Howden Re

Cygenesis: origins of cyber market cycles

May 2026

Executive summary

Section

1 The origin story

Examines the current cyber market using Howden Re's Industry Exposure Database. It shows that expected growth drivers, including geographic expansion, increased limits and tower sizes, have not materialised to the extent expected. Capacity has expanded ahead of demand, leaving excess supply concentrated within a largely unchanged buyer base, sustaining lower pricing.

2 Cyber's convergent evolution

Explores how underwriting performance, large loss events and macroeconomic conditions shape pricing cycles. Drawing on property catastrophe and D&O analogues show that no single factor drives market turns. In cyber, a 1-in-200-year event is not required; a moderate property-catastrophe equivalent loss could dislocate the market given its concentration and limited diversification.

At the same time, a shift towards longer-tailed third-party exposures may delay loss visibility, allowing softening to persist even as performance weakens. These dynamics are further influenced by capital markets, where inflationary pressures, driven by geopolitical or other volatility, may support a higher pricing floor.

3 Classifying a cyber-genus

Considers how the evolving threat landscape may shape the next phase of the cycle. Losses are becoming more frequent and increasingly weighted toward third-party exposures, with developments in Artificial Intelligence (AI) accelerating these trends. As a result, deterioration may take longer to appear, reinforcing the importance of forward-looking indicators.

Introduction

The cyber market has definitively entered its fourth consecutive year of rate softening, raising questions as to how much further rates may decline before reaching a theoretical pricing floor.

The following analysis aims to untangle the intricate dynamics underpinning market cycles by examining the key factors driving market change.

The report begins with a deep dive of Howden Re's Industry Exposure Database (IED) to examine developments in the cyber (re)insurance market over the past three years. It unpicks nuances between different segments, evaluates growth dynamics and analyses the trajectory of geographic diversification and market concentration. It then turns to an uncertain future, proposing a set of lenses through which to consider the duration of the current cycle and catalysts for it to change.

‘Cygenesis: origins of cyber market cycles’ draws on analogues from other classes to explore how markets evolve over time.

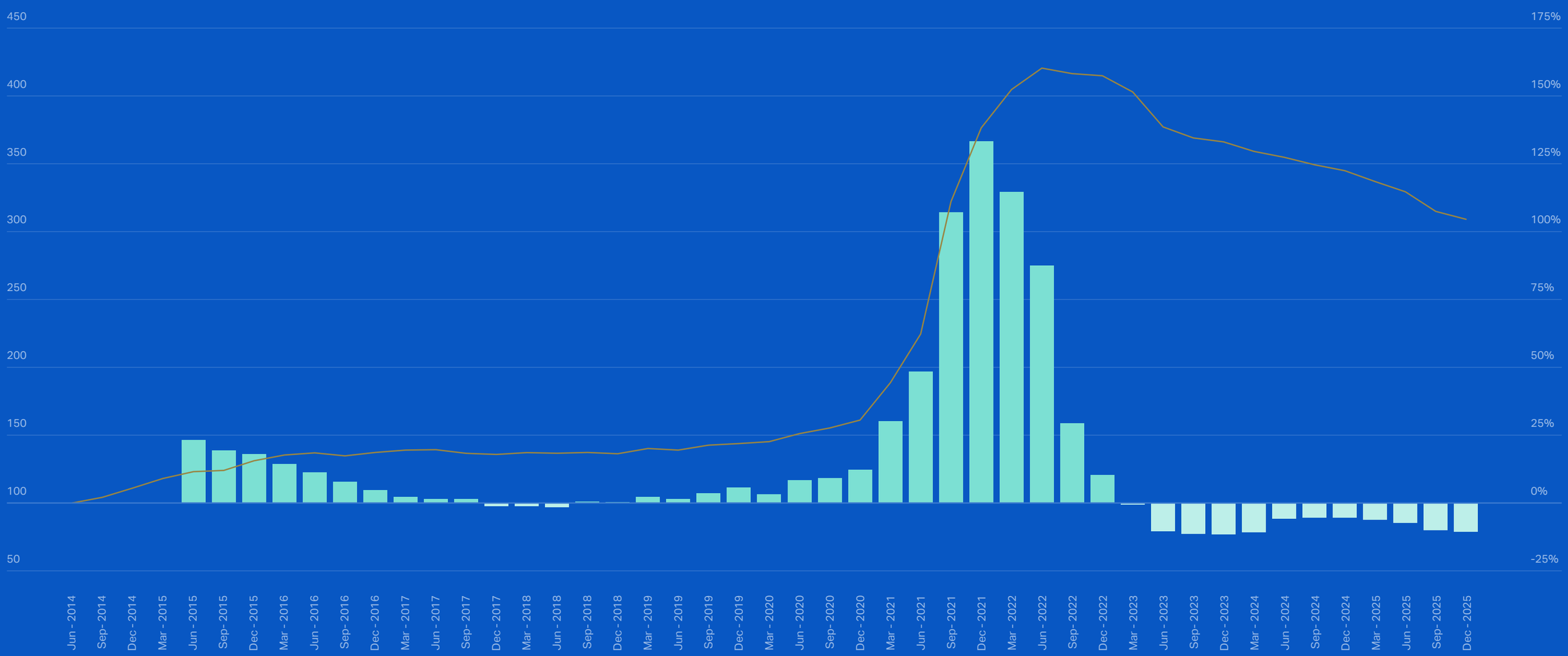
Across three distinct, but ultimately related sections, the report compares cyber with: property and property-catastrophe markets, to consider how market-dislocating events in property might manifest in cyber; the D&O market, to examine how margin compression and market concentration influence pricing dynamics; and broader macroeconomic and capital conditions, recognising that (re)insurance pricing does not operate in isolation from wider financial cycles.

Ultimately, shifts in the cyber market are driven by a combination of these forces, alongside developments in the underlying threat landscape. This report sets out the framework Howden Re uses to interpret market signals and to navigate the road ahead by viewing cyber through multiple perspectives.

Figure 1

Howden global cyber insurance pricing index: 2015–2025

Source: Howden



The origin story

Sustained softening in the cyber market has been discussed widely in recent years; it is important to contextualise this trend by examining the market's underlying components. Data from Howden Re's Industry Exposure Database, segmented across revenue bands, industry sectors and geography, provide a clearer view of the current operating environment. Understanding the nuance behind this softening is essential for gauging the next cycle shift.

1.1

Pricing dynamics across segments

Figure 2 illustrates two key dynamics underpinning current pricing trends.

First, rates have deteriorated most sharply within larger revenue segments, reflecting intense competition and saturated capacity in the high excess space, while small and medium-sized enterprises (SMEs) have proven more resilient to downwards rate pressure.

Second, there is a consistent divergence between new and renewal business. Renewal pricing has held up more effectively across all segments, indicating a degree of portfolio stickiness for incumbents. Competition for new business, however, remains strong.

Market participants reinforced this dynamic by readying additional capacity between 2023 and 2024, in anticipation of new growth opportunities over a three-to-five year horizon. As these expectations have not yet materialised, excess capacity has adversely impacted pricing.

- Large new
- Large renewal
- Medium new
- Medium renewal
- Small new
- Small renewal
- Micro new
- Micro renewal

Note: new indicates new to the carrier, not necessarily new to market

Figure 2

Pricing delineated by cyber market segment and new and expiring business

Source: Howden Re IED and Howden Re Analysis

1.2

(R)evolutionary expectations

In early 2025, Howden Re published 'Into the Cyberverse', which set out expectations for continued growth in the cyber market. Commentator forecasts for year-end 2025 estimated a market size between US$ 17.5 billion and US$ 23.5 billion, with further expansion anticipated into the latter part of the decade.

Three key drivers were expected to underpin this growth: increased limits purchased by large corporates, international expansion into underpenetrated markets and product simplification to unlock SME demand.

Chief amongst these assumptions was a pre-existing expectation that cyber towers within the large corporate segment would recover to pre-hard market levels following the 2021-2022 contraction and then expand further, as organisations sought greater protection against increasingly complex loss scenarios. In response, the market developed high-excess facilities to support this demand.

In practice, tower sizes contracted in 2021 and 2022 before stabilising between 2022 and 2024, indicating limited growth in purchased limits. While some growth has been observed, particularly amongst UK buyers, this has not been widespread. This could partly reflect the price elasticity of demand, with rates still above 2020 levels despite softening from their recent peak. Nevertheless, early signs of increases emerged in 2025, as shown in **Figure 3**, although the trend is nascent.

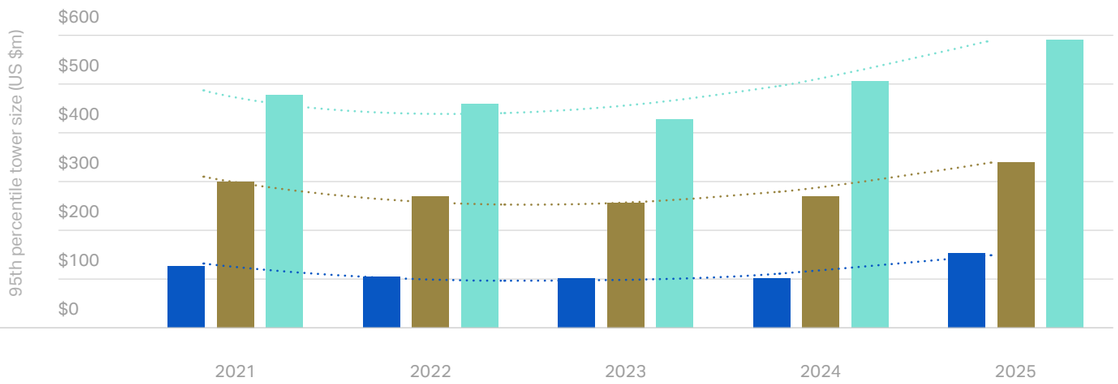
In this context, maintaining meaningful levels of cyber coverage remains important; however, the need to structure programmes to fully cover ground-up loss scenarios appears to have diminished. With limited growth in tower sizes, this source of demand has not absorbed the increase in available capacity.

- $1-10bn
- $10-50bn
- $50+bn

Figure 3

Cyber tower sizes over the past five years by revenue band

Source: Howden Re IED and Howden Re Analysis



1.3

A hard landing

65.4%

US share of the cyber market is now expected to remain significantly higher than previously projected for 2030

> In practice, international expansion has progressed more slowly than anticipated.

With increased limits failing to meaningfully stimulate demand, attention shifts to geographic growth. Low cyber insurance penetration across EMEA and APAC, as highlighted in Howden's 'Rebooting Growth' (2025), presented a clear opportunity for insurers to diversify portfolios and access new sources of business.

In 2024, Howden Re developed a forward-looking view of market composition based on insurer business plans and growth projections. At the time, insurers widely viewed international expansion as a strategic priority, expecting the US share of the cyber market to decline from approximately 70% in 2024 to 53.7% by 2030, driven by growth in international markets.

In practice, international expansion has progressed more slowly than the market anticipated. Cyber exposure awareness remains uneven across jurisdictions, and in many markets the perceived need for standalone cyber cover has not reached the same level as in the United States.

This disparity is reinforced by differences in both threat activity and regulatory environments. A significant proportion of cybercriminal activity continues to target US organisations. As such, demand for cyber insurance outside the US has developed more gradually.

Based on current trends, the US share of the cyber market is now expected to remain significantly higher than previously projected, at approximately 65.4% in 2030. This represents an 11.7 percentage point gap relative to earlier expectations, as observed in **Figure 4**, and demonstrates that the anticipated market diversification has yet to materialise.

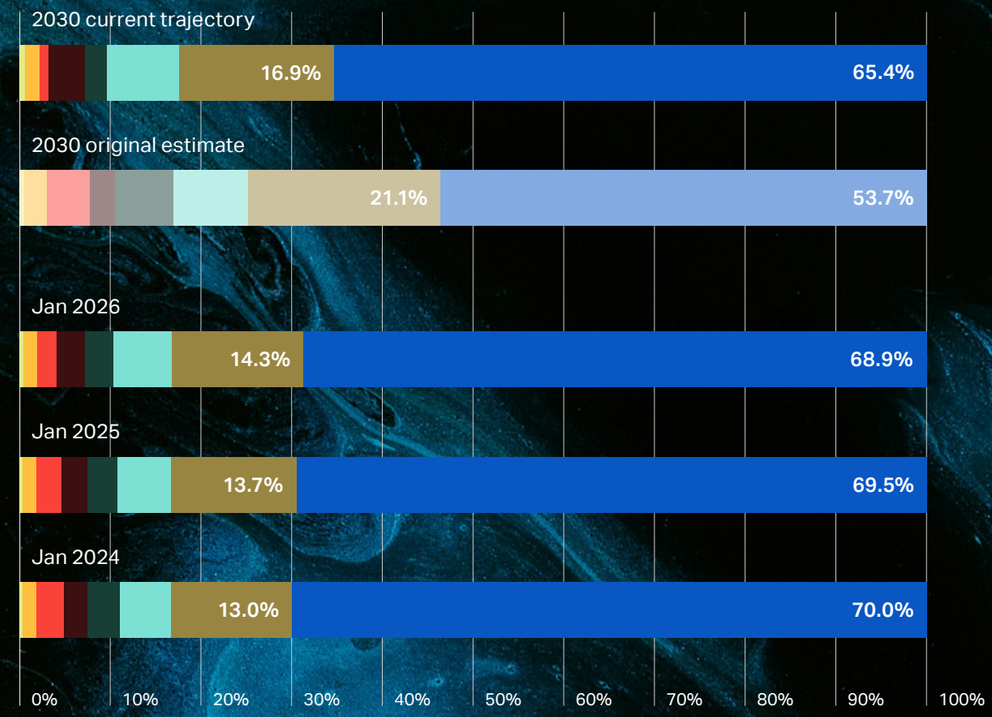
53.7%

Howden Re's original 2030 estimate of US cyber market share

Figure 4

Geographic composition of the cyber market (% of GWP)

Source: Howden Re IED and Howden Re Analysis



1.4

Meet your makers

Despite a notable increase in capacity over recent years, including new market entrants seeking to scale cyber portfolios, market share distribution has remained relatively stable.

As illustrated by **Figure 5**, the largest cyber writers comprise a significant proportion of the market. The top five insurance carriers (excluding MGAs) have maintained a consistent share, decreasing only marginally from approximately 33.4% to 32.1% over the past five years, while the top ten have continued to account for around 40% of the total market. This stability suggests that new entrants have not materially displaced incumbent carriers.

○ Equates to 20%

Figure 5

Market share concentration across cyber insurers

Source: Howden Re IED and Howden Re Analysis

2024

Top 5 (Entire market)	**33.4%**
5-10 largest (Entire market)	**18.5%**
Rest (Entire market)	**48.1%**

2025

Top 5 (Entire market)	**31.8%**
5-10 largest (Entire market)	**15.2%**
Rest (Entire market)	**53%**

2026

Top 5 (Entire market)	**32.2%**
5-10 largest (Entire market)	**15.1%**
Rest (Entire market)	**52.7%**

2026 SME

Top 5 (Other segments)	**32.1%**
5-10 largest (Other segments)	**8.7%**
Rest (Other segments)	**59.2%**

2026 large corporate

Top 5 (Other segments)	**37.3%**
5-10 largest (Other segments)	**15.1%**
Rest (Other segments)	**47.6%**

2026 large corporate (primary)

Top 5 (Other segments)	**53.8%**
5-10 largest (Other segments)	**14.5%**
Rest (Other segments)	**31.7%**

“

Capacity has increased, without the structural growth to absorb it.

-1.3pp

market share decrease over the past five years for the top five carriers (excluding MGAs)

New entrants, often targeting ambitious growth, have largely competed for new business rather than displacing established portfolios. This dynamic helps explain the observed divergence between renewal and new business pricing, with more competitive pricing typically seen on new placements **(Figure 2)**.

At the same time, market share distribution varies across segments. In large corporate primary business, the largest carriers retain a stronger position; supported by underwriting expertise and established client relationships. As a result, new capacity has concentrated in more price-sensitive segments, including high-excess layers and parts of the SME market. In these areas, placements are more transactional and differentiation is less pronounced, leading to greater competition and downwards pricing pressure.

These dynamics reinforce the broader theme observed across limits and geography. Additional capacity has not been absorbed through a structural expansion in demand, but has instead intensified competition within existing segments, contributing to continued softening in pricing.

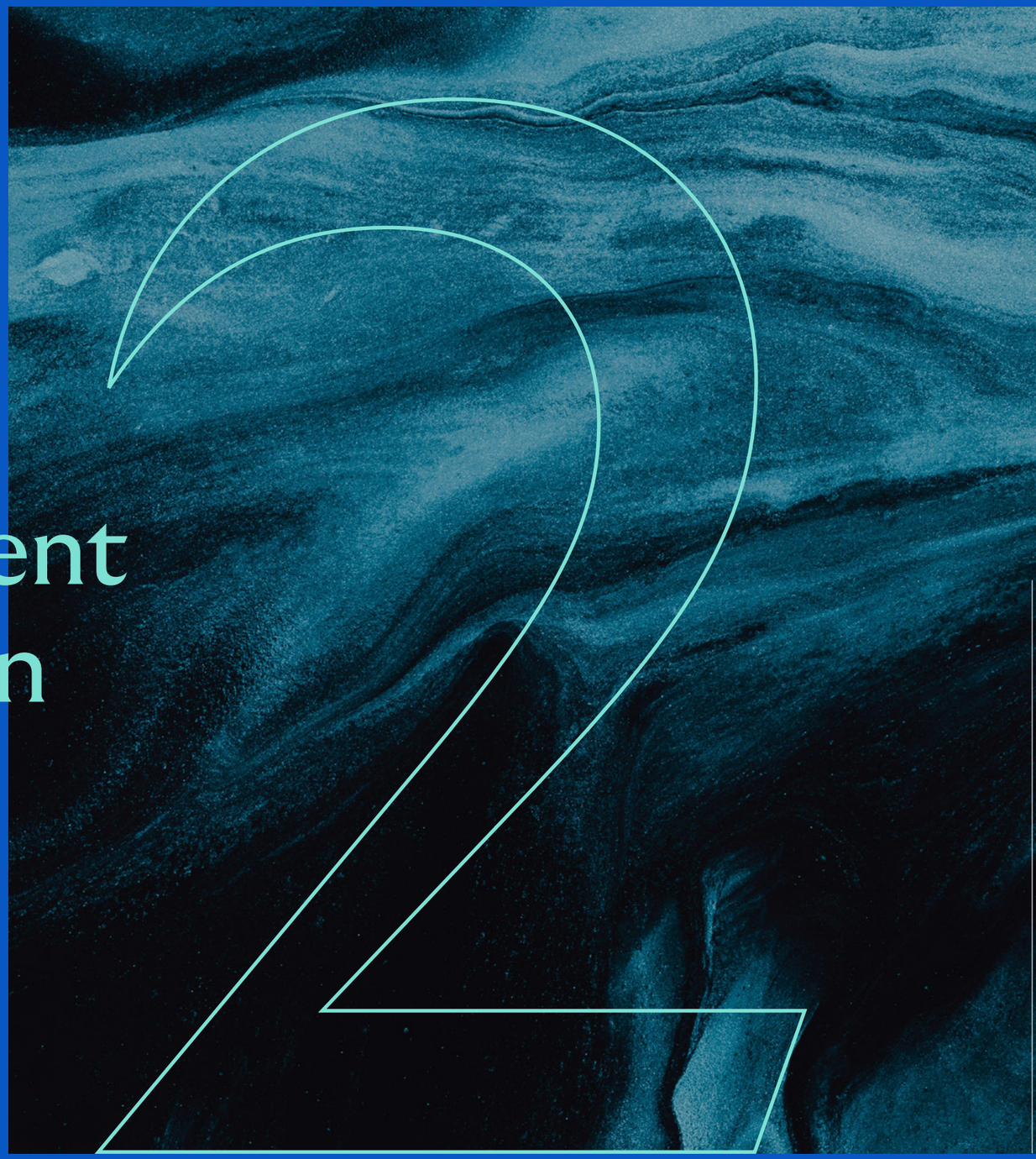
Constraints in context

When taken together, the expected drivers of cyber market growth have not developed as anticipated. Limit expansion has remained constrained, international diversification has progressed slowly and demand has remained relatively concentrated.

Capacity has increased, without the structural growth to absorb it. This has intensified competition within existing segments, most notably in new business, where pricing has come under the greatest pressure.

While understanding these dynamics is essential to assessing the trajectory of the cyber market, viewing the class in isolation risks missing broader signals of change. The following section draws on analogues from other classes to examine the conditions required to shift the cycle.

Cyber's convergent evolution



Cyber is exposed to a combination of systemic catastrophe risk, attritional loss experience and, as with all lines of business, broader macroeconomic conditions. This section examines how these interrelated forces influence pricing dynamics and, critically, how they have driven market turning points in more established classes.

Drawing on property, D&O and capital markets, the analysis seeks to identify the conditions that drive shifts in market cycles. These insights are then considered alongside the current cyber threat landscape, providing a framework to assess when the next phase of the cycle may emerge.

2.1

Property in the petri, a closer scan of cats

+78%
increase in direct pricing between 2001 and 2006

Property provides a useful point of comparison given its well-documented loss history and clearly observable market cycles. As a mature, catastrophe-exposed class, it offers a clear framework for assessing how large-scale events influence pricing.

Figure 6 provides a long-term view of the global property insurance and catastrophe reinsurance market. By overlaying direct and reinsurance rate-on-line indices with monthly natural catastrophe losses, it highlights how loss events have influenced pricing dynamics over time.

In the early 2000s, pricing was highly responsive to loss activity. Risk-adjusted property-catastrophe reinsurance rates-on-line increased by approximately +62% and direct commercial lines pricing by +78% between 2001 and 2006, following a series of market-defining events, including 9/11, the late-1990s liability crisis and major hurricane losses such as Katrina, Rita and Wilma. At that point in the cycle, the market operated with a significantly lower capital base (see **Figure 13** in Section 2.3), with large loss events therefore more likely to drive pricing dislocation.

Despite continued, elevated catastrophe activity (including the Tōhoku earthquake and tsunami, and major US hurricanes such as Sandy, Harvey, Irma and Maria), pricing across both reinsurance and direct markets softened considerably between 2006 and 2017, declining by approximately -38% and -45% respectively. This period marked a pronounced soft market trough, reflecting strong capital inflows, increased market scale and competitive supply conditions, which allowed losses to be absorbed without sustained dislocation.

While major catastrophe events in recent years such as Harvey, Irma, Maria, Ian and more recent wildfire losses, have been highly disruptive; the scale, diversification and capitalisation of the property market have enabled it to absorb these shocks without the same degree of dislocation observed in earlier periods. The subsequent hardening observed in the 2020s was largely driven by macroeconomic factors, discussed further in Section 2.3.

Figure 6
Property insurance and reinsurance pricing overlaid with monthly natural catastrophe losses
Source: Howden and NOVA

> The cyber market does not require a 1-in-200 year loss to trigger material hardening.

This evolution provides a useful reference point for cyber. In its current phase, cyber is more likely to behave in a manner consistent with the earlier stages of the property-catastrophe cycle, where large loss events had a more direct and immediate impact on pricing.

Figure 7 maps historical US property-catastrophe loss years onto the Howden Re CyberCube industry loss curve (ILC), highlighting the scale of event required to drive a comparable market response in cyber.

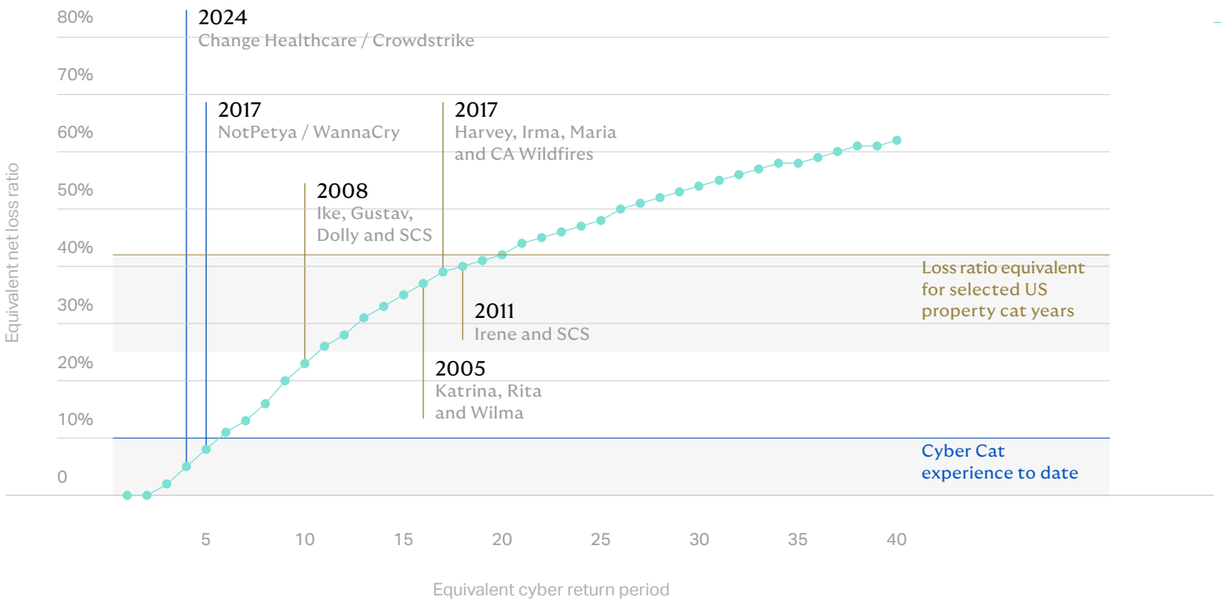
When translated into a cyber market loss ratio, major property-catastrophe loss years, such as 2005 or 2017, would fall within a 10 to 18 year return period on Howden Re's CyberCube industry loss curve, with a concentration around cat loss ratios of approximately 40%. Current cyber cat loss experience remains materially below this threshold. To reach a comparable level of market impact, cyber loss years would need to increase significantly in magnitude.

Importantly, the cyber market does not require a 1-in-200 year loss to trigger material hardening; losses comparable to a moderate property-catastrophe year, such as 2008, would likely prompt a significant response in cyber. Should a cyber event approach this scale, more meaningful market dislocation would be expected. Even at this level, aggregate stop loss protections may not attach, which could drive changes in reinsurance purchasing behaviour - for example, to event-based structures.

Figure 7

Cyber and Property-Cat loss years against Howden CyberCube ILC

Source: Howden Re analysis of events / Howden Re CyberCube ILC (Industry Loss Curve) – CyberCube v6 Howden View of Risk, 10k annual reports for top 20 US property writers, Time to Act – Howden Group)



40%
of cyber insurance premium is concentrated within the top ten carriers

87%
of the cyber reinsurance market is held by the top-ten

Similarly, market structure reinforces this sensitivity. As outlined in Section 1 and illustrated in **Figure 8**, the cyber insurance market remains relatively concentrated. The top ten carriers account for approximately 40% of total premium. Reinsurance is even more concentrated, with the top ten comprising around 87% of the market. This increases the potential impact of changes to underwriting strategies. A strategic retrenchment or withdrawal by one or more leading (re)insurers could have a disproportionate effect on available capacity and pricing dynamics.

Howden Re's inaugural 2024 cyber reinsurance report, 'Reframing cyber risk', highlighted that while some insurers hold large gross cyber portfolios, their net exposure varies materially once reinsurance is taken into account. Measuring a 1-in-200 year cat loss as a percentage of shareholder equity provides a clearer view of the level of risk each insurer is willing to retain.

Applying this framework to the top ten cyber carriers highlights a clear range of risk appetites, from confident (large cyber allocations) to considered and curious (more limited exposure). The underlying definitions and methodology are set out in 'Reframing cyber risk'.

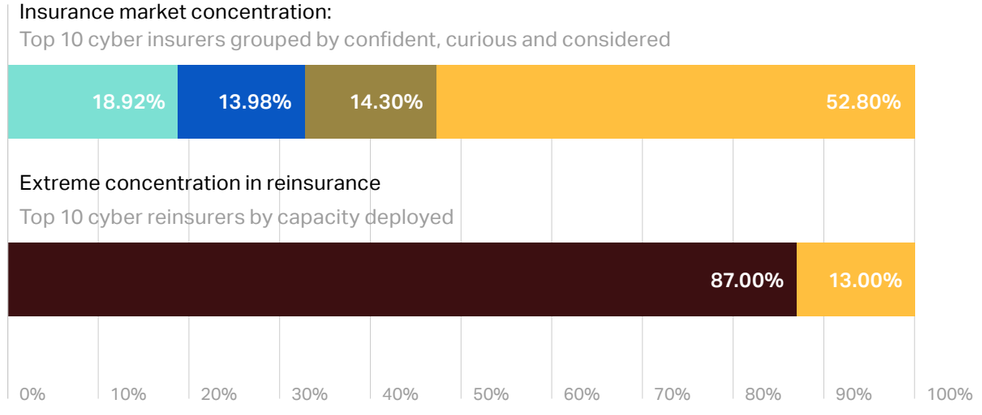
Even carriers in the confident category approach the class with a degree of caution. A shift in risk appetite following a large loss event could materially alter the supply-demand mechanics in the cyber market.

In this context, cyber remains less diversified and, therefore, less resilient to shocks than more mature classes, reinforcing its sensitivity to both loss events and changes in capacity. Yet catastrophe losses are only one driver of market cycle change. Equally important is consistent underperformance over time, which has been a key driver of cycle turning points in classes such as D&O.

Figure 8

Insurance and reinsurance market concentration (% of GWP)

Source: Howden Re



2.2

Organic attrition

>100%

pricing continued to soften even as combined ratios exceeded 100% for several consecutive years on an ultimate basis

A prevailing hypothesis around the next phase of the cyber cycle is that margin deterioration will ultimately force the market's hand, leading to rate stabilisation or a return to hardening. While this is directionally accurate - as there is a limit to the duration in which a portfolio can remain unprofitable before remediation is required - market responses to sustained unprofitability are not always immediate.

For the purposes of this analysis, D&O is used as a point of comparison given the similarities it shares with cyber. However, this dynamic is not unique to D&O and has been observed across a range of classes at different points in the cycle.

Figure 9 illustrates the relationship between underwriting performance and pricing in the D&O market, showing Howden's pricing index alongside accident year combined ratios over the same period. Despite a prolonged period of unprofitability, with combined ratios exceeding 100% (and worsening) for several consecutive years on an ultimate basis, pricing continued to soften.

> "Underlying underperformance is not always immediately visible.

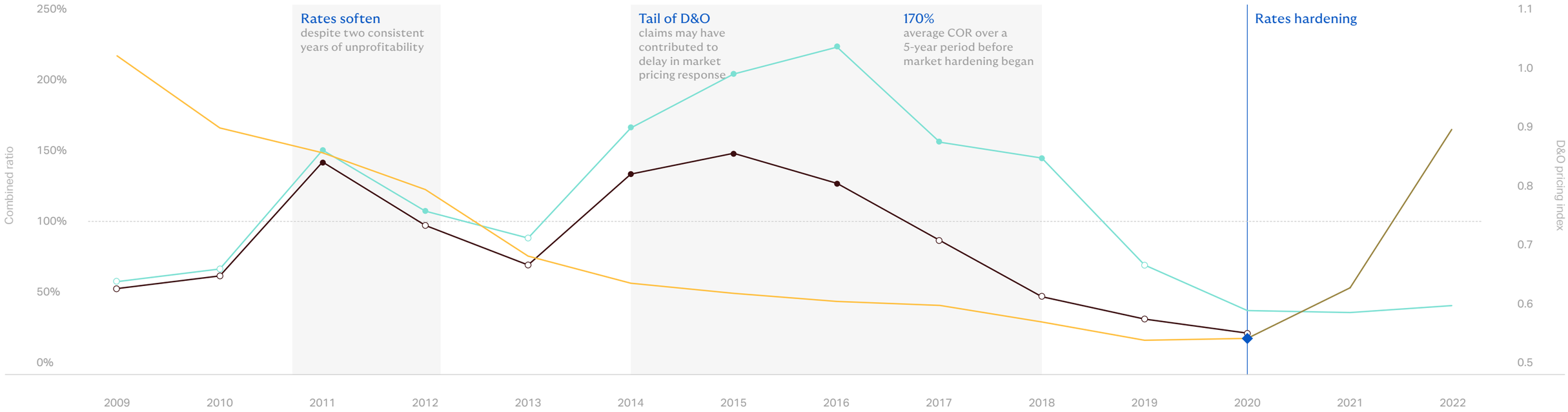
The distinction between the two combined ratio series is instructive. The ultimate view (light blue) reflects the full development of claims, while the contemporaneous view (brown) shows how profitability would have appeared in 2020. Although this incorporates an allowance for IBNR, it understates the extent to which losses ultimately developed. Despite indicating a challenging underwriting environment at the time, it did not appear as severe as it ultimately proved to be, which may have contributed to the slower market response.

This reflects the longer-tailed nature of D&O, where claims development can take time to fully emerge. As a result, the extent of underlying underperformance is not always immediately visible. It was only once the cumulative impact of these losses became clearer, alongside broader macroeconomic pressures, that pricing began to respond more decisively, leading to a more pronounced phase of market hardening.

Figure 9

D&O profitability and pricing across hard and soft market cycles (2009–2022)

Source: Howden's D&O LR Benchmark and NOVA



> Margin deterioration alone is not always sufficient to trigger an immediate market turn.

In comparison, the cyber market cycle has historically been more rapid and pronounced. The transition from hard to soft conditions, and from unprofitability to profitability, occurred over a shorter time horizon. The previous inflection point responded more quickly to deteriorating underwriting performance than was observed in D&O.

A key distinction lies in both the nature of loss development and the level of uncertainty surrounding the underlying risk. The ransomware-driven hardening between 2019 and 2021 was predominantly first-party, with insureds bearing the immediate financial impact and claims settled relatively quickly, resulting in faster loss visibility and a more immediate pricing response. At the same time, the rapidly evolving threat landscape and limited historical experience introduced a higher degree of uncertainty, which amplified market sensitivity and contributed to a sharper pricing adjustment when performance deteriorated.

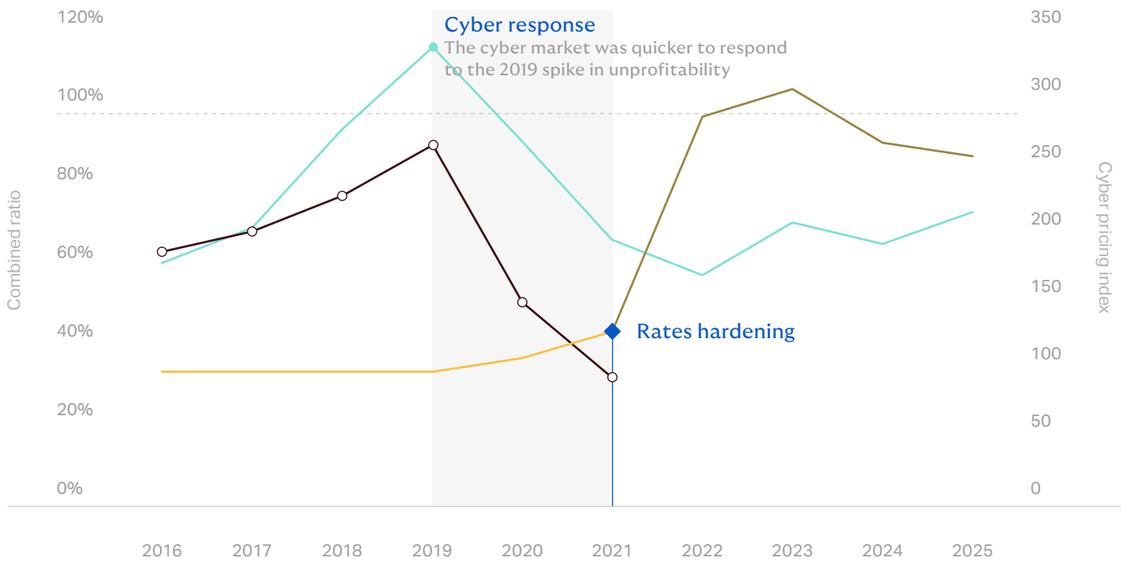
The current cyber landscape is more nuanced, with a greater proportion of data breach and third-party liability exposures alongside ransomware and outage events. These losses tend to develop over a longer time horizon, introducing a delay between loss occurrence and full recognition of their impact on profitability.

This difference is reflected in **Figure 10.1**. The faster convergence of first-party loss development to ultimate outcomes contrasts with the more gradual development associated with third-party claims, suggesting that market response times may lengthen or shorten, depending on how the composition of cyber losses evolves.

Figure 10.1

The cyber market pricing response to performance

Source: Howden's Cyber LR Benchmark and Cyber NOVA



Margin deterioration alone is not always sufficient to trigger an immediate market turn. As demonstrated in the D&O market, periods of sustained expected unprofitability can persist for several years before pricing responds decisively.

This suggests that the cyber market may be able to endure further softening, even in the presence of deteriorating underwriting performance, particularly where loss emergence remains uncertain, and in the absence of a more immediate catalyst such as a systemic event or broader macroeconomic disruption.

Figure 10.2

Cyber first-party versus third-party development patterns

Source: Howden's Cyber LR Benchmarks

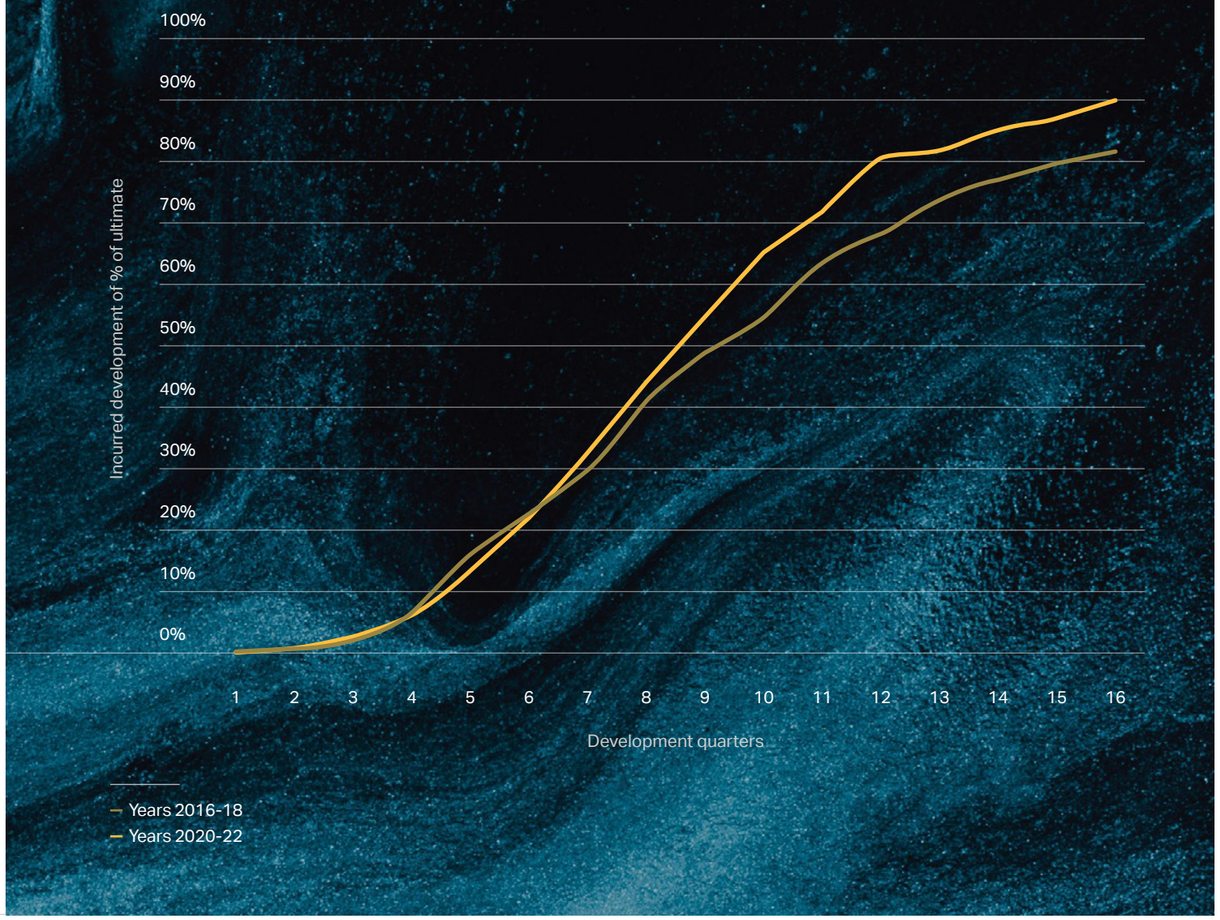


Figure 11.1

Data Leak Site (DLS) post count and reported victim payment rate 2019 to 2025

Source: Kela Security, Ransomware.Live, Coveware and Howden Re Analysis

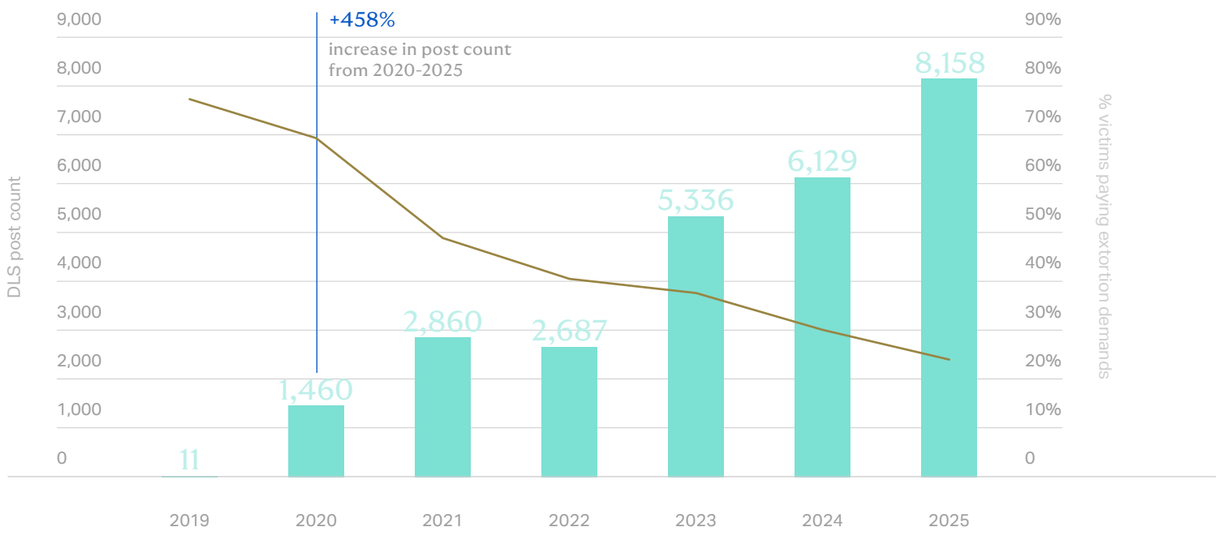
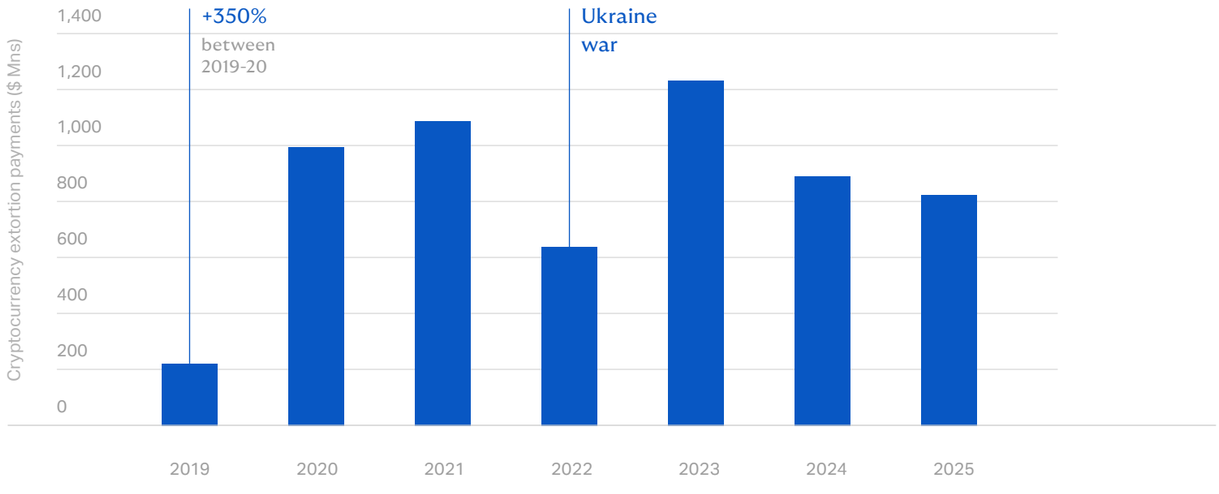


Figure 11.2

Tracked cryptocurrency extortion payments 2019–2025

Source: Chainalysis and FinCen Financial Trend Analysis



> "While first-party losses, such as ransom payments, have stabilised, the shift towards data extortion suggests a growing contribution from third-party costs.

The threat landscape provides additional context. Data leak sites (DLS) first emerged at the end of 2019, marking a shift in tactics to double extortion (data exposure and encryption). Although 2019 does not represent a full year of activity, **Figure 11.1** shows a sharp increase in DLS posts to 2020, followed by a further doubling in 2021. As this period coincided with the cyber market's ransomware-driven hardening, it highlights the type of step change in attack activity required to drive claims and, in turn, market cycles.

Yet the relationship between attack volume and financial impact has changed. While DLS activity has continued to rise, the reported proportion of victims making extortion payments has declined significantly. In effect, although more organisations are experiencing data leaks, fewer are paying.

While first-party losses, such as ransom payments, have stabilised, the shift towards data extortion suggests there will be a growing contribution from third-party costs. This reflects a combination of improved resilience and increased awareness around the limited utility of paying extortion demands.

As a result, the threat landscape is evolving towards a higher-frequency, lower-conversion model. For attackers, this implies a need to either increase the volume of attacks or enhance the effectiveness of extortion tactics to drive higher payment rates.

For the (re)insurance market, this suggests that while loss accumulation remains significant, it may not be sufficient on its own to trigger a market-dislocating period comparable to 2019-2021. A more pronounced shift in either loss severity or victim payment behaviour would likely be required to generate a similar pricing response.

Deteriorating underwriting performance also inevitably influences how insurers utilise reinsurance. In the past three to four years, many carriers have reduced cessions in order to retain more profit and create competitive tension to improve ceding commissions.

This approach has been largely successful, with most insurers achieving year-on-year increases in their commissions, although outcomes remain dependent on underlying performance and the commission base. However, should margin pressure intensify, incentives may shift, with insurers increasing cessions to protect net combined ratios.

These dynamics similarly extend to non-proportional protection. As catastrophe programmes typically attach at higher loss levels, they offer limited support to day-to-day underwriting performance while providing capital relief in more extreme scenarios. Also, within their own portfolio, insurers may place greater emphasis on attachment points and limit deployment as margins tighten given the potential impact on profitability.

In practice, quota shares can improve net combined ratios while aggregate stop-loss structures may have the opposite effect in the absence of triggering losses. As a result, reinsurance strategy becomes an important lever for insurers to manage profitability, particularly in more challenging underwriting environments.

2.3

Defined by determinism

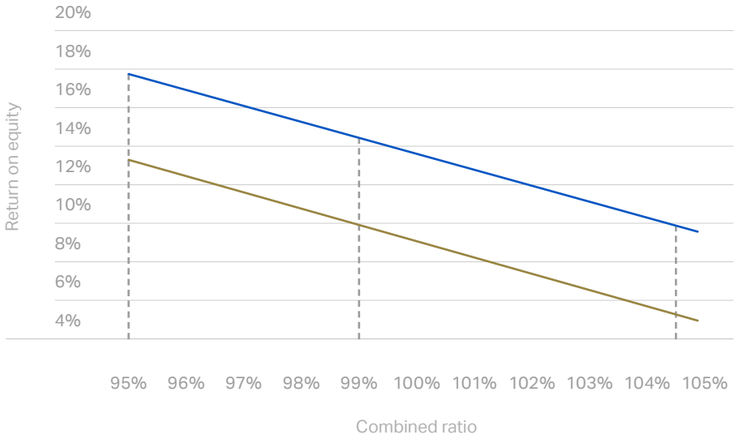
The final dynamic to consider is the influence of broader economic conditions on (re)insurance company performance. One key transmission channel is the effect of investment returns on carrier profitability. Figure 12 illustrates this clearly. Investment income can contribute approximately 75% of earnings for property and casualty insurers, meaning that macro-financial conditions play a significant role in overall profitability.

As a result, interest rates have a direct impact on the underwriting performance required to generate acceptable returns. Using a simplified balance sheet to illustrate this relationship, **Figure 12** shows that at higher investment returns (including running yields and realised gains) of around 6%, insurers can sustain combined ratios of approximately 102-103% while still delivering returns on equity of approximately 11-12%. In a lower rate environment, with investment returns closer to 4%, the same level of return on equity requires a stronger underwriting outcome, with combined ratios closer to 96% or 97%.

Figure 12

Impact of interest rates and investment returns on ROE and underwriting profitability

Source: Howden



Solvency margin	**80%**
Provisions / premiums	**200%**
Tax rate	**35%**

Investments	**280**
Technical reserves	**200**
Capital	**80**

Underwriting profits	**25%**
Net investment income	**75%**

Morgan Stanley

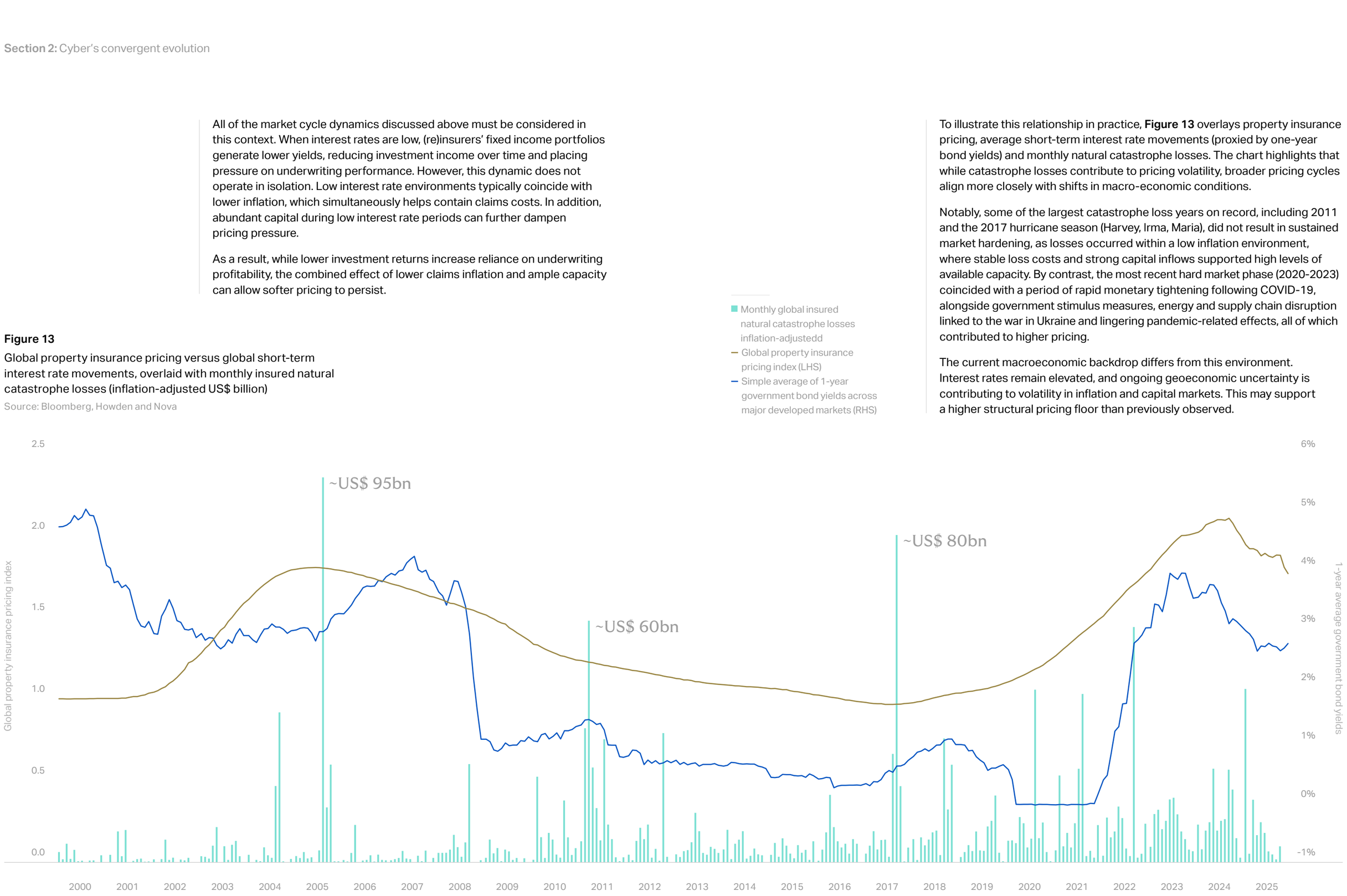
All of the market cycle dynamics discussed above must be considered in this context. When interest rates are low, (re)insurers' fixed income portfolios generate lower yields, reducing investment income over time and placing pressure on underwriting performance. However, this dynamic does not operate in isolation. Low interest rate environments typically coincide with lower inflation, which simultaneously helps contain claims costs. In addition, abundant capital during low interest rate periods can further dampen pricing pressure.

As a result, while lower investment returns increase reliance on underwriting profitability, the combined effect of lower claims inflation and ample capacity can allow softer pricing to persist.

Figure 13

Global property insurance pricing versus global short-term interest rate movements, overlaid with monthly insured natural catastrophe losses (inflation-adjusted US$ billion)

Source: Bloomberg, Howden and Nova



To illustrate this relationship in practice, **Figure 13** overlays property insurance pricing, average short-term interest rate movements (proxied by one-year bond yields) and monthly natural catastrophe losses. The chart highlights that while catastrophe losses contribute to pricing volatility, broader pricing cycles align more closely with shifts in macro-economic conditions.

Notably, some of the largest catastrophe loss years on record, including 2011 and the 2017 hurricane season (Harvey, Irma, Maria), did not result in sustained market hardening, as losses occurred within a low inflation environment, where stable loss costs and strong capital inflows supported high levels of available capacity. By contrast, the most recent hard market phase (2020-2023) coincided with a period of rapid monetary tightening following COVID-19, alongside government stimulus measures, energy and supply chain disruption linked to the war in Ukraine and lingering pandemic-related effects, all of which contributed to higher pricing.

The current macroeconomic backdrop differs from this environment. Interest rates remain elevated, and ongoing geoeconomic uncertainty is contributing to volatility in inflation and capital markets. This may support a higher structural pricing floor than previously observed.

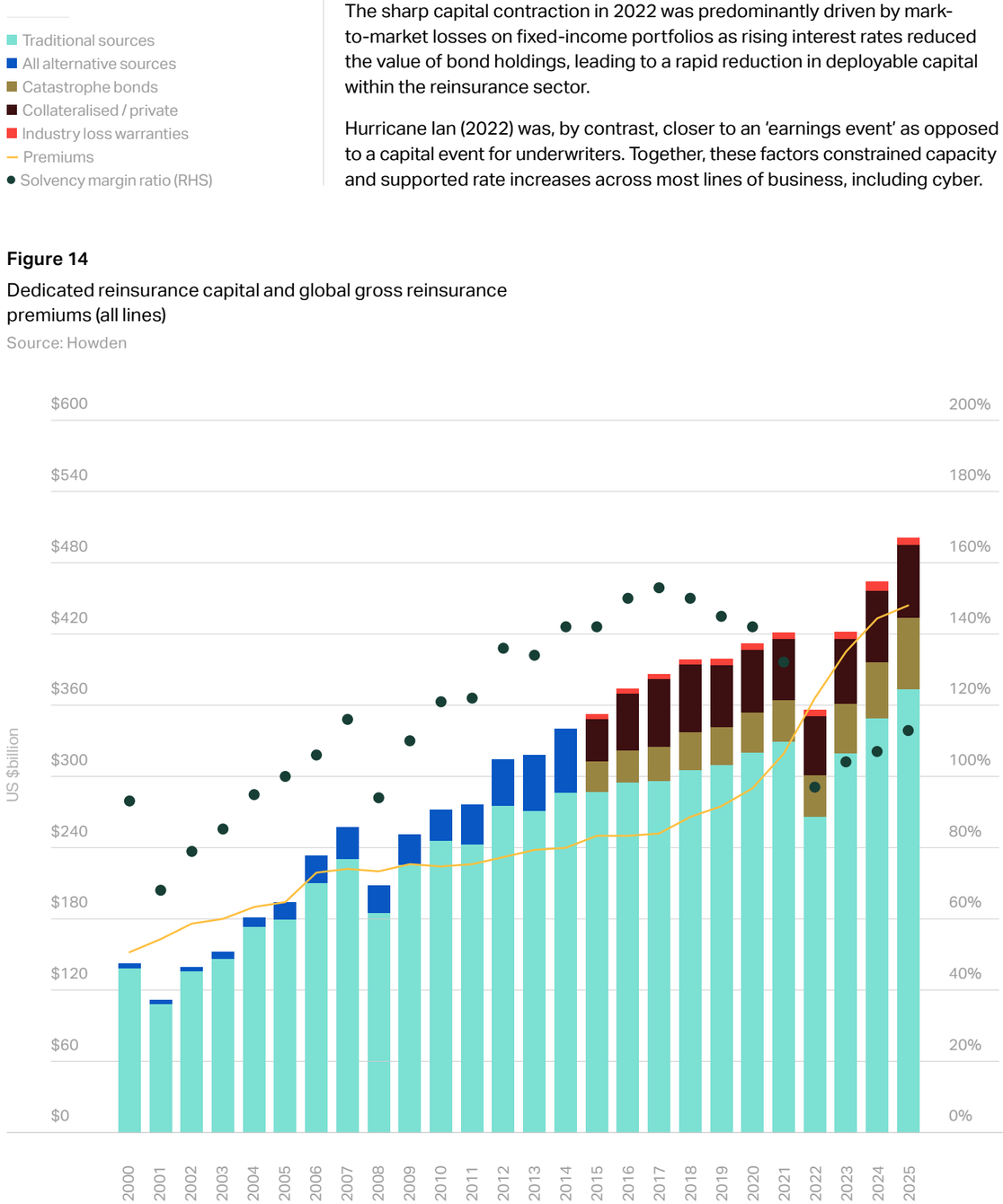
An alternative perspective is provided in **Figure 14**, which shows dedicated reinsurance capital alongside global gross reinsurance premiums written. The sharp capital contraction in 2022 was predominantly driven by mark-to-market losses on fixed-income portfolios as rising interest rates reduced the value of bond holdings, leading to a rapid reduction in deployable capital within the reinsurance sector.

Hurricane Ian (2022) was, by contrast, closer to an 'earnings event' as opposed to a capital event for underwriters. Together, these factors constrained capacity and supported rate increases across most lines of business, including cyber.

Figure 14

Dedicated reinsurance capital and global gross reinsurance premiums (all lines)

Source: Howden



The sector's capital structure also plays a role in shaping market response. Following a large loss event, capacity is typically constrained in the short term as balance sheets absorb losses, before higher pricing attracts new capital into the market.

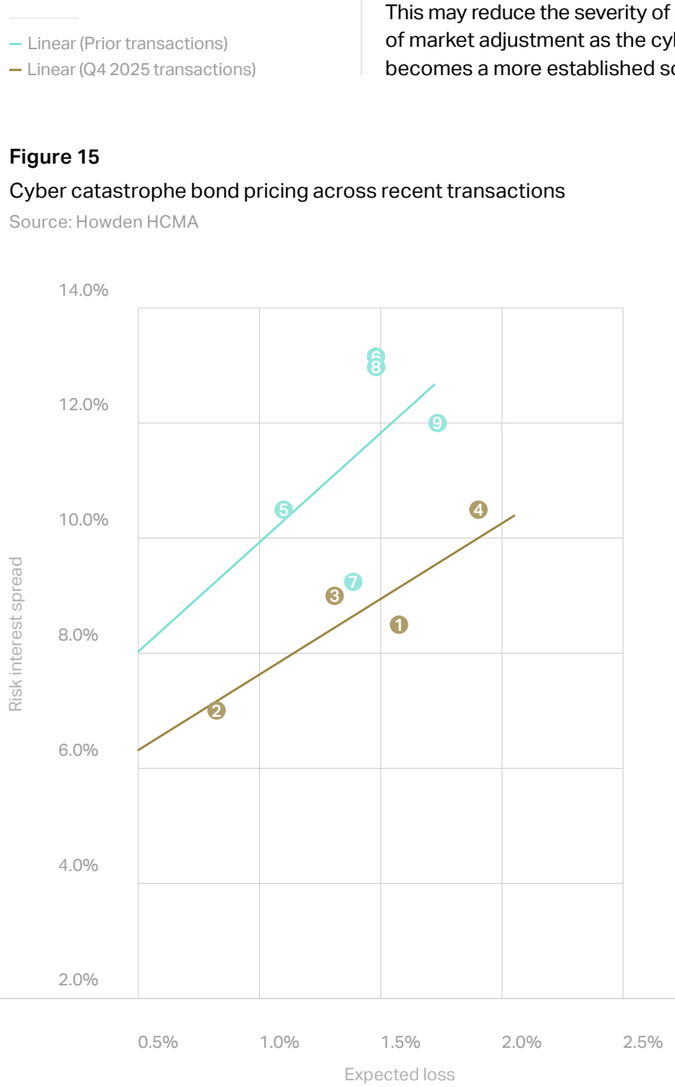
Figure 15 illustrates this dynamic in the context of cyber catastrophe bonds. While these instruments have historically traded at a premium, reflecting their relative novelty and structural complexity, recent transactions suggest this differential is narrowing as investor familiarity increases.

Although still relatively small in cyber, catastrophe bonds provide access to multi-year capacity, offering a more durable source of capital through the cycle. This may reduce the severity of post-event dislocation and moderate the speed of market adjustment as the cyber market matures and alternative capital becomes a more established source of capacity.

Figure 15

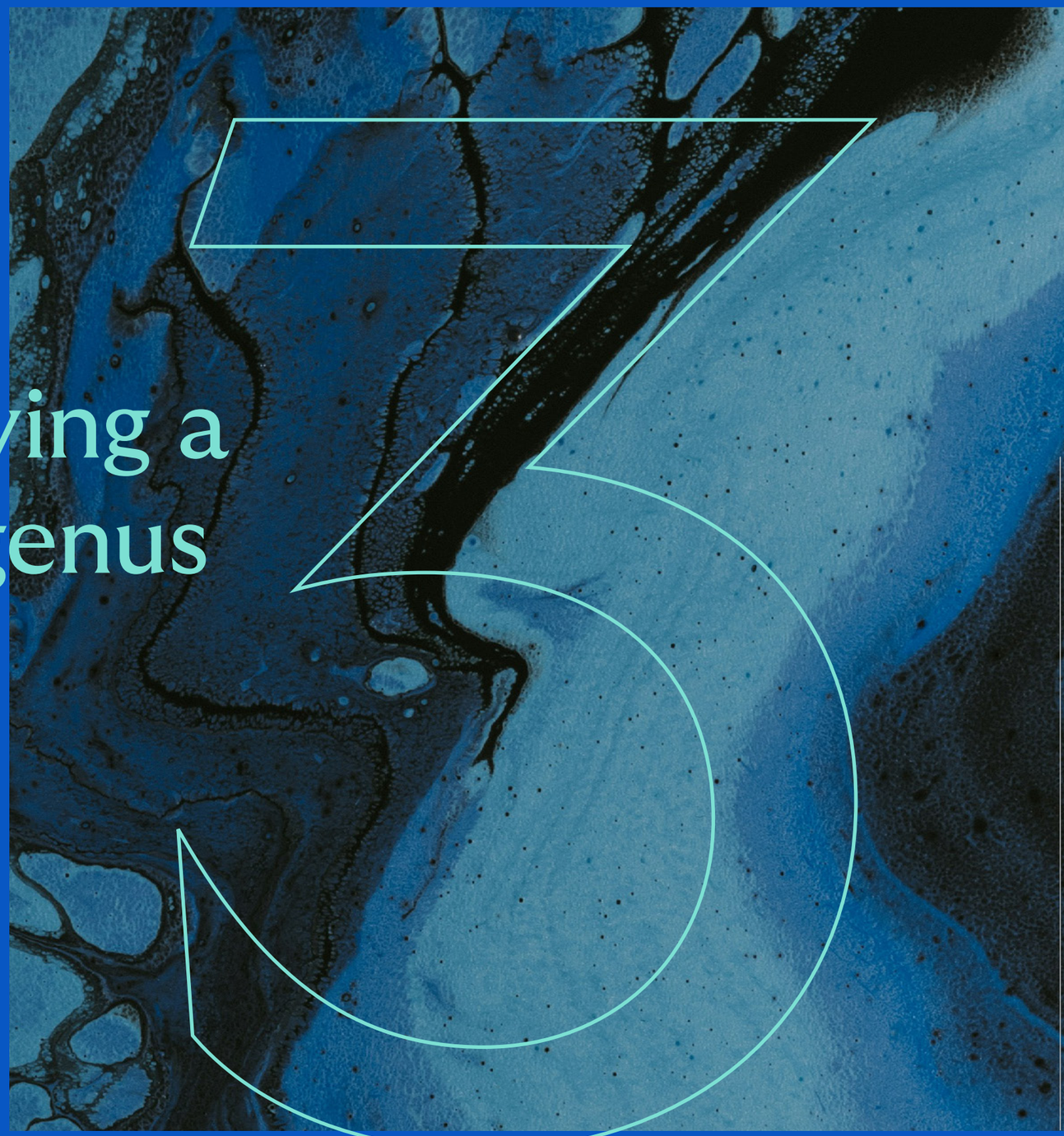
Cyber catastrophe bond pricing across recent transactions

Source: Howden HCMA



1	Eastlane for Chubb	**8.50%**
2	Polestar for Beazley	**7.00%**
3	Polestar for Beazley	**9.00%**
4	Polestar for Beazley	**10.50%**
5	Polestar for Beazley	**10.50%**
6	Polestar for Beazley	**13.25%**
7	Eastlane for Chubb	**9.25%**
8	Polestar for Beazley	**13.00%**
9	Matterhorn for Swiss Re	**12.00%**

Classifying a cyber-genus



Taken together, these dynamics highlight that the cyber pricing cycle is inherently more complex than in many other classes. Underwriting deterioration may ultimately drive an inflection point, although a shift towards third-party losses may delay the visibility of that deterioration and, in turn, the market response.

At the same time, given the relative immaturity of the class, a systemic cyber event of a magnitude comparable to a 2008 loss year in property-catastrophe could be sufficient to move the market.

However, loss experience is not the sole driver. Broader conditions, including sustained geopolitical and economic uncertainty, may also influence pricing through their impact on inflation, interest rates and capital availability. In this context, higher interest rates could support a structural pricing floor across multiple lines of business, including cyber.

Ultimately, market turning points will be determined by the interaction of these factors, with the timing and scale of any shift dependent on how they converge.

Howden Re's approach to navigating this uncertainty is to assess client portfolios holistically, combining proprietary threat intelligence with ongoing monitoring of geopolitical, economic and market conditions, alongside underwriting performance and claims experience.

3.1

A cyb-ionic future

Cyber-specific threat intelligence provides a forward-looking lens to assess how risks may materialise and the types of events that could ultimately trigger a shift in the cycle. Artificial Intelligence (AI) represents one of the most significant developments in this context. While AI has the potential to enhance defensive capabilities, it also lowers barriers to entry for threat actors and expands the overall attack surface.

Figure 16 shows that AI-related product detections are increasing across enterprise environments, particularly in areas such as generative AI and code development. The growing use of large language models has also led to an increase in AI-assisted software development, often referred to as 'vibe coding', which allows users to rapidly create applications and analytical tools. While these capabilities improve productivity, they also introduce new vulnerabilities and avenues for exploitation.

Given the pace of change, predicting the malicious use of AI remains inherently uncertain. At present, threat actors appear to be using AI primarily to accelerate established techniques rather than develop entirely new attack methodologies. However, this still has meaningful implications. As resource constraints fall and automation increases, the time between vulnerability discovery and exploitation is likely to shorten, reducing the defensive window available to organisations.

> "The shift towards data-driven attacks and breaches suggests a growing contribution from third-party losses.

Early indicators suggest that this is already translating into higher volumes of detected vulnerabilities and malicious activity **(Figure 17)**. Open-source malware tracking and CVE submissions show a clear increase in activity, while recent data indicates a notable rise in supply chain intrusion attempts. Together, these trends point towards a more scalable and accessible threat environment.

The primary implication is not necessarily a step change in individual event severity, but a sustained increase in event frequency. As attack methodologies scale, the loss environment is likely to become more attritional in nature, placing continued pressure on underwriting performance. At the same time, the shift towards data-driven attacks and breaches suggests a growing contribution from third-party losses, which are typically slower to develop and less immediately visible.

This has important implications for the market cycle. As observed in D&O, delayed loss visibility can slow the market's response to underlying deterioration. In this context, AI-driven developments may reinforce a pattern of gradual performance erosion rather than triggering a single dislocating event.

Figure 16

New product attribute detections

Source: HG insights

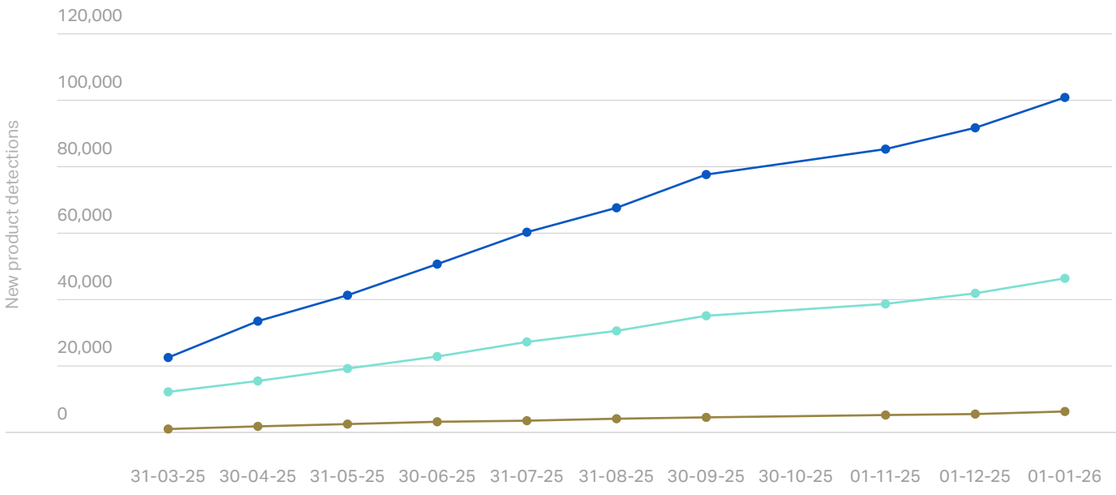
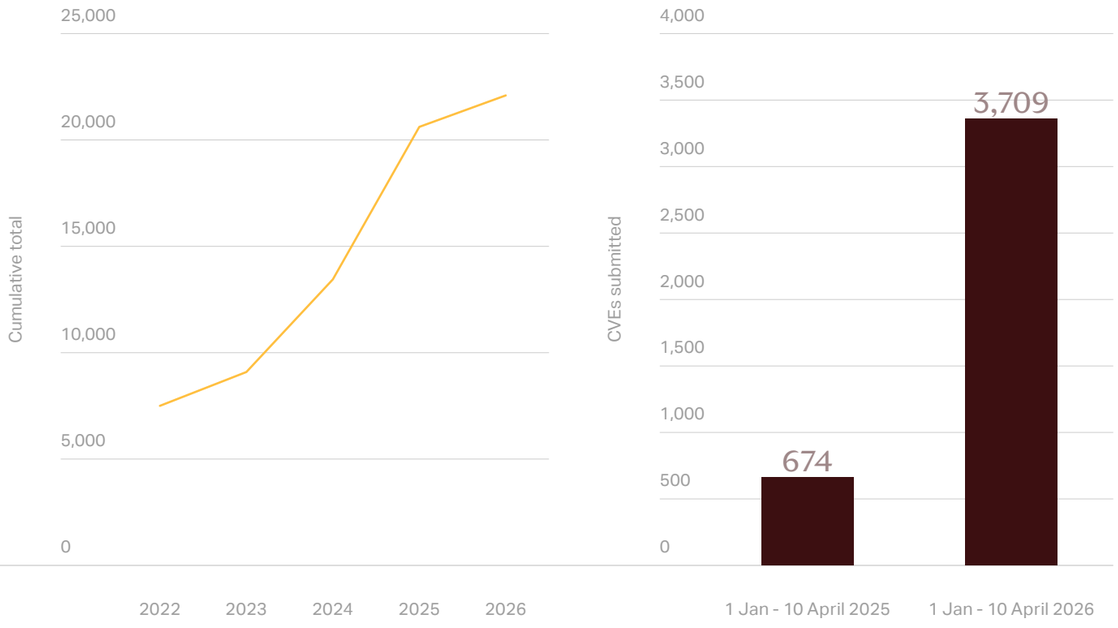


Figure 17

Cumulative total 'malware' tag in the Github Advisory Database and CVEs submitted by Github CNA to NVD

Source: Github Security Advisories, National vulnerability database and Howden Re Analysis



From a monitoring perspective, this reinforces the importance of forward-looking indicators **(Table 1)**. Metrics such as vulnerability disclosures, exploited-in-the-wild activity, malware propagation and AI-enabled fraud trends may provide early signals of deterioration that are not yet reflected in historical loss data.

Table 1

Indicators	Data sources	Inflection signal
Vulnerability disclosures and exploited-in-the-wild activity, zero-day exploitation uptick	CISA KEV/NVD	High
Monitoring reporting of MITRE ATT&CK tactics including Artificial Intelligence (T1588.007), and addition of novel TTPs to taxonomy	Threat reports/ data collection	Moderate
Open-source repositories & malware detections	Github	Moderate
Deep-fake/ AI generated cyber enabled fraud	Government fraud reporting	Moderate

> “The cyber market sits at the intersection of event-driven, accumulation-driven and macro-driven dynamics.

Conclusion

This report shows that the relationship between performance and pricing is not linear. As demonstrated through comparisons with property-catastrophe and D&O, market turning points are rarely driven by a single factor. Instead, they emerge from the interaction of loss experience, capital dynamics, claims visibility and broader macroeconomic conditions.

While these dynamics are well understood conceptually, their empirical expression in cyber reflects the market’s relative immaturity and short loss history. As such, this report seeks to frame the cycle through pertinent historical analogues and available data, rather than to attribute it to any single observable driver. This is particularly relevant given current technological, geopolitical and economic uncertainty.

In this context, cyber exhibits characteristics that may allow this non-linear relationship to persist. The market remains concentrated; shifts in capacity or risk appetite amongst a limited number of carriers can materially alter supply. At the same time, the evolving threat landscape suggests a transition from first-party dominated losses to more third-party and longer-tailed exposures, which may delay the visibility of underlying deterioration.

Importantly, a market-dislocating event may not need to reach the scale of a 1-in-200-year scenario. As observed in more mature classes, events of a lower return period may be sufficient to move the market, particularly where capital is constrained or risk appetite shifts.

This has direct implications for reinsurance strategy. If the market expects a series of moderate loss events, rather than a single extreme shock, designing protection that responds to accumulation and frequency becomes increasingly relevant. At the same time, securing stable sources of capacity, including through multi-year structures, may reduce the severity of post-event dislocation by limiting the extent to which capacity contracts immediately following a loss.

Ultimately, the cyber market sits at the intersection of event-driven, accumulation-driven and macro-driven dynamics. Forecasting the next phase of the cycle requires a forward-looking approach that integrates threat intelligence, capital conditions and evolving loss patterns. The challenge is not simply to predict the next event, but to identify the signals that precede a shift in market behaviour.

Report contributors

Luke Foord-Kelcey

Managing Director, Global Head of Cyber

luke.foord-kelcey@howdenre.com

Mark Lynch

Director, Head of Cyber Data & Analytics

mark.lynch@howdenre.com

Matthew Webb

Director, Head of Cyber Clients & Strategy

matthew.webb@howdenre.com

Harriet Gruen

Director, Head of Cyber Threat Intelligence

harriet.gruen@howdenre.com

Ram Ramakrishnan

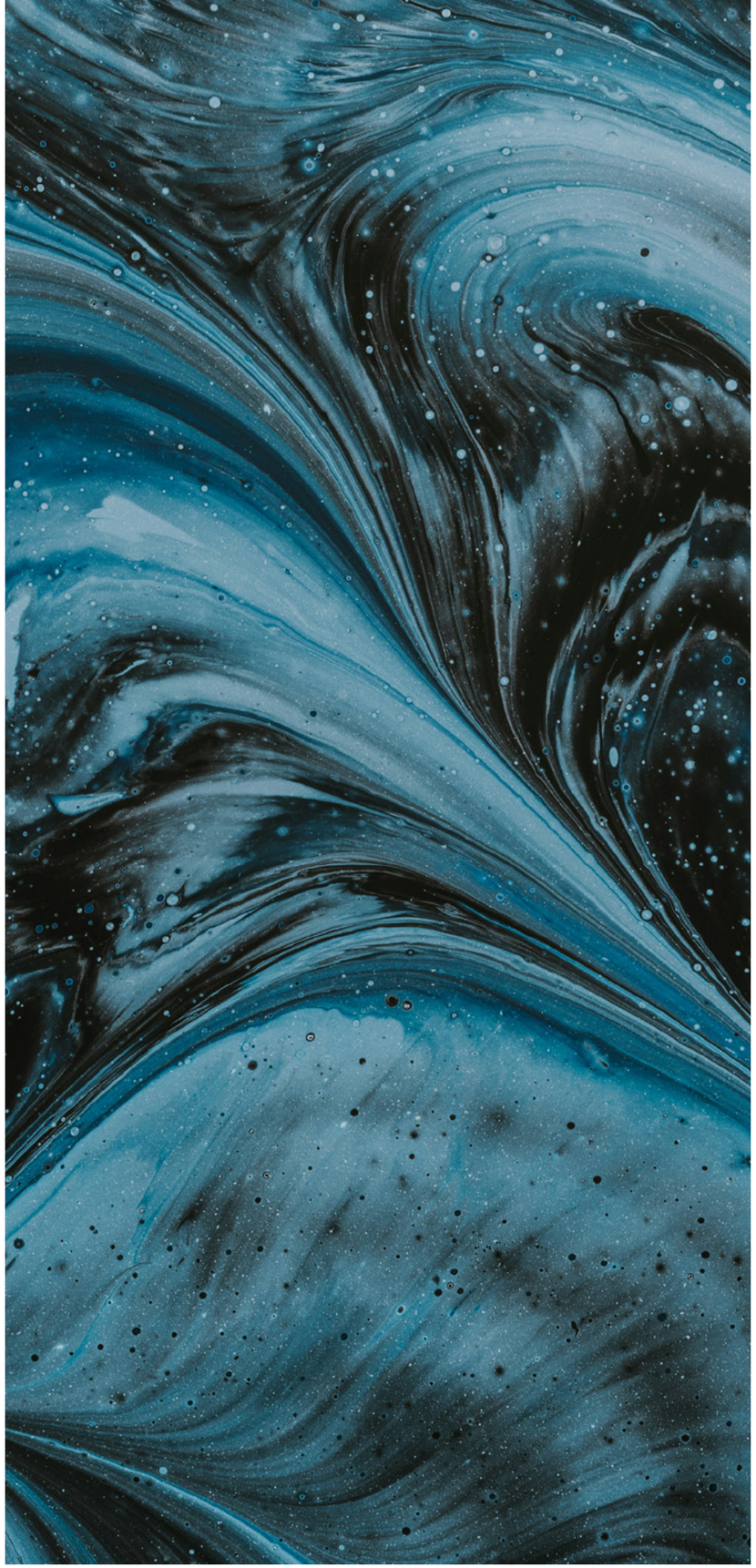
Director, Lead Cyber Actuary

ram.ramakrishnan@howdenre.com

Cecilia Assmundson

Associate Director, Cyber Data & Analytics

cecilia.assmundson@howdenre.com



Analytics and strategic advisory

David Flandro

Head of Industry Analysis & Strategic Advisory

david.flandro@howdenre.com

Michelle To

Head of Business Intelligence

michelle.to@howdenre.com

Nena Atkinson

Associate Director, Research

nena.atkinson@howdenre.com

One Creechurch Place, London EC3A 5AF

+44 (0)20 7623 3806
info@howdenre.com

howdenre.com