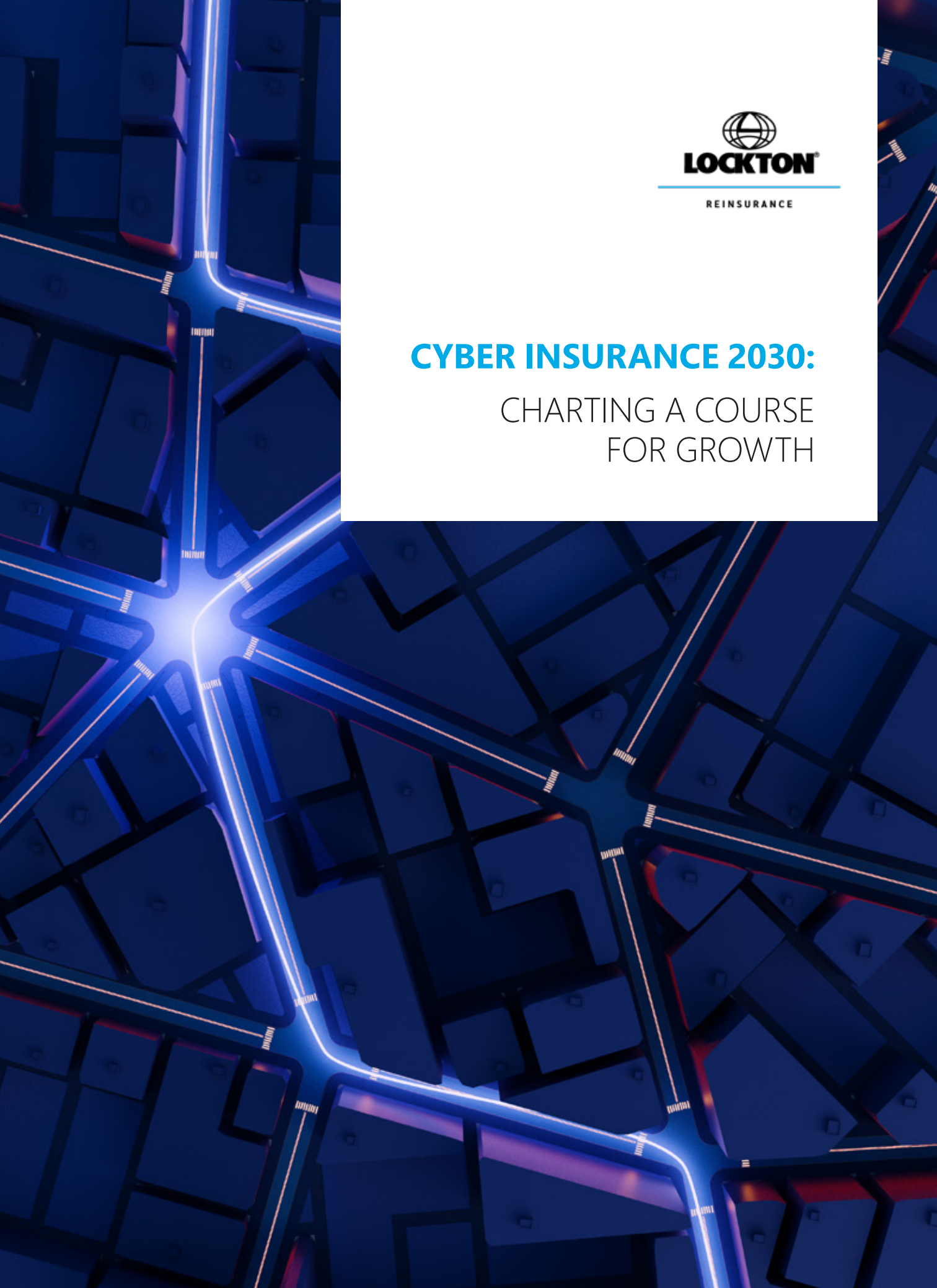


LOCKTON

REINSURANCE

CYBER INSURANCE 2030:

CHARTING A COURSE FOR GROWTH

- **Exposure**
- **Peril**
- Risk Transfer
- Placement

About Lockton Re

Lockton Re, the global reinsurance business of Lockton Companies, helps businesses understand, mitigate, and capitalise on risk. With over 500 colleagues in 23 locations globally, the business is continuing to grow, pushing the reinsurance industry forward with smarter solutions that leverage new technologies—delivered by people empowered to do what's right for clients.

Lockton Re's reports, market commentary and insights focus on key topics, occurrences or changes in the (re)insurance and broking market place which impact our clients and partners. In order to help guide relevance for the reader we categorise this content in four areas – Exposures, Perils, Risk Transfer and Placement. Lockton Re looks forward to working on behalf of our clients to deliver new insights and innovative products designed to address the multifaceted cyber risk environment.

Executive Summary

The cyber market is anticipated to more than double by 2030. Even conservative estimates suggest significant continued growth, which will have profound implications for both the cyber (re)insurance market itself and the wider industry. There is inherent uncertainty in any projection of market growth, so, rather than simply adding numerical estimates to the market projection, we look beyond the numbers to examine the conditions necessary to meet such expectations. The growth to meet the projections for 2030 is not inevitable. It will be the result of a series of deliberate actions. We have researched a range of perspectives from different stakeholders around the industry and sought answers to issues such as: How do we prepare for such a market? What are the product and capital innovations required to fulfill this growth ambition? We challenge and explore these issues, offering ideas to enable expansion. Three important themes are:

1. Improved data quality

2. Continued modelling investment

3. Flexible product approach for distribution

These are examined in more detail in this white paper.

Acknowledgements

This paper would not be possible without the contributions and input from several people around the cyber insurance industry. Some prefer to remain anonymous, and we are grateful for their time and insights. Others who have provided perspectives and commentary are:

YOSHA DELONG,
Global Engagement Officer,
Mosaic Insurance

TOM DRAPER,
Managing Director UK, Coalition

TIM GARDNER,
Global CEO Lockton Re

MARK GREISIGER,
President and CEO,
NetDiligence

THEO NORRIS,
Capital Markets Structuring and Cyber ILS Lead, Lockton Re Capital Markets

ERIC PAIRE,
Head of Capital Advisory Practice,
Lockton Re

Introduction

The cyber market has been one of the stand-out successes of property and casualty insurance in the last couple of decades. The combination of rapid technology adoption, a changing risk landscape with evolving tactics of threat actors and an increasing awareness of the peril has led to this growth. The market estimates for 2025 range from $16 billion to $20 billion,[1-2] Estimates for 2030 range from $30 billion to $40 billion or more.[3]

The average compound annual growth rate (CAGR) of the cyber (re)insurance market between 2015 and 2025 has been consistently over 20%. In some years, it has exceeded 30%. In recent years, the assumption that the cyber market will continue to grow at a similar pace has rarely been questioned. However, since rates peaked in late 2021 and early 2022, there has been a supply-led increase in insurance capacity, which has led to a slowing of CAGR. A range of estimates still suggests growth rates above 10% for the remainder of the 2020s, which implies an approximate doubling of the global premium by 2030.

There is a consensus that growth will continue, notwithstanding the current softening in rates. Indeed, AM Best reported a fall in absolute premium volume in the US for the first time,[4] reflecting intense competition for existing buyers of cyber insurance.

We examine the various hypotheses underlying the expected growth and explore the dynamics influencing the ongoing expansion of the market. This report is not intended as a predictor of the future but rather as an opportunity to take stock and review the current trends that are driving both opportunities and challenges for the market. This paper focuses on how these influences change to meet the high expectations of market growth. We have interviewed a range of stakeholders across the industry to better understand the common themes, compare what is happening today with the long-term view of the market horizon and determine how best to bridge the gaps.

[1] http://munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html
[2] https://www.rootsanalysis.com/cybersecurity-insurance-market
[3] https://www.reinsurancene.ws/beazley-forecasts-cyber-insurance-market-to-grow-to-40bn-by-2030/
[4] https://www3.ambest.com/ambv/sales/bwpurchase.aspx?record_code=354887&AltSrc=22&AltServ=640

Cyber Market growth: a self-evident truth?

It has been axiomatic among practitioners in the cyber insurance industry that rapid market growth is an ever-present fact of operating in this market. The property and casualty insurance market has grown at an average of high single-digit CAGR between 2015 and 2024.[5] The cyber (re)insurance market has grown at more than double this pace over the same period.

> The property and casualty insurance market has grown at an average of high single-digit CAGR between 2015 and 2024. The cyber (re)insurance market has grown at more than double this pace over the same period.

This growth has seen the cyber market transform from an obscure corner of specialty insurance into a more widely understood and integral part of the broader (re)insurance ecosystem. Cyber insurance products have become part of the wider cyber risk management landscape, particularly among larger companies. It is estimated that approximately 80% of large companies (over $10 billion USD in annual revenue) purchase cyber insurance, so, in this segment of the market, we have moved past the talking points and debate between cybersecurity spending on one hand and cyber insurance on the other. [6]

For smaller companies, it is a different story. Only 10% of small and mid-sized enterprises (SMEs) purchase cyber cover [7]. The reasons companies refrain from purchasing are numerous, and we will explore these further. Addressing this insurance take-up gap represents one of the biggest opportunities for the market in the coming years.

[5] https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/global%20insurance%20report%202025/global-insurance-report-2025-the-pursuit-of-growth.pdf

[6] https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html

[7] Ibid.

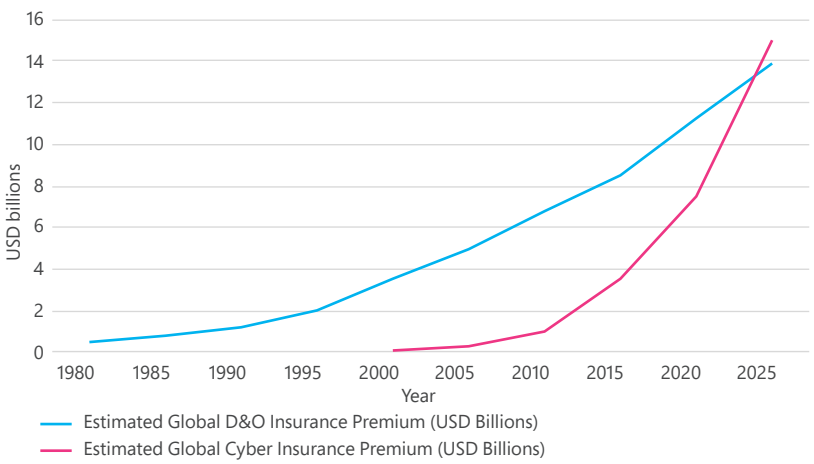
Learning from experience

Tim Gardner, CEO of Lockton Re, has compared the growth of the cyber market with that of the Directors and Officers (D&O) market. Both have emerged in response to the increasing risks companies face. The D&O market has grown more steadily, primarily due to heightened regulatory scrutiny and an increasingly challenging litigation environment. The cyber market has grown due in large part to the evolving threat landscape. Below, Figure 1 shows the comparative growth in the D&O and Cyber insurance markets. Adoption has been uneven, and take-up among SME companies in both D&O and cyber has been slower than for large companies.

New exposures drive market innovation and have created opportunities in both contexts. 'The insurance market is highly capitalized so it is always looking for new opportunities with long-term potential. Cyber is one of those,' Gardner states. Where potential exists for a significant delta between gross and net results, this creates opportunity for new capital. Some are nervous about tail risk, while others embrace the volatility, making a market in the process.

Given exposure will continue to grow and change, and as systemic risk drives the risk agenda among carriers, the biggest long-term challenge is the potential shortfall in capital. It is incumbent on us as a market to build confidence in pricing to attract sufficient new investors, both via traditional and alternative routes to market.

Figure 1: Estimates of global D&O and Cyber (re)insurance premiums



Source: Lockton Re

Eggs and baskets

'It is the part of a wise man to keep himself today for tomorrow, and not to venture all his eggs in one basket'.[8] Miguel de Cervantes effectively captured the concept of diversification in his novel Don Quixote, published in 1605. Diversification is not a new concept in a financial context; it is almost as old as the insurance and finance industry itself. Identifying assets or risks that do not correlate too much with each other is fundamental to how (re)insurers view their risk portfolios and assets.

Cyber insurance, in the context of the broader property and casualty (re)insurance market, is rightly seen as a significant diversifier. A material portion of risks the insurance industry takes fall into the categories of either property (mainly natural perils leading to short-tail exposure) or casualty (with liability driving long-tail risks). Cyber insurance has evolved with aspects of exposure analogous to property as well as risks that bear more resemblance to wider liability cases. Importantly, though, cyber risks are non-correlating with other major natural perils. This means that, in the event of a major catastrophe impacting property insurance (such as a hurricane), cyber risks are not affected in the same way. Similarly, trends that emerge in liability (such as social inflation or nuclear verdicts) have less spill-over into the domain of cyber risk.

Within cyber insurance itself, diversification plays an important role as well. Common sources of network contagion, which can impact multiple companies with the same technology incident, have always been a concern. In the early years of the cyber market, some insurers incorporated 'wild virus' exclusions into their policies to limit potential for an accumulation of losses.[9] This narrowing of coverage limited demand, as it did not support customer needs. Competition expanded coverage to innovate and meet demand.

One inescapable fact of the cyber insurance market is that there have only been a handful of true cyber catastrophe events where single incidents have led to multiple impacted parties. As a result, there are limited data points to understand how a technology incident would affect multiple companies simultaneously. Much research has been conducted on this, but, inevitably, there is an element of conjecture about how exactly this could manifest.

> "One inescapable fact of the cyber insurance market is that there have only been a handful of true cyber catastrophe events."

Currently, the biggest potential sources of contagion within cyber insurance are malware spread, a zero-day vulnerability exploit, and digital supply chain outages (including cloud services). These scenarios cover a very wide set of specific circumstances but help frame ways in which portfolios could be affected.

In cloud services, there is a growing understanding in the insurance industry of how these services operate, and the implications of outages for insured portfolios. Amazon Web Services was launched in 2006, and, during the 2010s, cloud computing adoption began to accelerate dramatically. In 2010, the global cloud computing market was valued at $24.6 billion, growing to $156.4 billion in 2020.[10] Figure 2 on page 8 illustrates the adoption of different cloud technologies. Today, it is pervasive, with 96% of enterprises using some form of cloud computing.[11] Much has changed in recent years in our understanding of what diversification means. It was only a few years

[8] "Don't Put All Your Eggs in One Basket." n.d. Grammar-Monster.com https://www.grammar-monster.com/sayings_proverbs/dont_put_all_your_eggs_in_one_basket.htm

[9] https://www.herrick.com/publications/cyber-liability-insurance-what-to-look-for-when-obtaining-coverage/

[10] https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/

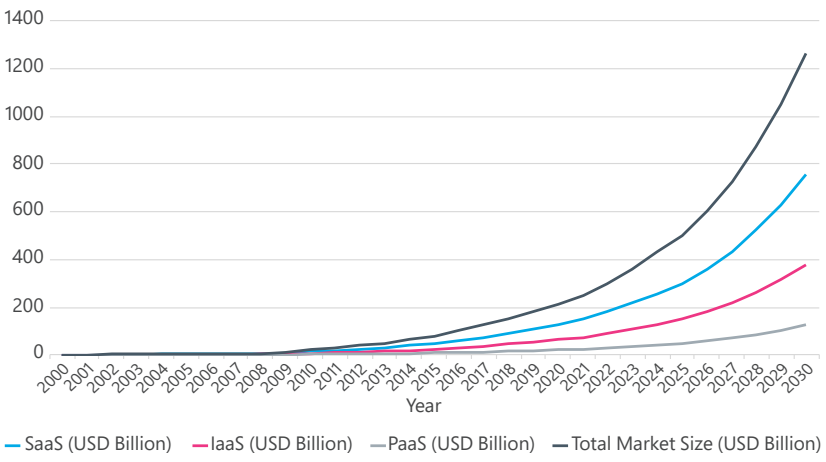
[11] https://www.itdeskuk.com/latest-cloud-statistics

ago that the concept of a 'cyber hurricane' implied uniform and pervasive exposure across national borders and common technologies.[12] We have learned and adapted our understanding of cyber systemic exposures, considering the experience of cyber incidents that have led to widespread economic losses.

The common technology components companies use have rapidly evolved, and the level of dependency has become better understood. The three largest participants in the cloud computing market are Amazon Web Services, Microsoft Azure and Google Cloud Platform. Between them, they were responsible for 63% of the global market share in cloud infrastructure spending in 2024.[13]

These companies' investment levels are enormous, and users of these services are better able to navigate how best to leverage different parts of cloud computing, such as infrastructure, platform and software. As the (re)insurance industry learns more about how these different segments of networked technology operate and interact, it reaches a fuller understanding of the pinch points and sources of potential failure. Modern cloud computing has increasingly focused on resilience, which means that failures are less likely to be catastrophic.

Figure 2: Cloud computing market size estimate from 2000 – 2030, including projections from 2025 – 2030.



Source: Lockton Re

[12] http://betterley.com/samples/cpims14_nt.pdf

[13] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Unlocking SME growth

For many years, there has been uncertainty about how to develop a compelling cyber insurance proposition that is accessible to SMEs. Estimates vary by territory, but, although the product has been available for many years, 10% or less of SMEs in most mature markets have purchased it. A combination of challenges has limited the adoption of insurance within the SME sector. Demonstrating value, educating the distribution networks, explaining the coverage and articulating its utility have been perpetual issues.

Even where specialty lines insurance is established (e.g. in the USA, UK and EU), stand-alone affirmative cyber insurance has been a complex topic for generalist retail insurance brokers to gain comfort. Some success has been achieved in different distribution models, such as online direct sales, as well as 'add-on' cyber coverage by endorsement. These approaches offer ways to introduce cyber insurance while reducing the friction involved in the process of insurance procurement. Additionally, a newer generation of cyber-focused MGAs has specifically targeted this segment of the market with simplified and more cost-effective insurance products.

One such MGA is Coalition. Tom Draper, Managing Director for the UK reflects on the issue of SME take up rate, saying that 'many SMEs do not think of cyber risk as an insurance challenge. It is up to us to reframe the conversation to enable insurance to become part of the solution set and resonate with current non-buyers'.

Diversification: catalyst for growth

There is a better understanding today of how correlations between risks within cyber insurance portfolios would manifest in the event of a major cyber incident. There a four primary perspectives, through which diversification helps limit potential insured losses.

These are:

- **Geographical:** different countries have varied deployments of technologies. Additionally time zones can make a material difference in the way cyber incidents spread.
- **Industry:** some technologies are specific to certain industries. They have a disproportionate impact on certain elements of a supply chain, where few providers may dominate a particular subsector
- **Revenue:** smaller companies tend to be more uniform in their deployment of technology, and are more reliant on public cloud infrastructure. By contrast, larger companies are more likely to have bespoke configurations, multi-layered and complex networks.
- **Technology infrastructure:** commonalities across technology stacks provide sources of potential vulnerability. Some technologies are used in many different settings, so understanding how versions of these are deployed and their interconnectivity is critical to the assessing systemic impact.

Understanding how diversification manifests in a particular portfolio is critical to assessing how a loss event may play out. Where diversification benefits are fully realized, capital can be more efficiently deployed and the analysis of probable maximum loss calculations reduced. Ultimately, more premium can be written on the same capital base if there is confidence in the approach to diversification. This enables improved market growth over time.

Despite much technological investment in insurance, there is still a process-based challenge as well, making the transaction process as smooth as possible for customers. If insurers can link decision makers with the language of cyber risk, it ensures the relevance of the market to a sector which will drive growth over the coming years.

“If insurers can link decision makers with the language of cyber risk, it ensures the relevance of the market to a sector which will drive growth over the coming years.”

To achieve the anticipated growth of the overall market, expanding the volume of new buyers is key. In the early years of the cyber insurance market, the policy was an indemnity-based cover with limited additional services. This has evolved significantly to become a much more comprehensive offering, including risk management benefits, active risk alerts and post-loss recovery services. Prioritizing the education of brokers and agents and creating aligned incentives for raising the value of cyber insurance are key to expanding the market.

New buyers

One of the original catalysts of growth in the nascent cyber market in the early 2000s was the rapid adoption of regulations around management and disclosure of personal information. This was exemplified by the California Information Privacy Act of 2003 (SB1386). The law required entities that experienced a data breach involving California consumers' personal information to notify the individuals. This law became a model framework for other states in the United States as well as other countries develop data breach notification laws and regulations. In turn, cyber insurance products and solutions were developed to help companies comply with these regulatory obligations. Additional regulations by industry (such as for healthcare and financial services) and context (for example publicly listed companies) were expanded to create a patchwork of rules for companies to follow, with related sanctions for breaches.

As more countries establish and develop cybersecurity and data protection regulatory frameworks, organizations are increasingly motivated to purchase cyber insurance. Parts of Asia have passed recent laws that have stimulated increased interest in insurance. China implemented its Personal Information Protection Law in 2021 and

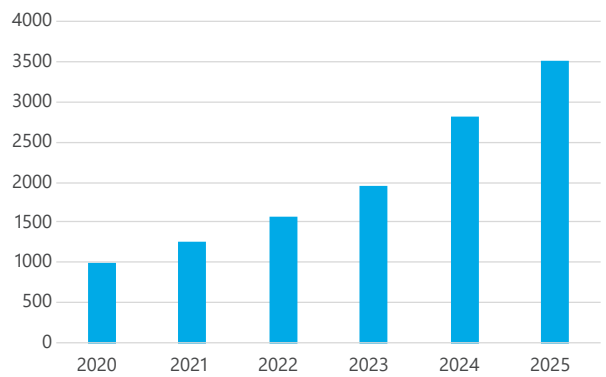
[14] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

introduced its new Network Data Security Management Regulations in 2025. India passed the Digital Personal Data Protection Act in 2023. Additionally, South Korea made robust updates to its Personal Information Protection Act in 2024, increasing liability for damages. These examples highlight the importance of this issue in these territories and how a ripple effect can occur. In Japan, the Act on Protection of Personal Information is in the process of a major overhaul to provide more comprehensive measures to protect data and review how fines and penalties are issued. Other parts of the world have also introduced new laws to address personal data.

Regulation is not the only catalyst. The impacts of cyber incidents have been persistent. Below, Figure 3 illustrates the growth of incidents in Latin America since 2020 making a high potential market for cyber insurance. Awareness has grown alongside a recognition that insurance can become part of the solution for companies. Clearly incidents alone are not sufficient to drive market growth, but they set an important backdrop for discussions around risk transfer.

One other area which is not discussed enough is that even among large companies, underinsurance is common. It is incumbent upon the cyber insurance industry to articulate and help explain the quantification of cyber risk in a way that is understandable to insurance buyers and bridges the gap between information security and risk management.

Figure 3: Growth in cyber incidents in Latin America 2020- 2025[14]



Source:World Bank

Long term capital

Competing in today's cyber insurance market can feel like a street fight, battling out for each client based on coverage, pricing, service and whatever else the customer considers important on that particular day. However, viewing the bigger picture is critical for the long-term sustainability of the industry. A few things need to occur to show outside capital providers the appeal of the insurance industry compared with other investments. Cyber insurance plays a role in this by improving the diversification of carrier portfolios. Second, the continual calibration of how capital is allocated, based on realistic disaster planning, needs to be refined. This allows for more efficient allocation of capital and has implications for how regulatory solvency and capital obligations are managed. Third, the understanding of systemic risks needs continued iteration to protect the viability (and reputation) of the industry.

As investors look to insurance as a source of potential investment, insurance risk offers a non-correlated asset class compared with other equities. The physical perils most insurance covers offer a differentiated exposure to risk that is independent of stock markets. Cyber risk offers a way for investors to access perils separate from natural catastrophes, and some investors are already participating in cyber as part of whole account protections in Lloyd's. As Eric Paire, Head of Lockton Re Capital Advisory said, 'investors can't be experts in everything. They rely on the (re)insurance markets to develop and refine diversified strategies to support investment goals.'

Insurance-Linked Securities (ILS) provide an effective mechanism for non-traditional capital providers to access insurance risk, with cyber becoming part of their investment toolkit. Over twenty investors have deployed capital since the initial formation of the cyber catastrophe bond in 2023. This market now approaches one billion dollars of coverage across eleven tranches and has

become a pillar of the catastrophe cover purchasing strategy of several leading cyber insurers. There was a flurry of activity in 2024, followed by a lull in deal flow in 2025. This was primarily due to the cost-effectiveness of traditional reinsurance capacity and a reduction in average reinsurance cession, in response to the softening of underlying rates. Whilst cyber cat bonds remain on an upward slope for new issuances, the journey has been stepped.

No discussion of ILS is complete without a nuanced understanding of cyber catastrophe modelling. Traditional natural catastrophe models draw upon decades of actuarial loss and incident data for natural disasters, while cyber catastrophe modelling must deal with limited historical precedents. This challenge creates inherent uncertainty, which means that ILS investors may demand a premium in their margin to reflect this, over and above that of property catastrophe risk. While models are still rapidly evolving, more capital is retained to take this uncertainty into account. One near-term consequence is that there could be insufficient capital to meet the tail risk metrics (re)insurers require. Until a major cyber event tests the models, perceived uncertainty in how event covers and bonds respond will persist.

Lockton Re takes a long-term view. Most market participants agree that traditional capital is simply unable to keep pace with cyber's growth trajectory. Capital markets will become a crucial and consistent part of the cyber reinsurance market moving forwards, and structures will continue to evolve. We are already beginning to see repeat bond issuances, and smatterings of secondary market bond trading activity as investors jostle for cyber risk exposure. According to Theo Norris, Cyber ILS Leader at Lockton Re Capital Markets, 'cedants are testing their event definitions and calibrating their view of risk behind the scenes, to ready themselves for the expansion of cyber cat protections, from event covers to catastrophe bonds'.

Chickens and eggs

One intriguing characteristic of the current cyber market is that, to attract capital investors, there needs to be a demonstrable growth path for the market. At the same time, to enable the growth of the market, there needs to be a line of sight to a sustainable source of capital. The relationship between market growth and the capital required to fuel it is a symbiotic one that is non-linear but critical to market success overall. It is an age-old question of which should come first. One way to solve this conundrum is the constant evolution of both the market response to the threat landscape and the adaptation of cyber catastrophe models, which will improve the parameters to assess the growth opportunities and capital requirements over time.

There is a trade-off in model usage between stability of the model that supports the long-term capital planning cycle on one hand and, on the other, the requirement to update and maintain a contemporary view of risk based on active adversaries and a rapidly changing threat landscape.

All models have limitations, so the better the industry can manage and operate effectively within these parameters, the more value can be derived from models in use to support third-party capital. Effective models incorporate a blend of scenario analysis, threat intelligence, technology dependency mapping and behavioral analytics to provide probabilistic loss estimates across portfolios. As regulatory frameworks and exposure profiles become more sophisticated, so too must the models.

This enables (re)insurers to more accurately assess aggregate exposures, identify systemic vulnerabilities and price risk with heightened confidence. Continual investment and the application of the learnings from these models will be vital as cyber risks increasingly intertwine with global economic systems and digital infrastructures.

The growth in technology dependencies presents a formidable challenge for cyber (re)insurers and cyber cat modelers alike. Modern organizations rely on a vast array of interconnected digital services, cloud platforms, third-party vendors and critical infrastructure, each introducing unique points of vulnerability. There are significant customizations across networks (especially for larger companies), which limit but do not eliminate potential risk. A single failure or compromise – whether in software supply chains, outsourced IT services or shared network environments – can cascade across multiple entities, amplifying the magnitude of loss and complicating risk assessments.

As digital ecosystems grow increasingly complex and global in scope, mapping these dependencies and understanding their potential for systemic impact becomes essential. Yosha DeLong, Global Engagement Officer at Mosaic Insurance, states that 'Supply chain failures are a source of concern for insurers and create the potential for volatility in how losses manifest.'

Effective cyber catastrophe models must not only identify direct exposures but also account for the indirect risks

> The growth in technology dependencies presents a formidable challenge for cyber (re)insurers and cyber cat modelers alike

arising from technology interdependencies, enabling (re) insurers to better gauge exposures.

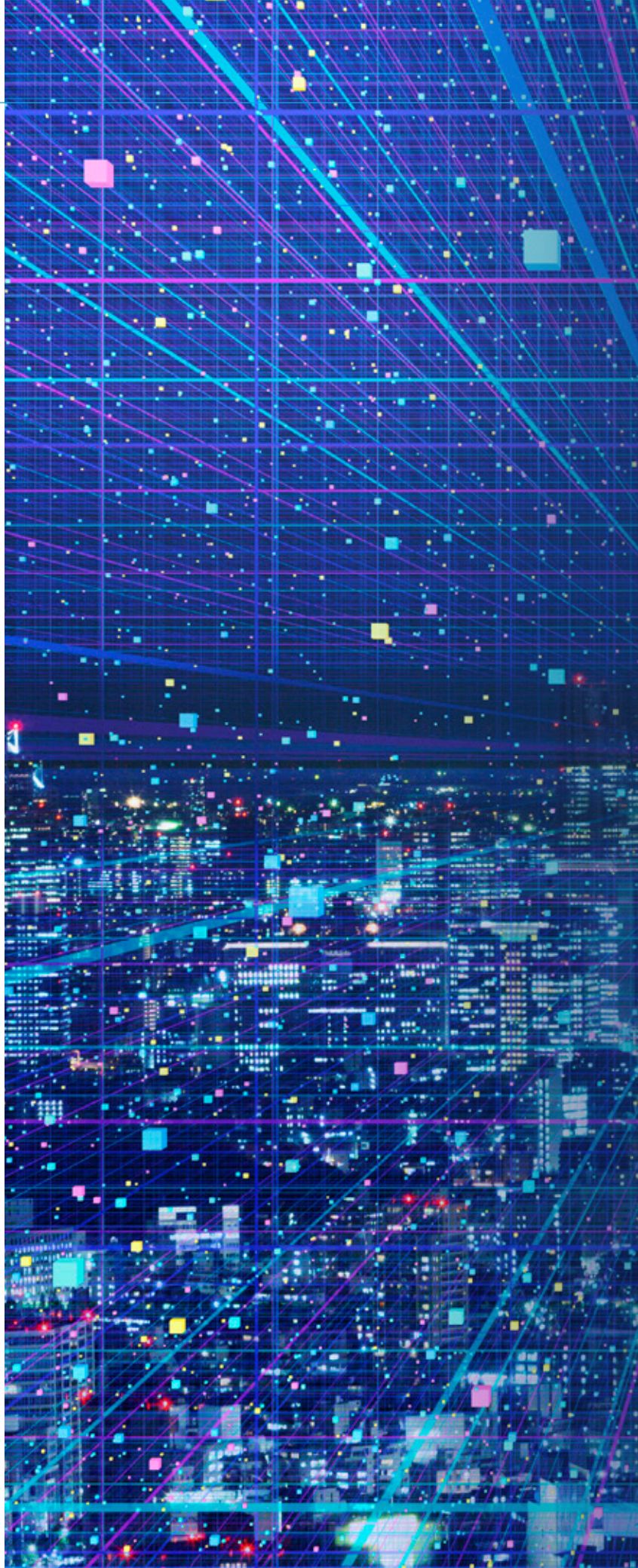
Small adjustments in cyber models can significantly amplify changes to modelled outcomes. For example, the method of calculating profit margins for business interruption losses has a big impact on modelled losses. Similarly, the way different types of security measures are represented in a portfolio and at the individual company level can have an outsized effect on potential losses. Another priority, which has been hamstrung by legacy systems despite material efforts by some across the industry, is the improvement of data quality. Where more refined information is captured (particularly at the point of underwriting), it reduces uncertainty about the underlying peril. In turn, this allows more efficient deployment of capital. This ranges from firmographic information about the company being insured (such as accurate website URL capture) to policy information (such as any coverage sublimits). Some data tools are available to automate this, but these are not yet widely used or trusted.

Product evolution

The direct cyber insurance product suite has been relatively static for more than a decade. Coverage has been tweaked and updated to reflect newer technologies and exposures, but the fundamental structure of a broad offering, encompassing both first- and third-party exposures (including business interruption), has been central to the market success to date. To support the growth expectations of the market, it may be time for a fundamental reimagining of the product structure. This could include more cost-effective product structures, offering coverage only for what a company perceives as its peak exposure – for example, covering only certain types first-party loss from the most sophisticated attacks, with a corresponding reduction in premium costs. Lockton Re has previously discussed the benefits of separating first- and third-party perils, and there remains potential to streamline distribution this way.[15]

Other opportunities to develop cyber insurance products include the integration of insurance products with other cybersecurity solutions. There have been multiple initiatives in this domain, including offering insurance with the take-up of cloud service provision. Separately, insurance has been bundled with security software. To date, there are few examples where this has successfully driven adoption. Given the multiple classes of insurance that involve offering insurance with other risk management or distribution, this deserves increased focus to support the wider value proposition.

[15] https://global.lockton.com/re/en/news-insights/the-all-risk-cyber-arc-challenge-an-assessment-to-simplify-cyber-reinsurance



Conclusion

Several headwinds are hampering the cyber insurance market's growth expectations by the end of the decade. There is a convergence of technical, operational and data-related challenges, while short-term excess supply is creating conditions that could make the market projections seem like a stretch. (Re) insurers face inevitable and persistent uncertainty due to the complexity and speed of change in digital infrastructures and threat actors. Cyber risk modeling is still in its relative infancy, further complicated by patchy or unreliable data, often stemming from legacy systems or insufficient underwriting information. As a result, it is hard to price risks appropriately and allocate capital efficiently. These issues are compounded by the static nature of most current product offerings, which have struggled to keep pace with clients' shifting needs and the nuanced contours of emerging cyber threats.

The good news is that innovation rarely takes a straight-line path, and though it can be messy and create unintended consequences, there is no shortage of enthusiasm for the market opportunity. We can draw lessons from experience in other classes, and with the amplifying impact of dramatically improved computational power, there are many reasons for continued optimism for the long-term robust health of the cyber insurance industry.

Mark Greisiger, President and CEO of NetDiligence and veteran participant in the market, offers a bullish sentiment. He states, 'Insurers are hiring technical underwriters, and account triage and efficiency are improving, which is a positive leading indicator.

"We can draw lessons from experience in other classes, and with the amplifying impact of rapidly improving computational power, there are many reasons for continued optimism"

There is continued investment in risk management services to support clients, which demonstrates the value customers receive. Additionally, cyber insurance is more frequently becoming a contractual obligation, driving uptake.'

The three common areas to address to achieve the anticipated market growth are:

1. **Improved data tools and quality to better understand portfolio risk**
2. **Continued investment in more granular models to mitigate systemic risk**
3. **Flexible, targeted products to improve distribution**

The cyber insurance market stands at a dynamic crossroads, shaped by evolving regulatory landscapes, increasing incident frequency, and the ever-growing complexities of technology dependencies. By fostering closer alignment between regulatory demands, investor expectations and technological realities, the industry can not only meet today's challenges but also unlock new pathways for growth and resilience in the digital age.

Authors and Contacts

AUTHORS

London

Oliver Brew ACII
Head of Cyber Centre of Excellence

+44 (0)7384 248 268
oliver.brew@lockton.com

New York

Brian Lewis
Cyber Practice Leader, North America

+1 646 279-1940
brian.lewis@lockton.com

CONTACTS

London

Matthew Silley FIA
Cyber Practice Leader, International

+44 (0)7391 387 699
matthew.silley@lockton.com

Jemima Hopper ACII
Broker

+44 (0)7855901856
jemima.hopper@lockton.com

New York

Jaimie Hunter
Senior Broker

+1 718 288 5337
jaimie.hunter@lockton.com

Chris Wafer
Senior Broker

+1 646 993 5029
cwafer@lockton.com

Caitlin Barnett
Broker

+1 929 675 9132
caitlin.barnett@lockton.com

MEDIA CONTACTS

London

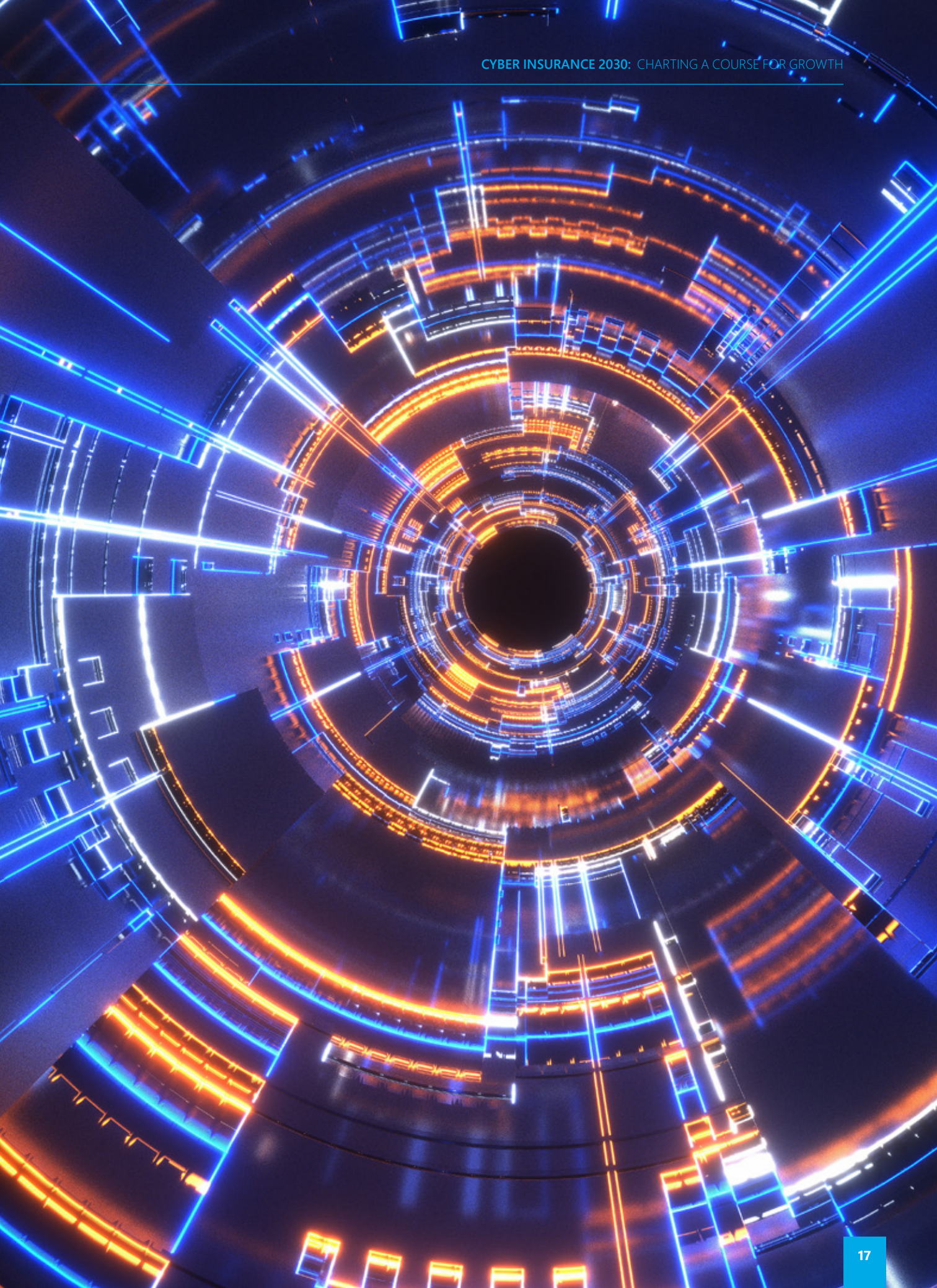
Isabella Gaster
Lockton Re Global Head of Marketing

+44 (0)7795 400981
isabella.gaster@lockton.com

New York

Elizabeth Miller Kroh
Lockton Re Head of Marketing, North America

+1 (445) 248 2228
elizabeth.kroh@lockton.com



Sources

1. "Cyber Insurance: Risks and Trends 2025 | Munich Re," Munich Re, updated March 4, 2025, https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html

2. Ronit Sharma, Nesa Kashyap, 2024. "Cybersecurity Insurance Market Size, Share, Trends, & Insights Report, 2035." Rootsanalysis.com. Roots Analysis. January 20, 2024. https://www.rootsanalysis.com/cybersecurity-insurance-market

3. Beth Musselwhite. 2024. "Beazley Forecasts Cyber Insurance Market to Grow to $40bn by 2030 - Reinsurance News." ReinsuranceNews. October 2, 2024. https://www.reinsurancene.ws/beazley-forecasts-cyber-insurance-market-to-grow-to-40bn-by-2030/

4. Market Segment Report: US Cyber: Pricing Cuts Bring First Ever Reduction in Direct Premiums Written (AM Best, 2025), https://www3.ambest.com/ambv/sales/bwpurchase.aspx?record_code=354887&AltSrc=22&AltServ=640 (paywall)

5. Alex Kimura et al., Insurance Practice Global Insurance Report 2025: The Pursuit of Growth (McKinsey & Co., 2024), https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/global%20insurance%20report%202025/global-insurance-report-2025-the-pursuit-of-growth.pdf

6. "Reality Check on the Future of the Cyber Insurance Market," Swiss Re, updated November 18, 2024, https://www.swissre.com/riskknowledge/advancing-societal-benefits-digitalisation/aboutcyber-insurance-market.html

7. ibid

8. "Don't Put All Your Eggs in One Basket." n.d. Grammar-Monster.com https://www.grammar-monster.com/sayings_proverbs/dont_put_all_your_eggs_in_one_basket.htm

9. Ronald J. Levine, Alan R. Lyons, Barry Werbin, "Cyber Liability Insurance: What to Look for When Obtaining Coverage." 2014. Herrick, Feinstein LLP. October 2014. https://www.herrick.com/publications/cyber-liability-insurance-what-to-look-for-when-obtaining-coverage/

10. "Hosting and cloud computing market size worldwide 2010-2020" n.d. Statista. https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/

11. "Latest 2025 Cloud Solutions Statistics | IT Desk," IT Desk, updated July 10, 2025, https://www.itdeskuk.com/latest-cloud-statistics

12. Richard Betterley, "Maybe next Year" Turns into "I Need It Now" (The Betterley Report, 2014), http://betterley.com/ samples/cpims14_nt.pdf

13. Felix Richter, The Big Three Stay Ahead in Ever-Growing Cloud Market (Statista, 2025), https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloudinfrastructure- service-providers/

14. "From Fiction to Reality: How Latin America Became the World's Most Critical Cyber Battleground," World Bank Blogs, November 28 2024, https://blogs.worldbank.org/en/latinamerica/seguridadcibernetica-en-america-latina-y-el-caribe

15. "The All Risk Cyber (ARC) Challenge – an Assessment to Simplify Cyber Reinsurance | Lockton." 2023. Lockton. 2023. https://global.lockton.com/re/en/news-insights/the-all-risk-cyber-arc-challenge-an-assessment-to-simplify-cyber-reinsurance

LOCKTON®

REINSURANCE

www.locktonre.com

261 Fifth Avenue, New York • NY 10016

The St. Botolph Building, 138 Houndsditch • London EC3A 7AG

#0810_08.25