The Insurance Supply Chain Is Broken - And Everyone Inside It Knows It

What corporate insureds deserve to know about structural conflicts, misaligned incentives, and the independent alternative.

A White Paper

Published by LCM Solutions | lcmsolutions.ca | 2026

LCM Solutions
Loss Control Management

About LCM Solutions

LCM Solutions operates at the intersection of risk management, insurance, and technology. We work exclusively for corporate insureds - not brokers, not insurers, not adjusters. Our team brings decades of insider experience from within the global insurance market, including the Lloyd's of London syndicate network, TPA operations, and claims program design.

We do not sell insurance. We do not accept commissions from the market. Our independence is not a marketing claim - it is the structural foundation of everything we do.

Our Predict | Prevent | Protect™ framework helps corporate clients reduce total cost of risk through smarter risk mitigation, better program design, and independent oversight of the relationships that exist to serve their interests.

Introduction: The Conversation Nobody Inside the Industry Will Have With You

If you are a CFO, COO, or senior executive at a company with a significant insurance program, you have almost certainly felt it at some point - a quiet sense that the renewal process is more about the market's needs than yours. That the risk management advice you receive is filtered through interests that are not entirely aligned with your own. That the industry talks about your best interests while being structurally organised around something else entirely.

You are not wrong.

This white paper is written for corporate insureds who are ready to have the conversation that brokers, insurers, and adjusters are structurally unable to initiate. It is not an attack on individuals within the industry. The great majority of insurance professionals are competent, hardworking, and personally well-intentioned. The problem is not the people. The problem is the system they operate within - and the incentives that system creates.

Understanding those incentives is the first step toward protecting your organisation's interests more effectively.

> ***"Every link in the insurance supply chain gets paid when you renew. Nobody gets paid when you reduce your total cost of risk. That asymmetry has consequences."***

How the Insurance Supply Chain Actually Works

To understand why structural conflicts exist, it helps to map the supply chain clearly. When your company buys insurance, the following parties are involved - and each has a financial stake in the transaction:

The Retail Broker

Your broker is contractually your representative. They are also compensated - primarily through commissions paid by your insurer, calculated as a percentage of your premium. In most jurisdictions, this commission is not disclosed as a line item on your renewal documentation. The larger your premium, the more your broker earns. The result is a compensation structure that does not systematically reward your broker for reducing your insurance costs.

Contingent commissions - additional payments made by insurers to brokers who direct sufficient business volume their way - add a further layer of complexity. A broker receiving contingent commissions from a specific insurer has a financial incentive to place business with that insurer that exists independently of whether it represents the best outcome for you.

The Insurer

Insurers are commercial entities with shareholders and profit targets. Their primary obligation is to their capital providers, not to their policyholders. This is not a criticism - it is simply an accurate description of how they are structured. Insurers manage claims costs, reserving, and underwriting profitability. All of these objectives can, under certain circumstances, create tension with the interests of policyholders at claim time.

The Adjuster and TPA

When a claim occurs, your insurer appoints an adjuster or Third Party Administrator (TPA) to manage it. In most cases, the adjuster or TPA is appointed by - and financially dependent on - the insurer. Their commercial relationship is with the party who appoints them, not with you. Adjusters and TPAs who consistently settle claims in ways that frustrate their insurer clients tend not to receive further appointments. This is not misconduct. It is a rational response to commercial incentives.

The Risk Manager

At larger organisations, the internal risk manager is the professional most directly responsible for your insurance program. Risk managers are frequently skilled and knowledgeable. They are also, in most cases, deeply embedded in relationships with the broker and insurer market. Their professional networks, industry associations, continuing education, and career progression are all interwoven with the existing supply chain. This does not make them adversaries of their

employers - but it does create a structural orientation toward the market that can affect how independently they challenge it.

> ***"Your broker represents you. They're paid by your insurer. Your adjuster is appointed by your insurer. Your risk manager's career is built on relationships with the market. At every stage, the question worth asking is: whose interest is structurally primary?"***

The Renewal Trap: Why Nothing Changes

One of the most predictable features of the insurance market is how little changes from one renewal to the next. Despite rising premiums, changing risk profiles, and periodic claim disputes, most large corporate insurance programs renew with the same broker and largely the same insurer panel, year after year.

This is not an accident. It is the natural result of a system in which every participant benefits from continuity.

- **Continuity benefits the broker:** The broker earns commission on renewal without the cost and risk of a re-tender process.
- **Continuity benefits the insurer:** The insurer retains a known risk with an established premium history.
- **Continuity benefits the risk manager:** The risk manager avoids the significant workload of a full market exercise and the relationship risk of disrupting established connections.

The only party for whom continuity is not automatically beneficial is the insured. Yet the insured is the one party in the supply chain with the least visibility into the alternatives, the least time to dedicate to a thorough review, and often the least expertise to challenge the status quo credibly.

The annual insurance renewal - an exercise theoretically designed to secure the best terms for your organisation - frequently functions as a ritual that reinforces existing relationships rather than genuinely testing the market.

SIDEBAR: THE RISE OF CAPTIVE INSURANCE

A growing number of mid-to-large corporations have reached a conclusion about the traditional insurance market: it does not serve them well enough to justify its cost. Their response has been to form captive insurance companies - entities they own and control - to self-insure some or all of their risks.

Captive insurance has moved firmly into the mainstream of corporate risk management. It offers premium retention within the corporate group, direct access to reinsurance markets, and the elimination of several layers of the supply chain whose costs and conflicts are described throughout this paper.

For organisations currently operating captives - or seriously considering one - the insider knowledge LCM brings to program design, claims oversight, and risk mitigation technology is directly applicable. Captive owners have already made the conceptual shift. The question is how to maximise what they have built.

What Independent Advisory Actually Looks Like

The solution to structural conflict is not to find better individuals within the existing system. The solution is to introduce a genuinely independent perspective - one that is accountable only to the insured and compensated in a way that does not create the same misalignments.

Independent risk advisory, done properly, looks like this:

An honest assessment of total cost of risk

Most organisations focus on insurance premiums as the primary metric of their insurance program's performance. Total cost of risk is a broader and more useful measure: it includes premiums, retained losses, risk management costs, claims administration costs, and the cost of risk mitigation investments. A genuine independent advisor helps you understand all of these components and the relationships between them.

Independent claims oversight

One of the highest-value services an independent advisor can provide is oversight of the claims process on behalf of the insured. When a significant loss occurs, the interests of the adjuster, the TPA, and the insurer are not necessarily aligned with yours. Independent claims advocacy - from someone who understands how the market works from the inside - can meaningfully affect outcomes.

Risk mitigation technology that reduces frequency and severity

The most effective way to reduce your total cost of risk over time is to reduce the frequency and severity of loss events. A growing ecosystem of risk mitigation technology - covering property

monitoring, business interruption resilience, security, and loss prevention - offers measurable impact. An independent advisor with access to this ecosystem and no commercial incentive to favour any particular solution is best placed to recommend what is actually useful for your specific risk profile.

Program structure review

Deductible levels, SIR (Self-Insured Retention) structures, limits, and coverage terms all warrant independent review. Many corporate insurance programs carry structural inefficiencies that have accumulated over years of renewal without meaningful challenge. An independent advisor with market knowledge can identify where your program is not performing as well as it should.

> ***"The goal of independent advisory is not to replace your broker or your risk manager. It is to give you a perspective that the rest of your supply chain is structurally unable to provide - one that is accountable only to you."***

The LCM Difference: Insider Knowledge, Independent Position

LCM Solutions was founded on a straightforward premise: that the most valuable advisory a corporate insured can receive comes from people who understand the insurance industry from the inside, but who are not commercially dependent on it.

Our team has spent decades within the global insurance market - building claims programs and TPA operations with virtually every Lloyd's of London syndicate, designing MGA programs, and working within the mechanisms that corporate insureds rarely see. We understand how underwriting decisions are made, how claims are managed from the insurer's perspective, and where the structural pressures within the supply chain are greatest.

We bring that knowledge to the other side of the table.

The Predict | Prevent | Protect™ Framework

LCM's advisory approach is structured around three integrated disciplines:

- **Predict:** Using data, technology, and risk intelligence to identify exposures before they become losses.
- **Prevent:** Deploying risk mitigation technology and operational best practices to reduce the frequency and severity of loss events.

- **Protect:** Ensuring that when losses do occur, the claims process is managed independently, transparently, and in the insured's interests.

This framework is not theoretical. It reflects how we actually work with clients - and the sequence matters. An organisation that only focuses on the 'Protect' element (claims management) is managing losses after they happen. The greater leverage is upstream.

No conflicts. No commissions. No ambiguity.

LCM does not receive commissions from insurers or brokers. We do not place insurance. Our commercial arrangements with technology partners are transparent and disclosed. When we recommend a solution, it is because we believe it serves your interests - and the independence of that recommendation is something you can verify, not just take on trust.

Who This Is For

This paper - and LCM's advisory services more broadly - is most relevant to organisations in the following situations:

- **Commercial organisations looking to be engaged in proactively reducing risk and claim costs with or without existing corporate risk management:** CFOs and COOs who have growing concerns about the value delivered by their current insurance program, the transparency of the broker relationship, or the performance of the claims process.
- **Post-loss organisations:** Organisations that have experienced a significant claim event and feel the process did not serve their interests well.
- **Companies undergoing significant change:** Companies at a stage of growth or acquisition activity where their risk profile is changing materially and their existing program may not reflect current exposures.
- **Captive owners and operators:** Companies operating captive insurance entities who want to optimise program performance, improve claims outcomes, and integrate risk mitigation technology into their overall risk strategy.

Beyond the Policy: What Insurance Cannot Cover

There is a question that rarely gets asked during an insurance renewal - and almost never gets answered honestly by the people around the table. The question is this:

> ***"If we suffer a major loss event, and our insurer pays every dollar we are owed under our policy - will our business survive?"***

For a growing number of organisations that have lived through a significant disruption, the answer has been no. Not because their insurer failed to pay, but because insurance - even well-structured, fully-paid insurance - covers only a fraction of what a major incident actually costs. The remainder is absorbed by the business. And the remainder, as the evidence increasingly shows, can be fatal.

The Six Things Your Policy Cannot Cover

- **Reputational damage and brand erosion:** When customers, suppliers, and partners lose confidence in your organisation's ability to operate, that confidence does not return automatically when your systems come back online. The long-term revenue impact of reputational damage routinely dwarfs the direct financial loss - and it is uninsurable.
- **Competitive displacement:** While your operations are disrupted, your competitors are not. Market share captured by a rival during your recovery period is rarely recovered in full, and no policy clause compensates you for customers who found alternatives while you were offline.
- **Loss of momentum:** Organisations in growth phases lose something irreplaceable during a major disruption: time and forward momentum. Delayed launches, stalled negotiations, and management capacity consumed by incident response represent real, material costs that fall entirely outside any indemnity calculation.
- **Key staff departure:** Prolonged uncertainty following a major incident triggers talent attrition. Senior people with options leave first. The institutional knowledge, client relationships, and operational capability lost can take years to rebuild.
- **Regulatory and legal exposure:** Investigations, class action proceedings, and contractual breach claims can extend the organisation's exposure for years beyond the event. Coverage depends heavily on policy wording, exclusions, and the specific circumstances of the claim.
- **Higher future premiums - or coverage denial:** Organisations that have experienced a significant incident face materially worse insurance terms at the next renewal. This ongoing cost of having been attacked is itself uninsured.

The CGL Misconception: Why Many Businesses Are More Exposed Than They Realise

Before examining what even a well-structured, purpose-built cyber policy fails to cover, there is a more fundamental problem to address: many organisations believe they already have meaningful cyber coverage - when in most cases they do not.

Commercial General Liability (CGL) policies are the foundation of most corporate insurance programs. They are broad, familiar, and widely understood to cover a wide range of third-party claims. As cyber incidents became more common, many businesses drew comfort from the assumption that their CGL policy would respond to a cyber event - at least partially. That assumption has proven, in case after case, to be wrong.

> ***"A business that relies solely on its CGL policy to cover cyber risks is likely in for an unpleasant surprise." Carter Ledyard & Milburn LLP, Insurance Advisory Series***

The Insurance Services Office (ISO) - the body that develops the standard policy forms adopted by most insurers - introduced formal electronic data exclusions into CGL forms in 2014. These exclusions systematically remove coverage for losses arising from the loss of, damage to, corruption of, or inability to access electronic data. Most CGL policies issued since then contain these exclusions as standard. The result is that for the vast majority of organisations, their CGL policy provides little to no meaningful protection against a cyber incident - regardless of what was assumed at renewal time.

Four mechanisms compound this exposure. The electronic data exclusion eliminates most direct cyber claims. The 'tangible property' ambiguity means even where no explicit exclusion exists, coverage is uncertain and will be contested. War and nation-state exclusions eliminate coverage for a growing category of sophisticated attack. And partial cyber endorsements - added to CGL policies with sub-limits of $25,000 to $250,000 - create false confidence without meaningful protection.

TYPICALLY COVERED BY CGL	TYPICALLY NOT COVERED BY CGL
Slip-and-fall injury on premises	Data breach and ransomware costs
Third-party physical property damage	Electronic data loss or corruption
Advertising injury and defamation	Business interruption from cyber events
Product liability (physical harm)	Regulatory fines and notification costs
	Cyber extortion and ransom payments

Even Dedicated Cyber Policies Have Significant Gaps

Organisations that have purchased standalone cyber insurance are better protected than those relying on a CGL alone - but not fully protected. The cyber market has matured rapidly, and with that maturity has come increasingly sophisticated policy language that narrows coverage in ways not always apparent at purchase.

- **Sublimits that cap key coverages well below actual exposure:** A $5 million policy may contain a $250,000 sublimit for ransomware payments and separate sublimits for business interruption and regulatory fines. Against a real incident, these exhaust quickly, turning headline coverage into a partial safety net.
- **Security requirement conditions that create denial risk:** Cyber insurers now require specific controls - MFA, endpoint detection, tested backups - as a condition of coverage. Coalition's 2024 data found 82% of denied claims involved organisations without multi-factor authentication. Many policyholders are unaware their coverage is conditional on security practices not audited since the policy was placed.
- **Dependent business interruption gaps:** The 2024 attacks on Change Healthcare and CDK Global disrupted thousands of organisations that had no direct relationship with the attacked entity. Standard cyber BI coverage responds only when the insured's own systems are affected - leaving cascading third-party disruptions entirely uninsured.
- **The 42% coverage adequacy problem:** Research found that 42% of companies with cyber insurance reported their policy covered only a small portion of actual damages. Having a policy is not the same as having coverage that responds to your actual loss.

> ***"42% of companies with cyber insurance reported that their policy covered only a small portion of actual damages incurred. Having a policy is not the same as having coverage that responds to your actual loss."***

The Cyber Incident: A Case Study in Uninsured Loss

No category of loss event illustrates the gap between insurance coverage and actual organisational impact more clearly than a cyber incident. Ransomware attacks and data breaches have become the defining corporate risk of the past decade - and the claims experience of organisations that have lived through them reveals how much falls outside the policy.

53%	**24 days**	**~$5M**
of ransomware victims reported brand damage - uninsured	average operational downtime per ransomware incident	average total cost of a data breach in 2024 - an all-time high

A well-structured cyber insurance policy may cover a meaningful portion of direct financial costs: forensic and legal fees, regulatory notification costs, and some lost revenue during the indemnity period. **What it does not cover is the rest of the story** - the customers who moved on, the key hire who resigned, the enterprise contract that stalled in due diligence, or the next renewal premium that arrived with a material loading.

40%

of businesses do not reopen following a major disruption event

Source: FEMA - and a further 25% of those that do reopen fail within the following year

FEMA data indicates that 40% of businesses do not reopen at all following a major disruptive event. Of those that do reopen, a further 25% fail within the first year. These are not organisations whose insurers refused to pay. In many cases, the claims were paid. The organisations failed anyway - because the things that killed them were not on the proof of loss form.

> ***"Insurance is designed to keep you solvent. It is not designed to keep you competitive, protect your reputation, retain your people, or maintain your momentum. Those outcomes require a different kind of thinking - before the event, not after."***

The gap between what insurance covers and what a major incident actually costs cannot be closed by buying more insurance. The organisations that recover most effectively are those that invested, before the event, in understanding their true risk exposure, reducing the likelihood and severity of disruptions, and building operational resilience. This is the logic behind LCM's Predict | Prevent | Protect™ framework - and the reason independent advisory matters most upstream of the loss, not downstream of it.

Conclusion: The Question Worth Asking

The insurance industry provides a service that every organisation needs. The professionals within it are, by and large, capable and well-intentioned. The structural conflicts described in this paper are not the result of bad faith - they are the result of a system that was designed around the market's commercial needs and has not fundamentally changed in decades.

The question is not whether your broker, insurer, or adjuster is a good person. The question is whether the system they operate within is structurally capable of prioritising your interests above their own commercial relationships.

For most large corporate insurance programs, the honest answer to that question is: not consistently.

The organisations that have recognised this earliest are the ones that have formed captives, sought independent oversight, and begun asking harder questions at renewal time. They are not the majority. But they are growing in number - and the results, measured in total cost of risk over time, are increasingly difficult to ignore.

LCM Solutions exists for organisations that are ready to ask the harder questions. If this paper has articulated something you have felt but not had the language to express, we would welcome a conversation.

Contact LCM Solutions

Mark Weir **Founder, Managing Partner** Greater Toronto, ON M: 905.506.5564 E: mweir@lcmsolutions.ca	**John Pagoumian** **Head of US Operations** Miami, FL M: 732.688.9697 E: jpagoumian@lcmsolutions.ca
Scott McFie **Founder, Managing Partner** Greater Vancouver, BC M: 604.771.4485 **E: smcfie@lcmsolutions.ca**	**Warren Stevenson** **Partner, Strategic Advisory** Greater Vancouver, BC M: 604.230.0143 **E: wstevenson@lcmsolutions.ca**

www.lcmsolutions.ca