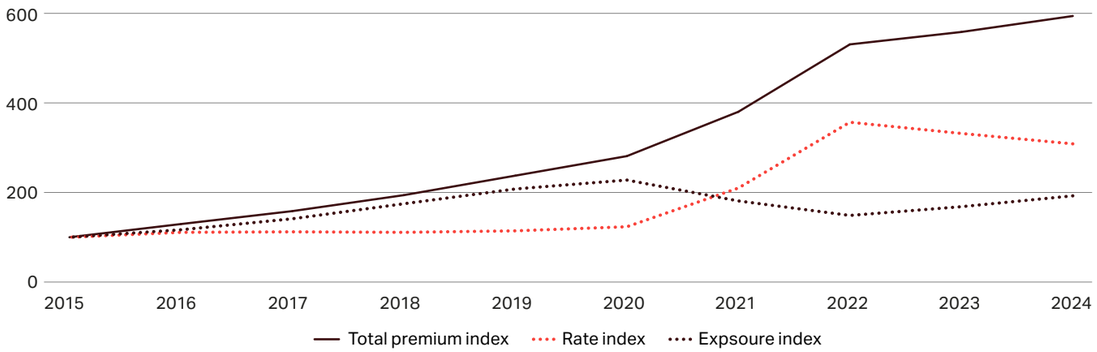
Cyber insurance

Rebooting growth

Key takeaways

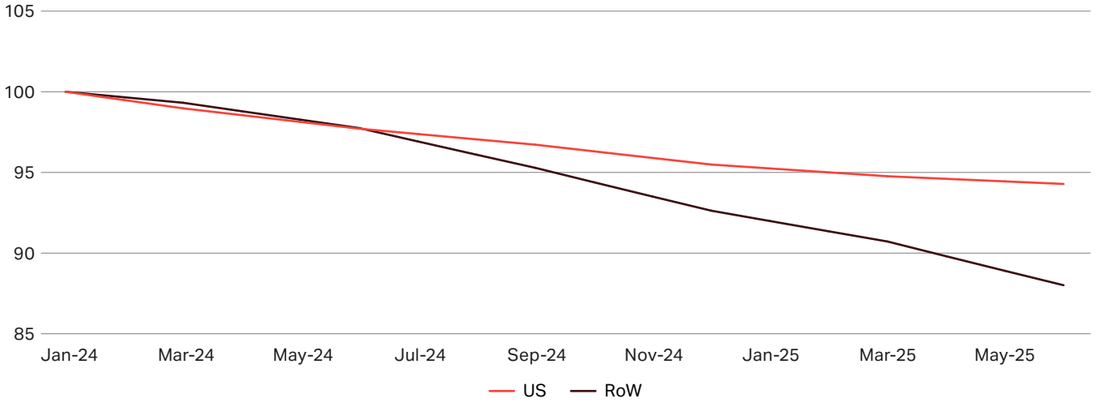
The cyber insurance market is at an inflection point, with premium growth faltering amidst declining rates and static exposures. The next growth cycle will focus on unlocking new risk pools, primarily through increased penetration in underserved regions, creating fresh opportunities for buyers and (re)insurers.

Plateauing global premium growth since 2022



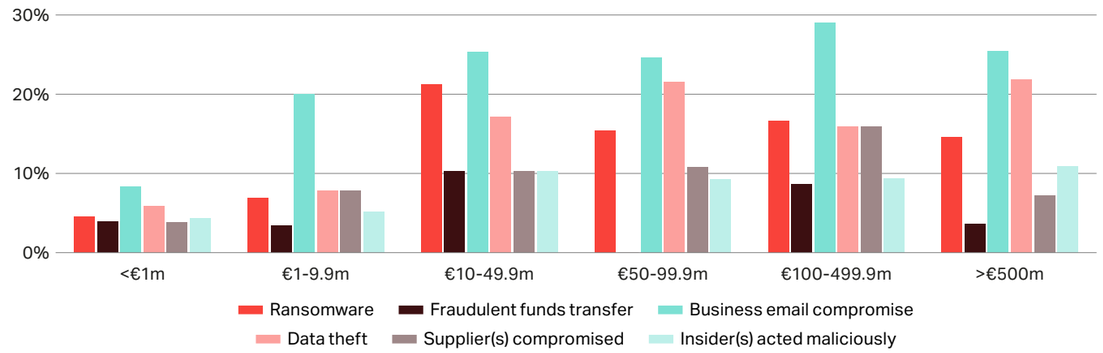
Favourable market conditions are allowing buyers to secure coverage at terms and rates not seen since before the hard market whilst insurers are deepening their commitment to a class that combines huge potential with a proven track record of profitability.

Softening rate environment in international markets in particular



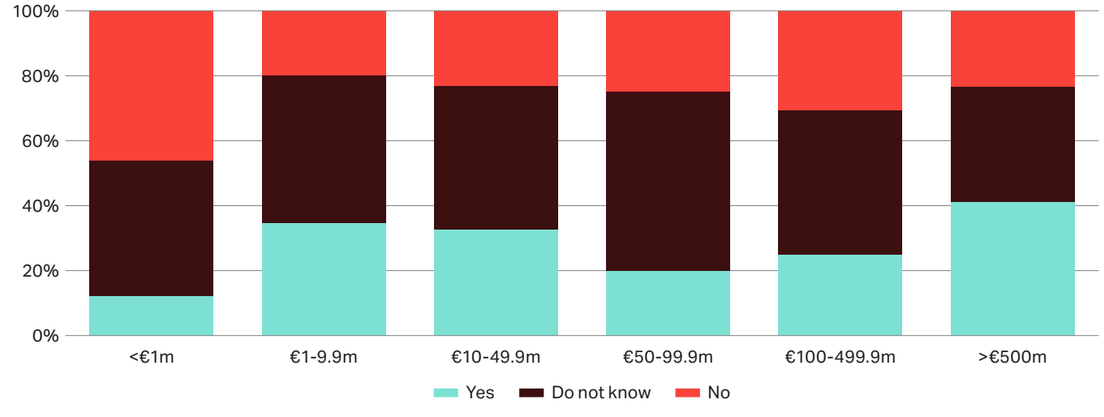
Future growth depends on securing new business, and Europe is the focus of this report. The estimated ~€300 billion economic impact of cyber attacks across France, Germany, Italy and Spain over the last five years underscores the scale of the threat and the urgent need for effective risk transfer.

Frequency of cyber attacks by revenue band for surveyed companies



This report reveals the compelling value of cyber insurance, with our analysis showing a 19% return on investment. Responsibility now lies with brokers and carriers to unlock latent demand – strengthening organisational resilience by accelerating recovery and reducing financial losses.

Future cyber insurance purchase intentions for non-buyer survey respondents



Executive summary

Cyber insurance has been one of the market's standout success stories of the past decade. Confronted by a complex and volatile threat landscape, costing businesses worldwide billions of dollars annually, the industry's response of combining proactive risk management services with traditional loss coverage has unlocked a powerful engine of growth and profitability.

Inflection point

For the first time, however, that growth story is encountering headwinds. Global rates continue to fall, down 22% on the mid-2022 peak, and the market's exposure base is not expanding quickly enough to compensate. Whilst performance remains stellar, with global combined ratios averaging 70% and generating approximately US$9 billion in underwriting profit between 2022 and 2024, global topline growth has slowed to 6% CAGR over the same period, a sharp drop from ~40% CAGR in 2020-22 when rates were rising at high double-digit levels.

Meeting even conservative premium targets will require a concerted effort to expand protection in underserved regions. Assuming current rate trends persist, our analysis shows that cyber insurers will need to grow exposures by approximately 15% annually over the coming years, with the bulk of that growth driven by new business rather than increases to existing limits.

Current market conditions offer a favourable entry point for new buyers, particularly in international markets, where rates have fallen by 12% since early 2024, compared to just 6% reductions in the US.

Europe: untapped potential

To better understand the opportunity in Europe, Howden recently surveyed a broad cross-section of businesses in Germany, France, Italy and Spain. The results reveal an acute need for coverage, a strong return on investment from risk management and insurance, and a receptive audience of first-time buyers ready to engage.

Half of surveyed businesses suffered a cyber attack between 2020 and 2025, resulting in an estimated economic cost of €307 billion across the four economies. Unsurprisingly, 69% of survey respondents believe their leadership accurately recognises cyber risk as a major threat.

Cyber insurance is proving highly effective in both reducing and transferring risk. In addition to paying claims, it incentivises the adoption of robust risk controls and provides access to crisis management services as standard, something only 20% of non-buyers currently have for incident response.

All told, for a business generating €500 million in annual revenue, purchasing cyber insurance can yield approximately €16 million in saved attack-related costs over a 10-year period. This equates to a 19% return on investment, more than enough to offset the cost of cover and a compelling demonstration of financial return.

The value proposition is clear. The market is pushing against an open door for companies that indicated their intention to purchase cyber insurance within the next five years, including 41% of those with revenues exceeding €500 million. The opportunity could be even greater, given the high proportion of non-buyers who remain undecided. This represents a clear call to action for the market to engage, educate and convert interest into uptake.

Howden has long championed cyber insurance by enhancing risk management, coverage and the buying experience. We produced this research to engage new audiences and inform decision-making.

Come and talk to us.

€307bn

Estimated economic cost of cyber attacks between 2020 and 2025 across Germany, France, Italy and Spain.

19%

Return on investment from cyber insurance for businesses generating €500m in annual revenue.

41%

Large enterprises (>€500m revenue) planning to purchase cyber insurance for first time within five years.

An inflection point

Cyber insurance is at a pivotal moment in its evolution. Having followed the distinctive trajectory of an emerging speciality line – early caution, rising confidence fuelled by strong results, a market-shifting loss phase and capacity retreat – the cyber market is now at an inflection point as competition ramps up and rates fall.

With current market conditions likely to persist for the foreseeable future (barring a major loss), future growth is dependent on expanding penetration across underserved markets such as SMEs and international territories.

The value of (and need for) cyber insurance has never been stronger. In a high-threat 18-month period marked by high-profile ransomware hacks on individual businesses, including the recent targeting of UK and US companies, and more widespread impacts from larger-scale attacks, alongside a separate non-malicious IT outage, cyber insurance has proved critical to the resilience of impacted firms and wider economies.

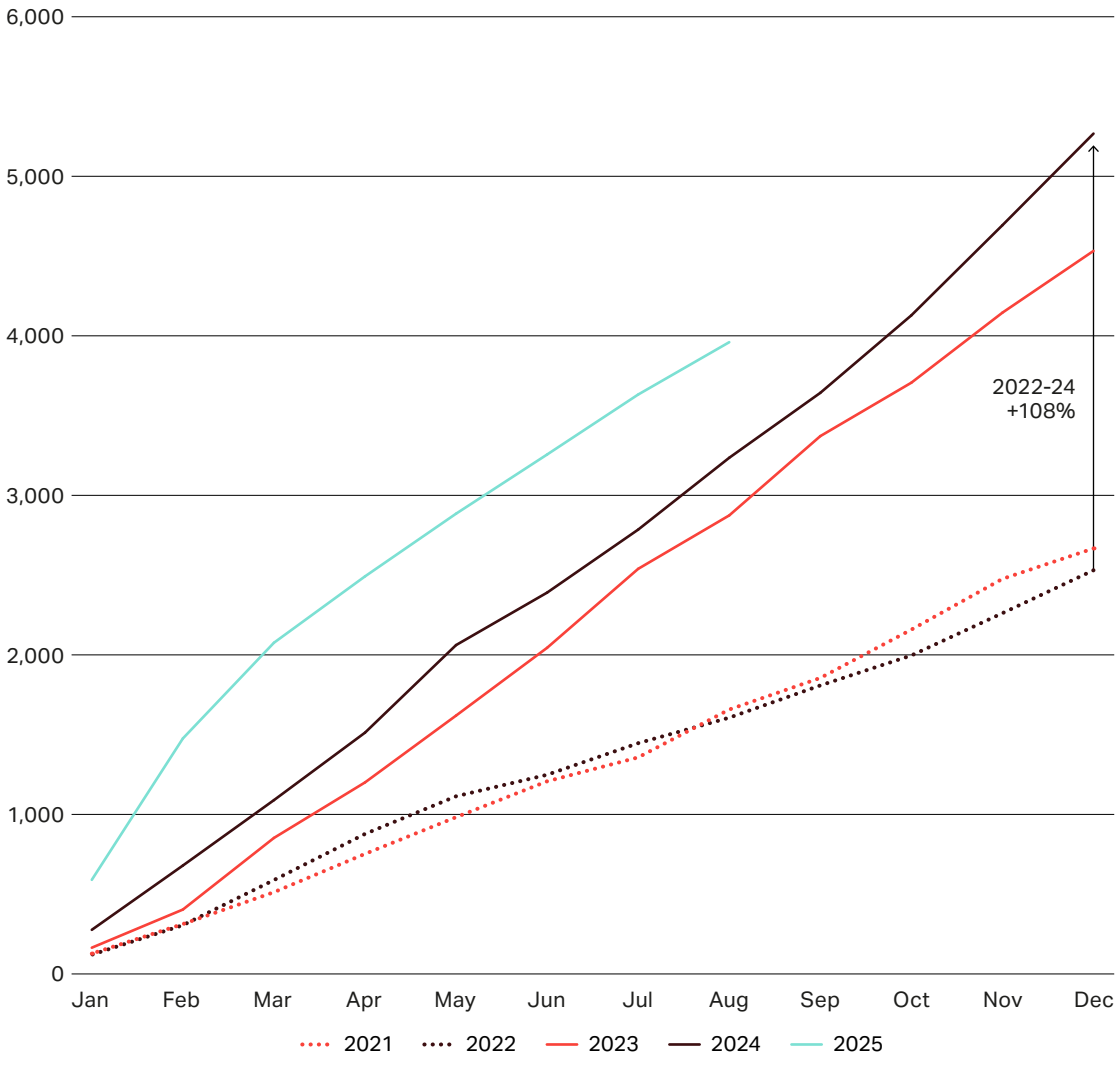
Beyond paying claims, cover also delivers immediate access to expert incident response services, enabling policyholders to contain threats, accelerate recovery and limit damage. Protected SMEs in particular have benefitted from the external expert services provided by their policies.

A pervasive threat

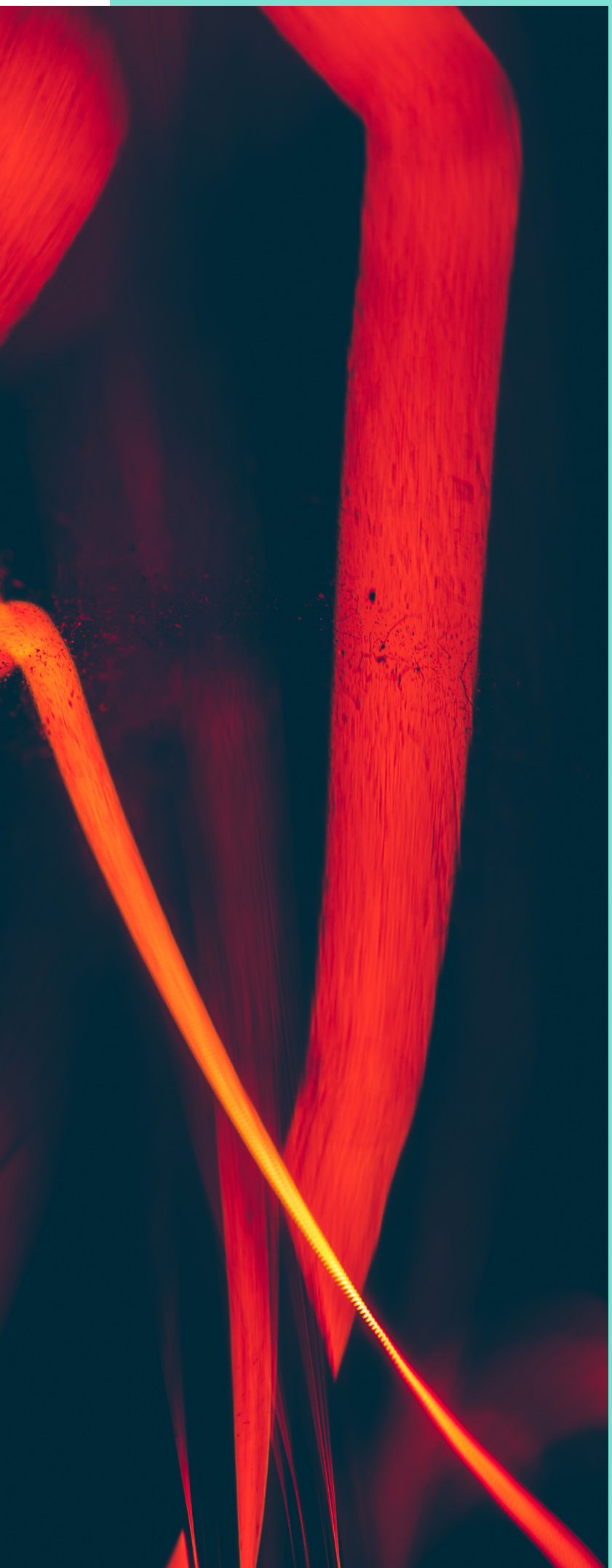
Strengthened cyber resilience is paying dividends for policyholders (and insurers) in what remains a hostile risk landscape. Ransomware persists as a leading threat, with every year since 2022 seeing more global incidents than the last (as shown by NCC data in Figure 1).

Still-elevated underwriting margins are now being squeezed by rising attritional losses and the continued occurrence of larger scale attacks. Microsoft recently confirmed that state-linked hackers exploited a vulnerability in its SharePoint servers, impacting at least 400 companies, whilst more than 700 firms were affected by a separate breach involving Salesloft Drift.

Figure 1: Cumulative global ransomware activity – 2021 to 3Q25[1]
(Source: Howden analysis based on NCC data)



[1] NCC Group tracks ransomware groups operating the hack and leak double extortion tactic by monitoring leak sites and scraping victims' details as they are released.



At the same time, a different kind of risk continues to intensify in the US, where privacy-related claims are climbing due to a surge in biometric breaches and pixel tracking lawsuits. Combined with the spectre of risk aggregation from systemic threats, the cyber insurance market is now navigating a unique loss environment characterised by attritional claims, large scale incidents and longer-tail-risks.

Despite the fluid threat landscape, made all the more uncertain by rising geopolitical tensions and rapid technological change, cyber is one of the better performing areas of insurance and remains a focal point for net new business and innovation. Businesses are benefitting from favourable market conditions whilst strong results and the draw of large, untapped risk pools (in non-US territories especially) are securing increased commitments from (re)insurers.

All of which underscores the compelling proposition offered by cyber insurance to buyers and capacity providers alike currently. The analysis that follows portrays a (complex) loss landscape that remains within tolerance levels, a softening rate environment, albeit with accelerating bifurcation between the US and other regions, and a major growth opportunity that hinges on a stronger flow of new business to reclaim cyber's position as one of the fastest-growing areas of insurance.

01

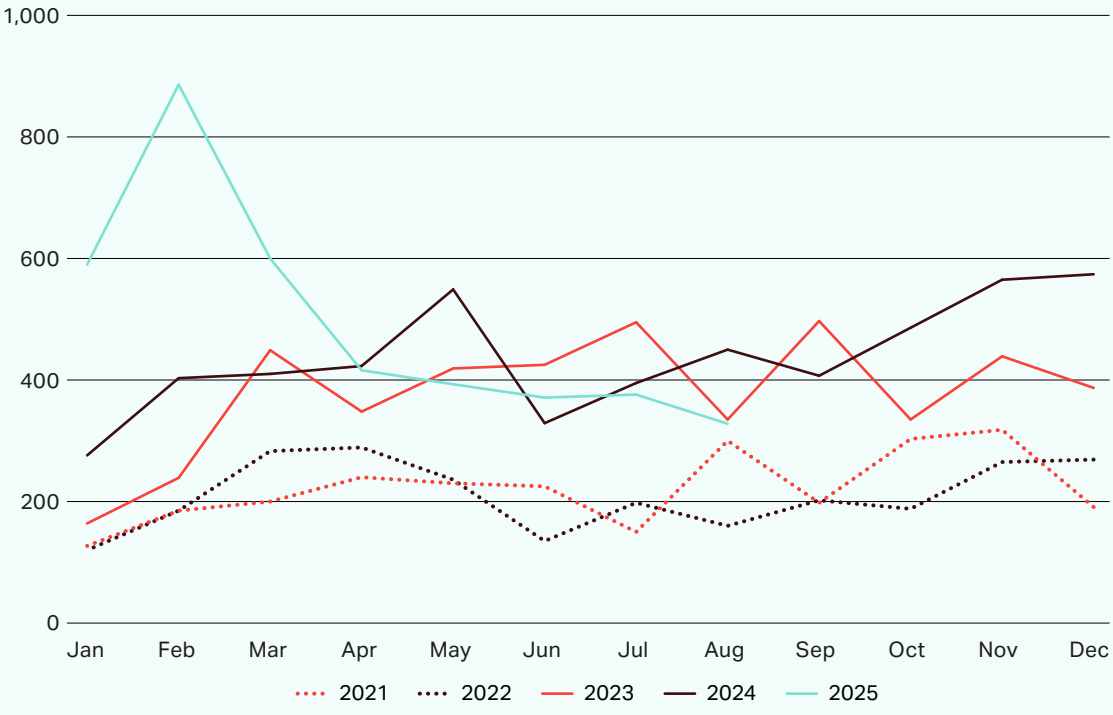
Reining in ransomware

Ransomware continues to dominate the cyber loss environment, as demonstrated this year by a number of devastating attacks and the involvement of threat actors beyond hostile nation states. The prominence of breaches exploiting third-party suppliers, often by using social engineering techniques carried out by English native speakers to deceive help desks and gain access, has been a notable development in 2025.

The increase in global ransomware attacks – driven in large part by a lagged spike in the first quarter from a mass exploitation campaign by ransomware group Cl0p and the series of Scattered Spider attacks against a wide array of UK and US firms in the second and third quarters – is indicative of the enduring threat to businesses.

Analysis in Howden Re's recently released Cyber Watch threat report[2] shows that 9% of ransomware victims in the first half of 2025 matched with insured entities in our proprietary industry exposure database (compared to 8% for full-year 2024). The majority of these were smaller companies (below US$50 million in revenue), demonstrating the impact of opportunistic campaigns on SMEs but also how coverage is being extended to vulnerable businesses.

Figure 2: Monthly breakdown of global ransomware activity – 2021 to 3Q25
(Source: Howden analysis based on NCC data)



[2] Howden Re, *Cyber Watch report: strategic threat review*, August 2025.

Ransomware losses in 2025 have reached alarming levels of severity at the micro level, with several high-profile attacks resulting in multi-million-dollar damages and exposing critical vulnerabilities of enterprise systems.

There are signs of progress at the macro level, however. The proportion of ransomware victims able to stop an attack before data encryption takes place rose from 27% in 2024 to 44% in 2025 (as shown by Figure 3), reflecting meaningful advances in monitoring and rapid response capabilities, and improved organisational resilience more broadly.

Figure 3: Data encryption rate in ransomware attacks – 2020 to 2025
(Source: Howden analysis based on Sophos data)

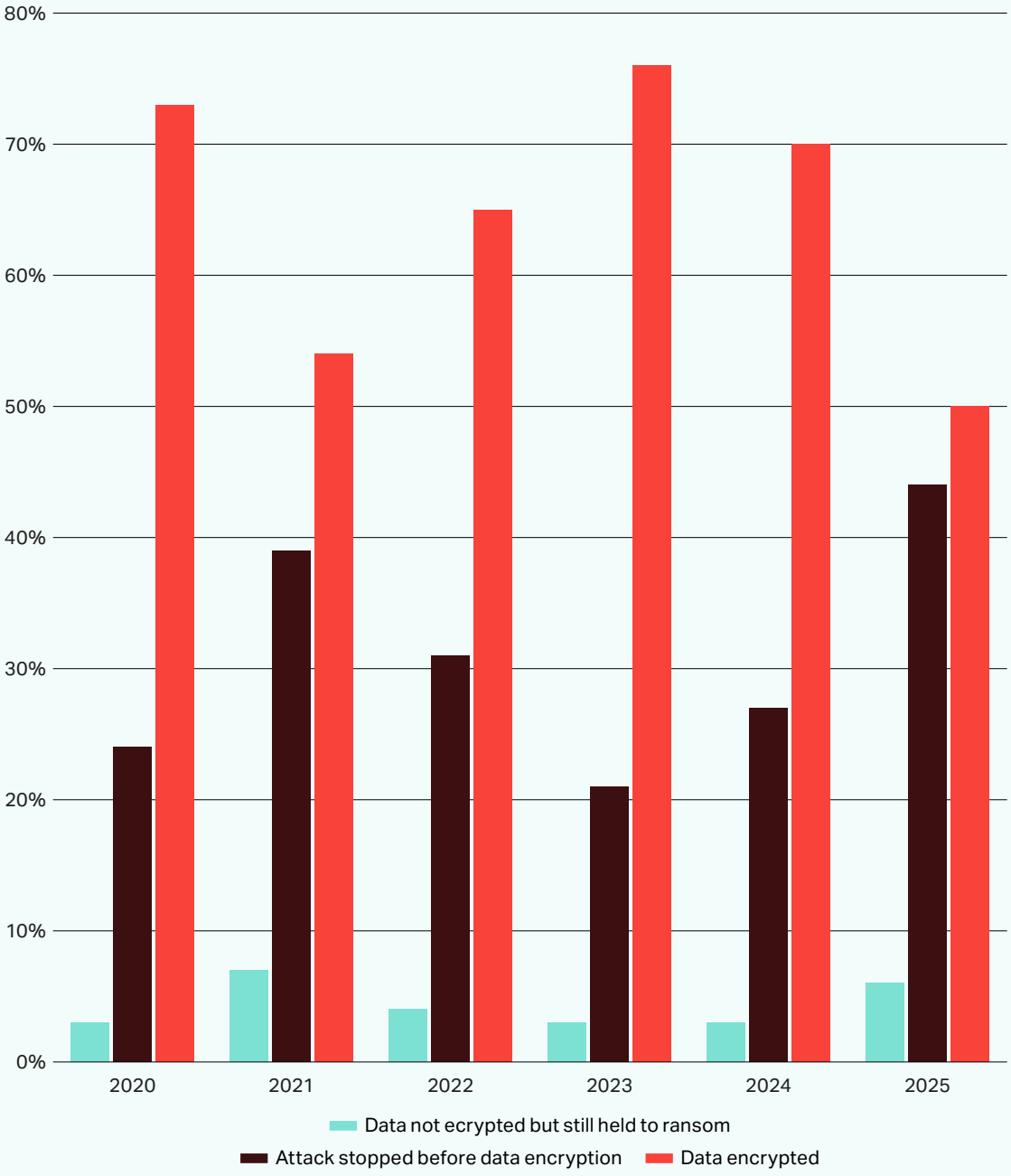
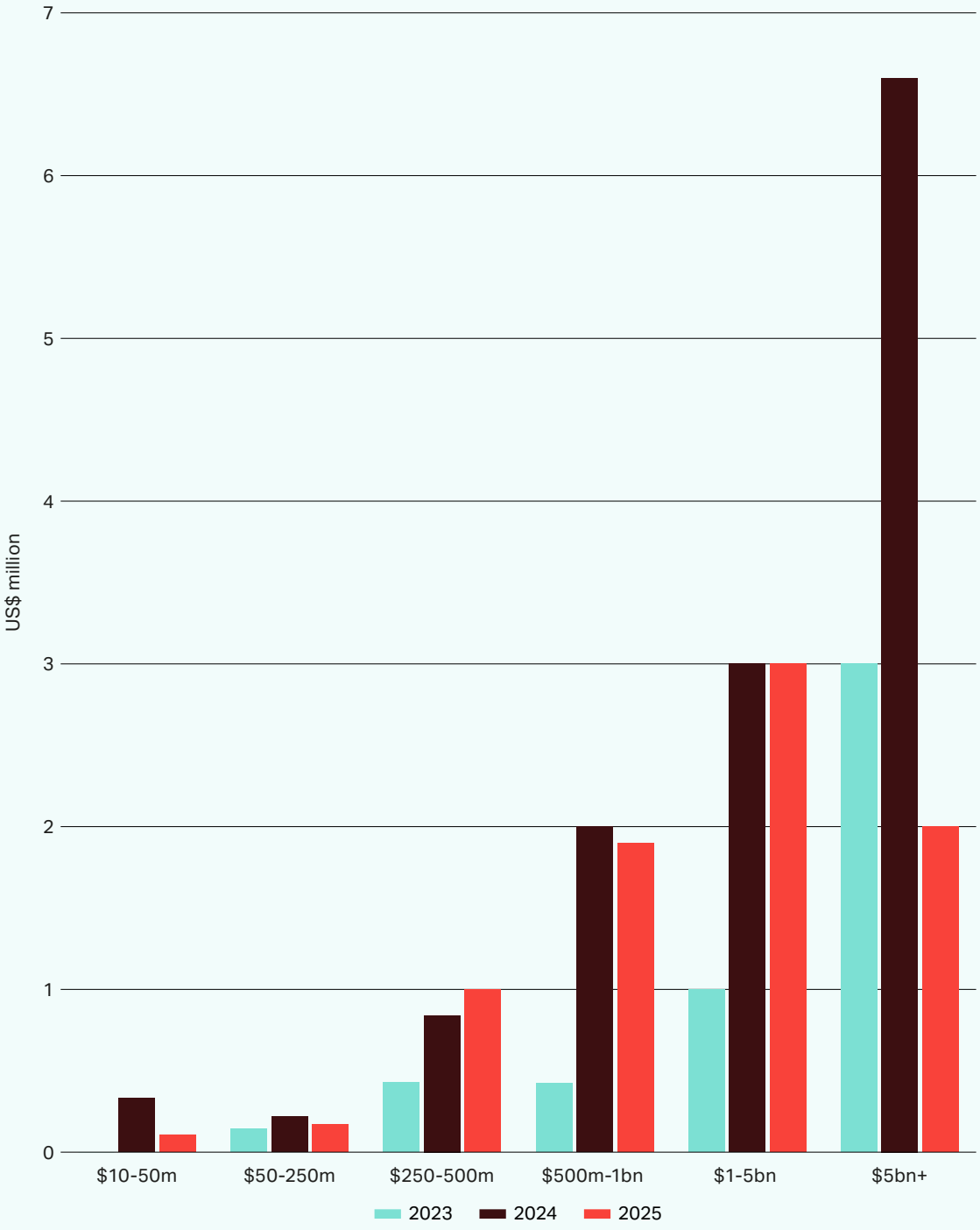


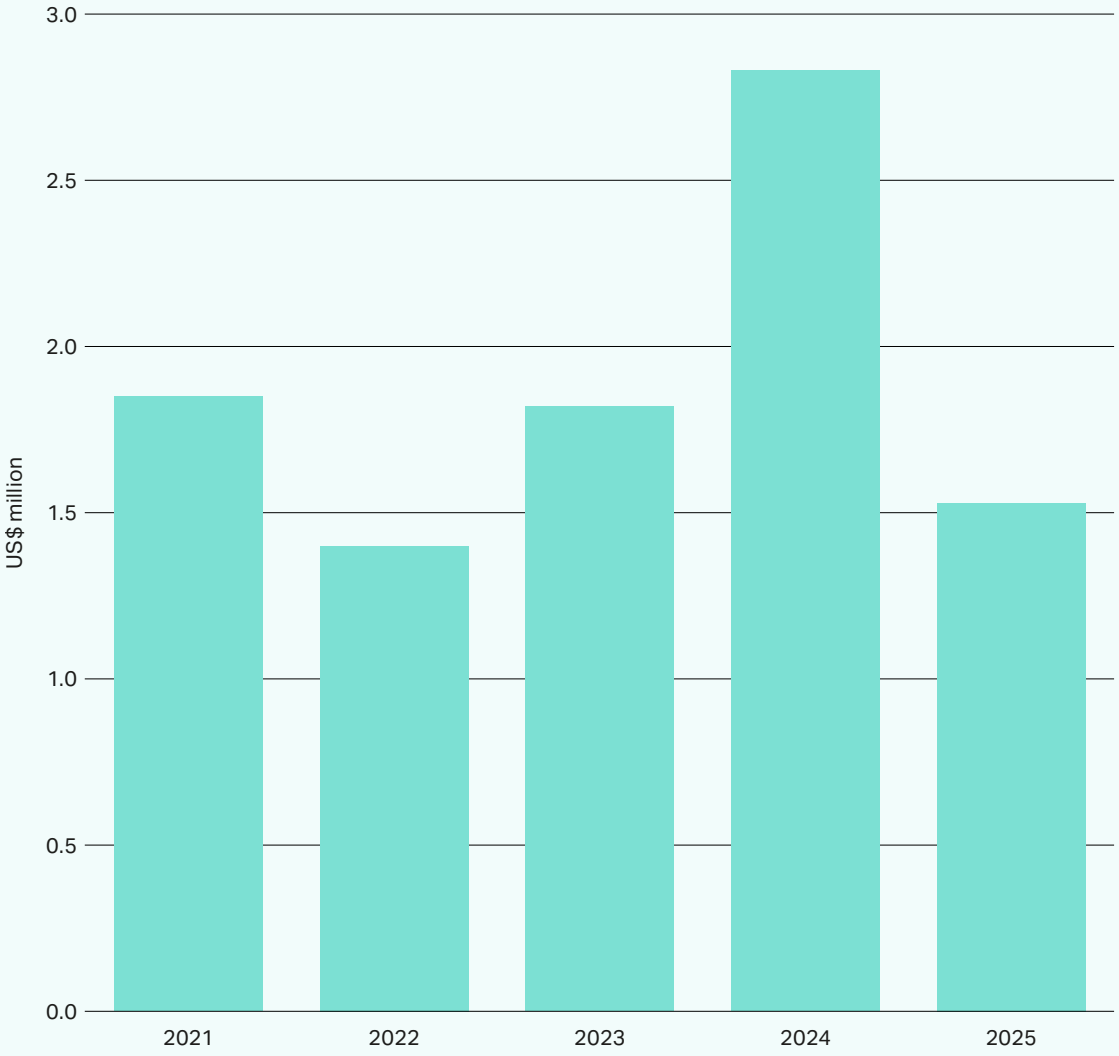
Figure 4 shows that median ransom payments have either remained stable or increased across most revenue bands, except for the US$5 billion plus category, which fluctuates depending on whether large companies are attacked. Ransom amounts are closely tied to company size, meaning that year-on-year changes in the overall average payment are more driven by the revenue profile of victims than shifts in the quantum of payments.

Figure 4: Median ransom payment by revenue band – 2023 to 2025
(Source: Howden analysis based on Sophos data)



Recovery costs are an additional burden on businesses that often exceed the quantum of ransom payments. Whilst Figure 5 shows a 45% reduction in average costs in 2025, US$1.5 million, on top of any ransom payment, remains a significant amount of money that carries serious implications for most organisations.

Figure 5: Mean recovery costs from ransomware attacks – 2021 to 2025[3]
(Source: Howden analysis based on Sophos data)



Despite an active start to the year on the ransomware front, improvements in cyber security are proving highly effective in making organisations more resilient overall. The value of cyber insurance is clear – not only as a financial safety net, but also as a facilitator of improved cyber hygiene, incident response and operational resilience.

[3] Recovery costs include downtime, people time, device costs, network costs, lost opportunities and exclude ransom payments.

02

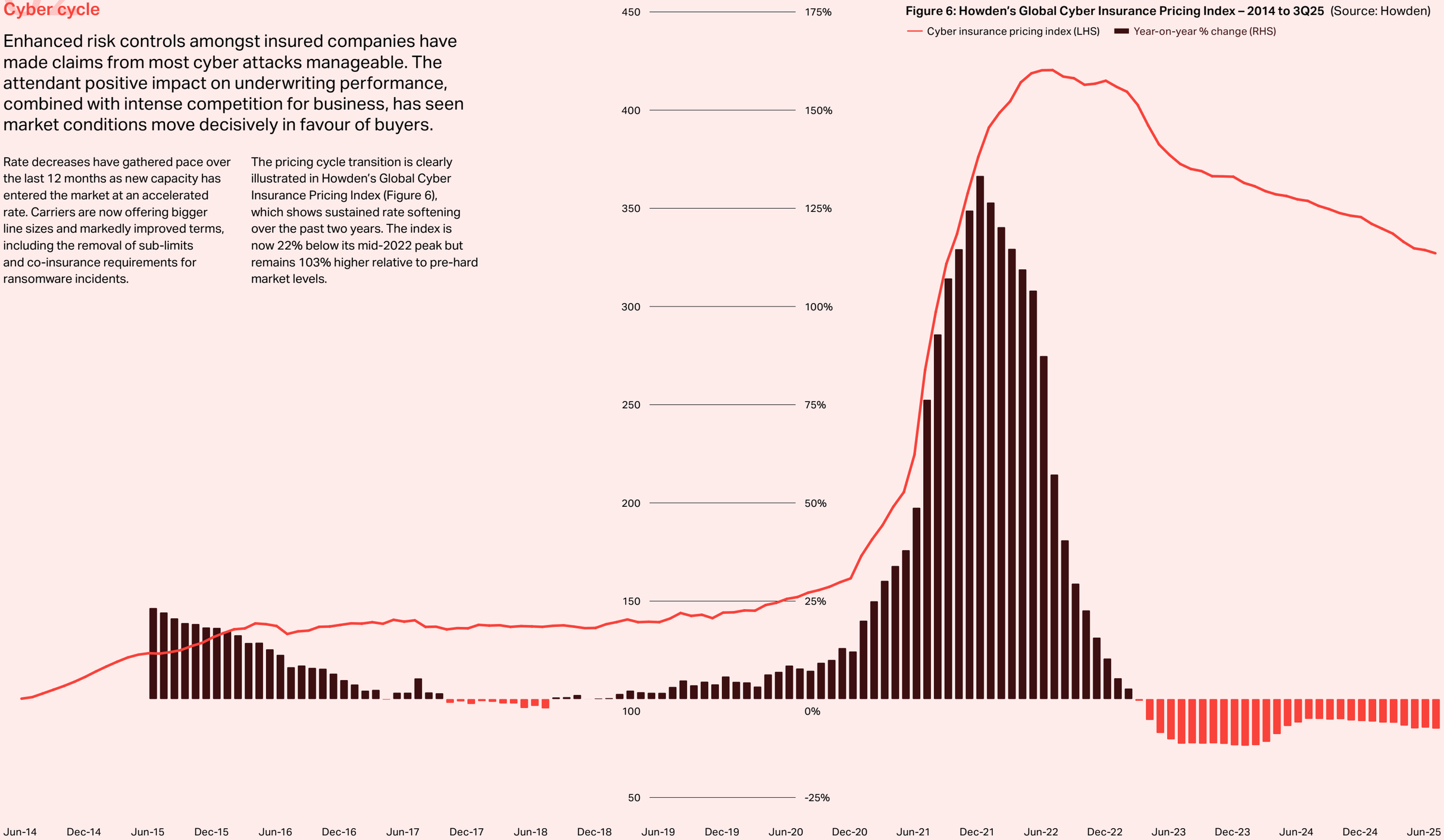
Cyber cycle

Enhanced risk controls amongst insured companies have made claims from most cyber attacks manageable. The attendant positive impact on underwriting performance, combined with intense competition for business, has seen market conditions move decisively in favour of buyers.

Rate decreases have gathered pace over the last 12 months as new capacity has entered the market at an accelerated rate. Carriers are now offering bigger line sizes and markedly improved terms, including the removal of sub-limits and co-insurance requirements for ransomware incidents.

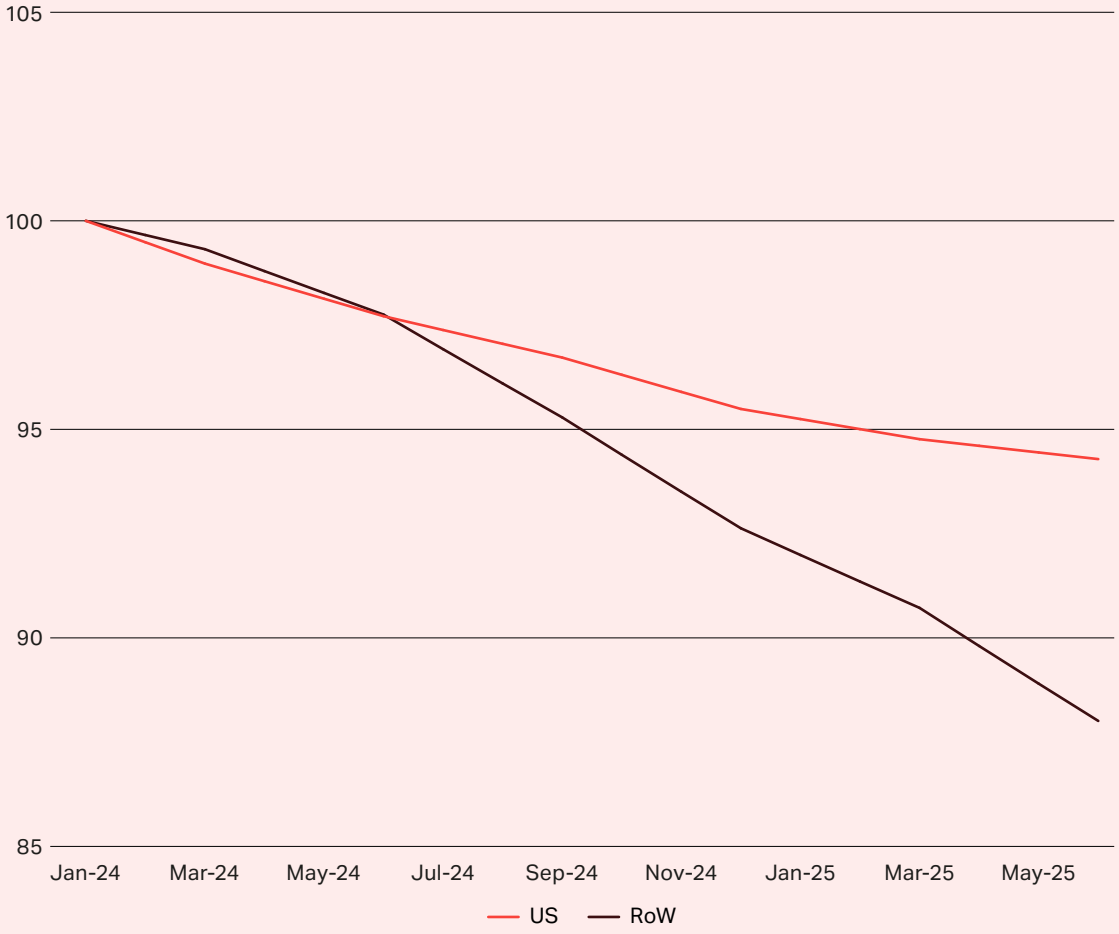
The pricing cycle transition is clearly illustrated in Howden's Global Cyber Insurance Pricing Index (Figure 6), which shows sustained rate softening over the past two years. The index is now 22% below its mid-2022 peak but remains 103% higher relative to pre-hard market levels.

Figure 6: Howden's Global Cyber Insurance Pricing Index – 2014 to 3Q25 (Source: Howden)



Pricing trajectories between the US and international markets have begun to diverge, as shown by Figure 7. In international markets, where conditions remain highly favourable for buyers, manageable loss experience and strong growth potential are yielding rate reductions in the low- to mid-teens range whilst the US market is starting to show price stabilisation as it contends with privacy-related claims that are unique to its regulatory and litigation environment.

Figure 7: Cyber insurance pricing indices for US vs rest of the world – 2024 to 1H25
(Source: Howden)

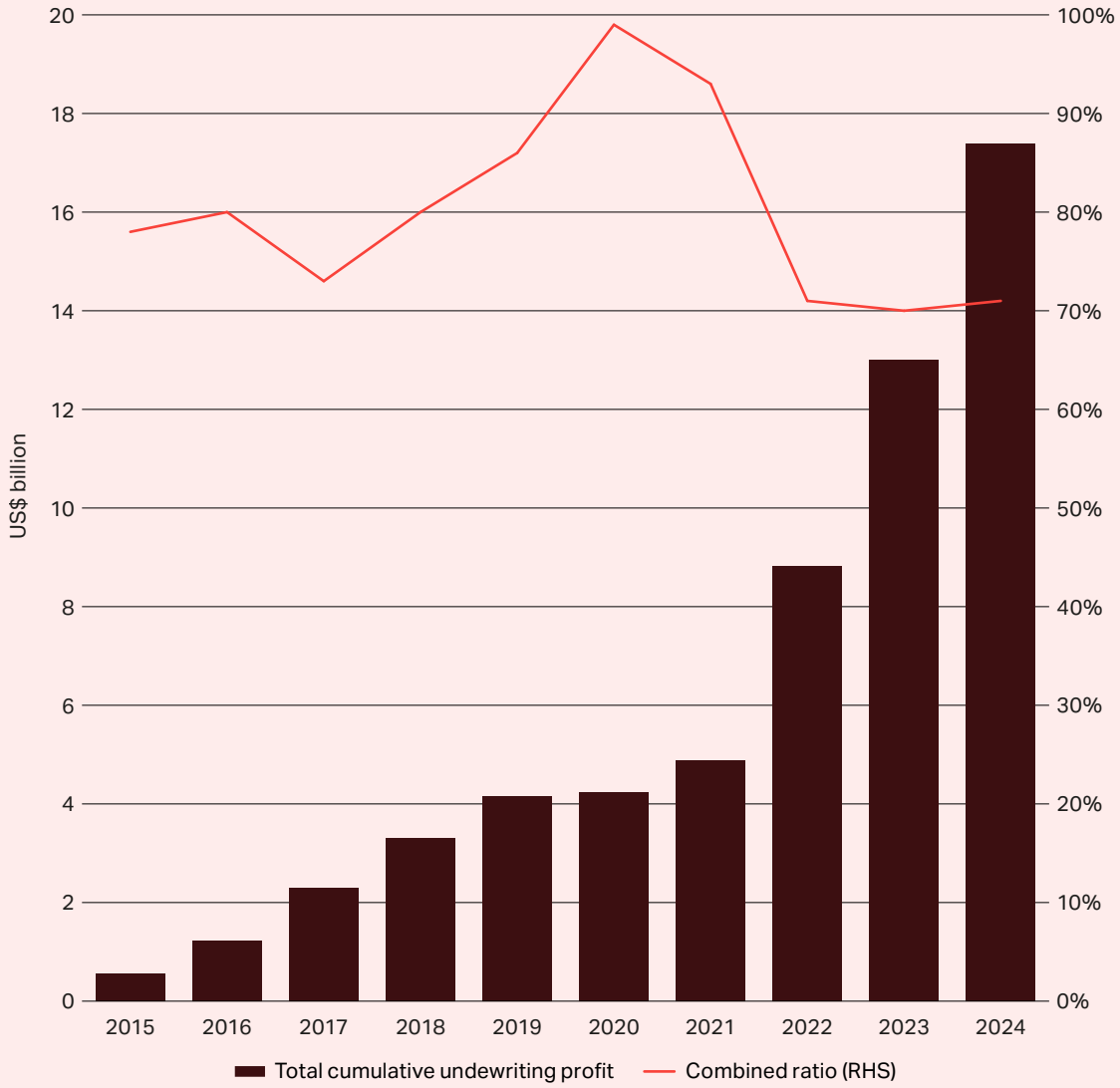


Note: RoW excludes Canada

Market maturity in pricing cyber risks, alongside ambitious growth targets for 2025/26, suggests a substantial earnings buffer is in place to absorb pressure from a softening rate cycle. Howden's analysis of underwriting performance supports this view, with Figure 8 charting cumulative profitability across the global cyber insurance market since 2015.

Following a period of positive but steady underwriting gains up to 2021, when profit increased at an annual average of US$0.7 billion, profitability has improved markedly in subsequent years. Between 2022 and 2024, higher rates and lower combined ratios applied to a significantly larger premium base saw average underwriting profits increase by US$4.3 billion per year, underscoring the market's ability to stay ahead of the fast-moving loss environment.

Figure 8: Cumulative underwriting profit for global cyber insurance market – 2015 to 2024[4]
(Source: Howden)



These supply-side developments have coincided with heightened awareness of cyber risk and increased uptake of protection, not only amongst new buyers (including an increasing number of companies looking to reinvest premium savings made in other areas as the wider P&C market softens) but also existing clients who are reassessing their coverage needs.

The sequence of losses in 2024 and high-profile attacks in 2025 have provided an additional wake-up call and prompted many businesses to re-evaluate the adequacy of their limits and the robustness of their incident response plans, all against a backdrop of an increasingly receptive market.

[4] Global market based on premium and loss ratio data from Howden and third parties, including NAIC, Lloyd's and Beazley.

03

Rebooting growth

Bringing everything together, current market conditions present a two-fold opportunity: for buyers, the chance to secure protection at favourable rates and terms; and for insurers, the ability to commit further to a class that offers considerable (exposure-led) growth potential and an impressive track record of profitability.

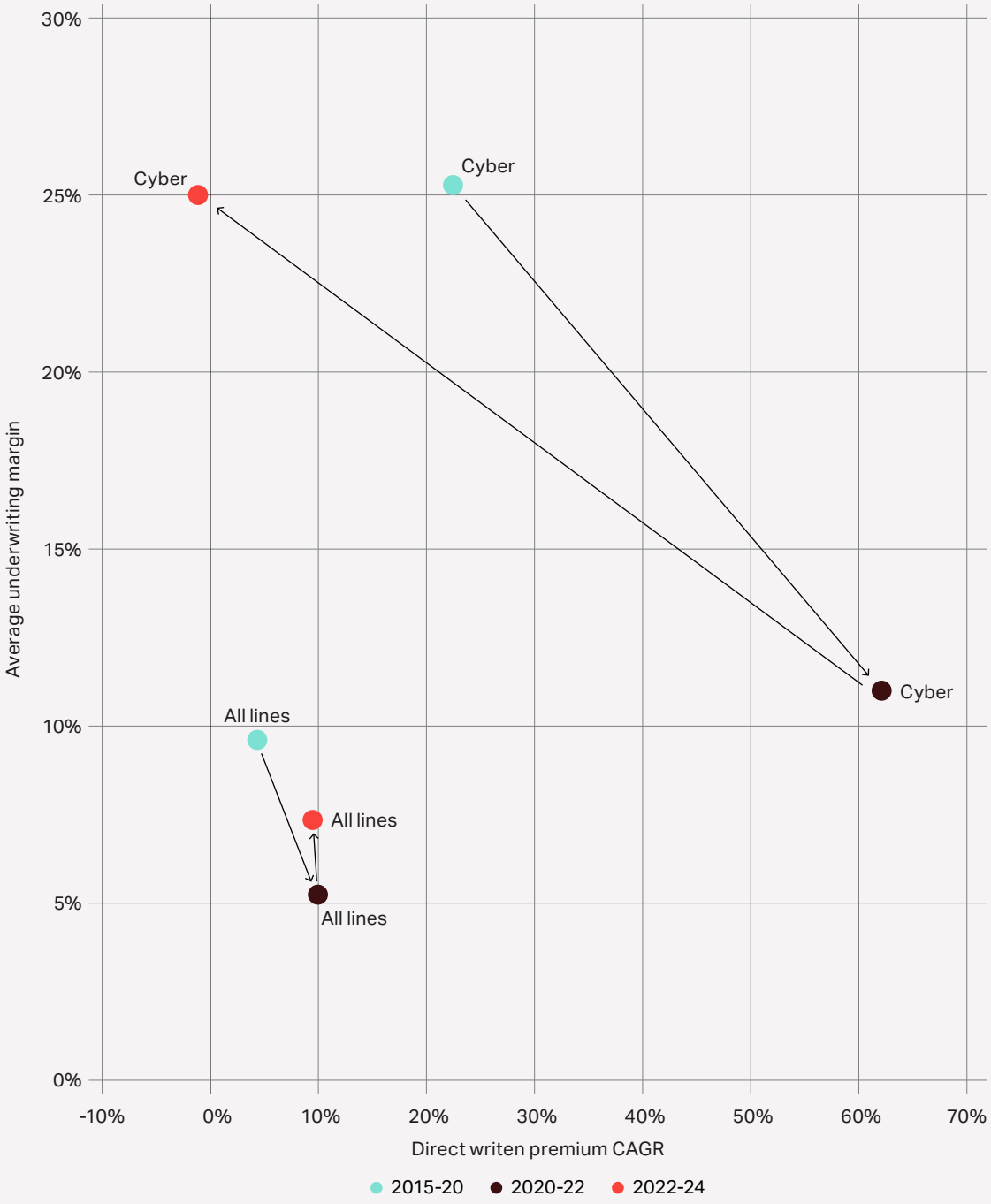
Figure 9 benchmarks growth and underwriting performance for US cyber insurers against the wider US P&C market over the last decade. By breaking down the analysis into three distinct phases, the results reinforce the degree of outperformance for cyber on both the expansion and underwriting fronts, but with growth stalling significantly in the post-hard market years of 2022-24.

Whilst this analysis is based on US-specific data (comparable quality / transparency for non-US cyber markets remains a work in progress), overriding trends apply internationally too, with premium in the French market, for example, contracting marginally in 2024 whilst posting a loss ratio of 17%.[5]

> “Current market conditions offer a favourable entry point for new buyers.

[5] Cyber premiums in France fell from €328 million in 2023 to €317 million in 2024, according to AMRAE.

Figure 9: Growth vs profitability for US cyber and broader P&C market – 2015 to 2024
(Source: Howden analysis based on NAIC data)

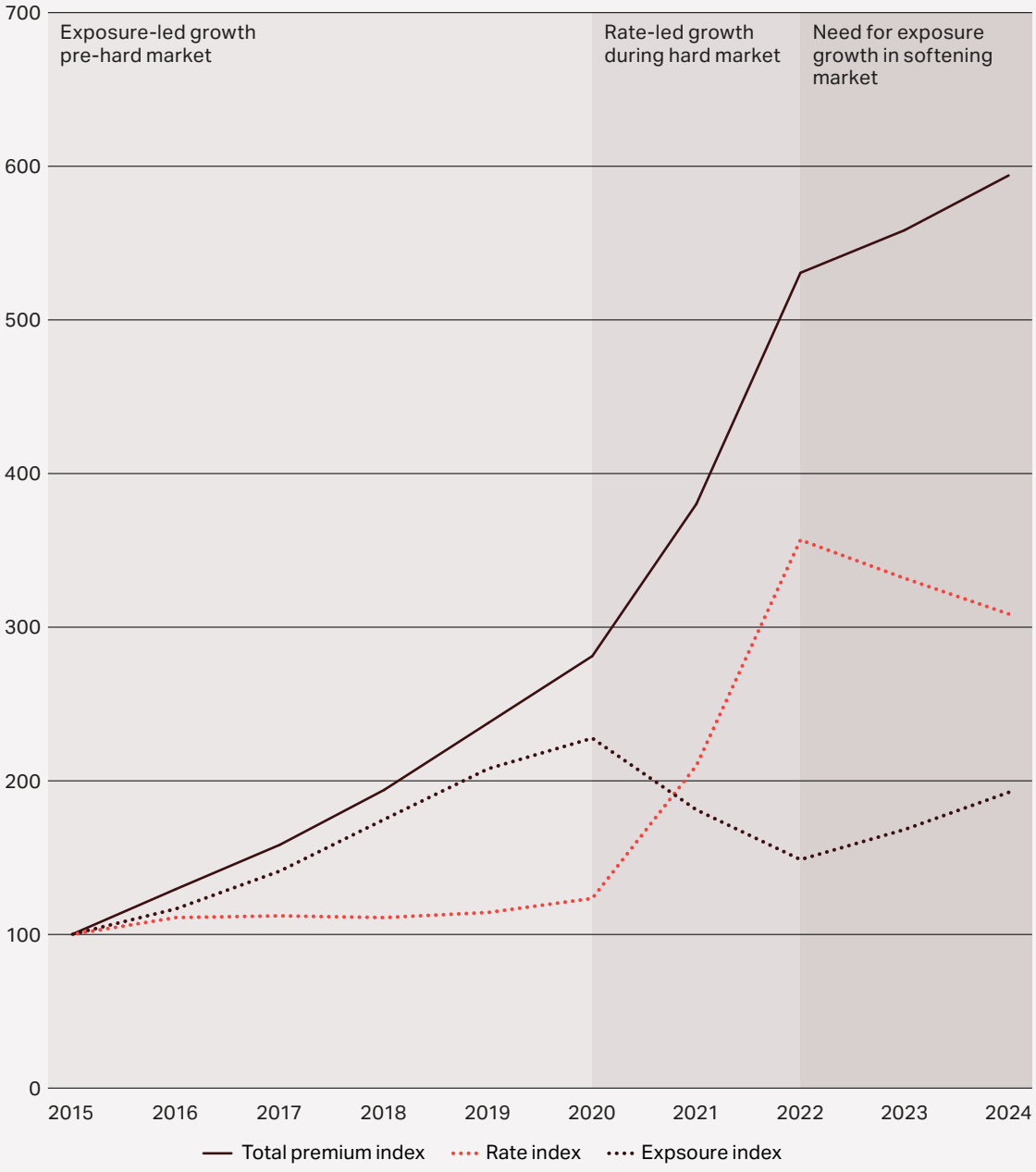


Note: underwriting margin = 100 minus average loss ratio and 30% for expense ratio
Analysis excludes alien E&S business

Figure 10 deepens the analysis by disaggregating the two primary drivers of premium: rate and exposure. Whilst growth was largely exposure-driven up to 2020, with pricing broadly stable, the rate environment precipitated a notable shift in 2021/22, when high double-digit annualised price increases more than offset underwriting actions and the resulting contraction in overall exposures.

Despite increasing in 2023/24, the market's exposure base remains below levels seen prior to the onset of the hard market, revealing considerable room for growth (and a key driver of market softening) in what is now a considerably more mature market.

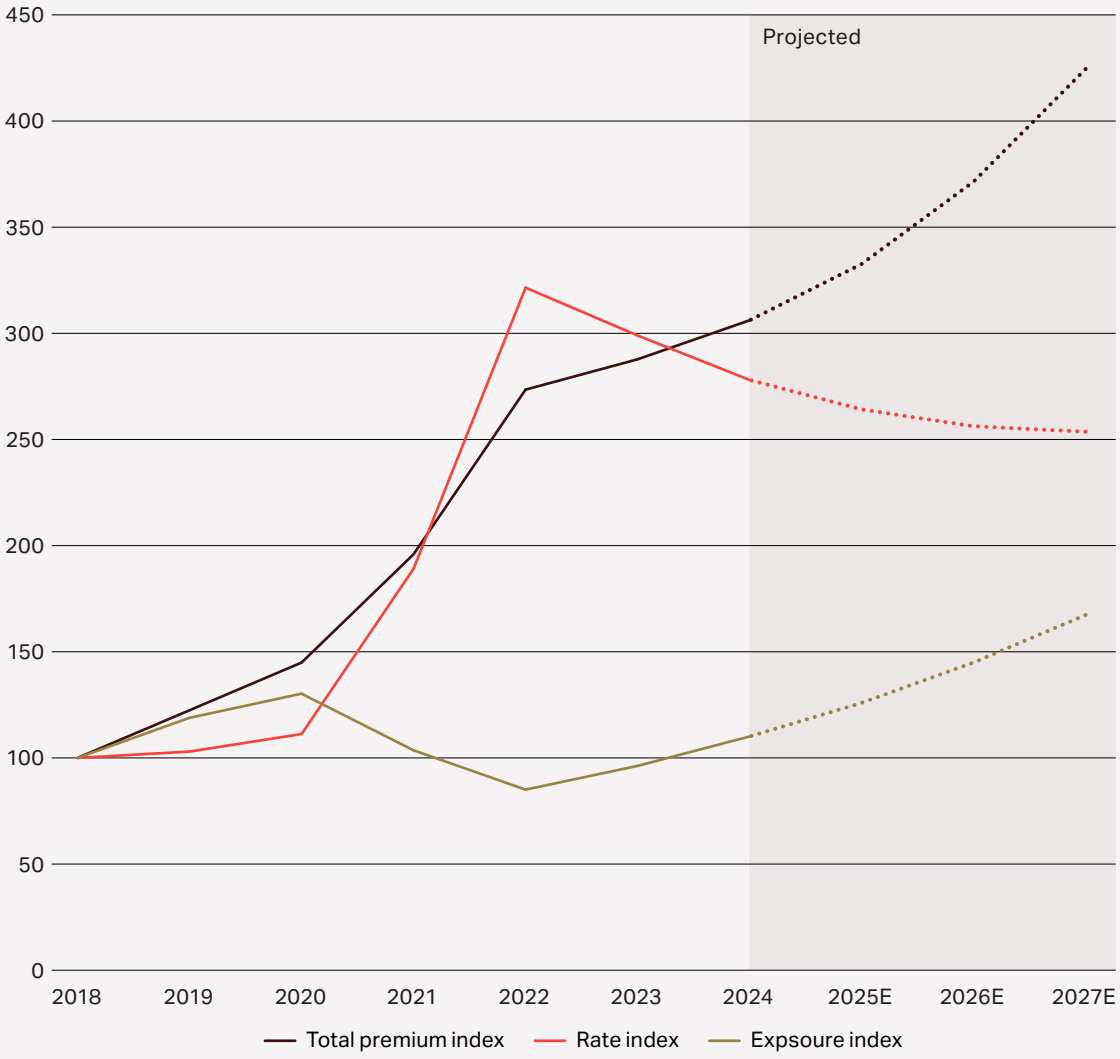
Figure 10: Premium growth of global cyber insurance market broken down by rate and exposure – 2015 to 2024 (Source: Howden)



This analysis encapsulates the crux of the challenge facing the cyber market over the coming years. Now that pricing tailwinds have reversed, unlocking new pools of risk, primarily by increasing penetration in underserved regions and company segments, is critical to accelerating growth.

Figure 11 illustrates the task ahead, based on the assumption of a stabilising rate environment over the next few years. To meet the (downwardly revised) market-wide premium target of close to US$20 billion by 2027, cyber insurers must embark on a new phase of disciplined growth that advances exposure expansion over the forecast period at a pace similar to the pre-hard market trajectory. There is ample reinsurance capacity, both traditional and alternative, available to support cedents in achieving this renewed growth cycle.

Figure 11: Projected premium growth of global cyber insurance market up to 2027
(Source: Howden, Munich Re, Swiss Re, Beazley)



Deepening cyber insurance penetration is critical to enhancing organisational resilience and securing long-term relevance for the market. With a stable and profitable foundation now firmly in place, the market is well-positioned to pivot again towards exposure-led growth.

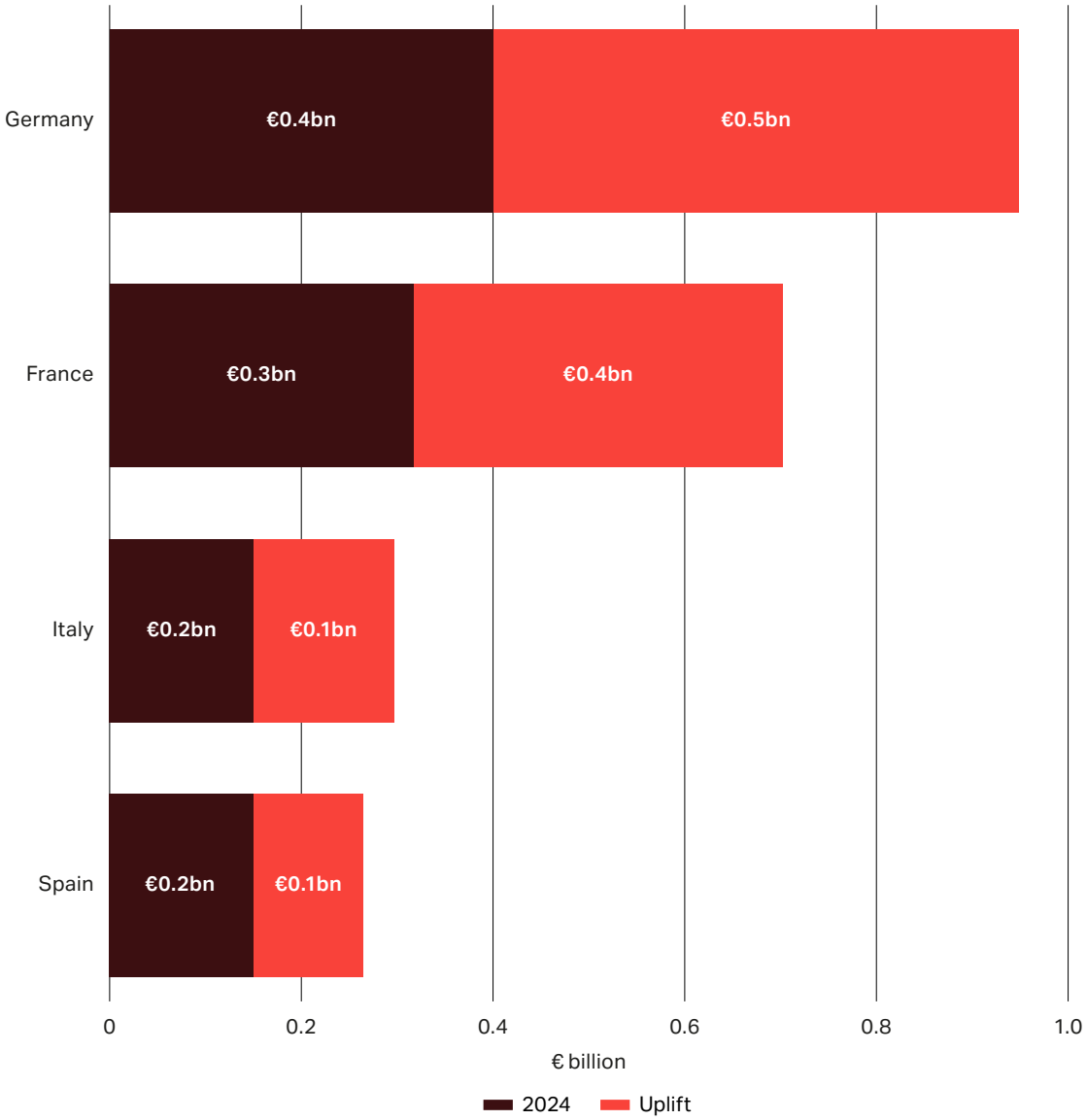
Europe: untapped potential

The opening of this report highlights the urgency of expanding the cyber premium pool in the current softening market cycle.

This section turns to the ‘how’ by exploring Europe’s standout growth potential and the approaches businesses in France, Germany, Italy and Spain are taking in terms of risk management and risk transfer to bolster cyber defences and mitigate losses.

Whilst the mature US market will continue to be a key driver of growth for cyber insurance, continental Europe's four largest P&C markets offer even greater upside potential given their lagging penetration rates. As shown in Figure 12, aligning with current US cyber penetration levels could unlock an estimated €1.2 billion of additional premiums across these markets.

Figure 12: Major European cyber insurance markets premium growth potential
(Source: Howden analysis based on data from SNL, Swiss Re, Lloyd's and AMRAE)



Note: uplift represents premiums at US level of penetration rate in terms of cyber / total non-life GWP
Total uplift of €1.2 billion is shown as €1.1 billion in the chart due to rounding

Unlocking the potential

Realising this potential hinges on understanding how European business leaders perceive cyber risk, the frequency and severity of attacks they face, the efficacy of risk management tools in mitigating impacts (insurance in particular) and the steps insurers and brokers must take to boost market penetration and close protection gaps.

To help answer these questions, Howden surveyed 1,200 senior IT decision-makers across a diverse range of private sector businesses in France, Germany, Italy and Spain. This builds on similar research Howden conducted in the UK, offering a valuable benchmark for comparison.[6]

The findings are encouraging for the cyber insurance market: business leaders recognise cyber as a leading (if not the leading) risk to their operations. They also confirm a strong link between cyber hygiene and reduced attack frequency and costs, which improves insurability and delivers significant economic benefits. With the vast majority of non-buyers open to purchasing cyber insurance, concerted efforts to communicate the value of the product will yield a surge in new demand.

[6] Howden, *The cyber security gap*, January 2025.

“

Our findings are encouraging for the cyber insurance market: business leaders recognise cyber as a leading risk to their operations.

01

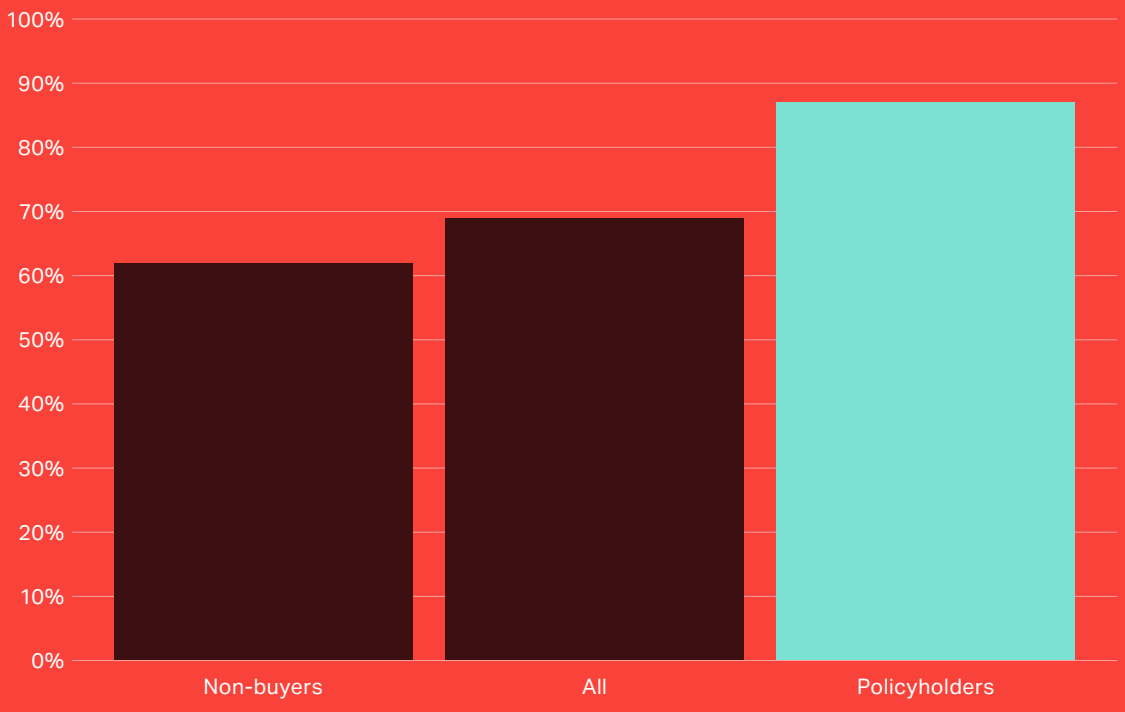
Threat landscape

In an environment defined by rapid and complex shifts in cyber threats, business leaders are acutely aware of the risks facing their organisations. Across all surveyed companies, 69% of respondents agreed that decision makers accurately assess cyber risk as a major threat.

Companies that adopt a strategic, as well as a technical, approach to cyber risk are more likely to benefit from stronger C-suite engagement and enhanced cross-functional resilience. Unsurprisingly, agreement was highest amongst companies that purchase cyber insurance, at nearly 90%, compared to approximately 60% for non-buyers (as shown by Figure 13).

This finding reflects what market practitioners often observe: businesses with a deeper understanding of cyber risk are more likely to purchase insurance protection than those with lower threat awareness.

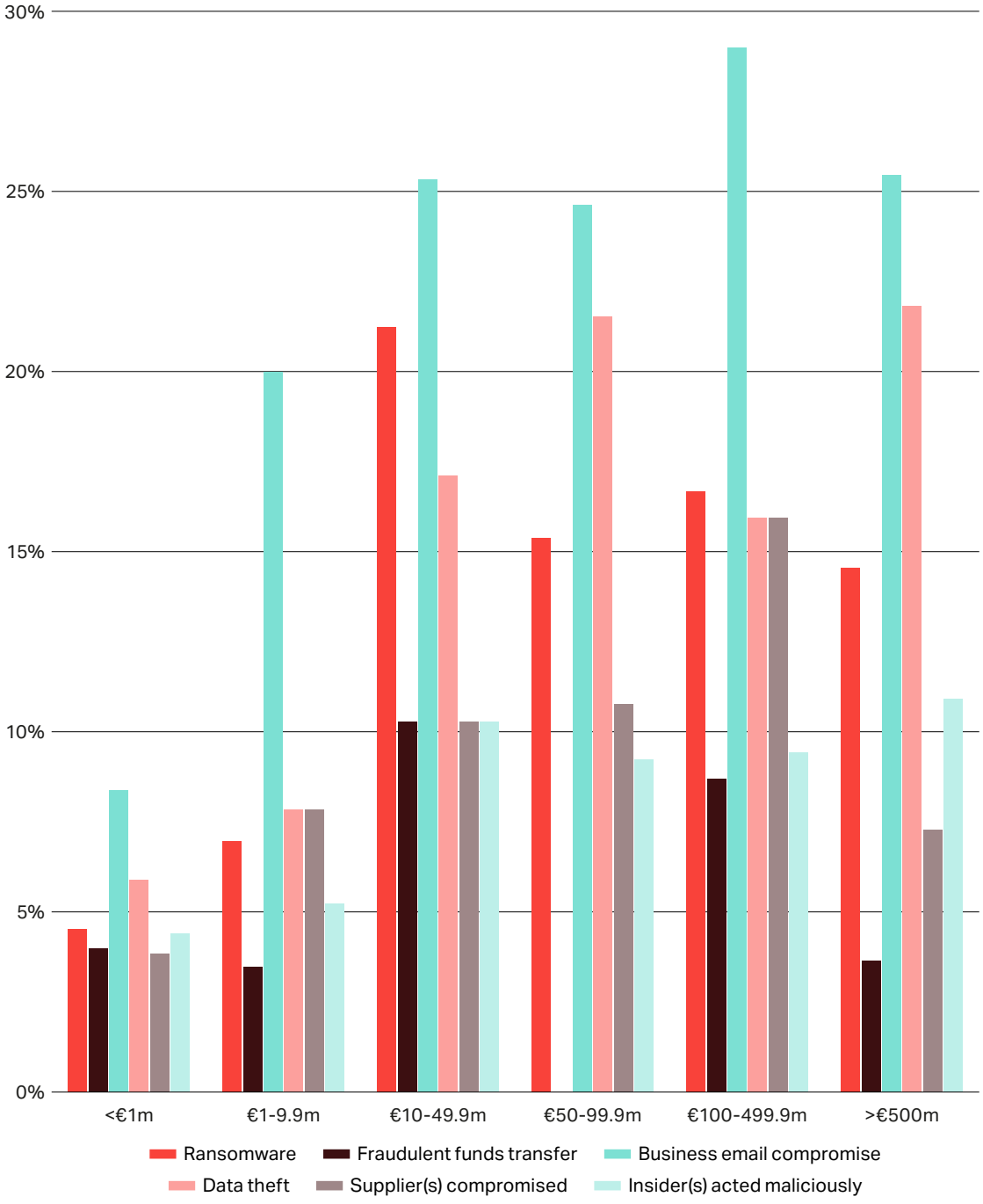
Figure 13: Agreement amongst respondents that their senior leadership understand and accurately assess cyber threats
(Source: Howden analysis based on survey data provided by YouGov)



Note: agreement level = sum of strongly agree and agree

Threat perception aligns with reality when analysing the frequency of attacks across company revenue bands. Put simply, many companies are being attacked across multiple vectors. Figure 14 shows that attack frequency generally increases with company size across all types of incidents. Business email compromise, data theft and ransomware are the most common forms of attack, consistent with findings from Howden's analysis of UK businesses conducted late last year.

Figure 14: Frequency of attacks by method and revenue band – 2020 to 2025
(Source: Howden analysis based on survey data provided by YouGov)



Forty-nine percent of surveyed companies reported experiencing at least one cyber attack between 2020 and 2025, closely aligning with the 50% figure from Howden's UK survey. When extrapolating frequency and severity trends across all private sector companies in France, Germany, Italy and Spain, the estimated economic impact reaches €307 billion in direct costs (e.g. excluding reputational damage) for the period of 2020-25, compared to £44 billion for the UK alone, highlighting the scale of financial exposure across Europe's four largest economies.

Figure 15: Estimated economic impact of cyber attacks in France, Germany, Italy and Spain – 2020 to 2025 (Source: Howden analysis based on survey data provided by YouGov)

Frequency		Severity		Revenue		Estimated cost
49%	×	2%	×	~€30tn	=	€307bn
Proportion of German, French, Italian and Spanish businesses attacked between 2020 and 2025		Average cost of most expensive attack as percentage of revenue		Estimated private sector revenue across France, Germany, Italy and Spain		

Note: frequency of attacks excludes 9% of respondents who did not know

“

Frequency and severity trends across all private sector companies in France, Germany, Italy and Spain show an estimated economic impact of €307 billion in lost revenue for the period of 2020-25, compared to £44bn for the UK alone.

02

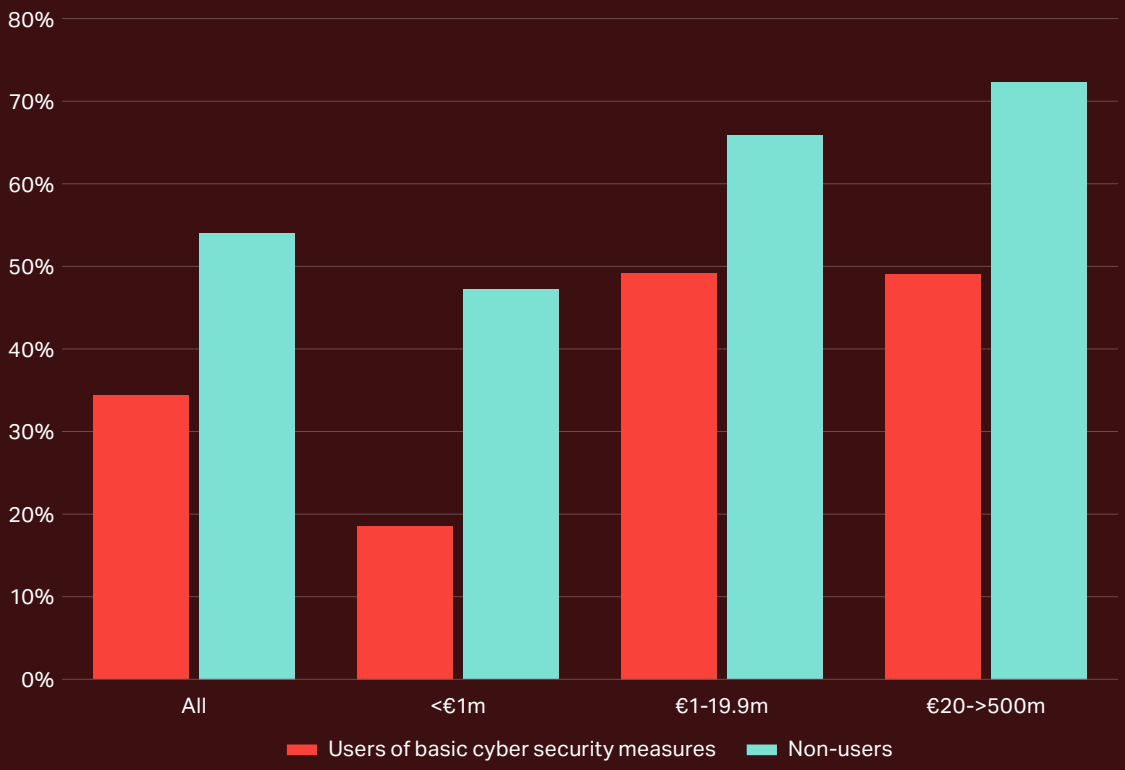
Risk management matters

Enhanced cyber resilience has led to a marked reduction in the financial impacts of attacks. Whilst market participants have long (anecdotally) cited a strong correlation between robust risk controls and fewer, less severe incidents, our survey provides empirical evidence to substantiate these claims.

The results underscore the critical role of cyber risk management in mitigating business disruption and enhancing firms' insurability. Insurance plays a key enabling role here by driving resilience through cyber hygiene requirements and, increasingly, premium incentives.

Figure 16 shows how basic cyber security measures reduce the frequency of attacks across different company revenue bands. Simple practices, such as regular software patching, strong passwords and email filtering, reduce frequency by more than one-third across all surveyed companies. The impact is particularly striking for firms with revenue under €1 million.

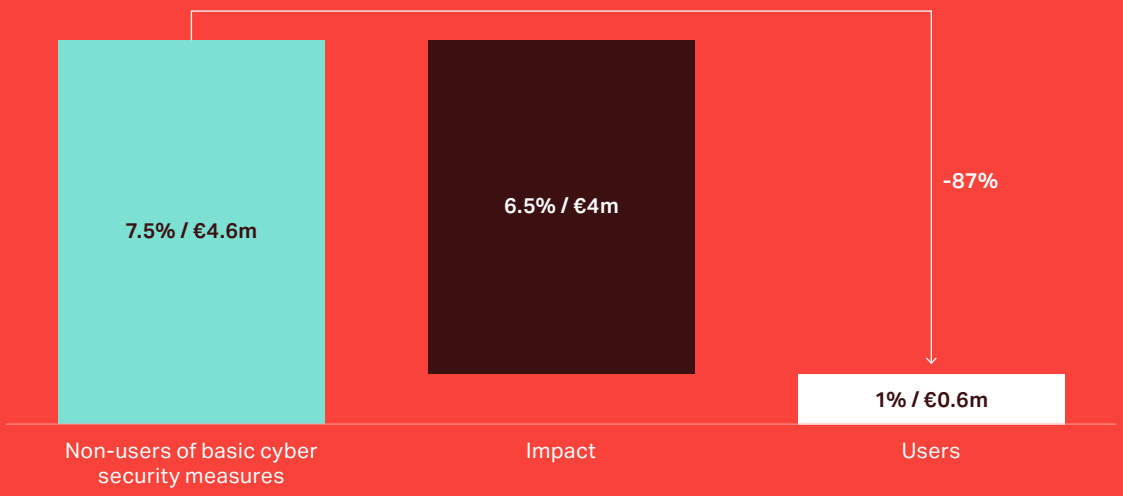
Figure 16: Impact of basic risk controls on the frequency of cyber attacks by revenue band – 2020 to 2025 (Source: Howden analysis based on survey data provided by YouGov)



Note: basics = regular software updates (patching), strong passwords and email filtering

The impact of good cyber hygiene is even more compelling from a severity perspective. Figure 17 shows that the average cost of a cyber attack is 87% lower for companies with average revenue (€62 million) that implement basic security measures, equating to a reduction of €4 million in the period of 2020-25 compared to those without such controls.

Figure 17: Average cost of cyber attack as a proportion of revenue and estimated value, users vs non-users of basic cyber security measures – 2020 to 2025
(Source: Howden analysis based on survey data provided by YouGov)



Note: basics = regular software updates (patching), strong passwords and email filtering

The substantial economic benefits of improved cyber resilience are illustrated in Figure 18. By extrapolating savings from reduced attack frequency and severity across France, Germany, Italy and Spain, total cyber-related costs across all four economies fall by 66%, a reduction of €204 billion over the period of 2020-25. The bulk of these savings emanate from reduced severity (€112 billion), with the remainder (€92 billion) attributed to lower frequency.

Despite these gains, significant residual exposure remains across all four economies, underscoring the importance of cyber insurance in the region. Whilst effective risk management can mitigate cyber risk, it cannot eliminate it entirely.

Figure 18: Economic benefits of implementing cyber security basics on business cyber attack costs – 2020 to 2025 (Source: Howden analysis based on survey data provided by YouGov)

03

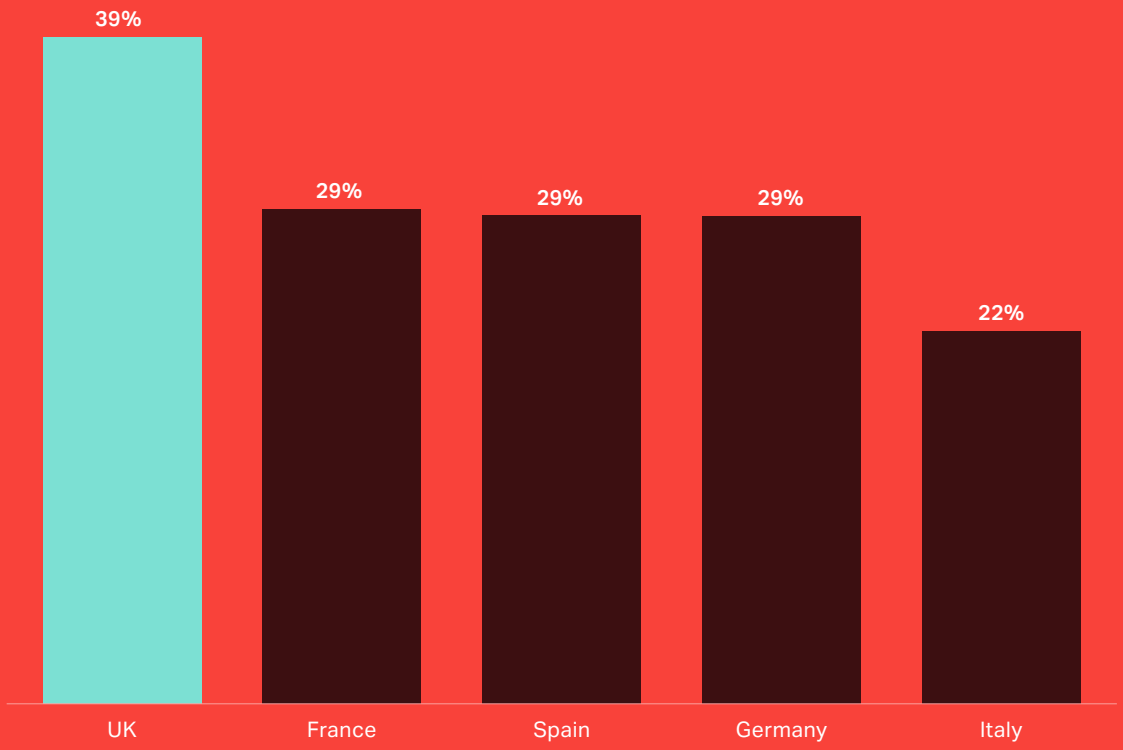
Cyber insurance

The significant (and quantifiable) value of cyber insurance stands out as the final key conclusion from our analysis. Beyond financial protection against the wide spectrum of cyber incidents facing businesses, it offers companies access to expert support – including incident response, legal counsel and PR guidance – and plays a critical role in fulfilling regulatory and compliance obligations.

Cyber insurance also drives better governance, which in turn enhances organisational resilience and, as our findings demonstrate, significantly reduces the scale of losses.

Given relatively low insurance penetration in France, Germany, Italy and Spain (less than 30% across all four countries and trailing significantly behind the UK's 39% – see Figure 19), cyber insurance presents an opportunity for both buyers and capacity providers.

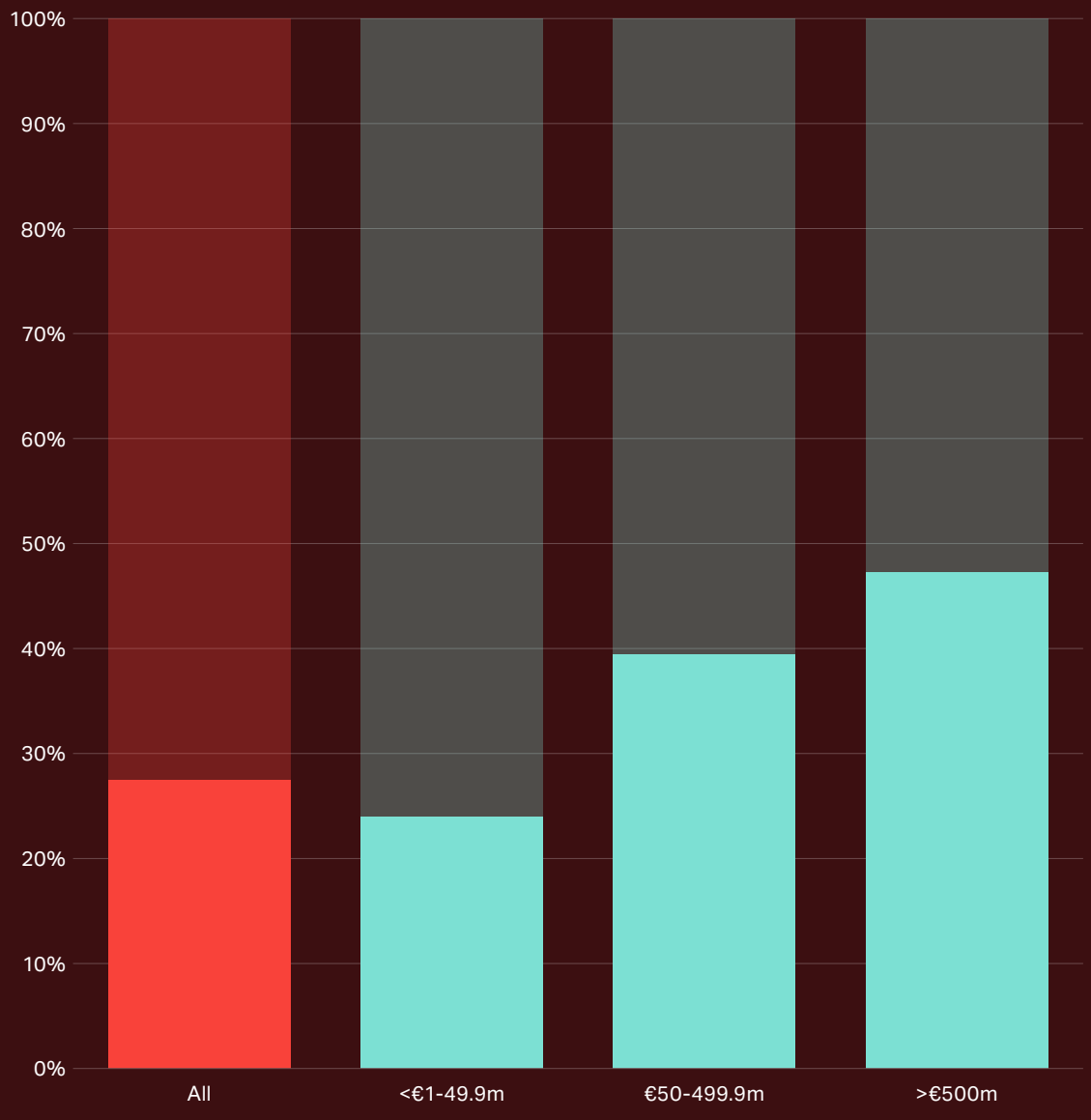
Figure 19: Cyber insurance penetration by country
(Howden analysis based on survey data provided by YouGov)



Note: UK data from Howden's *The cyber security gap* report in 2024

Figure 20 shows that cyber insurance uptake in Europe is highest amongst larger organisations, though even here there is considerable room for increased penetration. An even greater opportunity lies with mid-sized and smaller firms. SMEs in particular stand to benefit from on-demand embedded services, such as incident response, which offer a compelling value proposition for businesses that often lack the resources to hold these capabilities in-house.

Figure 20: Cyber insurance penetration by revenue band
(Source: Howden analysis based on survey data provided by YouGov)



Note: for France, Germany, Italy and Spain only (excludes the UK)

Figure 21 reinforces the role of cyber insurance as an enabler of good practice and strong governance, revealing a clear gap in attack response capabilities between buyers and non-buyers. Across every capability measured, insured organisations report greater access to these critical services than their uninsured peers, a disparity that is especially pronounced amongst lower-revenue companies.

Figure 22 shows that 36% of policyholders with revenue under €1 million report having access to incident response expertise, a critical resource for containing attacks amongst SMEs, compared to just 14% of non-buyers. In reality, the gap is even wider, with many of these capabilities embedded as standard in standalone cyber policies.

Figure 21: Cyber attack response capabilities, insured firms vs uninsured peers (Source: Howden analysis based on survey data provided by YouGov)

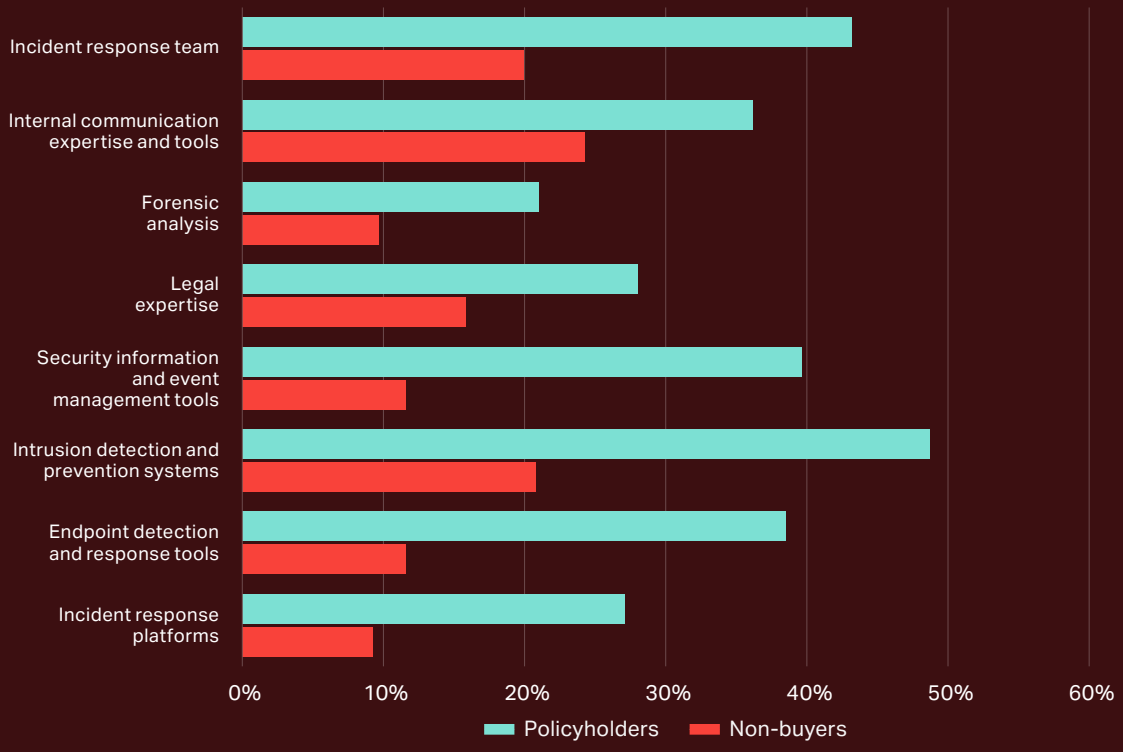


Figure 22: Firms with access to incident response capabilities by revenue band and cyber insurance holding (Source: Howden analysis based on survey data provided by YouGov)

Cyber insurance also proves its value in containing the financial impact of cyber attacks, even before factoring in claims recoveries. Our analysis shows that insured companies experience lower costs following an attack, a result of risk management best practice and strong governance.

For a company with €500 million in annual revenue, holding a cyber insurance policy translates into €16 million in savings over ten years, as illustrated by Figure 23. This equates to a 19% return on investment, driven by reduced attack severity (which more than offsets the costs of purchasing cover). Claims payments in the event of a loss further enhance returns.

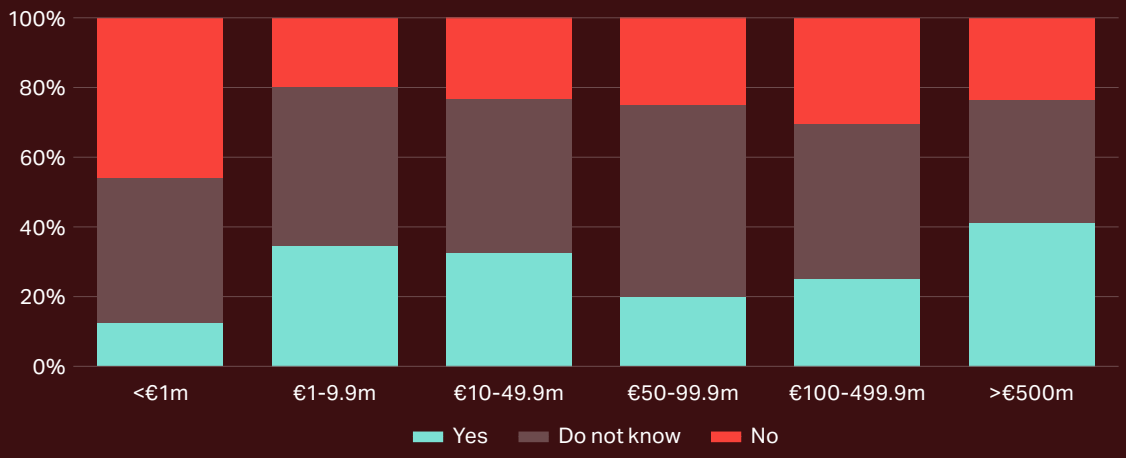
Figure 23: Estimated total cyber costs over a ten-year period for cyber insurance policyholders vs non-buyers with €500 million revenue
(Source: Howden analysis based on survey data provided by YouGov)

Note: risk management spend includes insurance premium for policyholders

All of which reinforces the strategic value of cyber insurance and the significant growth potential in Europe. Figure 24 illustrates strong latent demand across all company revenue bands, with the market effectively pushing against an open door as many current non-buyers confirmed they intend to purchase cyber insurance within the next five years.

This represents substantial new business that the market is well placed to absorb. The opportunity could be even greater, given the high proportion of non-buyers that are currently undecided about purchasing cyber insurance. To realise growth projections outlined earlier in the report, brokers and carriers must actively engage and persuade this firmographic. Amongst companies with revenues of €500 million and above, only 24% say they do not intend to purchase cover.

Figure 24: Future cyber insurance purchase intentions for respondents that do not currently buy by revenue band (Source: Howden analysis based on survey data provided by YouGov)

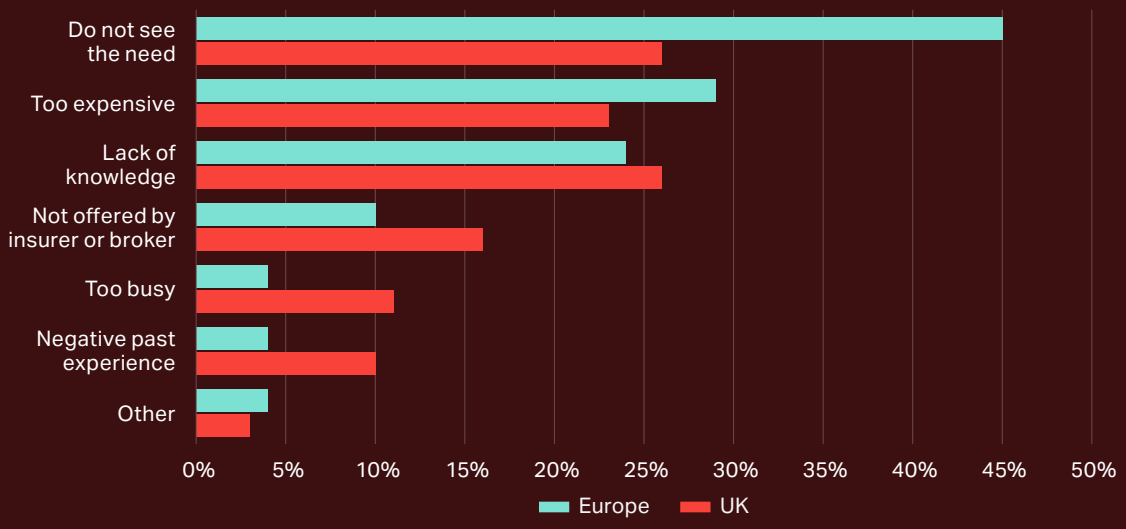


Note: purchase within the next five years

The barriers to unlocking this demand are outlined in Figure 25, alongside those identified in our UK survey. To fully realise the opportunity in Europe, and other underpenetrated international markets, the industry must do more to communicate the value of coverage, particularly given that protection can be self-financing in terms of saved attack costs, as demonstrated by Figure 23.

The fact that 45% of companies in Europe do not see the need for cyber insurance is a clear call to action. A similar outcome emerged in our UK analysis, where one in four companies expressed the same view, albeit in smaller numbers due to higher market penetration. Perceptions of high cost are being addressed by low double-digit rate reductions in most international regions.

Figure 25: Barriers to future cyber insurance purchase
(Source: Howden analysis based on survey data provided by YouGov)



Note: UK data from Howden's *The cyber security gap* report in 2024

Our analysis confirms the powerful role cyber insurance plays in mitigating one of the most critical threats facing businesses today.

Cyber insurance is not just a protective measure, but a strategic enabler of resilience that accelerates recovery, strengthens risk management and reduces financial losses.

With penetration still low and demand rising, Europe and other international markets offer significant growth opportunities. Yet, the market must do more to communicate this value and simplify its offering. Progress is now being made: since launching Cyber+ last year, we have achieved growth three times higher than the broader market – principally by improving access to cover for smaller companies and transforming the buying journey.

This is about more than insurance. Our research quantified the costs of European attacks at roughly €300 billion since the turn of the decade; the cyber protection gap is a societal issue that demands urgent attention.

Howden is committed to working with clients and markets to build lasting resilience.

Jean Bayon de La Tour
Head of Cyber, International

Meet the experts

“

Meeting clients’ needs requires deep sector knowledge, strong partnerships with third party experts and unrivalled relationships with (re)insurers and other capital providers. Howden’s cyber team provides all this and more.
Come and talk to us.

Authors

Julian Alovisi
Head of Research

julian.alovisi@howdengroup.com

Peter Evans
Research Director

peter.evans@howdengroup.com

Contacts

Adam Codrington
Global Head of Cyber

adam.codrington@howdengroup.com

Shay Simkin
Chair, Global Cyber

shay@howden.co.il

Jean Bayon de La Tour
Head of Cyber, International

jean.bayon@howdengroup.com

Manuel Pérez
Head of Cyber, Southern Europe and LatAm

manuel.perez@howdengroup.com

David Rees
Head of Cyber, UK

david.rees@howdengroup.com

Sarah Neild
Head of Cyber Retail, UK

sarah.neild@howdengroup.com

Contact us at info@howdenbroking.com
or call us on +44 (0)20 7623 3806.

One Creechurch Place, London EC3A 5AF

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

howdenbroking.com

Howden Group Holdings Limited is registered in England and Wales under company registration number 2937398. Registered office:
One Creechurch Place, London, EC3A 5AF. Calls may be monitored and recorded for quality assurance purposes. 09/25 13292