Brighton
You insure, We ensure

INSIGHTS

FEBRUARY 2026

ECONOMICS OF PREVENTION:
INSURANCE'S NEXT SHIFT

Insurance Under Synthetic Threat

Data Centres Are Reshaping Risks

Captives And Climate Resilience

Editor's Note

Dear Readers,

This month's issue captures a shift I see gaining real momentum across our industry. Insurance is no longer defined only by how well we respond to loss, but by how effectively we help prevent it.

Captives are evolving beyond financing vehicles into tools for climate resilience, supporting adaptation and bringing sustainability into strategic decision-making. At the same time, the rapid growth of data centres highlights how interconnected and complex modern risk has become. Traditional coverage alone cannot address exposures linked to power, cooling, and cyber vulnerability.

Insurers are also embedding monitoring tools and data-driven insights into policies, reducing claims and strengthening performance. Fewer disruptions for clients increasingly translate into steadier results for insurers. Even the rise of synthetic fraud is pushing underwriting and analytics to become more sophisticated.

Across these themes, a shared theme of resilience emerges. The industry is shifting its focus upstream, emphasising not only recovery but also minimising the chances and consequences of loss from the outset.

Enjoy the issue!

Annie Undikai

Annie Undikai, Managing Editor

Brighton
You insure, We ensure
INSIGHTS

FEBRUARY 2026

IN THIS ISSUE

OUR SOLUTIONS

- LICENSING & COMPLIANCE
- ACCOUNTING SERVICES
- WEBBIE, CLOUD-BASED ACCOUNTING SOFTWARE
- PAYROLL SERVICES
- GST/SST REPORTING
- E-INVOICING
- WORK PERMIT APPLICATION
- CORPORATE TAX SUBMISSION
- INTERNAL AUDIT
- SHARIAH ADVISORY
- COMPREHENSIVE CAPTIVE MANAGEMENT
- RUN-OFF MANAGEMENT
- SERVICED OFFICE FACILITIES

For more information, visit us at www.brighton.asia or scan the QR code

Economics of Prevention

INSURANCE'S NEXT SHIFT

For much of its modern history, insurance has operated on a disciplined sequence: evaluate risk, price it appropriately, collect premium, and indemnify when loss occurs. Profit depended largely on underwriting discipline and claims management efficiency. When a factory burned or a vehicle collided, the insurer would compensate for the financial loss. It is a system designed for compensation.

Today, that logic is being quietly but decisively reworked. Across property, health, motor, and commercial lines; the most economically compelling strategy is no longer simply paying claims efficiently. It is reducing the probability that claims occur at all.

In other words, the economic frontier has moved upstream. Industry analysts describe the change as driven by economic factors rather than superficial ones. It represents a fundamental transformation in incentives.

Customers want fewer interruptions and surprises, while insurers aim for consistent results and better margins. This mutual alignment is reshaping the industry's value perception, impacting capital allocation, and redefining its economic role.

Engagement Moves Upstream

Insurance has traditionally been characterised as a low-interaction product. Customers typically engage during three key moments: purchase, renewal, and claims. Of these, two moments are primarily administrative, while the third can often be quite stressful. The product remains in the background, quietly providing coverage until an issue arises. This limited interaction was deemed acceptable when the value of insurance was solely defined by financial protection.

For years, this low-frequency interaction was tolerated and engagement was not deemed crucial to the model. But that calculus is shifting. Carriers are now embedding services within policies to increase relevance and reduce risk exposure.

Property insurers are offering water leak sensors and monitoring tools. Health insurers are enhancing telehealth services and early screening programs. Motor carriers are implementing feedback systems for driver behaviour.

The insights gathered from these interactions improve the accuracy of underwriting and pricing, turning engagement initiatives into effective margin enhancement strategies.

Loss Avoidance and Financial Performance

Insurance profitability rests on a few core levers: premium adequacy, claims cost, operating expense, and capital requirements. Prevention influences each of these variable. For instance, connected home technology can detect abnormal moisture before structural damage occurs, reducing indemnity payments and adjustment expenses.

Health management programs can influence long-term claims development. In commercial auto, telematics that enhance driver behaviour can reduce accident frequency across fleets, stabilising combined ratios over time.

In competitive markets where premium growth is constrained, underwriting margin is often easier to improve through loss reduction than through price increases. Executives note that the financial impact extends beyond individual claims. Lower volatility can influence reinsurance purchasing strategies and overall balance sheet management.

Rethinking the Moment of Loss

The transition towards prevention also changes the perspective on how to handle losses when they arise. Traditional insurance often views financial reimbursement as the main goal. However, many policyholders prioritise swift assistance and effective coordination over monetary compensation.

For instance, when a pipe bursts, a homeowner seeks prompt repairs. Similarly, when a vehicle breaks down, the focus is on roadside assistance rather than dealing with paperwork.

Insurers are expanding their managed repair networks and service partnerships to address this expectation. These arrangements offer customers faster resolution while giving carriers greater cost predictability and control over outcomes. Early intervention often reduces secondary damage, limiting total loss costs even when claims occur.

Insurers are expanding their managed repair networks and service partnerships to address this expectation.

The result is a different kind of value proposition. Insurance extends beyond indemnification into operational support. And because early intervention often reduces total loss cost, even claims that occur can be economically moderated. Prevention and resolution, once seen as ancillary, are now central to portfolio management.

Data as Core Infrastructure

Prevention at scale depends on data. Traditional underwriting relied heavily on historical loss experience and broad demographic factors. With the advent of connected devices and digital platforms, we now have access to real-time behavioral and environmental data. For instance, water sensors flag irregular patterns, while telematics devices monitor driving habits.

Connected devices, digital platforms, and service interactions generate continuous insight into how risks evolve. A wearable device tracks changes in key health indicators, revealing emerging medical issues before they escalate into serious claims.

These data streams enable insurers to take proactive measures and categorise risks with greater precision. A decrease in claims results in enhanced portfolio stability, facilitating more accurate pricing and efficient capital distribution. Although uncertainty is inherent to insurance, timely information helps to refine the range of possible outcomes and improves decision-making throughout the entire value chain.

Systemic Risk and the Case for Resilience

The economic case for prevention becomes increasingly compelling in the face of systemic risks. Climate-related catastrophes, cyberattacks, and supply chain disruptions are increasing in both frequency and intensity. Reactive models exert pressure on reinsurance capacity and pricing stability.

Industry participants are prioritising resilience through enhanced building standards, improved cybersecurity, and advisory services to mitigate operational risks. These efforts not only support commercial goals but also contribute to economic stability. As collective exposure decreases and insurance pool volatility reduces, they promote affordability and long-term sustainability.

A Broader Redefinition of Value

Taken together, these developments signal a gradual redefinition of insurance's role. The industry is moving from episodic transactions to ongoing relationships, from reactive compensation to proactive mitigation, and from a financial settlement model to integrated service and risk management.

Claims payment is essential, yet competitive advantage now relies on minimising these payments. Product design, underwriting, technology, and distribution are evolving to focus on losses avoided and reduced volatility. While insurance historically restored financial balance after disruptions, its future may focus on preventing such disruptions altogether.

Insurance under Synthetic Threat

Identity fraud has long been a challenge for insurers, but its mechanics were predictable. A criminal would steal an individual's information, impersonate them, submit a claim, and vanish. While the impact was significant, it was also traceable, with a clear victim and a genuine identity at the heart of the situation. However, that clarity is fading.

Synthetic identity fraud presents a more intricate and less apparent danger. Rather than stealing a complete identity, fraudsters construct one by merging genuine data elements with fabricated personal details. For example, a valid national identification number may be linked to a fictitious name, a made-up address, and newly created digital profiles. The outcome is a policyholder who is nonexistent yet seems credible within underwriting and claims frameworks.

Fraudulent claims in historical data reduce underwriting accuracy, potentially resulting in higher premiums to offset losses.

Regulators are beginning to acknowledge the magnitude of the issue. Synthetic identity fraud has become a swiftly escalating financial crime, particularly impacting banking and digital finance sectors. This rapid growth is particularly pronounced in the Asia-Pacific (APAC) region, where synthetic identity document fraud skyrocketed by 233%, far exceeding the global rise of 195%. What initially posed a challenge for banks is now extending into insurance portfolios throughout the region.

How Identity Theft Impacts Claims

Stolen identities allow fraudulent claims under legitimate policies. Criminals can submit medical invoices, accident reports, or property claims without the real policyholder’s knowledge. In health insurance, this may involve billing for procedures never performed. In motor insurance, staged accidents can use stolen identity details to legitimise paperwork. Insurers process these claims because the policy is real.

The immediate impact of claims leakage is financial loss. Over time, repeated incidents lead to inflated loss ratios, skewing actuarial assumptions about frequency and severity. Fraudulent claims in historical data reduce underwriting accuracy, potentially resulting in higher premiums to offset losses.

Identity theft complicates claims operations as insurers must investigate fraudulent claims filed in customers' names, leading to increased administrative costs and delays for legitimate claims. This shift from assessment to forensic review can damage relationships. Additionally, reputational risk arises as policyholders expect their personal information to be protected, and even after resolving fraud, trust erosion can impact renewals and customer loyalty.

Synthetic Fraud: A More Engineered Threat

Synthetic fraud amplifies these vulnerabilities by fabricating identities entirely. Fraudsters may initiate small policies, consistently pay premiums, and establish a digital presence that seems credible. Over time, this profile develops within underwriting systems before a substantial claim is submitted.

Certain aspects of the documentation may appear authentic, complicating the detection process. For instance, a national identification number might belong to a student, an address might be real, and a phone number functional. The fraud lies in the deliberate combination of these fragments into a coherent but entirely fictional persona.

Traditional fraud detection typically centers on exaggerated damages, staged incidents, or organised schemes. However, synthetic fraud infiltrates the portfolio at an early stage, embedding fictitious identities into the underwriting process before any claims are made. When a claim does eventually arise, it is supported by what appears to be a credible policy history.

Artificial intelligence amplifies the risk. Fraudsters are now able to create realistic medical reports, invoices, and synthetic voice recordings. While quicker digital onboarding and automated claims processing ease the experience for legitimate customers, they also lower the barriers for advanced synthetic identities.

Economic and Portfolio Consequences

The consequences extend beyond isolated claims. When identity-based and synthetic fraud enter the loss dataset, frequency and severity patterns shift. Actuarial models based on compromised data may misstate risk across segments. Loss ratios rise without clear causes, creating upward pressure on premiums.

Reinsurers face similar issues. Accumulation modelling depends on authentic data. Artificially constructed identities undermine diversification assumptions, hiding concentrations across the portfolio. The regulatory implications are also substantial. Inadequate Know Your Customer (KYC) and anti-fraud measures may lead to increased scrutiny, fines, or even required remediation. Furthermore, public revelations regarding weak controls can tarnish reputation and diminish investor confidence.

Synthetic fraud also affects capital allocation. Insurers and lenders hold capital against expected and unexpected losses based on historical experience. If fraud inflates volatility or skews risk assumptions, capital buffers may be set incorrectly. Too little capital creates solvency risk. Too much capital constrains growth and reduces return on equity.

The financial impact extends beyond payouts. Detecting, investigating, and reversing fraudulent activity consumes operational resources. Claims handlers, fraud analysts, legal teams, and compliance officers devote time to cases that generate no genuine value. As a result, administrative costs increase, leading to diminished overall efficiency.

Rethinking Identity Verification in a Digital Market

Insurers must shift perspective. The question is no longer whether an identity appears valid at a single point. It is how identities behave across networks over time. Shared device fingerprints, repeated IP addresses, overlapping contact information, and unusual clustering of applications can reveal hidden patterns. Consequently, integrating network analytics into underwriting and claims processes is becoming increasingly vital.

Cross-industry collaboration is critical. Banks, telecoms, insurers, and regulators see different parts of the synthetic ecosystem. Data sharing, with privacy safeguards, can improve early detection and reduce systemic exposure. Successful implementation requires governance clarity and sustained leadership commitment.

Ultimately, identity theft and synthetic fraud do more than increase claims costs. They undermine the reliability of the data on which insurance depends. Insurers that integrate identity network analytics into core risk management processes protect profitability, regulatory compliance, and customer trust. Those that treat identity integrity as a peripheral issue may find losses quietly embedded in their portfolios long before they become apparent.

Data sharing, with privacy safeguards, can improve early detection and reduce systemic exposure.

Data Centres Are Reshaping Risks

Data centres are crucial facilities that power the digital world, housing servers, storage, networking gear, and backup systems operating 24/7. They support cloud platforms, databases, software for commerce, and hardware for AI, facilitating everything from emails to streaming videos. Despite their essential role, they remain largely invisible infrastructure underpinning online life.

The rapid expansion of this infrastructure is truly remarkable. In 2025, the global data centre market was estimated to be worth around $372 billion. Forecasts suggest that it could surpass $1 trillion by 2035, driven by the rising demand for digital services. Almost half of this growth is linked to cloud computing and enterprise workloads, while innovative applications such as AI and edge computing are propelling new facilities closer to end-users and devices.

Recent statistics indicate that approximately 68% of enterprises are currently dependent on centralised or cloud data centres for their core operations, and this trend is continuing to increase. In specific regions, the expansion of infrastructure is especially notable.

For example, in the United Kingdom, regulators have raised concerns that the proposed new data centre projects could require as much as 50 gigawatts of power—exceeding the peak national demand—prompting planners and grid operators to reevaluate the equilibrium between supply and demand.

In Malaysia, total data centre capacity is projected to double by 2030, with annual colocation revenue rising sharply as domestic and regional cloud adoption grows. This rapid expansion brings economic opportunity, but it also introduces exposures that insurers have not traditionally modelled at scale.

For insurers, the stakes are no longer about a single building in a flood zone. They are about clusters of digital dependency whose failures can ripple through entire industries.

In 2025, the global data centre market was estimated to be worth around $372 billion.

Case Study:
Grid Strain and Industry Shock

In summer 2023, the Pacific Northwest of the United State faced a heatwave, with temperatures exceeding historical averages. This increased strain on air conditioning systems led to heightened demand from residential and commercial sectors, pushing the electrical grid towards its critical load limits.

A group of data centres increased cooling and power usage to manage internal heat, resulting in higher regional energy consumption and local rolling outages. To avoid grid failure, utility providers restricted power to non-essential loads, while data centres used backup generators, leaving parts of the grid reliant on diesel and battery power for hours.

The event exposed the delicate interplay between climate stress, energy infrastructure, and digital operations. Although outages were brief, the financial and reputational consequences were significant. Some organisations implemented disaster recovery plans, transferring workloads to other regions, which incurred substantial expenses.

Insurers discovered that conventional models didn’t fully capture the interplay involved. Weather-related risks, energy infrastructure dependencies, and operational resilience all came together in loss scenarios that couldn't be classified as solely “property” events.

Case Study:
A Cooling Glitch, A Continent Offline

In 2021, a prominent cloud provider faced a significant cascading service outage that originated from a seemingly trivial problem: an anomaly in the cooling system at one of its main data centres. Consequently, temperatures within the server racks started to rise. To safeguard the hardware, automated safeguards ultimately initiated shutdowns of essential clusters.

The incident resulted in considerable downtime, affecting numerous businesses reliant on the provider's services. Applications experienced crashes, customer portals became inaccessible, and real-time services were disrupted.

E-commerce transactions experienced failures, development processes faced delays, and SaaS providers were inundated with complaints. Some businesses even suffered millions in losses over a single weekend due to a subsystem failure, which was unrelated to data breaches or natural disasters.

Claims involved issues like business interruption, contractual penalties, reputational damage, and regulatory scrutiny on data availability. Underwriters needed to assess whether the incident was a property failure, cyber outage, or a significant service disruption, marking it as an unconventional event and a wake-up call.

Claims involved issues like business interruption, contractual penalties, reputational damage, and regulatory scrutiny on data availability.

Systemic Risk in Plain Sight

These case histories highlight key lessons. Failures can stem from narrow technical issues like cooling subsystems and grid stress. The consequences can affect clients, sectors, and national economies. Additionally, losses can involve various coverage types, including property, business interruption, cyber-adjacent impacts, and contractual indemnities.

And this is happening in a context where demand keeps rising. AI is a major amplifier. Training large AI models is energy-intensive, needing high-density computing and advanced cooling. Facilities near capacity have less margin for error At the same time, businesses weave AI into core functions including forecasting, pricing, risk evaluation and customer engagement.

An interruption in an AI-driven workflow doesn't merely halt an application; it has the potential to disrupt strategic decision-making. For insurers, this means one thing: the risk landscape is no longer isolated.

What Insurers Should Do

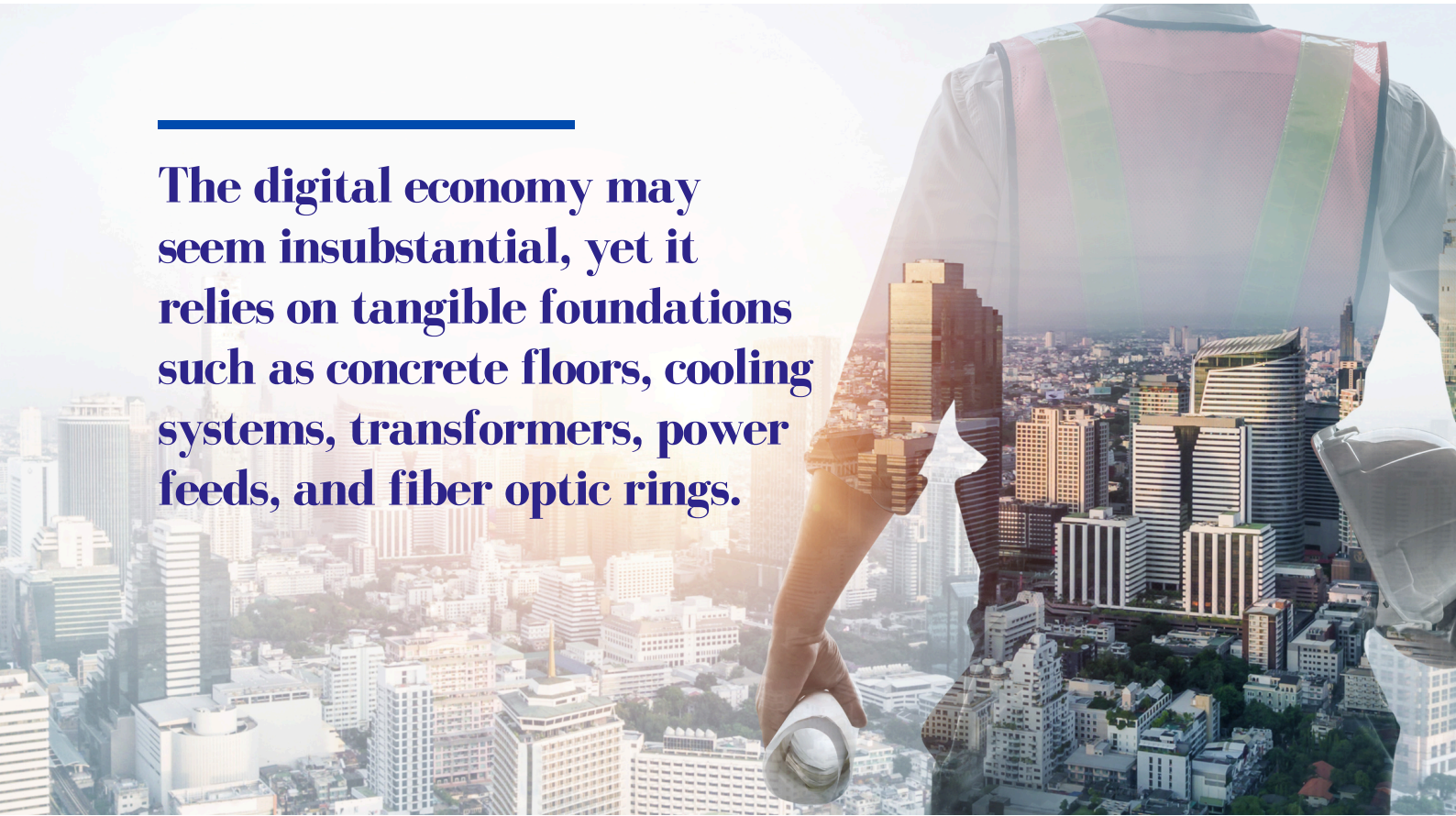
In rethinking accumulation models, merely mapping property locations isn't enough. Underwriters need to understand digital dependencies, identify insureds in the same cloud region, assess the value of multi-region failover strategies, and recognise silent correlations that may cause simultaneous losses across policies.

Clarifying policy wordings is crucial due to the growing overlap of property, cyber, and contingent exposures. Clearer language can reduce ambiguity, prevent disputes, and build trust while managing expectations before major outages.

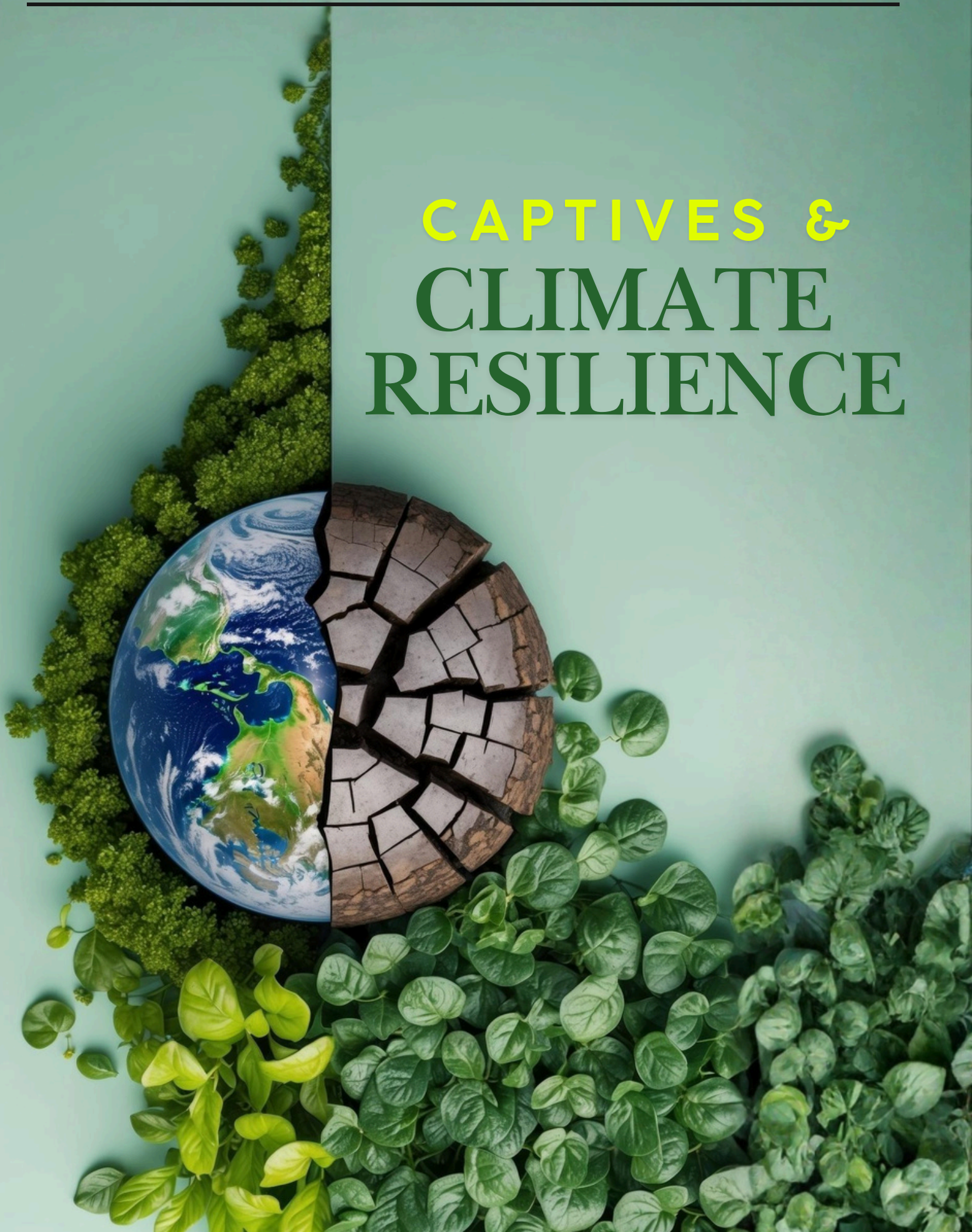
When it comes to enhancing risk engineering, assessing fire suppression systems is merely the beginning. Risk engineers should explore redundancy architectures, backup power designs, cooling resilience, and workload segmentation. The emphasis must be placed on operational factors, rather than solely on structural elements.

There are also significant opportunities ahead. Analysts project that data centre insurance could yield up to $11 billion in annual premiums within the next decade, particularly as specialty lines evolve to encompass blended risks. Solutions that integrate property, cyber, and contingent business interruption with parametric components linked to measurable thresholds are expected to see growing demand, as operators seek greater certainty.

The digital economy may seem insubstantial, yet it relies on tangible foundations such as concrete floors, cooling systems, transformers, power feeds, and fiber optic rings. As this infrastructure continues to grow, the complexity of risk also increases. Insurers that take the time to comprehend these changes today will not merely respond to future outages; they will play a crucial role in shaping how resilience is integrated into the backbone of tomorrow's economy.



CAPTIVES & CLIMATE RESILIENCE



Captives are no longer peripheral insurance vehicles. Over decades, their role has expanded to become a strategic pillar in enterprise risk management. Nowhere is this more evident than in the response to climate risk. Rising catastrophe losses, tightening commercial capacity, and mounting expectations for climate adaptation are pushing organisations to rethink how they finance and manage risk.

In this scenario, captives are becoming vital instruments for fostering long-term resilience. They are particularly well-suited to tackle both physical and transition risks. Captives provide adaptable, structured solutions that seamlessly blend risk management, finance, and sustainability.

Beyond Annual Insurance Cycles

Traditional insurance renewals follow a one-year cycle, which is not the case for climate risk. While effective for standard exposures, this approach leaves organisations vulnerable to climate risks that unfold over multi-year periods. Floods, wildfires, and extreme heat events often escalate gradually, while losses can spike unexpectedly.

A multi-year captive strategy smooths this volatility. Retained loss layers accumulate reserves during benign periods, which can then absorb losses from more severe events. Excess exposures can be transferred to reinsurers. The result is cost stability, better capital planning, and a predictable platform for managing climate risk.

Rising catastrophe losses, tightening commercial capacity, and mounting expectations for climate adaptation are pushing organisations to rethink how they finance and manage risk.

For example, a multinational manufacturer operating in flood-prone regions can retain moderate loss layers in a captive over five years, rather than relying solely on market renewals that spike premiums after each event. This approach stabilises earnings while providing a mechanism to fund resilience initiatives.

Five Ways Captives Drive Climate Resilience

As climate exposures grow more complex and interconnected, captives are taking on a broader mandate within corporate risk frameworks. Below are five practical ways they can support organisations in strengthening long-term resilience:

1. Covering Hard-to-Place Risks

Commercial insurers often find themselves challenged by high-risk areas and new exposures. Captive insurance can help address these gaps, covering physical hazards such as floods, wildfires, or hurricanes, as well as transition-related risks like business interruptions from decarbonisation initiatives.

Recognising these advantages, let's consider a specific example. A Japanese-based industrial conglomerate encountered limited flood coverage around its critical supplier networks. To address this issue, the company structured its captive to provide flood insurance for specific supply nodes that were previously uninsurable in the market. Over time, this internalised coverage allowed the organisation to negotiate improved external capacity beyond the captive's retention.

2. Financing Adaptation and Resilience

Captives are being increasingly utilised to fund capital projects aimed at minimising climate risks. A global logistics provider, facing rising flood threats at its terminals, chose to retain moderate loss layers within its captive. They directed their accumulated surplus towards flood mitigation initiatives, which included constructing elevated critical infrastructure and building flood walls.

By financing these projects through its captive, the company not only decreased its future risk but also enhanced its position in commercial insurance, leading to lower reinsurance costs over time.

Additionally, another multinational food company leveraged its captive surplus to enhance cold-chain systems in areas vulnerable to extreme heat. This initiative helped maintain the integrity of their inventory while significantly reducing the risk of spoilage.

3. Supporting Climate Disclosure and ESG Reporting Adaptation and Resilience

Credible climate reporting relies on consistent, decision-grade data. A well-structured captive serves as a central repository for loss experience, scenario analysis, and climate projections, integrating often fragmented information across business units.

An international mining organisation integrated captive claims data and climate stress-testing results into its yearly ESG disclosures. The captive compiled exposure changes over time, loss trends by hazard, and the financial implications of multi-year climate scenarios. This approach enhanced the credibility of external reporting while refining internal capital planning and risk prioritisation.

By aggregating climate risk intelligence across regions and operations, captives help ensure that sustainability commitments are anchored in measurable financial and operational outcomes.

4. Enabling Innovation and Green Technology Coverage

New technologies essential for decarbonisation often lack credible loss histories, causing insurers to be cautious. The absence of actuarial benchmarks leads to restrictive terms, higher deductibles, or declined participation, resulting in a protection gap where organisations are heavily investing in transition.

Captives can step into that gap as first-mover underwriters by taking on specific risks, enabling pilot projects to move forward while collecting operational data.

This data improves risk transparency and facilitates informed underwriting discussions with reinsurers and commercial markets over time.

This approach has been used to support early-stage battery energy storage systems, hydrogen facilities, carbon capture installations, and floating offshore wind projects. In each case, the captive with structured elements to manage volatility. As performance history stabilises, capacity can be gradually transferred to external markets.

The captive serves a purpose beyond merely offering coverage. It becomes an enabler of innovation, helping organisations advance decarbonisation initiatives without leaving material risks uninsured.

5. Integrating Climate Risk Across Functions

Climate risk spans multiple functions. It impacts various functions, including capital allocation, asset management, supply chains, regulatory compliance, investor relations, and long-term strategy.

Finance teams are concerned with earnings volatility, while operations focus on asset resilience. Sustainability teams monitor emissions targets and disclosures. However, these discussions often occur separately. A well-structured captive can bring those threads together.

One global consumer goods manufacturer provides a clear illustration. The company integrated its climate scenario modelling into its captive underwriting assumptions. It translated flood and drought projections into expected loss curves and capital-at-risk metrics, informing three-year capital planning. Operations prioritised site-level mitigation projects based on justified investment from reduced modelled losses, while sustainability used the data for climate disclosures and transition planning.

The captive board unified discussions on retention strategy, mitigation spending, and reinsurance purchases in one governance forum. This allowed for coordinated decisions based on shared metrics rather than separate discussions on climate, finance, and operations.

This data improves risk transparency and facilitates informed underwriting discussions with reinsurers and commercial markets over time.

In this way, the captive moves beyond risk transfer. It becomes a coordinating platform that links financial performance, operational resilience, and climate strategy within one disciplined structure.

Protecting Captive Capital with Structured Solutions

Retaining high levels of climate risk can strain a captive's reserves as extreme weather increases, potentially leading to capital loss and increased insurance costs. Structured risk transfer solutions help preserve capital while allowing for strategic retention benefits.

Parametric insurance is one key tool. Unlike conventional indemnity-based policies, parametric products activate payouts when predetermined environmental thresholds such as specific rainfall amounts, wind speeds, or temperatures are surpassed. This allows for quick liquidity post-event, bypassing lengthy claims processes and helping organisations maintain operations and fund mitigation efforts.

Parametric solutions can be incorporated with captives in various ways, including acting as an excess layer above the captive's retention, facilitating risk transfer for high self-retained exposures, or providing coverage for previously uninsured risks like drought affecting crop yields.

A Strategic Imperative

Captives are no longer optional for organisations with significant climate exposure. They stabilise costs, fund resilience investments, support climate reporting, enable innovation, and foster cross-functional coordination.

For insurance professionals and risk managers, understanding the mechanics of captives and their potential structure to tackle climate risk is crucial. In a time of increasing climate volatility, captives are emerging as key instruments through which sophisticated organisations can finance resilience and safeguard long-term value.