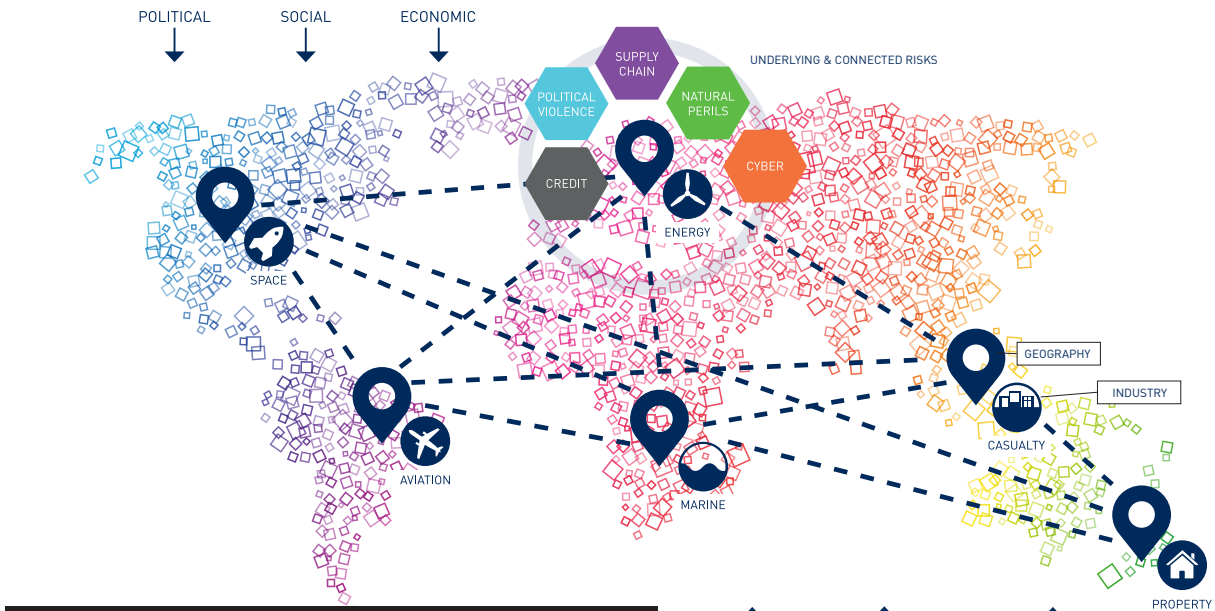

www.russell.co.uk

THE ERA OF LIABILITY

In the wake of the flooding in Thailand five years ago, computer hard disc prices rose to an average of $66 in one quarter, a 28% leap from the $51 average price in the previous quarter. Thailand assembles about 40 percent of the world's hard drives, and if one accounts for drive component manufacturing, it's the global leader. This clustering of a highly specialized industry has become common in the global trend toward lean supply chains and just-in-time manufacturing.

Lloyd's estimated at the time that it was liable for $2.22bn (£1.4bn) of net claims from the floods while combined estimates from other insurance groups, including Swiss Re and Munich Re put the total cost at $15bn to $20bn. The unique aspect of the Thai floods is that building damage was largely superficial in comparison to the machinery and business interruption losses incurred by manufacturers in the region.

This is significant because there is an increasing awareness that global interdependencies fostered by corporate connectivity, the internet of things (IoT) and Industry 4.0 are moving re/insurance companies and the corporate clients into a new era of liability. In this white paper, we ask what are corporates and their re/insurance counterparties' true underlying exposures and what solutions can be brought to bear on the issue of multi-class liability events?

Liability Era

For many years, the global re/insurance P/C market has been fixated with geo coding and a property-led debate. That is understandable to an extent because property is and will continue to be a valuable asset. Russell Group Limited is convinced, however, that we are in a new era of liability, in which property damage will be a secondary consideration.

In this new corporate environment, emerging technology is causing a change in consumer engagement, while companies are revising their strategies to stay relevant to a younger internet-savvy consumer base. The on-demand economy and peer-to-peer market is young, but it is expanding fast. The likes of Uber and Deliveroo are breaking the mould of traditional bricks and mortar stores and look set to test the limits of liability exposures.

This new environment poses new risks. Uber recently offered up a test case of the new era of liability that highlights insurance grey areas. Uber, for example, offers drivers insurance, but some uncertainty surrounds drivers' "contractor" status, and when this coverage is in effect.

According to reports, an example of the issues that can arise occurred when a San Francisco Uber driver killed a six-year-old girl because he was distracted while logging into his Uber app. Uber's said that as there was no passenger in the vehicle,

the car driver was not employed by Uber's at the time, which meant that the company was not liable. Such cases are bound to rise significantly.

Augmented and Virtual Reality (AR and VR) technologies are also literally creating a "new dimension of risk" according to a new report by KPMG. AR and VR technologies are anticipated to generate potential losses to the value of US$20 billion by 2020. Consumers will increasingly suffer accidents whilst playing AR games and companies will increasingly become responsible for securely storing ever more sensitive information, such as location data.

Falling off a Liability Cliff?

As the technologies evolve companies using them will need insurance for personal accidents, business reputation damage or enhanced data security cover. Whilst insurers are unlikely to cover the entirety or even most of this US$20bn risk, there is a huge new market at stake. Paul Merrey, KPMG Global Strategy Group Insurance Partner, comments: "There are some obvious risks associated with AR and VR technologies which aren't currently covered by insurers. Pokémon Go, for example, was a huge success but there were reports of some serious personal accidents, in California two distracted gamers fell around 50ft off a cliff.

"The uses of augmented and virtual reality are only beginning to be understood. It has potential well beyond gaming - it could revolutionise how insurers run their own businesses. Imagine a world where an oil rig risk assessment could be done through virtual reality goggles with an oil rig worker on the ground and the insurer at his desk in London."

A New Era of Super Liability

In this new era of liability therefore what are the big super events that people are most worried about? In Offshore Energy, we recently witnessed an event with no property damage, just a malfunctioning unit that resulted in a Business Interruption claim. Meanwhile, safety concerns resulted in the abandonment of the newly-constructed Yme oil platform in the North Sea, which led to a reported claim against insurers of $1.3bn towards the end of 2014.

These are real instances but what other potential scenarios are out there? What about big pharma, for example? You would think that the big pharmaceutical companies would manufacture their own drugs but they are actually outsourcing them to China and India along with the R&D too in some instances. Active Passive Ingredient (API) leaders are increasingly becoming second tier pharma companies that are South African, Mexican, Indian, and Chinese.

For example, a drug is an API mechanism in a capsule which is being branded by the pharma company but the key ingredient is being manufactured by somebody else even when the big pharma company has the copyright. That drug needs to be shipped across the planet in cargo containers, thereby introducing transportation as well as supply chain risks from a liability perspective to pharmaceutical companies.

According to a recent Contract Pharma survey, when asked if there is an increasing demand for outsourcing this year, 80% of respondents answered yes. The number one reason for this, according to 41% of respondents, is to focus on core competencies. Pharmaceutical company sponsors say they are also outsourcing more because they are virtual (30%), while a significant number say they lack the capabilities in-house (14%). Sponsors say they are also using contract service providers as secondary suppliers, with 43% saying they are using them for APIs, 36% for clinical materials and 28% for commercial supply.

At the same time, there is pullback in overall R&D spending by pharma and biotech and a growing tendency for these organisations to outsource their innovation. Several risks exist in the outsourcing relationship, explains Robert Schiff, president of Schiff & Company, a consultancy specializing in regulatory affairs and pharmaceutical manufacturing. This risk applies to outsourcing the manufacturing of raw materials, active pharmaceutical ingredients (APIs), excipients, packaging materials, and the finished drug product.

Shift to Multi-Line Covers

We are entering an era of hyper connectivity with new rules, opportunities and risks for (re)insurers and corporate risk managers. As Russell Group Limited has mentioned in previous papers, the connected cyber risk is also a mounting concern and one that is being fuelled by today's increased geo-political tensions that some reports attribute to state sponsored cyber hacks. The risk affects everyone in the insurance value chain – major corporates, their insurers and their reinsurers.

Insurance companies see this as an opportunity. Aon, for example, recently launched an enterprise-wide cyber product that can provide a broad range of coverage in a single policy offering up to $400mn in capacity. The Aon Cyber Enterprise Solution covers property, products liability, supply chain risk, technology platforms and information/ physical assets, as well as offering defences against privacy and security liability in an integrated offering.

The new product can address exposures to property damage from a network security breach;

products liability coverage for "internet of things" risks; BI and extra expenses from a systems failure; and contingent network BI for IT vendors and the supply chain. It can also incorporate cyber terrorism coverage and indemnify against EU General Data Protection Regulation fines and penalties, where insurable.

Shift to Multi-Line Covers is a Risk

Adriano Bastiani from Munich Re, however, is surprised about the growing enthusiasm in the insurance market for multi-line policies that bundle together new and difficult exposures to risk and covers them under a single contract with a common aggregate deductible and policy limit. A common multiline contract combines property and casualty risks together into a single policy.

According to Bastiani: "We are surprised about this shift towards multiline covers in this class of business where you end up covering property damage, business interruption, and bodily injury under one cyber product. A multiline product could be triggered by variety of different perils within a cyber incident. It could be a robot killing somebody. A car manufacturer would buy this product under one cyber policy so if somebody is hacking their software for driving assistance in the car and there is a fatality this policy will pay for that. It could be the ABS. This concept is still untested in the market and brings together long tail, short tail and very different exposures under one product. It can certainly not be written like a standard property or casualty insurance cover for a client, but requires a team of highly specialised underwriters an a very sophisticated underwriting process. It will take a brave liability underwriter to write this product alone!"

Is Cyber Cat the New NatCat?

Bastiani says: "I have been asked before is cyber cat the new NatCat? Well the answer is yes and no. One of the hottest topics in cyber at the moment is failure of external networks, which is not covered in treaties - for good reasons. This would be the worst case scenario for the market. Just imagine the internet being out of service for 12 hours due to a cyber-attack. For the internet, you have a number of US, European and Asian nodes. If you can hack one of these nodes you can probably turn off the internet worldwide. This would be a cat scenario but you can't insure it because you cannot limit it to a certain amount. Every policy would be concerned.

"The same applies to power grids. If you have a power outage in Germany there is a big likelihood this will extend across Europe but the footprint of such an event cannot be defined. For NatCat scenarios, however, we have a footprint for how such events emerge; it is not always the same but it always follows a certain pattern that you can model. If you have internet outage it is not limited to a footprint – all potential policies are in place."

Vulnerable Industrial Control Systems

Three utilities companies in the Ukraine, the Israel National Electricity Authority and most recently a German nuclear power plant have suffered cyber-attacks in recent months according to Allianz Global Corporate and Specialty. As energy, transportation or telecommunication companies, but also the manufacturing sector, become more reliant on automation, robot technologies and digital networks of connected devices, they are also increasingly vulnerable to cyber-attacks. Rather than stealing data, cyber-attacks against critical infrastructure and manufacturers are more likely to target industrial control systems (ICS) to manipulate or shut-down operations.

There is growing concern about the vulnerability of Industrial Control Systems, which are used to monitor or control processes in industrial and manufacturing sectors. For example, there were 295 recorded ICS cyber incidents in the US last year – up 20%. A cyber-attack against an ICS could result in physical damage, such as a fire or explosion, as well as business interruption (BI), says Nigel Pearson, Global Head of Fidelity, AGCS. "A number of ICS are still used by manufacturing and utilities companies today, which were designed at a time before cyber security became a priority issue."

Meanwhile, in a world of increased business automation, often the greatest cyber risk companies face is not data security, says NAS Insurance Services. Rather, "businesses that rely upon computers and software to manage their refineries and pipelines, power grids, and a wide range of manufacturing systems face enormous cyber risk should their control systems fail."

According to a report by Norton Rose Fullbright, maritime industries are also becoming increasingly reliant on technology and the use of data. The report says: "The threat is a real one, as demonstrated by a prominent example of a criminal hacking of a port, which occurred at the Port of Antwerp in 2011. In this case, hackers remotely accessed the Port's network to identify containers in which they had hidden illegal goods, and removed the goods before they were searched by authorities. This was done by sending Trojans to the port's staff, resulting in the port's IT system being infected, as well as key logging devices being installed to capture the passwords of port employees. The criminal enterprise is thought to have continued for two years."

Connected liabilities from the same event are rising in today's new era of liability, whilst liabilities that are currently uninsured are also on the rise. This unknown risk can be referred to as dark risk. Corporate risk managers are complaining that their insurers don't offer products that address their growing liability need. Meanwhile the insurance carriers are saying we can offer these products but the risk managers are not outlining the requirement. There is disconnect, which needs to be addressed and which means there is a role to play connecting insurers with their clients. It is also evident that the re/insurance market needs to change to address the disconnect between insurers and reinsurers and even disconnects within single insurance entities that have a global footprint.

Bastiani says: "I think that business models everywhere need to be re-thought, the fourth industrial revolution is a game changer for the insurance industry and the challenge for the insurance industry is to stay on top of these developments. If you want to serve your clients in the real economy, understand how his business model is being transformed to offer the right product. This is the biggest challenge for us."

Big data has been pushed by the C-suite, but the biggest problem is that the C-suite operates on a top down capital allocation model, whilst the underwriting is actually grass roots bottom up. The longer this soft market carries on the further those two models are going to unravel. A more collaborative approach is required.

Collaboration is Key for Addressing Connected Liability Risks

Modern liability insurance is expanding at a rapid pace. The risks and range of related liability products and requirement are also evolving at remarkable speed. Through the process of developing this white paper, we believe that the key to addressing such a fast-moving risk is constant collaboration among key re/insurer stakeholders and their direct corporate clients.

We need to build a more robust risk management framework that can be extended to insurance underwriting for new forms of liability risk. In this report, we've been able to identify several scenarios of organizations that might be impacted in our new era of liability. With these insights, we believe that a marriage of C-suite sponsored investment in new forms of liability modelling and data-led bottom up underwriting inputs can benefit companies and help them identify vulnerabilities in their organization whether that be a FTSE 350 corporate or its re/insurance partners.

In addition, as best practices become shared and companies become more familiar with the risk modelling process, we would hope that greater preparedness would lead to more favourable insurance pricing, better control of peak accumulations and re/insurance aggregate management. We hope that this white paper has prompted you to consider the broader liability risks facing companies today and helped you to identify new opportunities for improving your security programmes and risk management efforts.

Russell Group is a leading risk management software and service company that provides a truly integrated risk management framework for (re)insurance clients operating across the specialty classes through its ALPS suite of products.

Underwriting risk is, or should be, the primary concern of specialty (re)insurance companies in quantifying portfolio exposure, pricing risk, optimising reinsurance purchase and evaluating the amount of capital needed to support the portfolio. Russell through its ALPS product provides an underwriting risk framework which delivers a complete and integrated understanding of underwriting exposure, capital utilisation and portfolio return on equity.

If you would like to learn more about Russell Group Limited's ALPS solution for aerospace loss exposure management, please contact sbasi@russell.co.uk or rborg@russell.co.uk