Brighton NEWSLETTER

You insure, We ensure

Editor's Note

The Russian invasion of Ukraine continues to dominate headlines. With the war grinding into its fourth month, a new Black Swan has joined the flock in the form of geopolitical risks.

Despite being consistently ranked as the top 10 global risks over the years, institutions approach to political risk management is still very much reactive. Article on page 4 dives into the need for geopolitical risk management for business resilience and sustainability.

The economic and market ramifications stemming from the invasion illustrate the high level of interconnectedness of the global economy. The conflict together with sanctions imposed on Russia, have had spillover effect on the global supply chain, oil prices and inflation. With claims expected to rise, especially in aviation sector, the insurance industry is poised for a prolonged hard market against an already turbulent economic backdrop.

Emerging risks emanating from the renewable energy technologies dictate better understanding of the various risk elements related to them. The article on "Emerging Risk in Renewable Energy" highlights some of these risks.

On a brighter note, I am pleased to share that Brighton Management Limited (BML) was recently ranked LECA1 by RAM Ratings, indicating excellent capacity and competence in fulfilling performance obligations. I am proud of the amazing team at BML for this achievement. Well done!

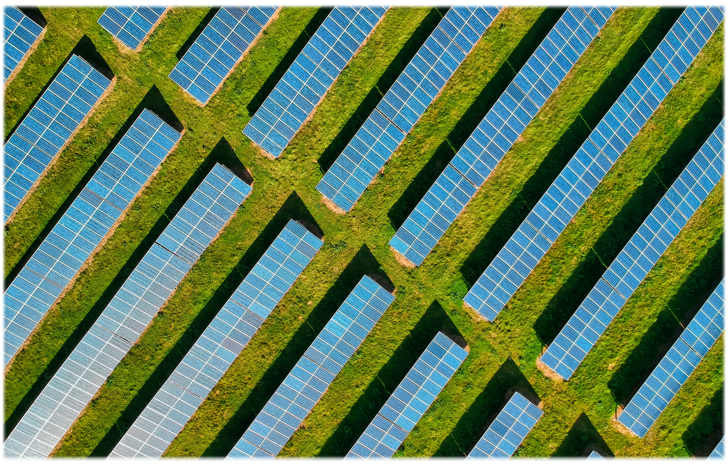
Annie Undikai,
Managing Director

Emerging Risks In Renewable Energy

Across the globe, countries are increasing their investment in renewable energy as part of their commitment to the Paris Agreement on Climate Change, on reducing greenhouse gas emissions by at least 55% by 2030.

In Asia Pacific, countries such as Japan, Malaysia, New Zealand and South Korea have set 2050 as their carbon-neutral targets. China, the world's biggest user of energy and emitter of greenhouse gases, has pledged its commitment to being carbon neutral by 2060. In the western world, the US, UK, and European Union aim to be climate-neutral by 2050.

As the market for renewable energy grows rapidly, new risks are emerging with climate change and cybersecurity risks becoming more prevalent and having wide-ranging impact.



Even though new technologies in renewable energy are expected to accelerate the transition to net zero, climate change presents a growing concern to renewable energy growth. Weather-related events may result in property damages, machinery breakdown, operational failure and disruption in the supply of clean energy. For example, floods, cyclones, and forest fires could damage the components and system of renewable energy technologies. With extreme weather events becoming more frequent and intense, climate change risks pose a threat to the security and reliability of clean energy supply.

Cybersecurity risk has become increasingly complex over the past decade and emerged as a critical risk to the quality and reliability of the power infrastructure. A series of cyber attacks causing disruption to energy supply has given energy companies a wakeup call to the security threats they now face.

A recent case was the cyber attack on Vestas, a Danish wind turbine manufacturer, which saw a data breach of its internal IT infrastructure. Mean while, the attack on a series of Ukraine's power grid substations left a quarter of a million people without power. Solar energy technologies can also be vulnerable to cyber attack through inverters and control devices that are designed to help manage the electric power grid. As the industry continues to expand and operate on increasingly integrated systems and online networks, the threats of cyberattacks and ransomware are becoming even more overwhelming.

Another key concern facing the renewable energy sector is cyber supply chain security. Since large-scale renewable energy relies on smart grids to distribute power efficiently and respond to changing power generation rates, such digitalisation increases the vulnerability of grid networks to attacks. The 2020 SolarWinds supply chain attack highlighted the vulnerability of this connected infrastructure.

The availability and access to rare earth metals such as dysprosium, neodymium, terbium, europium and yttrium, are vital for renewable energy technologies. They are used extensively in wind turbines and electric vehicle powertrains. While solar requires tellurium, which is one of the rarest elements on earth. However, production of these many essential elements is concentrated in just a few countries with China dominating the production (more than 80%). As a result, renewable energy technologies are exposed to supply chain risks for key inputs in the form of rare earth elements.

With the increasing use of renewable sources of power, there is greater demand for a new approach to risk management. Hence, understanding the various risk elements related to renewable energy is vital for insurers respond to the emerging risk profiles of renewable energy technologies.

Implications Of The Russia-Ukraine War On The Global Insurance Industry

The Russian invasion of Ukraine has brought repercussions to inflation, supply chains and cybersecurity. Prices for commodities and energy have remained elevated and volatile. Global supply chain, which is already in a fragile state after being battered by COVID-19, is now under more pressure following the invasion. With Russia and Ukraine accounting for almost one-third of global wheat exports, the ongoing conflict poses serious risks to global food security. All these combined together means higher commercial insurance premiums and decreased capacity across all lines. The conflict has also created new risks for insurers.

According to a report published by S&P Global Ratings, global insurance losses from this war could range from $16 billion to $35 billion, with reinsurers expected to assume 50% of those claims.[1] The report stressed that although specialty lines such as cyber, political risk, trade credit and marine hull insurance are likely to be affected; it is the aviation insurance market that is seen as most exposed. In the wake of the economic sanctions imposed on Russia, aircraft owners have been unable to repossess or salvage hundreds of jets that were leased to Russian carriers.

The conflict has also raised political risks and exposure on investments or assets in both countries. Companies with political risk insurance policies in Ukraine may have claims for losses or damages resulting from political violence or war, whilst companies will most likely submit claims for losses stemming from the confiscation or expropriation of assets by the Russian government as they withdraw from the country. Typically, insurance policies do not cover claims resulting from exiting a market due to an invasion or war. However, it is estimated that the insurance industry's political risk exposure in Ukraine and Russia could be as high as $2 billion.[2]

The invasion of Ukraine has increased the risk of cyberattacks across the globe. Accenture recently reported that there have been numerous ransomware and distributed denial of service (DDoS) attacks after countries imposed sanctions on Russia.[3] As highlighted in its Global Incident Report, attacks on government and national security entities of countries supporting Ukraine has been on the rise. Ransomware groups have targeted a Bulgarian refugee agency after it refused Russian demands to pay for gas in rubles and a German weapons manufacturing city as Germany was deciding to provide weapons to Ukraine. As the conflict continues, possible increase in the risk of systemic cyber attack could potentially lead to higher prices in an already hardening cyber market.

1 https://www.insurancejournal.com/news/international/2022/04/01/660894.htm
2 https://www.businessinsurance.com/article/20220301/STORY/912348228/Political-risk-insurers-face-$2-billion-exposure-to-Russia-Ukraine-war
3 https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/05/ACTI_POV_UkraineCrisis_20220512_TLP-WHITE-CLEAN.pdf

Navigating Geopolitical Risks For Business Resilience

When the World Economic Forum (WEF) published its Global Risks Report 2022, geoeconomic confrontation was placed as the 10th most severe risk over the next decade and 12th in its list of risks that have worsened during the pandemic.[1] The global risks outlook was dominated by environmental and societal threats.

However, with the Russian-Ukraine war intensifying and putting the global economic recovery at risk, geopolitical risks have now become front and centre issues. The heightened geopolitical risks have further contributed to volatility and uncertainty in a market that was already challenged with record levels of inflation, lingering supply disruptions, renewed pandemic-related challenges, and the prospect of rising interest rates.[2]

Dubbed as the new Black Swan event, the Russia-Ukraine conflict highlights the ever increasing important for businesses to have in placed geopolitical risk management. However, many executives are not paying enough attention to political risk management.

In the latest EY Global Capital Confidence Barometer, global executives recognised that geopolitical risks are impacting their strategic investments. However, only a minority of executives (14%) agreed that managing the potential impact of changing geopolitical risks is a main strategic consideration.[3]

The geopolitical crisis that is happening now in Ukraine demonstrates the critical need for resilient and robust organisations that can adapt and flex quickly to make informed decisions and actions. Hence, building a robust geopolitical risk management framework is key to business resilience.

According to research conducted by BCG, companies that have successfully turned geopolitical risk into strategic advantage are those who have applied a highly developed approach to geopolitical risk management with emphasis on opportunity rather than just mitigation.[4]

In today's shifting world with unexpected geopolitical outcomes, a deep understanding of geopolitical risk drivers and their impacts provides a strong foundation for an agile and resilient organisation.

1 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
2 https://content.naic.org/sites/default/files/capital-markets-special-reports-Russia-Ukraine-Oil-Gas-YE2021.pdf
3 https://www.ey.com/en_my/geostrategy/why-geopolitical-risk-management-is-an-opportunity
4 https://www.bcg.com/publications/2021/advantages-of-geopolitical-risk-management-organizations-and-processes

Guidelines on Anti-Money Laundering, Countering Financing of Terrorism, and Targeted Financial Sanctions for Labuan Key Reporting Institutions

The Labuan Financial Services Authority (Labuan FSA) had recently issued Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Labuan Key Reporting Institutions (Labuan KRIs).

Labuan KRIs here refer to all Labuan entities licensed under the Labuan Financial Services and Securities Act 2010 (LFSSA) and Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA), including Labuan KRIs that are undertaking digital financial services.

The guidelines, which will come into effect on July 1, 2022; require all Labuan KRIs to undertake preventive measures against ML/TF offences. The preventive measures include conducting risk assessment, application of customer identification and customer due diligence, submission of cash threshold reports and suspicious transaction reports, maintenance of records and retention of records, implementation of AML/CFT compliance programmes that is reflective of the reporting institution's ML/TF risk profile as well as targeted financial sanctions requirements.

In terms of risk assessment, Labuan KRIs are required to take appropriate steps to identify, assess and understand their ML/TF risks, in relation to their customers, countries or geographical areas, products, services, transactions, delivery channels, and other relevant risk factors.

Meanwhile the intensity and extensiveness of risk management functions shall be in compliance with the risk based approach and proportionate to the nature, scale, and complexity of the Labuan KRIs activities and their ML/TF risk profile.

Labuan KRIs are required to have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products, services and business practices. This shall include new digital assets, delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

The guidelines also set out the requirements for managing targeted financial sanctions involving customer and/or related parties that include freezing, blocking and rejecting and reporting of a positive match. This should be in compliance with the United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

Labuan KRIs must also undertake customer due diligence (CDD) measures, prior to entering into a business relationship or providing services. This shall include identifying and verifying the identity of the customer, the authorised person acting on behalf of the customer, and the beneficial owner. Labuan KRIs are required to also understand and obtain information on the purpose and intended nature of the business relationship, where relevant.

Brighton Celebrates Special Olympics Labuan Athletes At Hari Raya Open House

After more than 2 years of pandemic restrictions, Brighton Group Limited celebrated its Hari Raya Open House with staff, clients, regulators and other members of the business and financial community in Labuan IBFC. The event was clearly a wonderful opportunity to catch up, network and strengthen bonds. Guests who attended the open house were treated to a wide spread of mouth-watering local delicacies and festive delights. In the spirit of the celebration, Brighton hosted 31 athletes from the Special Olympics Labuan, together with their volunteers who are also people with disabilities.

In the welcoming speech by the Managing Director, Ms Annie Undikai expressed her joy and delight to be able to physically get together again and continue the unique tradition of hosting open houses during festivals. She said "while the pandemic has prevented us from interacting face to face and forced us to adapt to new norms in unprecedented ways; it actually showed our resilience, flexibility, and capability when faced with extraordinary challenges."

Adding that the pandemic had demonstrated the power of collaboration, she encouraged everyone present to continue working together as one collective voice to bring about changes and growth in Labuan IBFC.

She also expressed her appreciation and gratitude to all staff at Brighton whom she said had risen above various challenges during the pandemic and spared no effort in ensuring the continuity of business operations.

Ms Annie Undikai also thanked clients for their continued business and trust, and expressed her upmost appreciation to Labuan FSA for their swift response in ensuring uninterrupted business and market operations in Labuan IBFC during the pandemic. She added that the temporary reliefs provided had allowed players to focus on their business continuity measures and addressed challenges associated with the pandemic.

In a special announcement, Ms Annie Undikai shared that Brighton Management Limited (BML) had recently obtained a rating of LECA1 from RAM Ratings, which is the highest on a scale of six grades and indicates excellent capacity and competence in fulfilling performance obligations.

She commented that this rating underscores BML's capabilities and competencies in providing insurance management services to both licensed insurance and insurance-related entities in Labuan IBFC. As the largest insurance/underwriting manager in Labuan IBFC, this rating reflects BML's strengths and reputation as a credible insurance and underwriting manager.

Brighton

You insure, We ensure

HAPPY GAWAI
&
KAAMATAN

Wishing you a wonderful celebration. May your year be filled with peace, prosperity and happiness.

From all of us at
Brighton Group Limited