Trendtracker

# Megashifts Shaping the Future of Insurance

Nine forces redefining risk, value, and competitive advantage.

# Table of Contents

# About Trendtracker

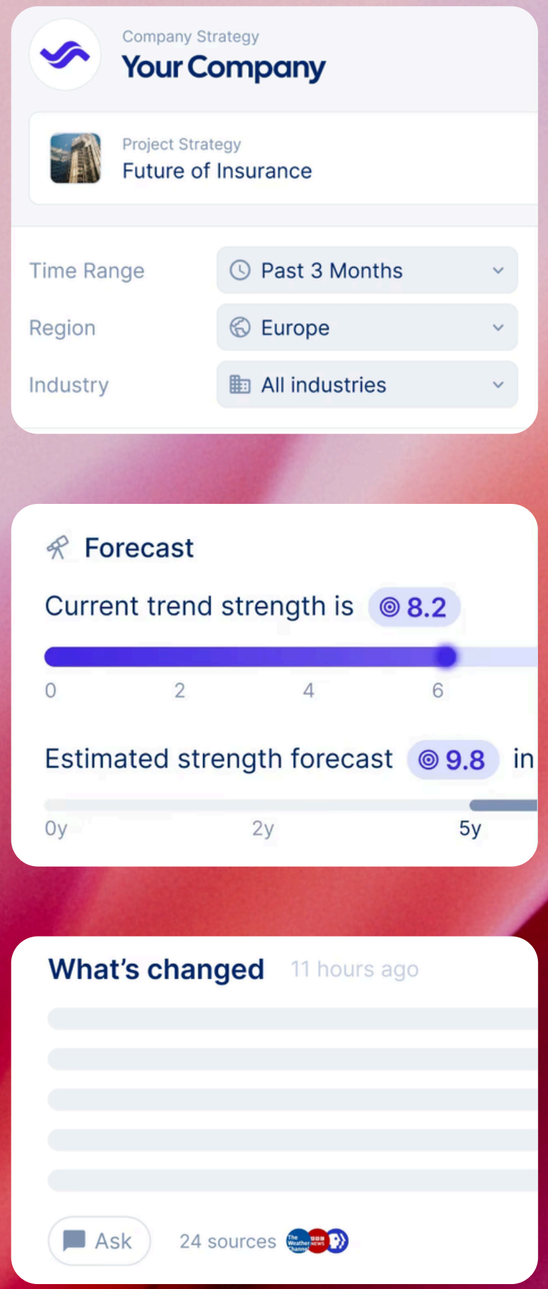
In an era where corporate lifespans are shrinking, and global data volume has grown twentyfold in just over a decade, strategic decision-making has become both more critical and more challenging.

Traditional planning cycles can't keep pace with the speed of change, leaving strategy teams overwhelmed by information overload. Market intelligence providers offer static reports, while media monitoring tools simply track mention volume; neither delivers the contextualized insights organizations need.

Trendtracker is an AI-powered strategic intelligence platform that transforms how organizations identify and act on emerging trends. We continuously monitor over 18,000 sources worldwide, applying proprietary machine learning models to surface weak signals before they become obvious. Our Trend Strength Index scores trends on source credibility, conversation evolution, and strategic relevance, not just popularity.

The result: transparent, explainable insights that help executive teams understand not just what's changing, but why it matters and what to do about it. Leading enterprises, including Zurich Insurance, Manulife, The Geneva Association, and Ageas rely on Trendtracker to reduce horizon scanning from months to minutes and maintain a strategic edge in an increasingly uncertain world.

Talk to our experts  Read our Customer Stories




**Adapt metrics** to your needs and strategic goals

Visualise the **strength of trends,** in one place

**Stay informed** with source-linked, concise updates

# A defining decade for insurance

Insurance is at an inflection point — not because of digitalisation, new products, or efficiency gains, but because the fundamentals are shifting: how risk is created, how it can be observed, how capital is allocated, and how value is ultimately generated. These are not short-term cycles. They are structural changes that will define which insurers lead, adapt, or fall behind over the next decade. And I believe many leaders underestimate how profound these changes will be.

This report exists because it connects signals that are usually analysed in isolation. When trends are viewed separately, they feel manageable. When viewed together, they reveal a much more disruptive reality. Anyone responsible for strategy, foresight, risk, or innovation in insurance will recognise the urgency once these forces are seen as a whole.

At Trendtracker, we call these deep, system-level forces Megashifts. A Megashift is not a trend or a technology — it is a long-term change that cuts across underwriting, claims, regulation, technology, workforce capabilities, and customer expectations at the same time.

Their real impact only becomes visible when you understand how they interact and reinforce each other.

This report focuses on nine Megashifts that we believe will have the greatest impact on insurance through 2030 and beyond. They were selected from a much broader body of foresight research and refined specifically for insurance leaders who need clarity, not noise. The goal is to provide a shared strategic language to discuss what is changing, why it matters, and where concrete action is required.

Consider just one example: as real-time health and behavioural data become ubiquitous, the insurer's role shifts from pricing historical risk to actively managing and preventing it.

That single shift alone forces a rethink of product design, distribution, claims operations, and the very definition of what an insurance company does.

Now multiply that across nine interconnected Megashifts — and the scale of strategic recalibration becomes clear.

Taken together, these Megashifts point to a fundamental transition: insurance is moving away from pricing static, historical probabilities toward managing dynamic, connected systems in real time. In this world, prevention, verification, and continuous risk assessment become core sources of value.

I encourage you to read this report not as a prediction of the future, but as a strategic tool. Use it to challenge assumptions, stress-test your current capabilities, and identify where decisions cannot be postponed.

The insurers that win the next decade will not simply be the fastest to adopt new technology.

They will be the ones who recognised structural change early — and acted on it before the window closed.

Enjoy the reading,

*Vincent Defour,*
*Founder & CEO, Trendtracker*

# 9 Megashifts you'll explore in this report

1 | Conscious Commerce

2 | The Demographic Divide

3 | Accelerated Intelligence

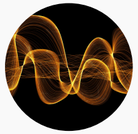
4 | The Exponential Industry

5 | Geostrategic Deglobalization

6 | The Robot Economy

7 | Ultra Urban Systems

8 | Engineered Humanity



9 | The Quantum Leap

# Executive summary

## The structural transformation of insurance risk

**Insurance is shifting from pricing historical probabilities to managing live, connected systems.** Risk is now a continuous condition to measure, price, and influence in real time, rather than an outcome to insure after the fact. Traditional underwriting, based on large pools, stable loss patterns, and standardized products, is becoming obsolete.

Operations are increasingly software-driven and sensor-enabled, spanning autonomous logistics, urban infrastructure, and precision biology. As systems become more interconnected, the distinction between insured events and behaviors disappears.

Losses now often result from software updates, sensor failures, network effects, and algorithmic decisions in production, mobility, and healthcare. Insurers must now price dynamic exposures, which requires real-time data access, technical understanding of system failures, and governance structures that manage complexity without sacrificing transparency.

> *"Insurers can no longer evaluate risks through the rear-view mirror."*
>
> ***-2025 global insurance outlook, Deloitte***

**The second transformation is driven by demographic and geopolitical fragmentation, reshaping both insurance economics and operations.**

Aging populations increase claims in health and long-term care, reduce the premium base, and shrink the talent pool for complex risk assessment. Simultaneously, geopolitical shifts are dividing the global regulatory landscape, creating competing blocs with different standards for data, capital, sanctions, and technology.

This removes the efficiency of centralized global models and increases hidden correlation risks across regions. Insurers can no longer rely on stable actuarial pools or uniform compliance. Products must become modular and tailored to life stages.

Underwriting must integrate new data sources and adapt to inconsistent legal standards. Operational resilience now depends on scalable workforce models that maintain expertise as experienced staff retire and regulations diverge by region.

**The third transformation concerns how value and trust are established.** Customers now expect verification rather than promises. They seek relevance, transparency, and alignment between service and stated principles, making loyalty conditional and reputation measurable in real time through reviews and ratings.

For insurers, this is not just a branding issue. It directly impacts pricing and retention, as trust now depends on consistent fairness, speed, and accountability in underwriting and claims. Leading organizations will treat customer experience, governance transparency, and values alignment as strategic infrastructure.

This requires clear responsibility for AI decision-making, data use and protection, and operational performance tracking. Insurers that make compliance, data integrity, and explainability sources of competitive advantage, rather than costs, will succeed.

# Executive summary Continued

> *"Insurers must ensure AI models are fair, unbiased, and transparent. "*
>
> ***Insurance 2025, BCG***

## The continuous insurance model

*From claims payer to operating partner*

The future insurance model integrates risk transfer and prevention, combining protection, monitoring, and intervention into a continuous operating layer. This approach shifts insurers from claims payers to operating partners.

- Quantum-safe upgrade packages link coverage to verified security improvements, making post-quantum readiness a measurable business goal with direct premium impact.
- Risk dividend contracts for smart factories use IIoT data and safety signals to automatically adjust premiums and expand coverage when risk reduction is sustained.
- Programmable resilience policies combine parametric micro-coverage with live prevention services across urban systems, providing immediate mitigation when sensors detect leak risks or grid instability.
- Autonomy assurance layers certify autonomous fleets through continuous telemetry scoring, with premiums adjusting dynamically as controls improve or decline.

The strategic shift is clear: insurance becomes a performance contract that rewards prevention through transparent pricing, embedded verification, and real-time response.

## From products to orchestration platforms

The second structural change shifts from standalone products to platforms that manage fragmented risk across connected ecosystems.

Resilience subscriptions combine insurance with integration dashboards that consolidate multinational coverage, track regulatory changes, and translate sanctions into clear triggers and pre-approved mitigation plans.

- Urban operating system insurance offers a single subscription for usage-based mobility coverage, AI-driven asset scoring, and cyber-physical grid protection, addressing fragmented responsibility and slow coordination in cities.
- Insurance risk wind tunnels provide synthetic-data testing environments for companies to stress-test operations and AI systems, using scenario outcomes to inform pricing, coverage, and trigger rules.
- Demographic readiness subscriptions support customers through retirement, caregiving, and mobility changes with services activated by life-stage events, rather than isolated policies.

These platforms succeed by reducing coordination friction, generating recurring revenue, and embedding distribution within key ecosystems.

# Executive summary Continued

> *“We can expect two new models to arise: the model ‘as a service’, where insurance services are offered through a platform of a third party, and the model ‘as a platform’, where the insurer opens its own platform for services from third parties. ”*
>
> ***View on Insurance in 2030,***
> ***Hans De Cuyper, CEO AG Insurance***

## From brand promise to verifiable governance

The third transformation is using governance as a competitive advantage, making trust a verifiable infrastructure rather than just a brand promise. Transparent trust layers provide customers with clear policy dashboards that show coverage logic, premium factors, claims status, and decision reasons, along with data controls for granting or revoking access within ecosystems.

- Member-governed bio-data trusts allow customers to control access to omics and health data, with clear rules for pricing and prevention, turning sensitive information into a trust asset.

- Retirement and transition support for displaced drivers reframes automation as a livelihood transition, with insurers offering retraining and financial guidance subscriptions to build goodwill and regulatory relevance.

The core principle remains: organizations that operationalize permission, explainability, and fairness will outperform those that only claim these values.

In markets where loyalty is conditional and reputation is monitored in real time, proving accountability through operational design becomes the key competitive advantage.

# 01 Conscious Commerce

# Introduction

**Conscious Commerce** has shifted insurance competition from what companies claim to what customers can verify. Customers now demand experiences, relevance, proof, and principles simultaneously.

This changes the core job of insurance. Winning is no longer only about pricing, distribution, and marketing reach. It is about consistently earning trust through transparent interactions, measurable service performance, and offers that feel both personal and fair.

Loyalty has become conditional, and reputation has become trackable. Insurers must treat customer experience and customer values as strategic assets, not branding topics.

# Dominant subtrends

Conscious Commerce must urgently reshape insurance to be experience- and relevance-driven. The Experience Economy now demands that protection becomes a lived service rather than a contract. Customers increasingly reward seamless experiences, quick responses, and consistent omnichannel delivery. They ruthlessly punish friction, as it signals unreliability.

**Hyper-personalisation** raises expectations even higher. Insurers must deploy AI and real-time data to precisely tailor offerings, communications, and services. This approach rapidly extends into underwriting and claims through automated workflows and more precise pricing. The upside: stronger retention and new revenue models. The challenge: trust. Personalisation only succeeds when decisions are explainable, defensible, and perceived as fair.

Market structure and payment models are shifting simultaneously. Phygital commerce blends digital and physical touchpoints. This increases access and engagement but multiplies exposure to fraud, breaches, and identity risk. Insurers must cover blended perils and upgrade their product design to be cyber-ready. Direct-to-consumer models shift distribution control toward platforms and ecosystems.

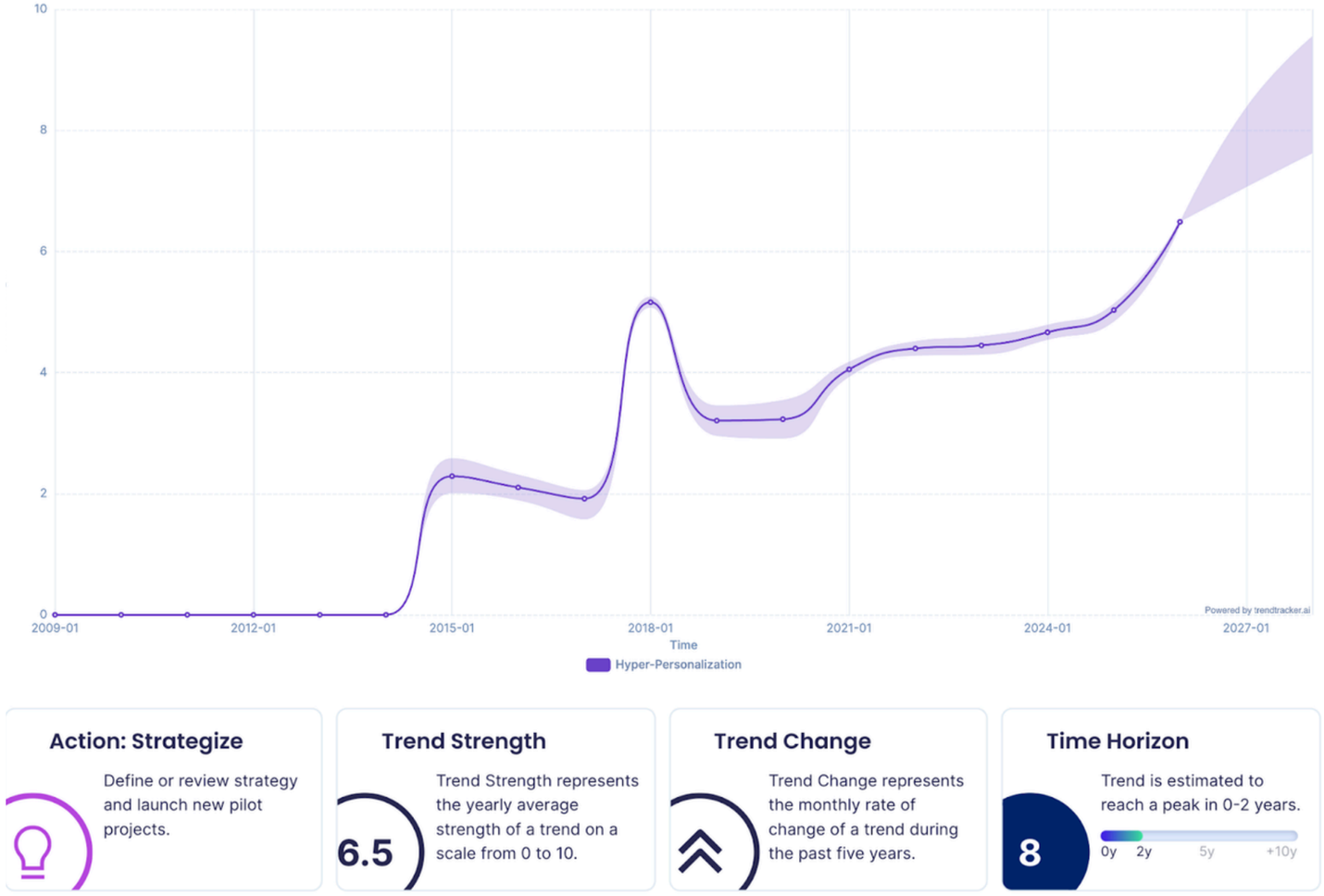



***Image 1:*** *Trendtracker data: Global hyper-personalization in insurance, structurally growing since 2017.*

# Dominant subtrends Continued

This compresses intermediary value and forces insurers to build native integrations and superior servicing to maintain relationships. The subscription economy completes the transformation by aligning protection with flexible lifestyles and recurring behaviours. It can stabilise revenue and expand micro-coverage, but only if transparency, simplicity, and data capability are engineered into the offer. Without these, dynamic pricing and adjustments lose credibility.

> *"The ongoing evolution of Usage-Based Insurance will include further growth of subscription models in parallel with increasing adoption of electric and autonomous vehicles."*
>
> ***EY, 2025 Global Insurance Outlook***

**Samples of articles analyzed by Trendtracker**

- Digital Insurance Maturity 2025 (EMEA digital customer interaction benchmark), Deloitte, 05 Jul 2025
- World Life Insurance Report 2026, Capgemini, 01 Oct 2025
- Insurance Predictions For 2026: Significant shifts in CX, AI, and microinsurance, Forrester, 30 Oct 2025
- 5 predictions for the insurance industry in 2026, Accenture, 02 Feb 2026

# Potential risks and blindspots

AI transparency failures will immediately trigger regulatory intervention and customer backlash. Hyper-personalisation, continuous underwriting, and AI-assisted claims rapidly raise conversion and efficiency.

Yet opaque decision-making swiftly triggers complaints and regulatory action. Pricing and claims outcomes are now fiercely contested. Model risk escalates. Governance costs skyrocket. At a societal level, when people cannot grasp the decisions shaping their financial security, distrust cascades far beyond a single insurer. Confidence in data-driven systems erodes everywhere.

Accountability in embedded ecosystems is fragmented. When AI-driven decisions, cyber incidents, or data misuse occur in platform-mediated insurance, liability is split among insurers, partners, and technology vendors.

This leads to coverage complications, legal ambiguity, and disputes about responsibility for remediation and compensation.

Blurred accountability slows recovery and weakens incentives to prevent problems. Actors shift blame instead of addressing root causes.

Better digital UX alone will not restore customer confidence. Conscious Commerce is not only about convenience.

It is about proof, fairness, and consistent delivery. If the industry continues to seem complex, slow, or evasive, the promise of insurance weakens. The result is lower loyalty, more churn, more disputes, and higher sensitivity to reputational shocks. Reduced trust increases societal fragility. People delay coverage and underinsure, worsening inequality and putting more pressure on public systems.

# Recommended strategic initiatives

**Build a real-time customer and risk operating core.**

Insurers without real-time customer and risk capabilities will lose to competitors who can price more accurately, settle claims faster, and personalise offers dynamically. Legacy data architecture is now a revenue constraint, not just technology debt.

This initiative modernises the foundation by integrating a data strategy, advanced analytics, and AI-enabled workflows across underwriting, claims, and servicing. It addresses data silos that block seamless experiences. It enables continuous underwriting, more accurate pricing, faster claims resolution, and tailored engagement.

This core becomes the multiplier for every other move, including embedded distribution and subscription logic. Insurers have 18-24 months before experience gaps translate to permanent customer migration in younger segments.

**Industrialise omnichannel and phygital journey design with trust built in.**

Customers already judge credibility through speed, clarity, and perceived fairness. Inconsistent experiences across touchpoints signal operational weakness

This initiative treats omnichannel as an operational discipline rather than a channel strategy. It delivers consistent interactions across digital, physical, and partner touchpoints, including phygital commerce environments. It hardwires transparency into digital journeys because trust gaps are now a direct competitive risk. Coherent journey design improves retention, reduces servicing costs, and creates a defensible reputation that is measurable through customer behaviour and feedback loops.

**Shift distribution and product architecture toward embedded, direct, and flexible coverage models.**

Embedded solutions are scaling quickly. Platform players are setting new expectations for frictionless insurance-as-a-feature.

Traditional insurers that maintain legacy distribution models will see acquisition costs rise and market access narrow. This initiative redesigns how insurance reaches customers and how products fit modern buying behaviour.

It prioritises embedded partnerships that place insurance at the point of need, strengthens direct channels that reduce acquisition friction, and expands flexible offerings such as usage-based and subscription-style protection. This is not a marketing pivot. It is a structural growth engine that changes unit economics, increases access in underinsured segments, and improves engagement through relevance and convenience. It forces insurers to simultaneously improve integration, personalisation, and compliance capabilities. Tech platforms will partner with insurers who reduce friction, complaints, and regulatory exposure.

Those partnerships will lock in for multi-year terms, creating distribution barriers for late movers.

# Growth initiative: Verifiable trust layer

Build a Verifiable Trust Layer that makes trust a product feature, not just a brand claim. Every customer sees a clear policy and claims cockpit, with straightforward coverage logic, premium drivers, claim status, service commitments, and reason codes. A permissioned data control layer shows what data is used and lets customers grant or revoke access for partners and embedded ecosystems.

This flips the default posture from defensive to accountable. It reduces disputes because decisions are explainable by design. It improves retention because customers feel treated fairly, even when outcomes are not perfect. The differentiation is structural. Embedded platforms will choose partners with lower complaint rates and clearer audit trails. Trust transparency becomes a distribution filter, not just a brand position.

Competitors can copy the interface, but they cannot easily replicate the data architecture, governance framework, and operational discipline required to deliver verified fairness at scale.

The regulatory positioning advantage is clear. The EU AI Act and similar frameworks will mandate explainability for automated insurance decisions. Early movers gain both compliance advantage and customer trust simultaneously.

Late movers face the cost of retrofitting governance while also repairing reputational damage from early enforcement actions. In Conscious Commerce, the insurer that can prove fairness at the interaction level will outcompete the insurer that only promises it.

# 02
# Demographic Divide

# Introduction

**Demographic Divide** is no longer a background macro theme. It is now an operating condition that reshapes demand, risk pools, workforce capacity, and the economics of long-duration promises.

Ageing populations increase claims intensity and long-term care exposure, while lower fertility and shifting labour markets pressure premium growth and the availability of skilled underwriting and claims talent. At the same time, mobility and migration create new customer segments with different income patterns, trust dynamics, and legal needs. For insurers, this

Megashift forces a re-architecture of products, planning, and execution: coverage becomes more modular and life-stage specific, underwriting must absorb new forms of data and new constraints, and operational resilience increasingly depends on talent models that can scale expertise even as experienced staff retire.

# Dominant subtrends

**Ageing populations** are creating a triple pressure on insurance operations: rising service intensity, escalating costs, and structural capacity constraints. Ageing is becoming a tech-enabled life stage rather than a passive decline. Seniors and caregivers now use digital tools, remote monitoring, assistive technology, and connected home environments. Adoption barriers and digital skills gaps slow momentum.

But the direction is clear: insurers that operationalise age-tech into coverage and underwriting can defend loss performance in older segments. Long-term care is moving from a niche product problem to a system-level affordability crisis.

Rising demand collides with cost inflation and longer life expectancy, pushing premiums upward and tightening underwriting. Insurers must combine AI-driven care planning with flexible benefit designs that match home-based care preferences.

Reinsurance becomes strategic, not technical, because duration risk and claims volatility can destabilise balance sheets without capital relief. The retirement wave amplifies this pressure by shifting industry economics toward a greater number of retirees relative to working-age contributors.

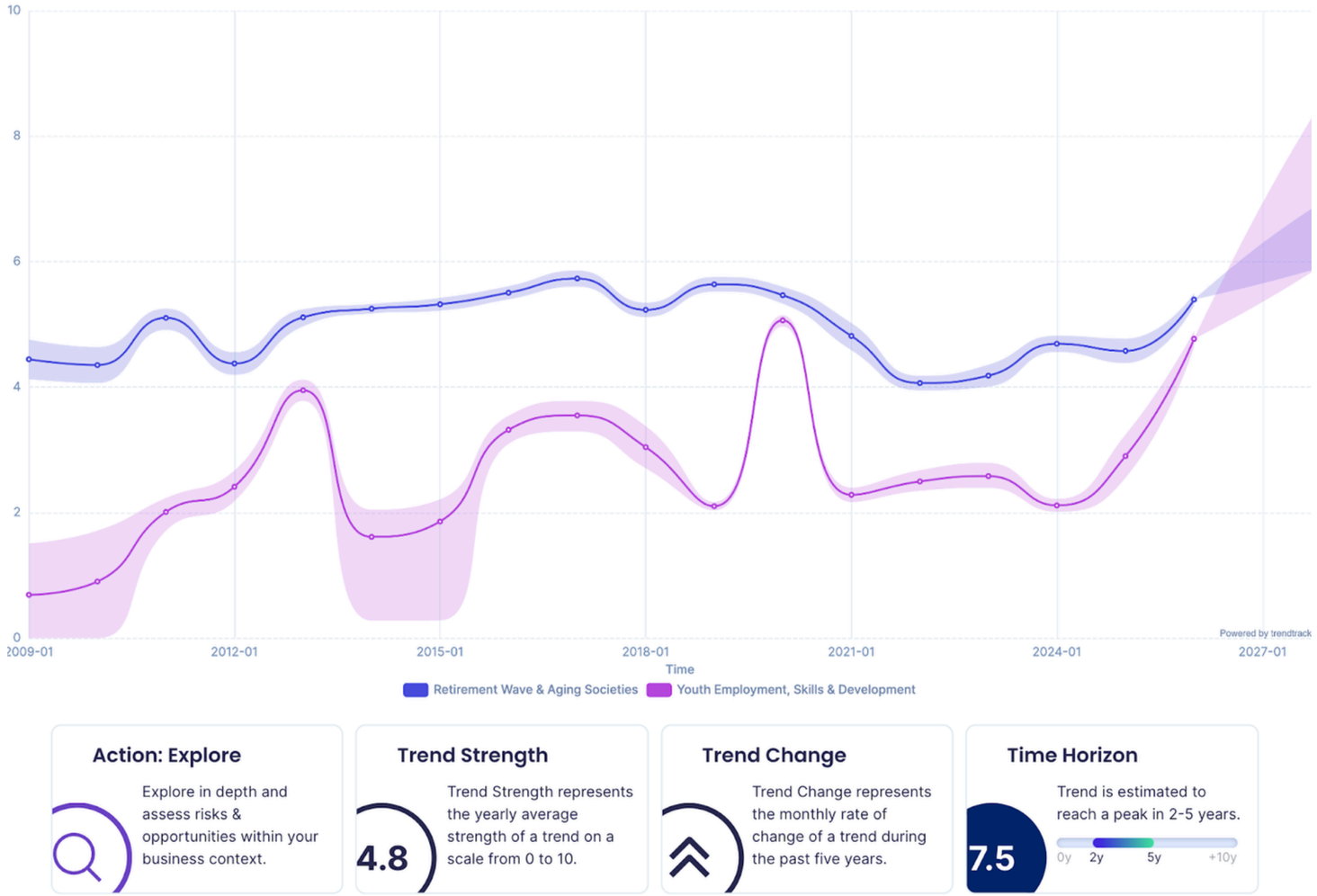



***Image 2*** *Trendtracker data: Retirement wave & aging societies steadily outpaces youth employment & skills development from 2022.*

# Dominant subtrends Continued

Demand concentrates on life, health, and retirement-related protection while claims pressure rises. Insurers must compete on relevance through guided decision support and tailored coverage structures, not just on brand familiarity.

> *"The silver population is expected to double to 1.6 billion by 2050 (representing 16 percent of the global population)."*
>
> ***-McKinsey & Company, Global Insurance Report 2025***

Workforce and mobility shifts are simultaneously changing operational capacity and customer composition. The industry cannot execute demographic adaptation without rebuilding how expertise is retained and deployed.

Multigenerational workforce models improve continuity and underwriting quality, but only if work is redesigned around flexible engagement and systematic knowledge transfer.

Hybrid models and phased retirement are not cultural perks. They are mechanisms to prevent experienced knowledge from draining faster than operational models can replace it.

When that happens, complexity shows up as slower cycle times, more escalations, and higher claims leakage. Migration creates new insurable needs and new friction points simultaneously.

Migrants and expatriates face unstable income patterns, complex legal exposure, and barriers of language, trust, and access. This changes the distribution, onboarding, and claims-handling requirements. It also changes product design.

Demand rises for specialised coverage that combines health, legal protection, and financial security, in formats that are easy to understand and activate. Insurers that build culturally accessible products and service models can capture underserved growth segments while reducing reputational risk tied to exclusion and confusion.

**Samples of articles analyzed by Trendtracker**

- Employment and Social Trends 2026, International Labour Organization (ILO), 14 Jan 2026
- Life (span) insurance, Swiss Re Institute, 22 Oct 2025
- Generational diversity, UNECE, 16 Nov 2025
- Health at a Glance 2025, OECD, 13 Nov 2025

# Potential risks and blindspots

**Shrinking and ageing core markets create hidden concentration risk.**

Premium stagnation appears to be a distribution problem when it is actually a structural pool problem. This drives higher expense ratios, increases concentration in legacy products, and weakens the diversification assumptions many portfolios rely on. The broader impact is societal: underinsurance rises precisely when households need more protection, amplifying fiscal strain on public systems and increasing volatility in retirement outcomes.

**Wealth inequality distorts both affordability and risk pooling.**

As income dispersion grows, insurers risk designing products for the most profitable segments while losing the middle market to affordability collapse. This is not only a growth problem. It becomes a claims and reputational problem because vulnerable households delay care, lapse coverage, and become harder to underwrite fairly. At scale, this erodes trust in insurance as a social stabiliser and increases political pressure for intervention.

**Migration-related accountability gaps create operational and legal fragility.**

The risk is not simply writing migrant-focused products. The risk is failing to align policy terms, communications, and claims practices with real-world mobility and changing immigration rules. When exclusions, documentation requirements, or service workflows do not align with customer reality, insurers create disputes and regulatory exposure. Poorly designed coverage for mobile populations increases reliance on emergency public services and worsens social fragility around integration.

# Recommended strategic initiatives

**Build a life-stage product architecture that treats ageing as a managed pathway.**

Insurers still selling one-size-fits-all products to ageing populations will face higher claims volatility and lower retention. Life-stage architecture shifts from generic coverage to structured journeys: pre-retirement planning, retirement income protection, long-term care readiness, and ageing-at-home support.

Better segmentation enables clearer underwriting assumptions, stronger pricing discipline, and fewer claims surprises due to mismatched benefits. It also improves retention because customers can evolve within a product ecosystem instead of shopping for disconnected fixes as needs intensify.

**Industrialise AI and analytics for long-term care planning and claims cost containment.**

The goal is not automation theatre. The goal is to reduce duration risk and care-cost volatility through smarter care planning, earlier interventions, and benefit designs aligned with home-based care preferences.

This directly addresses rising premiums and consumer affordability pressure while improving capital efficiency. When done well, it strengthens the insurer's position in regulatory discussions because decisions become more explainable and policy designs more defensible. Insurers that delay will see long-term care portfolios become profit drains rather than growth engines.

**Create scalable expertise through elastic staffing and structured knowledge transfer.**

Demographic shifts increase operational complexity right when experienced staff retire. Phased retirement, mentorship systems, and flexible expert pools are not soft initiatives. They protect underwriting quality, reduce claims leakage, and stabilise service levels in segments where customer expectations are higher and tolerance for errors is lower. When experienced underwriters retire without transferring their knowledge, complexity manifests as slower decision-making and higher loss ratios. This also unlocks new business models that monetise expertise externally rather than letting it walk out the door.

# Growth initiative: Demographic readiness subscription

Launch a Demographic Readiness Subscription that bundles planning, coverage, and activation across life shocks. Position it as a paid membership layer that sits above traditional policies and follows the customer through retirement planning, caregiving decisions, and mobility events. When a customer approaches retirement, the subscription activates structured longevity planning.

When caregiving needs appear, it activates care navigation and benefit optimisation. When mobility or job instability hits, it activates simplified protection and clear communications designed for trust.

This sets an insurer apart by turning demographic turbulence into a managed operating system rather than a sequence of isolated products. It creates defensible stickiness in segments where switching costs are typically low, and dissatisfaction is typically high.

The model integrates AI-supported long-term care planning, longevity planning, and migrant financial wellness into a single continuous service with clear triggers and actions.

Competitors can copy individual features, but they cannot easily replicate the integrated service architecture and data infrastructure required to deliver personalised activation at life-stage transitions.

# 03
# Accelerated Intelligence

# Introduction

**Accelerated Intelligence** moves AI from an assistive tool into the operating layer of the insurance value chain. It changes how risk is measured, priced, managed, and explained. AI is now embedded in underwriting decisions, claims triage, fraud detection, customer service, and product design.

This raises expectations for performance and reduces tolerance for unclear decisions, weak governance, and poor security. Insurers now face a key issue: deploying AI at scale with strong accountability, resilient controls, and measurable impact on loss ratio, expense ratio, and trust.

# Dominant subtrends

AI capabilities are becoming modular and purchasable, lowering experimentation barriers but compressing differentiation. Competitors can buy similar models and tooling. The advantage shifts to insurers that industrialise AI into repeatable workflows across underwriting, fraud detection, and claims, rather than running isolated pilots.

Faster adoption also expands exposure on two fronts. Internally, AI systems introduce new failure modes in decision-making, data handling, and security. Externally, clients demand coverage for AI-driven incidents and liabilities that remain poorly defined. The combined result is a larger attack surface and greater pressure to build robust risk frameworks, stronger cyber controls, and clearer liability structures that align with how AI actually fails in operations.

**Governance** and explainability are now operational requirements. Governance must be enforceable across model development, procurement, deployment, monitoring, and change management. This means compliance tools, auditability, and real-time oversight to defend AI decisions. Explainability is essential because underwriting and claims will be challenged. Without clear reasoning and solid documentation, insurers face more rework, escalations, and complaints.

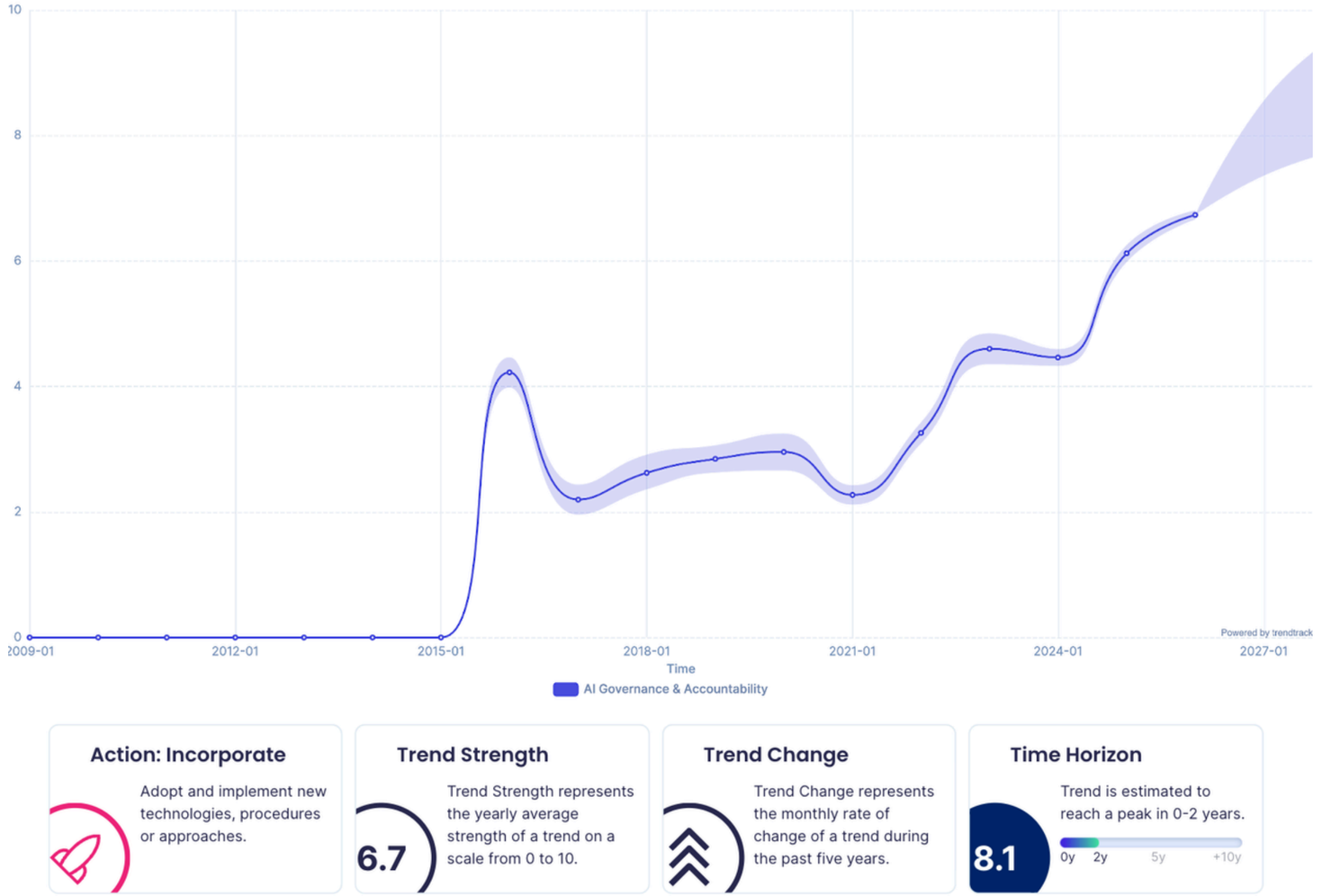



***Image 3:*** *Trendtracker data: AI governance & accountability accelerates post-2020, amid EU AI Act and state audits for insurers.*

# Dominant subtrends Continued

Agentic AI raises the stakes by moving from output generation to executing workflows. Agents create continuous loops: data triggers actions; actions update risk posture. This requires clean interoperability and modern infrastructure since agents can't rely on manual handoffs or poor data pipes. It also raises accountability when automated actions lead to poor outcomes.

> “AI Governance Software Spend Will See 30% CAGR From 2024 To 2030.”
>
> ***Forrester, Nov 2024***

Execution constraints are sharpening around compute costs, talent scarcity, and data privacy. AI compute appetite is becoming a strategic constraint as infrastructure costs and ESG exposure become more visible.

Sustainable AI practices protect the cost base while maintaining model quality improvements, particularly in climate risk modelling and fraud detection, where more compute improves signal detection.

Talent scarcity is the execution bottleneck. The constraint is not only hiring data scientists but building broad AI literacy so underwriters, claims leaders, product owners, and risk teams can operate AI-enabled workflows without creating hidden failure points.

Governance frameworks only work if people can apply them. Synthetic data is becoming a pragmatic solution to privacy constraints and sparse edge-case data. It strengthens fraud detection by enabling training scenarios without exposing sensitive customer information. It supports climate and catastrophe modelling by simulating detailed scenarios.

The strategic value extends beyond model performance to regulatory resilience because synthetic environments enable safer testing and validation under evolving rules.

**Samples of articles analyzed by Trendtracker**

- EIOPA survey on Generative AI, EIOPA, 02 Feb 2026
- AI transformation in financial services: 5 predictors for success, Microsoft, 18 Dec 2025
- Allianz “Project Nemo” agentic AI automating claims tasks), Allianz, 03 Nov 2025
- Synthetic Data: The New Data Frontier, World Economic Forum, 23 Sept 2025

# Potential risks and blindspots

**AI-related policy exclusions are creating coverage gaps and trust erosion.**

Insurers are excluding AI-related claims from traditional policies, which forces policyholders to scrutinise and augment coverage. This is not a small technicality. As AI becomes embedded in core business processes, exclusions give rise to frequent disputes over what is in or out of scope, especially when incidents blend cyber and operational failures with third-party liability.

The near-term consequence is friction in claims and renewal. The longer-term consequence is market fragmentation, where only specialist products remain credible while broad coverage becomes harder to defend commercially and legally.

**Regulatory uncertainty is becoming a growth brake, not just a compliance detail.**

Treating regulation as a box-check after building capability is a strategic error. Regulatory uncertainty and rising scrutiny directly constrain scaling AI in insurance.

If governance is not designed as an operating system, AI adoption stays stuck in pilots or narrow use cases.

That leaves productivity gains on the table, slows product innovation, and hands an advantage to competitors who can prove auditable, fair, and accountable AI fast enough to satisfy regulators and enterprise clients.

**Legacy infrastructure creates scale failure regardless of model capability.**

The assumption that model capability is the hard part misses where strategy quietly dies. If data cannot flow cleanly across underwriting, claims, fraud, and service, then agentic workflows stall, automation becomes brittle, and humans end up handling exceptions forever.

The impact is not only cost. It is a risk quality. Inconsistent data flows lead to inconsistent decisions, increasing error rates, operational risk, and complaints while making it harder to demonstrate control to regulators and large corporate buyers.

# Recommended strategic initiatives

### Build enforceable AI governance and model risk management.

Insurers without auditable AI governance will face regulatory blocks on new AI use cases, customer disputes on automated decisions, and compliance shocks that stall deployment. EU AI Act implementation begins in phases through 2025-2027. Early movers gain approval speed for new use cases, fewer disputes, and stronger trust signals in enterprise markets.

This initiative turns principles into controls through governance frameworks, compliance tooling, auditability, and clear accountability for AI decisions across underwriting, claims, and customer interactions. It operationalises explainability where it matters most: adverse decisions and high-impact claims. This creates fewer compliance shocks, fewer disputes, faster approvals for new AI use cases, and stronger market trust signals.

### Industrialise AI in core workflows where economics compound.

Competitors are already deploying AI-driven fraud detection and underwriting automation that improves loss ratios and compresses cycle times. Insurers that delay lose both margin advantage and the data accumulation needed to improve models over time. Focus on repeatable engines: fraud detection, underwriting decision support, claims triage and automation, and continuous underwriting patterns enabled by agents.

The goal is measurable improvement in the ratio through cycle-time compression, better risk selection, and lower claims leakage. This requires strong data pipelines, real-time monitoring, and scalable human oversight models. Without these, AI automation creates brittle workflows that leave humans to handle endless exceptions. These workflows compound economic impact across volumes.

### Modernise infrastructure for interoperability, secure AI operations, and privacy-safe innovation.

Weak interoperability blocks agent adoption. Weak security turns AI into a risk multiplier. Agentic systems, synthetic data, and scalable AI services all depend on modern integration patterns and secure architectures. Priorities include moving away from brittle legacy dependencies, enabling clean data flow, and building environments where models can be tested and validated safely.

Synthetic data should be treated as a strategic capability for privacy-preserving model training and edge-case simulation, not as a niche data science tool. This unlocks deployment speed without sacrificing control and enables governance at scale rather than governance as a bottleneck.

> *“Leadership from the highest levels of the organization helps ensure that AI investments and pilots are strategically prioritized and that successful experiments can be scaled and industrialized quickly.”*
>
> ***EY, Global Insurance Outlook 2025***

# Growth initiative: Insurance risk wind tunnel

Build a synthetic-data driven testing environment that lets corporates and public bodies stress-test operations, AI systems, and insurance programs before reality does it for them.

The platform generates synthetic scenarios to model claim patterns, fraud tactics, operational disruptions, and climate- or cyber-related stress. It translates outcomes into concrete insurance actions: pricing adjustments, coverage design, control recommendations, and pre-agreed trigger rules for rapid response.

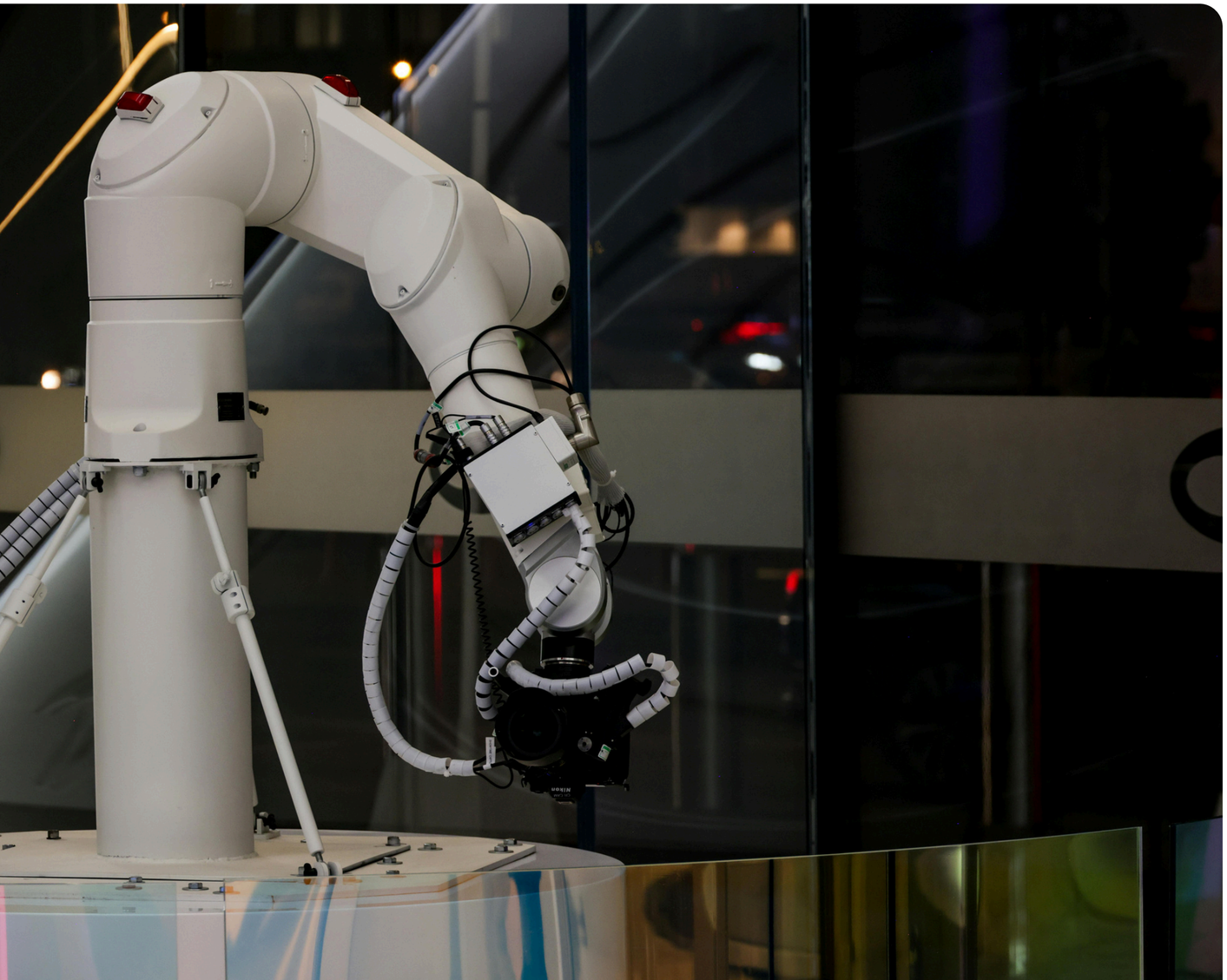
This productizes three capabilities simultaneously: synthetic data generation for risk testing, compliance simulation, and auditable, explainable decision trails for regulators and boards. It differentiates an insurer by turning risk transfer into risk engineering at scale.

It creates new revenue through platform licensing and advisory services while improving underwriting quality and portfolio resilience through a constant pipeline of stress-tested scenarios.

Competitors can build scenario modelling tools, but they cannot easily replicate the integrated platform that combines synthetic data generation, insurance product design, and real-time decision support within a single auditable environment.

# 04
# The Exponential Industry

# The Exponential Industry



**The Exponential Industry** is the shift from Industry 4.0 to Industry 5.0, where the priority moves from pure automation and output to resilience, sustainability, and human-centred performance. In insurance, this changes the nature of risk from isolated incidents to continuous operational exposure. Production becomes sensor-rich, software-driven, and tightly coupled to supply chains, cybersecurity, and compliance.

That increases the frequency of small failures that cascade into large losses, but it also creates a new advantage for insurers: the ability to price and manage risk dynamically using real-time data. The strategic consequence is clear: insurers will not win by simply insuring smarter factories. They win by underwriting behaviour, resilience, and control maturity across connected operations, then turning that into differentiated products, faster claims decisions, and better loss performance.

# Dominant subtrends

Industrial operations are becoming connected intelligence systems where data, automation, and control compound together. The Industrial Internet of Things creates the data backbone by connecting machines, infrastructure, and supply chains through continuous monitoring. Smart manufacturing then embeds sensors, robotics, AI, and digital twins into operations, creating new exposure surfaces: equipment failures, cyber-physical disruptions, and algorithm-driven operational errors.

**Industrial AI** completes the stack by industrialising prediction and control across factories, logistics, and quality systems. On the client side, AI-supported defect detection and predictive maintenance can reduce certain losses, but it also introduces new failure modes: model drift, automation bias, and opaque decision chains that complicate liability.

On the insurer side, the same technologies enable stronger fraud detection, faster claims automation, and sharper risk selection. The combined effect shifts the insurance problem from single-point failures to cascading systems risk. More devices mean more dependencies. More automation means more ways for cyber incidents to stop production, damage equipment, and trigger safety incidents.

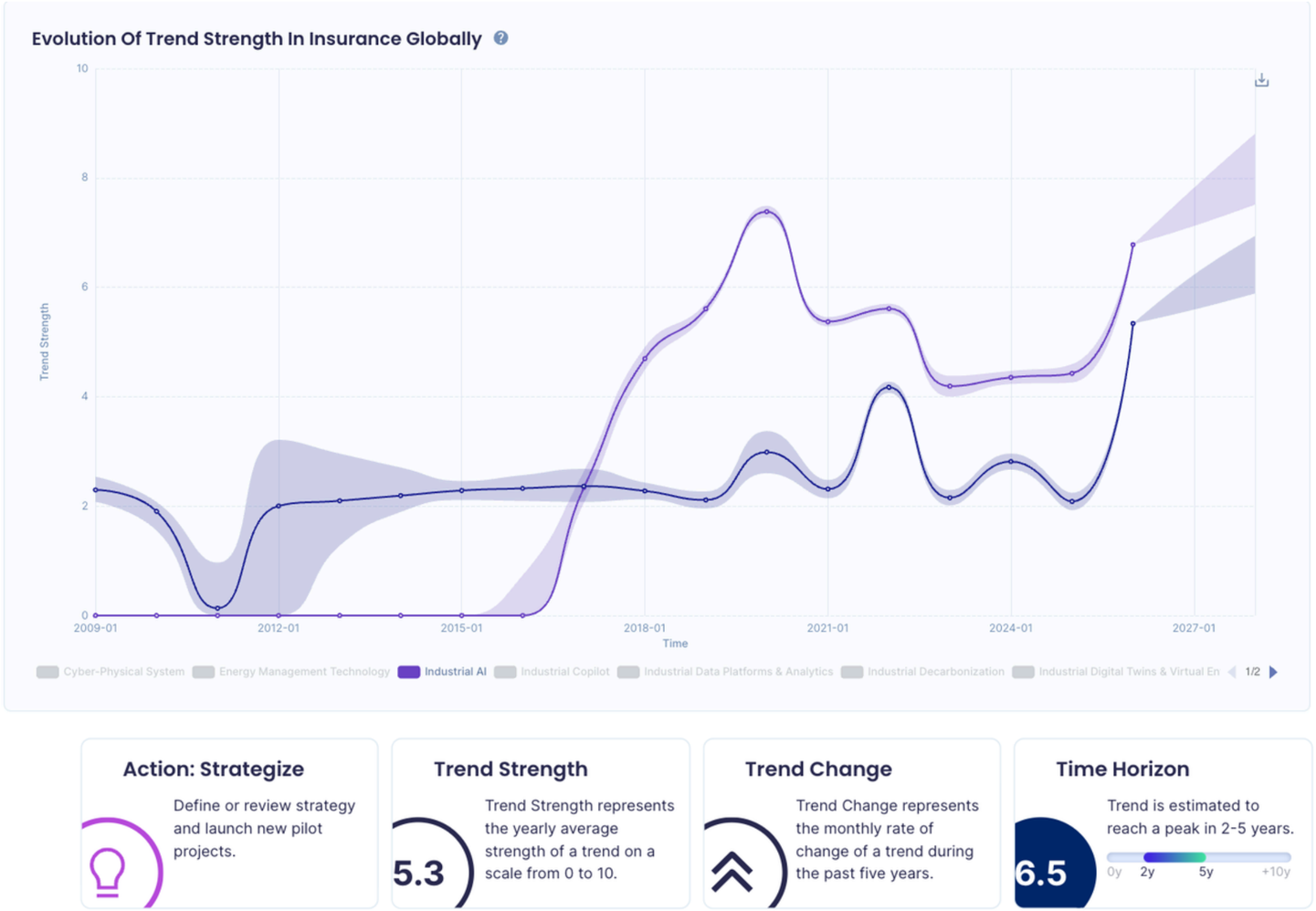



***Image 4:*** *Trendtracker data: on global hyper-personalization in insurance, structurally growing since 2017.*

# Dominant subtrends Continued

Accumulation risk rises when many insureds rely on similar platforms, protocols, and vendors. But this connected stack also gives insurers a pathway to move from static questionnaires to evidence-based underwriting. When production telemetry, maintenance signals, and safety data become available, pricing can reflect actual risk controls rather than assumptions.

> *"Global Factory Robot Workforce has more than doubled in 10 years."*
>
> ***IFR, International Federation of Robotics, 2025***

Industry 5.0 reframes this automation-first logic around **resilience and human performance**. The focus shifts to durability under disruption and the well-being and effectiveness of human workers inside automated systems.

This matters because many losses still originate in human-machine interfaces, training gaps, operational shortcuts, and safety culture.

The insurance implication is direct: product design must move toward resilience features, including sustainability-linked structures, workforce safety analytics, and coverage that rewards measurable risk reduction.

Underwriting must align with new compliance expectations around sustainability, consumer protection, and ethical operations, which increasingly affect both reputational loss and regulatory exposure. Resilience serves as both an underwriting variable and a customer retention strategy, as it determines whether policyholders can continue operating under stressed system conditions.

For insurers, this means the value proposition shifts from insuring assets to underwriting behaviour and control maturity across connected operations.

**Samples of articles analyzed by Trendtracker**

- Physical AI: Powering the New Age of Industrial Operations, World Economic Forum, 24 Sep 2025
- Towards human-centric, sustainable and resilient energy-intensive industries, European Commission (CORDIS / Horizon Europe), 28 Apr 2025
- 2026 Manufacturing Industry Outlook, Deloitte Insights, 13 Nov 2025
- How We Measure the Readiness of Countries for Industry 5.0, Oliver Wyman Forum, 2025

# Potential risks and blindspots

**Cyber incidents in connected factories are not only data events.**

They can stop production, damage equipment, and trigger safety incidents. Traditional cyber and property models underestimate correlation across systems and vendors, which leads to mispriced accumulation and surprise loss clusters. When production depends on always-on connectivity, cyber resilience becomes operational resilience. Insurers that cannot quantify this drift into coverage disputes, tighter exclusions, and weaker relevance to industrial clients.

**Operational accountability blurs as automation expands.**

Responsibility is fragmented among the manufacturer, the software vendor, the integrator, and the insured. That ambiguity accelerates claims disputes and litigation because loss causality is harder to prove, and duty-of-care standards evolve unevenly. This raises liability volatility and increases the burden on policy wordings, claims expertise, and governance-grade evidence trails.

**Connected production assumes stable energy and stable networks.**

When outages occur, they create cascading losses across production, logistics, safety systems, and quality compliance. The insurance impact extends beyond business interruption to supply chain contagion, delayed claims verification, and higher loss amplification. At a societal level, these failures raise the cost of physical goods, reduce the reliability of essential supplies, and increase political pressure on the resilience of critical infrastructure.

# Recommended strategic initiatives

**Build real-time risk assessment products anchored in industrial data.**

Industrial clients are deploying IIoT at scale. Insurers without data integration capabilities will be forced into commodity pricing or excluded from sophisticated buyers who demand evidence-based risk assessment. The window to build these capabilities is 18-24 months before market expectations harden.

Move beyond periodic risk surveys by using IIoT and operational data to continuously assess exposure and controls. This enables more accurate pricing, faster underwriting decisions, and better early-warning risk services. It creates a defensible path to expand coverage by actively managing risk, as the insurer can observe and control quality rather than assume it.

**Launch cybersecurity assurance for connected factories and cyber-physical interruption.**

Cyber risk is now embedded in production continuity and supply reliability. Specialised coverage should reflect the operational reality of connected production: downtime, recovery costs, and liability driven by industrial connectivity.

The differentiator is pairing coverage with measurable improvements in security posture through partnerships, monitoring, and control validation. This reduces loss volatility while increasing pricing power, as the insurer becomes a risk-improvement actor rather than merely a payer.

Insurers that treat cyber-physical risk as separate from traditional property and casualty lines will see higher claims correlation and weaker margin protection.

**Scale digital twin insurance services to proactively prevent risk.**

Industrial firms are rapidly adopting simulation and predictive tooling. This creates a market expectation that insurers can price and support risk proactively, not only pay claims reactively. Insurers without these capabilities will lose access to sophisticated industrial buyers.

Digital twins simulate failure modes, test resilience investments, and quantify the benefit of controls before losses occur. This supports better underwriting, faster claims triage, and more credible advisory services tied to annual contracts rather than one-off policies.

The commercial impact is higher retention and the ability to defend premium levels through demonstrated value beyond claim payment.

> *"Some insurers are collaborating with technology partners to cocreate hybridproducts, integrate protection with prevention through real-time underwriting, continuous portfolioassessment, and IoT-enabled sensor monitoring."*
>
> ***Deloitte,***
> ***Global Insurance Outlook 2026***

# Growth initiative: Risk dividend contract

Offer a Risk Dividend Contract for smart factories. Premiums and coverage conditions adjust automatically based on verified operational controls: IIoT data, safety wearables, and predictive maintenance signals.

The insurer sets a target risk trajectory with the client. They then share the economic upside when the measured risk reduction is sustained. This is achieved through automatic premium rebates, expanded coverage triggers, or reduced deductibles.

This turns prevention into a contractual mechanism rather than a marketing slogan. It monetises what clients actually want in Industry 5.0: safer operations, higher uptime, and fewer surprises.

It also directly addresses cyber-physical fragility and accountability gaps by establishing an auditable, data-backed control record that reduces disputes when things go wrong.

Competitors can offer usage-based pricing, but they cannot easily replicate the continuous verification infrastructure, actuarial modelling for dynamic risk trajectories, and the depth of client relationships required to deliver performance-based contracts that adjust in real time based on operational evidence.

# 05
# Geostrategic Deglobalisation

# Introduction

**Geostrategic Deglobalisation** is the shift from one global rulebook to multiple competing power blocs, each shaping its own rules for trade, technology, capital flows, and security. What used to be an efficiency game built on scale is becoming a resilience game built on adaptability. For insurance, this is not a background geopolitical narrative

It directly rewires risk frequency, severity, correlation, and legal interpretation across markets. It also increases operating friction due to divergent regulations, sanctions, data rules, and standards. Insurers that keep a single global operating model will accumulate hidden exposure and compliance drag.

Insurers that build region-ready underwriting, claims, and data capabilities will price risk with more confidence, protect margins, and stay relevant as clients restructure how they operate.

# Dominant subtrends

Tariffs, export controls, and sanctions are becoming routine operating conditions rather than rare disruptions. They fracture risk pools and amplify correlation across insureds who share trade corridors, suppliers, and logistics chokepoints. A single policy move can cascade from procurement disruption into business interruption, credit stress, insolvency, and litigation, often within one renewal cycle.

Corporations are responding through nearshoring, reshoring, and friendshoring, rebuilding supply chains around proximity and political alignment rather than cost alone. That relocation creates fresh accumulation zones in new industrial hubs and introduces transition risk: unstable early operations, labour availability constraints, infrastructure maturity gaps, and cyber exposure as supply chains digitise.

**Digital sovereignty** hardens this fragmentation into a technical reality. Data residency and sovereign cloud expectations are moving from policy debate to procurement requirement. For insurers, this is both an internal constraint on architecture and vendor choices and a market signal.

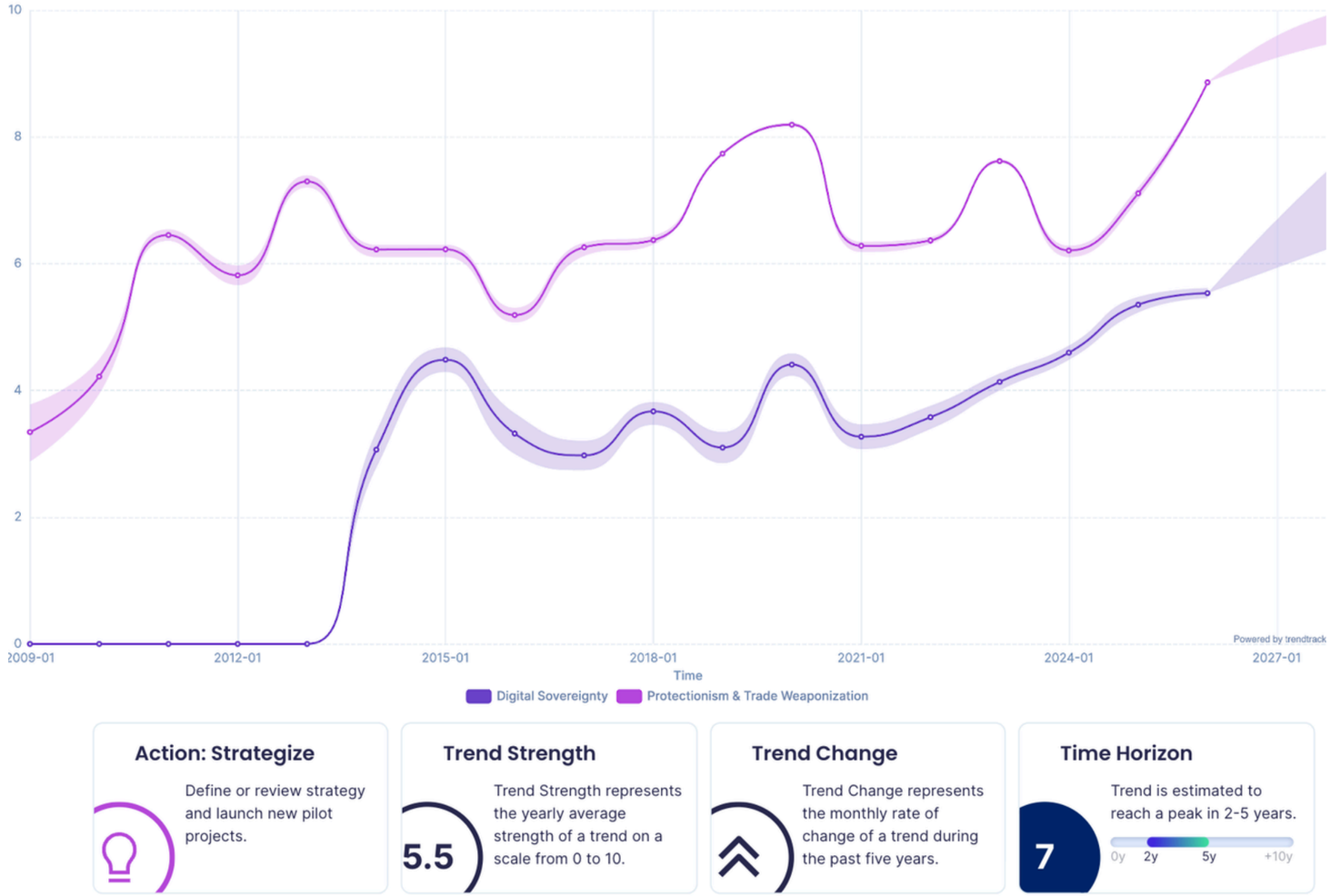



***Image 5:*** *Trendtracker data: Digital sovereignty surges past protectionism & trade weaponization post-2021, fueling insurer data localization.*

# Dominant subtrends Continued

Trust increasingly depends on proving region-ready security, auditability, and lawful data handling. This amplifies the cost of getting digital wrong while creating differentiation for insurers that can prove compliant, secure capabilities without collapsing efficiency.

> *"Sovereign clouds are designed so that sensitive information is held within the jurisdiction of the country whose data is on the network."*
>
> ***BCG, Sovereign Clouds Are Reshaping National Data Security2026***

Geopolitical decoupling is pushing the industry beyond trade shocks into the realm of model risk. Historical assumptions about market access, dispute resolution, and cross-border enforceability are becoming less reliable. Sudden rule changes turn tail risk into baseline volatility.

This shifts demand toward scenario-based underwriting, tighter accumulation control, and reinsurance strategies that can absorb higher variance when diversification benefits weaken across geopolitical blocs. Decoupling also intensifies cyber risk as state-linked activity and cross-border digital conflict become more material.

Supply chain rewiring turns that volatility into a systems problem. Disruption is less about single events and more about cascading failures across digitised logistics, regulatory delays, localised production complexity, and route volatility in trade-adjacent sectors. Insureds expect coverage that reflects failure points across logistics technology, regulatory delays, and production complexity.

This is especially visible in marine, shipping, and trade-adjacent sectors where volatility and route changes reshape accumulation risk. The competitive edge shifts toward insurers that can underwrite resilience as a measurable capability, rather than just insure disruption as a payout event.

That requires connecting geopolitical signals, operational telemetry, and coverage design into a single operating model that stays credible when the rulebook changes mid-game.

**Samples of articles analyzed by Trendtracker**

- Cloud Sovereignty Framework, European Commission, 01 Oct 2025
- Financial stability risks from geoeconomic fragmentation, European Central Bank, 30 Jan 2026
- Global Insurance Market Report 2025, International Association of Insurance Supervisors (IAIS), 09 Jun 2025
- Global Trade Outlook and Statistics, World Trade Organization, 07 Oct 2025

# Potential risks and blindspots

**Portfolio correlation is rising under the illusion of diversification.**

As markets fragment, many portfolios become more correlated, not less. Tariffs, sanctions, logistics shocks, and inflation hit multiple insureds simultaneously because they share suppliers, corridors, and regulatory dependencies. This overwhelms pricing assumptions and stresses reinsurance structures because multiple lines move together. The systemic impact is contagious disruption. When many firms optimise for the same corridors and compliance regimes, disruption spreads faster and recovery slows.

**Compliance failures invalidate coverage positions, not just create fines.**

In a multi-rulebook environment, compliance failures can void coverage, trigger disputes, and create reputational damage that weakens distribution and renewal economics. Digital sovereignty intensifies this because regulators can demand provable controls over data location, processing, and audit trails.

The broader impact is erosion of trust in financial infrastructure. When citizens and firms doubt that data is protected and decisions are defensible, adoption of digital services slows, and economic coordination becomes harder.

**Underwriting supply chain transformation without operational data drives adverse selection.**

Many insurers will try to sell supply chain and trade disruption coverage using legacy questionnaires and periodic reporting. That misses the reality that risk posture can shift weekly as suppliers change, routes reroute, and policies change. Without stronger data-sharing models and AI-supported monitoring, insurers drift into adverse selection where the most exposed clients buy the most cover at prices that do not reflect current risk.

The systemic impact is mispriced risk transfer. When insurance fails to reflect real risk posture, capital is allocated badly, and resilience investments are delayed.

# Recommended strategic initiatives

### Build a regulatory intelligence and compliance operating system.

Regulatory fragmentation is accelerating. Non-compliance now creates both direct penalties and coverage disputes that can invalidate entire policy positions. Insurers have 12-18 months before multi-jurisdiction operations become materially more expensive without proactive compliance architecture.

This initiative moves from periodic legal reviews to continuous monitoring of trade rules, sanctions, data residency requirements, and sector-specific obligations. It wires those signals into underwriting rules, policy wordings, claims triage, and vendor management. This delivers fewer compliance surprises, faster product localisation, and stronger defensibility under regulatory challenge.

It also protects distribution relationships, as sophisticated corporate buyers increasingly audit insurers' compliance capabilities before renewal.

### Industrialise AI-driven risk assessment for geopolitics and supply chains.

The goal is decision-grade analytics that improve underwriting selection, accumulation control, and pricing refresh cycles by combining external signals with insured-specific operational data. This shifts insurers from reacting to events after they occur to continuously pricing risk posture.

The commercial advantage is better loss ratios through selection and the ability to adjust pricing between renewal cycles as conditions change. This creates a platform advantage because the same capability supports trade-disruption coverage, supply chain resilience products, and cyber-related offerings as digital operations expand under decoupling pressure.

Insurers that delay lose the data accumulation needed to train models that can differentiate good risk from bad risk in fragmented markets.

### Create a modular product suite for trade disruption and resilience.

Clients do not treat geopolitical shifts as a single risk. They experience a stack of issues: business interruption, supply chain delays, cyber disruption, regulatory delays, liability, and governance exposure.

A modular suite allows insurers to tailor coverage to sector- and corridor-specific realities, then scale distribution without reinventing every product for every market.

This delivers growth with discipline through better risk selection, clearer triggers, and greater value to clients, rebuilding operations under uncertainty. Competitors offering generic global policies will see adverse selection as the riskiest clients concentrate on broad coverage while sophisticated buyers cherry-pick specialised protection.

# Growth initiative: Resilience subscription

Launch a resilience subscription that merges insurance, monitoring, and action into one contract. Sell a continuously updated risk posture service for multinational and mid-market firms that are rewiring suppliers and operating across blocs.

Add a Policy Integration Platform layer: one dashboard that consolidates all relevant coverages, tracks regulatory and sanctions changes, and translates them into clear triggers and guidance so clients know what is covered, where, and under which conditions.

The subscription adds dynamic risk scoring, automated alerts for tariff and sanctions shifts, pre-approved mitigation playbooks, and coverage that adjusts based on measured improvements such as supplier diversification, cyber controls, and verified compliance steps.

This sets an insurer apart because it stops being a claims payer and becomes the operating partner for staying insurable. In a deglobalising world, that is the rarest currency: confidence that a firm can keep operating, not only recover after it fails.

Competitors can offer parametric triggers or supply chain coverage, but they cannot easily replicate the integrated compliance intelligence, real-time monitoring infrastructure, and multi-year client relationships required to deliver adaptive coverage that tracks operational reality rather than annual declarations.

# 06
# The Robot Economy

# Introduction

**The robot economy** is moving from pilots to infrastructure. Autonomous robots and AI-controlled systems are becoming a practical answer to labour shortages, throughput pressure, and rising expectations for safety and reliability.

This matters for insurance because it shifts the centre of risk from individual human behaviour to engineered systems, software, and fleet operations.

Underwriting advantage will increasingly come from how well insurers can price physical execution risk using real operating data, shape liability frameworks as they evolve, and redesign products that reward prevention rather than pay after failure.

# Dominant subtrends

**Autonomous vehicles and robotaxi systems** are rewriting the fundamental logic of motor insurance. The insurable event is no longer human behaviour but system performance: sensors, perception models, software updates, safety cases, remote assistance, mapping dependencies, and cybersecurity posture.

Liability migrates from drivers to manufacturers, platform operators, and fleet managers because the cause of an incident becomes technical, auditable, and litigated across multiple parties. Underwriting shifts from person and history to machine and proof. Claims shift from witness statements to telemetry, logs, and version control. Robotaxis industrialise this at fleet scale, turning autonomy into public infrastructure with high-frequency rides and dense urban exposure.

Risk concentrates into fewer policies with higher limits and tighter scrutiny. Product design must evolve rapidly: per-trip micro-coverage, passenger injury embedded into fares, fleet cyber coverage, and component-level damage policies for expensive sensor arrays. The insured becomes an ecosystem-spanning operator, OEM, software supplier, mapping provider, and remote operations provider. Dispute resolution becomes a technical exercise rather than a narrative about behaviour.

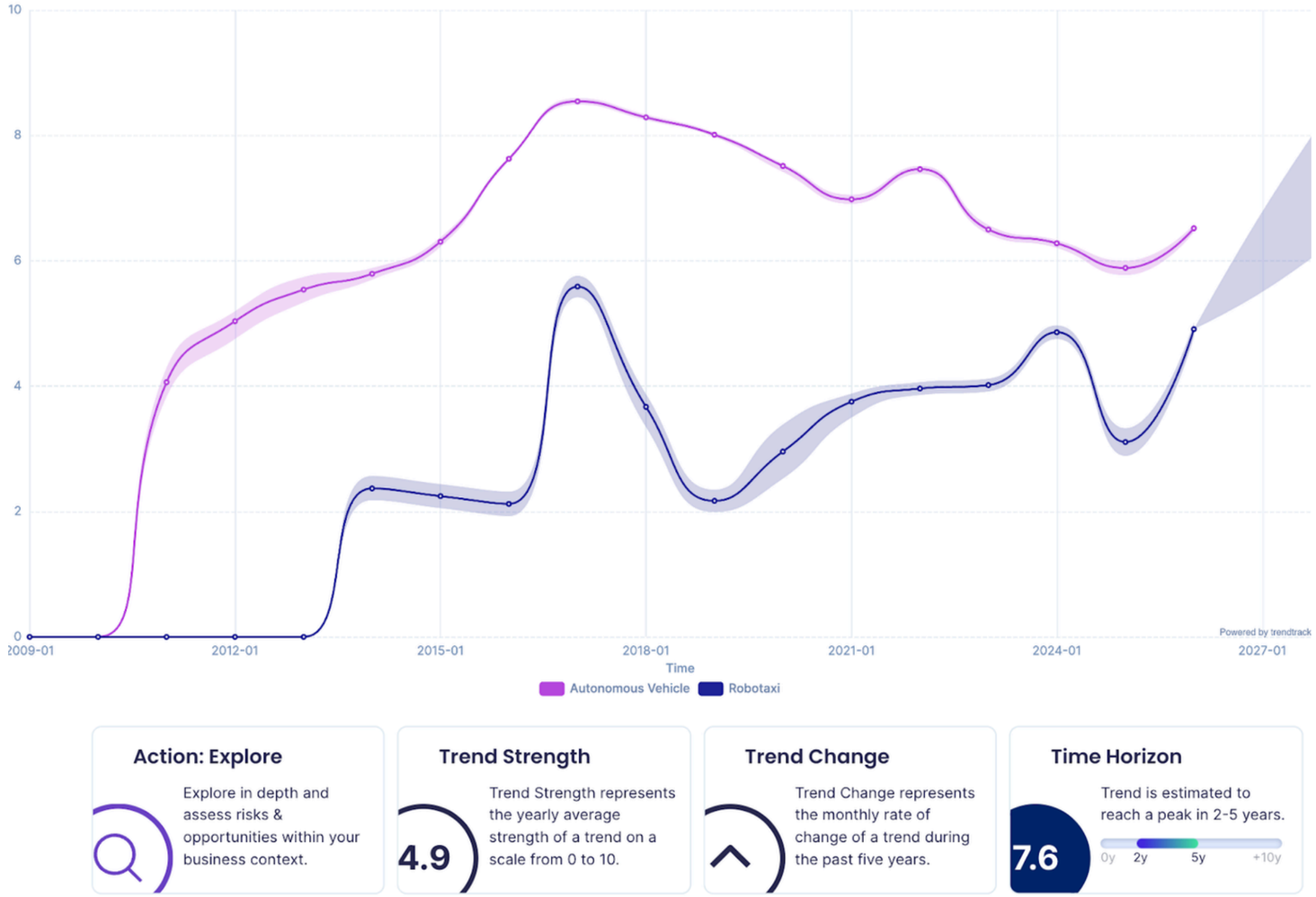



***Image 6:*** *Trendtracker's data show Autonomous vehicles & robotaxis diverge post-2022, with AVs accelerating amid liability shifts for insurers.*

# Dominant subtrends Continued

> *"The robotaxi market is expected to continue its rapid ascent, reaching an estimated $33.49 billion by 2030 with a CAGR of 57.1%"*
>
> ***The Business Research Company, 2026***

Physical AI extends this logic beyond roads into machines that sense, decide, and act across warehouses, hospitals, infrastructure, and construction. The attack surface expands because cyber risk now has physics. Data loss becomes uptime loss, safety loss, and continuity loss. Risk becomes more measurable in real time through operating signals, maintenance logs, anomaly detection, and performance metrics.

This turns insurance from a promise to pay later into a pricing and prevention engine now because verified signals allow dynamic premiums, automated claims triggers, and incentives tied to provable controls.

Healthcare robotics sharpens this pressure by placing Physical AI into regulatory oversight with human bodies at stake. Robot-assisted surgery, telesurgery, rehabilitation robotics, and hospital automation rewrite how insurers must separate malpractice, product liability, and cyber exposure when outcomes are co-produced by clinician, machine, software updates, and network reliability.

Patient safety and cyber resilience fuse into a single underwriting concern. Fewer complications and shorter recovery can reduce downstream payouts, while higher capital costs, maintenance dependencies, and high-severity tail risk increase the need for specialised coverage.

Agricultural robotics reveals the endgame clearly. As farms adopt autonomous tractors, drones, and precision systems, traditional labour exposure shrinks, but insurance relevance migrates into machine reliability, data integrity, and operational continuity.

This shows what happens when autonomy scales: safety improvements pressure legacy premiums, while connectivity and automation create new specialty lines for insurers who can price systems rather than people.

**Samples of articles analyzed by Trendtracker**

- How autonomous vehicles will change the future of car insurance, S&P Global Mobility, 3 Sept 2025
- Independent Audits of Waymo's Safety Case and Remote Assistance Programs, Waymo, 5 Nov 2025
- Boston Dynamics & Google DeepMind Form New AI Partnership to Bring Foundational Intelligence to Humanoid Robots, Boston Dynamics, 5 Jan 2026
- As AI enters the operating room, reports arise of botched surgeries and misidentified body parts, Reuters, 9 Feb 2026

# Potential risks and blindspots

**Liability becomes multi-party and technically complex.** Claims move from incident handling into attribution across manufacturer, software provider, fleet operator, and data vendor. This raises defence costs, lengthens settlement cycles, and increases correlation when a shared component fails across many insureds. Insurers underestimating this complexity will underprice liability exposure and face persistent dispute costs that erode margins.

**Cyber-physical accumulation, where digital and physical risks converge, is growing faster than pricing models can keep pace.** Autonomous fleets (vehicle groups that operate without human drivers) and Physical AI (artificial intelligence systems that control physical operations) create common-mode exposure, meaning a single event can affect many at once.

One vulnerability, an update failure, or data compromise can cause simultaneous losses across many policyholders. This risk combines bodily injury, property damage, business interruption, and liability in correlated ways. Treating these exposures as independent will lead to unexpected accumulation losses for insurers.

> *"Insurers must develop comprehensive cyber policies while working with fleet operators to implement robust cybersecurity measures."*
>
> ***BCG, Insurance 2025***

**Prevention reduces traditional premiums and demands a business model change.** If autonomy lowers accident frequency and cuts some operational losses, legacy premium pools shrink. Without new products linked to technology risk, performance guarantees, and service revenue, insurers may win safety but lose out on growth. For society, insurance shifts from a financial backstop to a market ruleset for safe autonomy.

If insurers cannot price multi-party accountability, manage cyber-physical accumulation, or replace shrinking legacy pools with prevention-linked products, autonomy may become underinsured or too costly to scale. This slows adoption, raises friction around safety and trust, and shifts risk to governments, courts, and consumers.

# Recommended strategic initiatives

**Build liability and risk assessment models for autonomous systems.**

Liability is shifting from individuals to manufacturers and operators. Design underwriting logic that treats autonomy as a system of components, software versions, operational controls, and fleet governance.

Insurers that operationalise product liability, cybersecurity, and operational accountability as an integrated model will price more accurately, defend claims more effectively, and avoid adverse selection as autonomy scales.

Early development of legal expertise and partnerships with autonomous vehicle manufacturers and fleet operators is critical. Policy language, data access, and loss forensics must mature at the same pace as deployment. Liability norms are being rewritten now. Insurers unable to defend causality and accountability will underprice risk or lose relevance in fast-growing autonomous segments.

**Industrialise embedded, usage-based, and dynamic pricing models using real telemetry.**

Move beyond pilot telematics. Focus on repeatable data ingestion, pricing adjustment, and claims automation. Autonomy increases transaction volume and compresses margins.

Winners will run high-frequency, data-driven underwriting at low cost. They will use verified signals to reward prevention in ways clients understand and trust. Traditional annual policies cannot serve per-trip robotaxi economics or real-time Physical AI deployments.

Insurers unable to operationalise continuous pricing will be locked out of the highest-growth autonomous segments.

**Develop specialised products for technology failure and fleet operations.**

Redesign underwriting to price technology failure, software updates, sensor performance, and fleet operations as primary risk drivers.

Align claims handling to investigate product and system failures rather than human error.

This matters because autonomous systems demand different coverage structures: component-level property damage, cyber-physical business interruption, multi-party liability, and performance guarantees. Insurers offering only adapted motor policies will see sophisticated fleet operators and manufacturers choose specialists who understand the actual risk drivers.

# Growth initiative: Autonomy assurance layer

Create an autonomy assurance layer that bundles insurance with continuous verification. Offer a certification-grade safety and cyber posture service for autonomous fleets and Physical AI deployments. Use live telemetry to score controls, detect drift, and trigger mandatory remediation before coverage lapses.

Premiums adjust automatically when verified risk controls improve or degrade. Claims handling is designed around system evidence, not testimony, which cuts dispute time and legal cost.

This approach makes the insurer a trusted referee of machine safety, not just a payer after failures. It directly addresses core risks. System evidence enables multi-party liability management. Continuous monitoring makes cyber-physical accumulation visible. Prevention generates revenue through verification services rather than shrinking premiums.

Competitors can offer similar policies, but not a proprietary assurance loop built from live data, dynamic actuarial risk models, technical expertise in autonomy, and strong ties with fleet operators and manufacturers focused on real-time risk verification.

# 07
# Ultra Urban Systems

# Introduction

**Ultra Urban Systems** represents a fundamental shift from cities as static infrastructure to cities as programmable, sensor-driven operating environments. Traditional risks in cities were often driven by isolated physical events, such as accidents or individual system failures. Now, roads, buildings, grids, and logistics are being instrumented to sense, predict, and optimise in real time.

For insurers, this transformation changes how risk is defined and assessed. Digitally managed urban systems mean that key risk factors shift from isolated, physical incidents to new, systemic behaviours: software updates can introduce new types of failures, real-time sensor data can alter liability decisions, and interconnected systems can turn minor disruptions into widespread, cascading claims.

As a result, insurers must shift from responding to individual losses to proactively managing risk arising from the behaviour of interconnected systems. Competitive advantage will be found in dynamic pricing of exposures, using connected data to reward preventive actions, and in monitoring accumulation risk that can now span entire urban platforms.

# Dominant subtrends

**Urban mobility and energy systems** are converging into programmable infrastructure. Mobility is becoming electrified, regulated, and data-rich. EV repair costs, battery risks, charging behaviours, and infrastructure dependencies require specialised coverage that traditional motor templates cannot address.

The real shift is that underwriting can move from driver history to live mobility context using telematics, charging patterns, and traffic optimisation signals. This enables continuous risk adjustment rather than annual static pricing. Urban transport compounds this complexity through usage-based mixes across ride-hailing, car sharing, micro-mobility, and subscription access.

Coverage must follow the user and the trip, not the vehicle and the annual policy. This drives reliance on AI-driven underwriting and claims automation because on-demand mobility creates high transaction volumes, small premiums, and frequent micro-claims. It also raises accumulation risk when a single platform change affects many insured journeys simultaneously.

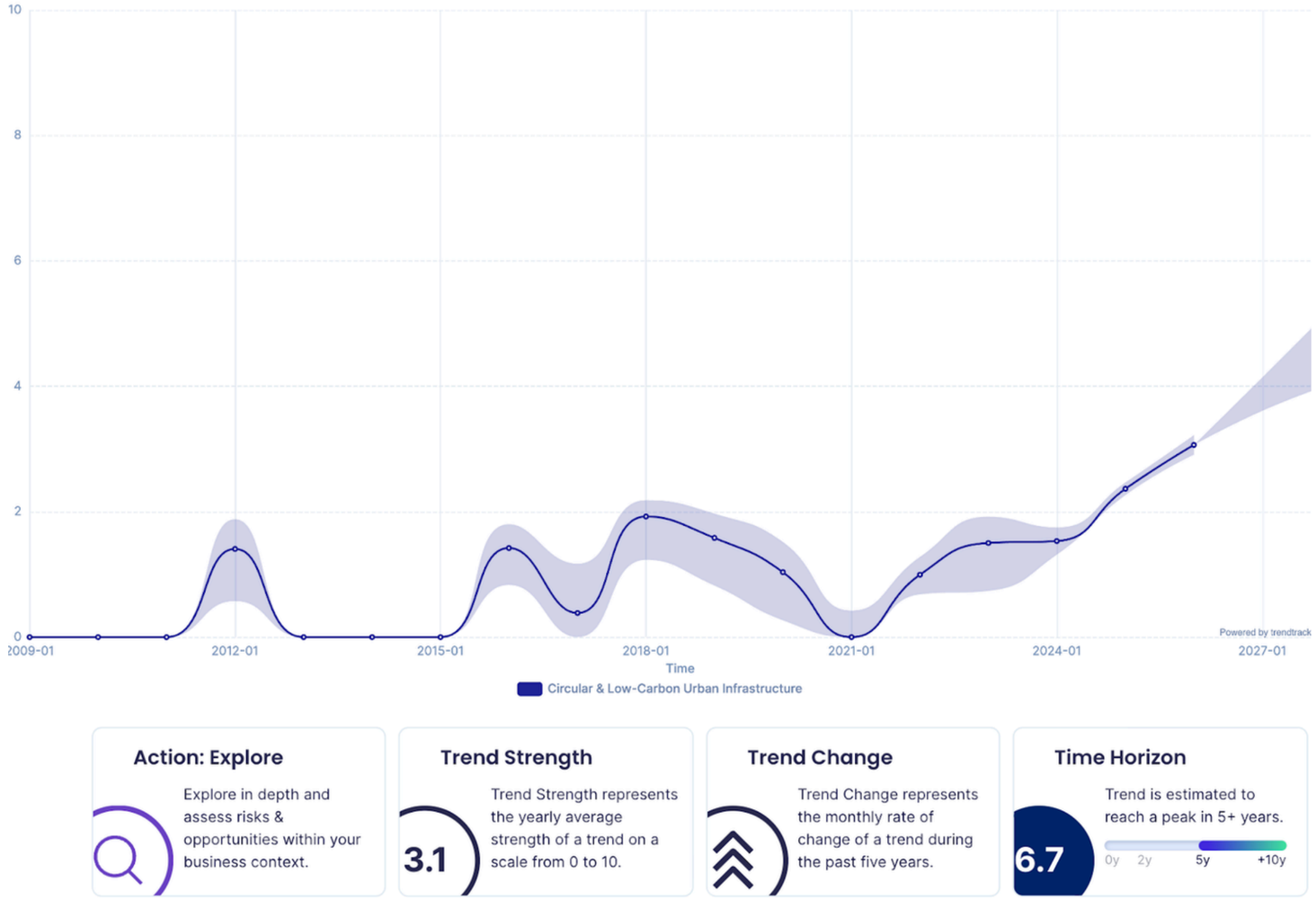



***Image 7:*** *Trendtracker data: Circular & low-carbon urban infrastructure stabilizes post-2022 surge, vital for insurers hedging climate risks.*

# Dominant subtrends Continued

The backbone enabling all of this is the decentralisation and software control of smart grids. Grids now manage microgrids and distributed energy resources, which improves adaptability but increases exposure to cyber and integration failure. When grids fail, everything fails together because mobility electrifies, buildings digitise, and infrastructure decarbonises only if energy systems become more adaptive.

> *"The global smart building market grows with an estimated compound annual rate between 21.8% and 29.7%."*
>
> ***Fortune Business Insights, 2025***

Buildings are becoming simultaneously measurable and sustainable environments. Sensors now detect leaks, fire risks, air quality, occupancy patterns, and equipment health.

This shifts property risk mitigation from periodic inspection to continuous prevention, altering claims frequency, reducing loss severity, and enabling premium logic tied to proven controls. Green building accelerates this because sustainability is becoming a compliance requirement and a capital allocation signal.

New materials, retrofit processes, and evolving standards create transition risk and novel failure modes. Better energy performance and water management can reduce certain loss drivers over time, but sustainability without measurement is just paperwork. **Circular and low-carbon urban infrastructure** connects these dynamics by pushing recycling, reuse, and low-carbon materials into construction and energy systems.

This raises new insurance questions about performance guarantees, supply quality, and long-tail liability, including decommissioning and waste streams from renewable hardware. When recycling systems break down or materials underperform, losses manifest as property damage, business interruption, and liability disputes across the same interconnected urban systems.

**Samples of articles analyzed by Trendtracker**

- Sustainable commuting around urban areas, European Court of Auditors, 4 Feb 2026
- Enhancing resilience: Climate-proofing power infrastructure, IRENA, Dec 2025
- Urban nodes, European Commission, 10 Dec 2025
- Buildings, Energy Efficiency 2025 (analysis), International Energy Agency, 2025

# Potential risks and blindspots

**IoT data dependencies create regulatory and product risks.**

When smart device data becomes part of underwriting decisions, privacy compliance failures stop being back-office issues and become product risks that trigger disputes, fines, and customer and regulatory credibility losses.

Regulation will increasingly define what data can be collected, how it can be used, and which technology standards must be met. Insurers treating this as a technical compliance question rather than a strategic product risk will face sudden coverage disputes and market access restrictions.

**Urban digitisation creates hidden accumulation exposure.**

When many insureds share the same mobility platform, grid control layer, or building management vendor, correlation rises sharply. A single vulnerability can become a city-scale loss event. This undermines portfolio diversification and makes volatility harder to manage. Efficient systems are optimised until they fail, then they fail in sync.

Insurers treating urban digitisation as a background trend rather than a new exposure topology will misprice accumulation and face surprise loss clusters.

**Electrification and digital control introduce new failure modes that are poorly captured by historical claims data.**

Grid instability, cyber disruption, or cascading outages can trigger simultaneous business interruption, property loss, supply chain impacts, and public safety claims. This tests policy wording, business interruption triggers, and event aggregation logic. At a societal level, urban life depends on power for mobility, healthcare access, heating, cooling, payments, and communications. An outage becomes a civic disruption, not an inconvenience.

# Recommended strategic initiatives

**Build connected-risk underwriting that prices prevention, not declarations.**

Productize data partnerships with building sensors, telematics, and energy systems to continuously verify risk controls. Competitors can copy product features, but they cannot quickly copy live risk signals integrated into underwriting and claims.

This delivers lower loss frequency through earlier detection, fewer disputes through better evidence, and defensible pricing that rewards real mitigation rather than self-reported compliance. Insurers that continue to rely on annual declarations while competitors price live risk will see adverse selection as the best risks migrate to evidence-based pricing.

**Redesign policies for platform-based mobility and urban services.**

Mobility and infrastructure are moving toward usage-based access rather than ownership. Coverage must follow the user, the trip, and the service relationship with clear triggers for liability handoffs across operators.

Transaction volumes will rise while the premium per event shrinks, making operational cost the differentiator.

This improves relevance in new distribution channels such as ride-hailing and shared fleets while reducing claims leakage through standardised, platform-native workflows. Traditional annual motor policies will become irrelevant for the growing segment of urban mobility users who never own vehicles.

> *"The market sizes of shared transport (such as ride-hailing) and micromobility (such as e-bicycles) are expected to double by 2030 in developed economies."*
>
> ***McKinsey & Company, Global Insurance Report 2025***

**Create an urban systems accumulation and scenario engine.**

Traditional catastrophe thinking is insufficient when the trigger is a software event, grid-control failure, or cyber-physical disruption that spreads through shared vendors. Institutionalise city-scale exposure mapping, vendor concentration analysis, and scenario-based pricing for interconnected urban risks.

Accumulation can build quietly through growth in smart buildings, EV adoption, and microgrid deployment. This protects portfolio stability, strengthens reinsurance strategy, and provides board-level risk confidence. Insurers that discover accumulation concentrations only after loss events will face reinsurance disputes and questions about capital adequacy.

# Growth initiative: Urban operating system insurance

Build a single subscription-based risk platform that insurers sell to city-linked ecosystems: mobility platforms, EV charging operators, fleet owners, and energy system operators. Bundle three capabilities into one contract: usage-based mobility cover priced through telematics, continuous AI-driven risk scoring across connected assets, and cyber-physical protection for smart grid dependencies.

Include real-time prevention triggers so that when sensors detect risks across the ecosystem (unsafe charging, equipment stress, grid instability), the system automatically activates approved mitigation partners and adjusts coverage parameters.

The differentiator is not coverage components, but orchestration: one onboarding, risk dashboard, claims workflow, and prevention actions, all triggered by live data. This attacks the biggest failure mode, fragmented responsibility and slow coordination. Commercially, it creates recurring revenue and locks in ecosystem distribution.

Competitors may offer usage-based insurance or parametric triggers, but cannot easily match a platform with multi-party coordination, unified data, automated claims, and ecosystem relationships for adaptive coverage across mobility, energy, and buildings.

# 08
# Engineered Humanity

# Introduction

**Engineered Humanity** is the shift from observing biology to actively engineering it. Biology becomes a programmable layer of the economy, driven by richer biological data from biomarkers to multi-omics, therapies tailored to smaller subgroups and even individuals, and the fusion of biology with electronics and computing, such as wearables and brain-computer interfaces.

For insurance, this is not a medical trend. It is a restructuring of risk itself. Underwriting moves from broad population averages toward molecular specificity. Claims move from standard pathways toward complex, individualised treatment regimens.

Product design is pulled into governance because privacy, non-discrimination, safety, and regulation become inseparable from pricing and coverage decisions. The insurers that win treat engineered biology as a new operating system for risk, not a niche benefit add-on.

# Dominant subtrends

Diagnostic precision is moving from population averages to molecular specificity. **Personalised and precision medicine** push insurance to pay for better signals before it can price risk more accurately.

Molecular diagnostics, pharmacogenomics, and targeted therapies raise upfront costs but reduce waste from wrong therapies and avoidable adverse events by matching treatment to biology. This shifts spending earlier in the care pathway, making underwriting politically sensitive. Once genetic and biomarker inputs touch risk assessment, privacy, and anti-discrimination move from compliance checkboxes to market permission requirements. Insurance built on broad averages becomes blunt in a world where care is engineered at the individual level.

**Omics and systems biology** scale this from diagnosis to trajectory forecasting through multi-omics, single-cell analysis, and spatial methods. This enables products that blend coverage with monitoring, prevention, and earlier intervention. It also tightens claims verification and data governance requirements because individualised regimens complicate processing and demand better systems to manage variability.

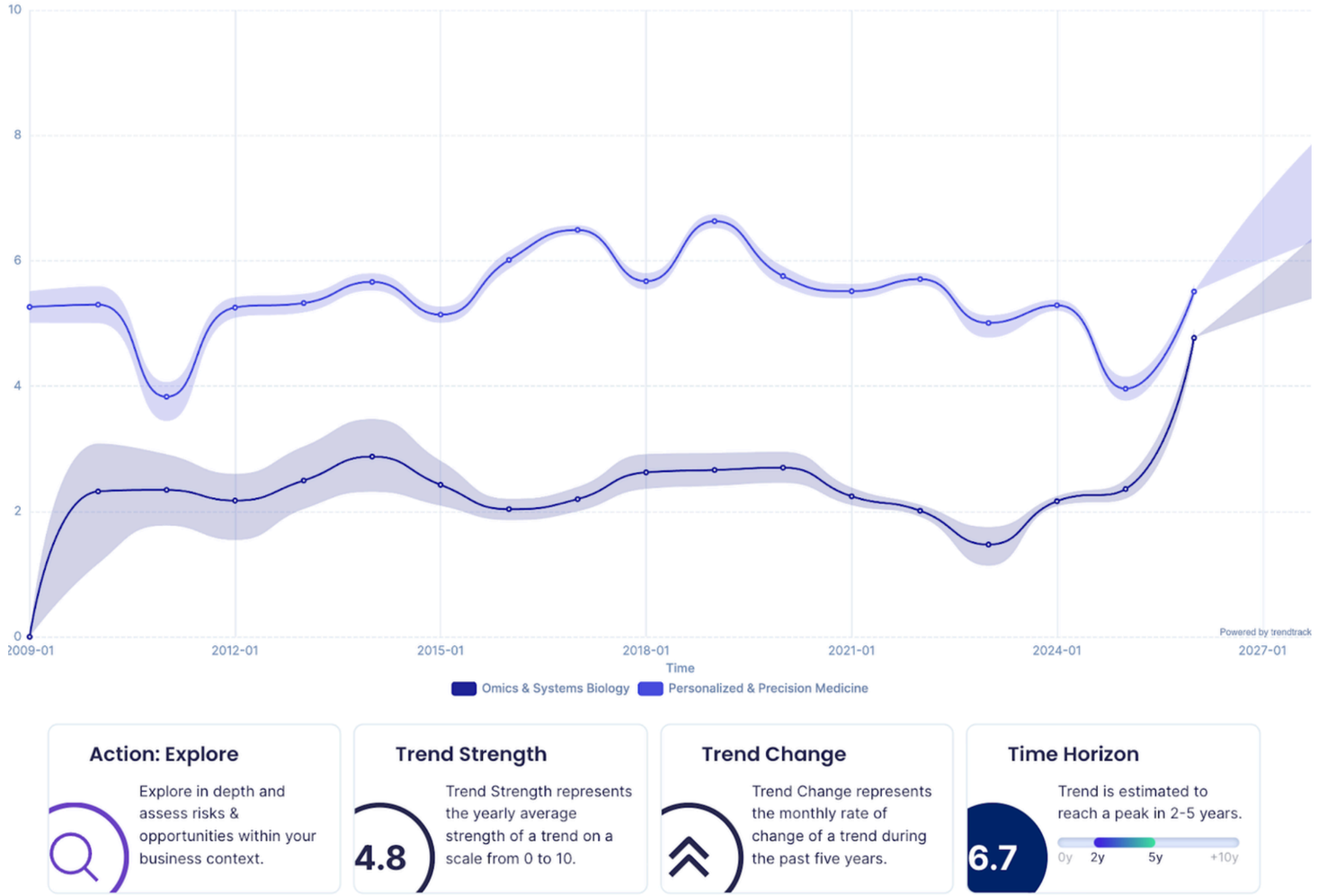



***Image 8:*** *Trendtracker data: Omics & systems biology surges post-2020, outpacing personalized medicine and reshaping insurance risk models.*

# Dominant subtrends Continued

> *"Precision medicine market is expected to reach roughly $213 billion by 2030, growing at a 14% CAGR, with some projections stretching toward $470 billion by 2034."*
>
> ***Mordor Intelligence, Feb 2026***

Therapeutic transformation is reshaping both longevity and high-cost claims. Artificial organs and replacement therapies introduce new cost spikes, complication profiles, and long-term monitoring needs. Replacement pathways and organoids increase pressure for more granular coverage structures, as outcomes vary by patient biology rather than just procedure type.

Patient-specific modelling is becoming standard practice, forcing insurers to price complexity rather than averages. Patient trust determines adoption rates, which directly affects portfolio performance.

If people do not trust these therapies, they will not use them, and the expected health outcomes will not materialise. Portfolio assumptions about mortality, morbidity, and long-term care costs depend on adoption patterns, not just technology capability.

This creates a new insurance dependency: therapeutic effectiveness requires patient engagement, regulatory approval, and provider adoption simultaneously.

**Samples of articles analyzed by Trendtracker**

- A roadmap to precision medicine through post-genomic electronic medical records, Nature Communications, 17 Feb 2025
- A soft robotic total artificial hybrid heart, Nature Communications, 3 Jun 2025
- Organoids for tissue repair and regeneration, Materials Today Bio (via ScienceDirect), Aug 2025
- Omics-based Clinical Trials Market (2025 - 2030), Grand View Research, 2025

# Potential risks and blindspots

**Genetic data becomes a pricing weapon before it becomes a trust contract.**

The blind spot is assuming data availability automatically equals an underwriting advantage. In reality, the use of genetic and biomarker data triggers privacy and non-discrimination scrutiny and forces new regulatory expectations. If insurers move faster than the trust and governance layer, the outcome is backlash, legal exposure, and product withdrawal risk.

Misuse or perceived misuse of genetic data amplifies inequality and erodes confidence in insurers and healthcare systems, slowing the adoption of early detection and personalised prevention that would otherwise reduce morbidity and costs over time.

**Cost shock from precision therapies creates coverage gaps and reputational liability.**

Precision treatments can reduce long-term costs by improving outcomes, but they raise immediate affordability concerns. A portfolio can become unstable if high-cost therapies rise faster than pricing models and reinsurance structures can adapt.

The practical impact is product mismatch: policies that do not reflect real-world care pathways, higher dispute frequency, and pressure to restrict coverage in ways that harm customer trust.

When engineered medicine exists but is inaccessible, it intensifies the health divide and increases long-term disability and dependency costs that re-enter the economy through employers, public systems, and families.

**Model confidence outpaces biological reality, creating silent mispricing.**

Omics increases predictive power, but translating complex signals into stable actuarial assumptions is difficult. Overconfident interpretation produces false precision in underwriting and claims adjudication.

This creates adverse selection and volatility when real-world outcomes do not match modelled trajectories. It also invites controversy when biomarker-based fraud detection or eligibility decisions are perceived as opaque or unfair.

Fragile model governance undermines acceptance of data-driven health systems and slows the shift toward prevention and early intervention that could benefit populations at scale.

# Recommended strategic initiatives

**Build a precision coverage stack that starts with diagnostics, not treatment.**

Move from reimbursing end-stage interventions to underwriting earlier decision points. Structure coverage for molecular diagnostics, pharmacogenomics, and precision screening paired with clear pathways into targeted therapies.

Insurers cannot price engineered medicine without paying for the signals that explain it. Medical outcomes improve when treatment selection is evidence-based, and claims volatility falls when avoidable adverse drug events and ineffective therapies decline.

Precision workflows are already being adopted in chronic disease and oncology pathways. Insurers that delay will subsidise costly late-stage care without the upstream controls that reduce it.

> *"It's now possible to imagine that a life insurer can predict and intervene in health events based on a simulated digital twin of a customer."*
>
> ***PWC, Insurance 2025 and Beyond***

**Stand up omics-ready underwriting and claims capability with auditable governance.**

Build analytics capability to interpret genomic and multi-omics inputs, train underwriters and actuaries, and create a compliance-grade data model that supports consent, access control, and traceability.

Modernise claims processing because individualised regimens complicate standard workflows and require better systems to manage variability. Engineered humanity breaks traditional rating factors.

This capability improves risk selection, accelerates claims handling, and creates defensible decisions when challenged by regulators, customers, or courts. The pace of data generation and the rapid spread of biomarker-based monitoring demand action now. Without this capability, insurers will either avoid the category or misprice it.

**Create collaborative health ecosystems that convert insurance into an outcomes partner.**

Partner with providers, precision medicine networks, and digital health platforms to enable value-based care mechanics, shared savings models, and continuous engagement through personalised insights and disease management tools.

Engineered humanity is not a one-time event. It is a longitudinal relationship with measurement, iteration, and adjustment. This creates a tighter link between prevention and pricing, better retention through tangible health value, and defensible differentiation as health insurance becomes increasingly commoditised. Ecosystems create switching costs.

If competitors own the provider and data partnerships, others will be left competing solely on premiums and exclusions.

# Growth initiative: Member-governed bio-data trust

Launch a member-governed bio-data trust that powers consented underwriting and pays customers back in value. Most insurers treat genomic and biomarker data as a compliance risk or a private asset. Flip the model. Create a governance-led bio-data trust where members explicitly control access to their omics and health signals, with clear rules governing how data can be used for pricing, prevention offers, and claims support.

This converts the most sensitive part of engineered humanity into a trust advantage rather than a reputational threat. It unlocks faster adoption of precision programs by enabling customers to see the exchange clearly through better coverage terms, targeted wellness support, or premium dynamics tied to verified health status. Engineered humanity will reward the insurers that can earn permission at scale.

This is how you industrialise permission. Competitors can launch genomic data programs, but they cannot easily replicate the governance infrastructure, member consent mechanisms, regulatory compliance framework, and transparent value-exchange model required to build trust at a population scale in the most privacy-sensitive category of personal data.

# 09
# Quantum Leap

# Introduction


**Computing capacity** is now a board-level competitive advantage. Insurers that can run more prediction, simulation, and personalisation at speed will outperform those that cannot. This matters because underwriting and claims are computation-heavy processes.

When your infrastructure is weak, the business consequences are direct: pricing errors, slower claims decisions, coverage disputes, and trust loss. Winning insurers treat infrastructure, data, models, operations, and security as one connected capability with clear ownership.

# Dominant subtrends

**Compute capacity** directly determines underwriting quality. Insurers with stronger server acceleration can iterate on models faster, improving fraud detection, claims triage, and pricing precision. When accelerator capacity becomes a constraint, business performance suffers through slower decision cycles, weaker service levels, and less accurate risk selection. This is not an IT problem. It is a competitive problem.

Simulation capability separates strong underwriters from weak ones. High-performance computing lets insurers run deeper scenario testing, stress-test assumptions, and improve portfolio steering. Simulation strength shows up as better pricing discipline and stronger defensibility when decisions are challenged. Insurers without this capacity are guessing more than they realise.

Decision speed now happens at the edge. Edge computing pushes fraud detection, claims decisions, and pricing closer to real-time events. This creates faster customer outcomes and more controlled data flows. It also raises operational expectations. Customers and regulators now expect continuous responsiveness, not batch processing from last week.

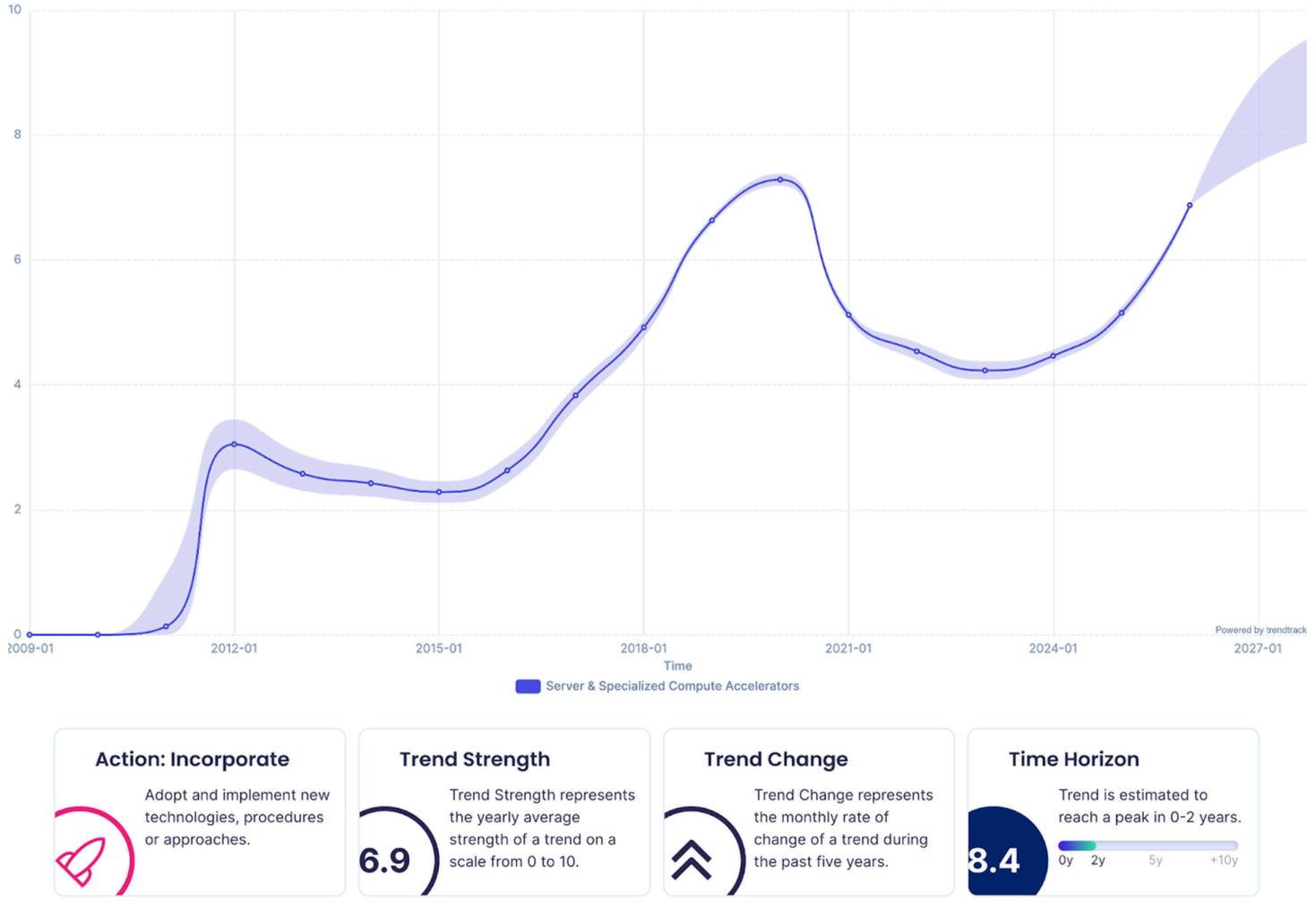



***Image 9:*** *Trendtracker data: Server & specialized compute accelerators in in insurance, structurally growing since 2016.*

# Dominant subtrends Continued

That always-on model expands the attack surface. Cyber defence becomes a core business requirement because threats are accelerating faster than internal skills can keep pace. Insurers need integrated risk management and automated threat assessment just to maintain baseline resilience. Manual security reviews no longer scale to the threat environment.

The cyber insurance market is tightening in response. Demand continues to grow, but standard policies are becoming fragile. Insurers are tightening underwriting, adding exclusions, and requiring clients to prove they are reducing risk.

The commercial result is clear: insurers that can measure cyber posture and support prevention can price with confidence. Insurers that cannot will attract the worst risks or offer coverage that matters less to clients.

**Samples of articles analyzed by Trendtracker**

- Cyber Insurance: Risks and Trends 2025, Munich Re, 03 Apr 2025
- The future of AI in the insurance industry, McKinsey & Company, 15 Jul 2025
- Cyber risk trends 2025, Allianz Commercial, 24 Sep 2025
- Report on the Cybersecurity Insurance Market, National Association of Insurance Commissioners (NAIC), 10 Nov 2025

# Potential risks and blindspots

**Blurred responsibility across AI systems creates legal and reputational risk.**

When AI-driven decisions cause harm, accountability fragments quickly across insurers, clients, vendors, and platforms. A denied claim or a supplier breach can turn into a legal dispute over who was responsible. For insurers, reputational damage often exceeds direct losses. For society, this ambiguity erodes trust in automated systems and slows the adoption of beneficial technology.

**Quantum computing threatens the encryption that underpins digital trust.**

Insurers rely on cryptography for identity verification, authentication, data confidentiality, and claims integrity. When those assumptions weaken, the consequences cascade: operational disruption, data exposure, contract disputes. This is not a niche technical problem.

Digital trust underpins finance, healthcare, and government operations. A breakdown becomes a question of stability for modern commerce.

**AI transparency pressure is a strategic fault line, not a compliance exercise.**

As automation deepens, regulators and customers demand justification for outcomes. Insurers must invest in decision traceability, data lineage, and governance that withstands scrutiny. Failure threatens licenses, distribution partnerships, and customer retention. For society, opaque decision-making in health, credit, and insurance amplifies perceived unfairness. This distrust undermines the risk pooling that makes insurance function.

# Recommended strategic initiatives

**Build an integrated computer and assurance capability now.**

Treat infrastructure capacity, data operations, model operations, security, and auditability as one managed system with clear ownership. Align accelerator and simulation capacity to the workflows that drive loss performance: underwriting automation, claims triage, and fraud detection. Insurers that delay will see the gap show up as pricing errors, slower claims, and regulatory exposure. The competitive advantage compounds because faster model iteration improves both risk selection and operational execution.

**Turn cyber insurance into risk reduction, not just risk transfer.**

Link coverage to measurable security improvements, including continuous monitoring, incident readiness, and supplier risk controls. This matters because cyber capability increasingly determines loss severity and volatility.

AI-enabled threats are raising the baseline for what clients need. Insurers that embed prevention into coverage will see better loss control, higher retention, and differentiation that competitors cannot easily copy through price alone.

**Harden trust infrastructure through post-quantum readiness and AI governance.**

Combine post-quantum security planning with AI systems that deliver defensible decisions, clear traceability, and strong audit trails. This aligns product credibility with operational resilience. Once regulators, courts, or major clients challenge your trust assumptions, retrofitting governance is slow and expensive. The insurers that act now gain credibility. Credibility remains one of the rarest assets in insurance.

> *“Insurance companies must evaluate this technology and its risks to continue providing effective cybersecurity protection coverage for themselves and their customers. ”*
>
> ***Alex Khan, www.insurancethoughtleadership.com***

# Growth initiative: Quantum-safe upgrade package

Offer clients a practical path to post-quantum security that combines assessment, planning, and insurance. Start with a quick review of where encryption is used across client systems and key suppliers. Provide a staged upgrade plan to make systems crypto-agile, enabling them to switch to new encryption standards without complete rebuilds. Tie insurance pricing to verified progress. Clients who complete each upgrade step earn better terms because their risk is measurably lower.

Distribute this through cloud and cybersecurity partners. Embed it in normal IT upgrades instead of selling it as a separate insurance product. This approach stands out because it turns quantum readiness into a business project with measurable returns, not a vague future threat. It also provides the insurer with better underwriting signals in a risk area where historical claims data is unavailable.

# Closing Thoughts

Insurance is undergoing a big change. The nine megashifts in this report are not separate trends. They are coming together to change the old insurance models and require new ones. The question for leaders is not whether to respond, but whether your response is real change or just surface-level.

Looking ahead, three strategic imperatives provide the foundation for navigating this transition effectively. Each imperative marks a clear step along the path forward.

**First, treat real-time operational intelligence as core infrastructure, not a competitive advantage.** The megashifts reveal a consistent pattern: risk is migrating from observable events to system behaviours, from annual declarations to continuous signals, from human decisions to algorithmic execution.

Quantum computing capacity, AI governance, industrial telemetry, urban sensor networks, autonomous fleet data, and genomic biomarkers are not separate initiatives. They are components of a single requirement: the ability to price and influence risk as it evolves, not as it appeared in historical data. Insurers that build this capability will price with confidence, defend decisions under scrutiny, and create products that reward prevention.

Insurers that do not will face adverse selection as the best risks migrate to evidence-based pricing, regulatory friction as governance expectations exceed operational reality, and margin erosion as competitors compress cycle times and improve loss ratios through verified signals.

The window to build is measured in quarters, not years. By 2027, real-time risk assessment will be table stakes in mobility, industrial operations, and urban infrastructure. By 2028, it will extend into healthcare and longevity products. Delaying infrastructure investment to preserve current operating costs is a choice of managed decline.

**Second, redesign the business model from risk transfer to risk partnership.** The competitive edge is shifting from scale in pooling to precision in prevention.

This is visible across domains. Quantum-safe upgrade packages tie coverage to security progress.

Risk dividend contracts adjust premiums based on verified factory controls. Programmable resilience policies trigger mitigation before losses occur. Autonomy assurance layers score controls in real time and dynamically adjust pricing. Member-governed bio-data trusts convert genetic information into consented value exchange.

The pattern is clear: insurance becomes a performance contract where pricing rewards measurable risk reduction, coverage adapts to verified improvements, and the insurer becomes the operating partner for staying insurable rather than the payer after failure. This is not product innovation. It is a business model transformation.

It simultaneously changes revenue composition, operational cost structure, talent requirements, technology architecture, and partnership strategy. The strategic choice is whether to lead this transition or be disrupted by it.

# Closing Thoughts Continued

Competitors are already operationalising prevention-linked products in cyber, industrial, and mobility segments. Platform players are embedding insurance into ecosystems with frictionless distribution and transparent pricing.

Insurers that continue optimising the transfer model while prevention becomes the market expectation will see premium pools shrink, relevance decline, and valuation multiples compress.

**Third, make trust infrastructure your primary moat.** Loyalty is now conditional. Reputation is trackable in real time. Customers demand verification, not promises. Regulators demand explainability, not assurances. This shifts competitive advantage from brand legacy and distribution scale to operational proof of fairness, accountability, and alignment.

The EU AI Act, digital sovereignty requirements, genetic non-discrimination frameworks, and platform partnership standards are converging into a single mandate: prove that decisions are defensible, data handling is lawful, and value delivery is measurable.

Insurers that treat this as a compliance cost will retrofit governance under regulatory pressure while repairing reputational damage.

Insurers that build verifiable trust as strategic infrastructure will unlock distribution partnerships, regulatory approval speed, customer retention, and pricing power that competitors cannot replicate through product features alone.

The investments required are governance frameworks that enforce accountability across AI development and deployment, data architectures that support consent management and traceability at scale, operational transparency that makes coverage logic and decision reasoning visible to customers, and ecosystem orchestration that reduces friction for partners while maintaining control quality.

These capabilities compound. Early movers gain approval for new use cases faster, attract sophisticated buyers who audit insurer capabilities before renewing, lock in multi-year platform partnerships, and build switching costs through demonstrated fairness rather than contractual lock-in.

The nine megashifts do not describe a possible future. They are documenting the present operating environment for insurers serving connected economies, ageing populations, fragmented markets, autonomous systems, and engineered biology.

The strategic implications are immediate. Insurers have 18-24 months to demonstrate operational progress in real-time risk assessment, prevention-linked products, and trust infrastructure before market expectations harden and competitive positions lock in.

Leadership teams that treat this transition as incremental will discover that structural change does not wait for consensus. The organisations that win will be those that recognise that insurance is being rebuilt from the operating system to the product layer, and act accordingly.

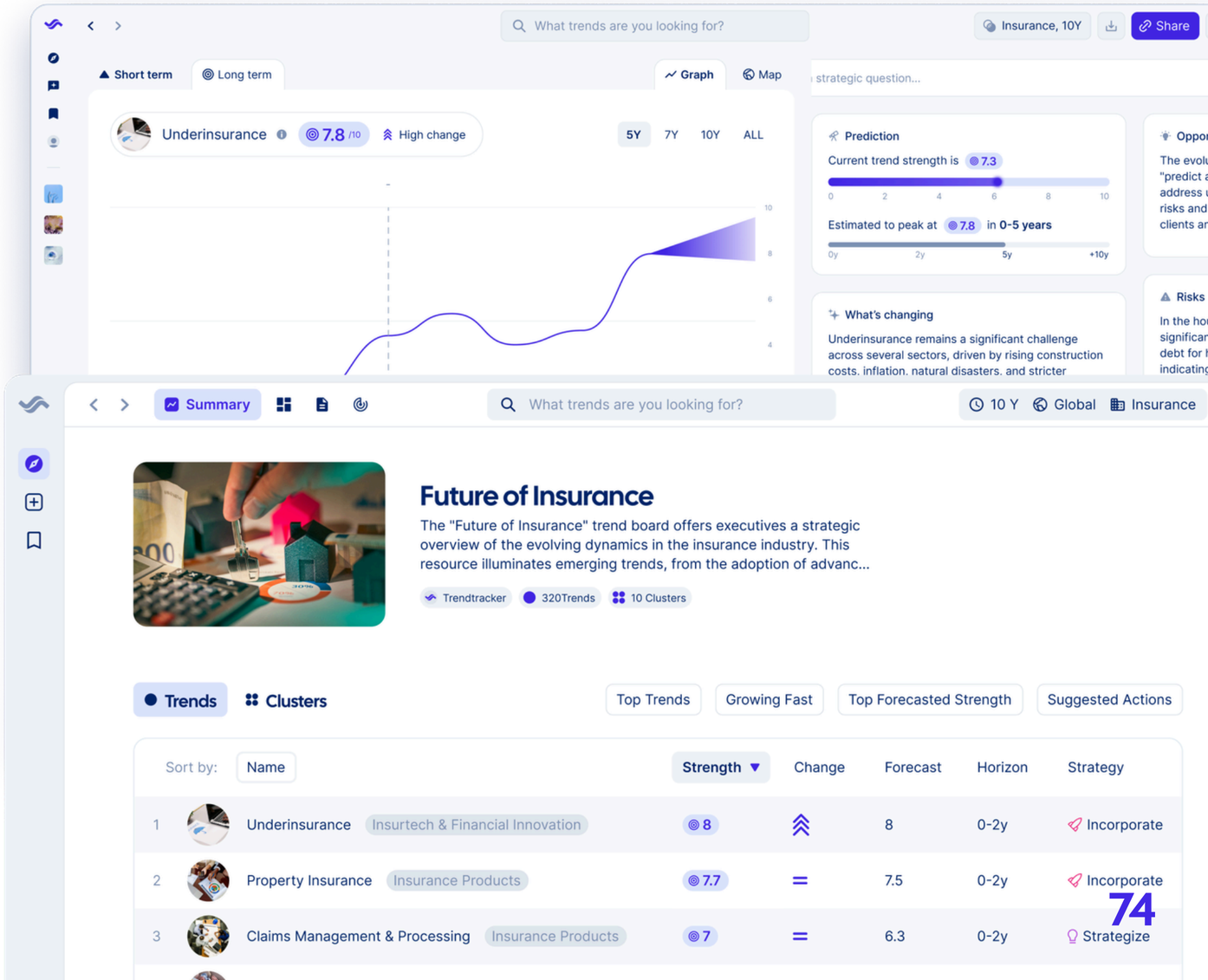
**The challenge now is action, not planning.**
**The strategy is already clear.**

# Explore how these Megashifts are impacting your business strategy

**Book a Deep Dive Session**

Trusted by strategy teams at leading global insurers.

THE GENEVA ASSOCIATION  ageas  ZÜRICH



# Colophon

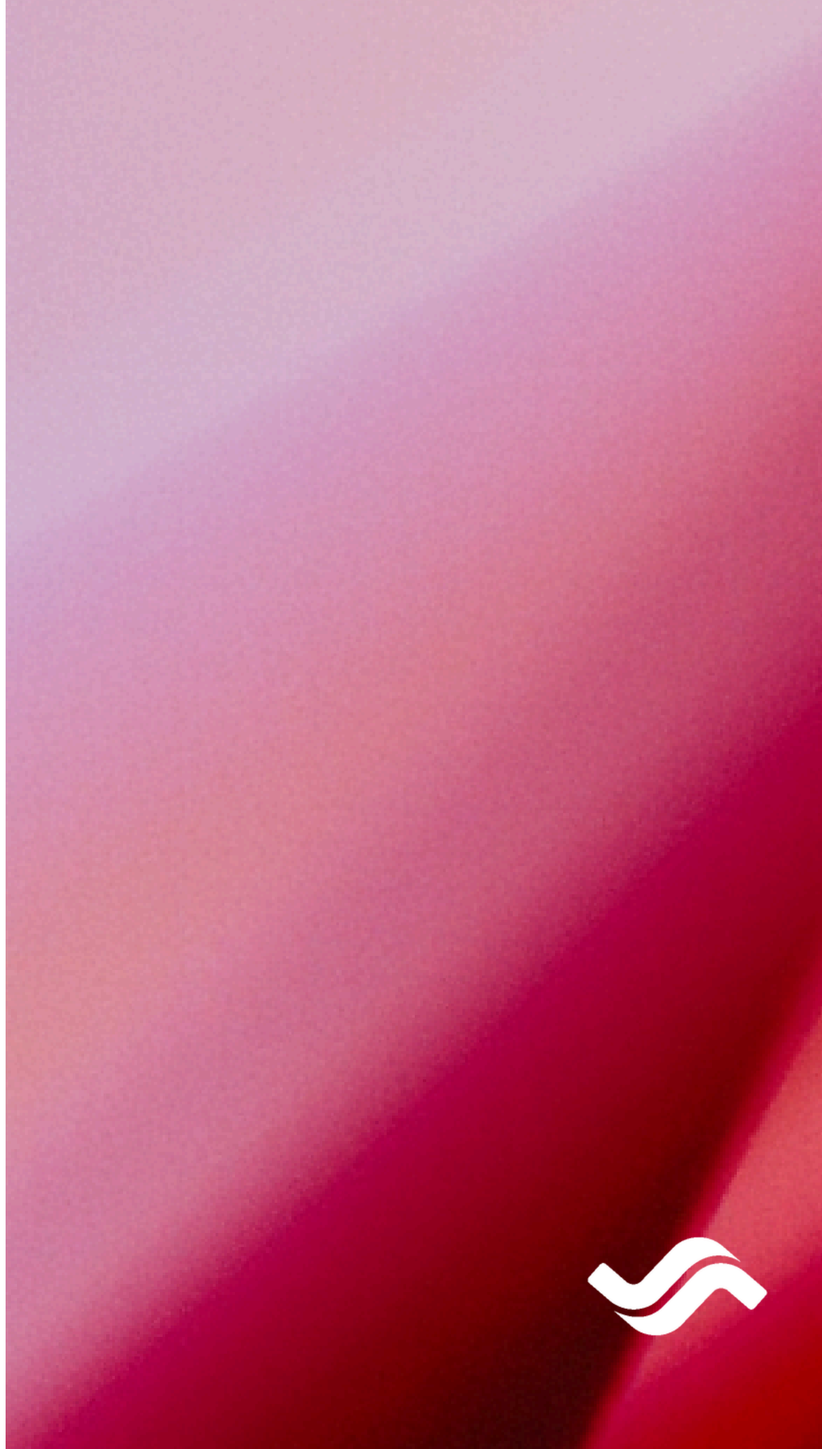
The report, *Megashifts Shaping the Future of Insurance*, is brought to you by Trendtracker.

**Editorial Team**
Christophe Jauquet
Paulina Puatany
Daniela Lomas

**Design and Layout**
Niels Vanderstraeten

**Feedback and Engagement**
Your perspectives are invaluable to us. We invite you to share your thoughts on this report by reaching out at info@trendtracker.ai.

Join the dialogue and help shape the future of strategic intelligence.



Trendtracker



**Europe**
Dok Noord 3A/202,
9000 Ghent, Belgium

**North America**
127 W 26th St 5th Floor
New York, United States

To find the latest Trendtracker content and register to receive e-alerts on this topic or others, please visit www.trendtracker.ai.