Third-Party Risk as Operational Accountability

This article is part of a series expanding on the themes explored in **Executive Brief: The Meditology 2026 Healthcare Security Outlook**. Each installment takes a deeper look at the strategic priorities shaping healthcare cybersecurity in 2026, drawn from executive interviews with CISOs and senior security leaders across the industry.

MEDITOLOGY SERVICES

EXECUTIVE SUMMARY

- **Metric Shift:** Third-party risk shifts from questionnaire compliance to measurable impact on operational continuity and care delivery.
- **The Goal:** Moving from "Did the vendor pass assessment?" to "Can this vendor disrupt critical clinical and business operations?"
- **The Bottom Line:** Organizations that treat vendor risk as operational accountability reduce systemic failures, strengthen resilience, and protect revenue and patient safety.

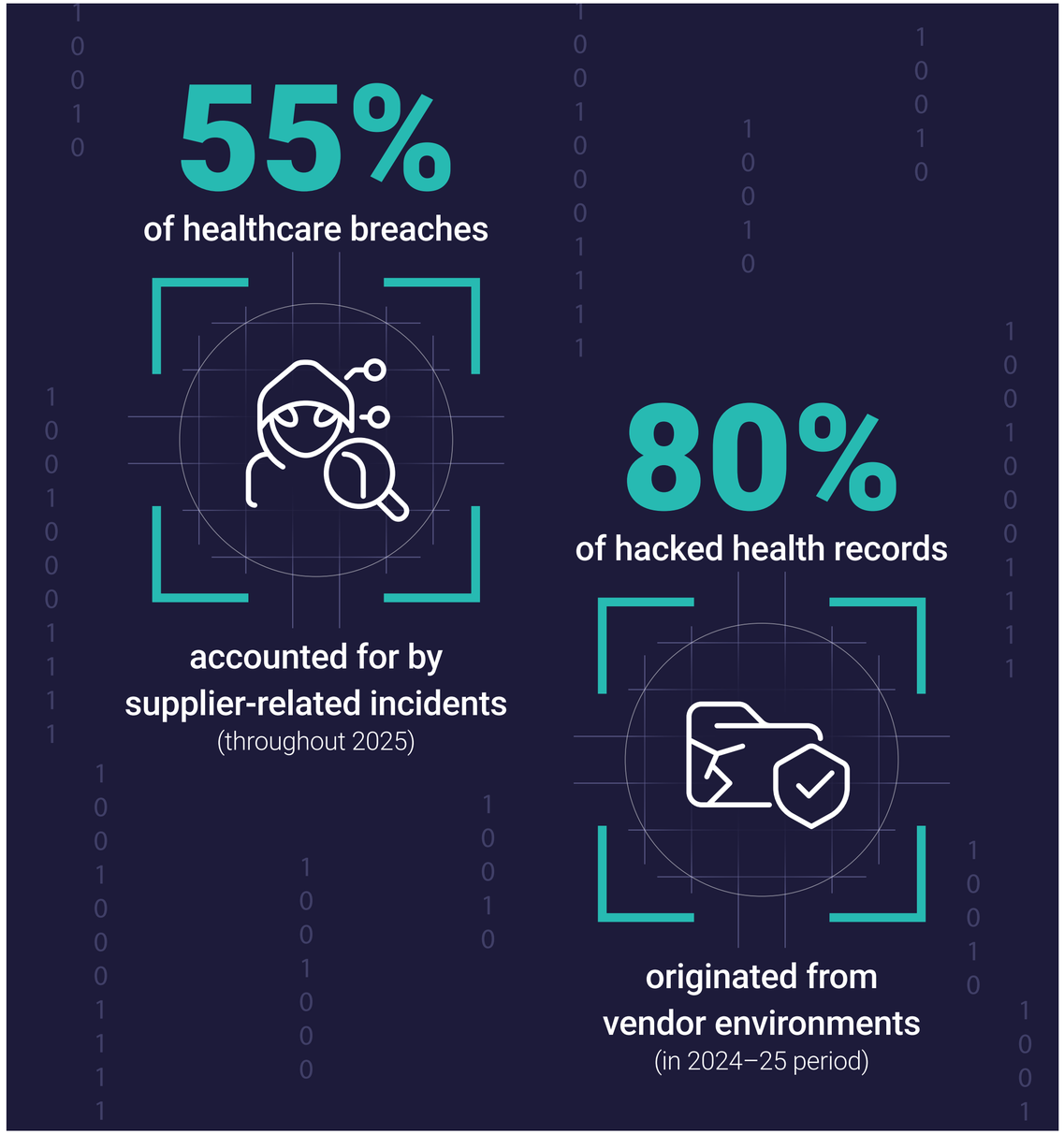
Across our interviews with CISOs and senior security leaders for the *2026 Healthcare Security Outlook*, the assessment was blunt: **the traditional model of Third-Party Risk Management is functionally broken.**[1]

This is old news…and yet we have not solved the problem. In February 2024, a ransomware attack struck Change Healthcare, a subsidiary of UnitedHealth Group that processes roughly 15 billion healthcare transactions per year. The breach affected an estimated 190 million individuals, making it the largest healthcare data breach in U.S. history.[2] But the statistics, staggering as they were, understated the real damage. Claims adjudication ground to a halt. Pharmacy dispensing was disrupted. Revenue cycle operations across the country seized up for weeks. Thousands of healthcare organizations that had no direct relationship with the threat actors found their operations crippled because a single vendor they depended on was compromised.

Change Healthcare did not just expose

data. It exposed a structural flaw in how healthcare manages vendor risk. And it elevated third-party risk from a compliance exercise to a board-level existential concern virtually overnight.

The lesson did not fade. Throughout 2025, supplier-related incidents accounted for over 55 percent of healthcare breaches,[3] and over 80 percent of hacked health records in the 2024 to 2025 period originated from vendor environments rather than organizations' own systems.[4] Yet the way most organizations manage that risk has not kept pace.



The Questionnaire Trap

For more than a decade, the standard approach to vendor risk management in healthcare has centered on self-reported assessments with 200 or more questions sent to vendors, often annually, asking them to attest to their own controls and practices. The responses are reviewed, scored, and filed, with little independent validation or ongoing context. The cycle repeats.

The CISOs we interviewed were unanimous in their frustration. The process is overhead-intensive, consumes enormous staff cycles, and produces very little actionable insight. The response to the questionnaire tells an organization whether a vendor claims to have a firewall. The responses do not reveal how that vendor connects into the organization's network, what data flows exist, or what happens operationally if that vendor went offline. Precisely the kinds of questions Change Healthcare forced every health system in the country to answer in real time.

> "A questionnaire doesn't tell me how a vendor connects into my network."
>
> — Healthcare CISO

The Conduent breach of 2025 drove the point home. Conduent Business Services is a backoffice processor that handles Medicaid claims, benefits disbursement, and healthcare data on behalf of state agencies and insurers. The SafePay ransomware group maintained unauthorized access to Conduent's systems for nearly three months before discovery, exfiltrating approximately 8.5 terabytes of sensitive data.[5] What initially appeared to affect roughly 4 million people eventually ballooned to over 25 million Americans, adding it to the list as one of the largest healthcare breaches in U.S. history.[6]

Critically, Conduent had standard certifications and passed typical vendor due diligence. Security analysts observed that vendor assessments based on SOC 2 reports and security questionnaires may have provided false confidence.[7] The questionnaires said Conduent was compliant. The breach said otherwise.

From Questionnaires to Operational Accountability

Forward-looking organizations are not abandoning vendor risk management; they are reinventing it. The shift is away from compliance-driven data collection via self-attestation questionnaires and towards a model built on operational accountability and supply chain resilience.

Focus on the Critical Vendors

Mature programs are moving away from treating all vendors equally and instead tiering vendors based on the operational risk they pose to care delivery. The traditional model applies the same assessment process to every vendor, using the same 200-question questionnaire whether the vendor handles a peripheral analytics function or serves as the backbone of the organization's claims adjudication system. That approach spreads resources too thin and fails to apply scrutiny where it matters most.

The most sophisticated approach begins not with the vendor, but with critical business process identification: which processes must the organization protect at all costs? One CISO described starting with the five most critical processes such as acute care delivery, claims adjudication, pharmacy operations, and others, and then mapping the vendors underpinning each to create a "vendor bill of materials." This

produces a tiered view of vendor criticality based on operational risk to care delivery, not just data sensitivity or contract size.

This approach concentrates deep scrutiny on the 10 to 20 vendors that provide 80 percent of critical service capacity. Those vendors face heightened, ongoing oversight including architectural risk reviews, continuous monitoring, inclusion in tabletop exercises, and direct integration into the organization's business continuity plans. One CISO described the target state: the most critical vendors face a level of scrutiny that creates a stickier commercial relationship and stronger mutual accountability. Vendors that meet the standard become more deeply embedded partners. Vendors that refuse to meet the standard risk being replaced.

The broader vendor population, the hundreds or thousands of lower-tier suppliers, is managed through lighter-touch mechanisms: certification reliance, continuous risk scoring, and industry-shared assessment data. The goal is not to ignore these vendors, but to stop spending the same resources on a peripheral analytics tool that you spend on the platform processing your pharmacy claims.

Had this tiered model been standard practice before 2024, more organizations would have recognized that Change Healthcare was not just a payment processor; it was embedded across claims adjudication, pharmacy dispensing, and revenue cycle operations at a scale that made its compromise a systemic event. And had organizations mapped their back-office dependencies with the same rigor, Conduent's role as the processing backbone for state Medicaid programs and health insurers would have surfaced as a concentration risk long before SafePay exploited it.

The Small-Vendor Blind Spot

Tiering by operational risk also exposes a counter-intuitive vulnerability that several CISOs described: the greatest risk often comes not from the large, well-known technology companies but from small, niche health-tech firms. These organizations, often 50-person companies building specialized clinical tools, frequently require access to large volumes of protected health information by virtue of their clinical function, yet lack the resources and maturity to maintain robust security programs. The asymmetry is stark: high data access, low security investment.

This represents one of the industry's most persistent blind spots. Because Third-Party Risk Management (TPRM) programs have historically focused their deepest scrutiny on the largest vendors by contract value, these smaller firms often receive the lightest

assessment despite carrying significant operational and data risk. A niche radiology AI startup with access to your entire imaging archive may get a cursory questionnaire, while your EHR vendor, which already holds a HITRUST certification, gets the full architectural review. The risk allocation is backwards.

The pattern played out repeatedly in 2025, with billing firms, diagnostic providers, and niche technology companies serving as entry points for attacks affecting millions of patients.[8] Addressing this gap requires that vendor tiering be driven by operational risk and data access, not contract size, and that small vendors with outsized access to PHI receive scrutiny proportional to the risk they actually carry.

Exchange Questionnaires for Architectural Reviews and Certifications

For top-tier vendors, leading organizations are replacing questionnaires with architectural risk reviews that examine how a vendor integrates with clinical and administrative systems including data flows, network connectivity, authentication mechanisms, and the operational dependencies affected during an outage. The goal is to understand the vendor's real-world risk posture in the specific context of the organization's environment.[9]

Alongside these reviews, organizations are increasingly requiring vendors to demonstrate security maturity through independent certifications or attestations such as HITRUST, SOC 2, ISO 27001, rather than self-reported questionnaire responses.

However, as the Conduent breach demonstrated, a certification alone is not sufficient and the type and breadth of certification or attestation matters. CISOs cautioned that scope varies significantly, and organizations must verify that any certification covers the specific services and data flows relevant to their use case. A SOC 2 that covers a vendor's corporate email environment does not tell you anything about the security of the system processing your Medicaid claims.

Beyond Third Parties: The Nth-Party Problem

The risk does not stop with an organization's direct vendors. It extends to the vendors' own supply chains including the nth-party layer where visibility drops to near zero.[10]

Both Change Healthcare and Conduent illustrate this dynamic from different angles. Change Healthcare was an nth-party problem for many of the organizations it affected. Most health systems did not contract directly with Change Healthcare but were exposed through clearinghouses or EHR platforms that relied on its infrastructure.

Conduent presented a similar pattern: the 25 million affected individuals were predominantly Medicaid recipients and state benefits enrollees who had no idea their data was being processed by Conduent. Their state agency or insurer contracted with Conduent; the individuals were downstream victims of a vendor relationship they never knew existed.

Contract language and right-to-audit clauses, while necessary, proved insufficient to manage this exposure in either case. The organizations making the most progress are integrating vendor risk outputs directly into business continuity planning and executive risk reporting and including critical vendors in tabletop exercises that test the full chain of dependencies, not just the first link.

Scaling TPRM Without Burning Out the Team

Every CISO we spoke with acknowledged the same fundamental tension: vendor ecosystems are expanding faster than internal risk teams can scale. This is why many view TPRM as the most outsource-ready function within cybersecurity. The work is process-driven, operationally heavy, and difficult to staff internally. Co-managed models where an external partner handles the volume of vendor outreach and assessment while the organization retains governance and decision authority are gaining traction across the industry.[11]

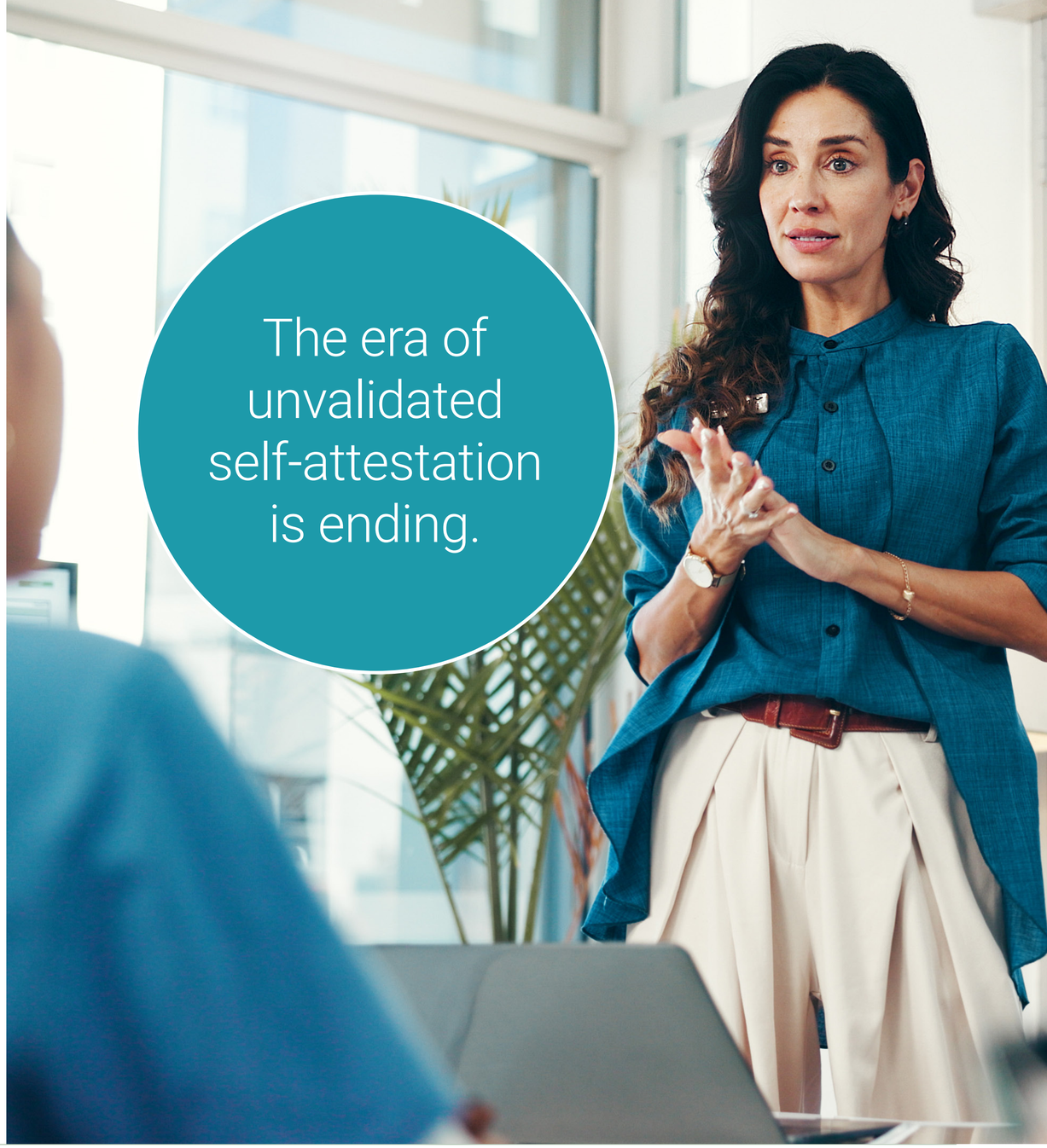
The critical boundary is clear: risk execution can be externalized, but risk ownership cannot be delegated. The final determination of whether a vendor's risk is acceptable is a business decision that must remain with the organization.

A New Standard for Vendor Risk

Change Healthcare was a turning point. Conduent confirmed the pattern. Together, they demonstrate that healthcare's supply chain is its most exposed attack surface, and that the traditional tools for managing that exposure are not working. Questionnaires did not prevent either breach. Certifications did not flag the risk. The organizations that were best prepared were those that had mapped their vendor dependencies to critical business processes and tested their resilience plans before the crisis arrived.

The organizations that will thrive are those that reimagine vendor risk management as an operational accountability function rooted in understanding how vendors connect to critical business processes, verified through architectural reviews and independent certifications, and integrated into the enterprise's broader resilience strategy.

The questionnaire era is ending. What replaces it will determine whether healthcare's supply chain becomes its greatest vulnerability or a source of genuine operational strength.



About Meditology Services and this Research

Meditology Services is a healthcare-exclusive cybersecurity advisory firm. As the facilitator of this research and a trusted partner to hundreds of healthcare organizations nationwide, Meditology translates peer insights into actionable programs that accelerate security program maturity.

To execute on the strategic priorities outlined in this report, Meditology partners with healthcare organizations across critical areas:

Operationalize Resilience & Third-Party Risk (TPRM)

Transition from reactive vendor assessment to proactive supply chain resilience through architectural risk reviews, continuous monitoring, and vendor integration into business continuity planning.

Achieve Industry-Standard Certifications

Pursue HITRUST certifications and SOC 2 attestations to provide validated proof of security maturity to partners, patients, and regulators.

Validate Security Through Continuous Technical Testing

Replace point-in-time assessments with continuous testing and ethical hacking to ensure controls remain effective against an evolving threat landscape.

Establish AI & Emerging Technology Governance

Proactively manage the risks of AI adoption through AI risk program and governance frameworks that ensure innovation does not outpace security.

This executive report is based on in-depth executive interviews conducted during January and February 2026 with CISOs and senior cybersecurity leaders representing multi-state integrated delivery networks, academic medical centers, regional and community health systems, health plans, and health technology companies.

Discussion areas included enterprise risk prioritization, budget strategy, vendor governance, security operations, regulatory readiness, and emerging technology risk. All findings are reinforced by Meditology's proprietary data derived from hundreds of healthcare cybersecurity engagements conducted annually.

Participants included:

- Gillian Lockwood, Director, Information Security, Mass General Brigham
- Matthew Webb, AVP, Cyber Risk Management, HCA
- Zishan Siddiqui, CISO, Sentara Health
- David Finklestein, CISO, St. Luke's University Health Network
- Raj Raju, CISO, Integra Connect
- Denis Tanguay, CIO, Sturdy Health
- Paul Curylo, CISO, Inova Health System
- Among others who requested anonymity.

All insights are presented in aggregate to reflect industry-wide themes rather than the position of any single organization.

1 Meditology Services, Executive Brief: The Meditology 2026 Healthcare Security Outlook. https://meditologyservices.com

2 HIPAA Journal, “Largest Healthcare Data Breaches of 2025,” January 2026. https://www.hipaajournal.com/largesthealthcare-data-breaches-of-2025/

3 CORL Technologies and RiskRecon by Mastercard “Partner to Deliver Continuous, Actionable Third-Party Risk Intelligence for Healthcare,” Business Wire, August 2025. https://www.businesswire.com/news/home/20250820551239/en/

4 Cyber Strategy Institute, “2026 Supply Chain & Third-Party Risk Reality Report – Cybersecurity Threat Landscape,” February 2026. https://cyberstrategyinstitute.com/2026-supply-chain-risk-report/

5 IDStrong, “What You Need to Know about the Conduent Data Breach,” February 2026. https://www.idstrong.com/sentinel/conduent-data-breach/

6 XeneX, “Conduent Data Breach (2025): What Happened, Who Is Affected & How It Could Have Been Prevented,” March 2026. https://www.xenexsoc.com/blog/conduent-data-breach-2025-what-happened-who-is-affected-amp-how-it-could-have-been-prevented

7 LlamaLab, “Conduent Breach Hits 25M: What Law Firms Need to Know,” April 2026. https://www.llamalab.ai/blog/conduent-breach-25-million-records-healthcare-2026

8 Healthcare Law Insights, “Supply Chain Attacks Expose Vendors and Patient Data,” March 2026. https://www.healthcarelawinsights.com/2026/02/supply-chain-attacks-expose-vendors-and-patient-data/

9 Bank Info Security, “2025 in Health Data Breaches and Predictions for 2026,” December 2025. https://www.bankinfosecurity.com/2025-in-health-data-breaches-predictions-for-2026-a-30321

10 Business Wire, “Meditology Services Expands Third-Party Risk Management Capabilities with Acquisition of CORL Technologies,” November 2025. https://www.businesswire.com/news/home/20251112255203/en/

About This Series

This article is the second in a series of deep dives from the **Executive Summary Brief: The Meditology 2026 Healthcare Security Outlook**. *Upcoming installments will explore modernizing third-party risk management, building AI governance frameworks, and operationalizing GRC programs for healthcare.*

MEDITOLOGY SERVICES

For more information, visit **www.meditologyservices.com** or contact your Meditology engagement team.