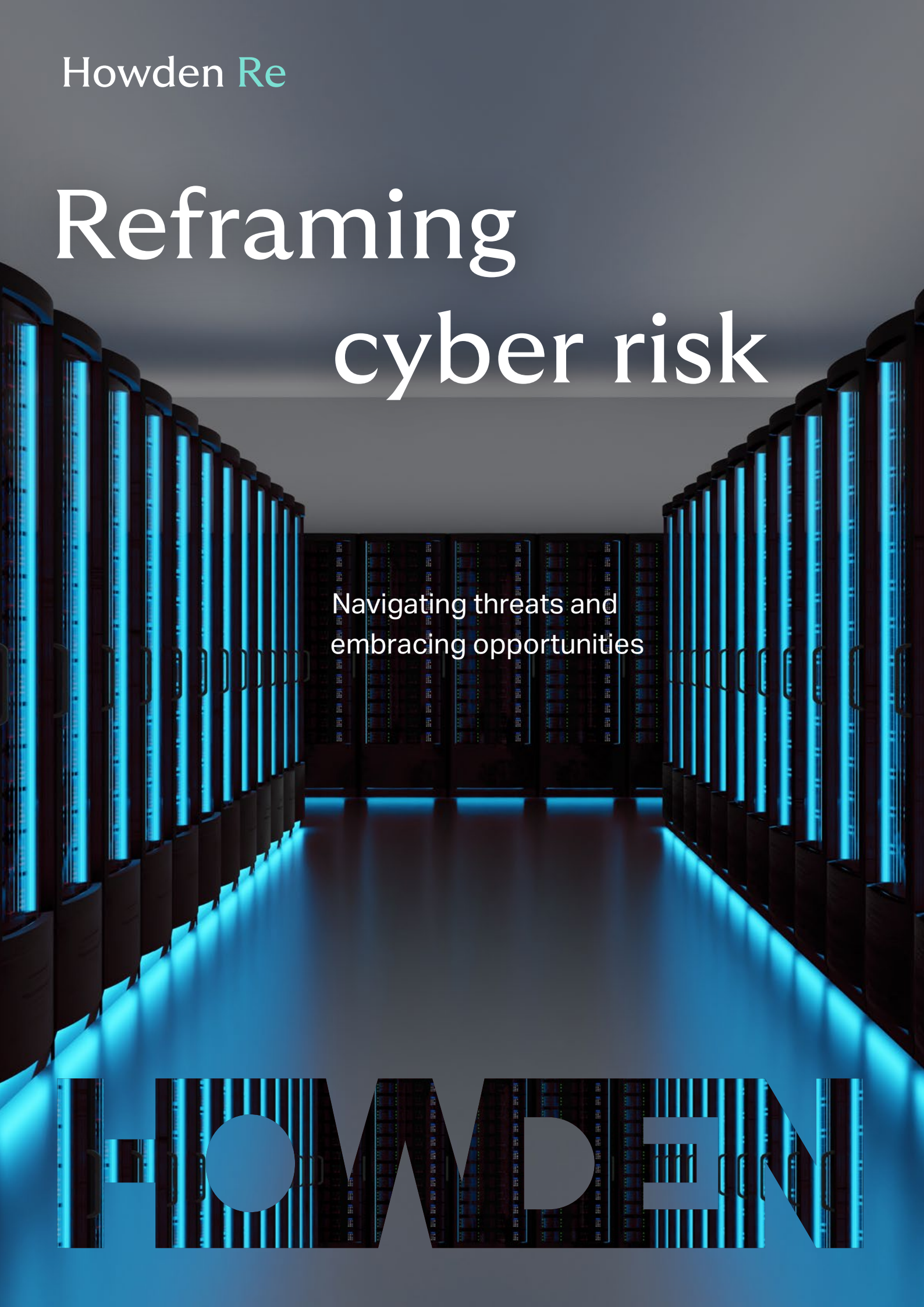
Howden Re

Reframing cyber risk

Navigating threats and embracing opportunities



01

Executive summary

The perception of cyber threats has significantly amplified in today's dynamic global risk landscape, at times painting a picture of imminent digital disaster.

This narrative, while captivating, overshadows an important reality: **the cyber (re)insurance market is not just a story of risk but a realm of untapped potential.**

This report navigates through the intricacies of cyber risk, juxtaposing it against traditional natural catastrophe (nat-cat) risks, unveiling a compelling case for the cyber (re)insurance opportunity.

Perception versus reality

The discourse around cyber threats often veers towards the catastrophic, drawing parallels with the most devastating natural disasters. However, the actual data and trends within the cyber (re)insurance landscape, to date, paint a markedly different picture. The frequency and impact of cyber events, while not negligible, are constrained by numerous factors, including the logistical complexity of orchestrating widespread cyber attacks, advancements in cybersecurity, the intrinsic motivations of threat actors, and the diversified uptake of, and reliance on, different technologies by different profiles of insureds.

A critical insight from our analysis is the comparative hesitancy of cedents to underwrite cyber risk versus traditional nat-cat risks. This is despite evidence suggesting that the utilisation of cyber reinsurance offers a favourable risk-return profile. Our findings highlight a persistent underestimation of the cyber opportunity, with larger carriers assuming comparatively greater exposure to nat-cat risks. This relatively conservative stance towards cyber risk is belied by a backdrop of historical data (despite its short history), which suggest that premiums have, in most years, outpaced losses in the cyber domain unlike in several high-profile nat-cat underwriting years.

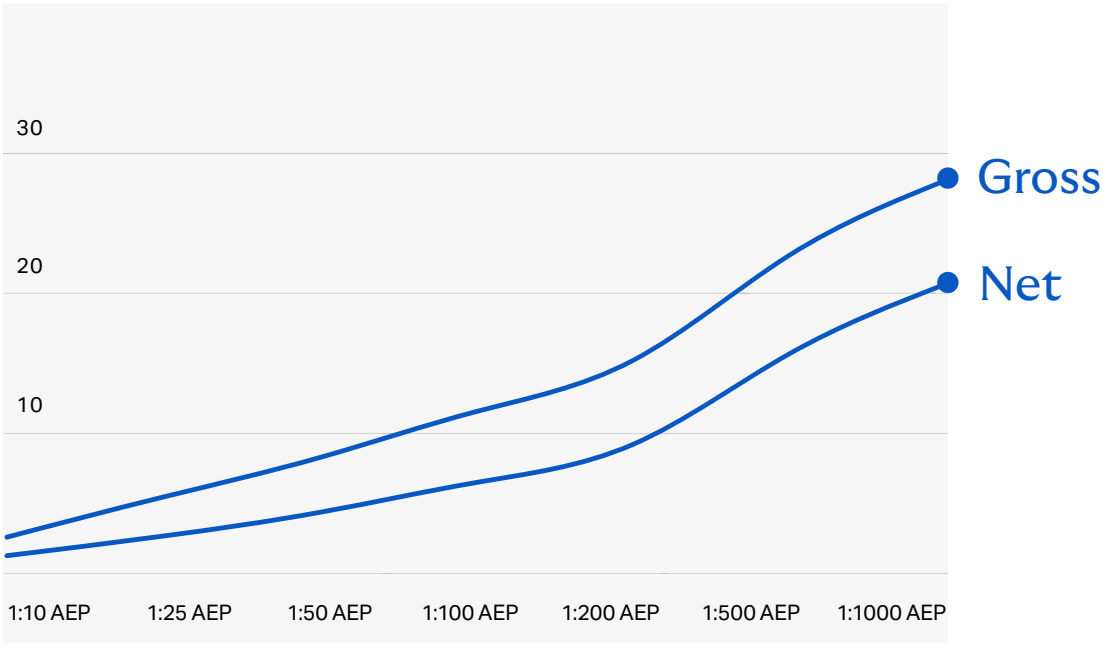
From perception to potential

The report advocates for a recalibration of the risk appetite within the (re)insurance industry, urging a shift towards a more balanced and informed approach to cyber risk underwriting. This recalibration is not merely a strategic adjustment but a necessary evolution to capitalise fully on the cyber (re)insurance opportunity.

The most advanced carriers are embracing refined risk models to navigate the nuances of cyber threats more effectively, transforming perceived vulnerabilities into competitive advantages.

Reinsurance purchasing: a diverse landscape

Average variation by return period



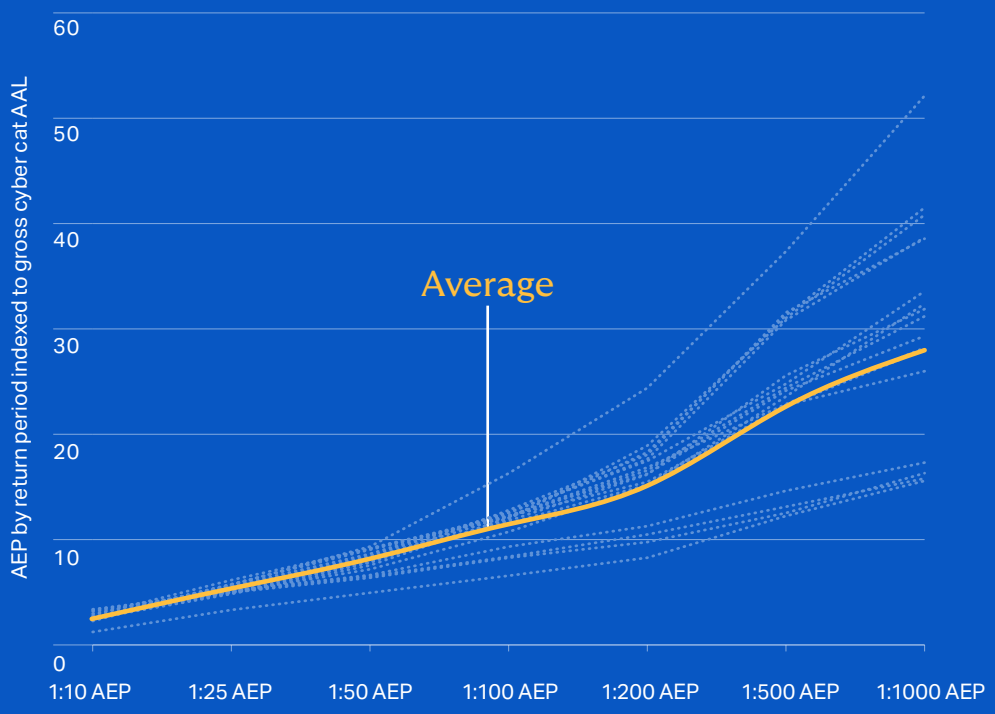
Analysis of sixteen carriers reveals marked variability in underwriting strategies, as evidenced by gross loss distributions that mirror the diversity of underlying portfolios, demonstrating that portfolio composition significantly influences tail-end loss experiences. SME-focused portfolios, displaying large modelled Aggregate Annual Losses (AALs), tend to exhibit a flatter loss curve, suggesting a broad risk spread. In contrast, portfolios in the median range, typified by their diversification, adhere more closely to industry averages.

Meanwhile, entities with a substantial share of high excess policies are susceptible to rare, but severe events, creating a stark distinction between average loss and cat risk. Additionally, the variation in net results underscores differing carrier appetites, informing distinct reinsurance buying behaviours. For the industry to grow profitably within the cyber domain, it is important that cedents optimally employ reinsurance as a mitigation tool.

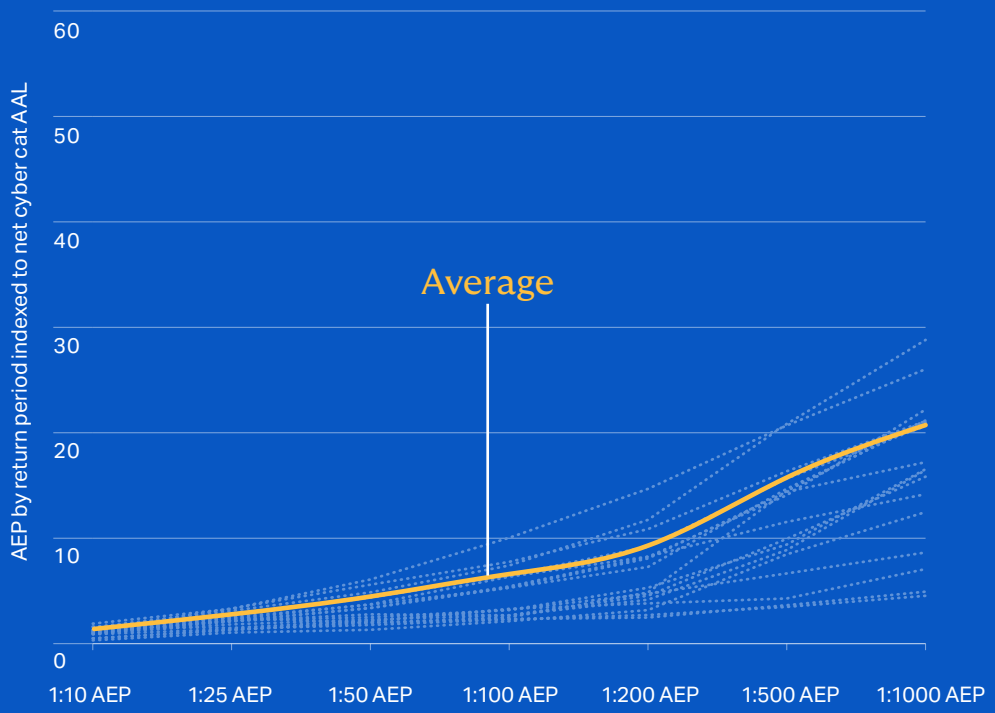
Figure 1:
Source:
Howden Re

Analysis of sixteen cyber carriers' gross and net variation by return period

Gross

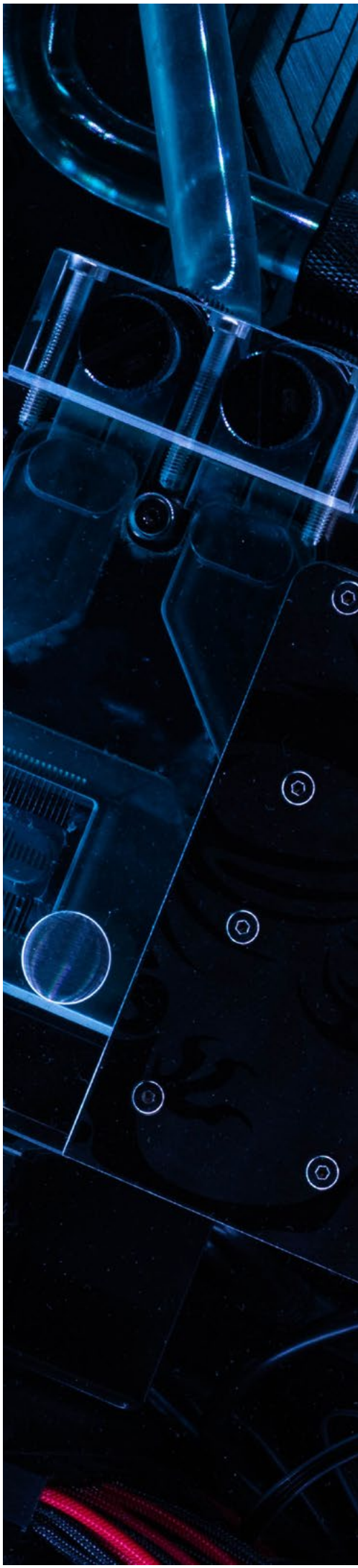


Net



Strategic imperatives to counterbalance cyber model variation

The path towards a sophisticated view of risk involves a strategic blend of enhanced risk modelling, deploying portfolio monitoring tools, and cultivating cyber-specific expertise. Carriers that do not already follow this approach are encouraged to leverage advanced analytics and probabilistic modelling to quantify exposure more accurately and tailor their offerings to meet the nuanced demands of the cyber market. Acknowledging that cyber models are still evolving, and each release can vary by 20-30%, adopting a blended approach of different models and/or proprietary scenarios may mitigate some of these challenges and provide a more comprehensive assessment of cyber risk, enabling carriers to grow their cyber exposure more effectively.




START

02

Fine tuning tolerance

An important challenge in setting cyber risk tolerances is the threat of cyber catastrophes (cats) generating losses which outpace reinsurance protections and capital reserves.

This fear is particularly acute in cyber underwriting as, globally, losses of the magnitude of Hurricane Katrina or 11 September 2001 have yet to occur in the cyber world. By contrast, in the associated classes of wind, quake and terrorism (re)insurance, historical, outlier events have provided the contours of a 'worst-case' scenario, lending important experience 'in the tail' and allowing carriers to price accordingly. In addition, unlike natural catastrophes, cyber cats are perceived to be shrouded in mystery; there is limited historical loss experience; and there is a lack of diversification in the extreme tail, which – on the face of it – makes them more difficult to understand and quantify.

The impact of future cyber catastrophes emanating from heightened systemic risk has been a key concern for underwriters in the burgeoning cyber (re)insurance market since the first coverages appeared over two decades ago. Theoretically, cyber cats encompass the potential for a single, massive, co-ordinated cyber attack, cluster of large attacks, or mass cloud outage to generate insured losses across many policies simultaneously. Systemic risks pose major accumulation and solvency threats that have the potential to surpass attritional cyber loss levels.

2.1

Challenges in executing systemic cyber attacks

While systemic attacks are rightly a key industry concern, in practice, scenarios are tempered. Unlike a naturally occurring earthquake or hurricane, for example, a large-scale cyber attack poses a significant logistical burden on the hacker.[1] At the same time, cyber security awareness and technologies are rapidly advancing to detect threats and prevent breaches.

Two key factors impact this logistical burden: (1) the complex technical skills and substantial resources required to execute an attack, and (2) the limited motivation for threat actors to carry them out.[2] A large proportion of the attacks that dominate the extreme tail of the vendor models (such as mass ransomware, cloud outage, or attacks on critical national infrastructure) are highly complex and would be beyond the technical and financial resources of most criminal gangs, likely limiting them to the sphere of state actors. Further, this should be understood in the context of a cyber (re)insurance market that excludes critical infrastructure and cyber nation-state warfare from policies, reducing the overall threat of systemic risk.

Similarly, the pool of potential actors capable of executing complex attacks is limited to nation states and sophisticated criminal groups. However, criminal gangs often avoid attacks that draw political attention, as demonstrated by the fallout following the Colonial Pipeline incident in 2021 and the recent takedowns of the two most dominant ransomware gangs of the 2020s, Conti and Lockbit. Systemic attacks are then more technically difficult to pull off, not to mention less attractive, as threat actors stand to make more money from individual, more-frequent ransomware attacks.

While nation states like North Korea, Russia and China have conducted large attacks such as WannaCry (North Korea), NotPetya (Russia) and other attacks from China's active cyber warfare functionality within the People's Liberation Army (such as PLA Unit 61486)[3], there are limitations to their actions outside of traditional nation-state conflicts. The lack of numerous Russian cyber attacks in the first two years of the Ukraine conflict, for example, underscores that – even during diplomatic crises – large-scale attacks are not inevitable.

Finally, technological advancements may enable threat actors to launch more sophisticated attacks, but they also help businesses strengthen cybersecurity systems. The greater the number of attacks, the more organisations sharpen their focus on cybersecurity. In 2017, global cybersecurity spending totalled ca. USD 101 billion. In 2024, that number is expected to reach USD 215 billion, a 14.3% increase on 2023 and an 11% compound annual growth rate from 2017.[4]

1 Kelly, S., E. Leverett, E. J. Oughton, J. Copic, S. Thacker, R. Pant, L. Pryor, et al. 'Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy.' Cambridge Centre for Risk Studies, University of Cambridge, January 2016.

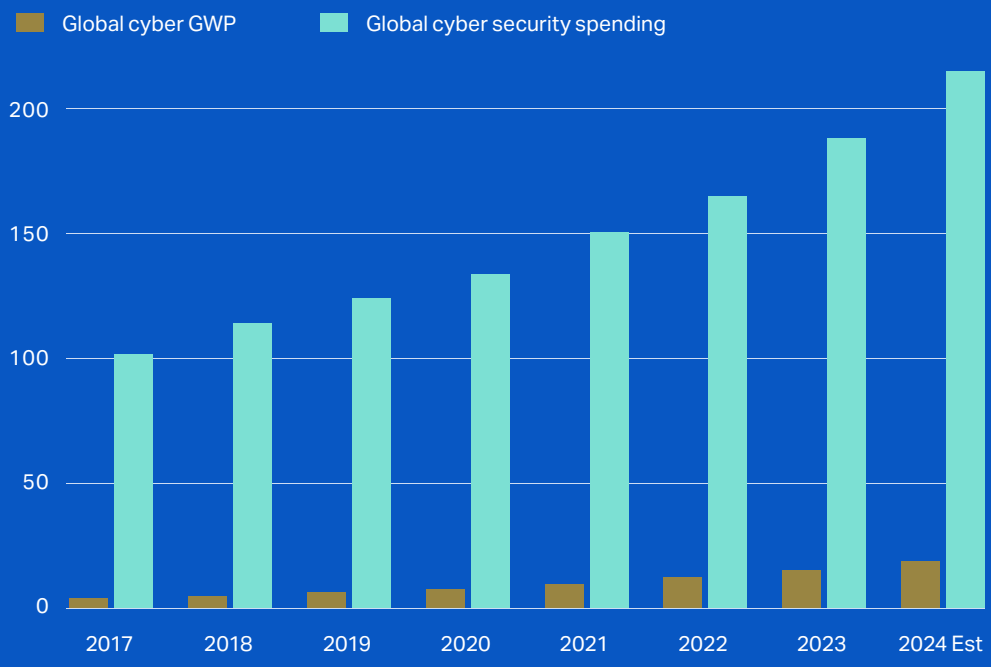
2 Guiliano, Craig. 'Has Ransomware Reached an Inflection Point?' LinkedIn, May 24, 2021.

3 Gaywood, Harriet. 'From Nuclear to Cyber: Evolution of the People's War in China.' (2022).

4 Gartner. 'Gartner Forecasts Global Security and Risk Management Spending to Grow 14 Percent in 2024.' Press release, September 28, 2023.

Figure 2
Source: Howden Re, Gartner

Global spending on cyber security vs. global cyber GWP 2017- 2024 Est
(USD billions)



While it is natural to fear a 'cybergeddon' event, the logistical burden on the threat actor is extensive. Those with the necessary resources, technical ability, and incentive to carry out a catastrophic cyber event would realistically require state sponsorship. However, as state-sponsored attacks are widely omitted by cyber warfare policy exclusions, their impact on the (re)insurance industry is subsequently diminished.

At the same time, rapid investment in cybersecurity infrastructure highlights the active protection measures in place to prevent systemic attacks. Governments, organisations and cybersecurity experts continuously work with increasingly advanced technologies to identify and patch vulnerabilities, monitor suspicious activities, and improve defensive strategies.

Therefore, the complexity of executing a successful large-scale cyber attack, combined with the limited pool of capable threat actors, significantly reduces the likelihood of a cybergeddon event.

This thesis is supported when examining previous cyber catastrophes side-by-side with catastrophes in other classes. As figures 3 and 4 show, cyber catastrophes have historically had a much less significant economic and market impact.

2.2 Beware of cats and kittens

When compared with nat-cat losses, for example, (re)insurers have been relatively well insulated from large cyber losses. Between 2017 and 2022, nat-cat premiums exceeded losses in just two of the six costliest nat-cat events, while premiums exceeded losses in every high-profile cyber event over the same period.

So far, the cyber risk landscape has been characterised by more contained events – systemic vulnerabilities with catastrophic loss potential – rather than cyber catastrophes with multiple impacts across the value chain. These so-called 'cyber kittens' significantly affect specific business segments but have a limited effect on the market overall. A cyber kitten, therefore, can be understood as a digital hurricane that makes landfall as a tropical storm but does not cause widespread damage. To further illustrate this point, a study conducted by Kovrr, as illustrated in Howden's A Hard Reset,[5] reveals that the Solar Winds 'systemic' cyber attack impacted a much smaller portion of the market than one might expect from a cyber catastrophe.

Figure 3
Source: Howden Re, PCS, Cresta

Insured loss estimates for high profile cyber events vs global cyber GWP 2017-2022 (USD billions)

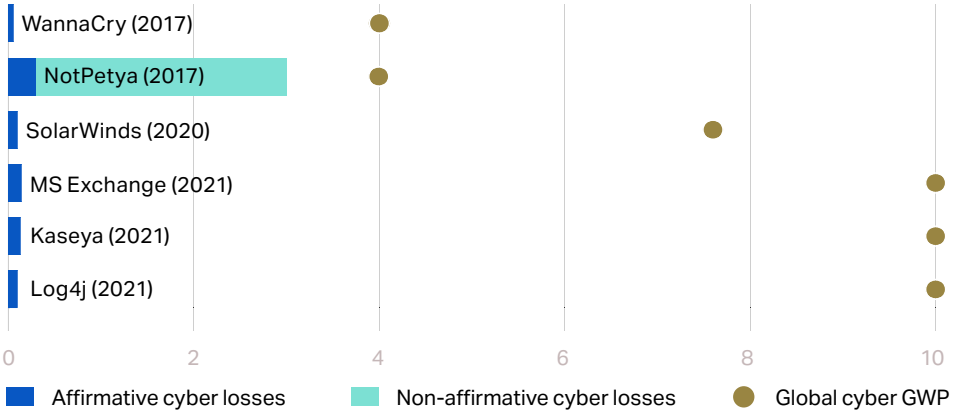
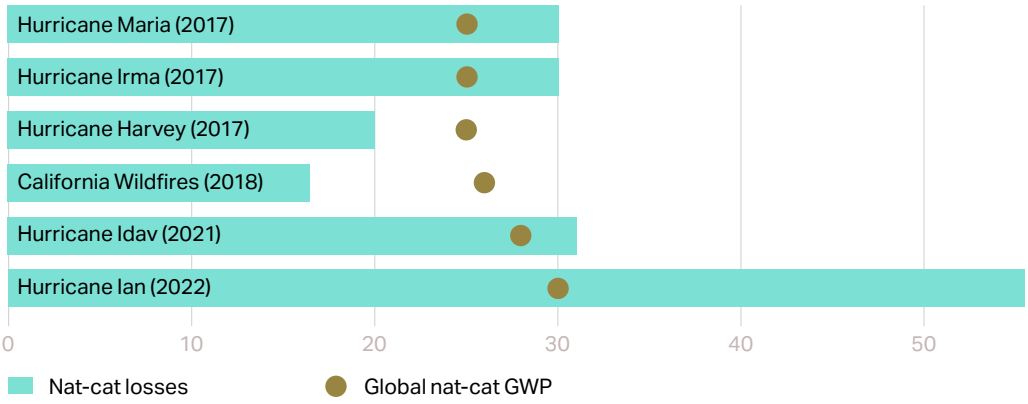


Figure 4
Source: Howden Re, PCS, Cresta

Insured loss estimates for high profile nat-cat events vs global nat-cat GWP 2017-2022 (USD billions)



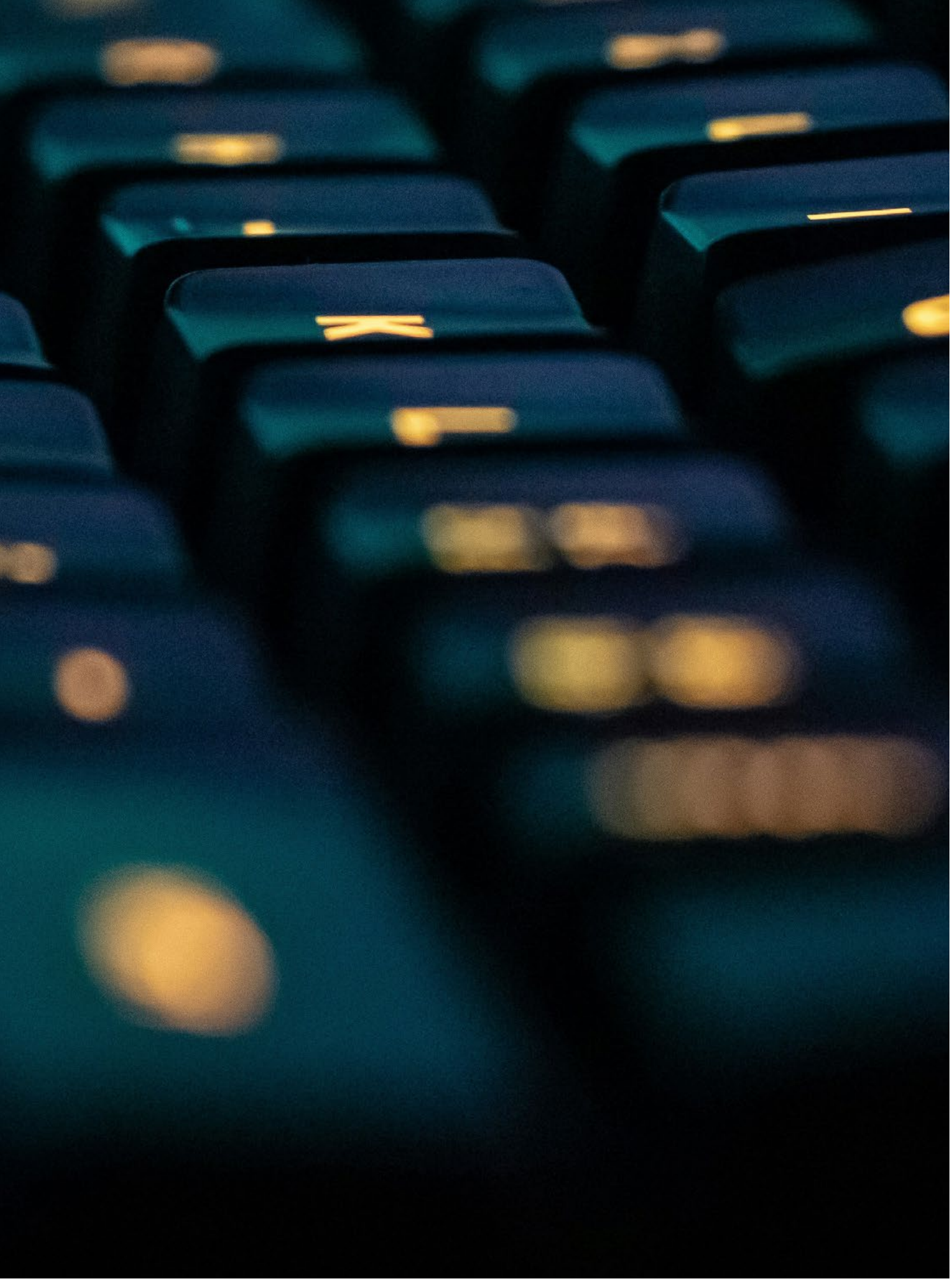
5 Howden, 'Cyber Insurance: A Hard Reset,' (pg.18).

One of the major fears around the potential downside of cyber risk is the ability to diversify a portfolio to avoid overarching accumulations of risk.

In nat-cat, this is done by underwriting a wide geographical spread of risk by, for example, writing premium in California or Minnesota to offset the potential for a southeastern hurricane to cause a total loss to your book. The worry is that cyber does not have an equivalent lever.

This might be the case in the very extreme tail (i.e. zero-day wormable OS vulnerabilities), but this is not true for the 'kittens' that have hit the cyber market so far. The analysis by Kovrr shows that the majority of events either impact a specific market segment (i.e. SME, large corporate) or a specific cluster of industries. As a result, the technology stack that insureds use becomes the source of diversification rather than geography, challenging the common misconception that everything in the cyber world is interlinked and therefore will be hit simultaneously.

Therefore, unlike other lines of business, which can rely on more experience-driven data sources to understand the loss potential of major catastrophes, examining systemic cyber perils requires more nuance. Instead of examining the loss potential of cyber cats and kittens in isolation, the market needs more granular models that can pinpoint the vulnerabilities and loss pathways within and across industries. With greater insight into the connectivity of impacts, the market can evolve beyond simplified assumptions and lean into the upside of what remains one of the most promising emerging risk classes this century.



03 Tale of tails

Another challenge in setting cyber risk tolerances is how to approach the modelling. Determining the amount of cyber risk to underwrite is as much a deterministic exercise as it is probabilistic.

Cyber offerings require capital providers to have some tolerance level for potential cyber-related financial losses, but many investors are understandably cautious about the systemic component of cyber coverage and do not want to be overweight in a nascent class. Instead, they predominantly favour the better-understood volatility of more mature classes. Only a few carriers publicly disclose their cyber tolerance, a practice that is considered standard in other classes, including nat-cat.

A better sense of capital risk preference can be formed through 'war-gaming' exercises. For example, posing the question: how would you feel about a USD Xm loss in your cyber book? Given market reactions to such a loss, follow-up questions might be:

- ↘ Should we buy more reinsurance?
- ↘ Would you reload us with more capital?
- ↘ Should we write more cyber, or retrench?

To answer these questions, it is important to understand the existing methods of measuring cyber exposure and just how likely that USD Xm loss is to happen.

Exposure

3.1 Approaches to quantifying exposure

From an operational standpoint, the key criteria for quantifying risk are stability and repeatability. The ability to measure movements in exposure is critical to staying within tolerance.

From a commercial standpoint, it is also essential to capture diversification, accurately incorporate vulnerability and assess the threat landscape (hazard). This is no easy task in the complex and ever-changing cyber world.

The framework below is based on Howden Re's observations of carriers' approaches to cyber exposure management. Available methods can be split broadly into the following categories, where positive gradation between levels addresses more challenges and increasingly satisfies key criteria:

- Entry
- Bronze
- Silver
- Gold

	Entry	Bronze	Silver	Gold
Data	Policy limit, attachment point, SIR and premium collected on each client.	Data classification framework set across the business to standardise data collection. Data also collected on: • sub-limits • revenue • industry • geography	Key secondary modifiers captured to augment data including Gross Profit Margin, URL, employee count and record count split out by PII, PHI and PCI.	Data on risk characteristics such as backups, redundancy, patching cadence, etc. Augmented by third party data sources and underwriter data collection.
Exposure monitoring and reporting (probabilistic modelling)	Regular modelling carried out by reinsurance broker or third party.	License a cyber model, which is run on default settings. Regular reporting to underwriting management.	License a cyber model and adjust the settings to develop a proprietary view of risk based on internal research. Regular reporting to underwriting management.	License one or more cyber models and adjust the settings to develop a proprietary view of risk. Outputs from the cyber model(s) either informs internal model* directly, or feeds into proprietary internal scenarios.
Exposure monitoring and reporting – (deterministic modelling)	Lloyd's RDS default or standardised market scenarios.	Adjusted Lloyd's or other market RDS based on own research and broad assumptions around secondary modifiers.	Proprietary scenarios developed to stress test carrier's specific portfolio based on externally validated R&D.	Proprietary scenarios used to calibrate probabilistic modelled outputs or feed directly into internal model.*
Exposure monitoring and reporting – limit aggregation	Decisions based on aggregation of total limits deployed.	Monitoring of total limits deployed within sub-segments (split by revenue and industry).	Monitoring of total limits deployed in sub-segments compared against defined underwriting appetite.	Data compared against industry data to show where concentrations exist compared to peers (Industry Exposure Database (IED) benchmarking).
Portfolio tools	No portfolio tool.	Stacking algorithm to monitor tower aggregations.	Portfolio is uploaded into a monitoring tool and can be reactively queried when new vulnerabilities are discovered.	Portfolio is uploaded into a monitoring tool is proactively assessed. Carrier and client updated when vulnerabilities are discovered.
Resourcing and expertise	Cyber forms part of an individual's role within a broader exposure management function.	Dedicated individual focusing on cyber within a non-nat-cat exposure management function.	Dedicated cyber exposure management team with expertise spanning exposure management, modelling. 1-2 pieces of research conducted each year on assumptions. Horizon scanning conducted to assess future exposures.	Dedicated cyber exposure management team including threat intelligence and cyber research. 3-5 pieces of research conducted each year on model assumptions.

*internal model refers to capital or risk tolerance setting model across all lines of business

Volatility

3.2 Setting risk appetite

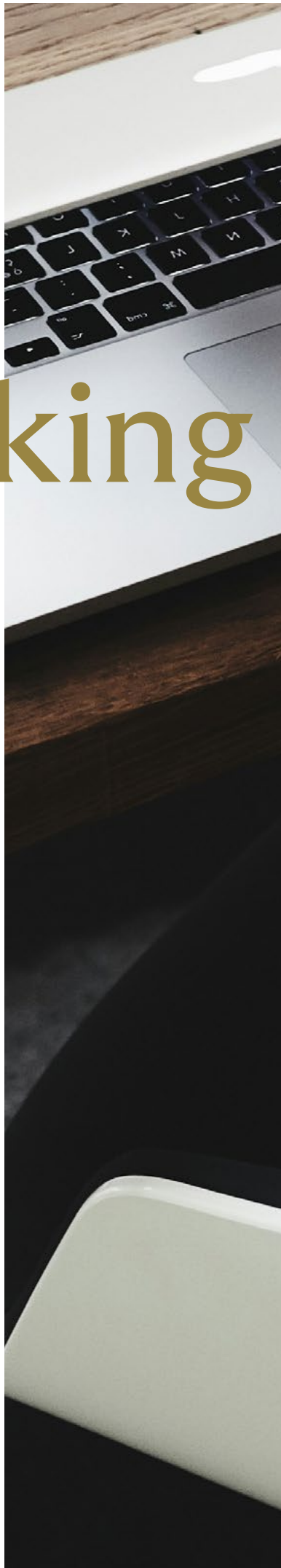
The framework proposes that, to define risk appetite, a complete distribution of losses, i.e. generating an exceedance probability (EP) curve, should first be built. Probabilistic models should be calibrated using bespoke scenarios by incorporating multiple frequency modelling approaches to estimate deterministic scenarios. This enables carriers to answer important questions about the volatility of their cyber portfolio, such as:

- What is the effect on technical earnings volatility, e.g. deviation from mean at the 5-10 year return period?
- What is the volatility in the tail, e.g. deviation from mean at the 200 year return period?

Risk appetite can then be defined as volatility vs. shareholders' equity, setting appropriate tolerances around this measure. Deterministic scenarios and exposure limits are then used as underwriting controls to give comfort around specific exposures, capturing underwriter expertise and past performance.

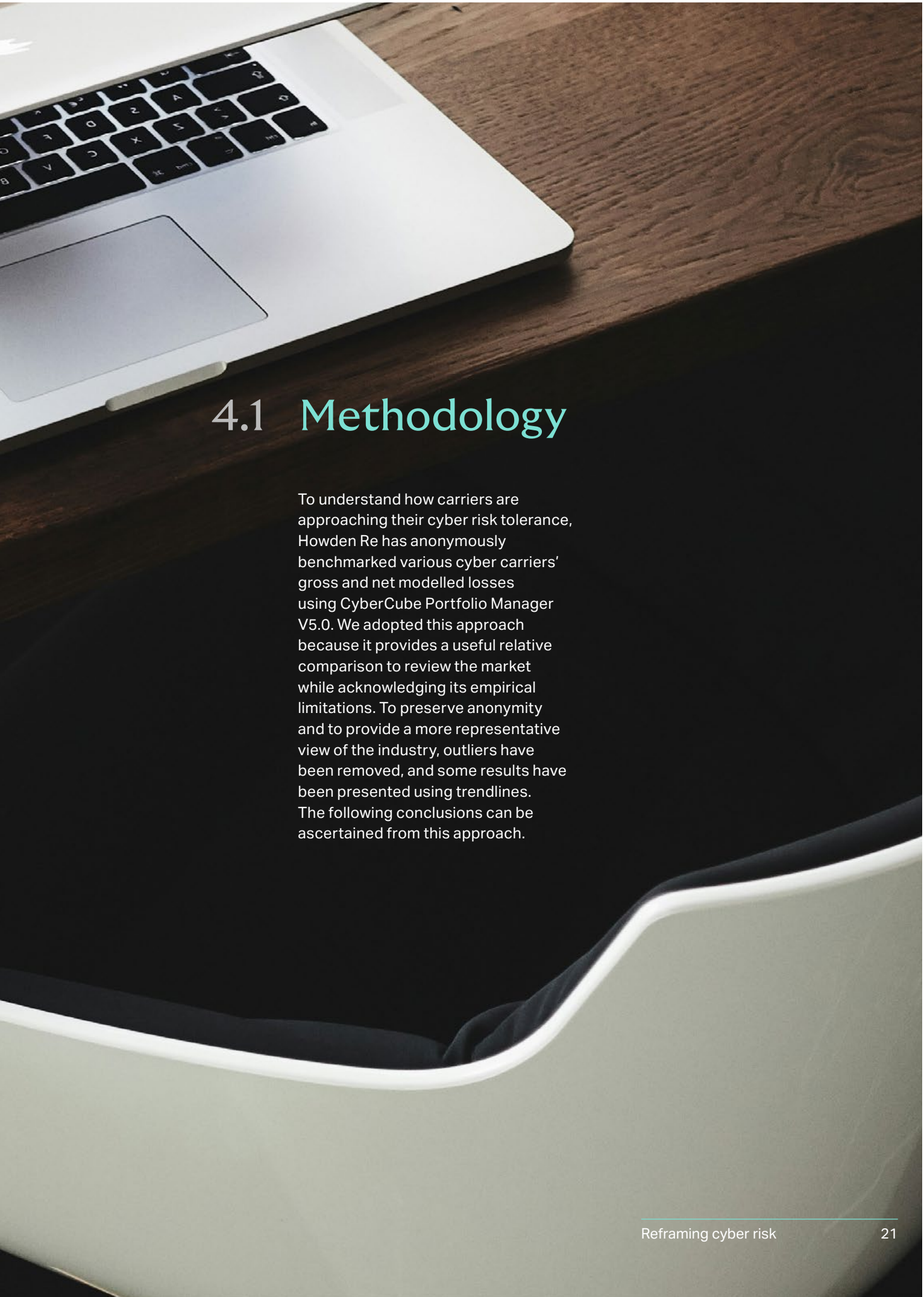
04

Peer benchmarking analysis



The cyber (re)insurance market has experienced significant growth in recent years, driven by increasing demand for coverage.

However, the extent to which carriers are exposing their portfolios to cyber risk varies considerably. The following analysis evaluates how carriers are currently managing their cyber risk exposure while identifying potential opportunities for insurers to scale their cyber business.



4.1 Methodology

To understand how carriers are approaching their cyber risk tolerance, Howden Re has anonymously benchmarked various cyber carriers' gross and net modelled losses using CyberCube Portfolio Manager V5.0. We adopted this approach because it provides a useful relative comparison to review the market while acknowledging its empirical limitations. To preserve anonymity and to provide a more representative view of the industry, outliers have been removed, and some results have been presented using trendlines. The following conclusions can be ascertained from this approach.

4.2 Analysis one

The average cedent takes far more nat-cat risk than cyber risk – even though the nat-cat market historically produces more significant relative losses than cyber.

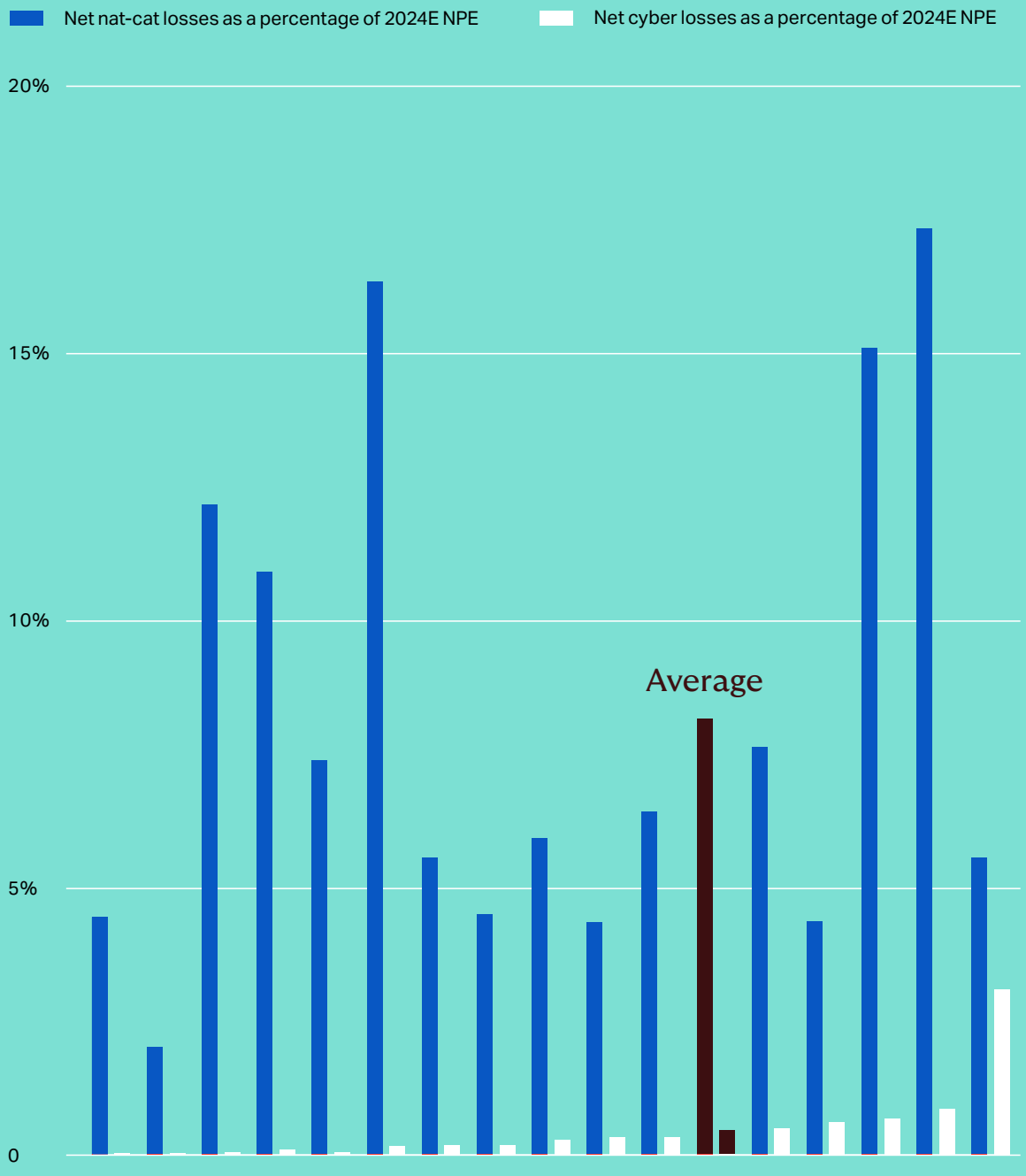
Earlier, a comparison of nat-cat losses and premium levels from 2017 to 2022 revealed that premiums only covered losses in two of the largest nat-cat events. In contrast, premiums exceeded losses in every high-profile cyber event during the same period. This disparity suggests that the industry has a much larger buffer when it comes to absorbing cyber losses, and therefore opportunity for insurers to take on more cyber risk.

Pushing this thesis further, figure 5 examines individual companies' nat-cat loss ratio versus their cyber loss ratio. On an average, company-by-company basis, carriers are willing to assume roughly 8% of net premiums earned on nat-cat AALs versus <1% on cyber AALs. This finding supports the view that, in some cases, carriers may have more balance sheet capacity to take on additional cyber exposure.

Figure 5

Source: Howden Re, NOVA, Bloomberg data

Analysis of sixteen companies' natural catastrophe aggregate annual losses vs cyber aggregate annual losses as a percentage of group NPE



4.2 Analysis two

Using exponential 'best fit' trendlines of nat-cat 1:200 aggregate exceedance probabilities (AEPs) and cyber 1:200 AEPs: the smaller an entity's balance sheet, the more cyber risk it assumes and the less nat-cat.

Conversely, the larger an entity's balance sheet the more nat-cat risk it assumes, and the less cyber as a percentage of equity.

One explanation for the trend demonstrated by figure 6 is that smaller insurers may have limited capacity to take on significant nat-cat exposure as the potential for large, concentrated losses could threaten their regulatory solvency and/or rating capital. In contrast, larger insurers with more diversified portfolios most likely have a greater appetite for nat-cat risk, as they can spread the risk across a wider base. As previously discussed, nat-cat losses appear to have the potential to impart a much greater economic impact on insurer balance sheets than cyber events. Cyber risks, while still potentially severe, may be perceived as more manageable within the scope of smaller insurers' capital constraints.

Second, smaller insurers may focus on cyber as an area of growth, using it to differentiate themselves and capture market share. Conversely, larger insurers are likely to maintain more traditional portfolios dominated by more established classes, such as nat-cat. In this context, larger carriers with more extensive stakeholder accountability may find it challenging to increase their exposure to cyber risk significantly.

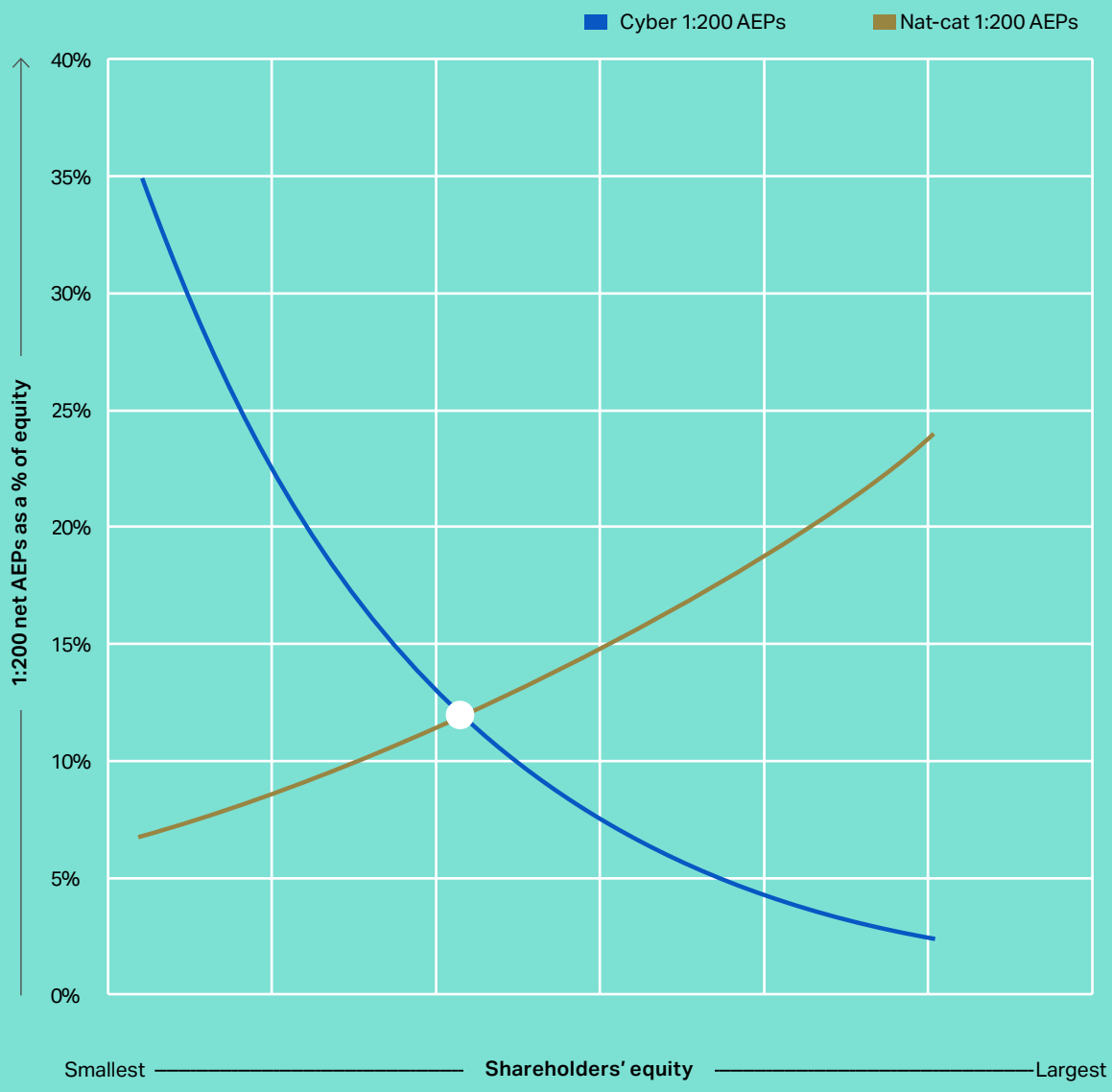
Third, larger entities that assume more nat-cat risk than cyber risk may be hesitant to expose their portfolio further to additional catastrophe risk because they have substantial experience with the impact of large losses. Given that they already allocate a significant portion of their balance sheet to nat-cat, they may be unwilling to take on additional exposure in cyber, which they potentially perceive as more volatile and less mature compared to more established classes, despite the fact it would likely diversify their cat risk.

All this considered, as the cyber (re)insurance market is projected to grow and as the threat landscape continues to evolve, there is an opportunity for larger insurers to balance the scales across their portfolio. By growing their cyber market presence now, they can position themselves to capitalise on future growth opportunities in a risk class with unparalleled potential, while simultaneously diversifying their portfolio.

Figure 6

Source: Howden Re, NOVA, Bloomberg data, S&P Capital IQ

Analysis of twenty-five companies' nat-cat vs. cyber net 1:200 AEPs by group shareholders' funds



4.2 Analysis three

On average, carriers are willing to accept an 11 percentage point (ppt) deterioration in their group combined ratio from a 1-in-200-year cyber event.

However, within this cohort, larger carriers, with substantial balance sheets, are adopting a more conservative approach to cyber exposure.

Pursuant to buyer behaviour, an 11ppt increase in group combined ratios is expected from a 1-in-200-year cyber event. Within cyber portfolios specifically, the expected average annual cyber cat loss is 11.8ppt. The largest underwriting coalescence is comprised of carriers targeting group cyber Probable Maximum Losses (PMLs) and cyber-specific cat Aggregate Annual Losses (AALs) of less than 10%. There is, within this, a large divergence, both in terms of group exposure and cyber underwriting philosophy. This is based on different risk appetites and portfolio construction – even within this 'cyber curious/cautious' segment. The average cat AAL and 1:200 PML are nevertheless higher, driven by the 'cyber confident' category.

As detailed above, figure 7 further demonstrates that on a company-by-company basis, carriers with more substantial balance sheets (more than USD 20 billion in equity) are taking the least amount of portfolio risk on cyber. Although industry experts have primarily called for increased capacity from reinsurers and capital providers, Howden Re believes that figure 7 highlights a substantial opportunity for insurers to leverage their balance sheet capacity to underwrite more cyber.

On the other hand, carriers with smaller balance sheets (less than USD 10 billion in equity) are markedly more exposed to cyber, accepting a short-term deterioration in their combined ratio to prioritise growth with the expectation of long-term profitability. Whether these insurers see cyber as an attractive opportunity to expand their premium base or whether they are taking advantage of what others might deem an immature class, they are identifying opportunities to establish themselves as leaders in this rapidly evolving market.

Cyber cautious

Carriers recognise the opportunity cyber presents, but are taking a more cautious approach.

Cyber curious

These carriers could be grouped in this section because of model variability. As the modelled numbers provide a theoretical assessment, in practice, they would be adjusted based on experience. As such, carriers in this category may either be taking a more cautious or confident approach (which is not adequately represented here) depending on actual losses.

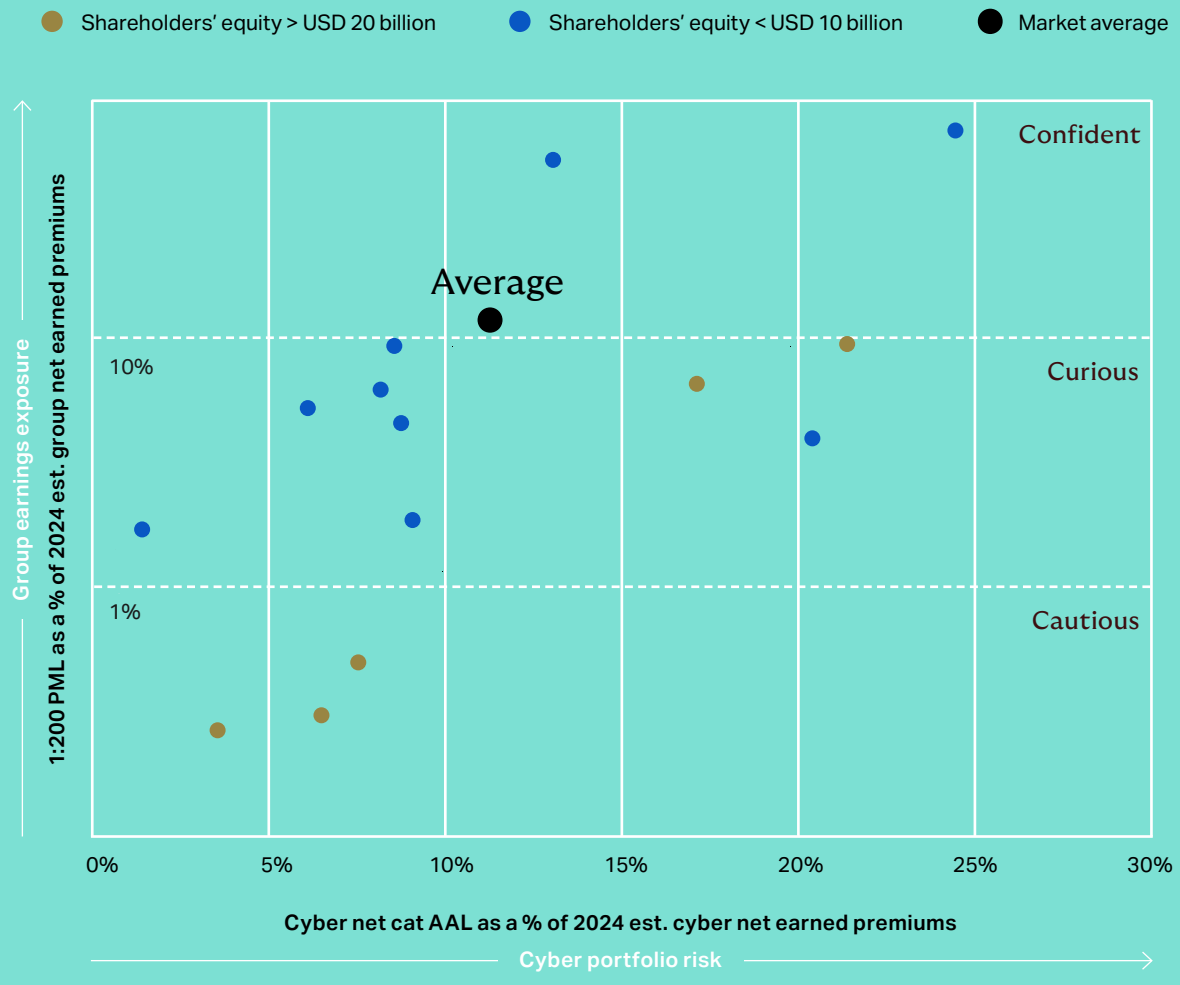
Cyber confident

Represents carriers that have most likely invested resources to develop an in-depth understanding of cyber risk.

Figure 7

Source: Howden Re, NOVA, Bloomberg data

Logarithmic analysis of fourteen cyber carriers' earnings exposure compared to cyber portfolio risk



4.2 Analysis four

On average, markets are retaining 65% of their cyber premium while ceding 56% of their cyber cat AAL.

This means that insurers are keeping a significant portion of the revenue generated by their cyber policies while transferring a larger share of potential cyber cat losses to reinsurers. Therefore, each carrier in the cohort is efficiently using reinsurance to retain more premium.

On the whole, the market average (figure 9) reveals a favourable trade-off between the cohorts' retained premiums and retained losses. By ceding 56% of their cat AAL while retaining 65% of their premiums, insurers are optimising their risk-reward balance in the cyber (re)insurance market. This tailwind is likely driven by the use of non-proportional reinsurance structures to protect carriers from extreme tail risk.

In line with this trend, some cedents have recently reduced quota share cessions and moved away from aggregate stop-loss, with occurrence-based products that deal directly with systemic exposure increasing in popularity (figure 8). While quota share remains the dominant form of risk transfer, an uptick in event-based cover highlights cedents' increasing concern over systemic risks, as these covers attach specifically to catastrophic cyber events.

The shift towards non-proportional reinsurance structures and the increasing adoption of event-based covers suggests a growing understanding and management of cyber risks within the (re) insurance market. The effective use of reinsurance in this manner could indicate reinsurers' increased confidence in managing potential cyber losses and insurers' confidence in the attritional loss ratio. As reinsurers become more comfortable with the cyber risk landscape, they may be willing to take on more of this risk, thereby enabling primary cyber insurers to write more business.

Figure 8
Source: Howden Re analysis of 25 risk carriers

Percentage of insurers purchasing cyber treaty structures (2020-2024)

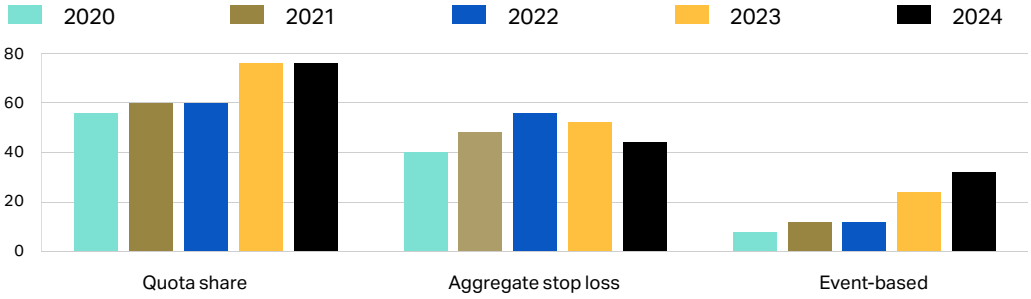
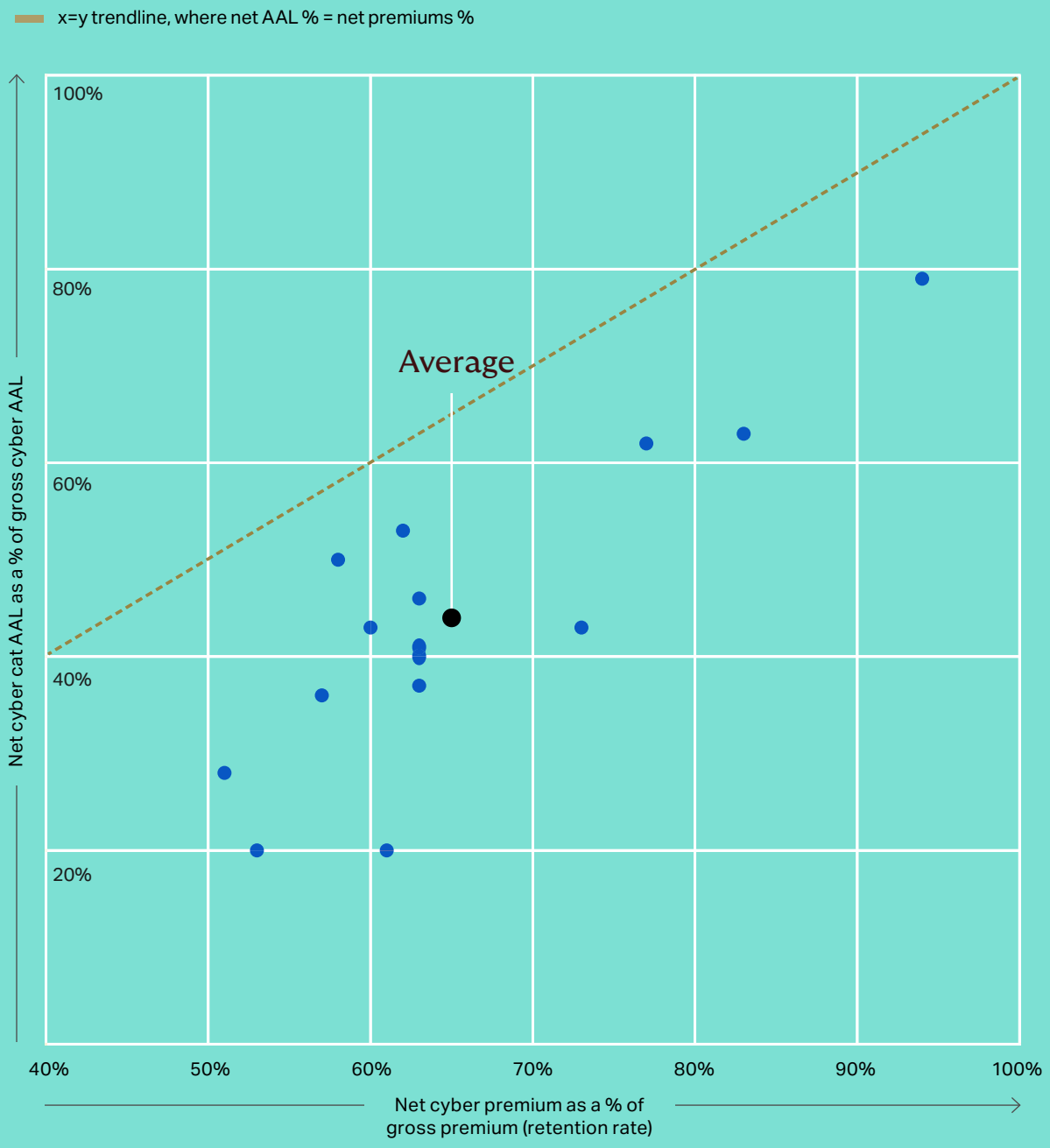


Figure 9

Source: Howden Re

Analysis of sixteen companies' retained premiums versus retained losses



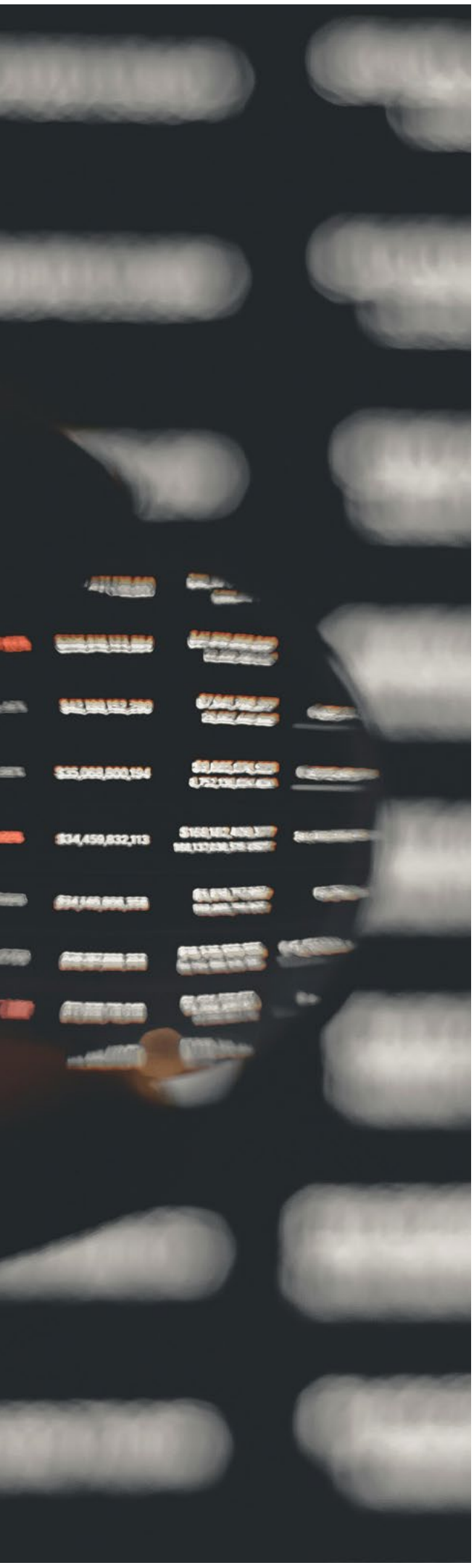
05

Shape the future

Conclusion

The contrast between the heightened perception of cyber risk and the tangible opportunities it presents is stark. Our analysis strips away the veneer of imminent cybergeddon to reveal a landscape ripe with potential for the (re)insurance sector. On average, the data highlights a cautious yet underleveraged appetite for cyber risk among (re)insurers. This opens the door to recalibrating risk thresholds, suggesting that the industry could, and arguably should, bear more cyber risk than it currently does. Leveraging advanced risk assessment and modelling, (re)insurers are positioned to expand their portfolios meaningfully in this arena, navigating the complexities of cyber threats with a more informed and nuanced approach.

This report ultimately serves as a call to action for the (re)insurance industry, encouraging a pivot towards greater cyber risk assumption backed by rigorous analysis and strategic foresight. This shift is not merely about embracing risk but about recognising and seizing growth opportunities that the digital age affords. As the industry moves forward, the ability to discern between perceived threats and actual vulnerabilities will be key. In doing so, (re)insurers can redefine their roles in the digital landscape, not as cautious observers but as proactive participants shaping the future of cyber resilience and security.



“

(Re)insurers can redefine their roles in the digital landscape, not as cautious observers but as proactive participants shaping the future of cyber resilience and security.

06

Meet the team

Luke Foord-Kelcey

Managing Director, Global Head of Cyber

+44 (0)7521 775 995
lfk@howdenre.com

Matthew Webb

Director, Cyber Reinsurance

+44 (0)7736 439 459
matt.webb@howdenre.com

Mark Lynch

Director, Cyber Reinsurance

+44 (0)7521 775 989
mark.lynch@howdenre.com

Toby Lampier

Director, Cyber Reinsurance

+44 (0)7596 872 768
toby.lampier@howdenre.com

David Flandro

Managing Director, Head of Industry Analysis and Strategic Advisory

+44 (0)7719 928 552
david.flandro@howdenre.com

Jack Sandford

Director, Cyber Reinsurance

+44 (0)7521 775 984
jack.sandford@howdenre.com

Cecilia Assmundson

Associate Director, Cyber Reinsurance

+44 (0)7596 872 776
cecilia.assmundson@howdenre.com

Nena Atkinson

Research Associate, Industry Analysis and Strategic Advisory

+44 (0)7596 874 286
nena.atkinson@howdenre.com

Contact us at info@howdenre.com
or call us on 020 7623 3806.

One Creechurch Place, London, EC3A 5AF

T +44 (0)20 7623 3806
F +44 (0)20 7623 3807
E info@howdenre.com

howdenre.com