STRUCTURAL INTELLIGENCE BRIEF

Information

NAICS 51 | Critical Infrastructure (IT Sector)

THINNESS	PERMISSION	MANAGEMENT	ABSENCE
VULNERABLE	VULNERABLE	STRAINED	VULNERABLE

S.J. Bridger
Four Frequencies Framework

April 2026
sjbridger.com/intelligence/information/

Executive Summary

The Information sector is the structural backbone of every other sector's digital operations, yet it exhibits the same fragility patterns it is supposed to help others avoid. Platform concentration has reached levels where a handful of companies control the infrastructure that the rest of the economy depends on: three cloud providers hold 67% of global market share, two companies capture over 50% of digital advertising revenue, and three carriers control more than 95% of U.S. wireless subscriptions. That concentration has not produced stability. It has produced structural dependency at scale.

This brief applies the Four Frequencies diagnostic framework to the U.S. Information sector (NAICS 51) using 16 federal and industry data metrics from BLS, FCC, DOJ, FTC, and CISA. It identifies structural conditions that organizational leaders inside this sector inherit whether or not they recognize them. The severity scores are not predictions. They are measurements of conditions that already exist.

> *Three of the four frequencies score VULNERABLE. The remaining frequency scores STRAINED. No frequency in the U.S. Information sector scores STABLE.*

THINNESS	PERMISSION	MANAGEMENT	ABSENCE
VULNERABLE	VULNERABLE	STRAINED	VULNERABLE

Sector Structural Profile

The Information sector (NAICS 51) encompasses software publishing, telecommunications, data processing and hosting, broadcasting, motion picture and sound recording, and traditional publishing. CISA designates the IT Subsector as critical infrastructure under PPD-21, with the FCC serving as Sector Risk Management Agency for Communications. The sector comprises approximately 162,000 establishments, employs 3.4 million workers, and generates over $2.2 trillion in annual revenue.

Platform Concentration

The structural story of the Information sector over the past decade is concentration through platform dominance rather than traditional horizontal consolidation. Google and Meta together capture over 50% of U.S. digital advertising revenue. Amazon Web Services, Microsoft Azure, and Google Cloud hold approximately 67% of global cloud infrastructure market share. In wireless telecommunications, the top three carriers control more than 95% of subscriptions following the T-Mobile/Sprint merger.

This concentration operates differently from healthcare or manufacturing consolidation. Platform economics create winner-take-most dynamics where network effects, data advantages, and ecosystem lock-in concentrate structural power in ways that traditional antitrust metrics struggle to capture. The DOJ's August 2024 finding that Google operates an illegal monopoly in search confirmed what structural analysis

had already revealed: market share figures understate the actual structural dependency.

Workforce Paradox

The Information sector presents a structural paradox: it simultaneously produces mass layoffs and reports critical workforce shortages. Technology companies laid off 152,922 workers in 2024 and another 124,201 through early 2025 (Layoffs.fyi), while ISC2 reports 4.76 million unfilled cybersecurity positions globally. The layoffs are concentrated in mid-career knowledge workers. The shortages are concentrated in specialized security, infrastructure, and legacy system roles.

This is not a simple supply-demand mismatch. It is a structural reallocation: capital is moving from human workforce to AI infrastructure, with major platforms tripling AI capital expenditure toward a projected $1.4 trillion by 2027. The workforce that remains operates under median tenure of 1.3 to 1.9 years at major technology companies, creating an institutional knowledge drain that no hiring pipeline can offset.

Four Frequency Assessment

The Four Frequencies framework measures structural resilience across four dimensions of organizational and sector health. Each frequency captures a distinct pattern of structural vulnerability. Severity scores reflect the current state of measurable conditions, not projections or sentiment.

THINNESS	VULNERABLE

Thinness measures the structural depth of critical capacity. In the Information sector, it surfaces as platform dependency, infrastructure concentration, workforce knowledge gaps, and the erosion of entire subsector ecosystems.

The evidence for VULNERABLE is layered. Cloud infrastructure concentration means that an outage at any one of three providers can cascade across industries that have built their digital operations on that platform. The 2024 CrowdStrike incident demonstrated the structural consequence: a single software update propagated through concentrated infrastructure and disabled 8.5 million Windows devices globally. That is not a technology failure. It is a thinness failure, where insufficient structural depth meant there was no alternative pathway when the primary one broke.

Local news infrastructure has thinned to the point of structural absence. Newspaper employment has fallen 82% since 1990. The United States now has 213 counties with no local news outlet at all, and over 50 million Americans live in areas with severely limited local news access. Information infrastructure is not just digital. The collapse of local journalism removes the verification layer that communities depend on for institutional accountability.

Thinness in the Information sector operates at two scales simultaneously: platform concentration thins the digital infrastructure layer, while local news collapse thins the civic information layer. Both create single points of failure.

PERMISSION — VULNERABLE

Permission measures how structural conditions distribute or concentrate decision authority and autonomy. In the Information sector, it surfaces as platform gatekeeping power, regulatory fragmentation, and the structural asymmetry between those who control digital infrastructure and those who depend on it.

The DOJ's August 2024 ruling confirmed that Google operates an illegal monopoly in search distribution. The proposed Chrome divestiture was rejected by Judge Mehta in September 2025, but the court imposed search distribution deal restrictions and mandatory index data sharing with competitors. The structural reality these rulings reveal: a single company's decisions about search ranking, advertising placement, and data access shape what information reaches billions of users. That is Permission concentration at civilizational scale.

The regulatory environment is fragmenting in ways that compound Permission strain. The EU has imposed fines under the Digital Services Act (120 million euros against X) and Digital Markets Act (500 million euros against Apple, 200 million euros against Meta). The AI Act introduces penalties up to 7% of global turnover. Domestically, 20 states have enacted comprehensive privacy laws with varying requirements. The AI safety governance ratio stands at approximately 10,000 to 1: for every dollar spent developing AI capabilities, a fraction of a cent goes to safety governance. Permission is VULNERABLE because the structures that should distribute decision authority are either too concentrated or too fragmented to function.

MANAGEMENT — STRAINED

Management frequency measures how structural conditions shape leadership effectiveness, operational coordination, and the capacity to execute strategy under pressure. In the Information sector, it surfaces as capital allocation distortion, technical debt accumulation, and the structural gap between investment velocity and organizational capacity.

The AI capital expenditure race is the defining Management pressure. Major technology companies are tripling AI infrastructure spending toward a projected $1.4 trillion by 2027, while simultaneously executing the largest workforce reductions in the sector's history. This is not a contradiction from a capital allocation perspective. It is a structural bet that AI infrastructure will replace the human capacity being removed. Whether that bet pays off is an open question. What is measurable today is that 40% of IT budgets are consumed by maintaining existing technical debt, leaving less than 60% for the transformation these investments are supposed to enable.

Venture capital dynamics amplify the strain. Approximately 75% of venture-backed companies never return invested capital, and 90% of startups fail outright. The sector's innovation model structurally depends on a high failure rate, but those failures consume management capacity, workforce talent, and institutional knowledge that do not regenerate. When a startup fails, the organizational learning it accumulated typically disperses. The sector's management structures are STRAINED because they are attempting to execute a generational technology transition while carrying the accumulated weight of deferred maintenance and structural workforce instability.

ABSENCE **VULNERABLE**

Absence measures what happens when structural conditions create gaps in critical functions, and what fills those gaps. In the Information sector, it surfaces as workforce displacement patterns, institutional knowledge evaporation, cybersecurity capacity deficits, and the disappearance of entire information infrastructure layers.

The 277,000 technology layoffs across 2024-2025 are not a cyclical correction. They represent a structural reallocation of capacity from human knowledge workers to AI infrastructure. Median tenure at major technology companies ranges from 1.3 to 1.9 years. At that velocity, institutional knowledge does not accumulate. It passes through. Each departure removes context that documentation cannot capture and onboarding cannot replace. The cybersecurity workforce gap of 4.76 million unfilled positions globally (ISC2) means the sector responsible for protecting digital infrastructure cannot staff its own defense functions.

These frequencies do not operate independently. In the Information sector, they compound. Thinness (concentrated infrastructure) intensifies Absence (when a platform fails, there is no alternative). Permission concentration (platform gatekeeping) reduces the adaptive capacity of dependent organizations. Management strain (AI transition costs plus technical debt) prevents the sustained investment required to build structural depth. The four frequencies form a self-reinforcing loop where concentration enables efficiency gains that fund further concentration, while the structural resilience required to sustain that concentration erodes.

> *When the sector responsible for building digital resilience across the economy cannot maintain structural depth in its own workforce, infrastructure, or governance systems, the vulnerability propagates to every sector that depends on it.*

Federal Data Evidence Base

This assessment draws on 16 metrics from federal agencies and authoritative industry sources. Each metric maps to one or more Four Frequencies dimensions. The data is publicly available; the structural interpretation through the Four Frequencies lens is proprietary.

Source	Metric	Key Finding
BLS / QCEW	Establishment count (NAICS 51)	~162,000 establishments
BLS / OES	Sector employment	3.4 million workers
Census	Annual sector revenue	Over $2.2 trillion
DOJ	Search market concentration	Google illegal monopoly (Aug 2024)
Statista	Digital ad revenue concentration	Google + Meta > 50% of market
Synergy	Cloud infrastructure market share	Top 3 providers hold 67%
FCC	Wireless subscription concentration	Top 3 carriers > 95%
BLS	Newspaper employment decline	78,800 employed; down 82% since 1990
Medill	News desert counties	213 counties with zero local news
ISC2	Cybersecurity workforce gap	4.76 million unfilled globally
Layoffs.fyi	Tech sector layoffs	152,922 (2024) + 124,201 (2025 YTD)
LinkedIn	Big Tech median tenure	1.3 to 1.9 years
EU Comm.	DSA / DMA enforcement	EUR 820M+ in fines imposed
NCSL	State privacy law adoption	20 states with comprehensive laws
IDC / Co.	AI capital expenditure trajectory	Tripling toward $1.4T by 2027
FCC	Rural broadband penetration	72% vs 98% urban

Sources: Bureau of Labor Statistics (BLS), Federal Communications Commission (FCC), Department of Justice (DOJ), Federal Trade Commission (FTC), Cybersecurity and Infrastructure Security Agency (CISA), U.S. Census Bureau, European Commission, National Conference of State Legislatures (NCSL), ISC2 Cybersecurity Workforce Study, Medill School of Journalism, Synergy Research Group, IDC, Company filings.

Structural Risk Scenarios

Structural conditions do not predict specific events. They define the envelope of probable outcomes. The following scenarios are structurally plausible given current conditions. They are not forecasts. They are the shapes that failure takes in a sector with this structural profile.

Cascade Scenario: Cloud Provider Disruption

A major cloud provider experiences a sustained outage exceeding 48 hours due to a coordinated cyberattack or infrastructure failure. With three providers controlling 67% of global cloud infrastructure, dependent organizations across every sector lose access to critical business systems simultaneously. The structural conditions that made this scenario possible: infrastructure concentration that created single points of failure, a cybersecurity workforce gap that left defensive capacity understaffed, and institutional knowledge turnover that degraded the depth of operational response teams. The CrowdStrike incident of July 2024 demonstrated this pattern at smaller scale.

Compounding Scenario: Information Desert Expansion

Local news contraction crosses a threshold where remaining outlets cannot sustain operations. Advertising revenue that once supported local journalism has structurally migrated to platform intermediaries. The 213 counties already without local news coverage expand to 400 or more. Communities lose the verification infrastructure that holds local institutions accountable. The compounding effect: without local reporting, institutional dysfunction goes undetected until it produces visible failure. Municipal governance, healthcare systems, and educational institutions in news deserts operate without the external scrutiny that serves as an early warning system.

Structural Freeze Scenario: AI Transition Stall

AI capital expenditure reaches projected levels but fails to produce proportional productivity gains. Organizations that laid off experienced workers to fund AI infrastructure find they lack the institutional knowledge to integrate AI systems effectively. The 40% of IT budgets consumed by technical debt remains unresolved because the engineers who understood legacy systems were among those laid off. Venture-backed AI companies fail at the historical 90% rate, but each failure consumed workforce talent that does not re-enter the sector. The structural freeze: too committed to AI investment to reverse course, too depleted of human institutional knowledge to execute the transition.

> *Each scenario describes a pattern, not an event. The structural conditions that enable these patterns are measurable today. Whether a specific organization experiences them depends on its internal structural profile, which is what the diagnostic measures.*

The Diagnostic Gap

This brief assesses structural conditions visible from federal data and public sources. The Four Frequencies framework measures 20 dimensions. Sixteen are assessable from public data for this sector. Four require diagnostic access to an organization's internal structural patterns through behavioral intelligence from raters inside the organization.

What Public Data Reveals (16 Dimensions)

The 16 public dimensions capture sector-level structural conditions: platform concentration and market power, workforce supply and displacement patterns, infrastructure dependency depth, regulatory fragmentation, capital allocation trajectory, institutional knowledge velocity, cybersecurity capacity gaps, and information ecosystem erosion. These are the dimensions scored in this brief. They describe the structural environment that every organization in this sector inhabits.

What Requires Diagnostic Access (4 Dimensions)

Institutional Knowledge Mapping

Where critical knowledge actually lives. Sector data shows median tenure of 1.3 to 1.9 years at major technology companies. It cannot tell you which specific knowledge domains have departed your organization or which individuals currently absorb compensatory load for those departures.

Decision Authority Distribution

Who can make which decisions, and how far authority sits from the point of impact. Platform concentration data shows centralization at the market level. It cannot map the internal decision architecture that determines how quickly your organization responds when a critical dependency fails.

Adaptive Capacity Under Stress

How the organization's structural profile changes under pressure. The scenarios in the preceding section describe sector-level patterns. How a specific organization responds depends on dimensions only visible through diagnostic engagement, including the informal networks and workarounds that carry operational load.

Strategic Alignment Depth

Whether stated strategy and actual structural capacity point in the same direction. An organization pursuing AI transformation while its cybersecurity positions remain unfilled and its technical debt consumes 40% of IT budget has a strategic alignment problem that only internal data can quantify.

The gap between what is publicly visible and what is structurally real is where organizational risk lives. The brief tells you the weather. The diagnostic tells you whether your roof can hold.

Methodology

The Four Frequencies framework measures structural resilience across four dimensions: Thinness (depth of critical capacity), Permission (distribution of decision authority), Management (leadership and operational effectiveness), and Absence (gaps in critical functions and their consequences). Each frequency is assessed across five dimensions, for a total of twenty structural measurements.

Sector-level assessments draw on federal data mapped to the publicly-measurable dimensions. Organization-level diagnostics add behavioral intelligence from internal raters to score all twenty dimensions. The combination produces the Structural Resilience Index (SRI), a composite score calibrated to a six-band severity scale.

Severity terminology: RESILIENT (structural depth across all frequencies), STABLE (adequate structural capacity with minor gaps), STRAINED (measurable structural pressure in one or more frequencies), VULNERABLE (significant structural gaps with compounding risk), FRAGILE (structural conditions that amplify disruption), CRITICAL (structural failure in progress or imminent).

What This Means for Your Organization

This brief describes the structural environment your organization operates inside. Whether these sector-level conditions are amplified or mitigated within your specific organization depends on your internal structural profile.

The Four Frequencies diagnostic measures all 20 dimensions for a single organization, producing a 40-page structural analysis with the Structural Resilience Index.

sjbridger.com/organizations

contact@sjbridger.com

About S.J. Bridger

S.J. Bridger is a structural resilience diagnostics practice. We analyze the structural conditions that determine whether organizations hold together when key people leave, when systems fail, and when the relationships that carried institutional knowledge disappear. The Four Frequencies framework was developed through forensic analysis of organizational failures across multiple sectors and refined through diagnostic engagements that measure what traditional assessments miss.

Structural Intelligence Briefs are published assessments of sector-level conditions. They are updated quarterly as federal data sources release new information. The Information brief is part of a series covering critical infrastructure and high-structural-risk sectors across the U.S. economy.