance was entirely unexpected.**

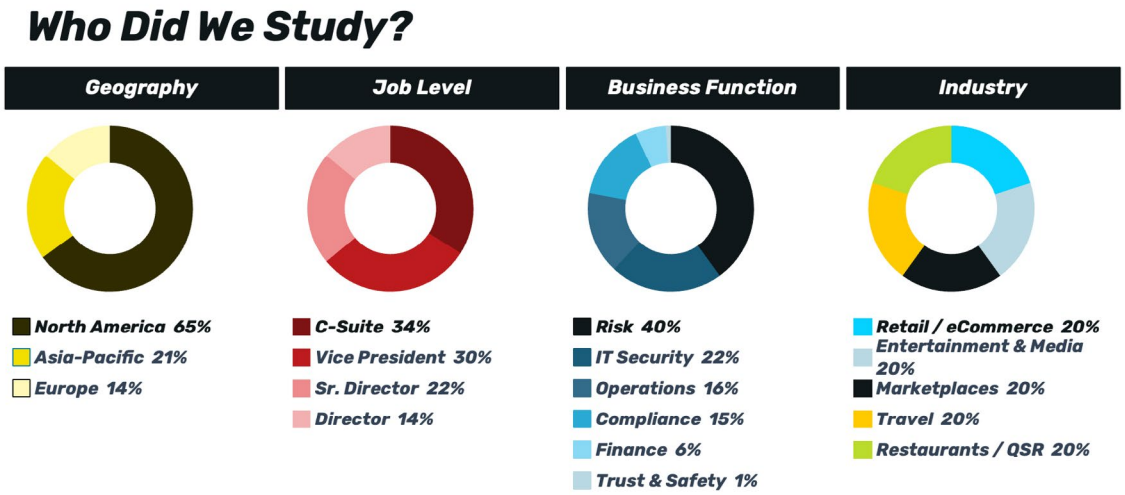
## II / How We Measured Performance

But first, let's discuss how we defined "fraud performance." To compare 250 organizations on a single dimension, we needed a metric that captured the core fraud tradeoff: approving good customers while stopping bad ones. To that end, we used a measurement of precision, the "Precise Yes Score" (PYS hereafter). The calculation was approval rate on dollar volume divided by fraud chargeback rate on dollar volume, which in the end yields, "How many dollars did the organization approve in revenue for every dollar of fraud chargeback?"

A higher score means more approved dollars for every dollar lost to fraud chargeback, which helps us measure decisioning precision. The range of approval rates across the 250 organizations was small: the 5 industries averaged as low as 97.5% (Entertainment and Media) and as high as 98.2% (Retail). Given this limited range, we thought it would be best to further refine the performance metric by understanding how precise these "Yes" decisions were, not just how frequent.

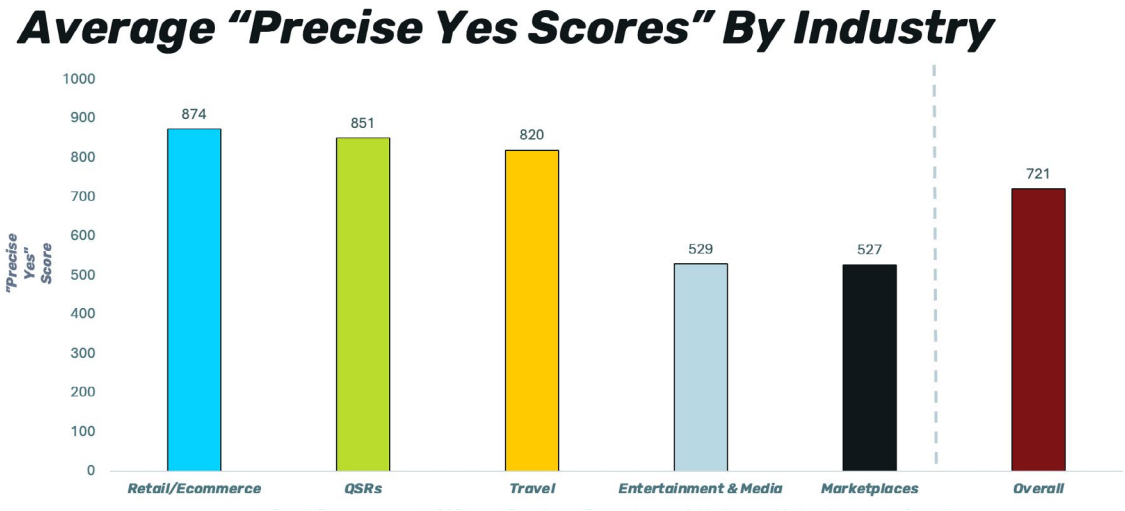
It is worth pointing out that the Precise Yes score is NOT an optimization target, because it is incredibly sensitive to the fraud chargeback rate in the denominator. The PYS was simply a way to retroactively compare the performance of the 250 organizations in the research sample on a single consistent dimension.

**Figure 1 : Breakdown of the 250 decision-makers sampled in the study**




***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

**Figure 2 : Average Precise Yes scores by industry, defined as $ approved/$ lost to fraud chargebacks**

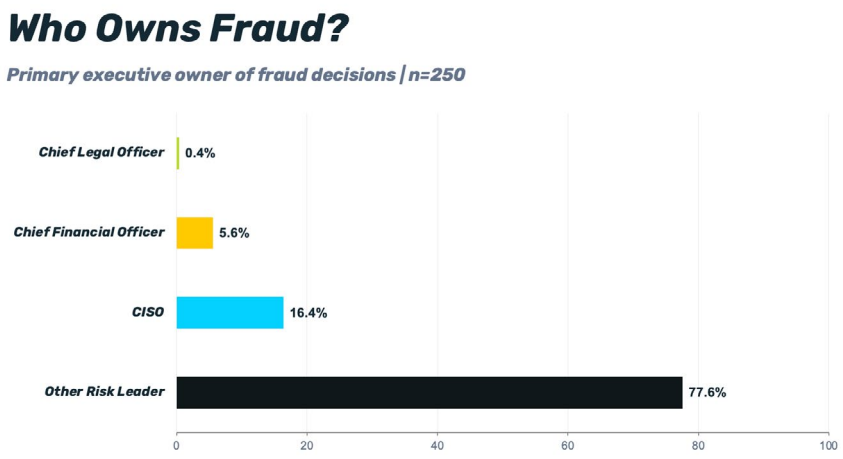



***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

# III What We Expected to Find vs. What We Found

16% of organizations in our study (41 out of 250) responded that fraud reported up to the CISO.

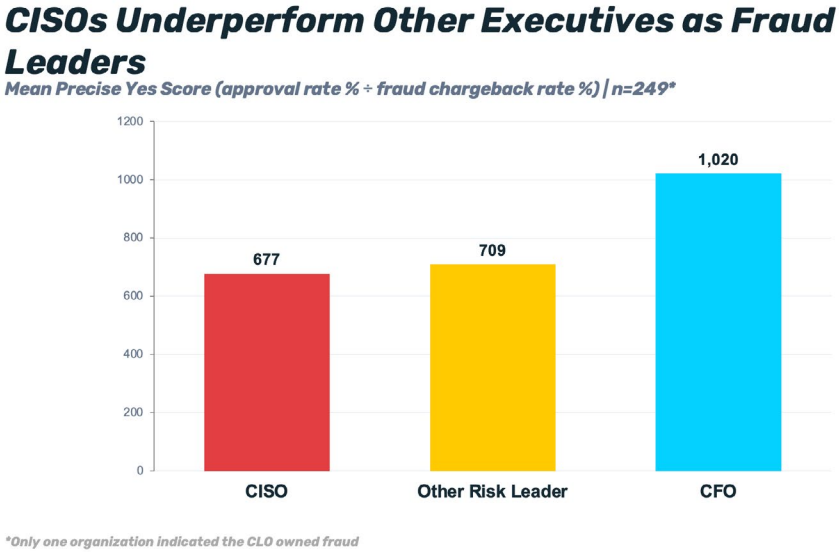
**Figure 3 : To which C-suite executive does fraud report in your organization?**




*Source:* Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

We expected to find that the organizations where fraud was CISO-led would also lead on the Precise Yes score, given the argument that shifting left and joining signals across the customer journey would be an effective approach to more precisely stopping fraud. That was not the case.

**Figure 4 : How CISOs compare against other C-suite executives who commonly own fraud in their organizations**




*Source:* Accertify-Liminal Study on Fraud-Cyber Convergence, 2026 (N=249). 1 organization reported that their Chief Legal officer led fraud, which was omitted from the chart due to the low N.

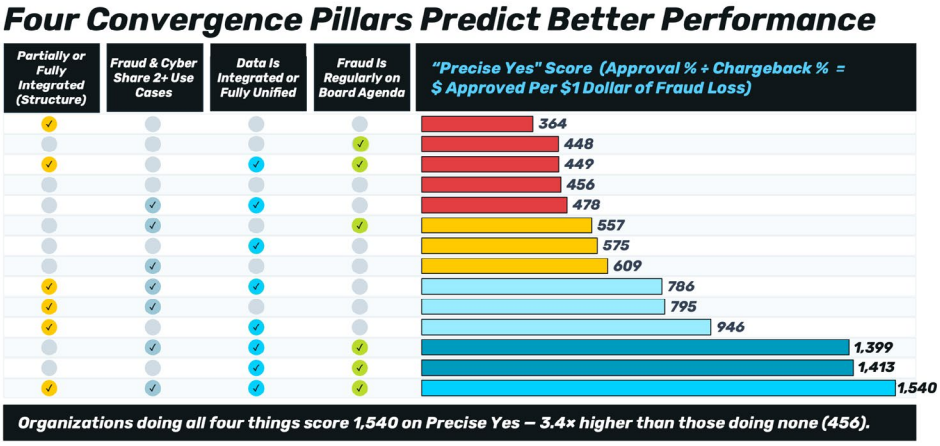
CISO-owned fraud organizations recorded the lowest Precise Yes Score of the three primary ownership structures, below CRO-owned organizations, and statistically significantly below CFO-owned organizations. And even below the overall study mean of 721.

**Why? We devote the rest of this brief to answering this question.**

# IV / The Missing Convergence Pillar

The Accertify-Liminal seminal research identified four convergence pillars that were linked to better fraud decisioning precision across the 250 organizations we studied. Three of the four pillars are operational behaviors, while the fourth is a structural characteristic. Each of these convergence pillars is binary – either the organization demonstrated it, or it did not. Organizations that demonstrated all four convergence pillars performed the best by far.

## Figure 5 : The Four Convergence Pillars Linked to a Higher Precise Yes Score




***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

**The four pillars are:**

- **Structural:** Fraud and cyber are either partially or fully integrated under the same organization.
- **Use Cases:** Co-ownership of outcomes. Fraud and cyber teams share joint accountability for two or more specific threat types.
- **Data Sharing:** Data integration or a fully unified pipeline for fraud and cyber data, providing one integrated view of the customer, not disparate systems.
- **Board Agenda:** Fraud is regularly on the board agenda, not just discussed within operational or executive teams.

Individually, each pillar is associated with better performance. But together, organizations with all four pillars record a mean Precise Yes Score of 1,540. Organizations performing with zero pillars record a mean PYS of 456. That is a 3.4x gap.

Having the fraud and cyber team sharing accountability for 2+ Use Cases seems to be the difference maker: it is the only pillar where CISO-owned organizations dramatically trail both CRO- and CFO-owned organizations. On every other pillar - structural integration, data sharing, board visibility - CISO-owned organizations either lead or are competitive. But on Sharing 2+ Use Cases, the gap is stark: CFO-owned organizations are at 86%, CRO-owned at 65%, CISO-owned at just 39%.

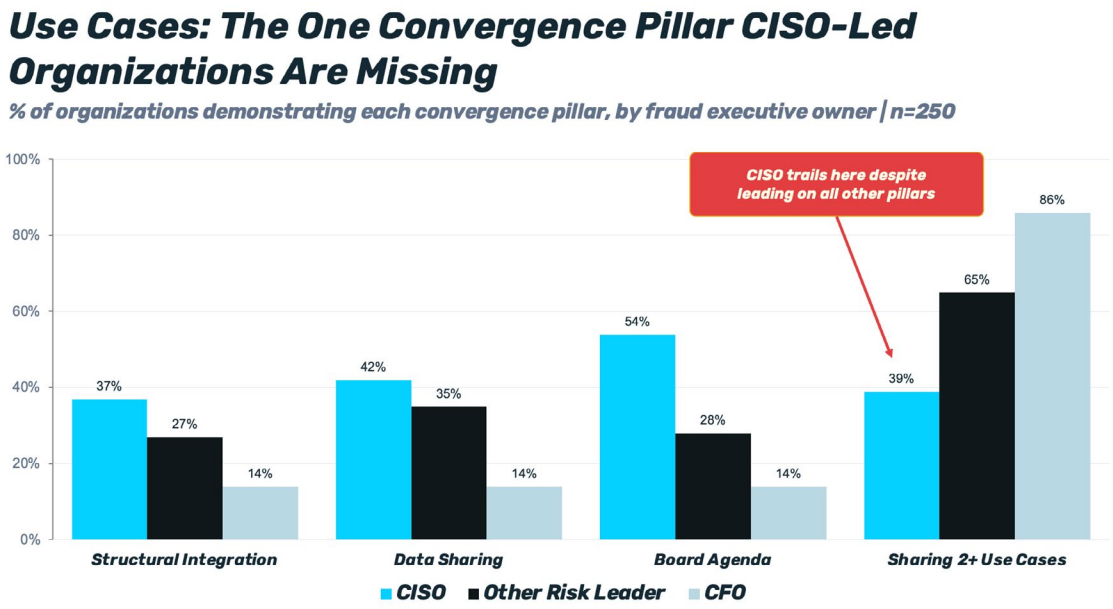
This gap is striking for a reason we will return to: both fraud and cyber teams are already working from the same underlying signal types. The problem is not what data each team has access to - it is whether they are bringing their expertise to bear on it together.

Strikingly, the organizations that perform the worst in our study are those with three of the four convergence pillars (Structure, Data-sharing, and Board-level discussions about fraud, but no Use Case sharing). These organizations score lower than organizations doing nothing at all.

Sharing responsibility for 2+ Use Cases requires fraud and cyber teams to co-own specific threats - to share accountability for outcomes, not just pass back and forth a report or workbook. That is a different kind of change, and it is the one CISO-owned organizations are most consistently missing.

**This is how CISO-owned organizations compare to CRO-owned and CFO-owned organizations on each signal:**

## Figure 6 : The CISO's Missing Convergence Pillar




***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

The pattern is striking. CISO-owned fraud organizations lead on every pillar where the CISO has direct authority: they are more likely to have fraud on the board agenda, more likely to have integrated data pipelines, and more likely to have structural convergence on the org chart. These are the pillars a CISO is likely driving from the top down.

But on use case sharing - joint accountability between fraud and cyber teams for specific shared threats - CISO-owned organizations trail dramatically.

**CISO-owned organizations are doing more of almost everything. The one thing they are not doing is the thing that matters most.**

# V / Ownership Without Collaboration Is Not Convergence

The performance data reflects a specific and costly pattern. Of the 41 CISO-owned fraud organizations in our study, 61% (or 25 organizations) are missing the use case sharing pillar entirely. Among those, 7 have achieved three convergence signals (structural integration, data integration, and board visibility) but have not built shared use case accountability between their fraud and cyber teams.

Those 7 organizations record a mean Precise Yes Score of 287 - lower than the 456 recorded by organizations with zero convergence pillars. In other words, doing more things in the wrong sequence is actually worse than doing nothing. This is what the research calls "convergence purgatory."

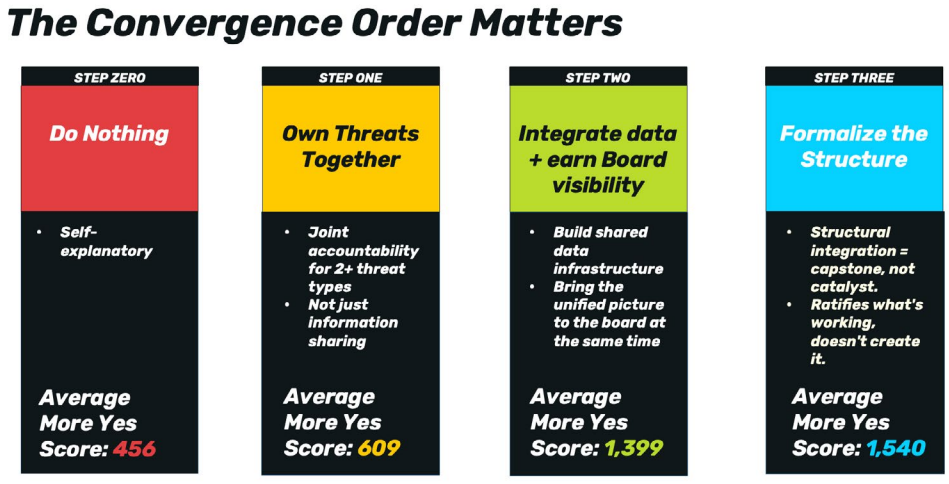
The fraud team has a new reporting line.  The data is integrated. Fraud appears on the board agenda. But the fraud and cyber teams are not working together on shared threats. So in the end, the working relationship between the teams has not changed, and the performance numbers reflect it.

**Taking over fraud on the org chart without first building joint accountability for shared threats does not produce convergence. It produces disruption.**

### The Convergence Sequence That Works

Our research identifies a specific three-step sequence for convergence to achieve Elite-tier performance. The order matters.

**Figure 7 : The Order of Convergence for Best Results**




***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

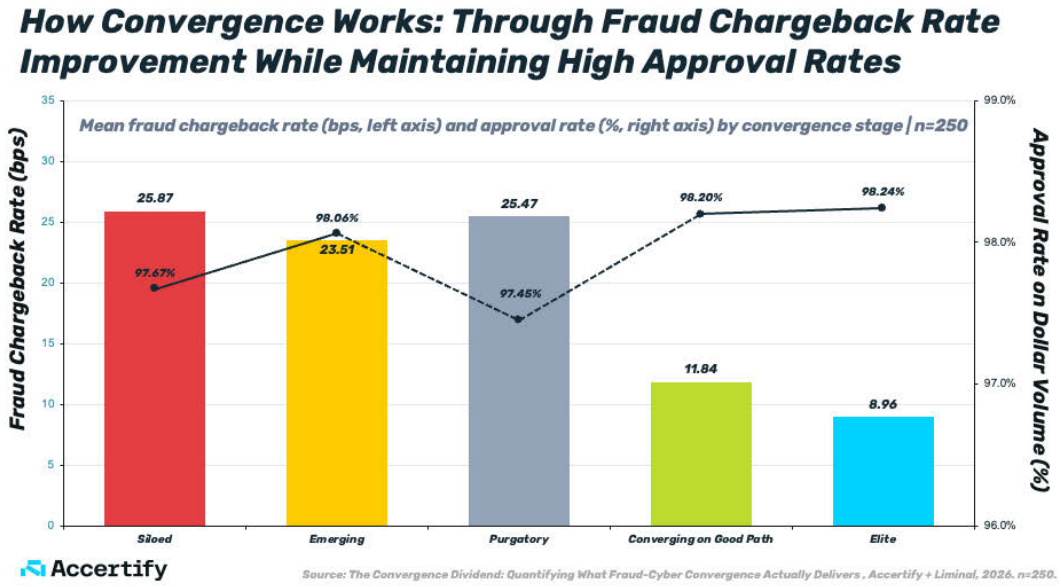
Putting fraud and cyber under the same organizational umbrella is the last move, not the first. CISO-owned organizations that reorganized fraud under security without first building shared operational accountability skipped Steps 1 and 2. Structural convergence on the org chart, used as a capstone after the collaboration is already working, lifts performance meaningfully. Used as a catalyst before the collaboration exists, it does not.

# VI / What Top-Performing Organizations Actually Do

The Elite tier in our research - organizations with all four convergence pillars - records a mean Precise Yes Score of 1,540, compared to 456 for organizations with zero pillars. That is a 3.4x performance gap.

This gap is driven primarily by fraud chargeback reduction: Elite-tier organizations record fraud chargeback rates of 8.96 basis points versus 25.87 basis points for zero-pillar organizations, a 62% reduction. Approval rates, by contrast, show little variation across tiers - the enterprise organizations in the study were already approving 97-99% of transactions, leaving little room to improve. However, even with the small variation across the sample, at the Elite tier, there is a statistically meaningful lift in approval rates vis-à-vis the other levels of convergence maturity.

**Figure 8 : Precision in fraud decisioning is where the real performance gap lives.**




***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

The natural next question is: which two use cases should the fraud and cyber teams start to co-own? Our data offers some direction. The use case pairs that produce the strongest performance lift when fraud and cyber teams share accountability are as follows:

**Figure 8: Precision in fraud decisioning is where the real performance gap lives.**

| Use Case Pair | Mean PYS – Shared by Both Fraud & Cyber | Mean PYS – Siloed in either Fraud or Cyber |
|---|---|---|
| ATO + Customer Authentication | 1,106 | 622 |
| CNP Fraud + Credential Stuffing | 1,301 | 657 |

These pairings are not arbitrary. ATO and customer authentication share the same signal surface - both require visibility into credential validity, session behavior, and device reputation. CNP fraud and credential stuffing share the same attacker infrastructure - the same automated tooling that tests stolen credentials also drives card-not-present fraud attempts. When fraud and cyber teams own these problems jointly, they see the full attack chain. Separately, each team sees half of it.

For CISOs, these are not unfamiliar problems. ATO, credential stuffing, and authentication abuse sit squarely in the security domain. The shift is not in the threat categories - it is in the accountability model. Taking joint ownership of these use cases with the fraud team is the first step to make.

## VII / The Shared Signal Problem

Across the 250 organizations in our study, both teams draw heavily from the same signal types. Yet 65% of organizations share data through processes rather than shared platforms - meaning in most cases, those signals are being interpreted in parallel rather than together.

| Signals Used | Fraud Teams | Cyber Teams |
|---|---|---|
| Identity & Authentication | 69.2% | 68.0% |
| Network / IP Intelligence | 64.0% | 63.2% |
| Device Intelligence | 50.8% | 56.0% |
| Behavioral Signals | 28.0% | 30.0% |
| Transaction / Payment Data | 43.6% | 40.8% |
| Threat Intelligence Feeds | 19.6% | 17.6% |
| Bot Detection | 6.4% | 9.6% |

***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

The overlap is not marginal. Identity and authentication signals are used by 69.2% of fraud teams and 68.0% of cyber teams. Network and IP intelligence: 64.0% and 63.2%. In each case, the two teams are drawing from essentially the same underlying data pool.

This matters because signal interpretation is where expertise lives. A device intelligence signal means something different to a fraud analyst - who sees it in the context of transaction history, velocity, and order value - than it does to a security engineer who sees it in the context of session anomalies, IP reputation, and prior breach data. When both teams see the same signal through their own lens but never compare notes, the organization gets two incomplete pictures instead of one complete one.

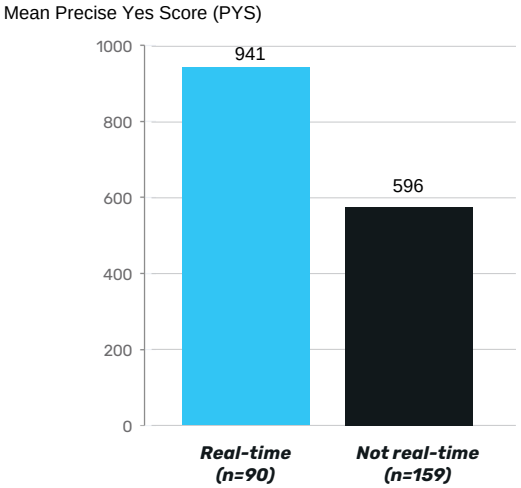
A shared platform does not just eliminate redundancy. It creates the conditions for both teams to bring their expertise to bear on the same signal at the same time - which is precisely what use case co-ownership requires in practice. The data and the collaboration are not separate initiatives. They depend on each other.

**Both teams are already looking at the same signals.**
**The question is whether they are looking together or separately.**

## VIII Real-Time Distinction: What CISO Involvement Can Unlock

There is one capability that separates high-performing organizations from the rest - and it is one that CISO involvement is uniquely positioned to deliver.

Our research asked organizations whether they could distinguish between a cybersecurity attack and a fraud attack in real-time. 36.4% said yes. The remaining 63.6% - whether they could only distinguish after the fact or could not distinguish at all - could not do so when it mattered most.




Organizations that can distinguish a cyber attack from a fraud attack in real-time record a mean Precise Yes Score of 941 - 58% higher than the 596 recorded by those that cannot. The difference is directionally significant (p=0.058).

***Source:*** Accertify-Liminal Study on Fraud-Cyber Convergence, 2026

This capability is not a fraud operations capability. Knowing in real-time that a site is under active credential stuffing - rather than discovering it in a report the following morning - is what a security operations center does. It requires threat intelligence infrastructure, incident response workflows, and cross-signal visibility that sit squarely in the CISO's domain.

This is the affirmative case for CISO involvement that the use case data points toward but does not fully articulate. CISO-owned organizations lead on structural integration, data sharing, and board visibility - the pillars a CISO can drive from the top down. The missing piece is use case co-ownership, which cannot be mandated. But the performance data on real-time distinction shows what becomes possible when the CISO's threat visibility is genuinely integrated with the fraud team's operational response. That integration is what 63.6% of organizations have not yet achieved - and it is what the convergence sequence, executed in the right order, is designed to build.

**63.6% of organizations cannot distinguish a cyber attack from a fraud attack in real-time. The ones that can perform 58% better on fraud outcomes.**

## IX The Convergence Sequence Is the Strategy

The case for CISO involvement in fraud remains sound. The left-of-boom advantage is real. The kill chain visibility is real. The ability to link investments directly to downstream fraud outcomes - and tie security spending to measurable financial results - is a genuine and historically underutilized lever.

But our data suggests that how that involvement is structured matters a great deal. Taking ownership of fraud on the org chart without first building shared use case accountability between fraud and cyber teams does not produce the outcomes the logic promises. It reorganizes the structure without changing real-world working relationships, and the data reflects that gap.

The shared signal picture makes this even more pointed. Both teams are already working from the same underlying data - identity signals, device signals, network signals - but in most cases interpreting them through separate platforms. The performance gap between organizations that can distinguish attacks in real-time and those that cannot (941 vs. 596 PYS) shows what becomes possible when that parallel work becomes joint work.

For CISOs who have already reorganized fraud under security, the data is not an indictment - it is a diagnostic. The structural move is not wrong. It may simply have arrived before the operational collaboration that makes it work. The most urgent priority now is building use case accountability, not unwinding what has been built. Assign joint ownership to both fraud and cyber teams for ATO and customer authentication, or for CNP fraud and credential stuffing. Those two pairs produce the strongest performance lift when shared. With that collaboration established, the data pipeline and board visibility tend to follow naturally. The org chart, in that case, reflects a convergence that already exists in practice - and the real-time attack distinction that 63.6% of organizations are missing becomes achievable.

## Read the Full Research. Request a Briefing.

**The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. Based on 250 senior fraud and risk decision-makers across five industries. Download the report or contact your Accertify representative to request an executive briefing and map your organization against the convergence maturity framework.**

**Accertify enables commerce by doing one thing extraordinarily well: pinpointing fraud.**
The company's Predictive Yes Platform helps businesses say yes to more - more good customers, more revenue, and more growth - without getting burned. It's a precise, confident, data-backed yes, made possible by joining signals across the entire customer lifecycle through unmatched data volume, layered AI-powered models, and a consortium approach that protects clients from bad actors spotted anywhere in the network while unlocking business with good actors verified anywhere in the network. With more than 10 billion transactions and over $1 trillion in commerce processed in 2025 alone, Accertify delivers the intelligence and precision that fraud and payments teams need to say yes confidently and enable growth. That's the More Yes difference. Learn more at **accertify.com**.

Accertify