DAC BEACHCROFT

Technology
Predictions 2022

For further information or enquiries, please contact:

Tim Ryan
Partner
tryan@dacbeachcroft.com
+44 (0) 207 894 6978

Hans Allnutt
Partner
hallnutt@dacbeachcroft.com
+44 (0) 207 894 6925

AVIATION

1. Drone deliveries: a buzz in the sky

We remain confident that drone deliveries will make a buzz in the UK skies, albeit on a slower trajectory than we previously forecast. In the medical field, last year saw drones complete deliveries 17km beyond visual line of sight (BVLOS) between hospitals in Argyll and Bute in the Scottish Highlands. This was a first phase of a long-term project to integrate drone operations into NHS supply chains. In April 2021, the UK Civil Aviation Authority (CAA) authorised a Sussex-based drone company to begin flight operations BVLOS at three locations in the UK, in a move heralded by the CAA as *"[firing] the gun for the next phase of growth of the drone industry."* Then in May 2021, Royal Mail announced the start of drone deliveries from the UK mainland (near Newquay) to the Scilly Isles. Elsewhere in the world, drone package deliveries are already a reality, and on a significant scale. In 2020 some 800,000 medical supplies and products to include blood samples and vaccines were transported by drones in Ghana and Rwanda. The service, a partnership between a US start-up and governments, began operations in 2016. In the arena of drone package deliveries, Africa is a continent to watch. From an aviation insurance perspective, higher levels of drone traffic in our skies dials up heightened potential for accidents and incidents and associated insurance liability claims.

CASUALTY

2. Regulators will demand more vigilance on cyber security threats

The HSE will be raising operators' focus on cyber security to ensure appropriate protection against major accidents especially within the UK's major hazard industries. The HSE will be looking for greater integration of IT and industrial control systems and requiring greater precautions against cyber attacks on systems delivering major accident controls. The HSE will be undertaking a programme of inspections at targeted major hazard sites to assess risks that may impact industrial control systems.

3. The HSE will focus on a safe transition to a carbon neutral economy

As part of Build Back Greener, the HSE will be supporting the delivery of the Government's 10-point plan for a green industrial revolution and a safe transition to a carbon neutral economy. The HSE will also be working with the Government and other stakeholders on new and emerging technologies in the workplace to reduce risk from activities such as 3D printing, systems involving artificial intelligence and the use of drones. In 2022 the HSE will focus on a review of its regulatory framework as it applies to current and future net zero activity – identifying the policy, regulatory, operational and evidential steps needed to support the innovation and development of new technology during the transition to net zero.

CONSTRUCTION AND ENGINEERING

4. The time for construction technology

The construction industry is set to embrace a brave new world, with the increasing and broader use of technology. Beyond BIM and CAD drawings, designers are now using virtual and augmented reality, enabling developers to walk around their future buildings in a 3D environment, so they may truly understand the space they have procured. Monitoring and auditing the progress of any development and the improvement of safety risks on site are improving construction risks through the use of machine learning and artificial intelligence. Developments in wearable technology are also gaining ground. Smart wear improves safety and performance by monitoring fitness and worker fatigue and supporting continued working in adverse weather conditions through heated jackets and temperature cooling vests. Insurers have much to gain from the support of modern construction businesses, with improved safety records and defect free buildings, built by a technology assisted workforce.

CYBER AND DATA RISK

5. Deepfake technology will be used to compromise corporate security

The widespread use of communication platforms such as Zoom and Microsoft Teams, and the increased propensity for senior leaders to release audio and video in corporate communications during the COVID pandemic, has provided the perfect opportunity for cybercriminals to carry out impersonation fraud via sophisticated "deepfake" scams. Deepfakes are generated by machine learning, a type of artificial technology, to synthetically create or modify images, video and audio recordings in a hyper-realistic way. Most often, this is to convincingly imitate someone, to portray them as doing or saying something they did not do. Dark web tutorials are educating criminals on how best to use this technology for maximum gain and impact. As most organisations have increasing awareness and are improving defences to protect against phishing emails which seek to obtain credentials or misdirect financial payments, cyber criminals could use deepfake technology to continue their scams in a novel and unexpected manner.

6. Ransomware and extortion attacks will continue to cripple global businesses

Ransomware attacks are crippling businesses globally. The attacks use malicious software to encrypt systems and data in order to deny their availability, and are increasingly accompanied by the theft of data. Attackers seek to extort a ransom for decryption as well as the non-publication of stolen data. Cryptocurrencies, allowing untraceable money transfers, have exacerbated the problem, making it often impossible for law enforcers to identify cybercriminals. Governments are taking action, including issuing sanctions over criminal groups and cryptocurrency exchanges, but so far these measures are only a small drop in the ocean in the fight against the cyber criminals. The impact of these attacks can be catastrophic with losses arising from business interruption, the cost of restoring data and IT systems, and reputational damage. Businesses have no guarantee that data will be deleted if the ransom is paid. Strong cyber security measures, reliable and rehearsed ransomware recovery plans and appropriate insurance will help mitigate against the risk of ransomware.

7. Evolving ransomware threat actor tactics require new breach responses

2020 was the year when data exfiltration accompanied ransomware (double extortion) became a mainstream approach by cyber criminals. 2021 saw even more methods of leverage used by attackers to force organisations to pay out: extorting employees, threatening customers, making personal calls to board members, and distributed denial of service attacks have all been used. 2021 was the year of 'triple extortion'. As the arms race continues between threat actors and law enforcement, the evolution of threat actors' tactics has sped up. Threat actors have engaged in PR stunts and large scale attacks that are, more often than not, affecting more than one organisation. We will continue to see threat actors exploiting the backdoors provided by managed service providers to achieve their objectives. It is likely that further tactics will be deployed, including where the integrity of data has been compromised rather than simply the confidentiality or availability of that data. When responding to ransomware, therefore, a wide variety of tools, approaches and expertise is required to mitigate against these new tactics.

8. Extended EU rules on cyberattacks leave insurers uncertain over ransom payments

On 17 May 2021, the European Council extended the decision on restrictive measures against cyberattacks that threaten the European Union or its Member States for one further year. The aim of the decision is to establish a common framework for measures by the Member States against persons, entities and organisations responsible for or supporting cyberattacks or attempted cyberattacks against critical infrastructures within the EU. The subject of the resolution is not only the freezing of assets, but also payment bids to certain persons, entities or bodies and organisations mentioned in the resolution. The resolution does not contain a general prohibition on the payment of ransoms or on the insurability of ransoms. This question remains open and is currently the subject of controversial discussions in many Member States, including Germany. At the same time, many insurers are considering whether they want to offer insurance for ransoms at all.

Contributed by our German Legalign partner, BLD.

9. Germany enacts new law on IT and cyber security in companies

Germany revised its IT Security Act in summer 2021. The law previously targeted the IT security of so-called critical infrastructure operators (energy providers, banks, insurers, public healthcare, etc.). Now, however, companies of "special economic interest" will also have to comply with the requirements of the law. It is currently unclear which companies fall under this category because further implementation of the law is still taking place. The IT Security Act contains organisational requirements for companies. On the basis of this, German authorities have issued detailed specifications for corporate networks, their structure, set-up, monitoring and IT security. These specifications are an important basis for the question of what the respective "state of the art" of a network is – which is of course also of importance in insurance matters.

Contributed by our German Legalign partner, BLD.

10. Is data breach cover in cyber insurance a "sleeping giant"?

At the end of November 2020, the EU Parliament approved the Directive on Representative Actions for the Protection of the Collective Interests of Consumers (Directive (EU) 2020/1828). The Directive subsequently came into force on 25 December 2020. The Member States now have until 2023 to transpose the regulations into their laws. The Directive raises some new issues for German procedural law. In particular, it will enable consumer groups and associations to sue directly for damages including lump-sum compensation for non-material damages. While an individual may only seek to recover a small amount, representative claims are expected to significantly increase the risk of lawsuits and the sums claimed against companies and their insurers. The Directive also introduces a "discovery" procedure similar to the discovery procedure in the US, and the group or class will have the right to file a request for the disclosure of evidence. With the exception of antitrust law, German civil procedural law does not yet have a disclosure or discovery procedure. In Germany, there is also a parallel discussion as to whether there needs to be a low value threshold for damages under Art. 82 GDPR and it is expected that this question will be submitted to the ECJ sooner or later.

Contributed by our German Legalign partner, BLD.

DIRECTORS AND OFFICERS AND FINANCIAL INSTITUTIONS

11. Technology used to produce deepfakes will be employed by hackers to evade AI fraud prevention measures

The most well-known deepfakes are synthesised images of a person in an existing image replaced with someone else. However, there are early warning signs that the same techniques are being used by hackers to manipulate customer data held by financial institutions and other organisations. Those companies use artificial intelligence (AI) to spot and prevent fraudulent transactions – the systems highlight unusual or unexpected transactions by recognising normal activity on an account. By manipulating the data, hackers can make what would be a fraudulent transaction look common place for a particular customer and so evade AI fraud prevention measures.

INSURANCE WORDINGS

12. Policy wordings for autonomous vehicles play catch-up

Year on year we move towards increased automation, as the pace of development accelerates. Historically, the focus has been on the regulatory landscape and the functionality of autonomous vehicles. This is now evolving, as the complexity of data protection and cyber issues can no longer be ignored. It is no surprise then, that the focus for the motor insurance industry is on policy wordings and in particular, consideration of data protection, cyber and product liability exposure. We are seeing clients in the motor insurance industry actively looking at their policy wordings to consider whether they have the scope of cover and clarity required. DACB has established an autonomous vehicles policy wordings focus group combining our data protection, cyber and policy wording expertise and are here to support clients in this fast changing landscape.

MARINE, ENERGY AND TRANSPORT

13. Will electronic bills of lading trade one problem for another?

On 30 April 2021, the England and Wales Law Commission published a consultation paper asking whether electronic trade documents should have the same legal standing as their paper equivalents. Many laypeople would be surprised to know that the vast majority of international maritime trade is still administered on physical pieces of paper. Advocates of modernisation have been pushing for industry wide digitisation for many years, yet relatively few jurisdictions recognise the validity of electronic bills of lading. Possession of a physical bill of lading is sufficient, not only to evidence the existence of a contract of carriage, but also to establish title to the goods in question. However, English law does not currently recognise that electronic documents are capable of being "possessed" in the same way. Having numerous versions of the same bill on different hard drives around the world prevents them being exclusively controlled by one party before being fully divested on transfer. The creation of distributed ledger technology, such as blockchain, may be the answer to this problem as parties will be able to evidence when they received possession of an e-bill and what changes were made along the chain. It is hoped that this would avoid a great deal of the fraudulent amendments that can happen along a global supply chain. It is also hoped that moving away from a paper only model would significantly reduce the ecological impact of the estimated 28.5 billion paper trade documents created every year, as well as speeding up transactions. Critics, however, will say that an electronic document is much more susceptible to outside interference from malicious agents (cyber risks) and the industry would be trading one problem for another. But with the theorised efficiency savings running into the billions of dollars each year, it seems likely that electronic bills will become commonplace in the near future.

14. Green hydrogen will fuel a new energy insurance market

Analysts have estimated the green hydrogen market could be worth €10 trillion by 2050. Given the market potential and the numerous green hydrogen projects already planned, including the US$36 billion Asian Renewable Energy Hub in Australia's Pilbara region, energy insurers should expect to see a significant increase in global demand associated with constructing and operating green hydrogen plants and pipelines. Green hydrogen developments are a positive news story for the world, particularly in the wake of the IPCC's 2021 Climate Change Report. However, the new technology comes with risks that underwriters will need to carefully consider. For example, green hydrogen is highly flammable and is difficult to store and transport. While these issues are being addressed through extensive global research and development, insurers will need to stay on top of these developments. This includes monitoring how the marine industry embraces ammonia, a fuel derived from green hydrogen, as a potential transportation solution.
Contributed by our Australian Legalign partner, Wotton + Kearney.

15. Cyber piracy a key concern for shipping companies

Cyber risk is now front and centre for the shipping industry following high-profile incidents, such as the Petya cyber attack, the 2020 cyber attack on CMA CGM's systems, and the ransomware attack against the Colonial oil pipeline in the US in May 2021. The issue is also a key focus of regulatory guidance from the International Maritime Organisation. With the increased interconnectivity between vessels and shore based systems, use of automated systems and the development of unmanned or autonomous vessels, the spectre of a significant physical damage loss at sea looms larger. To date, most cyber-attacks in the shipping industry have focused on onshore operations, but it is conceivable that cyber criminals could take control of vessels at sea. A common vulnerability is the industry's generally low level of preparedness for cyber incidents, including low levels of risk awareness, ineffective procedures and high levels of human error in offshore security breaches.
Contributed by our Australian Legalign partner, Wotton + Kearney.

MEDICAL MALPRACTICE

16. Telemedicine technology is here to stay

COVID-19 significantly reduced the frequency of face to face consultations and caused a seismic shift to telemedicine, particularly the use of video consultations, which is here to stay. Telemedicine technology reduces the spread of infectious diseases in clinics and enables swift access to healthcare at a distance with associated cost and time-saving efficiencies. However, the virtual doctor-patient relationship poses risks. Doctors will need to exercise caution to avoid misdiagnosis and to ensure that older or less tech-savvy patients remain able to access medical services.

17. Genomic technology will revolutionise medicine but patient expectations will require careful management

The UK is at the forefront of the use of genomics in healthcare. These allow a more targeted, effective and tailor-made approach to patient care based on the individual's needs. They can lead to early diagnosis or even the prevention of medical conditions. But genomics may raise patient expectations and when expectations are not met, litigation often ensues. As genomics play a larger role in healthcare, questions relevant to medical negligence liability will start to shift from 'why didn't you diagnose my condition?' to 'why didn't you prevent my condition from developing in the first place?' This potentially broadens the scope of liability in the med-mal arena.

18. Data-driven technology will improve healthcare but cyber security and data theft remains an ongoing challenge

The healthcare industry is rapidly onboarding technologies to improve operational efficiencies and deliver better patient-centric care. Both artificial intelligence (AI) and genomics rely on the generation of big data for algorithms and prediction models, but this comes with data integrity risks. Cyber security, data misuse (such as discrimination between population subsets) and data privacy claims are on the rise and remain a challenge for the industry. The availability of clinician performance data, while promoting transparency and the evaluation of healthcare quality, also creates litigation risk and the need for bespoke insurance covers supported by individualised ratings.

MOTOR

19. The brakes will be put on automated lane keeping systems

Despite the UK Government's appetite to find a first use case for automated driving under Part 1 of the Automated and Electric Vehicles Act 2018 in the form of automated lane keeping systems (ALKS), concerns have been voiced by industry stakeholders about the safe deployment of these technologies under the current UN-ECE Regulation 157 which does not allow for lateral movements out of lane. The Department for Transport's Centre for Connected and Autonomous Vehicles recently announced that Thatcham Research and Zenzic are working on a proof of concept for an Automated Driving System Consumer Rating to be delivered in the Spring of 2022. We do not expect the Secretary of State for Transport to list any vehicles as automated any time soon, nor do we expect manufacturers to release ALKS vehicles for use on UK roads before late 2022 at the earliest.

20. Expect more automated evidence gathering in low value claims

Part of the widespread reform around the management of low value whiplash claims was the introduction of the Official Injury Claim portal, designed to simplify the process and reduce the costs associated with soft tissue injuries arising out of road traffic accidents. Under the new rules, insurers must upload a compliant signed statement from their driver to the portal within 30 working days if they wish to dispute liability, failing which they will be deemed to admit. Expect to see new digital solutions that use automation to speed up the collation of evidence in portal claims, such as the Automated Compiling of Evidence solution jointly developed by DAC Beachcroft and Automated Insurance Solutions.

21. New legislation for electric scooters in Ireland

The legalising of e-scooters in Ireland will create new underwriting opportunity. Currently under Irish law, the use of electric scooters is not specifically regulated and by default is covered under the Road Traffic Act 1961. In an attempt to formally legalise their use, the Irish Government is set to enact new legislation in the form of the Road Traffic (Miscellaneous Provisions) Bill. The Bill would create a new vehicle category called Powered Personal Transporters (PPTs) that would not need a driving licence, tax or insurance. It is expected that a significant number of e-scooter service providers will start to operate rental services in major towns and cities. This will create an opportunity for insurers who can underwrite schemes for e-scooter sharing platforms and provide personal accident products without the requirement to have regard to road traffic legislation and regulations. In the UK, e-scooter trials are already in operation as part of the Government's strategy to tackle both the future and green mobility agendas, with legislation expected to follow an analysis of the data collected. It remains to be seen if the UK Government will follow Ireland's lead in legislating to legalise private e-scooters akin to electrically assisted pedal cycles (e-bikes), without mandating the provision of insurance against third party liabilities, nor the use of helmets.
Contributed by our Dublin office.

22. Electric vehicles heading for repair capacity crunch

The Institute of the Motor Industry predicts that by 2030 the UK will need around 90,000 qualified technicians to service the rapid growth of electric vehicles (EV) as the government ban on the sale of new petrol and diesel vehicles from 2030 – and hybrids from 2035 – approaches. Based on current growth estimates, there could be a shortfall of 35,700 technicians trained to handle EV. With the technology constantly evolving, the challenge of ensuring enough skilled repair technicians are available can only grow. Scarcity of skilled labour is pushing up repair costs, already higher because of the complexity of the vehicles. The cost of EV claims is also influenced by repair delays, with an EV repair taking significantly longer to complete than one on a vehicle with an internal combustion engine. Insurers are rushing to collect data to help them rate EVs more accurately but they need to be sensitive to the public policy demands to encourage EV.

PRODUCT SAFETY, LIABILITY AND RECALL

23. As new liability risks emerge, is unintended "coverage creep" inevitable?

The information age has allowed rapid global communications and networking to re-shape modern society. Loss of control over global supply matrices, the interaction between tangible products and digital services, and the environmental impact of global manufacturing give rise to new liability exposures for insurers. At the same time, the inability of regulation to keep abreast of such developments, coupled with heightened social expectation, is leading to more litigation and claims inflation. It is increasingly the case that companies are incurring liabilities they had not envisaged and liability insurers are being called upon to respond to losses which were not anticipated by underwriters or reflected in the premium. Learning lessons from silent cyber and the COVID-19 pandemic, general liability underwriters need to move towards more explicit affirmative coverage for catastrophic risks, or to tighten up contract wordings so that they clearly articulate underwriting intent. This should focus on clarifying insuring agreement clauses and definitions as much as policy exclusions. At the same time as achieving contract certainty, liability insurers need to develop new ways of assessing and managing risk if they are to deliver the claims certainty that global corporate policyholders are seeking in these unpredictable times.

24. AI, updates, law outdated?

Our current legislation is unfit for the digital age. With smart products being less tangible, reliant on digital content and artificial intelligence (AI), are product laws keeping up? The UK Product Safety Review is underway. The Consumer Rights Act has addressed the quality of digital content since 2015. But fundamental legal obligations about safety and quality still sit more easily with traditional tangible products. Expect the debate to move to whether tech products, reliant on software updates and algorithms, are more like services, currently unregulated in product safety terms. New legislation is required to address who consumers can look to for redress in the digital age. Where consumers are effectively buying experiences more than tangible products, where AI enables products to self-learn and consumers can produce 3D printed products, the law will still need to ensure safety and predictability for consumers and businesses alike.

PROFESSIONAL INDEMNTIY

25. Solicitors: Solicitors need to "up their game" on technological advances

Many law firms are running to keep up with technological advances as many of the tools now available in this sector add genuine value for clients. Blockchain, cryptocurrency and the courts' focus on IT means that law and tech increasingly go hand in hand. The Master of the Rolls has stated that solicitors need to "up their game" in this area as his focus will be on the use of portals and extending the types of cases to which the portal will apply. Innovation is therefore increasingly on firms' agendas but, once again, "new" can often create risk, unless handled with appropriate care. What happens if and when the tech fails? Tech unfortunately inevitably creates risk and uncertainties as to where liability lies as well as opportunities. Finally, as a profession we should not allow smaller firms whose ability to invest in technology is more limited to be left behind. Freedom of choice is an important issue and a key element of our justice system. It may not, however, be easy for all to ensure they keep up to speed.

26. Technology Professionals: Rise in tech E&O claims based on cyber incidents expected

We anticipate an increase in claims against IT professionals arising from their involvement in the design, maintenance or implementation of IT infrastructure that has been subject to data breaches and/or ransomware attacks. The recent dramatic increase in these attacks and their financial impact on organisations (including significant breach response costs and potential ransom payments) means that those entities that have suffered attacks and/or their insurers are likely to seek recovery from third parties involved with the IT infrastructure. This might be based on allegations that security considerations were not, or not adequately, factored into the service provision or that the systems lacked sufficient protections to withstand attacks.

PROPERTY

27. Smart tech is only part of the solution for cities

Cities will need to marry an improving investment in smart technology with better planning, mapping and an understanding of the built environment in order to avoid future climate disasters. It was encouraging to hear Sadiq Khan, Mayor of London, highlight at COP26 that our cities are leading the way for national governments to follow, proving to be more nimble, progressive and responsive. However, while measuring footfall, rainfall, ground stability or pollution is a great step forward, it is not the whole solution. We are still seeing serious flooding in our cities, so now we need to join up the data with real action on response planning specific to each location. As shown in our thought leadership on the interconnectivity of solutions, a co-ordinated response with structured goals is the key to real results.

REINSURANCE

28. Cyber war exclusions – new clause now published

Cyber risks have continued to escalate, with particular focus on increasing ransom demands and new modes of attack. Insurers have escaped an attack on a scale similar to NotPetya in 2017, but no-one seriously doubts the threat of a serious event of equal or greater magnitude. State sponsored attacks, whether in the course of kinetic conflict, or more akin to state-sponsored terrorism, remain a serious concern with a number of nation states actively encouraging cyber criminals or turning a blind eye to their activities. In either case, the cyber war and cyber operations of criminals are systemic risks which the market should limit or exclude. Over the last two years, the Lloyd's Market Association has reviewed the prevailing war exclusion, NMA464, drafted long before cyber risk became a daily part of business life. We worked with the LMA committee on this exercise. Drafting the new exclusion raised challenging issues, such as threshold and attribution. The clauses were published in late November and the rate of take-up will be interesting to monitor. We anticipate further clauses emerging, adding further refinements, as the nature of cyber risk evolves.