MOODY'S

Supply chain insights:

Navigating disruption in pharmaceutical supply chains

Explore some of the forces reshaping healthcare supply chain risk and how disruption is emerging across the sector

$25bn

The annual cost to U.S. hospitals due to avoidable supply chain issues[1]

Introduction

Pharmaceutical supply chains have entered a period of sustained instability in which risk no longer arrives as an isolated incident but as a convergence of simultaneous pressures.

Over the past two years, active drug shortages have been at their highest since tracking began in 2001, with 323 medications in shortage in Q1 2024 alone[2]. These shortages are not anomalies. They reflect decades of decisions that optimized for cost rather than resilience, concentrating manufacturing capacity into a handful of geographies, building lean inventories across critical drug categories, and treating risk management as a compliance obligation rather than an operational capability.

At the same time, cyberattacks, climate-driven disruptions, global trade volatility, and regulatory enforcement have intensified, exposing structural fragility across every tier of the supply chain.

Drawing on recent data, regulatory findings, and real-world incidents, this paper highlights a select number of risk types to show how supply-side vulnerabilities propagate across global networks, and what supply-side pharmaceutical manufacturers may do to stay ahead of accelerating disruption.

THE KEY FINDINGS?

1. **Pharmaceutical supply chains** today are under active, multidimensional threat, and resilience is becoming a strategic capability rather than a defensive reaction.

2. **Geopolitical tensions, cybersecurity threats, and counterfeit drugs** are among the key supplier-related risks.

3. **Organizations are adopting a unified risk management approach** to counter the modern interconnected supply chain risk. Aggregating risk signals into a single unified view helps to break down silos between traditionally separate risk functions.

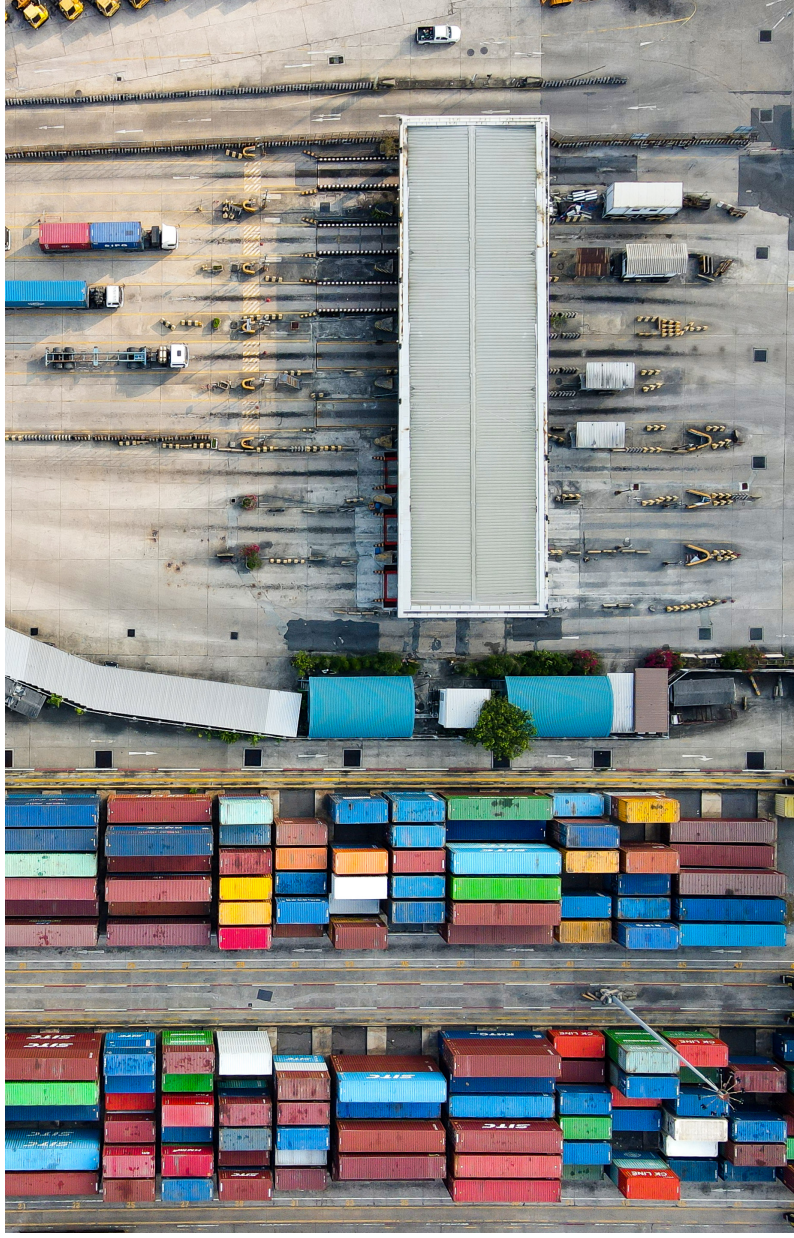
[1]pmc.ncbi.nlm.nih.gov/articles/PMC9986569/

[2]www.ashp.org/drug-shortages

Top risks for pharmaceutical supply chains

Geopolitical tensions and tariffs are reshaping access to essential materials. The Red Sea crisis in 2023 slashed Suez Canal traffic by 66% and more than doubled freight costs, disrupting the movement of Indian generics and extending global lead times.[3] At the same time, tariff actions have pushed active pharmaceutical ingredients (APIs) and input costs sharply higher, with U.S. policy scenarios adding up to $51 billion in annual drug costs.[4]

Similarly, the ongoing conflict with Iran is rapidly creating shockwaves throughout the pharmaceutical supply network as the supply of Indian-sourced APIs is severely restricted. The United States imports nearly 40% of its generic medicines using APIs sourced from India.[5] These APIs are in short supply in the near and longer term, and shortages are compounded by delays from alternate routes, and capacity constraints remain a structural weakness. Meanwhile, warning letters issued by the U.S. Food and Drug Administration (FDA) for drug quality concerns rose to 105 in FY2024 (an 11% increase on the previous year), with many targeting foreign facilities.[6] Quality shutdowns at high throughput sites create prolonged disruption to supply chains. Supplier insolvency can be equally disruptive.



Cybersecurity threats now pose one of the most severe forms of operational risk. In 2023, 133 million U.S. health records were compromised, and cyberattacks on distributors and processors increasingly disrupt the flow of products to hospitals and clinics.[7] The Change Healthcare attack halted claims processing for 70,000 pharmacies, exposed 190 million patient records, and generated more than $1.6 billion in financial impact.[8]

Counterfeit and substandard drugs are proliferating through multi-tier global networks. With the counterfeit market exceeding $200 billion according to the World Health Organization (WHO)[9], weak oversight in upstream tiers and expanding ecommerce channels increase the likelihood of harmful products infiltrating legitimate supply chains. Recent global seizures highlight the scale of the threat.

[3]www.maersk.com/insights/resilience/2024/07/09/effects-of-red-sea-shipping

[4]www.zs.com/insights/us-pharma-policy-strategies-to-future-proof-your-supply-chain

[5]www.linkedin.com/pulse/role-indian-api-manufacturers-global-pharma-supply-es28e/

[6]www.scilife.io/blog/worst-fda-warning-letters-pharma

[7]from www.censinet.com/perspectives/pharmaceutical-supply-chain-vulnerabilities-third-party-risk-lessons-applicable-across-industries

[8]www.unitedhealthgroup.com/investor-relations

[9]truemedinc.com/blog/the-economic-impact-of-counterfeit-healthcare-products/

1. Tariff risk and geopolitical uncertainty

Geopolitics now shapes every stage of the pharmaceutical supply chain. Years of cost-driven consolidation concentrated the production of active pharmaceutical ingredients in China and India and funneled global logistics through a handful of maritime chokepoints. Those decisions created efficiencies, but they also built structural exposure to geopolitical tension, trade policy, and transport disruption. The result is a system where events unfolding thousands of miles away can rewrite manufacturing schedules overnight.

Nowhere was this more visible than during the Red Sea shipping crisis of 2023–2024. Houthi attacks on commercial vessels forced six of the ten largest container carriers to halt or sharply reduce passage through the Red Sea. Traffic through the Suez Canal collapsed by two thirds. Ships rerouted around the Cape of Good Hope, adding close to two weeks and roughly 4,000 miles to each voyage.

For pharmaceutical manufacturers, especially those in India exporting generic medicines to Europe, the effect was immediate: shipping costs more than doubled, lead times stretched, and the just-in-time model that governs much of generic drug production left limited margin to absorb the delay. Leading global financial services firm J.P. Morgan estimated that the crisis cut global container capacity by close to a tenth and added 0.7 percentage points to global core goods inflation in the first half of 2024.[10] A regional conflict had choked the route on which most Indian generics depend, exposing how little buffer the industry has built into its logistics backbone.

The U.S.–China tariff escalation in 2025 underscored similar structural fragility from a different angle. A proposed 25% pharmaceutical import tariff threatened to add nearly $51 billion to annual U.S. drug costs and push consumer prices up by as much as 12.9%.[11] Manufacturers reported double-digit cost increases for staple molecules such as amoxicillin, acetaminophen, and metformin.[12] What's more, freight prices from China to the U.S. West Coast jumped from $3,500 to $6,500 per container.[13] These effects cascaded beyond U.S. border, too. India relies on China for around 70% of its bulk drug imports. Over the same period, freight prices from China to the U.S. West Coast increased from $3,500 to $6,500 per container. The implications cascaded beyond the U.S. border, too. India, which sources around 70% of its bulk drug imports from China, was particularly exposed. In this context, U.S. tariffs on Chinese goods may have functioned as a second-order

[10]www.jpmorgan.com/insights/global-research/supply-chain/red-sea-shipping

[11]www.zs.com/insights/us-pharma-policy-strategies-to-future-proof-your-supply-chain

[12]ibid

[13]ibid

[14]patentpc.com/blog/pharma-supply-chain-disruptions-how-are-drug-shortages-impacting-the-market-latest-stat

shock to India-manufactured generics, with possible knock-on effects for global drug availability. In a sector where 90% of U.S. prescriptions are generics[14], thin margins create a real risk of manufacturer exits when tariff driven costs rise faster than reimbursed prices.

Companies that view disruptions as isolated incidents may remain exposed. Those that treat them as early warning signals—indicating stress in critical routes, suppliers, or policy assumptions—may be better positioned to act before the shock fully materialises. In the case of the Red Sea, the pattern of attacks was visible weeks before carriers withdrew from the corridor.

The long-term takeaway is clear. Pharmaceutical supply chains may benefit from shifting from a model optimized for cost to one built for resilience. Diversification of sources, alternative routing, regionalized production, and real-time geopolitical monitoring can help pharmaceutical companies respond to the operating requirements of a sector that now sits squarely inside the world's geopolitical currents.

2. Manufacturing quality issues and capacity constraints

Regulatory action remains one of the most disruptive forces in pharmaceutical supply chains. A warning letter, Form 483, consent decree, or facility shutdown can take an essential plant offline overnight, abruptly removing capacity. Unlike other disruptions that build gradually, regulatory events can strike suddenly, and in a system already operating close to its limits, even a single enforcement action can trigger sustained shortages across critical drug categories. What's more, regulatory pressure around drug quality has grown, as exemplified by increasing warning letters being issued by the FDA in recent years. When deficiencies are identified, the impact is significant on the global pharmaceutical supply chain: product classes that rely on a handful of qualified sites face near-instant supply-demand imbalance.

The root of this fragility is capacity. Many sterile injectable and high-volume generic facilities already operate above 80% utilization, leaving limited meaningful headroom to offset a shutdown.[15] When a site pauses production for remediation, there is rarely another manufacturer with both the capability and unused capacity to absorb the displaced production. Qualifying an alternative plant can require anywhere between 12 and 24 months for review, far longer than the market can tolerate without interruption. What could be a short-term compliance correction may become a prolonged shortage simply because the system lacks structural redundancy.

The collapse of Akorn Pharmaceuticals in February 2023 illustrates how regulatory consequences can be triggered by financial failure as easily as by quality issues. Although Akorn closed due to insolvency, FDA rules required the immediate recall of its entire product portfolio, eliminating supply across multiple therapeutic categories with no advance warning.[16] In generic markets already strained by thin margins and rising compliance costs, no manufacturer had the capacity or regulatory clearance to backfill the lost volume. Akorn's exit shows that supplier viability and regulatory exposure are often closely related; a financially weakened manufacturer is less able to maintain quality systems, modernize equipment, or withstand compliance pressure.

3. Cybersecurity threats

Digitalization has transformed pharmaceutical operations, helping to improve coordination across manufacturing, regulatory submissions, distribution, and reimbursement. Simultaneously, it has created an expanded attack surface that now extends far beyond the four walls of any single manufacturer. Many significant cyber risks in this landscape increasingly originate from third-party platforms, claims processors, logistics providers, distributors, and IT vendors, whose systems are tightly coupled to the continuity of drug supply.

The rapid adoption of artificial intelligence (AI) across the pharmaceutical sector is extending that exposure in ways the industry has not yet fully mapped. Companies are deploying AI across drug discovery, manufacturing quality control, regulatory documentation, and supply chain optimization, often at speed, and in some cases

[15]www.ncbi.nlm.nih.gov/books/NBK611681/

[16]artofprocurement.com/blog/supply-symptoms-of-disruption-in-the-pharmaceutical-supply-chain

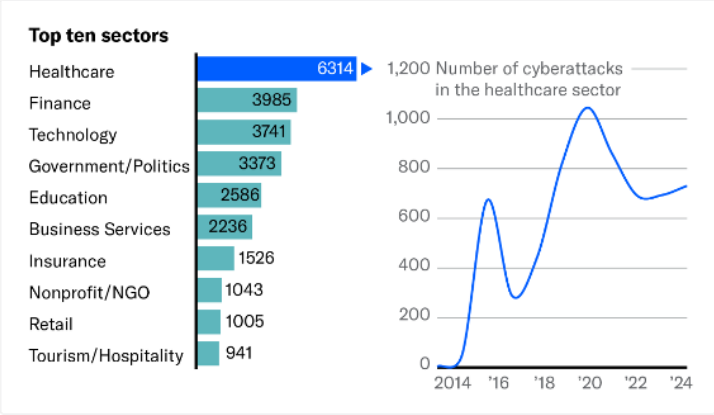
without commensurate investment in AI-specific risk frameworks. The attack surface implications are significant given that AI systems can bring new risk vectors. Indeed, if any vulnerabilities exist in third-party APIs and cloud infrastructure on which most AI deployments depend, then data privacy can be compromised.

The sector has already seen early incidents that have exposed patient data embedded in training sets, and data integrity breaches (which bypass traditional cybersecurity controls) targeting AI-assisted regulatory workflows. Continued investment in the technology ecosystem required to remain compliant and competitive in a world of rapid AI adoption is important to future success, but it exposes companies to a class of threats that existing cybersecurity frameworks were not designed to address.

Multi-year data trends reveal the extent of the industry's exposure. In 2023 alone, cyber incidents compromised 133 million health records in the United States, with the country averaging roughly two major health data breaches per day. The average cost of a breach exceeded $5 million, and organizations took about 257 days on average to detect and contain each incident. A large share of those attacks exploited basic weaknesses: 63% of breaches in pharmaceutical settings were linked to weak access controls, such as missing multifactor authentication or poorly segmented networks.[17] The third-party dimension is equally stark. According to research by Moody's affiliate Bitsight, the majority of cyber breaches involving protected healthcare information since 2022 involved compromised vendors, partners, or other third parties, a finding that reinforces why supply chain integrity and third-party oversight are now increasingly viewed as closely connected to any credible enterprise cyber risk management program in this sector (see exhibit 1 below).[18]

EXHIBIT 1

The healthcare sector has experienced the most cyberattacks since 2022



Source: Moody's affiliate Bitsight

[17]www.censinet.com/perspectives/pharmaceutical-supply-chain-vulnerabilities-third-party-risk-lessons-applicable-across-industries

[18]www.moodys.com/research/Healthcare-Global-Cybersecurity-Healthcare-providers-perform-well-but-gaps-Sector-In-Depth--PBC_1459467#0d1e1c31ef83dfb60e12d0a553a0f418

Case study: Change Healthcare ransomware attack (February 2024)

Affecting over 190 million individuals, the Change Healthcare ransomware attack in February 2024 remains the largest healthcare data breach in U.S. history. The case illustrates how a single digital failure can cascade across the wider healthcare and pharmaceutical ecosystem.

Attackers from the BlackCat/ALPHV group gained entry via a Citrix remote access portal that did not enforce multi-factor authentication and remained undetected for nine days.[19]

Change Healthcare ransomware attack: timeline, root causes, and downstream impact

- → **Feb 12, 2024:** hackers enter Change Healthcare's IT system via a portal lacking multi-factor authentication (MFA).
- → **Feb 21, 2024:** With the hackers finally detected after nine days, Change Healthcare shuttered its platform, halting 50% of U.S. medical claims and disrupting 90% of the chain's 70,000 pharmacies.
- → **March 2024:** Parent company UnitedHealth pays a $22 million ransom, but compromised health records are still published.

When Change Healthcare took its systems offline on 21 February, it temporarily interrupted a platform that processes 50% of all U.S. medical claims and supports more than 100 critical healthcare functions.[20] Over 90% of the nation's 70,000 pharmacies were suddenly unable to process insurance claims. UnitedHealth Group ultimately paid a $22 million ransom, and protected health information (PHI) for an estimated 190 million Americans was exposed, the country's largest ever health data breach.

The operational and financial consequences were significant. Hospitals, many already operating on thin margins, reported daily revenue losses of $1 million or more.[21] In a March 2024 survey of nearly 1,000 hospitals, the American Hospital Association found that 94% reported financial impact, 74% reported direct patient care impact, and 60% needed two to three months to restore normal operations following the attack. UnitedHealth Group estimated the total cost of the incident at $1.35–$1.6 billion and extended more than $6 billion in advance funding and loans to stabilize affected providers.[22]

Root cause

Following its acquisition by UnitedHealth Group, Change Healthcare continued to operate elements of legacy IT infrastructure. In his testimony, UnitedHealth CEO Andrew Witty acknowledged that a critical remote access system "lacked multi factor authentication", meaning attackers gained entry using compromised credentials.

Downstream impact

- → 190 million patient records exposed.
- → $1.6 billion estimated cost to UnitedHealth.
- → Over 70,000 pharmacies disrupted.
- → 94% of hospitals financially impacted

[19]www.medscape.com/viewarticle/change-healthcare-breach-still-affecting-physician-hospital-2026a100083b?form=fpf
[20]www.msspalert.com/news/change-healthcare-cyberattack-event-timeline
[21]www.pharmacytimes.com/view/consequences-of-the-change-healthcare-cyberattack-continue
[22]www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and

In testimony before the U.S. Senate, CEO Andrew Witty stated that the attack succeeded because the organization had "failed to update internal security procedures after the acquisition," underscoring a critical but often overlooked weakness: post-merger security integration.[23] The acquired entity's systems had not been brought up to the parent company's security standard, and remote access infrastructure remained on single factor authentication. With limited redundant claims processing pathway in place, a single compromise materially disrupted a core digital utility across the healthcare system.

For pharmaceutical manufacturers, the Change Healthcare incident exemplifies a supply chain event; not only a healthcare IT story. It illustrates that digital dependencies, including ordering platforms, and third-party logistics systems, are as critical to supply continuity as physical plants and warehouses. A cyberattack on a claims' processor, distributor, or logistics provider can delay shipments, disrupt demand signals, and destabilize revenue flows even when manufacturing lines are operating as expected. In an environment where advanced therapies, biologics, and cold-chain products rely on tightly orchestrated data exchanges from factory to bedside, cyber risk has become a significant factor influencing operational resilience.

The case also reinforces a broader risk intelligence imperative. Mergers and acquisitions in healthcare and pharma can introduce "invisible" cyber exposure when newly acquired systems are connected to core operations without a comprehensive security uplift. Treating post-merger integration as an IT housekeeping task rather than a supply chain risk event may open critical infrastructure to exploitation. Manufacturers that map their digital dependencies, scrutinize the cyber posture of their third-party providers, and integrate security risk into procurement, and M&A decisions may be better positioned to withstand the next attack. Those who don't may face significant operational or financial impacts that ripple across production, distribution, and patient access.

4. Counterfeit drugs

Counterfeit drugs have become a significant challenge to pharmaceutical supply chains, exploiting the very structures designed to ensure safe, consistent access to medicines. These falsified and substandard products, which can mimic legitimate medicines but lack active ingredients, contain the correct dosages, or harmful contaminants, can infiltrate legitimate global distribution channels with increasing sophistication. These products, in turn, may pose clinical risks to patients and pharmaceutical companies to potential regulatory, financial, and reputational harm. According to the World Health Organization (WHO), an estimated $30.5 billion is spent on substandard and falsified medical products, with regions lacking stringent controls or oversight the most heavily impacted.[24]

What's more, research by the United Nations Office on Drugs and Crime (UNODC) and the WHO has highlighted how falsified raw materials and excipients can enter upstream production where oversight is weakest. When a raw material provider falls short of Good Manufacturing Practice (GMP) standards, or a contract manufacturer sources ingredients through unvetted intermediaries, the resulting contamination is often invisible until well after products reach the market.[25]

Broader geopolitical factors accentuate these risks. Pharmaceutical firms sourcing products from regions where regulatory capacity is still developing, or where regulatory enforcement remains limited, can introduce oversight issues. At the same time, the surge in e-commerce and small parcel shipments has created new distribution channels for counterfeiters, enabling rapid cross-border movement of falsified medicines that appear indistinguishable from legitimate products.

The infiltration of counterfeit drugs into legitimate pharmaceutical supply chains carries severe consequences for patient safety, organizational credibility, and financial stability. Clinically, counterfeit medications can lead to treatment failures, adverse reactions, and preventable deaths. For example, as reported by INTERPOL during Operation Pangea XVII, counterfeit drugs seized in a coordinated global operation frequently contained unknown or dangerous ingredients, posing a serious risk to public health.[26] The FDA has similarly reported instances of counterfeit injectable drugs, including Ozempic, entering the U.S. supply chain, with their sterility, identity, and safety unverifiable.[27]

[23]www.nixonpeabody.com/insights/alerts/2025/11/12/change-healthcare-cybersecurity-breach-impact-on-healthcare-providers

[24]www.who.int/health-topics/substandard-and-falsified-medical-products [who.int]

[25]www.who.int/news/item/24-07-2025-who-and-unodc-release-landmark-report-on-contaminated-medicines--urging-action-to-protect-patients-from-preventable-harm

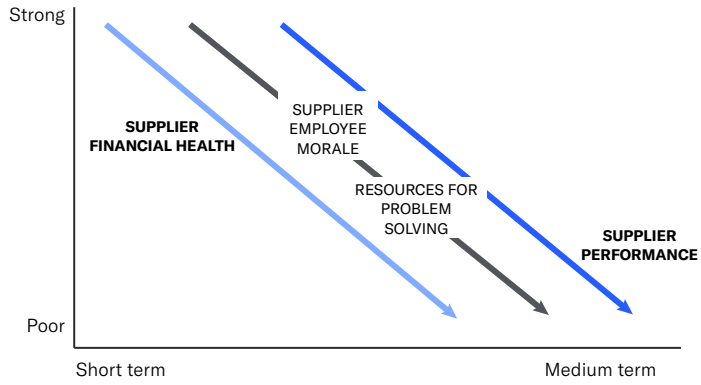
[26]www.interpol.int/en/Crimes/Illicit-goods/Pharmaceutical-crime-operations

[27]www.drugs.com/fda/novo-nordisk-warns-consumers-counterfeit-ozempic-semaglutide-1-mg-us-14780.html

Why continuous supplier monitoring is essential

Most pharmaceutical supply chain failures follow patterns that can be traced back months (sometimes years) before the disruption becomes visible. Compliance observations accumulate, financial ratios weaken, and operational performance begins to slip. The FDA issues hundreds of drug recall events every year, and many are rooted in quality failures with identifiable precursors. The gap between the first warning signs and a full crisis can be influenced by gaps in visibility or monitoring.

Financial pressure offers a clear example. When margins tighten, investments that support performance, workforce stability, quality controls, and process improvements are often reduced. In turn, morale declines, problem solving capacity weakens, and production issues follow. By the time these pressures surface through delivery failures or quality escapes, the deterioration may have been developing for months. The graphic below illustrates how financial stress at the top of the supply chain often becomes operational failure at the bottom, with a lag that can obscure the connection.



Deterioration in a supplier's financial health often leads to lower employee morale and shortage of problem-solving resources, which translate to poor product quality, increasing cost, and delivery problems.

Early detection is critical. Proactive monitoring can help organizations to identify and address risks before localized issues evolve into systemic failures. It also helps to increase transparency by mapping supplier relationships and dependencies across multiple tiers.

Coverage remains a significant challenge. A pharmaceutical company with hundreds of direct suppliers, and thousands more across Tier 2 and beyond, cannot track this network manually. The entities most likely to cause disruption can sometimes be the least visible: contract manufacturers and raw material providers several steps removed from the buying organization, with no obligation to reveal financial or operational stress until it is advanced.

How Moody's can help

Moody's proprietary data estate covers hundreds of millions of entities worldwide, enriched with financial, operational, and compliance intelligence across every tier of the supply chain. For pharmaceutical companies, access to this data estate may help them to build higher visibility across the signals that matter most:

→ **Financial indicators** (liquidity ratios, leverage, liens, signs of distress)

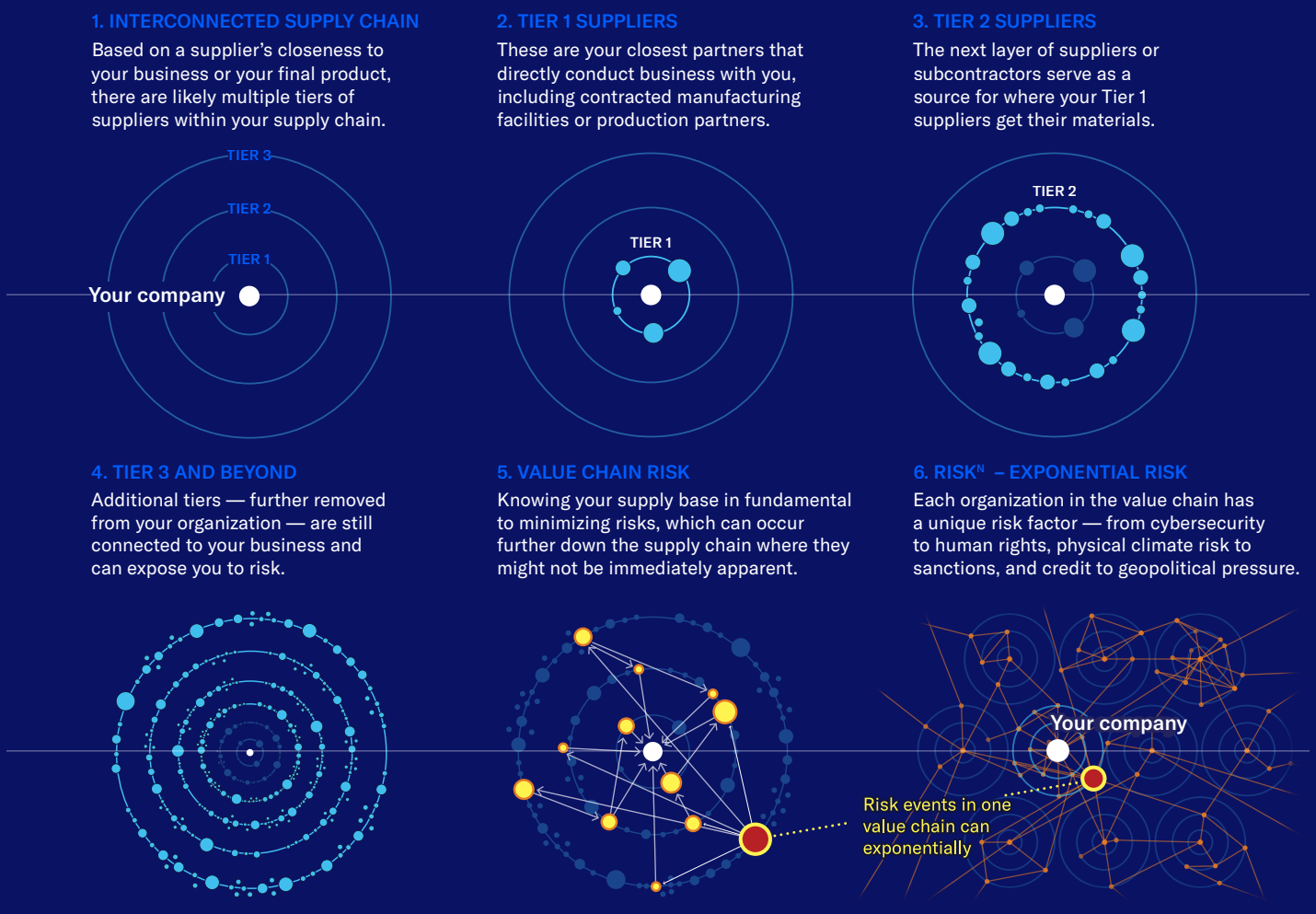
→ **Operational signals** (quality issues, missed delivery deadlines, premium freight incidents)

→ **Compliance alerts** (regulatory findings, safety violations, negative media coverage)

→ **Geopolitical and environmental risks** (trade restrictions, export bans, natural disasters)

→ **Cybersecurity vulnerabilities** (third-party vendors targeted in ransomware attacks)

When any of these signals deteriorate, Moody's data can help procurement teams to surface them early. This, in turn, may provide additional time for teams to diversify, intervene, or qualify an alternative supplier before disruption materially reaches the supply chain.



Summary

The pharmaceutical sector faces complex, fastmoving risks that span suppliers, geographies, regulations, and digital infrastructure. In this environment, organizations may consider shifting from reactive, plan-based supply chain risk management (SCRM) to a unified risk management (URM) framework.

Siloed or static SCRM models may struggle to manage crosscutting risks, as a disruption originating in one area, from a supply shortage to a regulatory action, can potentially cascade across multiple functions and amplify its impact. In contrast, URM can provide proactive, cross functional visibility by consolidating risk signals from procurement, quality, compliance, finance, cybersecurity, and other areas into an integrated overview. This may help leadership to anticipate issues and act before they escalate.

By dismantling silos across the organization, URM can strengthen a company's ability to build operational resilience and mitigation strategies. It turns risk management into a strategic capability that supports resilience in an increasingly volatile operating environment.

Covering hundreds of millions of entities and enriched with financial, operational, and compliance intelligence, Moody's provides pharmaceutical companies with trusted intelligence to help them vet suppliers thoroughly, detect vulnerabilities early, and build supply chain resilience with confidence.

7-10%

Of pharmaceutical products expire on hospital shelves before they can be administered[28]

$200bn

The annual estimated value of the counterfeit drug market, which threatens global supply chain integrity[29]

276m

Number of patient records exposed globally due to cyberattacks in 2024[30]

62%

Estimated percentage of medical devices in the United States that are imported from overseas[31]

[28] gitnux.org/supply-chain-in-the-healthcare-industry-statistics/
[29] gitnux.org/supply-chain-in-the-healthcare-industry-statistics/
[30] blog.checkpoint.com/securing-user-and-access/with-the-right-tools-you-can-prevent-this-healthcare-scam-from-hurting-employees/
[31] kpmg.com/us/en/articles/2025/impact-tariffs-healthcare-2025.html

Moody's compliance and supplier risk management solutions offer leading sources of global data; analytics and a context layer so standardized company and ownership information can be integrated into due diligence activity and ongoing risk workflows.

If you would like to explore how this approach could benefit your business, please visit our website or get in touch any time to speak with a member of the team.

Contact us

AMERICAS

+1.212.553.1658
clientservices@moodys.com

EUROPE

+44.20.7772.5454
clientservices.emea@moodys.com

ASIA (Excluding Japan)

+85.2.2916.1121
clientservices.asia@moodys.com

JAPAN

+81.3.5408.4100
clientservices.japan@moodys.com

MOODY'S