Hilco Global

AN ORIX COMPANY

SMARTER PERSPECTIVE: CYBERSECURITY

Data Is Your Most Valueable Untapped Asset - Until It Becomes Your Biggest Liability

By Bob Olsen and Aidan Morrissey

April 2026

The current era of technology and artificial intelligence unlocks fast, exponential growth. Companies are scaling faster than ever, often outrunning their ability to ask the right risk questions before they're asked. The growing trend of market centralization has created a real opportunity for quick acquisition; but underneath it all, sits a large, hidden problem. One that surfaces as litigation exposure, state enforcement actions, and in M&A contexts, a direct tax on deal valuation that can cost millions.

When a PE firm or strategic investor comes in, the most problematic questions are typically ones that companies are least prepared to answer. Not revenue, nor customer concentration. The uncomfortable ones are quieter: Can you show us your data inventory? Which systems and vendors have access to PII? Do you have a concrete risk-balanced strategy governing the use and storage of valuable customer data? Is your data mapped cleanly enough to support risk-informed decision-making and built to maximize the return as an actual asset?

These are not just compliance questions, they are revenue questions. Major revenue growth, propelled by data monetization, depends on clean and organized data. These gaps are overlooked, and when they are, they create both a governance liability and a significant missed opportunity to drive value creation. This

is not a startup problem or an enterprise problem. It belongs to every organization in between, those that grew fast, added SaaS tools every quarter, accumulated customer data across a dozen systems, and never had a forcing function to get organized.

Why This Stage Is Different

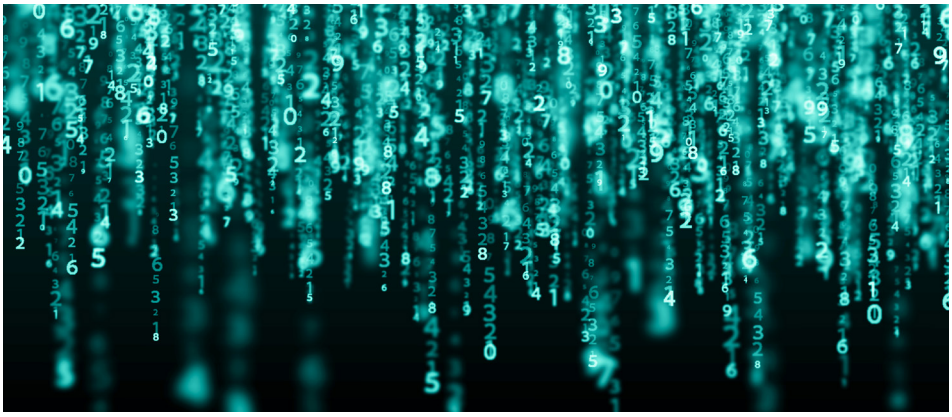
Often, startups get a pass: culturally if not legally. They are moving fast, the regulation spotlight is elsewhere, and investors have yet to ask the hard questions. Enterprises have legal teams, privacy officers, and the institutional memory to sustain governance programs over time.

Mid-market organizations exist in a governance no-mans land. They have accumulated the data complexity of a large organization -- sprawl across legacy systems, multiple SaaS platforms, and a web of third-party vendors, but they still operate with startup era policies and documentation habits. At this stage, that mindset becomes expensive.

What the Gap Actually Looks Like

The data inventory problem is nearly universal; if one exists, it is rarely in a state that can actually be leveraged. Most mid-market organizations can tell you where their CRM data lives yet cannot tell you where the data flows, how it is processed downstream, what strategies would optimize its ROI, or what risks should be guiding revenue generating decision making.

AdTech and tracking technology compliance issues have compounded into a regulatory and civil nightmare. These tools have become major revenue-generating infrastructure for many organizations — sometimes eclipsing what was originally considered the company's core purpose. But their risk



profile is almost never properly understood or documented. A 2025 peer-reviewed study published in the Proceedings of the ACM SIGSAC Conference on Computer and Communications Security analyzed the top one million websites and found Meta Pixel — one of the most litigated tracking technologies in this space — present on nearly one in five. More concerning, 65.45% of those sites were actively configured to transmit personally identifiable information to Meta, including email addresses, phone numbers, names, and geolocation data, in most cases without meaningful user awareness.[1] The enforcement and civil litigation exposure that follows — CCPA, VPPA, CIPA, and an expanding patchwork of state wiretapping statutes — is well-documented and accelerating.

In practice, when an investor's technical team runs a technology audit, it is not uncommon to find 15, 20, sometimes more undocumented tracking technologies operating without proper consent management. That's not a theoretical risk. It's a line item. And it lands in the deal structure accordingly.

The Moment of Reckoning

Data governance gaps don't stay internal forever — when they surface, the context determines whether they become a growth obstacle, a deal liability, or a regulatory event. A new enterprise customer in a regulated industry sends a security questionnaire. A vendor asks for a DPA. A data subject submits an access request under CCPA and the company realizes it can't actually locate all of their data.

Each of these is the same underlying event: an external party is demanding evidence of governance that does not exist. And the cost is not just the scramble to produce answers on a compressed timeline. Where data risks cannot be reliably scoped, investors and acquirers may require additional diligence phases or condition closing on the implementation of baseline data governance controls, which can mean delayed timelines, reduced valuations, or deal structures that shift risk to the seller through escrow holdbacks and indemnification clauses.[2]

The remediation work doesn't disappear. It gets deferred, on someone else's timeline, at someone else's price.

Reframing the Problem

Data governance at this stage isn't a compliance investment, rather, it is one of valuation.

The data sitting inside a mid-market company is simultaneously its most underleveraged asset and its most underestimated liability: often at the same time. A well-mapped, well-governed data estate enables real monetization: cleaner segmentation, defensible attribution, faster enterprise sales cycles, and the ability to actually answer an investor's diligence questions on day one. An unmapped, ungoverned one creates exactly the exposure described above, and discounts the very asset the company thinks it's being valued on.

Well leveraged governance separates a data asset from a data liability on a cap table. The companies that internalize that distinction before an investor asks the question will transact on their terms. The ones that do not will fund the remediation out of their own pockets.

Sources:

[1] Passive Identification of Personally Identifiable Information Leakage through Meta Pixel

[2] How to Spot Data & Cybersecurity Risks That Impact M&A Transactions

BOB OLSEN, MBA, MS, CISSP, CCSP
MANAGING DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Bob can be reached directly at rolsen@hilcoglobal.com.

AIDAN MORRISSEY
DIRECTOR
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Aidan can be reached directly at *amorrissey@hilcoglobal.com.*