Brighton
You insure, We ensure

INSIGHTS

APRIL 2025

CRACKING THE CODE OF CYBER RISK: THE THREE ESSENTIALS

INSURING THE AGE OF LONGEVITY

THE HIDDEN COST OF IT SKILLS GAP FOR THE INSURANCE INDUSTRY

Editor's Note

Dear Readers,

The ongoing trade war has cast a long shadow over the global economy, creating a ripple effect that businesses are still struggling to navigate. Rising costs, disrupted supply chains, and the unpredictability of trade policies have left corporations in a constant state of uncertainty.

Companies are rethinking their strategies, and adjusting forecasts as they try to weather the economic storm. What many don't realise is how deeply these disruptions are intertwined with other global challenges.

This interconnectedness is particularly evident in the insurance industry, where the trade war exacerbates several existing challenges as highlighted in this April issue: climate change, cyber security, insuring ageing population, and IT skills gap.

Climate change continues to escalate risks, with the trade conflict hampering investments in sustainable technologies. Similarly, the rising complexity of cyber threats grows more urgent in a volatile economy, where businesses face pressure to bolster their defences.

The rapid ageing of populations in Asia also compounds the pressure on insurers to address the financial and healthcare needs of an older demographic. Finally, the IT skills gap remains a critical issue, as the trade war's disruptions further strain the industry's ability to attract and retain the digital talent necessary for transformation.

Despite these mounting challenges, the insurance industry has historically proven its resilience—adapting time and again to shifting landscapes through innovation, strategic partnerships, and a steadfast commitment to managing risk.

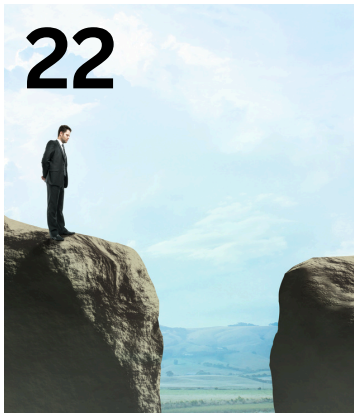
Annie Undikai

Annie Undikai
Managing Editor

Brighton
You insure, We ensure
INSIGHTS

APRIL 2025

IN THIS ISSUE



WWW.BRIGHTON.ASIA

Brighton
You insure, We ensure

Empowering Your Insurance Journey

You Insure, We Ensure

At Brighton, we don't simply offer solutions — we elevate your journey to unparalleled excellence.

Our cutting-edge software, business solutions and dedicated technical support are crafted to propel your business forward in the competitive insurance industry.

Rated LECA1 by RAM Ratings, Brighton represents the pinnacle of capability and performance. We also stand at the forefront of global standards with the successful compliance to IFRS 17.

You insure, we ensure — driving your future forward with confidence and exceptional performance.

Our Solutions:

- Licensing & Compliance
- Accounting Services
- Webbie, Cloud-Based Accounting Software
- Payroll Services
- GST/SST Reporting
- E-Invoicing
- Work Permit Application
- Corporate Tax Submission
- Internal Audit
- Shariah Advisory
- Comprehensive Captive Management
- Run-Off Management
- Serviced Office Facilities

For more information, visit us at www.brighton.asia or scan the QR code

Climate-Proofing the Planet

The Strategic Role of Insurance in Adaptation and Mitigation

Climate change is changing our planet's structure, and with it reshaping global risk. Intensifying natural disasters are not only shifting the earth's landscape and threatening livelihoods; they are also exposing the fragility of the financial and governance systems. As extreme weather events become more frequent and intense, the need for effective strategies to manage and reduce climate-related risks has never been more pressing.

In this evolving risk landscape, the insurance sector has a central role. It can catalyse both adaptation and mitigation, not merely by transferring risk but by guiding behaviour, unlocking investment, and strengthening systemic resilience.

Redefining Adaptation and Mitigation

Climate adaptation involves adjusting systems and practices to minimise the damage caused by climate-related events. This includes measures like constructing flood defences, developing drought-resistant crops, and implementing early warning systems. Adaptation addresses the immediate impacts of climate change, while helping communities cope with its current effects.

Climate mitigation, by contrast, seeks to slow or reverse climate change. Mitigation focuses on reducing greenhouse gas (GHG) emissions, decarbonisation, and large-scale ecosystem restoration. Efforts encompass transitioning to renewable energy sources, enhancing energy efficiency, reforestation initiatives and rethinking infrastructure for low-emission performance. Mitigation aims to prevent future environmental degradation by addressing the root causes of climate change.

While distinct in focus, adaptation and mitigation are interdependent. Adaptation ensures continuity under stress; mitigation reduces future exposure. Both require long-term capital, coordinated policy, and insurance innovation. And are essential components of a comprehensive climate strategy.

However, the challenge is that most capital markets prioritise mitigation over adaptation, despite the urgent need for both. According to the Climate Policy Initiative, only 5.2% of global climate finance in 2022 was allocated to adaptation efforts. Bridging this imbalance requires financial mechanisms that reward risk reduction and build long-term resilience. This is where insurance comes into play.

While distinct in focus, adaptation and mitigation are interdependent.

Insurance As An Engine for Adaptation

Insurance provides a financial safety net against climate-induced disasters, enabling individuals, businesses, and governments to recover more swiftly. By distributing the financial burden of disasters across a broader pool, insurance minimises the economic impact on affected parties. This risk-sharing mechanism promotes greater economic stability and ensures that communities can rebuild and resume their lives more quickly.

Insurers often offer lower premiums or better coverage terms to policyholders who implement risk-reducing measures, such as adopting sustainable farming practices or installing early warning systems. These incentives encourage proactive behaviour, leading to increased resilience against future climate-related events.

In this context, parametric insurance is emerging as a valuable tool for climate adaptation. Unlike traditional policies, it offers fixed payouts that are triggered by measurable criteria, such as rainfall levels or wind speed. This allows for swift financial assistance without the need for lengthy loss evaluations.

In Africa, the African Risk Capacity (ARC) showcases how regional risk pools can deliver prompt and effective assistance. In Mexico, the state of Quintana Roo has taken the initiative to insure coral reefs as natural storm barriers, enabling funding for swift restoration following hurricanes. Meanwhile, in Southeast Asia, small-scale farmers are now benefiting from parametric microinsurance that activates within days of a climate-related event.

However, large protection gaps persist. In cities like Jakarta, high exposure to flooding coexists with low insurance penetration. Factors such as affordability, lack of distribution infrastructure, and low product awareness continue to limit access to risk transfer solutions.

Insurance as a Lever for Mitigation

Beyond adaptation, insurance can drive climate mitigation efforts by shaping investment behaviour and guiding capital toward sustainable assets. As underwriters, insurers have the power to determine which projects move forward and under what conditions. By integrating climate risk into their pricing and capacity decisions, they establish financial incentives that encourage decarbonisation.

The scale of the climate transition is staggering. A joint report by Howden and BCG estimates that $19 trillion is needed by 2030 to reach net-zero, with at least $10 trillion requiring insurance coverage to unlock financing. This spans sectors such as renewable energy, green mobility, and climate-resilient infrastructure.

To support this shift, insurers are increasingly embedding climate considerations into their underwriting practices through a strategy known as impact underwriting. This approach assesses the environmental impact of insured activities and encourages sustainable behaviours among clients. Offering better terms for low-carbon initiatives and excluding high-emission sectors, insurers are reallocating capital costs and shaping behaviours in the real economy.

In a recent pilot exercise, the European Insurance and Occupational Pensions Authority (EIOPA) partnered with 31 insurers across 14 European countries to assess how climate adaptation is incorporated into underwriting. While some progress is evident, the study identified a lack of consistency in how adaptation measures are reflected in insurance contracts, highlighting the need for standardised frameworks.

De-risking Nature-Based Solutions

Nature-based solutions, such as reforestation and wetland restoration, play a crucial role in carbon sequestration and climate mitigation. Yet these projects often struggle to attract investments due to perceived investment risk and uncertain returns.

Insurance can help de-risk nature-based projects. Products such as parametric coverage or performance guarantees can protect against environmental variability and operational setbacks. In the Galápagos, for example, a debt-for-nature swap backed by insurance is directing funds into marine conservation efforts. This initiative serves as a model for how insurance can support large-scale ecological restoration projects.

These mechanisms are still in early stages, but their potential is significant. By quantifying and underwriting ecological risk, insurers can unlock billions in capital for high-impact, nature-positive initiatives.

Internalising Climate Risk

Insurers must also manage their own exposures. As climate risk becomes systemic, traditional actuarial models fall short. Institutions need to assess both physical risks to portfolios and transition risks arising from regulatory shifts, reputational damage, and market revaluation.

Transparency in assessing and disclosing climate-related risks is essential for effective mitigation. To support this effort The United Nations Environment Programme (UNEP) Finance Initiative has published guidance to help insurers assess and disclose climate-related risks.

This includes scenario analysis, emissions profiling, and integration of climate metrics into asset allocation and underwriting. The initiative encourages insurers to integrate climate considerations into their risk management and investment strategies, aligning the industry with global sustainability goals.

Insurance as Strategic Infrastructure

Insurance is no longer just a financial product—it is a mechanism for societal resilience and an enabler of sustainable development. Its reach extends beyond indemnity into behavioural change, investment steering, and risk governance.

But for insurance to fulfil this expanded role, it must be embedded within broader climate strategies. This requires coordination with various stakeholders including governments, development banks, and the private sector. It also demands accessible and inclusive solutions, particularly for vulnerable populations on the frontlines of climate risk.

Ultimately, insurance holds the potential to fortify the global economy against climate change. It can promote adaptation, speed up mitigation efforts, and direct capital to the most critical areas. However, it must transition decisively from being a passive risk carrier to becoming an active risk architect.

CRACKING THE CODE OF CYBER RISK

THE THREE ESSENTIALS

In today's digital economy, where data holds immense value and cyber threats are ever-present, cyber risk has emerged as a top concern for businesses across all sectors. According to IBM's Cost of a Data Breach Report 2024, the global average cost of a data breach has risen to $4.88 million—a 10% increase from last year and the highest on record.

For many companies, a single cyber incident can cause devastating financial, legal, and reputational damage. While organisations differ in size, complexity, and exposure, the foundational steps for understanding cyber risk remain consistent. It starts with a structured approach that addresses potential losses, current cybersecurity measures, and organisational readiness.

Identify Potential Losses

The first step in assessing cyber risk is to understand what is truly at stake. This goes beyond identifying technical vulnerabilities—it involves quantifying the potential financial, legal, and operational impacts of a cyber incident. Two key factors form the basis of this analysis: revenue exposure and the volume and sensitivity of data held.

Cyber incidents are no longer isolated IT problems; they are full-scale business disruptors. When systems go down, revenue stalls. In some sectors, such as retail, logistics, and digital services, even a few hours of downtime can trigger substantial losses.

In 2021, a ransomware attack forced global meat producer JBS Foods to halt operations across North America and Australia. The company paid an $11 million ransom in Bitcoin to regain access to its systems. However, the more significant cost came from operational disruption, halted production, and lost revenue during peak supply chain periods.

While organisations differ in size, complexity, and exposure, the foundational steps for understanding cyber risk remain consistent.

The financial impact of a cyber incident tends to scale with size. IBM reported that companies with annual revenues above $1 billion face average breach costs of $5 million, compared to $3 million for mid-sized firms. For financial institutions, the expenses are even steeper, with approximately $6 million spent on managing data breaches, representing a 22% increase over the global average.

The type and volume of data that a company collects and retains is crucial. Organisations that manage sensitive information, such as personally identifiable information (PII), financial records, or health data, face greater risks. The more sensitive the data, the greater the potential liability.

A stark example is the 2022 cyberattack on Australian health insurer Medibank, which affected around 9.7 million individuals. The breach exposed personal details, including names, addresses, birth dates, and medical claims data. Medibank refused to pay the ransom, leading to the data being released online. The incident triggered widespread public outrage, government investigation, and a sharp decline in customer trust.

Understanding revenue exposure and data sensitivity helps businesses accurately estimate potential losses. This knowledge enables more effective cybersecurity budgeting, tailored insurance coverage, and prioritised risk mitigation investments. Without it, even advanced security measures may not align with actual risks.

Evaluate Cybersecurity Measures

Once the scope of potential loss is clear, businesses must take a hard look at their existing cybersecurity infrastructure. This is not a checklist exercise; it requires a contextual and strategic approach. Cybersecurity must align with the business's size, operational complexity, and specific threat landscape. Without this alignment, even well-resourced programs can potentilly leave serious vulnerabilities.

Cyber maturity differs greatly between small businesses and multinational corporations. While smaller enterprises might not require the complex security systems that larger organisations use, they are still vulnerable to risks and often lack the resources to effectively manage them.

A 2023 Sophos survey revealed that 78% of small and medium-sized businesses affected by ransomware could not fully recover their data, primarily due to poor backup systems and insufficient incident response planning.

Larger organisations have a wider attack surface due to multiple offices, legacy systems, remote teams, and complex supply chains. They need layered defences, including zero-trust architecture, 24/7 security operations centres (SOCs), threat intelligence feeds, and endpoint detection and response (EDR) tools.

But sophistication doesn't guarantee security. Over engineered systems, if poorly configured or inconsistently managed, can produce a false sense of safety.

Threats differ not only based on the size of a business but also on its sector. For instance, a manufacturing company relying on just-in-time production and operational technology (OT) systems encounters different risks compared to a financial institution or a hospital. In the manufacturing sector, ransomware attacks and breaches of OT systems can disrupt production lines, lead to expensive delays, and jeopardise trade secrets.

Healthcare organisations face even higher stakes. Medical records are among the most valuable assets on the dark web, often fetching 10 to 20 times the price of stolen credit card data. Financial institutions, in contrast, are prime targets for credential theft, wire fraud, and phishing schemes.

The Financial Services Information Sharing and Analysis Center reported that financial institutions faced a 130% increase in phishing and smishing attacks between 2021 and 2023. These risks demand strong encryption, secure digital identity protocols, and rapid incident response frameworks.

Another important aspect is ensuring that cybersecurity measures are fit for purpose. While they must be technically robust, their suitability is even more crucial. There isn't a one-size-fits-all solution. What works effectively in a tightly regulated banking environment may be inadequate or unnecessarily complicated for a logistics company with decentralised operations and a limited IT staff.

Ultimately, security is not about having the most tools. It's about having the right tools, properly integrated, and effectively governed. A targeted, risk-based approach that is tailored to the company's actual threat environment is far more effective than one-size-fits-all solutions.

Assess Organizational Commitment

No cybersecurity strategy can succeed without having robust organisational commitment. A well-designed defence against cyber threats is only as effective as the organisation's dedication to integrating security into its culture, governance, and operational priorities. This alignment is supported by two essential pillars: executive support and employee training.

Cybersecurity requires strong leadership, particularly at the board and C-suite levels. The role of top executives in securing their organisations goes beyond approving budgets or signing off on IT policies. It's about understanding the broader strategic risks posed by cyber threats and ensuring that cybersecurity is prioritised alongside other business objectives.

In PwC's Global Digital Trust Insights Survey 2024, 52% of executives recognised a lack of leadership support as a significant barrier to improving their cybersecurity efforts. Without executive backing, initiatives are often deprioritised, underfunded, or poorly implemented. Active involvement from top management is critical—not only in setting the right risk appetite, but also in guiding budget decisions and establishing effective governance frameworks.

The 2017 Equifax breach illustrates the high cost of insufficient executive oversight. The personal data of 147 million Americans was exposed due to unpatched software vulnerabilities. Investigations revealed a failure to prioritise cybersecurity at the leadership level, ultimately resulting in $700 million in settlements and long-term reputational damage.

While technological solutions are critical, human error remains a leading cause of cyber breaches. The World Economic Forum's Global Cybersecurity Outlook 2023 highlighted that over 80% of cybersecurity incidents are linked to human error, whether through phishing attacks, poor password hygiene, or mishandling sensitive data.

The solution? Regular, comprehensive employee training. Employees are often the first line of defence against cyber threats. Hence, their ability to recognise and respond to these threats directly impacts the organisation's security resilience. Phishing simulations, awareness campaigns, and gamified training modules can significantly reduce the likelihood of employees falling victim to attacks.

Ongoing training is crucial in cybersecurity, as it must evolve alongside emerging threats. Continuous learning ensures that employees stay informed about new attack methods, such as spear-phishing and social engineering, enhancing their ability to detect and prevent advanced persistent threats (APTs).

Cyber Risk is a Business Risk

Understanding a company's cyber risk is not merely an exercise in checking boxes, but a strategic imperative. By identifying potential losses, evaluating the suitability of cybersecurity tools, and measuring organisational commitment, businesses can build a realistic and proactive risk profile. This foundation not only supports better decision-making but also enhances the ability to respond effectively when threats arise.

As cyber threats continue to evolve, so too must the frameworks businesses use to assess and mitigate risk. A structured approach is the first step toward resilience.

Phishing simulations, awareness campaigns, and gamified training modules can significantly reduce the likelihood of employees falling victim to attacks.

Insuring
The Age of Longevity

Across Asia, societies are undergoing a demographic transformation that will define the coming decades. The region's population is ageing faster than ever before. In some economies like Japan, and South Korea, the effects of ageing are already deeply embedded. For others such as Thailand and Malaysia, the transition is underway and gaining pace.

This shift presents a profound challenge and an opportunity for the insurance industry. The central question is whether insurers are prepared for a world in which longevity is not just a marker of progress, but also a defining financial and social risk.

Until recently, the needs of older adults have not been a central focus in product design, underwriting frameworks, and insurance accessibility. As populations continue to age, it's increasingly important for insurers to shift toward long-term strategies that thoughtfully address the evolving needs of this growing demographic.

By 2050, one in four people in Asia will be over the age of 60, according to the United Nations.

Structural Shifts, Systemic Impacts

Demographic change is not just another market cycle or trend. It is a profound and irreversible transformation that is reshaping the very foundations of society. Unlike temporary disruptions such as economic downturns or geopolitical tensions, demographic shifts play out over decades. Yet their impact is deeply structural and systemic.

Across much of Asia, life expectancies are rising while birth rates continue to fall. This combination is leading to rapidly ageing populations and a shrinking base of working-age individuals who traditionally support social safety nets. The proportion of people aged 65 and above is expected to double in countries like South Korea and Singapore, within the next two decades. By 2050, one in four people in Asia will be over the age of 60, according to the United Nations.

These changes are creating mounting pressure on healthcare systems, public pension schemes, and critically, insurance portfolios. As people live longer, they often spend more years in retirement, a stage of life that brings a higher likelihood of chronic illnesses, cognitive decline, and the need for assisted or long-term care. This longevity challenge is compounded

by the fact that medical inflation in Asia consistently outpaces general inflation, raising both the frequency and severity of health-related claims.

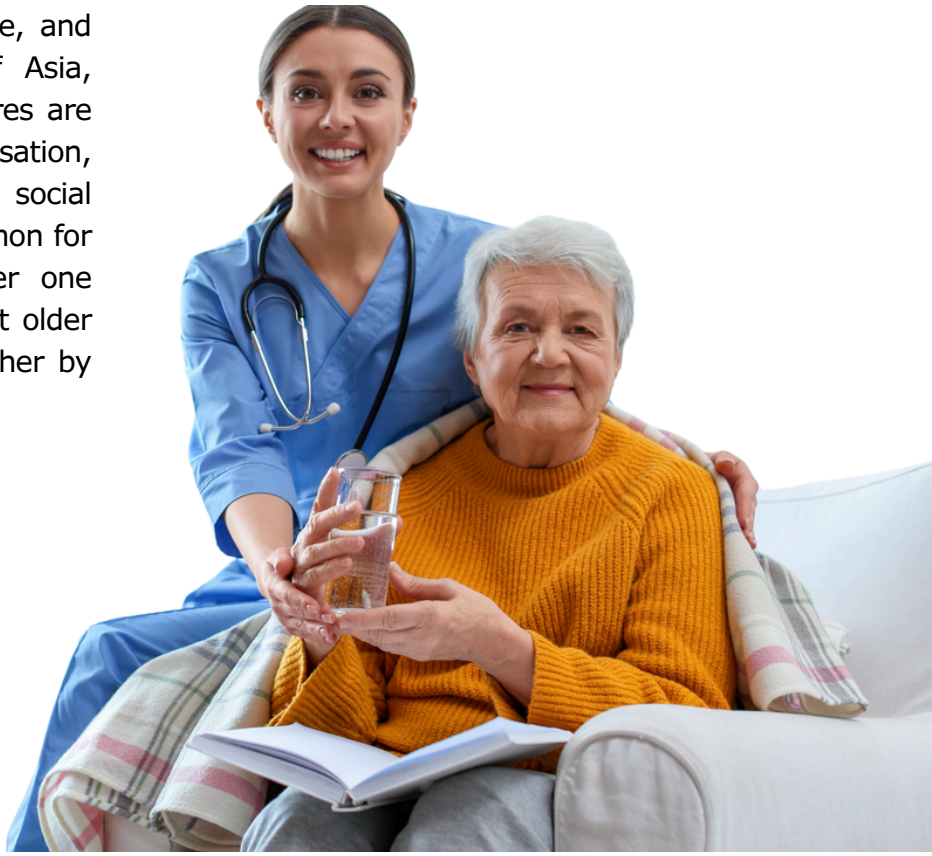
The implications are already visible. Many insurance policies either cease coverage at retirement age or become prohibitively expensive for seniors. Coverage for chronic conditions or long-term care is often limited or excluded entirely. As a result, a significant portion of the elderly population in Asia remains underinsured. Swiss Re reported that the global health protection gap is over $800 billion, with Asia contributing a substantial share of this shortfall.

Cultural Shifts and Changing Lifestyles

Ageing is not only transforming the demographic landscape, but also reshaping the way people live, age, and seek support. In many parts of Asia, traditional extended family structures are evolving in response to urbanisation, economic mobility, and changing social dynamics. Where once it was common for multiple generations to live under one roof, it is increasingly the case that older adults are living independently, either by choice or necessity.

In urban centres, the cultural expectation that adult children will care for their ageing parents is weakening as younger generations pursue careers in different cities or countries.

These changes are contributing to an increase in "solo ageing," a rising population of seniors who are living independently without family support. This demographic trend is creating a greater need for formal care options, including community-based services, assisted living facilities, and professional caregiving networks. At the same time, there is a growing need for stronger healthcare infrastructure and financial solutions to ensure independence and quality of life in old age.



For insurers, this presents both a challenge and opportunity. The industry must adapt by offering flexible in-home care coverage, integrating preventive health services, and providing retirement solutions that offer both income and care access. Policies should also address mental health, mobility support, and digital tools to help seniors manage their wellbeing.

Making Technology Work for Seniors

As insurers innovate and develop solutions tailored for an ageing population, they must also focus on the delivery methods of these solutions. Technology is now a fundamental part of insurance services, but its role in serving seniors requires careful consideration. While older adults are increasingly connected, simply providing digital tools is not enough.

In South Korea, for example, nearly 80% of individuals aged 60 and above are using smartphones, indicating high levels of connectivity. However, the widespread use of smartphones does not necessarily mean that seniors are comfortable or proficient with complex digital applications.

To truly support this demographic, insurers must invest in technology that is user-friendly and accessible. This means developing platforms with intuitive interfaces, simple navigation, and features that are easy to understand.

Technology alone is insufficient for seniors, who often prefer traditional communication or need assistance with digital tools. Insurers should use a hybrid approach that blends user-friendly technology with accessible human support, ensuring elderly policyholders can confidently manage their insurance needs.

Harnessing Data

Data and analytics are reshaping how insurers serve ageing populations, enabling a shift from age-based to individualised risk assessment. With tools like wearable devices, health apps, and electronic medical records, insurers can monitor real-time health indicators and build more accurate risk profiles. This allows for dynamic underwriting and the design of products that reflect actual health conditions rather than generalised age brackets, resulting in fairer and more sustainable pricing.

Wearable devices can monitor key health metrics like heart rate, sleep patterns, and physical activity. They also track indicators of chronic diseases, such as blood pressure and glucose levels. These real-time insights help insurers evaluate a policyholder's health and customise their coverage, offering a more personalised approach to underwriting.

Similarly, health apps that monitor nutrition, exercise, and medication adherence provide insurers with a holistic view of a senior's health, enabling more accurate risk profiling and the development of policies that reflect actual health status rather than simply age.

Predictive analytics, powered by big data, is another key tool in personalising protection. By analysing patterns in an individual's health data alongside broader population trends, insurers can forecast potential risks and better understand the evolving needs of older adults. This allows for the creation of more sustainable pricing models that reflect the actual risk associated with each policyholder.

As health and lifestyle data volume grows, insurers can use this information to create affordable, tailored products for the elderly. Through leveraging data-driven insights, they can develop customised plans emphasising preventive care, chronic condition management, and long-term support, empowering older adults in managing their health.

The ability to personalise coverage in this way shifts the focus from age-related risk to a more nuanced understanding of each individual's health and lifestyle. Rather than penalising older adults for the natural ageing process, data-driven solutions can offer them protection that is better suited to their needs, encouraging greater participation in the insurance market and improving outcomes for the elderly population.

Innovation Through Regulation

Of course, insurers cannot address the challenges of ageing alone. Regulators play a crucial role in shaping the insurance landscape, creating an environment that both encourages innovation and ensures the protection of consumers. Regulatory frameworks must evolve to support new solutions tailored to the specific needs of older adults.

A forward-thinking regulatory approach is essential to fostering the necessary innovation. Regulators should focus on striking a balance between consumer and enabling insurers to experiment with new products and business models. By setting flexible guidelines and frameworks, they can facilitate the introduction of more inclusive insurance solutions.

Japan, for instance, has made significant strides in this area, particularly in the realm of dementia care and telehealth services. The country has embraced products that focus on dementia-specific coverage and services tailored to seniors with cognitive decline, allowing insurers to provide more personalised care options.

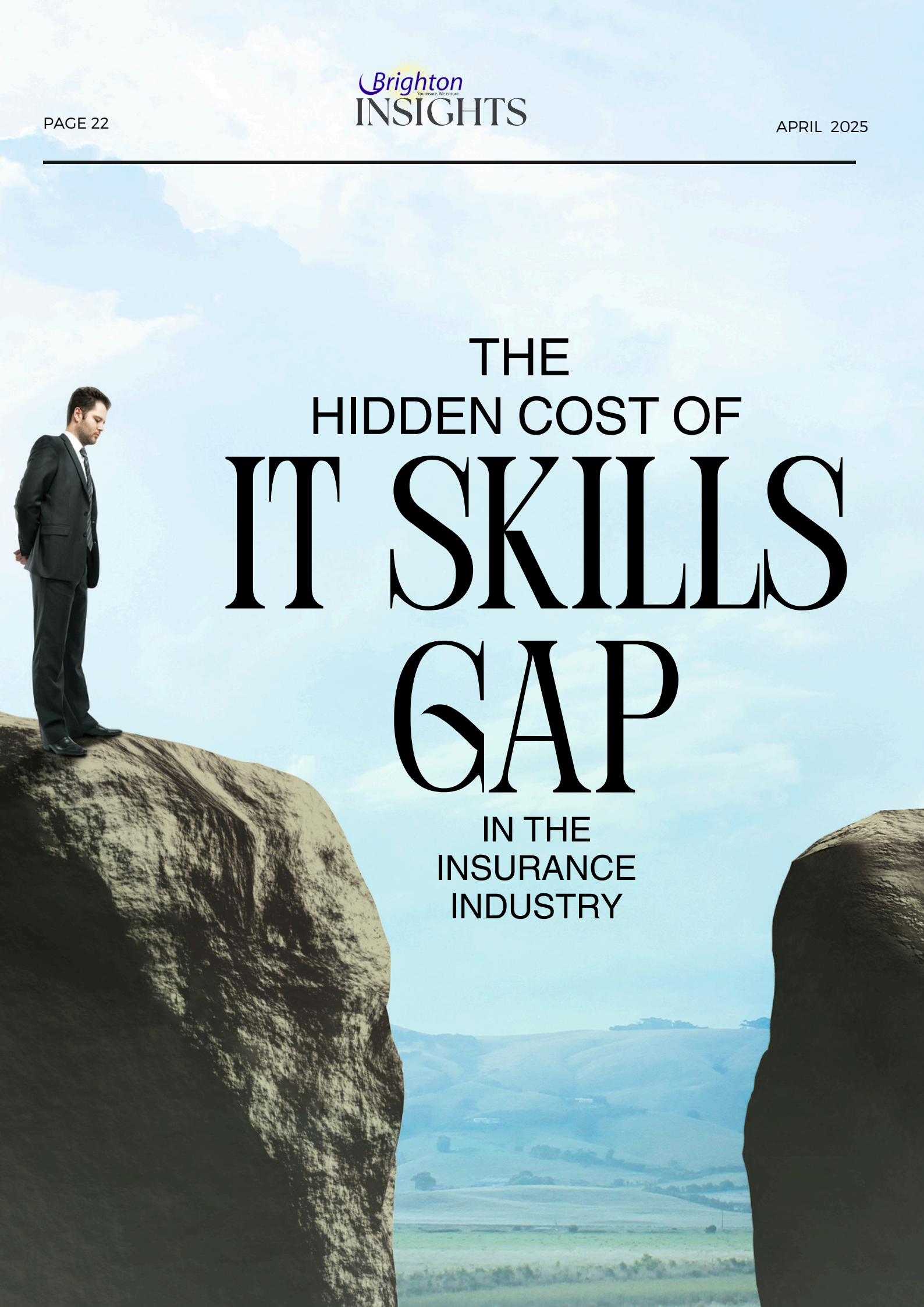
Japan's regulatory approach has supported the use of telehealth technology and enables elderly patients to receive healthcare remotely. It makes accessing services easier and reduces the need for physical visits to healthcare facilities. These regulatory advancements in Japan provide a model for others to follow.

The Silver Economy

The ageing population is not just a challenge to address—it represents a significant growth opportunity. As people live longer, there is an increasing demand for products and services tailored to older adults. The global silver economy is projected to reach $15 trillion by 2030. In Asia, this market is still significantly underserved.

The challenge of ageing requires insurers to rethink traditional age brackets and view protection as a lifelong journey. It emphasises the need for empathy in product design, inclusivity in technology, and responsibility in public engagement. By addressing these aspects, the industry can close the protection gap and establish a new era of relevance and trust.

The global silver economy is projected to reach $15 trillion by 2030. In Asia, this market is still significantly underserved.



THE HIDDEN COST OF IT SKILLS GAP

IN THE INSURANCE INDUSTRY

The insurance industry stands at a crossroads, where digital transformation is no longer optional, but essential for survival. However, many insurers face a persistent, often underestimated barrier to modernisation: the IT skills gap. This shortage of digital talent goes beyond a mere human resources challenge; it has become a significant threat to operational efficiency, cybersecurity, innovation, and long-term profitability.

Systemic Talent Shortage

The gap between available tech talent and the needs of the insurance sector is widening. A survey by Capgemini Research Institute found that 62% of insurance executives globally identified a shortage of skilled tech professionals as a major obstacle to digital transformation.

Across the global economy, the demand for tech skills is outpacing supply. The World Economic Forum projects that by 2027, over 85 million jobs may go unfilled due to skill mismatches, with the digital and financial sectors among the hardest hit.

This shortage is even more pronounced in insurance, which has historically struggled to attract tech talent. Younger professionals often view the industry as conservative, slow-moving, and less innovative. The Global Talent Trends Report reveals that insurance is one of the least sought-after industries for software developers and data scientists.

Compensation adds to the challenge. Insurers must compete with tech giants and startups offering higher salaries, equity, and more flexible work environments. As a result, even when insurers succeed in hiring, retention remains a problem.

Specialised roles, in particular, are the hardest to fill. Insurers are competing for data scientists, AI engineers, cybersecurity analysts, and cloud architects. These are roles that are in high demand across every industry. Emerging technologies compound the issue. The rise of generative AI, blockchain, and real-time underwriting is accelerating demand for new technical skill sets.

Cybersecurity Risks Escalate

Cyber threats are evolving faster than most insurers can respond. As the industry digitises more of its operations, from underwriting and claims to customer portals and cloud infrastructure, it is becoming an increasingly attractive target for cybercriminals.

The gap between available tech talent and the needs of the insurance sector is widening.

Insurers sit on a goldmine of sensitive data: financial records, health information, and personally identifiable details of millions of policyholders. A breach not only compromises this data but also damages trust. Yet, despite the rising risk, many insurers lack the internal expertise to effectively defend against today's threats.

Outsourcing cybersecurity functions to third parties can fill short-term gaps, but it's not a long-term solution. As cyberattacks grow in frequency and complexity, the cost of underinvesting in cybersecurity talent will only rise. Building strong internal capabilities today is the only way to ensure resilience tomorrow.

Innovation Bottlenecks

Innovation suffers most when critical skills are missing. Insurers are investing in AI underwriting, predictive analytics, and digital platforms to remain competitive. However, without the internal capabilities to build, manage, and scale these systems, even well-funded innovation strategies often fail to deliver results.

The Geneva Association reports that only 30% of insurers feel "highly prepared" to adopt emerging technologies. The key barrier? Talent. Many lack the in-house data scientists, machine learning experts, and cloud engineers needed to operationalize new ideas.

This shortfall has real consequences. Usage-based auto insurance requires telematics integration and dynamic pricing models. Parametric climate products depend on real-time data pipelines and automated triggers. These are not one-off builds but require constant iteration. In short, the innovation gap is not about vision or funding.

Mitigating the Hidden Cost

Addressing the IT skills gap requires more than reactive hiring. It demands a multi-pronged, strategic approach. First is to build internal talent pipelines by investing in training and upskilling existing employees

Another critical step is to reimagine employer branding. To attract top tech talent, insurers need to change the narrative. Insurers must showcase real digital transformation efforts, meaningful career paths, and the industry's broader social impact. When positioned as a tech-forward, mission-driven industry, insurance becomes far more appealing to digitally skilled professionals.

By taking proactive steps, insurers can turn the IT skills gap from a hidden liability into a competitive advantage. It's not just about filling vacancies. It's about building the digital muscle needed to thrive in a changing industry.